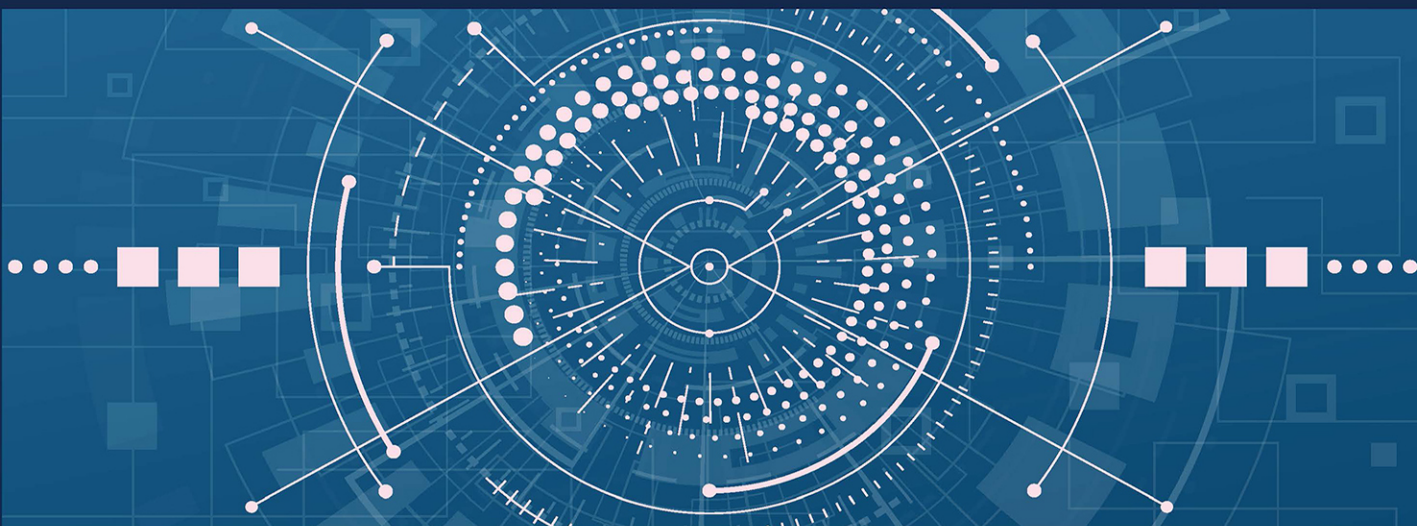


Cyber Defense for the Hybrid Enterprise in the Age of AI

Zero Trust and the Anatomy of Cyber Breaches



ciscopress.com

LUIS MATOS
CCIE X5 (RS, SP, DC, VC, SEC) No. 17528

FREE SAMPLE CHAPTER |



Cyber Defense for the Hybrid Enterprise in the Age of AI

Zero Trust and the Anatomy of Cyber Breaches

Luis Matos

CCIE No. 17528

Cyber Defense for the Hybrid Enterprise in the Age of AI

Luis Matos

Copyright© 2027 Cisco Systems, Inc.

Published by:

Cisco Press

Hoboken, New Jersey

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit <https://www.pearson.com/global-permission-granting.html>.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Please contact us with concerns about any potential bias at www.pearson.com/en-us/report-bias.html.

\$PrintCode

Library of Congress Control Number: 2026944107

ISBN-13: 978-0-13-547277-4

ISBN-10: 0-13-547277-6

Warning and Disclaimer

This book is designed to provide information about digital security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates. Other company names, product names, logos, and marks referenced in this publication are the property of their respective owners and are used for identification and educational purposes only. Use of these names, logos, and marks does not imply affiliation with, endorsement by, or sponsorship from their respective owners.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

Head of IT & Professional Learning, Enterprise Learning and Skills: Julie Phifer

Alliances Manager, Cisco Press: Caroline Antonio

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Christopher A. Cleveland

Senior Project Editor: Mandie Frank

Copy Editor: Kitty Wilson

Technical Editors: Naiguel Clemente, Flavio Costa, Vagner Silva

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Brad Herriman

Proofreader: Barbara Mack



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

About the Author

Luis Matos, CCIEx5, is a Principal Architect in Cisco's CX Advanced Services organization for the LATAM region, bringing more than 26 years of experience in cybersecurity and networking, including over 23 years as a university professor at several national institutions. Throughout his career, he has specialized in designing and implementing complex solutions for data centers, Internet/MPLS backbones, and enterprise security architectures, with a strong focus on telecommunications providers, large financial institutions, airports, and critical infrastructures.

Luis served as the technical lead for the security team during the Rio 2016 Olympic Games and also worked as a security consultant for the Toronto 2015 Pan American Games. Over the years, he has participated in strategic projects involving Zero Trust architectures, segmentation, fraud prevention, ransomware defense, behavioral analytics, and large-scale hybrid security infrastructures across Latin America.

A recognized speaker and cybersecurity specialist, Luis frequently presents technical sessions at Cisco events, IEEE conferences, universities, and industry forums, in addition to participating in interviews with major broadcast television networks and media organizations across LATAM. He is also actively involved in cybersecurity education initiatives, including presentations for public schools and Cisco Networking Academy programs, helping inspire and develop the next generation of technology professionals.

Luis holds multiple industry certifications in networking, security, and software development, including CCIE (Enterprise Infrastructure, Service Provider, Security, Voice, and Data Center), DevNet, CCNP, CCNA, CCDA, IPv6 Gold, MCP, MCP+Internet, and MCSE.

About the Technical Reviewers

Flávio Augusto Corrêa da Costa is a Brazilian cybersecurity specialist with 18 years of experience in networking, security architecture, cyber defense, threat detection, and incident response. He previously spent nearly a decade at Cisco and is an alumnus of Cisco's Sales Associate Program (CSAP). His ransomware research contributed to MITRE ATT&CK and has been referenced by the FBI and CISA. Flávio is an author, university professor, cybersecurity instructor, and CompTIA Subject Matter Expert (SME). He holds three MBA degrees covering Cybersecurity, IT Infrastructure Architecture, and Artificial Intelligence and Data Science, in addition to postgraduate studies in Cyber Defense. His certifications include Cisco CCNP Enterprise, CCNP Security and CyberOps, together with CompTIA A+, Network+, Cloud+, Security+, CySA+, PenTest+, and CASP+/SecurityX, as well as EC-Council C|CISO, E|CSA and (ISC)² CC.

Naiguel Clemente is a Brazilian Security Consulting Engineer with nearly two decades of experience in the technology industry. He began his career in service provider network operations before transitioning to cybersecurity, where he has helped organizations design, implement, and optimize Cisco security solutions. He currently serves as a Security Consulting Engineer with Cisco CX LATAM, supporting some of the region's largest financial institutions in designing and delivering advanced cybersecurity solutions. Over the course of his career, he has developed deep expertise in enterprise security architectures, large-scale deployments, and security operations for highly regulated environments. His areas of expertise include Cisco security technologies, with a strong focus on Cisco Identity Services Engine (ISE) and Cisco Secure Network Analytics (SNA). Naiguel studied Computer Networks at Universidade Nove de Julho (UNINOVE) and is currently pursuing a degree in Computer Science at Universidade Presbiteriana Mackenzie. He holds Cisco CCNA and CCNP Security certifications.

Vagner Silva, CCIE No 59752, is a Brazilian Security Solutions Engineer with more than two decades of experience in Information Technology, including more than 15 years specializing in cybersecurity. Throughout his career, he has progressed from Security Analyst to Information Security Director, designing, implementing, and delivering enterprise cybersecurity solutions for organizations across multiple industries. His expertise spans Security Operations, Network Security, Identity and Access Management (IAM), Zero Trust, Secure Access Service Edge (SASE), cloud security, and enterprise security architecture. Vagner holds a degree in Computer Networks from FIAP and two postgraduate specializations: Cybersecurity and Cyber Intelligence from Universidade Presbiteriana Mackenzie and Cyber Threat Intelligence from Daryus Educação. He has earned several industry-recognized certifications, including Cisco CCIE Security, Certified Ethical Hacker (CEH), CompTIA Security+, and CompTIA CySA+. In addition to his industry experience, Vagner has served as a cybersecurity instructor, delivering specialized technical training and helping IT professionals develop practical expertise in modern security technologies, best practices, and cyber defense strategies.

Dedications

To my parents, Marina and Agnaldo: Thank you for being the foundation upon which my entire life was built. Your love, sacrifices, guidance, and constant encouragement taught me the importance of discipline, humility, perseverance, and integrity. Every achievement in my life reflects the values you instilled in me from the very beginning. I will always carry your teachings with pride and gratitude.

To my wife, Margot: Thank you for standing beside me through every challenge, every sacrifice, and every long night dedicated to this project. Your support, patience, and understanding gave me the strength to continue when the journey felt overwhelming. You believed in me even during moments when I doubted myself, and your presence transformed difficult times into manageable ones. This accomplishment is as much yours as it is mine.

To my son, Arthur: You are my greatest inspiration and the reason I always strive to become a better man every single day. Your smile, your energy, and the way you look at me with admiration give purpose to everything I do. Thank you for motivating me to keep moving forward and for allowing me to be your “GOAT.” That title means more to me than any professional achievement ever could.

Acknowledgments

First and foremost, I would like to express my sincere gratitude to my leader at Cisco, Alex Gonzalez, who, two years ago, asked the simple question that ultimately became the beginning of this entire journey: “Why don’t you write a book?” What initially sounded like a casual conversation eventually became the spark that encouraged me to embrace one of the greatest challenges of my professional life. Truly great leaders often transform people not only through strategy, direction, or technical guidance but through the right questions asked at exactly the right moment—sometimes without even realizing the profound impact those words have.

I would also like to thank those who have stood beside me throughout my professional journey: Ana Rider, Renata Macedo, Naiguel Clemente, Rogério Freitas, Paulo Magalhães, Henrique Monjardim, Daniel Dobrioglo, and Gustavo Garcia. Every challenge I have overcome and every milestone I have achieved have been possible because of our hard work and also because of your friendship, support, encouragement, and trust along the way.

Writing a book that covers such a wide range of technologies and security domains would not have been possible without the support of several brilliant professionals. I would like to express my special gratitude to Naiguel Clemente (SNA), Thomas Howard (ISE), Renan Hingel (Secure Firewall), and Rodrigo Floriano (XDR) for generously dedicating your valuable time, sharing your expertise, and providing essential technical feedback throughout the development of this book.

Throughout this project, the technical reviewers contributed far beyond a traditional review process. They worked with the same level of dedication, attention, and commitment as true co-authors, treating this book as if it were their own project. And in many ways, it truly is partly yours as well. My sincere gratitude goes to Flavio Costa, Naiguel Clemente, and Vagner Silva for your incredible support, technical insight, and dedication throughout this journey.

And finally, I would also like to express my deepest appreciation to the Pearson team, especially James Manly, Christopher Cleveland, Mandie Frank, and Kitty Wilson, whose guidance, patience, and continuous support were invaluable throughout the development of this book. Their professionalism, encouragement, and dedication played an important role in transforming this project into reality.

Contents at a Glance

	About the Author	iv
	Introduction	xxvi
Chapter 1	The Evolution of Cyber Threats: Digital Fraud, Ransomware, and AI-Driven Attacks	1
Chapter 2	The Hackers' Modus Operandi: The Attack Anatomy	55
Chapter 3	The Security Journey: Business Strategy Alignment	111
Chapter 4	Mapping the Threat Landscape: A Strategic Approach to Network Security Assessments	151
Chapter 5	Field Validation: A Step-by-Step Case Study in Threat and Risk Assessment	193
Chapter 6	Inside the Insider Threat: How Fraudulent Devices Undermined a Bank's Defenses	263
Chapter 7	Behind the Scenes: The Setup of Fraudulent Devices	301
Chapter 8	The Live Attack: Showtime	339
Chapter 9	Strategic Foundations of Defense: Zero Trust, SAFE, and AI	371
Chapter 10	Identity and Access Control: Building Security with Cisco ISE	467
Chapter 11	East–West Defense: MACsec Encryption and TrustSec Microsegmentation	573
Chapter 12	North–South Defense: Secure Firewall and the Macrosegmentation Strategy	677
Chapter 13	Proactive Threat Defense: Leveraging NDR, XDR, and SIEM	749
	Index	897

Contents

	About the Author	iv
	Introduction	xxvi
Chapter 1	The Evolution of Cyber Threats: Digital Fraud, Ransomware, and AI-Driven Attacks	1
	A Call to Secure the Future	1
	The Rise of Digital Fraud and Ransomware Attacks: A Shifting Battlefield	4
	A Shifting Battlefield	4
	The Digital Fraud Techniques	5
	<i>Phishing and Spear Phishing: The Evolution of Deception</i>	5
	<i>Business Email Compromise (BEC): The Billion-Dollar Scam</i>	6
	<i>Deepfake Scams: AI-Generated Fraud at Scale</i>	6
	<i>Synthetic Identity Fraud: The Invisible Cybercriminals</i>	6
	<i>Account Takeover (ATO) Attacks: The Silent Hijacking</i>	7
	<i>Hacking Manipulation: Exploiting Individuals Through Social Engineering</i>	8
	The Psychology Behind Social Engineering: How Cybercriminals Exploit Human Nature	9
	Understanding Human Vulnerabilities in Cybersecurity	10
	Case Study: The Deepfake CEO Fraud	10
	<i>How the Attack Was Executed</i>	10
	<i>Lessons Learned</i>	11
	Ransomware from Simple Lockers to Organized Crime: The Rise of Ransomware-as-a-Service (RaaS)	13
	The Expansion of RaaS Beyond Traditional Targets	13
	Ransomware and Cyberattacks on Critical Infrastructure	14
	<i>The Colonial Pipeline Attack: A Wake-Up Call for Critical Infrastructure Security</i>	14
	<i>Cyber Warfare: The Ukrainian Power Grid Attacks</i>	16
	<i>The Triton/Trisis Attack: Cyber Threats to Industrial Safety Systems</i>	17
	Ransomware in the Healthcare Sector	18
	<i>WannaCry Against Healthcare: The Global Ransomware Pandemic</i>	19
	<i>Universal Health Services Ransomware Attack: A Healthcare Network Paralyzed</i>	20
	<i>Springhill Medical Center Attack: When Ransomware Becomes Fatal</i>	21

Ransomware in Government	23
<i>The Atlanta Ransomware Attack: A City Paralyzed</i>	23
<i>The Baltimore Ransomware Crisis: A Government Held Hostage</i>	25
<i>The Argentina National Government Attack: A Digital Lockdown</i>	25
<i>The Washington, DC Police Department Attack: Ransomware Meets Extortion</i>	26
The Future of Ransomware: AI-Powered and Nation-State–Backed Attacks	27
AI-Driven Ransomware: The Next-Generation Cyber Threat	28
Ransomware as a Geopolitical Weapon	29
Ransomware in Smart Cities and IoT Ecosystems	30
The Expanding AI/ML Target: Ransomware in AI and Machine Learning	31
Defense Strategies: Preparing for the Future of Ransomware	31
AI-Powered Threats: The Next Frontier of Cyber Warfare	32
<i>The Rise of AI-Powered Cyberattacks</i>	33
<i>The Future of Cybersecurity in the AI Era</i>	35
Defending the New AI Era: How Cisco AI Defense Mitigates Emerging Cyber Threats	35
<i>The Core Capabilities of Cisco AI Defense</i>	36
<i>The Role of AI in Strengthening Cybersecurity</i>	37
The AI in Cybersecurity: Workforce Adaptation and the Skills Gap	38
<i>Expanding the Security Talent Pool: Beyond Traditional Qualifications</i>	39
<i>AI and Cybersecurity Unified Defense Strategy</i>	39
<i>The Future of Cyber Threats and Defensive Strategies</i>	40
<i>The Next Evolution of Cybersecurity Challenges</i>	41
<i>Strengthening Cyber Defenses</i>	41
Key Tactics Used by Cybercriminals	42
AI-Enhanced Phishing and Social Engineering	42
The Rise of Cybercrime-as-a-Service (CaaS)	43
Supply Chain Exploitation: The Weakest Link in Cybersecurity	43
<i>Lessons Learned: Strengthening Cyber Resilience</i>	43
Insider Threats: The Enemy Within	44
Types of Insider Threats	45
Real-World Examples of Insider Threats	46
The Economic Impact of Cybercrime on Businesses, Financial Institutions, and Individuals	46

Financial and Operational Disruptions	47
Regulatory Compliance and Cyber Insurance Challenges	47
Understanding the Cybercriminal Economy: Key Trends and Statistics	47
Understanding Cybercriminal Motivations and Attack Vectors	48
The Most Common Attack Vectors	49
Summary	49
Lessons Learned	50
References in This Chapter	52
Chapter 2 The Hackers' Modus Operandi: The Attack Anatomy	55
Step-by-Step Breakdown: A Call to an Old Friend	55
Cybercrime Group Organization, Structure, Roles, and Law Enforcement Countermeasures	57
The Organizational Structure of Cybercrime Groups	58
Sophisticated Attacks on Financial Institutions	60
On-Path Attacks with Fraudulent Devices in LATAM Banks	61
<i>Attack Breakdown</i>	63
<i>Security Implications</i>	64
Case Study: Fraudulent Devices on the Wire	64
<i>How the Attacks Were Executed</i>	65
<i>Lessons Learned</i>	66
Law Enforcement Tactics: How Authorities Track and Dismantle Cybercrime Networks	67
Investigative Techniques Against Cybercrime	68
<i>Cyber Threat Intelligence and Honeypots</i>	68
<i>Undercover Operations and Dark Web Surveillance</i>	68
<i>Blockchain Analysis and Cryptocurrency Tracing</i>	69
<i>International Cooperation and Joint Task Forces</i>	69
<i>Arresting Key Members and Seizing Infrastructure</i>	70
<i>Public–Private Partnerships</i>	70
The Future of Cybercrime and Law Enforcement Strategies	70
The Role of AI in Cybercrime and Law Enforcement	71
Blockchain Forensics to Trace Criminal Transactions	72
The Global Collaboration Against Cybercrime	73
Strengthening Cybersecurity for Businesses and Individuals	74
Understanding Attacker Movement Inside Enterprise Networks	74
Reconnaissance and Information Gathering	75

Establishing Persistence and Remaining Undetected	76
Evasion Tactics: Avoiding Detection and Security Controls	77
Anti-Forensics and Evidence Elimination Techniques	79
<i>File and Disk Wiping Techniques</i>	80
<i>Memory Manipulation and Process Injection</i>	80
<i>Source Address Manipulation</i>	80
<i>Self-Destructing Malware and Kill Switches</i>	81
<i>The Role of AI and Automation in Evidence Destruction</i>	82
Countering Evidence Destruction: The Forensic Response	82
Automating Evidence Analysis in the AI Era	83
The Hacker's Toolbox: Cybercriminals Find Their Tools and Use Them	84
The Rise of Open-Source Hacking Tools	84
The Dark Web and the Black Market for Hacking Tools	85
The Growth of Cybercrime-as-a-Service	85
The Legal and Ethical Landscape of Hacking Tools	86
<i>United States: Computer Fraud and Abuse Act (CFAA)</i>	86
<i>European Union: General Data Protection Regulation (GDPR)</i>	87
<i>Ethical Hacking and Modern Defense Operations</i>	88
Hactivism, Cyber Terrorism, and Nation-State Operations	89
The Rise of Hactivism: The Era of Digital Protest	90
Cyber Terrorism: Digital Weapons in the Hands of Extremists	91
Nation-State Cyber Operations: The Silent War in Cyberspace	91
The Future of Cyber Conflict	92
The Underground Economy	92
How Hackers Profit from Cybercrime	93
<i>Stolen Credentials and Data Leaks</i>	93
<i>The Global Fight Against Cybercrime</i>	94
<i>Money Laundering and Financial Fraud</i>	94
Law Enforcement and Regulatory Responses	96
Foundations of Security Frameworks	97
The Cyber Kill Chain Model	97
<i>The History and Evolution of the Cyber Kill Chain Framework</i>	98
<i>The Seven Phases of the Cyber Kill Chain</i>	99
The MITRE ATT&CK Framework	102
<i>Adversary Tactics, Techniques, and Procedures</i>	103
<i>Mapping Cybercriminal Behavior</i>	104

	The DETT&CT Framework	104
	The RE&ACT Framework	105
	Summary	107
	Lessons Learned	108
	References in This Chapter	110
Chapter 3	The Security Journey: Business Strategy Alignment	111
	A Change in Perspective	111
	The Security Strategy Roadmap	113
	Define Business Outcomes	114
	Identify Technical Domains	116
	Select Strategic Frameworks, Knowledge Bases, Standards, and Regulations	117
	Map Strategy to Solutions	118
	Map Solutions to Services	120
	Establish KPIs and Governance	122
	<i>Business-Focused KPIs</i>	123
	<i>Technical KPIs</i>	124
	<i>Governance Models</i>	125
	Translating Security Requirements into Solutions	126
	Core Components of Zero Trust Architecture (ZTA)	127
	Understanding the Core ZTA Components	128
	Supporting Capabilities and Technologies	128
	Translating Security Requirements into Risk	130
	How Effective Cybersecurity Supports Risk Management and Brand Protection	131
	From Reactive Defense to a Living Security Strategy	132
	Executive Engagement: Governance and Strategy	132
	Evolving Security with the Business: A Living Strategy	134
	Building the Business Case: Regulatory Compliance and Strategic Alignment	135
	Cybersecurity Return on Investment (ROI)	137
	Understanding ROI in a Security Context	138
	Calculating Cybersecurity ROI: A Practical Model	140
	<i>Step 1: Estimate the Annual Loss Expectancy (ALE)</i>	140
	<i>Step 2: Calculate the Cost of the Prevention Strategy</i>	141
	<i>Step 3: Estimate the Risk Reduction (RR)</i>	141

<i>Step 4: Apply the ROSI Formula</i>	142
<i>Making ROSI Visible to Stakeholders</i>	142
Case Study: ACME Petroleum OT Infrastructure	142
ROSI Calculation for ACME Petroleum	143
<i>Step-by-Step Breakdown</i>	143
Strategic Interpretation for Executives	145
Summary	146
Lessons Learned	147
References in This Chapter	148

Chapter 4 Mapping the Threat Landscape: A Strategic Approach to Network Security Assessments 151

Revealing the Unknown	151
The Strategic Zero Trust Readiness Assessment: A Framework to Start a Zero Trust Journey	155
Step 1: Mapping the Network to Technical Domains (Protect Surfaces)	157
Step 2: Mapping the Technical Domains to Security Frameworks and Methodologies	159
Step 3: Conducting the Interview Process Based on Control Areas	161
Step 4: Evaluating the Technical Domains Maturity Level	162
Step 5: Evaluating the Technical Domains' Risks and Severities	164
Step 6: Mapping the Technical Domains' Risks to MITRE ATT&CK TTPs	166
Step 7: Mapping Business Flows to Cisco SAFE	167
Step 8: Building the Roadmap	168
Zero Trust Network Assessment Blueprint: Details of the Process	169
Baseline: Mapping the Network to Technical Domains	171
Baseline: Mapping Technical Domains to Zero Trust Frameworks	173
<i>Mapping Technical Domains to the CISA Zero Trust Framework</i>	173
<i>Mapping Technical Domains to the NIST 1800-35B Zero Trust Architecture</i>	175
Analyze: The Maturity Level and Risk Severity Evaluation	177
<i>Maturity Level Evaluation: CISA 2.0</i>	178
<i>Risk Severity Evaluation: NIST SP 800-30, Risk Heat Matrix, and MITRE ATT&CK</i>	180
<i>Executive Risk Summary: Heat Map Calculation</i>	181
Recommend: Mapping the Business Flows to Cisco SAFE	183

	Recommend: Mapping SAFE Capabilities to Zero Trust Core Components	185
	Summary	188
	Lessons Learned	189
	References in This Chapter	190
Chapter 5	Field Validation: A Step-by-Step Case Study in Threat and Risk Assessment	193
	Turning Strategy into Execution: Stepping Out of the Shadows	193
	ACME Bank Case Study: Strategic Zero Trust Network Architecture Assessment	194
	Project Kickoff: Defining the Scope and Methodology	196
	<i>The Assessment Scope</i>	196
	<i>The Assessment Methodology</i>	197
	The Five-Phase Security Lifecycle Approach	198
	Security Baseline Phase	198
	<i>Mapping the Enterprise Network Architecture to Technical Domains</i>	199
	Environment Analysis Phase	203
	<i>Gaining Insight into the Current State</i>	204
	<i>Applying Control Area Reviews to Assess Zero Trust Maturity</i>	215
	<i>Evaluate the Current Maturity Level</i>	236
	<i>Evaluate Key Findings and Gaps</i>	239
	Evaluate the Current Risk Severity	245
	Recommend Phase	249
	<i>Building the Three-Year Roadmap</i>	249
	Execute Phase	253
	<i>Using MITRE ATT&CK Techniques to Enhance SOC Operations</i>	253
	Measure Phase	257
	<i>Measuring Security Performance Through KPIs</i>	257
	Summary	259
	Lessons Learned	260
	References in This Chapter	261
Chapter 6	Inside the Insider Threat: How Fraudulent Devices Undermined a Bank's Defenses	263
	The Insider Actor Recruitment: Planting the Seed of Betrayal	263
	The Proposition	263
	The Dilemma	265

The Call	266
The Handoff	267
The Installation	269
Exposing the Weaknesses of Wired Corporate LANs	270
The Evolution of 802.1x Attacks over Two Decades	271
<i>Early Generations (2001–2005): LAN and WLAN Bypasses</i>	271
<i>The Rise of Encryption Challenges (2008–2011): MACsec and Bridge Attacks</i>	274
<i>The 802.1x Authentication Weakness (2012–2016): Protocols Exposed</i>	277
<i>Advanced Exploits (2017–2020): Packet Injection and Defeating MACsec</i>	280
<i>The Emerging Threat (2023–2024): Undetected Mobile Access</i>	285
Fraudulent Device Attacks: Generations and Evolution	287
<i>Fraudulent Device Attacks: The Old Generation</i>	288
<i>Fraudulent Device Attacks: The New Generation</i>	289
Summary	296
Lessons Learned	297
References in This Chapter	299

Chapter 7 Behind the Scenes: The Setup of Fraudulent Devices 301

Fraudulent Devices Exposed	301
Chupacabra Rising	303
Fraudulent Devices in Action	304
Case Study: How Fraudulent Devices Penetrated a State-Owned Financial Giant	304
Case Study: Fraudulent Device Exploitation at a Prominent State-Owned Bank	305
Key Takeaways from the Case	305
Configuring a Fraudulent Device for Attack	306
<i>Requirements for the Attack Topology</i>	308
<i>Step 1: Perform a Configuration Reset</i>	309
<i>Step 2: Configure the Fraudulent Device</i>	310
<i>Step 3: Configure the Management Bridge</i>	316
<i>Step 4: Configure the Attack Bridge</i>	319
<i>Step 5: Configure the 4G/5G LTE Interface</i>	320
<i>Step 6: Configure the L2TP Remote Access VPN</i>	328

Summary	335
Lessons Learned	335
References in This Chapter	337

Chapter 8 The Live Attack: Showtime 339

The Deal Was Sealed	339
The Attack Execution: Assuming the Victim's Identity	340
Step 1: Gain Remote Tunnel Access	341
<i>Step 1a: Configure the Windows PPTP VPN Client</i>	341
<i>Step 1b: Configure the Client VPN Connection</i>	342
Step 2: Identify the Victim Endpoint's Network Addresses	344
Step 3: Clone the Victim Endpoint's IP and MAC Addresses	346
<i>Step 3a: Assign the Victim's MAC Address to Interface ether1</i>	346
<i>Step 3b: Assign the Victim's IP Address to Interface ether1</i>	347
The Attack Execution: When Security Fails to See the Deception	348
Inside the Access Switch: The Invisible Guest	348
The Human Breach: The Insider's Dilemma	352
Borderless Security: No Firewall Can Stop a Desperate Heart	353
The Money Mules: The Human Conveyor Belt	357
Who They Are	357
Recruitment and Control	358
Modus Operandi: High Level, Non-Actionable	358
<i>The Mule Manager</i>	359
<i>The Human Logistics of Money Laundering</i>	359
<i>Indicators for Investigators</i>	360
Maria's Story: A Transaction of Desperation	360
Noise in the Network: When Skill Fails, Silence Breaks	361
The Enhancement for the Generation 7 On-Path Attack	361
Summary	366
Lessons Learned	367
References in This Chapter	370

Chapter 9 Strategic Foundations of Defense: Zero Trust, SAFE, and AI 371

The Counterattack: Building Digital Resilience	371
Zero Trust Principles Applied to Mitigate the Attack	373
NIST 800-207: Zero Trust Tenets	374
<i>Tenet 1: All Data Sources and Services as Resources</i>	374
<i>Tenet 2: Secure All Communications Regardless of Network Location</i>	374

<i>Tenet 3: Per-Session, Least-Privilege Access</i>	375
<i>Tenet 4: Dynamic Policy Based on Identity, Device, and Behavior</i>	375
<i>Tenet 5: Continuous Monitoring of Asset Integrity</i>	375
<i>Tenet 6: Dynamic Authentication and Authorization</i>	376
<i>Tenet 7: Intelligence-Driven Feedback and Policy Refinement</i>	376
Zero Trust Assumptions	376
Cisco SAFE: From Complexity to a Defensible Architecture	377
Translating SAFE into the ACME Bank Architecture	378
Cisco SAFE in Action: Applying the Three Phases	379
<i>Applying SAFE to the ACME Bank Incident</i>	379
<i>Closing the Gaps: SAFE Capabilities in Action</i>	380
<i>SAFE Defense by Place in the Network: The ACME Architecture Blueprint</i>	384
Integrating the PINs: Defense in Depth and Secure by Design	390
<i>SAFE Secure Domains That ACME Needed</i>	391
AI-Assisted Vulnerability Discovery: Exploration at Machine Speed	398
Project Glasswing	398
The Evolution from Human Speed to Machine Speed	399
<i>Uncovering Decades of Hidden Vulnerabilities</i>	405
<i>The AI-Assisted Vulnerability Lifecycle</i>	406
<i>Growth of Publicly Disclosed CVEs from 1999 Through the 2026 Forecast</i>	409
Defending Against Machine-Speed Threats	411
<i>The Vendor Domain: The Patch Development Cycle</i>	412
<i>The Attacker Domain: The Exploit Development Cycle</i>	412
<i>The Enterprise Domain: The Exposure Window</i>	413
<i>The AI-Driven Threat Defense Framework: Foundation Pillars</i>	414
<i>The End-of-Life Challenge</i>	419
<i>Zero Trust Capabilities as Continuous Protection</i>	419
<i>The AI-Driven Threat Defense Framework: From Principle to Implementation</i>	420
<i>Security at Machine Speed: From Prevention to Resilience</i>	423
<i>The Future Security Operations Center</i>	423
<i>Strategic Implications for Security Leaders</i>	425
Case Study: Using an AI-Assisted Vulnerability Discovery Tool	426
Lab: Environment Overview	427

Lab: Code Overview	428
<i>Vulnerability 1: SQL Injection in Authentication</i>	429
<i>Vulnerability 2: Authentication Bypass Through Trusting Client Headers</i>	430
<i>Vulnerability 3: Insecure Direct Object Reference (IDOR)</i>	431
<i>Vulnerability 4: SQL Injection in Administrative Search Functions</i>	432
<i>Vulnerability 5: Broken Administrative Authorization</i>	433
<i>Vulnerability 6: Business-Logic Flaw in Funds Transfers</i>	434
<i>Vulnerability 7: Improper Transaction Approval Workflow</i>	435
<i>Vulnerability 8: SQL Injection in Audit Logging</i>	436
Lab: AI Vulnerability Scanning Execution	437
<i>Preparing the Vulnerable Target</i>	437
<i>Framing the Assessment Task</i>	438
<i>Running the Scan</i>	440
Lab: Reviewing the Results	442
<i>Interpreting the Outcome</i>	444
<i>Conclusion</i>	446
AI-Driven Cyber Defense: Leveraging Machine Learning and Security LLMs Against Modern Threats	447
Following the Ghost in the Network: Mapping the Intrusion Path	448
Behavioral Profiling Analysis in Splunk	449
<i>Configuring the Splunk App for Behavioral Profiling</i>	449
Elevating SOC Operations with Security-Specialized LLMs	457
<i>Purpose-Built LLMs for Cybersecurity</i>	457
Case Study: Leveraging Foundation-Sec-8B to Investigate ACME Bank's Fraud Incident	459
Summary	463
Lessons Learned	463
References in This Chapter	465
Chapter 10 Identity and Access Control: Building Security with Cisco ISE	467
The Nemesis Revelation: Restoring Trust at the Access Layer	467
Designing a Zero Trust–Aligned Cisco ISE Architecture	469
ISE as the Identity Control Plane: NAC-Focused Scope	470
<i>Mapping Zero Trust PDP, PEP, and PIP Concepts to Cisco ISE Architecture</i>	470
ISE Deployment: Solution Sizing Calculation	471

<i>Sizing Calculation: ISE Deployment Model</i>	472
<i>Sizing Calculation: SNS Physical Hardware Profile</i>	473
<i>Sizing the PANs: Calculation Method and Recommended Hardware/VM Profiles</i>	476
<i>Sizing the MnTs: Calculation Method and Recommended Hardware/VM Profiles</i>	476
<i>Sizing the pxGrids: Calculation Method and Recommended Hardware/VM Profiles</i>	477
<i>Sizing the PSNs: Calculation Method and Recommended Hardware/VM Profiles</i>	481
<i>Estimate Transactions per Second: TPS Requirement</i>	483
<i>PSN Sizing per Country: Poisson-Based Method</i>	484
<i>ISE Deployment: PSN Node Distribution and Redundancy</i>	488
<i>ISE Deployment: Dot1x Supplicant Selection</i>	491
<i>The Role of the Supplicant in Zero Trust Access Control</i>	492
<i>Supplicant Selection by Access Type</i>	492
<i>ISE Deployment: Licensing Model</i>	496
<i>Cisco Secure Client Licensing Fundamentals</i>	497
<i>Cisco Secure Client Licensing Calculation</i>	501
<i>Cisco ISE Licensing Fundamentals</i>	503
<i>Cisco ISE Smart Licensing and Compliance</i>	504
<i>Cisco ISE Licensing Calculation</i>	504
<i>Case Study: Licensing Calculation for ACME Bank</i>	505
<i>ISE Deployment: Use Cases</i>	506
<i>Use Case 1: Allowlist Devices</i>	508
<i>Use Case 2: Denylist Devices</i>	509
<i>Use Case 3: Quarantine Devices</i>	510
<i>Use Case 4: Corporate Workstation (Wired)</i>	511
<i>Use Case 5: Corporate Printer (Lexmark)</i>	514
<i>Use Case 6: Corporate Printer (Legacy)</i>	516
<i>Use Case 7: Corporate IP Phone</i>	517
<i>Use Case 8: Corporate Telepresence</i>	519
<i>Use Case 9: IoT Security Camera</i>	520
<i>Use Case 10: IoT Security Alarm</i>	521
<i>Use Case 11: Corporate Workstation (Wireless)</i>	522
<i>Use Case 12: Corporate Mobile Device</i>	525
<i>Use Case 13: BYOD Mobile</i>	527

<i>Use Case 14: Guest</i>	530
<i>Use Case 15: Corporate Workstation (VPN)</i>	531
<i>Use Case 16: Access Points</i>	534
<i>Use Case 17: Access Points Onboarding</i>	539
IoT Devices: The Authentication Challenge	542
<i>Challenges in Traditional IoT Deployments</i>	542
<i>Device-Led Authentication Limitations</i>	543
<i>IoT Device Authentication: No-Gratuitous-ARP Authentication Problem</i>	543
<i>IoT Device Authentication: Best Practices</i>	544
Network and ISE Segmentation: BYOD and Guest	545
<i>Network Segmentation</i>	546
<i>Public Digital Certificates</i>	548
<i>ISE Segmentation</i>	548
<i>Guest-Access Legal Responsibilities: Brazil and the United States</i>	553
ISE Integrations: Active Directory and Load Balancer	554
<i>Active Directory Integration</i>	555
<i>Load Balancer Integration</i>	562
Summary	569
Lessons Learned	569
References in This Chapter	572

Chapter 11 East–West Defense: MACsec Encryption and TrustSec Microsegmentation 573

When the Enemy Moves in Silence: Thinking Like the Attacker Inside the Network	573
Microsegmentation in Context: Granularity, Scope, and Control	575
Segmentation: Practical Examples	576
<i>Example 1: Data Center Intersegment Enforcement</i>	576
<i>Example 2: Internet Edge Intersegment Enforcement</i>	577
<i>Example 3: Data Center Intrasegment Enforcement</i>	578
<i>Example 4: LAN Intrasegment Enforcement</i>	579
<i>Practical Examples Summary</i>	579
Introducing TrustSec: Identity as the Basis for Segmentation	580
Case Study: ACME Bank Microsegmentation Project	582
PDI Methodology Introduction	582
PDI Approach with Zero Trust Guidance	583
<i>Plan Phase: Scoping, Assumptions, and Risk Definition</i>	584

<i>Design Phase: Policy Modeling, Architecture, and Enforcement Strategy</i>	587
<i>Implement Phase: TrustSec Policy Deployment, Enforcement, and Operational Validation</i>	602
<i>Validating TrustSec Policy Enforcement</i>	622
<i>MTU Considerations with TrustSec Inline Tagging</i>	623
MACsec: Establishing Trust and Confidentiality	629
Cryptographic Protection at the First Hop	631
MACsec Pre-deployment	633
MACsec Deployment	634
<i>Step 1 (Switch): Configure the MACsec Feature</i>	635
<i>Step 2 (ISE): Configure Authorization Rules and Profiles</i>	637
<i>Step 3 (Switch): Validate MACsec Operational Status</i>	638
<i>Step 4 (Secure Client): Configure Secure Client XML</i>	642
<i>MACsec Security Levels and Fallback Behavior</i>	642
<i>MTU Considerations with MACsec</i>	645
<i>MACsec Encapsulation and Frame Overhead (Byte-Level View)</i>	646
OT Segmentation Strategy: From Purdue Architecture to Zero Trust Enforcement	647
Designing OT Segmentation: Purdue, ISA/IEC 62443, and NIST SP 800-207	649
<i>Understanding the Purdue Model's Role in OT Security</i>	650
<i>ISA/IEC 62443: Enabling OT Macrosegmentation Through Zones and Conduits</i>	664
<i>NIST SP 800-207: Adding a Zero Trust Layer to OT Macrosegmentation</i>	666
<i>Industry 4.0 and the Rise of OT Microsegmentation</i>	668
Summary	671
Lessons Learned	672
References in This Chapter	674

Chapter 12 North–South Defense: Secure Firewall and the Macrosegmentation Strategy 677

When the Perimeter Is Not Enough: Rethinking North–South Defense	677
Classic North–South Security Macrosegmentation: The Foundational Theory	680
Classic North–South Security Macrosegmentation: The Hands-On Approach	685
<i>The Classical Three-Zone Topology</i>	685

<i>Implementing the Design with Cisco Secure Firewall (FTD)</i>	686
<i>Why Rule Order Matters</i>	699
<i>Architectural Impact</i>	700
Macrosegmentation as a Zero Trust Control Layer: The Foundational Theory	716
Macrosegmentation as a Zero Trust Control Layer: The Hands-On Approach	719
<i>Step 1: Configure pxGrid Integration Between ISE and FMC</i>	720
<i>Step 2: Build Access Control Rules Using Security Group Tags</i>	724
Hybrid Mesh Firewall Architecture: The Foundational Theory	727
Hybrid Mesh Firewall Architecture: The Hands-On Approach	733
<i>Hybrid Mesh Firewall Scenario 1: Context-Based Segmentation and Risk Score</i>	734
<i>Hybrid Mesh Firewall Scenario 2: AI Application Protection</i>	740
Summary	745
Lessons Learned	746
References in This Chapter	748
Chapter 13 Proactive Threat Defense: Leveraging NDR, XDR, and SIEM	749
A Different Way of Seeing	749
When the Invisible Becomes Visible	750
From Visibility to Understanding: The Role of NDR, XDR, and SIEM	753
NetFlow and IPFIX: The Telemetry Foundation for Threat Detection	754
Network Detection and Response (NDR): The Network Analysis Layer	762
Extended Detection and Response (XDR): The Correlation Layer	765
Security Information and Event Management (SIEM): The Intelligence and Investigation Layer	767
Advanced Lateral Movement and Remote Access Techniques	771
LTR-SMB: Identity Abuse and Covert Data Exfiltration	772
<i>The Anatomy of the LTR-SMB Attack</i>	773
<i>LTR-SMB Attack Demo</i>	781
<i>LTR-SMB Attack Mitigation</i>	792
<i>LTR-SMB Context Sharing, Threat Detection, and Containment</i>	810
<i>LTR-SMB SNA and ISE Integration Workflow</i>	815
<i>LTR-SMB War Games Scenario</i>	831
LTR-Inject: Exposing the Wireless Attack Surface	844
<i>The Anatomy of the LTR-Inject Attack</i>	845

<i>LTR-Inject Attack Mitigation</i>	846
<i>LTR-Inject MACsec Configuration Steps</i>	849
Validate the Interface Authentication State	858
Validate the MACsec Session State	859
Validate the MKA Session	859
<i>MACsec Implementation Validation Summary</i>	859
L.U.M.A.: Extending the Layer 2 Attack Surface Beyond the Enterprise	860
<i>The Anatomy of the L.U.M.A. Attack</i>	860
<i>Why Traditional Security Controls Fail with L.U.M.A.</i>	869
<i>L.U.M.A. Attack Detection</i>	870
<i>L.U.M.A. Attack Mitigation</i>	873
Summary	890
Lessons Learned	891
References in This Chapter	895
Index	897

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ({[]}) indicate a required choice within an optional element.

Introduction

The cybersecurity battlefield has changed dramatically over the past decade. Modern attacks no longer depend exclusively on brute-force exploitation, isolated malware campaigns, or traditional perimeter evasion techniques. Today's adversaries operate with unprecedented levels of stealth, automation, intelligence, and adaptability. They abuse legitimate identities, trusted enterprise protocols, wireless infrastructures, mobile networks, encrypted communication channels, and even the security controls themselves to move invisibly across enterprise environments. The modern enterprise no longer faces isolated cyber incidents; it faces an evolving digital battlefield.

Cyber Defense for the Hybrid Enterprise in the Age of AI was written to help security professionals understand this transformation and prepare for the next generation of cyber threats. Based on real-world enterprise incidents, Cisco security research, penetration testing exercises, and operational experience across hybrid infrastructures, this book provides a practical and strategic guide for understanding, detecting, and defending against modern cyberattacks using vendor-agnostic methodologies such as NIST SP 800-207 Zero Trust architecture, NIST SP 800-30 Risk Assessment, ISA/IEC 62443 cybersecurity for OT, CISA Zero Trust Maturity Model 2.0, Cyber Kill Chain, MITRE ATT&CK, and Cisco SAFE aligned with world-class security architectures.

One of the most unique aspects of this book is that it allows you to experience the battlefield from both perspectives: the attacker's side and the defender's side. Through adversary emulation exercises, penetration testing simulations, malicious device deployments, and real-world attack scenarios, you will gain a practical understanding of how modern attacks evolve across the complete attack lifecycle, including reconnaissance, persistence, lateral movement, ransomware propagation, identity abuse, wireless infiltration, malicious device operations, and covert data exfiltration.

This book also demonstrates how defenders can detect and contain these threats using behavioral analytics, Zero Trust principles, adaptive security architectures, and technologies such as Cisco ISE, TrustSec, MACsec, Secure Firewall, Secure Network Analytics, and Splunk integrated into modern enterprise environments.

This book also introduces three advanced attack models created and validated in Cisco laboratory environments:

- L.U.M.A. (Layer 2 Undetected Mobile Access)
- LTR-SMB (Little Red SMB Attack)
- LTR-Inject (Little Red Wireless Inject Attack)

These attack models demonstrate how adversaries can abuse Layer 2 communication, trusted SMB traffic, wireless infrastructures, LTE and 5G networks, covert tunneling mechanisms, and identity spoofing techniques to bypass traditional security controls and remain operationally difficult to detect.

The purpose of these attack simulations is not simply to demonstrate offensive techniques but to help defenders understand how modern attacks behave operationally, why traditional controls frequently fail against them, and how behavioral analysis and continuous verification are essential components of modern cybersecurity architectures.

Traditional cybersecurity must evolve. Static prevention alone is no longer sufficient in environments where attackers increasingly operate behind legitimate authentication, valid certificates, encrypted communication channels, and authorized network segmentation policies. The future of cybersecurity depends on adaptive security architectures capable of continuously validating trust, correlating behavior, and dynamically responding to operational anomalies across hybrid environments.

The emergence of AI-driven vulnerability discovery initiatives such as Project Glasswing and models like Mythos Preview 5 further accelerates this transformation. As defenders and adversaries gain access to machine-speed capabilities for discovering vulnerabilities, analyzing code, and identifying attack paths, organizations must adopt security architectures capable of operating at the same pace. What previously required weeks of manual analysis can now be accomplished in hours or even minutes, significantly reducing the time between vulnerability discovery and exploit development. As AI systems become increasingly capable of identifying complex attack chains, generating proof-of-concept exploits, and uncovering weaknesses hidden within large code bases, organizations must assume that newly discovered vulnerabilities may be weaponized at unprecedented speed. This shift requires security teams to move beyond traditional patch-and-prevent models toward continuous monitoring, rapid risk assessment, automated detection, and adaptive response capabilities capable of operating at machine speed.

At the same time, the growing convergence of IT and OT environments significantly expands the industrial attack surface, making OT segmentation a fundamental security control for protecting critical operations. By establishing clear trust boundaries between enterprise networks, industrial zones, control systems, safety systems, and field devices, organizations can reduce exposure, contain threats, and limit lateral movement within operational environments. In the machine-speed era, OT cybersecurity can no longer rely solely on perimeter defenses and preventive controls. It requires continuous visibility into industrial communications, behavioral analysis of operational processes, and the ability to rapidly detect and respond to anomalies that could impact production, safety, or operational continuity.

This book therefore focuses heavily on concepts such as these:

- Behavioral analytics
- Continuous verification
- Microsegmentation
- Macrosegmentation
- Identity-aware security

- Automated threat containment
- Adversary emulation
- Network detection and response
- Extended detection and response
- SIEM correlation
- Malicious device detection
- Ransomware containment
- Zero Trust architectures

More importantly, this book emphasizes practical implementation. Throughout the chapters, you will find deployment guidance, penetration testing scenarios, behavioral analysis workflows, real-world enterprise case studies, and operational examples designed to help security architects, engineers, SOC analysts, penetration testers, incident responders, and security leaders apply these concepts directly in modern enterprise environments.

Goals, Objectives, and Approach of the Book

The primary goal of this book is to provide a comprehensive and operational guide for understanding how modern cyberattacks evolve and how enterprise security architectures must adapt to defend against them. This book aims to shift your mindset from traditional perimeter-focused security toward a behavioral, identity-aware, and continuously adaptive security model capable of operating effectively across hybrid enterprise infrastructures.

This book was intentionally designed to combine theoretical foundations with practical implementation guidance. Rather than focus exclusively on concepts or technologies in isolation, it demonstrates how modern attacks operate in real-world environments and how defenders can implement integrated security architectures capable of detecting and containing them.

Throughout this journey, you will understand how attackers abuse legitimate trust relationships, how behavioral analytics expose operational anomalies that are invisible to traditional controls, and how integrated security platforms can dynamically respond to threats through context sharing, automation, and adaptive enforcement.

The book also aims to bridge the gap between strategic cybersecurity concepts and practical operational deployment. Security leaders will gain insight into modern resilience architectures and risk reduction strategies, and technical professionals will obtain actionable guidance for implementing detection, segmentation, behavioral analytics, and automated response workflows in enterprise environments.

This book will help you understand the operational evolution of modern cyberattacks. It will also show you how to do all the following:

- Analyze how attackers abuse legitimate enterprise trust relationships.
- Design Zero Trust architectures aligned with behavioral security principles.
- Implement microsegmentation and macrosegmentation strategies.
- Deploy identity-aware security controls using Cisco ISE and TrustSec.
- Understand how MACsec protects enterprise Layer 2 communication.
- Apply behavioral analytics using NDR, SIEM, and XDR platforms.
- Detect malicious device operations and advanced lateral movement techniques.
- Build adaptive security architectures capable of continuously validating trust.
- Understand the impact of AI-driven threats on modern enterprise environments.
- Understand Project Glasswing and its implications for defenders.
- Develop security architectures capable of protecting OT environments.

This book presents cybersecurity not simply as a collection of technologies but as a continuously evolving operational battlefield where understanding attacker behavior is just as important as deploying defensive controls.

Who This Book Is For

This book was written for cybersecurity professionals, architects, engineers, SOC analysts, penetration testers, incident responders, consultants, researchers, technology leaders, and students seeking a deeper operational understanding of modern cyber threats and adaptive security architectures.

Security engineers and architects will find practical implementation guidance for Zero Trust, segmentation, identity-aware security, and behavioral analytics deployments. SOC analysts and incident responders will gain visibility into attack behavior, telemetry correlation, threat hunting, and automated response workflows. Penetration testers and red team professionals will better understand how modern adversaries abuse legitimate enterprise trust relationships and covert communication mechanisms.

Technology leaders, CISOs, and decision makers will benefit from the strategic perspectives related to cyber resilience, operational risk reduction, adaptive security architectures, and the future evolution of enterprise cybersecurity.

Above all, this book serves those responsible for defending modern infrastructures in an era when attackers continuously evolve faster, move more stealthily, and increasingly hide behind legitimate trust itself.

How This Book is Organized

Chapter 1, “The Evolution of Cyber Threats: Digital Fraud, Ransomware, and AI-Driven Attacks,” explores how the cyber threat landscape has evolved from traditional malware and perimeter-based attacks into highly sophisticated operations driven by automation, identity abuse, ransomware ecosystems, malicious devices, and artificial intelligence. This chapter introduces the concept of the digital battlefield and demonstrates how modern adversaries increasingly leverage stealth, behavioral evasion, and trusted enterprise protocols to bypass conventional security architectures. It establishes the strategic foundation necessary to understand why traditional cybersecurity models are no longer sufficient against modern hybrid threats. The chapter also highlights an important professional evolution experienced by many senior cybersecurity practitioners throughout their careers. As security professionals gain experience and credibility within their organizations, their role naturally expands beyond technical implementation and operational activities. They become increasingly involved in business discussions, risk management, executive decision-making, and long-term strategic planning. You will learn why understanding business objectives, operational priorities, regulatory requirements, and organizational risks is just as important as understanding security technologies. The chapter demonstrates how successful security leaders transition from focusing exclusively on technical controls to helping define and influence the organization’s security strategy, ensuring that cybersecurity initiatives directly support business goals, resilience objectives, and long-term growth. This business-oriented perspective serves as a foundation for the strategic concepts developed throughout the remainder of the book.

Chapter 2, “The Hackers’ Modus Operandi: The Attack Anatomy,” analyzes how modern attackers plan, structure, and execute advanced cyber operations across the complete attack lifecycle. This chapter explores the operational methodology behind reconnaissance, initial compromise, persistence, lateral movement, privilege escalation, covert communication, data exfiltration, and ransomware propagation. Through real-world attack patterns and adversary emulation concepts aligned with Cyber Kill Chain and MITRE ATT&CK methodologies, the chapter demonstrates how attackers think, adapt, and exploit legitimate trust relationships inside enterprise environments. The chapter also examines the organizational structure of modern cybercriminal groups, showing how many threat actors operate as highly specialized enterprises with defined roles, including hackers, internal employees, initial access brokers, money laundering specialists, and social engineering teams. By understanding how these criminal organizations coordinate their operations, you will gain a deeper appreciation of the sophistication, scale, and business-like nature of today’s cyber threat landscape.

Chapter 3, “The Security Journey: Business Strategy Alignment,” shifts the discussion from purely technical controls toward strategic cybersecurity alignment with business objectives. The chapter explores how organizations must design security programs that support operational resilience, regulatory compliance, risk reduction, fraud prevention, and executive governance. It introduces the concept of cybersecurity as a business enabler rather than simply a technical requirement, helping security leaders build long-term security roadmaps aligned with organizational priorities. The chapter also

emphasizes the importance of understanding the business outcomes that security initiatives are intended to support. Rather than viewing security technologies as the objective, you will learn how security methodologies, frameworks, and best practices serve as strategic guidance, while security products and solutions act as tools used to achieve business goals. This business-first perspective helps organizations make informed security investments that not only reduce risk but also enable growth, innovation, operational efficiency, and long-term business success.

Chapter 4, “Mapping the Threat Landscape: A Strategic Approach to Network Security Assessments,” presents a structured methodology for performing enterprise security assessments using Zero Trust principles, risk analysis methodologies, and threat-based evaluation techniques. This chapter introduces practical assessment models aligned with NIST SP 800-207, NIST SP 800-30, CISA Zero Trust principles, MITRE ATT&CK, and Cisco SAFE. You will learn how to identify architectural weaknesses, evaluate operational maturity, map attack surfaces, and prioritize remediation strategies across modern hybrid infrastructures. The chapter also establishes the foundational knowledge required to conduct real-world security assessments, providing practitioners with practical guidance that can be directly applied in customer and enterprise environments. By understanding the assessment process, data collection techniques, maturity evaluation methods, and risk prioritization approaches, you will be prepared to initiate security assessments in the field and develop the business-aligned roadmaps that serve as the foundation for future cybersecurity.

Chapter 5, “Field Validation: A Step-by-Step Case Study in Threat and Risk Assessment,” transforms theoretical assessment methodologies into a practical operational case study. Through a simulated enterprise engagement, the chapter demonstrates how security teams conduct interviews, identify security gaps, evaluate operational risks, classify threats, and develop actionable remediation roadmaps. You will gain practical insight into how real-world security assessments operate across enterprise environments. The chapter also emphasizes that a security assessment should be the first phase of any cybersecurity transformation journey. Before investing in technologies, deploying new controls, or defining target architectures, organizations must first understand their current security posture, business-critical assets, operational dependencies, and risk exposure. Through a structured assessment process, security teams can identify the capabilities most important for protecting the organization and ensuring business continuity. The resulting roadmap becomes the foundation of the security journey, providing a prioritized and business-aligned strategy that guides future investments, architectural decisions, and security initiatives toward measurable risk reduction and long-term organizational objectives.

Chapter 6, “Inside the Insider Threat: How Fraudulent Devices Undermined a Bank’s Defenses,” introduces the initial compromise scenario that serves as the foundation for the technical attack narrative developed throughout the book. The chapter demonstrates how malicious devices can infiltrate enterprise environments while abusing legitimate trust relationships, wireless infrastructures, identity validation mechanisms, and operational blind spots. You will begin to understand how advanced adversaries weaponize covert infrastructure inside the enterprise network itself. The chapter also illustrates

how a real-world attack can originate long before any malware is deployed or network access is obtained. Through the story of a financial institution, you will follow the attack from its earliest stages, including the recruitment of an insider, the personal and social circumstances that influenced the individual's decisions, and the human interactions that enabled the compromise. The narrative demonstrates how a hardworking father facing significant financial difficulties can become vulnerable to manipulation, not because of malicious intent, but because of a genuine desire to provide for and protect his family. In many cases, attackers do not target greed; they target desperation, hope, fear, and the emotional pressures that affect ordinary people during difficult moments in their lives. By examining the motivations, pressures, and vulnerabilities that influence human behavior, the chapter highlights a fundamental reality of cybersecurity: despite continuous advances in technology, the human factor often remains the weakest link in the security chain. Understanding this human dimension is essential for building effective security strategies that address not only technical vulnerabilities but also the trust relationships, emotional pressures, and behavioral factors that attackers routinely exploit.

Chapter 7, "Behind the Scenes: The Setup of Fraudulent Devices," presents the operational preparation phase behind the attack infrastructure. The chapter demonstrates how attackers configure covert communication channels, LTE and Internet connectivity, Layer 2 extension mechanisms, remote management paths, malicious bridges, tunneling infrastructures, and stealth communication models capable of bypassing traditional security visibility. This chapter introduces the technical foundations required for attacks such as the new generation on-path attacks. You will gain detailed insight into how these modern infrastructure threats are built and operated, including the deployment of fraudulent devices inside enterprise environments, the use of 5G networks for covert remote access, and the establishment of encrypted VPN tunnels that provide attackers with persistent connectivity to compromised locations. Through practical examples, the chapter demonstrates how adversaries can extend trusted network segments across untrusted infrastructures, enabling remote interception, traffic manipulation, and unauthorized access while remaining largely invisible to traditional security controls.

Chapter 8, "The Live Attack: Showtime," places you directly inside the active attack execution phase. This chapter demonstrates how attackers weaponize legitimate enterprise communication paths, identity spoofing, SMB abuse, covert tunneling, and wireless infrastructures to perform stealthy lateral movement and data exfiltration. You will experience the attack from both offensive and defensive perspectives and observe how traditional security controls struggle to detect advanced operationally stealthy threats. Beyond the technical preparation, the chapter reveals the extensive planning and human manipulation that occur before the attack ever begins. You will follow the activities of the criminal organization as it recruits participants, assigns specialized tasks, acquires infrastructure, and coordinates the various elements required for a successful operation. The chapter also explores a darker aspect of cybercrime: the exploitation of innocent victims to influence decision-making inside the target organization. Through the kidnapping of the financial manager's daughter, the attackers force her cooperation during critical stages of the operation, demonstrating how coercion, fear, and emotional pressure can be more effective than financial incentives. This scenario highlights an important lesson: the

human factor remains one of the most vulnerable components of any security program, especially when attackers target not only employees themselves, but also the people they care about. By understanding these pre-attack activities, you will gain a deeper appreciation for the social, psychological, and operational dimensions of modern cybercrime.

Chapter 9, “Strategic Foundations of Defense: Zero Trust, SAFE, and AI,” introduces the strategic defensive architecture used to counter the advanced attacks demonstrated throughout the book. The chapter explores how Zero Trust principles, Cisco SAFE architectures, behavioral analytics, AI-assisted security operations, and adaptive security models combine to create resilient enterprise security ecosystems capable of continuously validating trust and dynamically responding to operational anomalies. The chapter also examines the emergence of AI-driven threats and the growing impact of machine-speed attack operations, where artificial intelligence can accelerate vulnerability discovery, exploit development, reconnaissance, and attack automation. You will learn how organizations can leverage AI as a defensive force multiplier while implementing security architectures capable of detecting, validating, and responding to the next generation of AI-assisted threats operating across enterprise and industrial environments.

Chapter 10, “Identity and Access Control: Building Security with Cisco ISE,” explores how identity-aware security is one of the foundational pillars of modern cybersecurity architectures. This chapter demonstrates how Cisco ISE operates as the Policy Decision Point (PDP) of the environment, enabling authentication, authorization, posture validation, profiling, segmentation enforcement, context sharing, and dynamic threat containment across enterprise infrastructures. The chapter also includes a complete Cisco ISE Plan, Design, and Implementation (PDI) methodology, providing practical guidance for planning, deploying, and operating a Network Access Control (NAC) solution in real-world environments. Through detailed design recommendations, deployment considerations, sizing methodologies, and configuration examples, you will learn how to implement the most important NAC use cases for both corporate endpoints and IoT devices, including wired and wireless 802.1X authentication, EAP-TLS deployments, device profiling, posture assessment, guest access, BYOD onboarding, printer and IP phone authentication, segmentation enforcement, and policy-based access control. The chapter also covers the architectural considerations required for large-scale and globally distributed deployments, including node placement strategies, regional resiliency, high availability, load balancing, geographic redundancy, latency considerations, and capacity planning for enterprise environments supporting tens or even hundreds of thousands of endpoints across multiple countries and regions. By the end of the chapter, you will have the foundational knowledge required to design, size, and deploy a scalable Cisco ISE architecture capable of supporting modern Zero Trust initiatives in both regional and worldwide enterprise environments.

Chapter 11, “East–West Defense: MACsec Encryption and TrustSec Microsegmentation,” focuses on the protection of internal enterprise communication through identity-based microsegmentation. The chapter demonstrates how Cisco TrustSec, security group tags (SGTs), security group access control lists (SGACLs), and identity-aware segmentation policies reduce lateral movement opportunities and contain advanced threats operating inside the network. You will learn how microsegmentation transforms internal security

from static VLAN-based isolation into adaptive identity-driven enforcement. The chapter includes a complete Plan, Design, and Implementation (PDI) methodology for deploying enterprise microsegmentation initiatives, providing practical guidance for planning, designing, validating, and implementing TrustSec-based segmentation architectures in real-world environments. Through detailed design recommendations, policy development methodologies, and deployment considerations, you will learn how to implement the most important microsegmentation use cases, including corporate workstation isolation, IoT and printer segmentation, IP camera protection, privileged access segmentation, and data center workload segmentation scenarios. By the end of the chapter, you will have the knowledge required to design and deploy scalable microsegmentation architectures that align security enforcement with business intent while supporting Zero Trust principles across enterprise and industrial environments. The chapter also introduces the application of segmentation principles within Operational Technology (OT) environments, where industrial assets, control systems, engineering workstations, and supervisory systems require distinct trust boundaries. You will learn how OT segmentation reduces the attack surface, limits the propagation of cyber threats across industrial networks, and supports the protection of critical operational processes while maintaining reliability and operational continuity. The chapter also examines the evolution of industrial security architectures, beginning with the traditional Purdue Model and its hierarchical approach to industrial network segmentation, progressing through the zone-and-conduit concepts introduced by ISA/IEC 62443, and culminating in the application of Zero Trust principles within modern OT environments. You will learn how industrial security architectures have evolved from static network boundaries toward identity-aware, context-driven, and continuously validated trust models capable of protecting increasingly connected and converged IT/OT infrastructures. By understanding this evolution, security practitioners will be better equipped to design modern OT security architectures that preserve operational requirements while addressing today's sophisticated cyber threats.

Chapter 12, “North–South Defense: Secure Firewall and the Macrosegmentation Strategy,” explores the role of macrosegmentation and hybrid firewall architectures in controlling communication between enterprise trust zones, data centers, and external networks. The chapter demonstrates how Cisco Secure Firewall, Cisco Identity Intelligence, policy correlation, and Zero Trust enforcement help organizations contain threats, reduce attack surfaces, and protect critical communication boundaries across hybrid infrastructures. The chapter begins by examining traditional firewall segmentation architectures and the evolution of firewall technologies over the past several decades, from early packet-filtering firewalls to stateful inspection, application-aware firewalls, next-generation firewalls, and AI-assisted security platforms. You will learn the design principles behind classic enterprise firewall architectures, including the well-known firewall sandwich model, where multiple security layers are strategically positioned to protect internal resources and enforce trust boundaries. Building on these foundations, the chapter demonstrates how modern organizations are evolving toward Hybrid Mesh Firewall architectures that extend consistent security policies across campuses, data centers, cloud environments, remote users, and distributed workloads. By understanding both traditional and modern approaches, you will learn how macrosegmentation continues to

play a critical role in Zero Trust architectures while adapting to the demands of increasingly distributed and hybrid enterprise environments.

Chapter 13, “Proactive Threat Defense: Leveraging NDR, XDR, and SIEM,” concludes the technical journey by introducing behavioral detection, telemetry correlation, and automated threat response mechanisms capable of identifying attacks that bypass traditional preventive controls. The chapter demonstrates how Cisco Secure Network Analytics (NDR), Cisco ISE (NAC), Splunk (SIEM), and Cisco Extended Detection and Response (XDR) together make it possible to detect covert attack behaviors such as abnormal crypto tunnel instability, identity abuse, data exfiltration, malicious device activity, and advanced Layer 2 extension attacks. It establishes behavioral analysis and continuous verification as fundamental pillars of modern cyber defense. The chapter also presents the detection and mitigation strategies developed to identify the attack models introduced throughout the book, including LTR-SMB (Little Red SMB Attack), LTR-Inject (Little Red Wireless Inject Attack), and L.U.M.A. (Layer 2 Undetected Mobile Access). Through these examples, you will learn how behavioral analytics, identity context, network telemetry, and automated enforcement can expose adversaries operating behind legitimate credentials, encrypted communications, and trusted network infrastructure, even when traditional security controls fail to identify malicious activity. The chapter also provides an in-depth methodology for planning, designing, and implementing behavioral security analytics programs, demonstrating how detection use cases can be systematically developed and mapped across the various phases of the Cyber Kill Chain. You will learn how to build behavioral detection strategies for reconnaissance, initial access, persistence, privilege escalation, lateral movement, command-and-control communications, and data exfiltration activities. By combining threat modeling, behavioral baselines, identity awareness, and telemetry correlation, the chapter provides a practical framework for transforming behavioral analytics into a structured and measurable security capability capable of detecting threats throughout the entire attack lifecycle.

Figure Credit

Cover	royyimzy/AdobeStock
Figure 1.1	Image generated by Author via Open AI
Figure 1.2	Image generated by Author via Open AI
Figure 1.3	Image generated by Author via Open AI
Figure 1.4a	Image generated by Pearson using AI
Figure 1.4b	Image generated by Pearson using AI
Figure 1.4c	Image generated by Pearson using AI
Figure 1.4d	Image generated by Pearson using AI
Figure 1.4e	Image generated by Pearson using AI
Figure 1.5	Image generated by Author via Open AI
Figure 2.1	Image generated by Author via Open AI
Figure 2.2	Image generated by Author via Open AI
Figure 2.3	Image generated by Author via Open AI
Figure 2.5a	Courtesy of MikroTik
Figure 2.5b	Image generated by Pearson using AI
Figure 2.5c	Image generated by Pearson using AI
Figure 2.5d	Image generated by Pearson using AI
Figure 2.5e	Image generated by Pearson using AI
Figure 2.5f	Image generated by Pearson using AI
Figure 2.5g	Image generated by Pearson using AI
Figure 2.6	Image generated by Author via Open AI
Figure 2.7	Image generated by Author via Open AI
Figure 2.8	Image generated by Author via Open AI
Figure 2.9	Image generated by Author via Open AI
Figure 2.11	Figure adapted from the Lockheed Martin Cyber Kill Chain® framework; artwork recreated by Pearson using AI
Figure 2.12	Image generated by Author via Open AI
Figure 2.13	Image generated by Author via Open AI
Figure 3.1	Image generated by Author via Open AI

Figure 3.5	Image generated by Author via Open AI
Figure 3.10	Image generated by Author via Open AI
Figure 4.1	Image generated by Author via Open AI
Figure 4.16	Image generated by Author via Open AI
Figure 5.1	Image generated by Author via Open AI
Figure 5.3	National Institute of Standards and Technology (NIST), Zero Trust Architecture, NIST SP 800-207
Figure 5.10	Image generated by Author via Open AI
Figure 6.1	Image generated by Author via Open AI
Figure 6.2a	Image generated by Author via Open AI
Figure 6.3	Image generated by Author via Open AI
Figure 6.6	Courtesy of MikroTik
Figure 6.14	Image generated by Author via Open AI
Figure 7.1	Image generated by Author via Open AI
Figure 7.2	Image generated by Author via Open AI
Figure 7.3a	Courtesy of MikroTik
Figure 7.15	Image generated by Author via Open AI
Figure 7.30	Image generated by Author via Open AI
Figure 8.1	Image generated by Author via Open AI
Figure 8.13	Image generated by Author via Open AI
Figure 8.14	Image generated by Author via Open AI
Figure 8.19	Image generated by Author via Open AI
Figure 8.20	Image generated by Author via Open AI
Figure 8.23	Routerboard.com OUI Public Database; screenshot captured by the author.
Figure 8.26	Image generated by Author via Open AI
Figure 9.1	Image generated by Author via Open AI
Figure 9.18	Image generated by Author via Chat GPT 5.5
Figure 9.19	Image generated by Author via Chat GPT 5.5
Figure 9.20	Image generated by Author via Chat GPT 5.5
Figure 9.21	Image generated by Author via Chat GPT 5.5

- Figure 9.22 Image generated by Author via Chat GPT 5.5
- Figure 9.23 Image generated by Author via Chat GPT 5.5
- Figure 9.24 Image generated by Author via Chat GPT 5.5
- Figure 9.25 Image generated by Author via Chat GPT 5.5
- Figure 9.26 Image generated by Author via Chat GPT 5.5
- Figure 9.27 Image generated by Author via Chat GPT 5.5
- Figure 9.43 Image generated by Author via Open AI
- Figure 10.1 Image generated by Author via Open AI
- Figure 10.15a Screenshot of the Polycom® VVX 601 IP Phone administration interface;
phone image generated by Pearson using AI.
- Figure 10.36 Image generated by Author via Open AI
- Figure 11.34 Image generated by Author via ChatGPT 5.5
- Figure 11.35 Image generated by Author via ChatGPT 5.5
- Figure 11.36 Image generated by Author via ChatGPT 5.5
- Figure 11.37 Image generated by Author via ChatGPT 5.5
- Figure 11.38 Image generated by Author via ChatGPT 5.5
- Figure 11.39 Image generated by Author via ChatGPT 5.5
- Figure 12.1 Image generated by Author via Open AI
- Figure 12.3 Image generated by Author via Open AI
- Figure 12.4 Image generated by Author via Open AI
- Figure 12.30 Image generated by Author via Open AI
- Figure 12.38 Image generated by Author via Open AI
- Figure 12.40 Image generated by Author via Open AI
- Figure 12.49 Image generated by Author via Open AI
- Figure 13.1 Image generated by Author via Open AI
- Figure 13.9 Image generated by Pearson using AI
- Figure 13.16 Screenshot from MikroTik RouterOS, used for educational purposes
- Figure 13.29 Image generated by Author via ChatGPT 5.5
- Figure 13.31 Image generated by Author via Open AI
- Figure 13.33 Image generated by Author via Open AI

Figure 13.35 Image generated by Author via Open AI

Figure 13.37 Image generated by Author via Open AI

Figure 13.39 Image generated by Author via Open AI

Figure 13.41 Image generated by Author via Open AI

Figure 13.43 Image generated by Author via Open AI

Figure 13.44 Image generated by Author via Open AI

Figure 13.45 Image generated by Author via Open AI

Figure 13.46 Image generated by Author via Open AI

Figure 13.61 Image generated by Author via Open AI

Figure 13.62 Image generated by Author via Open AI

Figure 13.74 Image generated by Author via Open AI

Figure 13.75 Image generated by Author via Open AI

Figure 13.76 Image generated by Author via Open AI

This page intentionally left blank

Mapping the Threat Landscape: A Strategic Approach to Network Security Assessments

“Security is always excessive until it’s not enough.”

—Robbie Sinclair, Head of Security, Country Energy, NSW Australia

Revealing the Unknown

Andrew stood in the stillness of his office, the city skyline stretching out behind him. The calm he had found on the beach with Henry had given way to a growing sense of urgency. It wasn’t just instinct anymore; it was a fact: He lacked the visibility he needed to protect the company’s corporate network. Due to the surging ransomware attacks across critical infrastructure sectors, the board’s concern had reached a tipping point.

He couldn’t postpone it any longer. Guided by Henry’s advice, Andrew picked up the phone and called Fredy, a seasoned network security advisor with a reputation for precision and deep expertise in Zero Trust Network Architectures (ZTNA), to invite him to a meeting. Fredy was someone Andrew trusted; he had worked with Henry in the past, a connection that only reinforced Andrew’s confidence in the decision. “Let’s meet in person, at the company’s headquarters,” Andrew said.

Two days later, Fredy arrived at the company’s headquarters and stepped into the executive conference room (see Figure 4-1). The walls were lined with architectural diagrams and risk dashboards, but what was missing was exactly what they had come to solve: a full, honest picture of the current security posture.

After catching up briefly, Andrew laid out the challenge: “We need to understand where we are today. No guesswork, no gaps. The board needs answers and a consistent plan.”

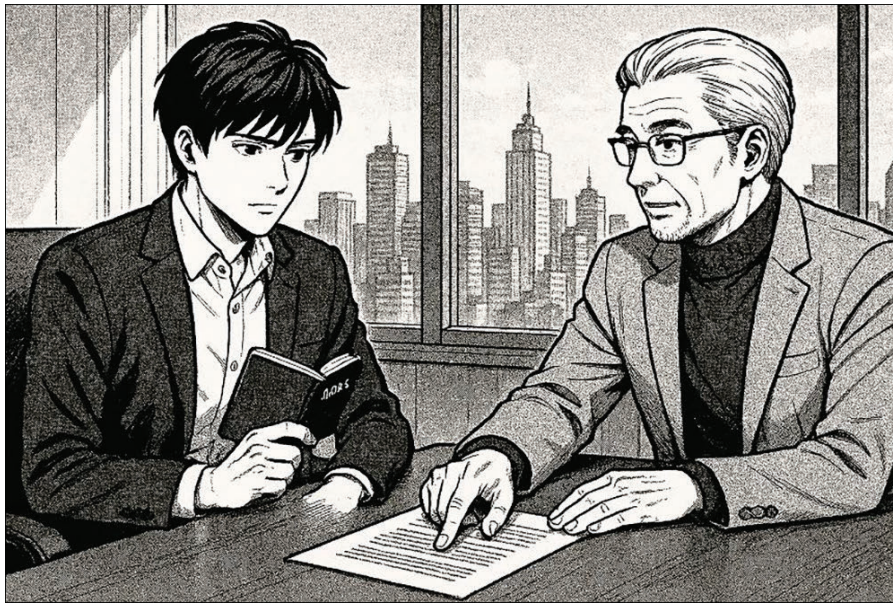


Figure 4-1 *The Meeting to Start a Security Assessment Plan*

Fredy nodded and said, “Then we start with a comprehensive security network assessment based on Zero Trust. Not just a checklist; a real evaluation.”

After setting the context, Fredy introduced a structured five-phase security lifecycle methodology. The first three phases focused on the assessment process itself, while the final two phases concentrated on the post-assessment roadmap and long-term transformation strategy. He emphasized that the objective was not simply to produce a static report, but to establish a living security strategy capable of guiding continuous business and technology evolution.

Fredy clarified that this methodology differed from the concepts previously introduced by Henry in Chapter 3. Henry’s five pillars defined the foundational components required to build a modern cybersecurity strategy aligned with business priorities. During the organization’s initial strategic analysis, however, the leadership team realized that although the five-pillar model helped structure the strategic vision, it did not provide enough visibility into the organization’s actual security maturity level, operational gaps, or risk exposure.

To establish that visibility, the organization initially analyzed its cybersecurity strategy through five strategic pillars:

1. Outcomes, including user trust and safety, corporate endpoint protection, risk reduction, and threat visibility
2. Domains, including enterprise LAN, enterprise wireless, enterprise VPN, and data-center environments

3. Frameworks, including Zero Trust, Cisco SAFE, MITRE ATT&CK, NIST SP 800-207, and NIST SP 800-30
4. Solutions, including user protection, network visibility, and segmentation capabilities
5. Services, including advisory services that incorporated the security assessment process itself

Fredy explained that these five pillars established the strategic foundation for the cybersecurity program. His new proposal, however, focused on the organization's next major challenge: conducting the security assessment itself. The assessment represented the first practical step toward understanding the organization's real maturity level, identifying operational and architectural gaps, evaluating risks, and defining a prioritized roadmap for remediation and long-term improvement.

To achieve this objective, the assessment methodology followed its own independent five-phase structure, specifically designed to guide the organization from initial discovery through future-state planning, strategic alignment, and long-term execution.

As the conversation deepened, the importance of structure became increasingly clear to Andrew. Fredy explained that each phase of the methodology served a distinct purpose, produced specific outcomes, and played a strategic role in aligning cybersecurity investments with business priorities. This was not simply another technical assessment. It was a structured transformation model designed to help the organization evolve its security posture over time.

Noticing Andrew's expression, Fredy paused briefly and smiled.

"I know this may sound similar to the five pillars Henry introduced earlier," he said. "But they are not the same thing."

Andrew nodded. "That was exactly what I was trying to understand."

Fredy walked toward the whiteboard and drew two separate diagrams.

"The five pillars Henry presented in Chapter 3 define the strategic foundation of the cybersecurity program," Fredy explained. "They help the organization understand what it needs to protect, which environments require visibility, which frameworks guide the strategy, which technologies support the controls, and which services enable execution."

He pointed to the first diagram.

"Those pillars focus on strategic alignment:

1. Outcomes
2. Domains
3. Frameworks
4. Solutions
5. Services

They help establish the business and architectural vision.”

Andrew crossed his arms while studying the board carefully.

“But,” Fredy continued, “during the initial strategic discussions, the leadership team realized something important. Even with a well-defined strategy, nobody truly understood the organization’s actual security maturity level. The company still lacked visibility into operational gaps, architectural weaknesses, and overall risk exposure.”

“So the pillars define the strategy,” Andrew said, “but they don’t measure the current state.”

“Exactly,” Fredy replied.

He then pointed to the second diagram on the board.

“Those pillars focus on security lifecycle methodology:

1. **Security Baseline:** Conduct technical interviews, analyze device configurations, and review network topology information to establish the organization’s current security posture.
2. **Environment Analysis:** Compare the current “as-is” environment against security best practices, industry frameworks, and architecture methodologies.
3. **Recommend:** Identify security gaps, evaluate risks, and develop prioritized roadmaps for each environment.
4. **Execution:** Plan, design, test, and implement the proposed remediation and transformation roadmaps.
5. **Measure:** Measure roadmap evolution and security maturity progression through defined KPIs and operational metrics

They help establish the company’s security maturity level, identify operational gaps, and evaluate risk exposure. That is where the assessment methodology comes in. The five-phase methodology is independent from the five strategic pillars. Its purpose is to evaluate the organization’s real environment, identify weaknesses, measure maturity, analyze risks, and create a practical roadmap for improvement.”

Andrew immediately understood the distinction.

Henry’s pillars established the strategic vision. Fredy’s methodology transformed that vision into a measurable execution plan.

Fredy continued walking through the process step by step. The first two phases, Security Baseline and Environment Analysis, focus on assessment activities, including discovery, technical analysis, and security maturity evaluation. The third phase, Recommendations, focuses on roadmap creation and serves as the transition point between the assessment process and the execution of the proposed transformation initiatives. The final two phases, Execute and Measure, concentrated on future-state planning, strategic recommendations, and long-term transformation guidance.

“The objective,” Fredy explained, “is not to produce a static report that becomes outdated in six months. The goal is to establish a living security lifecycle strategy that evolves together with the business.”

Andrew looked again at the diagrams. For the first time, the relationship between business strategy, Zero Trust maturity, and operational execution started to connect as a single transformation journey rather than isolated technical projects.

Fredy then shifted the discussion toward the methodology itself, beginning with a deep analysis of the current environment and concluding with the development of an adaptive roadmap for Zero Trust maturity. As the discussion progressed, Andrew realized that the methodology provided something many organizations lacked: a structured way to connect technical controls, operational risks, and executive priorities into a unified security lifecycle strategy.

Each phase built upon the previous one, creating a progressive transformation model grounded in real-world operational challenges and measurable business outcomes. What Fredy presented was far more than a traditional assessment framework. It was a blueprint for evolving the organization’s security posture with purpose, structure, and long-term strategic direction.

The Strategic Zero Trust Readiness Assessment: A Framework to Start a Zero Trust Journey

Every meaningful security transformation begins with visibility—an honest, structured view of where the organization stands today. Without this clarity, it is nearly impossible to design an effective security roadmap. However, many organizations struggle to achieve this foundational understanding. Years of accumulated complexity, fragmented infrastructure, and disconnected operational practices make it difficult to define what “secure” looks like in their environment. A security assessment is indispensable—not as a checklist but as a strategic lens.

The assessment framework introduced in this chapter was crafted to cut through that complexity. It brings structure to the discovery process, allowing both technical teams and business stakeholders to move past assumptions and operate from facts. This is more than identifying vulnerabilities; it’s about mapping risk to business impact, prioritizing action based on critical exposures, and delivering a blueprint that aligns technology with long-term strategic goals. It enables decision makers to see beyond individual technologies and understand the maturity of the entire security posture.

Today’s cybersecurity ecosystem includes dozens of reference models and frameworks such as NIST, CISA, MITRE ATT&CK, Cisco SAFE, and others, each designed to solve different parts of the problem. The framework presented in this chapter does not seek to replace them; instead, it builds a cohesive, phase-based structure that leverages their strengths at the right moment. It allows organizations to map security controls to Zero Trust principles, link them to technical domains, and evaluate them under standardized maturity and risk criteria.

This chapter introduces the *Strategic Zero Trust Readiness Assessment*, a structured framework designed to evaluate cybersecurity maturity and risk across key technical domains. This security assessment provides a structured approach to evaluate an organization's cybersecurity posture across multiple technical domains. It aligns each domain with the core principles of Zero Trust, using industry-recognized models such as the CISA Zero Trust Maturity Model and the NIST Zero Trust Architecture (NIST SP 800-207).

This assessment framework enables security teams to do the following:

- Identify the current maturity level for each technical domain
- Analyze control effectiveness and architecture alignment
- Evaluate associated risk severities using a hybrid model based on NIST SP 800-30, MITRE ATT&CK, and risk heat mapping
- Map technical controls to CISA Zero Trust Maturity Model pillars, NIST SP 800-207 core elements, and Cisco SAFE architecture

This security assessment serves as the foundation for future roadmap development. While it does not include solution design or implementation planning, its findings establish the necessary baseline for defining next steps in a Zero Trust transformation.

This chapter sets the stage for a unified assessment journey that serves as the launch point for Zero Trust. It offers not just a methodology but a mindset: one that values cross-functional collaboration, continual improvement, and decisions grounded in real operational data. Whether you're at the beginning of your Zero Trust journey or refining your current implementation, this framework is designed to guide you with precision, discipline, and business alignment.

A security lifecycle journey typically involves multiple projects, each structured around five core phases, as illustrated later in Figure 4-12.

Phases 1 and 2, Security Baseline and Environment Analysis, focus on the assessment itself. These phases establish the organization's current security maturity level through technical interviews, configuration analysis, topology reviews, and comparisons against security best practices, frameworks, and architecture methodologies.

Phase 3, Recommend, focuses on the creation of strategic roadmaps. This phase acts as the bridge between the assessment findings and the future execution activities by translating identified gaps, risks, and operational weaknesses into prioritized remediation and transformation plans.

Phases 4 and 5, Execute and Measure, focus on the implementation and continuous evolution of the roadmap developed during the Recommend process. These phases transform the assessment results into operational improvements, validated controls, measurable outcomes, and long-term maturity progression.

Together, the Security Baseline and Environment Analysis phases represent the complete assessment portion of the methodology and consist of seven defined steps. An additional step, Step 8, operates as a transition point between the assessment activities and the roadmap development process created during the Recommendations phase. Although Step 8 is not formally considered part of the assessment itself, it serves as the critical connection between analysis and execution, ensuring that the assessment findings evolve into actionable transformation initiatives.

This section provides a concise summary of the Strategic Zero Trust Readiness Assessment framework, highlighting the key phases that guide the security evaluation process. From the initial mapping of technical domains to the identification of control areas, risk severity, and alignment with MITRE ATT&CK techniques, each step plays a strategic role in building a comprehensive threat-informed defense model. The goal is to offer a clear view of how the framework connects assessment data to actionable insights, enabling organizations to prioritize improvements and design effective security roadmaps. The following sections provide an overview of the key steps in the assessment framework, summarizing the sequence of activities from technical domain definition to risk evaluation.

Step 1: Mapping the Network to Technical Domains (Protect Surfaces)

The first step in the assessment journey is a systematic analysis of the organization's current network infrastructure. This analysis aims to deconstruct the environment into distinct technical domains—logical segments that reflect how security controls, technologies, and operational requirements differ across the enterprise. This domain-based segmentation ensures that the evaluation is both scalable and relevant, avoiding generic recommendations that fail to reflect operational reality.

Each technical domain corresponds to a specific “protect surface,” a concept central to Zero Trust strategy. Rather than defending an ever-expanding attack surface, the protect surface approach focuses on identifying and safeguarding what matters most: critical assets, sensitive data, and essential services. This shift in perspective makes the assessment more actionable by narrowing the focus to assets that have the greatest impact on business operations and regulatory compliance. To help visualize the relationship, think of a technical domain as a SAFE PIN (place in the network) in the Cisco SAFE framework. However, a technical domain represents only a subset of a PIN because each PIN may encompass multiple technical domains within the security architecture. For example, within the Data Center PIN, both the Data Center Network and the Data Center Firewall technical domains represent specific subsets. By using technical domains instead of broader PINs, the assessment adopts a more granular view that captures the precise controls and solutions required to design an effective and actionable security journey. Another useful comparison is between SAFE domains and Cisco SAFE control areas, which you will explore in more detail in the following sections. Both structures serve to organize and align security capabilities, helping translate technical implementations

into strategic Zero Trust outcomes. Figure 4-2 illustrates the relationship between Cisco SAFE PINs and technical domains, highlighting how each domain maps to specific places in the network.

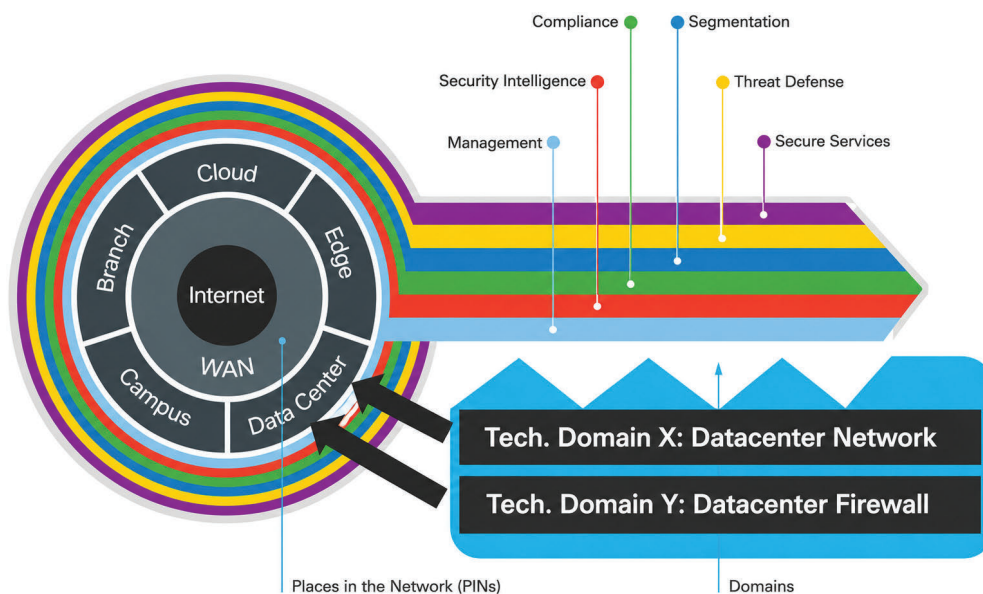


Figure 4-2 *Cisco SAFE PINs Versus Technical Domains*

Importantly, not all domains require the same security posture. For instance, the controls necessary to enforce access in a wireless network differ from those required in a data center network environment or on VPN gateways. Even when applying the same overarching principle, such as identity enforcement or segmentation, the underlying technologies, trust models, and operational workflows vary significantly. Therefore, domains like Wired LAN, Wireless LAN, Data Center Firewalls, Data Center Network, Corporate Endpoints, and VPN Access must be treated independently. Figure 4-3 illustrates the mapping of three technical domains within a customer’s network environment: Email Security, Corporate Endpoints, and Wired and Wireless LAN.

By clearly identifying and mapping these domains up front, the framework ensures that subsequent evaluation steps, such as maturity scoring, risk analysis, and MITRE ATT&CK mapping, remain aligned with real-world operational contexts. This tailored approach lays a solid foundation for meaningful insights and effective roadmap planning later in the assessment. The section “Zero Trust Network Assessment Blueprint: Details of the Process,” later in this chapter, explains this phase in greater detail.

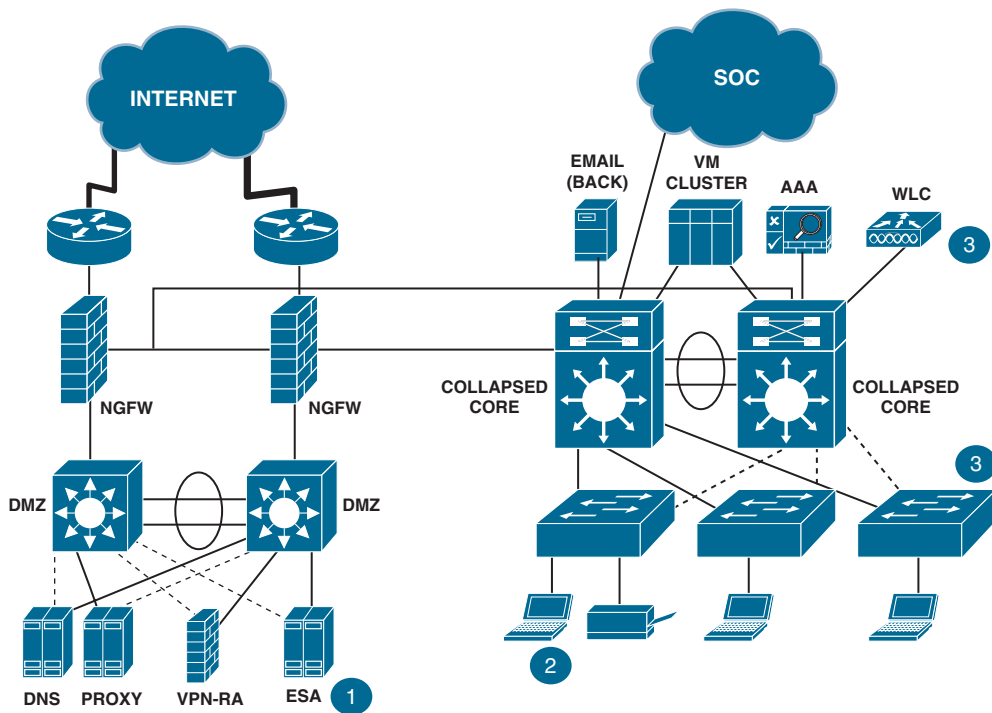


Figure 4-3 *Technical Domains Selection*

Step 2: Mapping the Technical Domains to Security Frameworks and Methodologies

Once the technical domains are defined, the next step is to map each one to the relevant security frameworks and methodologies. This mapping is essential to ensure that each domain is evaluated using industry-accepted principles and controls rather than in isolation.

By aligning the assessment to mature frameworks such as CISA Zero Trust, Zero Trust Architecture (NIST Special Publication 800-207), and Cisco SAFE, security teams can ground their evaluation in trusted, well-documented models that provide clear expectations for control effectiveness, maturity, and risk mitigation.

Each technical domain is associated with one or more Zero Trust pillars: Identity, Devices, Network, Applications & Workloads, and Data. This classification ensures a structured approach where gaps are not only identified but contextualized against security outcomes that are critical for business resilience. For example, a technical domain like Corporate Endpoints maps directly to the Devices pillar in CISA's model and can be further evaluated using Center for Internet Security (CIS) benchmarks, endpoint

EDR/XDR control objectives, and MITRE ATT&CK technique coverage. Table 4-1 illustrates how the technical domains map to the CISA Zero Trust pillars.

Table 4-1 *Technical Domains Mapped to CISA Zero Trust Pillars*

Technical Domain	CISA Zero Trust Pillar
Email Security	Devices
Corporate Endpoints	Devices
Wired and Wireless LAN	Network

After mapping the technical domains to the CISA pillars, we can map the technical domains to the NIST Zero Trust pillars, as illustrated in Figure 4-4.

Technical Domains Mapped to NIST SP 800-207 Pillars

Technical Domains	E-mail Protection (PEP) 	Endpoint Protection (PEP) 	Network Segmentation (PEP) 	NS Firewall Segmentation (PEP) 	Workload Segmentation (PEP) 	Behavior Analysis (PIP) 	Public Detection (PDP) 	Cross Layer/Components 
 Email Security	★							
 Corporate Computers		★						
 Wired and Wireless LAN			★					

Figure 4-4 *Technical Domains Mapped to NIST Zero Trust Pillars*

Finally, we can map the technical domains to the Cisco SAFE pillars, as shown in Table 4-2, to identify business flows and core technologies that will guide future roadmap planning.

Table 4-2 *Technical Domains Mapped to Cisco SAFE Pillars*

Technical Domain	Cisco SAFE Pillar
Email Security	Email Security Architecture
Corporate Endpoints	Endpoint Security Architecture
Wired and Wireless LAN	Access Network Segmentation

This step involves defining the verification criteria for each technical domain. Rather than relying on anecdotal controls or informal configurations, the *Strategic Zero Trust Readiness Assessment* leverages measurable benchmarks derived from recognized

industry frameworks. By doing so, the methodology enables consistent scoring, repeatable assessments, and a structured remediation process aligned with established security guidance.

By integrating Cisco SAFE architecture guidance, organizations also benefit from architecture-level recommendations that connect identified control weaknesses with practical platform and design enhancements. This approach incorporates vendor expertise into the methodology while preserving strategic and architectural neutrality.

Ultimately, this mapping step transforms a fragmented view of technical assets into a structured foundation for Zero Trust planning. It ensures that every domain is treated not as a standalone concern but as part of a unified defense model grounded in best practices.

Step 3: Conducting the Interview Process Based on Control Areas

Once the technical domains are defined and mapped to industry frameworks and methodologies, a team continues the *Strategic Zero Trust Readiness Assessment* process by conducting structured interviews using predefined control areas as the foundation. Each technical domain is broken into a series of control areas, identified using the standardized format ZTA-X.Y, where X refers to the domain number and Y corresponds to a specific control within that domain. This format creates a modular and scalable structure that supports repeatable assessments and facilitates future audits, roadmap creation, and benchmarking efforts.

Table 4-3 presents an example of the control areas to be reviewed for the Wired and Wireless LAN technical domain during the assessment interviews.

Table 4-3 *Control Areas Review*

Domain 3: Wired and Wireless LAN	
Control Area Reviewed	ID
Wired Network Segmentation & Microsegmentation	ZTA-3.1
Wireless Network Segmentation and Microsegmentation	ZTA-3.2
Zero Trust Network Access Based on Posture	ZTA-3.3
NAC—Wired Network Security Authentication (802.1X EAP-TLS)	ZTA-3.4
NAC—Wired Network Security Encryption (802.1AE MACsec)	ZTA-3.5
NAC—Wireless Network Security Authentication (WPA3 and EAP-TLS)	ZTA-3.6
NAC—Wired/Wireless Network Security Authentication (MAB)	ZTA-3.7
DNS Security and Sinkholing	ZTA-3.8
CIS Controls	ZTA-3.9
Deception and Honeytokens	ZTA-3.10

Domain 3: Wired and Wireless LAN	
Control Area Reviewed	ID
IT and OT Weak Authentication Security Monitoring	ZTA-3.11
Network Traffic Analytics (NDR)	ZTA-3.12

The interview process focuses on capturing both the design and operational state of each control area. For example, in the VPN Remote Access domain, one control area might focus on the enforcement of multifactor authentication, while another investigates whether secure web gateway inspection is applied to split-tunneled traffic. This level of granularity allows the assessment team to surface not only major architectural gaps but also subtle misalignments in configuration, integration, and policy enforcement.

Interview sessions are typically conducted with the subject matter experts (SMEs) responsible for operating or managing each respective domain—including network engineers, security analysts, system administrators, identity specialists, and application owners. To maximize the accuracy and efficiency of these sessions, the assessment team prepares domain-specific agendas in advance, outlining which control areas will be covered, who should participate, and what supporting documentation is recommended. This preparation minimizes disruptions and ensures that the discussion stays aligned with the control verification objectives.

Throughout each session, interviewers record observations, ask clarifying questions, and request artifacts such as architecture diagrams, configuration screenshots, and operational workflows. These artifacts play a vital role in verifying responses and identifying risks that might not surface with dialogue alone. The assessment team documents any misalignment with Zero Trust best practices and flags areas where controls are either missing, improperly enforced, or not monitored.

By structuring interviews around defined control areas, SZTRA transforms what could be an informal or inconsistent data-collection process into a focused, auditable, and evidence-based evaluation. This structured approach allows security leaders to confidently make decisions based on accurate insights, paving the way for a tailored roadmap that addresses real gaps with measurable actions.

Step 4: Evaluating the Technical Domains Maturity Level

After completing the interviews and documenting the current “as-is” state across each control area, the security assessment advances to the maturity evaluation phase. This step involves using the CISA Zero Trust Maturity Model 2.0 to benchmark each technical domain and classify its maturity as either Traditional, Initial, Advanced or Optimal. This model provides a government-backed, standards-aligned framework that reflects both cybersecurity best practices and the evolving threat landscape.

The goal of this step is to assess not just whether a security control is present but how effectively and consistently it is enforced. For example, an endpoint protection solution might be deployed, but if it lacks posture validation or fails to enforce least privilege

access, the technical domain may still fall into the Initial category. Similarly, a firewall with advanced threat detection may be categorized as Traditional if it lacks dynamic policy adaptation or is not integrated with a centralized policy engine. This step demands a comprehensive review of both technical capabilities and operational discipline. Technical domains are evaluated based on specific criteria, such as control automation, telemetry integration, identity validation, enforcement consistency, visibility, and threat detection response. These attributes, when mapped across all technical domains, create a complete maturity matrix that highlights which areas are lagging and which have reached advanced implementation.

To ensure objectivity, the security assessment team assigns maturity levels based on observed controls, corroborated evidence, and SME feedback. Subjective impressions or assumed capabilities are not accepted. Where possible, security logs, screenshots, policies, and system configuration files are used to validate enforcement depth.

Here's an example of a maturity level evaluation for the technical domains Email Security and Wired and Wireless LAN:

Technical Domain 1: Email Security; Maturity Level: Advanced

This domain showcases a robust and operationally mature security posture. The organization has implemented Cisco Secure Email Gateway (ESA) to full capacity and adheres to key email authentication protocols like DMARC, DKIM, and SPF. It also incorporates advanced threat detection technologies, such as sandboxing and behavioral analytics, to proactively detect phishing threats and malicious payloads before they reach end users. Regular security awareness training reinforces the organization's human defense layer, equipping users to recognize and respond to phishing attempts and social engineering. These collective efforts align with ZTA IDs ZTA-1.1 through ZTA-1.5, positioning the technical domain confidently in the "Advanced" category. The consistent implementation of essential controls across the enterprise reflects a well-integrated defense strategy, aligned with the layered protection principles defined by the CISA Zero Trust Maturity Model.

Technical Domain 2: Wired and Wireless LAN; Maturity Level: Initial

The network relies on VLAN-based segmentation, but it lacks the enforcement of microsegmentation required for granular traffic control. Critical safeguards like MACsec encryption and 802.1X authentication remain absent, and posture validation has been only partially implemented. The environment also lacks DNS-layer protections and does not incorporate Network Detection and Response (NDR) capabilities. These gaps reflect an early stage of Zero Trust maturity, signaling that foundational controls are in place but advanced enforcement is still missing. This domain depends heavily on static port security, with no comprehensive NAC framework in place and no use of certificate-based authentication for the corporate SSID. These limitations firmly anchor the domain within the "Initial" stage of maturity. Without identity-centric enforcement mechanisms, the environment lacks the foundational capabilities required to support a Zero Trust strategy.

Creating a graphical view of the current CISA Zero Trust maturity levels, as illustrated in Figure 4-5, helps communicate the organization's security posture to the executive board.

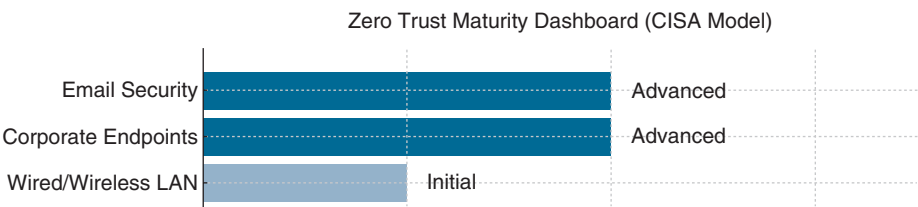


Figure 4-5 CISA Maturity Level Dashboard for the Domain Evaluation Example

Understanding maturity levels allows stakeholders to visualize the current security posture across domains. It helps establish a baseline, prioritize remediation plans, and forecast the level of effort required to advance to higher levels of resilience. Most importantly, it transforms the Zero Trust journey from a conceptual goal into an operational roadmap supported by measurable milestones and business-aligned security investments.

Step 5: Evaluating the Technical Domains' Risks and Severities

After assessing maturity, the next step is to determine the risk severity level for each technical domain. This process is guided by the NIST SP 800-30 risk assessment methodology, which offers a structured and repeatable approach for evaluating cybersecurity risk. The analysis considers two critical dimensions: the likelihood of a threat scenario occurring and the impact it would have on the organization if realized.

Likelihood is influenced by factors such as exposure to known attack vectors, the presence of threat intelligence indicators, existing vulnerabilities, and observed adversary behaviors mapped to MITRE ATT&CK techniques. For example, if a domain lacks MFA and is externally exposed through VPN, the likelihood of credential-based attacks is very high.

Impact, on the other hand, is evaluated by examining the potential business consequences of an attack, ranging from data breach exposure to service disruption, regulatory noncompliance, and reputational damage. The criticality of the assets within the domain plays a significant role in this evaluation. Domains that support identity systems, financial transactions, and business continuity functions typically carry high inherent risk impact. Each domain is rated using a risk matrix that plots likelihood against impact, resulting in a risk severity classification of Low, Moderate, or High (see Table 4-5). In some cases, a qualitative scale is supplemented with quantitative indicators such as incident logs, historical breach records, vulnerability scores (such as CVSS scores), or threat intelligence feeds. The goal is to maintain objectivity and enable comparative analysis across all domains.

Table 4-5 NIST SP 800-30 Risk Severity

Score	Severity Level
1, 2	Low
3, 4, 6	Medium
9	High

The following example presents a risk severity evaluation for the technical domain Wired and Wireless LAN:

Technical Domain: Wired and Wireless LAN; Risk Severity Level: Medium

Network segments provide limited isolation due to the absence of full microsegmentation, weak NAC posture enforcement, and insufficient traffic visibility. These shortcomings allow for potential lateral movement across the environment. In addition, wireless networks suffer from inadequate authentication mechanisms, specifically the lack of digital certificate-based access for the corporate SSID. Combined with minimal detection capabilities, these weaknesses significantly increase the technical domain's overall exposure and hinder Zero Trust enforcement. Given the breadth of access this technical domain controls and the number of missing advanced controls, the calculated risk severity is Medium (Likelihood: Medium $\times$ Impact: High) = $(2 \times 3) = 6$.

Figure 4-6 show a graph that illustrates the risk severity levels across technical domains, making it easier for the board of executives to understand and prioritize critical areas.



Chart Interpretation: Calculated as **Likelihood $\times$ Impact** for each technical domain.

High Risk (Score 9):

- **Email Security** is critical due to high exposure and systemic impact.

Medium Risk (Score 3, 4, or 6):

- Domains such as **Corporate Computers (Endpoints)** and **Wired/Wireless LAN** show considerable gaps that could enable lateral movement or data compromise.

Low Risk (Score 1 or 2):

- **No Other Technical Domains** had a low score in this example.

Figure 4-6 NIST SP 800-30 Risk Severity Level Dashboard for the Risk Severity Evaluation Example

By combining maturity data with risk severity, the assessment framework builds a multi-dimensional view of the organization's current posture. Domains that are both immature and carry high risk become immediate priorities for remediation, while advanced domains with low risk may only require monitoring and optimization. This step transforms isolated technical observations into a strategic risk map that supports executive decision making, investment justification, and compliance reporting. It ensures that remediation actions are technically sound and also aligned with business risk tolerance and operational urgency.

Step 6: Mapping the Technical Domains' Risks to MITRE ATT&CK TTPs

Once the assessment identifies the risks, severities, and uncovered security gaps within each technical domain, the next critical step is to contextualize these findings against the tactics, techniques, and procedures (TTPs) documented in the MITRE ATT&CK framework. This process shifts the analysis from abstract weaknesses to concrete adversarial behaviors observed in real-world attacks.

MITRE ATT&CK offers a globally recognized knowledge base that captures how threat actors operate during each phase of the attack lifecycle, ranging from initial access (for example, phishing or drive-by compromise) to command and control, persistence, and exfiltration. By mapping each identified gap or weak control area to specific ATT&CK techniques (for example, T1566: Phishing or T1078: Valid Accounts), the assessment team enhances visibility into what is vulnerable and how those vulnerabilities are most likely to be exploited in a live scenario. This correlation enables a more tactical and prioritized remediation plan. Instead of addressing gaps in isolation, organizations can frame security improvements through the lens of active threats, making each mitigation step more purposeful. For example, if the assessment reveals weak MFA enforcement in VPN access, linking this directly to T1078 (Valid Accounts) and T1021 (Remote Services) reinforces the urgency and justifies investment in Zero Trust access mechanisms.

Furthermore, this step enhances the organization's threat modeling capability. It allows security architects to simulate potential attack paths across domains and visualize how adversaries might move laterally from an initial compromise to more critical systems. The alignment between internal risk conditions and ATT&CK techniques also supports integration with detection engineering and SOC operations, allowing for refined alerting, telemetry enrichment, and playbook development.

The following example shows a MITRE ATT&CK mapping based on the previously identified risks for the Wired and Wireless LAN technical domain:

Technical Domain 1: Wired and Wireless LAN; Risk Severity Level: High

Network segments provide limited isolation due to the absence of full microsegmentation, weak NAC posture enforcement, and insufficient traffic visibility. These shortcomings allow for potential lateral movement across the environment. In addition, wireless networks suffer from inadequate authentication mechanisms, specifically the lack of digital certificate-based access for the corporate SSID. Combined with minimal detection capabilities, these weaknesses significantly increase the

domain's overall exposure and hinder Zero Trust enforcement. Given the breadth of access this domain controls, and the number of missing advanced controls, the calculated risk severity is High (Likelihood: Medium $\times$ Impact: High) = $(2 \times 3) = 6$.

MITRE ATT&CK Mapping: Techniques such as T1021: Remote Services and T1071: Application Layer Protocol are particularly relevant, given the identified gaps in the Wired and Wireless LAN domain. T1021 highlights how adversaries move laterally within the network by exploiting protocols like SMB, RDP, or SSH, especially in environments lacking proper segmentation and access control. T1071 focuses on how attackers use common application protocols, such as HTTP/S or DNS, to exfiltrate data or establish command-and-control channels, often blending into legitimate traffic. These techniques underscore the importance of enforcing least privilege, monitoring east-west traffic, and applying application layer controls.

Ultimately, by leveraging MITRE ATT&CK as a lens through which to interpret technical domain-level risks, the framework ensures that findings are translated into operational relevance. It helps CISOs and security leaders communicate threats in business-aligned language and accelerates decision making based on adversary-informed priorities.

Step 7: Mapping Business Flows to Cisco SAFE

To fully align security controls with business operations, the next step involves mapping critical business flows to the Cisco SAFE framework. Cisco SAFE provides a practical architectural blueprint that helps visualize the end-to-end journey of data, applications, and user interactions across the network. This structured mapping allows organizations to identify which protection points and control mechanisms must be in place to secure each stage of the digital interaction.

Using Cisco SAFE as a reference, Strategic Zero Trust Readiness Assessment overlays key business flows, such as user access to enterprise applications, branch connectivity to data center resources, or SaaS transactions, onto technology domains. This visual model highlights where controls like email protection, endpoint posture validation, threat analytics, microsegmentation, or identity-based access enforcement are required to reduce exposure and block lateral movement.

Figure 4-7 illustrates a business flow mapped to Cisco SAFE, highlighting the security technologies required to ensure effective protection based on the flow's origin and destination.

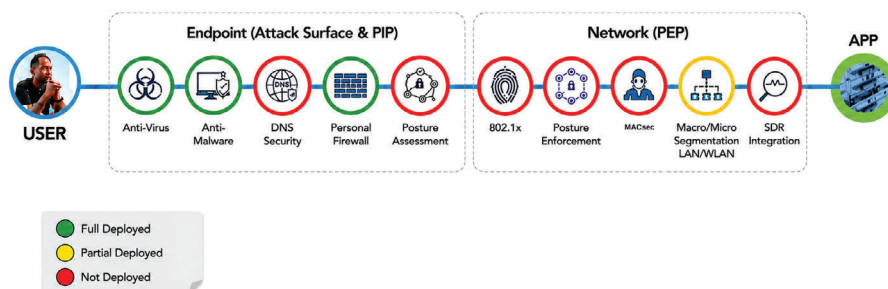


Figure 4-7 Cisco SAFE Business Flows Mapping

Ultimately, this step bridges technical controls and business realities, ensuring that security isn't built in isolation but supports operational continuity, user productivity, and resilience against modern threats. Mapping business flows to Cisco SAFE transforms abstract architectures into practical, threat-informed roadmaps. After completing all mappings and analyses, the assessment team will have the foundational material needed to develop a new technical roadmap. While this roadmap falls outside the scope of the assessment, it represents the logical next phase in the Zero Trust journey.

Step 8: Building the Roadmap

With all technical domains assessed and analyzed, Strategic Zero Trust Readiness Assessment bridges the gap between assessment and execution, marking the transition from diagnostic insight to strategic action. Step 8 marks the beginning of transformation, where insights gained from interviews, maturity evaluations, and risk analyses are synthesized into a clear, outcome-oriented roadmap. It's important to clarify that the roadmap is not part of the assessment itself. Instead, it represents a subsequent phase in the journey—one that builds on the findings gathered during the assessment. This roadmap does more than outline recommended improvements; it establishes a phased strategy that aligns cybersecurity evolution with the organization's overarching business objectives.

At this point, each recommendation is prioritized based on its impact on reducing risk, improving maturity, and closing critical security gaps. Rather than rely on generic guidelines, the roadmap integrates context-specific findings drawn directly from the technical environment. It proposes security enhancements that are feasible, measurable, and tailored to the existing infrastructure and operational capacity. The roadmap also reflects a long-term perspective: It separates tactical remediations from strategic investments, enabling security leaders to differentiate what must be addressed immediately from what should evolve over time.

The team should prioritize quick wins, such as refining policies or adjusting configurations, early in the implementation timeline. It should reserve more complex initiatives—such as rearchitecting access control with a NAC solution such as Cisco ISE or deploying microsegmentation through TrustSec—for later phases, when they can be aligned with available resources and the organization's readiness.

By using a technical domain-based structure, the roadmap supports cross-functional execution. Each technical domain is mapped to clear actions, maturity milestones, and performance indicators. This structure ensures that each improvement contributes to a coherent Zero Trust posture across the enterprise, without siloed or redundant efforts.

Ultimately, the roadmap serves as a living artifact. It guides decision making, facilitates stakeholder alignment, and provides measurable checkpoints for future assessments. In this way, the assessment evolves into a continuous journey that transforms isolated security efforts into a resilient, strategic architecture built on maturity, visibility, and risk-aware governance.

Figure 4-8 presents a proposed roadmap for the Wired and Wireless LAN technical domain example we've been looking at in this chapter, based on identified gaps and the risk severity assessment.

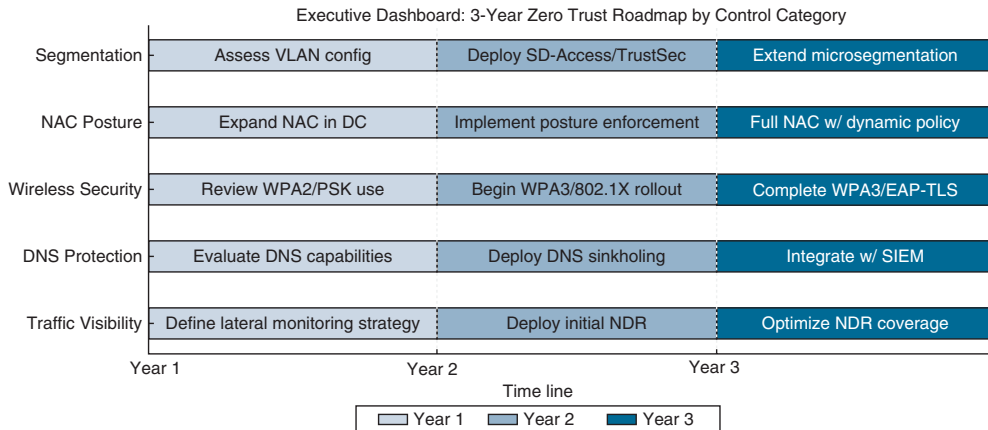


Figure 4-8 Roadmap Executive Dashboard for the Wired and Wireless LAN Technical Domain Example

Within the five phases of the security journey, the roadmap takes shape in Phase 4, and its effectiveness is evaluated in Phase 5. The next section provides a more detailed view of each phase.

Zero Trust Network Assessment Blueprint: Details of the Process

The Zero Trust journey is built to be modular, scalable, and repeatable across diverse industries and organizational sizes. Whether deployed for a multinational enterprise or a public-sector agency, the process enables decision makers to transition from uncertainty to informed action. It provides a snapshot of cybersecurity posture and a compass for navigating the future, where risk is understood, controls are optimized, and security becomes an enabler of innovation and trust. A security team should organize the journey into distinct technical projects, each divided into phases with clearly defined, structured steps. These steps provide the clarity and precision needed to guide the assessment process effectively. Figure 4-9 illustrates the five core phases of an individual Zero Trust project, each representing a distinct stage in the security journey lifecycle. Together, these phases form an end-to-end process that guides organizations from initial discovery through to resilience and continuous improvement.

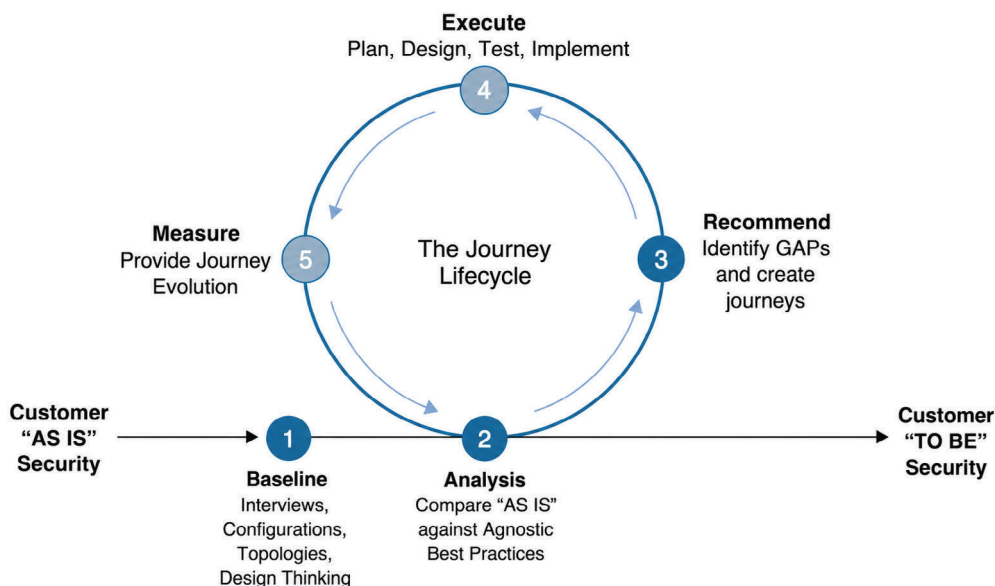


Figure 4-9 *The Five Lifecycle Phases of Each Project in the Journey*

This section provides a detailed explanation of each of the five phases, offering insight into how they collectively support a structured, outcome-driven security assessment and transformation journey:

1. **Security Baseline:** This phase begins with a deep and structured discovery process to document the “as-is” scenario. Through structured technical interviews and domain-specific analysis, the assessment team captures a detailed picture of the existing architecture, control implementations, and operational practices. The goal is to remove assumptions and replace them with evidence, capturing how security is truly operating on the ground.
2. **Environment Analysis:** With the current state documented, the next step is to uncover security and capability gaps. Through a maturity-based evaluation, the assessment benchmarks the organization against leading frameworks such as CISA’s Zero Trust Maturity Model. Also at this stage, risks are identified, quantified, and prioritized using the NIST 800-30 risk assessment guide. More importantly, these risks are tied to both adversarial threat behavior, using MITRE ATT&CK, and organizational maturity levels, to help stakeholders understand not just what is missing but why it matters.
3. **Recommend:** The analysis leads to a defined “to-be” scenario based on the details of the current gaps: a vision of the future that is more secure, more resilient, and strategically aligned with Zero Trust principles. This future state is not merely aspirational; it is supported by architectural diagrams, control recommendations, policy updates, and clear operational guidance. It is a scenario built for implementation, not theory.

4. **Execute:** In this phase, the recommendations are transformed into action. Technical plans, solution designs, testing protocols, and phased implementation strategies ensure that the journey from vision to execution is well managed. This phase emphasizes user adoption and operational excellence, recognizing that successful transformation requires more than deploying new tools; it requires activating them meaningfully.
5. **Measure:** Finally, the assessment framework incorporates a feedback loop to measure progress, track KPIs, and evolve the architecture in response to changing threats and business priorities. You can find additional details about both business and technical KPIs in Chapter 3, “The Security Journey: Business Strategy Alignment.”

With routine reassessment and strategic checkpoints, the Zero Trust journey becomes a continuous evolution, not a one-time initiative. The following sections provide a more detailed exploration of the core phases, offering greater clarity on their purpose, execution, and impact within the Zero Trust transformation journey.

Baseline: Mapping the Network to Technical Domains

Establishing a clear and structured foundation is essential for any cybersecurity assessment. To achieve this, the first phase of the assessment involves mapping the customer’s network infrastructure into distinct technical domains. This segmentation allows for a more targeted evaluation of each area, enabling the application of relevant security methodologies, risk models, and maturity benchmarks appropriate to the technologies and use cases involved.

The rationale behind this technical domain–based segmentation lies in the diversity of controls and implementation patterns required for different network components. For example, although Zero Trust principles recommend microsegmentation for both wireless access and data center environments, the technologies, operational practices, and architectural designs involved in securing these domains are vastly different. Evaluating them independently ensures a more accurate gap analysis and tailored set of recommendations.

Considering a generic production network topology, as illustrated in Figure 4-10, was dissected and aligned with the following 10 technical domains (which map to the numerals in the figure):

1. **Email Security:** This domain focuses on detecting and blocking email-borne threats such as phishing, malware payloads, and business email compromise (BEC). The assessment examines the configuration and effectiveness of email gateways, including controls like DMARC, DKIM, and SPF and advanced threat protection technologies.
2. **Corporate Endpoints:** In this domain, workstations and endpoint devices are evaluated for protection against malware execution, lateral movement, and privilege escalation. This includes reviewing the deployment of endpoint detection and response (EDR/XDR), Zero Trust policy enforcement, DNS filtering, and least-privilege configuration.

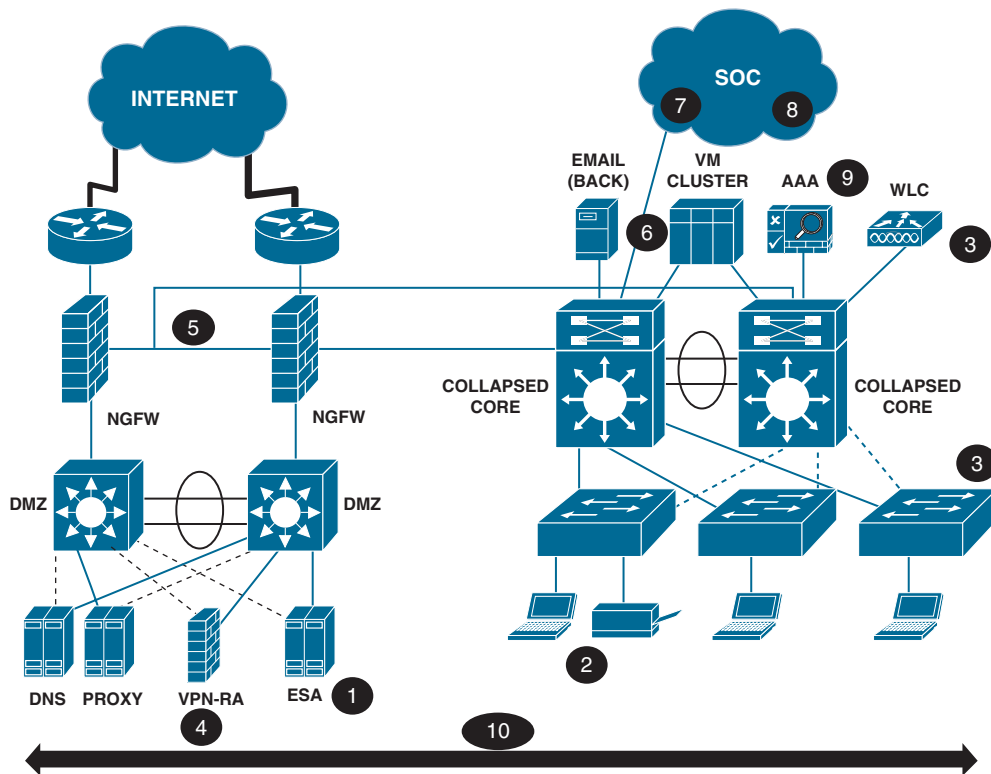


Figure 4-10 *Technical Domains Mapping*

3. **Wired and Wireless LAN:** In this domain, internal network access is assessed through the lens of network access control (NAC), segmentation policies, 802.1X enforcement, and encryption mechanisms like MACsec. The objective is to identify vulnerabilities that may allow unauthorized access or propagation of threats.
4. **VPN Remote Access:** This domain covers the secure enablement of inter-site and remote user connections. The analysis includes encryption strength, access segmentation, posture validation, and protections against command-and-control (C2) threat vectors.
5. **Data Center Firewall:** Firewalls play a critical role in isolating workloads and enforcing security policies within the data center. This domain evaluates intrusion prevention systems (IPSs), policy management practices, and microsegmentation readiness.
6. **Data Center Network:** In this domain, the virtualization layer, including hypervisors and virtual machines, is reviewed for workload segmentation, hardening standards, endpoint protection, and administrative access controls. Weaknesses in this domain can lead to lateral threat movement and containment failure.

- 7. Threat Detection and Response:** This domain involves the customer's capabilities for detecting, correlating, and responding to security events. The review includes SIEM, SOAR, and XDR integration, as well as the effectiveness of threat hunting and containment procedures.
- 8. Observability:** In this domain, observability solutions are assessed for their ability to provide performance visibility and context for threat detection. This domain analyzes tools like AppDynamics and ThousandEyes and evaluates how telemetry data is integrated into the broader response architecture.
- 9. Device Admin Control—AAA:** In this domain, privileged access to network infrastructure is reviewed for centralized policy enforcement, RBAC, audit logging, and multifactor authentication. The goal is to ensure that administrative actions are both secure and traceable.
- 10. Resilience and High Availability:** Finally, this domain addresses system redundancy and failover strategies, evaluating the customer's ability to maintain security operations during outages or attacks. This includes high-availability implementations across firewall, SIEM, VPN, and backup infrastructures.

Each of these domains has been mapped using the high-level topology provided, offering a clear view of how the assessment framework applies across the organization's infrastructure. This visual and contextual mapping establishes the baseline for evaluating security controls, maturity levels, and risk exposure in each area.

By mapping the customer's network to these technical domains, the assessment framework establishes a comprehensive structure for identifying maturity gaps, assessing risk, and designing targeted improvement roadmaps. This foundational step ensures that all future evaluations and recommendations remain grounded in the operational reality of the customer's infrastructure.

Baseline: Mapping Technical Domains to Zero Trust Frameworks

Establishing a reliable baseline requires more than just listing technologies. It demands the precise alignment of technical domains with recognized cybersecurity frameworks to ensure both contextual accuracy and strategic direction. This section defines that baseline by mapping each technical domain to the most appropriate pillars in two foundational models: the CISA Zero Trust Maturity Model and the NIST SP 800-207 Zero Trust Architecture.

This structured alignment ensures that each assessment area is evaluated under a consistent lens of best practices and architectural logic.

Mapping Technical Domains to the CISA Zero Trust Framework

The Cybersecurity and Infrastructure Security Agency CISA Zero Trust Maturity Model provides a clear and pragmatic structure for implementing Zero Trust architectures by organizing cybersecurity capabilities into five core pillars: Identity, Device, Network,

Applications and Workloads, and Data. These pillars establish the foundational security domains required to validate trust continuously, enforce least-privilege access, and reduce organizational risk exposure.

In addition to the five pillars, the framework also defines three cross-functional capability layers: Visibility and Analytics, Automation and Orchestration, and Governance. Unlike the primary pillars, these capabilities operate across the entire architecture rather than within a single domain. They provide the operational intelligence, coordination, and policy consistency necessary to sustain a mature Zero Trust strategy.

Visibility and Analytics plays a particularly important role within the framework because it acts as the operational “nervous system” of the Zero Trust architecture. This capability continuously collects telemetry from users, endpoints, applications, workloads, and network infrastructure to provide centralized visibility, behavioral analysis, anomaly detection, and threat correlation. Technologies such as SIEM, XDR, NDR, telemetry platforms, NetFlow, and threat intelligence services operate within this layer to help organizations detect malicious activity, validate policy enforcement, and support incident response activities across all Zero Trust pillars.

Because Visibility and Analytics spans the entire architecture, technical domains such as Observability naturally align with this cross-functional capability rather than with a single isolated pillar. Similarly, Device Administration Control solutions, including AAA and TACACS+ services, primarily align with the Identity pillar because they focus on administrator authentication, authorization, role-based access control, and privileged access enforcement across the infrastructure.

By mapping technical domains to the CISA Zero Trust Framework, organizations gain a structured methodology for evaluating security maturity, identifying operational gaps, prioritizing remediation activities, and aligning cybersecurity investments with recognized industry standards and business objectives.

For the customer in our example, each of the 10 technical domains is strategically mapped to the corresponding CISA Zero Trust pillar or Cross-Cutting Capabilities to ensure a cohesive evaluation that aligns with federal cybersecurity guidance and best practices:

- **Email Security and Corporate Endpoints:** These domains are assigned to the Device pillar because endpoints are frequently entry points for phishing, malware, and lateral movement. The Device pillar emphasizes posture validation, secure configuration, and endpoint-centric controls.
- **Wired and Wireless LAN, VPN Remote Access, and Data Center Firewall:** These domains fall under the Network pillar. These domains require robust segmentation policies, access enforcement, and encrypted traffic flows to mitigate internal threats and lateral traversal.
- **Data Center Network and Threat Detection and Response:** These domains align with the Applications and Data pillar. Controls within these domains must be tightly integrated into runtime environments, enabling security to follow the workload regardless of location.

- **Observability—AAA:** This domain belongs to the Visibility and Analytics cross-functional capability. This supports visibility, telemetry analysis, centralized logging, and least-privilege enforcement—critical components for both proactive defense and incident response.
- **Device Admin Control—AAA:** This domain maps primarily to the Identity pillar because it focuses on administrator authentication, authorization, and accountability across the infrastructure.
- **Resilience and High Availability:** This domain maps to the Cross-Domain pillar. This domain supports enterprisewide continuity and disaster recovery strategies that uphold Zero Trust principles, even during infrastructure failures or large-scale disruptions.

Table 4-4 provides a visual representation of how the technical domains map to the corresponding pillars of the CISA Zero Trust framework.

Table 4-4 *Technical Domains Mapped to CISA Zero Trust*

Technical Domain	CISA Zero Trust Pillar/Cross-Functional Capability
Email Security	Devices (Pillar)
Corporate Endpoints	Devices (Pillar)
Wired and Wireless LAN	Network (Pillar)
VPN Remote Access	Network (Pillar)
Data Center Firewall	Network (Pillar)
Data Center Network	Applications & Workloads, Data (Pillar)
Threat Detection and Response	Applications & Workloads, Data (Pillar)
Observability	Visibility and Analytics (Cross-functional)
Device Admin Control—AAA	Identity (Pillar)
Resilience and High Availability	Cross-Domain (None)

This mapping allows the organization to evaluate each domain’s maturity within CISA’s three-tier model (Traditional, Advanced, and Optimal), highlighting gaps and informing the roadmap for control evolution.

Mapping Technical Domains to the NIST 1800-35B Zero Trust Architecture

NIST’s 800-207 defines a practical Zero Trust reference model grounded in the concepts of Policy Decision Points (PDP), Policy Enforcement Points (PEP), and Policy Information Points (PIP). These core functions interact with control components such as ICAM, end-point security, analytics, and data protection.

Each technical domain is then mapped to the appropriate control component in the NIST 1800-35B reference architecture:

- **Email Security:** This domain maps to Email Protection (PEP), focusing on secure access to communication tools and protecting against phishing, spoofing, and malware-based attacks.
- **Corporate Endpoints, Wired/Wireless LAN, and VPN Remote Access:** These domains map to Endpoint Protection (PIP) and Network Segmentation (PEP), reflecting their combined responsibility in enforcing posture checks, segmentation, and secure remote access.
- **Data Center Firewall and Data Center Network:** These domains map to NG Firewall Segmentation and Workload Segmentation (PEP), given their critical role in protecting application workloads and enforcing east–west traffic control within data center environments.
- **Threat Detection and Response and Observability:** These domains map to both Behavior Analysis (PIP) and Policy Decision Points (PDP). These domains are essential for enabling real-time threat visibility, correlation, and dynamic policy enforcement based on observed behavior.
- **Device Admin Control—AAA:** This domain maps primarily to the Identity pillar because it focuses on administrator authentication, authorization, and accountability across the infrastructure. Solutions such as TACACS+, RBAC, and multifactor authentication help enforce least-privilege access and strengthen administrative security controls. This domain also supports Zero Trust principles by validating administrator identity before granting privileged access to network devices, reducing the risk of unauthorized configuration changes, credential abuse, and privilege escalation attacks.
- **Resilience and High Availability:** These domains map to Cross-Layer Components, which support authentication, identity governance, and operational continuity across all architecture layers. These components ensure robust policy validation and uninterrupted access even during adverse events.

Figure 4-11 illustrates the alignment between the technical domains and the corresponding control components of the NIST SP 800-207 Zero Trust Architecture, offering a visual reference for how core capabilities map across the framework.

This mapping enhances granularity and enables teams to identify which enforcement or decision point is most critical for each technical domain. By correlating the domains with the CISA and NIST Zero Trust models, organizations gain clearer visibility into how security controls, operational processes, and architectural components contribute to the overall Zero Trust strategy.

Technical Domains Mapped to NIST SP 800-207 Pillars

Technical Domains	E-mail Protection (PEP)	Endpoint Protection (PEP)	Network Segmentation (PEP)	NS Firewall Segmentation (PEP)	Workload Segmentation (PEP)	Behavior Analysis (PIP)	Public Detection (PDP)	Cross Layer/Components
 Email Security	★							
 Corporate Computers		★						
 Wired and Wireless LAN			★					
 VPN Remote Access		★	★					
 Data Center Firewall				★				
 Data Center Network					★			
 Threat Detection & Response						★		
 Observability						★		
 Device Admin Control - AAA							★	
 Resilience & High Availability								★

Figure 4-11 *Technical Domains Mapped to NIST SP 800-207 Zero Trust*

Once the technical domains in the ACME Bank scenario were successfully mapped to both the CISA and NIST Zero Trust frameworks, the team could begin evaluating the organization's current security posture. The next phase focused on assessing maturity levels across each domain and then progressing into risk severity analysis to identify the areas that required the highest remediation priority.

Analyze: The Maturity Level and Risk Severity Evaluation

To support organizations in strengthening their cybersecurity posture, the Cybersecurity and Infrastructure Security Agency (CISA) released the Zero Trust Maturity Model 2.0, which is a practical framework designed to guide the progressive adoption of Zero Trust principles. Rather than expect agencies and enterprises to immediately implement advanced Zero Trust capabilities, CISA provided this updated model, which introduces clear, structured benchmarks that accommodate organizations at various stages of maturity.

After the maturity level evaluation, the approach continues with NIST SP 800-30: Guide for Conducting Risk Assessments, which offers a structured process to identify assets, threats, and vulnerabilities and estimate the likelihood and potential impact of incidents. NIST SP 800-30 supports both qualitative and semi-quantitative methods, aligning well with regulatory requirements such as FISMA and ISO 27005. Its structure also aligns naturally with CIS Controls and Zero Trust domain assessments.

To enrich this assessment with real-world adversary context, the MITRE ATT&CK framework complements the NIST approach. MITRE provides a detailed mapping of TTPs used by threat actors. This enables teams to directly associate technical control gaps with common attack vectors such as credential dumping, phishing, and lateral movement.

Finally, to prioritize and communicate the results effectively, a risk heat matrix is applied. This model uses intuitive scoring for likelihood and impact, classifying risks as low, medium, or high. The matrix visually reinforces key risk areas, helping stakeholders quickly interpret the risk posture and prioritize mitigation strategies accordingly. The following sections explain the maturity level and risk severity methodologies in greater detail, providing the foundation for a structured security assessment.

Maturity Level Evaluation: CISA 2.0

The CISA Zero Trust Maturity Model has emerged as one of the most authoritative frameworks for evaluating the maturity of an organization’s Zero Trust journey. Designed to help public- and private-sector entities transition from traditional perimeter-based security toward a modern, identity-centric approach, the model offers both strategic guidance and actionable assessment criteria.

CISA’s model is structured around five foundational pillars: Identity, Device, Network, Applications & Workloads, and Data. These pillars are assessed across four maturity levels: Traditional, Initial, Advanced and Optimal. Each represents a stage in the evolution toward a fully integrated Zero Trust architecture. Figure 4-12 illustrates the Zero Trust maturity levels defined in CISA’s evaluation framework, providing a structured view of how organizations progress from foundational capabilities to a fully mature Zero Trust posture.

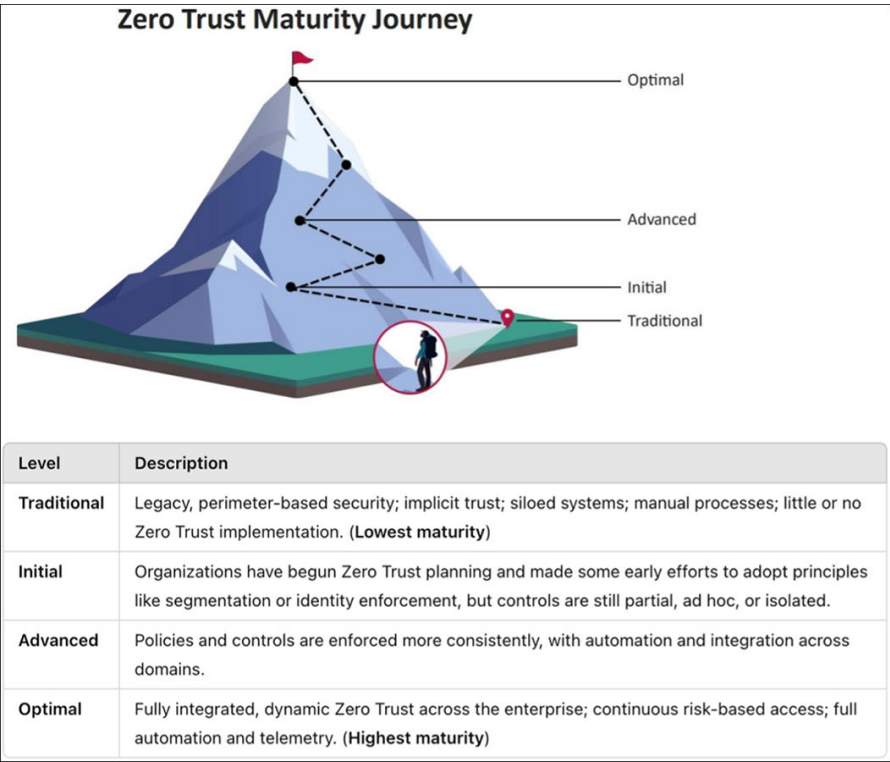


Figure 4-12 *The Zero Trust Maturity Journey*

These are the maturity levels in the CISA Zero Trust Maturity Model:

- **Traditional:** An organization at this maturity level relies heavily on manual processes, with limited visibility and perimeter-based controls. Identity validation often depends on passwords or static MFA, and network segmentation and data governance are minimal or ad hoc.
- **Initial:** An organization at this maturity level has some foundational Zero Trust practices, such as the use of single sign-on (SSO), basic endpoint health checks, early microsegmentation efforts, and structured inventory for data and applications. However, many functions remain siloed and lack orchestration or automation.
- **Advanced:** An organization at this maturity level is beginning to consolidate identity across systems, automate enforcement policies, and implement broader analytics across the environment. Technologies like phishing-resistant MFA, policy-based microsegmentation, continuous device posture assessment, and automated data classification are standard.
- **Optimal:** An organization at this maturity level has a fully integrated Zero Trust architecture. It achieves continuous validation and real-time risk analysis, dynamic policy enforcement across all domains, and deep visibility across the entire IT environment. Automated access decisions are made based on behavior, risk, and posture, and data is encrypted both in transit and at rest, with enterprisewide policy enforcement.

What distinguishes the CISA model is its practical alignment with operational realities. It avoids an all-or-nothing approach, recognizing that organizations progress incrementally. Each domain within the model is evaluated independently, allowing security leaders to identify specific gaps and prioritize improvements based on business risk and resource constraints.

Unlike theoretical frameworks, the CISA model is designed with implementation feasibility in mind. The model supports layered integration with existing cybersecurity programs such as NIST SP 800-207, the NIST Cybersecurity Framework (CSF), and the MITRE ATT&CK knowledge base. It also encourages adoption of automation and orchestration technologies as indicators of maturity, without prescribing specific vendor solutions. As a result, the CISA model serves as both a diagnostic tool and a strategic roadmap. It enables organizations to benchmark their current capabilities, communicate risk posture to executive leadership, and align technology investments with measurable security outcomes. Security architects and advisory teams benefit from having a shared language to structure assessments, define milestones, and guide Zero Trust transformation in a coherent and repeatable way.

In this chapter, the CISA model plays a central role in the assessment phase of the proposed framework. By measuring each technical domain against the CISA maturity stages, an organization gains a clear view of its “as-is” posture and the distance to an “Advanced” Zero Trust maturity level. Such insight is critical for building informed, risk-aligned roadmaps that convert strategy into security impact.

Risk Severity Evaluation: NIST SP 800-30, Risk Heat Matrix, and MITRE ATT&CK

Risk severity evaluation involves a hybrid risk evaluation model that integrates NIST SP 800-30, a risk heat matrix scoring system, and the MITRE ATT&CK framework. This combination offers a balanced approach to cybersecurity risk analysis, bridging structured governance, threat intelligence, and business-prioritized visualization in a scalable and practical way.

Together, these models offer a balanced approach that blends structured risk analysis, real-world threat intelligence, and executive-level prioritization. This combination ensures that strategic decisions are grounded in security best practices and also in the current threat landscape and the organization's operational context.

NIST SP 800-30: Guide for Conducting Risk Assessments provides the structural foundation of this approach. As one of the most recognized frameworks in the industry, it defines a formal methodology for identifying, evaluating, and prioritizing risk based on asset value, vulnerabilities, threat likelihood, and potential impact. In this assessment, NIST SP 800-30 is applied systematically across all technical domains. Analysts begin by identifying relevant assets, threat actors, and potential vulnerabilities. From there, they evaluate the likelihood of each threat exploiting a given vulnerability, taking into account existing security controls and environmental conditions. The resulting risk score is derived from the estimated likelihood and the projected impact of a successful exploitation. This method ensures that the evaluation remains consistent across technical domains while also aligning with widely adopted standards such as the NIST Cybersecurity Framework, FISMA, and ISO 27005. Because it supports both qualitative and semi-quantitative analysis, it also enables effective integration with broader Zero Trust initiatives and frameworks such as the CIS Controls framework.

To enrich the NIST-based structure with threat intelligence, the MITRE ATT&CK framework is used to map real-world adversarial behavior. MITRE ATT&CK catalogs hundreds of TTPs observed in actual cyberattacks. These TTPs are mapped to each domain based on relevance and known threat actor behavior. For example, phishing and credential theft tactics are mapped to email and identity security, while lateral movement techniques are associated with LAN and virtual machine domains. By mapping known attack techniques to existing control gaps, this model provides context for each technical domain's exposure to real-world threats. Furthermore, the integration of MITRE ATT&CK allows organizations to identify where detection and response capabilities, such as EDR, XDR, and SIEM telemetry, may be insufficient. In this way, MITRE ATT&CK adds a dynamic layer to the assessment, enabling security teams to align risk findings with active threat campaigns, detection engineering strategies, and red/blue team operations.

While the NIST and MITRE models support technical depth and operational relevance, executive stakeholders require a clear, visual way to understand and prioritize risk. To address this need, the assessment incorporates a qualitative risk heat matrix. This model applies a scoring grid that measures both likelihood and impact on a scale from low to high, typically using values from 1 to 3. Each identified risk is assigned a pair of scores: one for likelihood and the other for impact. These values are then multiplied to produce a severity score. For example, a high-likelihood, high-impact risk receives a score of

9 ($3 \times 3 = 9$) and is categorized as critical. A high-likelihood, medium-impact risk scores a 6 ($2 \times 3 = 6$) and is categorized as high. This scoring model enables analysts to present cybersecurity risks in a format that resonates with business leaders. It supports dashboard visualizations, facilitates prioritization discussions, and provides a shared language for risk management across security and executive teams.

This hybrid assessment model is applied individually across all technical domains. For each domain, the assessment begins by identifying relevant threats using MITRE ATT&CK mappings. It then applies the NIST SP 800-30 framework to evaluate the likelihood and impact of each threat scenario, taking into account the organization's existing control maturity. A risk heat map is then generated to visualize the results and highlight areas of elevated risk. These findings are then cross-referenced with the Zero Trust Maturity Model, particularly focusing on where the domain's controls align with "Initial" or "Traditional" levels. Where risk and low maturity intersect, the report delivers actionable recommendations to close the gap, referencing the Cisco SAFE architecture, NIST best practices, and CIS Controls model.

Finally, each domain includes an executive risk summary. This summary identifies the domain in question, describes the specific risk or vulnerability, and presents the calculated severity score based on the product of likelihood and impact. These summaries are crafted to facilitate risk-based decision making at the leadership level, enabling security teams to communicate technical findings in a format that drives strategic alignment. The result is a comprehensive, threat-informed, and maturity-aware assessment that not only identifies weaknesses but provides a clear path to remediation and long-term resilience within a Zero Trust framework.

Executive Risk Summary: Heat Map Calculation

To evaluate risk in a way that is both structured and actionable, the assessment model assigns a risk score to each observed threat scenario within a specific technical domain. This score is not arbitrary. Instead, it results from a logical breakdown that considers five core elements derived from the National Institute of Standards and Technology NIST SP 800-30 risk assessment methodology: threat, vulnerability, likelihood, impact, and overall risk. Together, these elements provide a complete picture of how and where risk manifests within the environment.

The threat represents the potential event or adversarial action capable of causing harm. The vulnerability identifies the weakness or exposure that could allow the threat to succeed. Likelihood measures the probability of the event occurring, while impact evaluates the potential operational, financial, or business consequences if the event takes place. The resulting risk score combines these elements to help prioritize remediation activities and strategic decision-making.

To start a risk analysis, the assessment methodology evaluates the environment step by step, or more specifically, element by element. This structured approach, aligned with the National Institute of Standards and Technology NIST SP 800-30 methodology, helps ensure that risks are analyzed consistently, objectively, and within the correct operational

context. Rather than relying on subjective assumptions, the model breaks risk evaluation into multiple analytical elements that together provide a complete understanding of the organization's exposure.

The first element of the analysis is the technical domain itself, the functional area where the risk has been identified. This domain represents the environment in which threats, vulnerabilities, and operational exposures are evaluated. Examples include the VPN remote access infrastructure, the email security environment, or the data center firewall layer. Each domain contains different technologies, user interactions, trust boundaries, and exposure points. As a result, every domain must be assessed independently to preserve analytical accuracy and contextual relevance.

The second element is the threat. Within the context of the assessment, the threat represents the potential adversarial action, attack technique, or operational event capable of causing harm to the environment. Examples include phishing campaigns, credential theft, ransomware deployment, unauthorized remote access, or lateral movement activities. The threat defines what could potentially happen to the environment if adequate protections are not in place.

The third element is the vulnerability. This represents the specific weakness, exposure, or missing control that could allow the threat to succeed. For example, within the email security domain, the vulnerability might involve the absence of DMARC enforcement or inconsistent SPF alignment. Within the VPN remote access environment, the vulnerability could involve missing multifactor authentication or inadequate posture validation controls. The objective of this phase is to identify clearly which weakness could be exploited and how the exposure could enable a successful attack or operational compromise.

The fourth factor is likelihood, which represents the estimated probability that the identified threat could successfully exploit the observed vulnerability. This estimation does not rely on assumptions or guesswork. Instead, it results from contextual analysis involving the organization's existing controls, detection capabilities, threat intelligence, operational maturity, and current attack trends. A vulnerability actively targeted in real-world attacks, combined with weak monitoring or detection mechanisms, would naturally receive a high likelihood score.

Impact represents the fifth element of the model. This component evaluates the potential business consequence if the threat successfully exploits the identified vulnerability. Impact is analyzed using business-oriented criteria, including operational disruption, financial losses, data exposure, regulatory violations, reputational damage, or service interruption. For example, a successful credential-dumping attack against an Active Directory-integrated environment could enable privilege escalation, lateral movement, and compromise of critical identity infrastructure, resulting in a high-impact classification.

After evaluating threat, vulnerability, likelihood, and impact, the assessment calculates the overall risk severity score. Both likelihood and impact are evaluated using a three-point scale: low (1), medium (2), or high (3). The final severity score results from multiplying the likelihood and impact values. A scenario with high likelihood and high impact

receives the maximum score of 9, which classifies the risk as critical. A medium likelihood combined with a high impact produces a score of 6, categorized as high severity. This methodology allows security teams to convert technical findings into a measurable and business-oriented prioritization model that executives and operational teams can easily understand (see Figure 4-13).

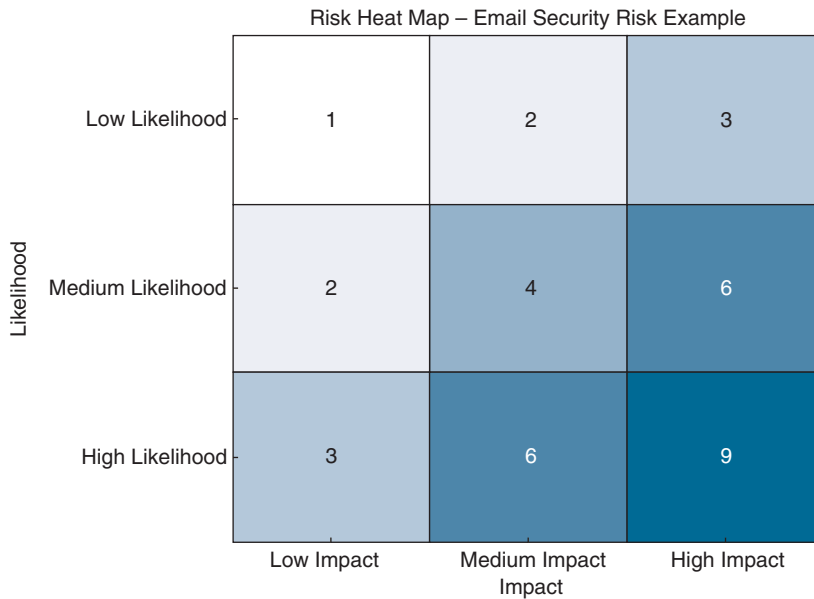


Figure 4-13 *Risk Score Heat Map*

This structured methodology enables organizations to prioritize risks in a consistent, data-driven manner, aligned with both operational context and strategic goals. It transforms the abstract idea of risk into a quantifiable, explainable, and actionable insight.

Recommend: Mapping the Business Flows to Cisco SAFE

With the foundational knowledge developed in Chapter 3 (how to engage stakeholders, connect cybersecurity initiatives to business priorities, and construct a roadmap anchored in risk reduction and operational resilience) and what you have learned so far in this chapter, you are now prepared to translate strategic intent into practical architectural blueprints.

This section introduces the next logical step: bringing strategy to life through architecture. While Zero Trust is based on universal principles such as least privilege, identity verification, segmentation, and telemetry correlation, its implementation must adapt to each organization's operational realities. Cisco SAFE provides a practical, technology-neutral framework to guide this effort. SAFE focuses on protecting business-critical interactions

between users, applications, and data by defining enforcement points where security controls must operate with precision.

Figure 4-14 illustrates this concept by overlaying business flows onto a real-world technology stack, categorized into architectural layers such as endpoint, network, data center, email, and analytics. Each segment is marked with controls—such as antivirus, posture assessment, SSL decryption, microsegmentation, and behavioral analytics—that are mapped to their respective ZTNA enforcement points (Policy Enforcement Points [PEPs]) and trust decision engines (Policy Decision Points [PDPs]). This visual map categorizes deployments into fully implemented, partially implemented, or not yet deployed, allowing teams to quickly identify exposure areas and prioritize remediation.

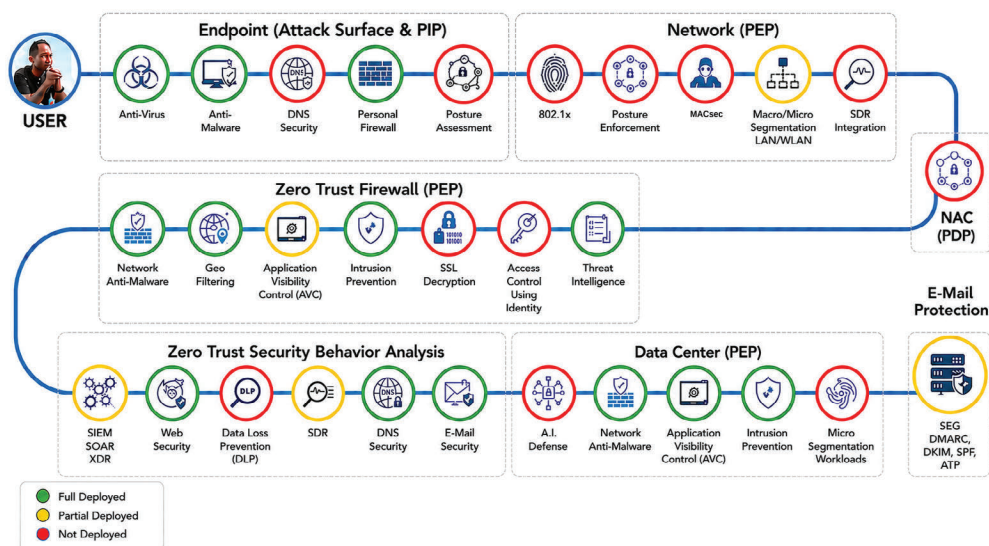


Figure 4-14 Core Technologies Map

The strength of this mapping lies in its ability to connect security decisions to business processes. For example, a retail organization might prioritize endpoint posture and email threat defense to protect against phishing-led fraud, while a healthcare provider might emphasize segmentation and data loss prevention (DLP) to guard patient data under regulatory constraints. This tailored view ensures that security architecture is contextual, deliberate, and responsive to business risk rather than generic.

Moreover, this model reinforces the idea that *Zero Trust is not a product*; it's a journey of incremental adoption, anchored in visibility and continuous improvement. SAFE acts as the compass, ensuring that each business-critical flow, from users to cloud applications, from branch offices to core services, passes through clearly defined security checkpoints.

Organizations should maintain this architectural map as a living artifact. It should evolve in tandem with digital transformation initiatives, new threat vectors, and shifting business models. By periodically updating the SAFE-based diagram, security leaders can maintain

alignment between evolving risks and deployed controls, ensuring long-term security posture relevance and investment efficiency.

In practice, this approach is the cornerstone of an adaptive security strategy. It empowers architecture teams to communicate clearly with executives and auditors, justifies investment decisions based on visible control gaps, and ensures that security initiatives always contribute to business outcomes, not just compliance checklists. Ultimately, mapping business flows to Cisco SAFE transforms Zero Trust from theory into day-to-day, operational security excellence. Ultimately, this will serve as the foundation for the future roadmap presented to the customer, offering clear visibility of the solutions required throughout the security journey.

Recommend: Mapping SAFE Capabilities to Zero Trust Core Components

This section bridges strategy with execution by mapping each Zero Trust domain to representative control area that enable control, visibility, and resilience. Each domain corresponds to a critical security area, ranging from endpoint protection and network access to data center security and email infrastructure. Within each domain, selected technologies are listed not just for their technical capabilities but for their strategic role in supporting Zero Trust outcomes.

It is important to emphasize that this mapping serves only as a reference model. The actual technologies selected will vary based on the organization's business priorities, security maturity, regulatory environment, and existing architecture. What works for one enterprise may be inappropriate for another. Therefore, each implementation should be guided by a contextual evaluation of current gaps, future goals, and specific risk exposures.

To build an effective Zero Trust architecture, organizations must implement layered technologies that secure key control points across the infrastructure. Rather than focus solely on tools, this section explains why each technology matters within the Zero Trust journey, bridging technical functionality with strategic security goals. Figure 4-15 presents a graphical illustration of how Cisco SAFE business flows align with Zero Trust Network Access (ZTNA) principles.

Here is a detailed explanation of the mapping illustrated in Figure 4-15:

1. **Securing the endpoint: The first line of defense (PIP):** Zero Trust begins at the user's device, which is the most exposed and frequently targeted entry point. To secure this layer:
 - Antivirus and anti-malware solutions identify and neutralize known threats before they establish persistence on the device.
 - DNS security blocks access to malicious domains, disrupting command-and-control communications.
 - Personal firewalls manage inbound and outbound traffic for each device, limiting exposure and reducing the local attack surface.

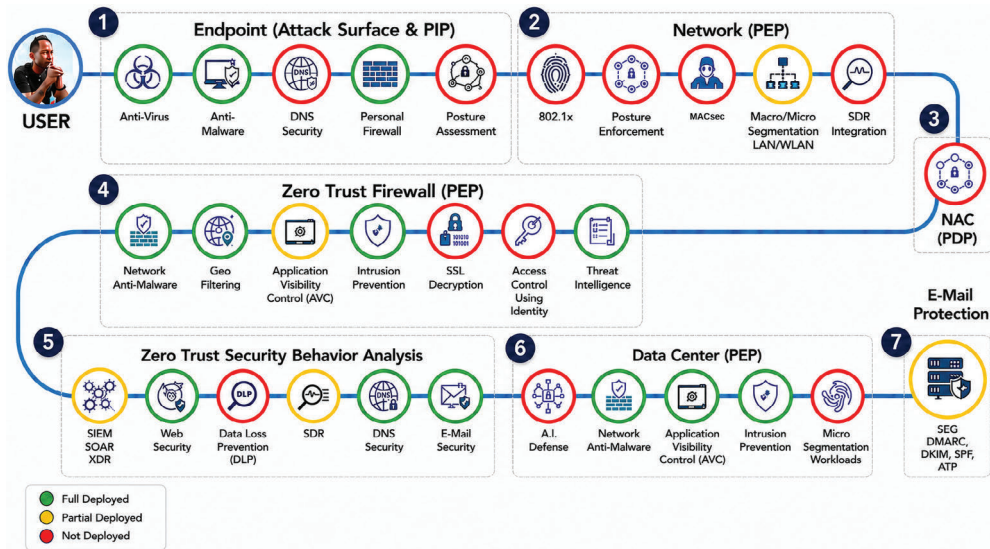


Figure 4-15 Cisco SAFE Versus ZTNA Core Mapping

2. **Enforcing the policy across the network layer (PEP):** The network acts as a powerful policy enforcement point when properly segmented and secured:
 - 802.1X authentication ensures that only validated devices and users gain network access.
 - Posture enforcement dynamically grants access based on the endpoint's compliance status.
 - MACsec encrypts Layer 2 traffic to prevent unauthorized monitoring of local segments.
 - Microsegmentation isolates workloads, even within the same VLAN, to block lateral movement.
 - Network detection and response (NDR) systems analyze NetFlow metadata to uncover hidden behavioral anomalies.
3. **Centralizing access decisions with network access control (PDP):** Network access control (NAC) solutions serve as the policy decision point for user and device access. They apply rules based on identity and posture, making them essential for enforcing least privilege and dynamic segmentation across enterprise environments.
4. **Defending network boundaries with Zero Trust firewalls (PEP):** Modern firewalls play a key role in preventing unauthorized access and threat propagation:
 - Network anti-malware engines inspect and block malicious traffic at the perimeter.
 - Geofiltering restricts traffic from untrusted or unnecessary geographic regions.

- Application visibility enforces usage of sanctioned business applications, blocking unauthorized software.
 - Intrusion prevention systems detect and halt adversarial techniques and exploits in real time.
 - TLS decryption reveals threats hiding in encrypted traffic, enabling deeper inspection.
 - Identity-based access control applies security policies based on user roles, reinforcing least privilege.
 - Threat intelligence feeds add global context to improve detection accuracy and decision making.
- 5. Enabling continuous monitoring and threat response:** Behavioral analytics provide the visibility and context necessary to detect and respond to threats in real time:
- SIEM, SOAR, and XDR platforms collect telemetry, automate responses, and support proactive threat hunting.
 - Web security solutions block access to phishing sites and known malicious URLs before users are compromised.
 - Data loss prevention (DLP) tools detect and prevent the unauthorized transfer of sensitive data.
 - Flow analytics monitor both internal and external traffic for anomalies that indicate compromise.
 - DNS security reinforces visibility and blocks outbound attempts to reach attacker infrastructure.
 - Artificial intelligence defends against unknown threats by identifying behavioral deviations and improving detection speed.
- 6. Securing the data center and core workloads (PEP).** The data center contains the organization's most critical assets. To protect this core:
- AI-based defenses identify advanced persistent threats aimed at servers and critical infrastructure.
 - Network anti-malware scans data traffic to prevent infection or propagation within the data center.
 - Application visibility and control ensure that only approved applications can operate.
 - Intrusion prevention mechanisms block exploitation attempts and limit attacker movement within internal segments.
 - Microsegmentation restricts access between workloads, reducing the blast radius in the event of compromise.

7. Protecting the email channel—A high-risk entry point: Email remains one of the most targeted vectors in cyberattacks:

- Secure email gateways (SEGs) prevent phishing, business email compromise (BEC), and malware before messages reach end users.
- Email authentication standards such as DMARC, DKIM, and SPF stop domain spoofing and impersonation attacks.
- Advanced threat protection (ATP) solutions analyze email content in real time, detonating suspicious attachments and links in sandboxes before delivery.

With the technology landscape now clearly mapped and aligned to business priorities, the strategic intent of the Zero Trust journey begins to take tangible shape. Each architectural layer, whether it protects endpoints, enforces segmentation at the network, or provides behavior-based detection across the environment, serves a defined purpose in reducing exposure, detecting threats, and supporting resilient operations.

However, knowing what controls should be in place is only part of the equation. The next critical step is to assess how well these controls are implemented, identify where meaningful gaps remain, and understand the risks associated with current weaknesses. This is where analysis becomes essential—not just to verify deployment but to evaluate maturity, measure effectiveness, and prioritize improvements.

Chapter 5, “Field Validation: A Step-by-Step Case Study in Threat and Risk Assessment,” focuses on evaluating maturity levels and risk severity in a simulated real-world scenario.

Summary

The scent of coffee and the quiet hum of the office had replaced the ocean breeze, but Andrew carried Henry’s lessons with him. His mindset had changed. He no longer viewed cybersecurity as a collection of isolated technologies. Now, every tool, every control, needed to serve a purpose: advancing the business. But before he could build a strategy, he needed to understand where the business stood. And for that, he needed help.

That’s when Fredy stepped in, not just as a colleague but as a guide through the complexity of assessments. Together, they began shaping the first phase of the journey: planning the steps to diagnosing the current state. They carefully defined the technical domains, mapped them to Zero Trust pillars, and developed the questions that would surface hidden risks and operational blind spots. It wasn’t just about finding gaps; it was about building a foundation for transformation.

Andrew hadn’t launched the assessment yet, but he was ready. This phase marks the shift from strategy to structure, from vision to planning. He and Fredy weren’t chasing checklists; they were building the lens through which the business’s real security posture would be revealed. Now they are finally ready to turn that lens toward reality.

Lessons Learned

This chapter marks a critical transition in Andrew's cybersecurity journey, from strategy design to operational execution. Andrew's collaboration with Fredy involved using a structured and repeatable framework, the Strategic Zero Trust Readiness Assessment (SZTRA), to assess cybersecurity maturity and evaluate risk severities across multiple technical domains. Several important takeaways emerged from their planning phase:

- **Clarity emerges through mapping.** Translating high-level Zero Trust principles into technical domain assessments requires a deliberate mapping process. By aligning each domain with CISA's Zero Trust pillars, NIST's core components, and Cisco SAFE architecture, Andrew and Fredy ensured that their evaluation would reflect both technical depth and business relevance.
- **Frameworks guide the process.** CISA Zero Trust Maturity Model, NIST ZTA Core, and MITRE ATT&CK offered more than structure; they provided a common language for evaluating current states, identifying risks, and planning remediation.
- **Interview design is strategic.** The value of the technical interviews lies in their intentional design. By planning who to interview, what to evaluate, and how to correlate controls with maturity, Andrew and Fredy laid the foundation for a highly effective diagnostic phase.
- **Visual communication matters.** The use of matrixes, heatmaps, and SAFE flow diagrams enhanced Andrew and Fredy's ability to present findings to both technical and executive audiences. Clear visuals became a bridge between complex technical data and high-level decision making.
- **The assessment is not the destination.** While this chapter emphasizes planning and framework alignment, it reinforces a key truth: Assessments are valuable only if they feed into actionable roadmaps. The real transformation begins when findings are used to define prioritized actions, risk mitigation, and long-term governance strategies.
- **Stakeholder alignment is foundational.** Andrew and Fredy's early efforts to involve domain experts and align with business goals will be critical to the success of the next phase. The groundwork they laid here will streamline the execution and adoption of Zero Trust initiatives across the organization.

Andrew and Fredy wrapped up the day with a sense of accomplishment. Through hours of discussion and analysis, they had built a structured and detailed plan that was solid enough to serve as the foundation for the upcoming security assessment execution (see Figure 4-16). The roadmap was clear, the objectives were aligned, and their roles were well defined.

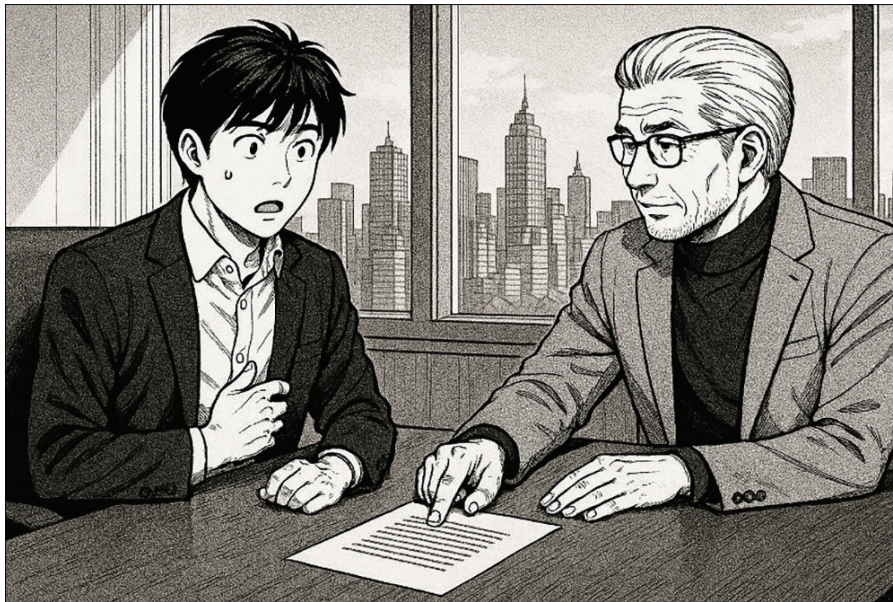


Figure 4-16 *The Next Step: Execute the Security Assessment Plan*

As they gathered their notes and prepared to leave, Fredy offered one final piece of advice. He reached into his bag, pulled out a small book, and handed it to Andrew. “Before we dive into execution,” he said, “I want you to read this: *The Allegory of the Cave* by Plato. It’s philosophy, not cybersecurity, but trust me, the insights in there will help you during the final phase of our assessment.”

Andrew looked at the worn cover and then at Fredy. He smiled, intrigued but puzzled. “Philosophy?” he asked with a raised brow.

“You’ll understand when the time comes,” Fredy replied, already walking toward the door.

Andrew tucked the book under his arm, unsure of its relevance, but something about Fredy’s confidence made him take it seriously. As the sun dipped behind the skyline, casting long shadows across the office floor, Andrew felt both ready and curious—for the work ahead and for the deeper meaning hidden in the pages of that old book.

With strategic planning, mapping, and interview preparation in place, the next chapter shifts the narrative from theory to real-world application.

References in This Chapter

Center for Internet Security (CIS). (2023). *CIS Critical Security Controls*. Retrieved from <https://www.cisecurity.org/controls>

- Cisco Systems. (2023). *Cisco SAFE Overview Guide*. Retrieved from <https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.html>
- Cisco Systems. (2026). *Protect Your Hybrid Workforce with Converged, Cloud-Native Security*. Retrieved from <https://www.cisco.com/site/us/en/products/security/secure-access/index.html>
- Cisco Systems. (2026). *Zero Trust Everywhere: Cisco's Zero Trust Access Solution Overview*. Retrieved from <https://www.cisco.com/c/en/us/products/collateral/security/secure-access/zero-trust-access-so.html>
- MITRE. (2023). *MITRE ATT&CK*. Retrieved from <https://attack.mitre.org>
- U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Zero Trust Maturity Model*. Retrieved from <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>

Index

Numbers

4G/5G LTE interfaces, configuring, 320–328
20-day patch deployment, 400
802.1X attacks, 271
 bridge, 274–277
 bypasses, 271–274
 MACsec, 274–277, 280–285
 packet injection, 280–285
 protocol exposure, 277–280
 undetected mobile access, 285–287

A

access layer, restoring trust, 467–469
access points, use cases, 534–538
access points onboarding, use cases, 539–542
access switches, attacks, 348–352
account takeover (ATO) fraud, 7–8, 49
ACME Bank Management Project case study, 582

PDI (Plan, Design, and Implement) methodology, 582–583
Zero Trust, 583–629

ACME Bank: Strategic Zero Trust Network Architecture Assessment case study, 193–196
 environment analyze phase, 203–245
 execute phase, 249–253
 five-phase security lifecycle, 198
 recommend phase, 249–253
 scope and methodology, 196–198
 security baseline phase, 198–203
ACME Petroleum OT Infrastructure case study, 142–145
Active Directory, Cisco ISE integration, 554–562
advanced lateral movement, 771–772
advisory services, 121
AI (artificial intelligence)
 AI Defense, 120
 CaaS (Cybercrime-as-a-Service), 43
 cybercrime, 71–72
 cybersecurity, 38–42
 evidence analysis, 83–84

- evidence destruction, 82
- law enforcement countermeasures, 71–72
- networking, 117
- phishing, 42
- AI-assisted vulnerability discovery, 398
- AI-assisted vulnerability lifecycle, 406–407
- AI-driven ransomware attacks, 27–29, 32–35
 - defense strategies, 35–38
- AI-enhanced social engineering, 6
- AI-generated fraud, 6
- alignment, cybersecurity strategies, 135–137
- allowlist devices, use cases, 508–509
- anti-forensics techniques, 79–82
- APT29 (Cozy Bear) cybercrime group, 78
- architecture
 - macrosegmentation, 700–715
 - TrustSec, 581
- Argentina National Directorate of Migration ransomware attack, 25–26
- Art of War, The*, 55, 111
- artificial intelligence (AI). *see* AI (artificial intelligence)
- Atlanta city government ransomware attack, 23–24
- ATO (account takeover) fraud, 7–8
- attack bridges, configuring, 319–320
- attack execution teams, cybercrime group organizations, 58
- attacks, 339–340. *see also*
 - cybercrime; fraudulent device attacks; insider threats
 - 802.1X, 271
 - bridge, 274–277
 - bypasses, 271–274
 - MACsec, 274–277, 280–285
 - packet injection, 280–285
 - protocol exposure, 277–280
 - undetected mobile access, 285–287
- access switches, 348–352
- clues, 360
- counterattacks, 371–373
 - AI-assisted vulnerability discovery, 398, 426–447
 - behavioral profiling analysis, 449–456
 - Cisco SAFE translation, 378
 - Foundation-Sec-8B leveraging, 459–462
 - intrusion path mapping, 448–449
 - PINs, 390–398
 - Project Glasswing, 398–410
 - security-specialized LLMs, 457–459
 - SOC operations, 457–459
 - Zero Trust, 373–377
- detection failures, 348
- execution, 340–341
- financial institutions, 60–61
 - Brazilian hackers, 60–61
 - on-path attacks with fraudulent devices, 61–67
- fraudulent device
 - case studies, 304–306
 - Chupacabra, 303–304
 - configuring, 306–334
 - exposure, 301–302
- fraudulent device attacks, 287–295
- Generation 7 on-path, 361–366

- insider, thinking like, 573–574
- insider threats, motivations, 360–361
- modus operandi, 358–360
- phases, 56–57
- remote tunnel access, 341–343
- targets
 - endpoint IP and MAC address cloning*, 346–348
 - endpoint network addresses*, 344–345
 - identification*, 341–348
- audit logging, SQL injection, 436–437
- authentication
 - SQL injection, 429–430
 - TPS (transactions per second), 483–484
 - TrustSec, 580
 - weaknesses, 802.1X, 277–280
- authority bias, 10
- authorization, broken administrative, 433–434
- automated attack deployment, 14

B

- Babuk ransomware group, 26–27
- Baltimore city government
 - ransomware attack, 25
- Bangladesh Bank heist, 92
- Baudelaire, Charles, 339
- BEC (business email compromise), 6
- BEC (business email compromise)
 - scams, 47
- behavioral analytics, Zero Trust, 414, 420
- behavioral profiling analysis, 449–456
- Berra, Yogi, 193
- black market, hacking tools, 85
- BlackEnergy malware, 16
- blockchain analysis, 69
- blockchain forensics, tracing criminal transactions, 72–73
- botnet operators, cybercrime group organizations, 58
- botnets, 86
- brand protection, preserving, 115
- Brazilian hackers, 60–61
- breach protection, 119
- bridge attacks, 274–277
- bridge bypass, 276–277
- bridges
 - attack, configuring, 319–320
 - cellular, bypasses, 292
 - management, configuring, 316–319
 - wireless, bypasses, 290–292
- broken administrative authorization, 433–434
- brokers, cybercrime group organizations, 59
- business email compromise (BEC), 6
- business email compromise (BEC)
 - scams, 47
- business flows, mapping to Cisco SAFE, 167–168
- business outcomes, 147
 - defining, 114–115
- business-focused KPIs, 123–124
- business-logic, funds transfers flaws, 434–435
- BYOD access, managing, 115
- BYOD mobile devices, use cases, 527–530
- bypasses
 - 802.1X attacks, 271–274
 - authentication, client headers, 430–431

cellular bridge, 292
 IoT devices, 280
 transparent bridge, 276–277
 wireless bridge, 290–292

C

CaaS (Cybercrime-as-a-Service)

AI, 43
 hacking tools, 85–86

campaign coordinators, cybercrime
 group organizations, 58

case studies

ACME Bank Management
 Project, 582
*PDI (Plan, Design, and
 Implement) methodology,*
 582–583

*PDI (Plan, Design, and
 Implement) methodology
 with ZeroTrust, 583–629*

ACME Bank: Strategic Zero
 Trust Network Architecture
 Assessment, 193–196
environment analyze phase,
 203–245
five-phase security lifecycle, 198
scope and methodology,
 196–198
security baseline phase,
 198–203

ACME Petroleum OT Infrastructure,
 142–145

AI-Assisted Vulnerability Discovery
 Tool, 426–447

Deepfake CEO Fraud, 10–12

Fraudulent Device Exploitation at a
 Prominent State-Owned Bank, 305

Fraudulent Devices on the Wire,
 64–67

How Fraudulent Devices Penetrated
 a State-Owned Financial Giant,
 304–305

Leveraging Foundation-Sec-8B to
 Investigate ACME Bank's Fraud
 Incident, 459–462

cash-out specialists, cybercrime
 group organizations, 58

Catalyst 9000 Flow Exporter,
 configuring, 756

Catalyst 9000 Flow Monitor and
 Interface, configuring, 758

Catalyst 9000 Flow Record,
 configuring, 757

cellular bridge bypass, 292

Chainanalysis, 69

chain-hopping, 95

choke router filters, 729

Chupacabra attack, 303–304

CipherTrace, 69

CIS Critical Security Controls
 (CIS v8), 118

CISA (Cybersecurity and
 Infrastructure Security Agency), 14
 maturity levels, 178–179
 Zero Trust Maturity Model, 118

Cisco Customer Experience (CX), 121

Cisco ISE (Identity Services Engine)
 Active Directory integration, 554–562
 deployment

Dot1x supplicant selection,
 491–496

licensing model, 496–506

*PSN node distribution and
 redundancy, 488–491*

solution sizing calculation,
 471–488

use cases, 506–542

as identity control plane, 470–471

- Load Balancer integration, 562–569
- NAC (network access control), 470–471
- network segmentation, 545–554
- restoring trust at access layer, restoring, 467–469
- Cisco Lifecycle Services (LCS), 121**
- Cisco SAFE**
 - mapping business flows to, 167–168, 183–185
 - mapping capabilities to Zero Trust core components, 185–188
 - phases, 379–390
 - PINs, 390–398
 - PINs versus technical domains, 158
 - translation, 378
- Cisco security portfolio, 119–120**
- Cisco Success Tracks, 122**
- Cisco support services, 122**
- Cisco Talos Incident Response (CTIR), 122**
- Cisco Talos Intelligence reports, 2, 70**
- client headers, authentication bypass, 430–431
- cloning, IP and MAC addresses, 346–348
- cloud networking, 116
- cloud protection, 119
- Colonial Pipeline ransomware attack, 14–16
- compromised insiders, 45
- concurrent active sessions, maximum, 474–475
- conditional execution, malware, 81
- confidentiality gaps, 275
- configuration, fraudulent device attacks, 306–307
 - 4G/5G LTE interface, 320–328
 - attack bridges, 319–320
 - L2TP remote access VPNs, 328–334
 - MAC address on ether1, 312
 - management bridges, 316–319
 - NAT outbound traffic, 313–315
 - objectives, 307–308
 - physical hairpin creation, 314–316
 - prerequisites, 307–308
 - reset, 309–310
 - RFC 1918 network static route, 312–314
 - securing device, 310–311
 - temporary IP address ether1, 312–313
 - topology requirements, 308–309
- control areas**
 - interview process, 161–162
 - reviews, applying to Zero Trust maturity, 215–236
- control layer, Zero Trust, 716–727**
- core technologies map, 184, 193**
- Corporate Computers domain, Zero Trust Architecture (ZTA), 207–208, 217–218, 240, 246**
- corporate endpoints, securing, 115
- corporate IP phones, use cases, 517–518
- corporate mobile devices, use cases, 525–527
- corporate printers, use cases, 514–517
- corporate telepresence, use cases, 519–520
- corporate workstations, use cases, 511–514, 522–525, 531–534
- counterattacks, 371–373**
 - AI-assisted vulnerability discovery, 398, 426–447
 - machine learning leveraging, 447–448*
 - behavioral profiling analysis, 449–456
 - Cisco SAFE translation, 378

- Foundation-Sec-8B leveraging, 459–462
- intrusion path mapping, 448–449
- PINs, 390–398
- Project Glasswing, 398–410
- security-specialized LLMs, 457–459
- SOC operations, 457–459
- Zero Trust
 - assumptions*, 376–377
 - NIST 800–207 tenets*, 374–376
- Coyote banking Trojan, 61
- CrashOverride malware, 16
- credential stuffing, 7
- credential theft, 49
- cryptocurrency tracing, 69
- cryptographic protection at first hop, MACsec, 631–633
- CSF (Cybersecurity Framework), 117
- CTIR (Cisco Talos Incident Response), 122
- Customer Experience (CX), 121
- Cutting Sword of Justice, 91
- CX (Customer Experience), 121
- cyber inequality, 48
- cyber kill chain model, 97–102, 108
 - phases, 99–102
- cyber resilience, 43–44
- cyber resilience drills, 32
- cyber terrorism, 91, 109–110
- cyber threats, 4
- Cyber warfare, 92
- cyberattacks. *see* attacks
- cybercrime, 4–8. *see also* attacks; hackers
 - anti-forensics techniques, 79–82
 - digital fraud, 5–8
 - economic impact, 46–48
 - evasion tactics, 77–79
 - evidence-elimination techniques, 79–82
 - group organization, 57–60
 - human vulnerabilities, 10–12
 - law enforcement countermeasures, 57–60, 96–97
 - persistence techniques, 76–77
 - ransomware, RaaS (ransomware-as-a-service), 13–14
 - regulatory responses, 96–97
 - roles, 57–60
 - social engineering, 8
 - psychology*, 9–10
 - structure, 57–60
 - underground economy, 92–96, 109
- cybercrime group organizations, roles, 108
- cybercriminals
 - mapping behavior, 104
 - money mules, 357–358
 - motivations, 48–49
- cybersecurity, 49–51, 749
 - frameworks, 97
 - cyber kill chain model*, 97–102
 - DETT&CT*, 104–105
 - MITRE ATT&CK*, 102–104
 - RE&ACT*, 105–107
 - human vulnerabilities, 10–12
 - perspectives, 111–113
 - reconnaissance, 75–76
 - risk management, 130–131
 - ROI (return on investment), 137–142
 - strategies, 113–114
 - alignment*, 135–137
 - business outcome definition*, 114–115

executive interpretation, 145–146
executive sponsorship, 132–134
frameworks, 117–118
governance, 122–126
knowledge bases, 117–118
KPIs (key performance indicators), 122–126
living, 134–135
mapping solutions, 118–122
reactive defense, 132
regulations, 117–118
regulatory compliance, 135–137
standards, 117–118
technical domain identification, 116–117
technologies, 128–130
translating requirements into risks, 130–131
ZTA (Zero Trust Architecture), 127–128
 strengthening, 74
Cybersecurity and Infrastructure Security Agency (CISA), 14
 cyberthreat intelligence, 68

D

dark web, hacking tools, 85
 dark web marketplace operators, cybercrime group organizations, 59
 dark web surveillance, 68–69
 Darkrode forum, 59–60
 data, protecting, 115
 Data Center Firewall domain, Zero Trust Architecture (ZTA), 210–211, 224–226, 242, 247

data centers, 116
 intersegment enforcement, 576–577
 intrasegment enforcement, 578
 data hoarding, 46
 Deepfake CEO Fraud case study, 10–12
 deepfake scams, 6
 defense
 counterattacks, 371–373
 Zero Trust, 373–377
 machine speed threats, 411–425
 denylist devices, use cases, 509–510
 design phase, PDI (Plan, Design, and Implement) methodology, 587–602
 detection, rapid, 306
 DETT&CT framework, 104–105
 developers, cybercrime group organizations, 58
 Device Admin Control-AAA domain, Zero Trust Architecture (ZTA), 213–214, 232–234, 244, 248
 device flooding, 280
 devices
 fraudulent attacks, 287–295
 MikroTik RouterBOARD, 289–290
 use cases
 access points, 534–538
 access points onboarding, 539–542
 allowlist, 508–509
 BYOD mobile, 527–530
 corporate IP phones, 517–518
 corporate mobile devices, 525–527
 corporate printers, 514–517
 corporate telepresence, 519–520

corporate workstations,
511–514, 522–525, 531–534
denylist, 509–510
guest, 530–531
IoT security alarms, 521–522
IoT security camera, 520–521
quarantine, 510–511

DevSecOps lifecycle, 403–404
Digital Crimes Unit (Microsoft), 70
digital fraud, techniques, 5–8
discovery process, interview
process, 204
disk-wiping techniques, 79–82
domains, security evaluation details,
215–236
Dot1x, supplicant selection, 491–496
double extortion models, 13
drive-by downloads, 101
Duckwall, Alva, 278, 288
transparent bridge bypass, 276–277
dynamic policy, Zero Trust, 375

E

EAP-GTC (Generic Token Card)
attack, 280
EAP-MD5, 284–285
EAP-TLS, 284–285
east-west defense. *see*
microsegmentation
economic impact, cybercrime, 46–48
EDR (endpoint detection and
response), 77
EHRs (electronic health records),
disruption, 19
Eisenhower, Dwight D., 371
Email Security domain, Zero Trust
Architecture (ZTA), 207, 215–216,
240, 246
Emotet botnet, 70
endpoint detection and response
(EDR), 77
endpoints, network address
identification, 344–345
enforcement validation, TrustSec
policies, 622–623
ENISA (European Union Agency for
Cybersecurity), 14
Enterprise campus, 116
Enterprise LANs, 116
enterprise risk management (ERM),
131–132
Enterprise VPNs, 116
Enterprise WANs, 116
EOL (end-of-life), software, 419
Equifax breach (2017), 101
ERM (enterprise risk management),
131–132
espionage, 102
ethical hackers, 55–57
ethical issues, hacking tools, 86–89
European Union Agency for
Cybersecurity (ENISA), 14
evasion tactics, 77–79, 109
evidence analysis, AI (artificial
intelligence), 83–84
evidence-elimination techniques,
79–82, 109
AI (artificial intelligence), 82
countering, 82–83
evil twin access point attack,
279–280
execute phase, strategic zero trust
readiness assessment, 253–256
execution phase, cyberattacks, 57
exploit development cycle, 412–413
exploit writers, cybercrime group
organizations, 58

exposure windows, 413–414

extortion models, 13

F

facilitators, cybercrime group
organizations, 59

FENRIR (packet injection), 281–282

file-wiping techniques. *see also*
hackers

financial institutions

attacks, 60–61

Brazilian hackers, 60–61

*on-path attacks with fraudulent
devices*, 61–67

financial theft, 7

financiers, cybercrime group
organizations, 58

firewalls

hybrid mesh firewall architecture,
727–745

insider threats, 353–357

firmware rootkits, 77

fraud detection system bypassing, 7

fraudulent device attacks, 287–295

case studies, 304–306

Chupacabra, 303–304

configuring, 306–307

4G/5G LTE interface, 320–328

L2TP remote access VPNs,
328–334

*MAC address on ether1
customization*, 312

management bridges, 316–319

*NAT (Network Address
Translation) outbound
traffic*, 313–315

objectives, 307–308

physical hairpin creation,
314–316

prerequisites, 307–308

reset, 309–310

*RFC 1918 network static route
addition*, 312–314

securing device, 310–311

*temporary IP address to ether1
assignment*, 312–313

topology requirements,
308–309

exposure, 301–302

Fraudulent Devices on the Wire case
study, 64–67

Frost, Robert, 677

G

gaps, MACsec, 275

GDPR (General Data Protection
Regulation), 118

General Data Protection Regulation
(GDPR), 118

Generation 7 on-path attacks,
361–366

generative AI-driven attacks, 48

geopolitical conflicts, cyber
threats, 48

governmental entities

ransomware attacks, 23–27

*Argentina National Directorate
of Migration*, 25–26

Atlanta city government, 23–24

Baltimore city government, 25

*Washington, D.C. police
department attack*, 26–27

governance, 147

cybersecurity strategies, 122–126

executive sponsorship, 132–134

Grandoreiro banking Trojan, 61
group organization, cybercrime, 57–60
Grove, Andy, 573
guest devices, use cases, 530–531
guests, managing, 115

H

hackers. *see also* cybercrime
Brazilian, 60–61
ethical, 55–57
evidence-elimination techniques, 109
hacktivism, 89–91
modus operandi, 55–57
tools, 84, 108–109
black market, 85
CaaS (Cybercrime-as-a-Service), 85–86
dark web, 85
legal and ethical issues, 86–89
open-source, 84–85
hacking manipulation, 8
hacktivism, 89–91, 109–110
handoffs, insider threats, 267–268
hardware inventory processes, 414, 416
healthcare sector
ransomware attacks, 18–23
disabling of medical devices and hospital networks, 19
disruption of electronic health records (EHRs), 19
exposure of sensitive patient data, 19
Springhill Medical Center attack, 21–23
Universal Health Services (UHS) attack, 20–21
WannaCry, 19–20

heat map calculation, risks, 181–183
honeypots, 68
hospital networks, disabling, 19
hosting operators, cybercrime group organizations, 58
hub bypass, 273–274
Hulton, David, 278
human vulnerabilities, cybercrime, 10–12
hybrid mesh firewall architecture, macrosegmentation, 727–745

I

IABs (initial access brokers), cybercrime group organizations, 58
ICS/IoT environments, protecting, 115
identity control, Zero Trust, 414, 420
identity theft, 7
IDMZ (industrial demilitarized zone), 657–659
IDOR (Insecure Direct Object Reference), 431–432
immunity, MACsec, breaking, 282–284
implementation phase, PDI (Plan, Design, and Implement) methodology, 602–622
improper transaction approval workflow, 435–436
incident response, 122
insider data hoarding, 46
industrial demilitarized zone (IDMZ), 657–659
industrial disruption, 13
industrial protection, 120
industrial safety system attacks, 17–18
Industry 4.0, microsegmentation, OT (operational technology), 668–671

- infrastructure providers, cybercrime group organizations, 58
 - initial access brokers (IABs), cybercrime group organizations, 58
 - initial access phase, cyberattacks, 56
 - inline tagging, TrustSec, MTU, 623–629
 - insider collusion, 46
 - insider threats, 49
 - 802.1X attacks, 271
 - bridge*, 274–277
 - bypasses*, 271–274
 - MACsec*, 274–277, 280–285
 - packet injection*, 280–285
 - protocol exposure*, 277–280
 - undetected mobile access*, 285–287
 - dilemma, 352
 - firewall limitations, 353–357
 - fraudulent device attacks, 287–295
 - handoffs, 267–268
 - installations, 269–270
 - money mules, 357–358
 - motivations, 360–361
 - ransomware, 44–46
 - recruitment, 263–267
 - thinking like, 573–574
 - wired corporate LANs, weakness exploitation, 270
 - installations, insider threats, 269–270
 - integration
 - Cisco ISE
 - Active Directory*, 554–562
 - Load Balancer*, 562–569
 - integrity gaps, 275
 - interface authentication state, validation, 858
 - international cooperation
 - law enforcement, 69
 - law enforcement countermeasures, 73–74
 - Internet Edge, intersegment enforcement, 577–578
 - intersegment enforcement
 - data centers, 576–577
 - Internet Edge, 577–578
 - interview process
 - discovery process, 204
 - organization, 205
 - questionnaire, 205
 - interview process based on control areas, conducting, 161–162
 - intrasegment enforcement
 - data centers, 578
 - LANs (local area networks), 579
 - intrusion path mapping, 448–449
 - IoT bypasses, 280
 - IoT devices, authentication, 542–545
 - IoT ecosystems, ransomware attacks, 30–31
 - IoT security alarms, use cases, 521–522
 - IoT security camera, use cases, 520–521
 - IP addresses, cloning, 346–348
 - IPFIX (IP Flow Information Export), 754–762
 - ISA/IEC 62443 zones, Purdue Model architecture, 649–668
 - ISE (Identity Service Engine). *see* Cisco ISE
 - ISO/IEC 27001, 118
- ## J
-
- joint task forces, 69
 - Joyce, Rob, 73

K

kill switches, 81

KPIs (key performance indicators),
122–126, 133, 147
business-focused, 123–124

L

L2TP remote access VPNs,
configuring, 328–334

Langner, Ralph, 650

LANs (local area networks)
802.1X attacks, bypasses, 271–274
intrasegment enforcement, 579

LATAM banks, on-path attacks with
fraudulent devices, 61–67

lateral movement, proactive threat
defense, 771–772

lateral movement phase,
cyberattacks, 57

law enforcement countermeasures,
96–97

cybercrime, 57–60

cybercrime network dismantling,
67–74

FinCEN (Financial Crimes
Enforcement Network), 96

global collaboration, 73–74

layered defense, 306

Lazarus Group, 92, 101–102

LCS (Lifecycle Services), 121

leadership, cybercrime group
organizations, 58

least-privilege access, 375

legal issues, hacking tools, 86–89

Legrand, Valerian, 288

FENRIR (packet injection), 281–282

licensing calculation process, Cisco
ISE, 504–506

licensing model, Cisco ISE
deployment, 496–506

Lincoln, Abraham, 749

LLMs (large language models),
security-specialized, 457–459

LM-CIRT (Lockheed Martin's
Computer Incident Response
Team), 98–99

Load Balancer, Cisco ISE integration,
562–569

Lockheed Martin's Computer Incident
Response Team (LM-CIRT), 98–99

long-term financial fraud, 7

LotL (living-off-the-land) techniques,
76–77

LTR-SMB (Little Red SMB), 772–844

L.U.M.A. (Layer 2 Undetected Mobile
Access), 294–295, 860–889

M

MAC addresses, cloning, 346–348

machine learning, leveraging,
447–448

machine learning model lockout
(MLML) ransomware, 31

machine speed, 399–410

threats, defending against, 411–425

macrosegmentation, 677–699

architecture, 700–715

hybrid mesh firewall architecture,
727–745

versus microsegmentation, 575–579

rule order, 699–700

Zero Trust control layer, 716–727

MACsec, 67

breaking immunity, 282–284

- gaps, 275
- implementation validation, 859–860
- L.U.M.A. (Layer 2 Undetected Mobile Access), 860–889
- microsegmentation, 629–630
 - cryptographic protection at first hop*, 631–633
 - pre-deployment*, 633–634
- MKA (MACsec Key Agreement), 859
- over EoIP/VPLs, 293–294
- session state validation, 859
- MacSec**, 574
- MACsec attacks**, 274–277, 280–285
- malicious insiders**, 45
- malware**
 - self-destructing, 81
 - SUNBURST, 78–79
 - Ukrainian power grid attacks, 16–17
- malware engineers, cybercrime group organizations**, 58
- management bridges, configuring**, 316–319
- manufacturing execution systems (MESs)**, 660
- mapping**
 - business flows, Cisco SAFE, 183–185
 - business flows Cisco SAFE, 167–168
 - intrusion path, 448–449
 - MITRE ATT&CK framework, 167
 - SAFE capabilities to Zero Trust core components, 183–185
 - technical domains
 - networks to*, 157–158, 171–173
 - risks to MITRE ATT&CK TTPs*, 166–167
 - security frameworks and methodologies*, 159–161
 - Zero Trust frameworks*, 173–177
 - mapping cybercriminal behavior, 104
 - Marlinspike, Moxie, 278
- maturity, Zero Trust Architecture (ZTA), applying control area reviews**, 215–236
- maturity levels**, 177–183
 - CISA 2.0, 178–179
 - technical domains, 162–164
 - Zero Trust Architecture (ZTA), evaluating current, 236–239
- Mean Time to Detect (MTTD)**, 133
- Mean Time to Respond (MTTR)**, 133
- measure phase, strategic zero trust readiness assessment**, 257–259
- medical devices, disabling**, 19
- memory manipulation**, 80
- MESs (manufacturing execution systems)**, 660
- MFA (multifactor authentication)**, 77
- microsegmentation**, 582
 - versus macrosegmentation, 575–579
- MACsec**, 629–630
 - cryptographic protection at first hop*, 631–633
 - pre-deployment*, 633–634
- OT (operational technology), Industry 4.0**, 668–671
- PDI (Plan, Design, and Implement) methodology**, 582–583
 - Zero Trust*, 582–629
- Microsoft Digital Crimes Unit**, 70
- migration services**, 122
- MikroTik RouterBOARD devices**, 289–290, 302
- Mispadu Trojan**, 61
- MITRE ATT&CK framework**, 102–104, 118
 - risk severity evaluations, 180–181

MKA (MACsec Key Agreement), 859
 MLML (machine learning model
 lockout) ransomware, 31
 MnTs, sizing, 476–477
 money launderers, 359
 cybercrime group organizations, 58
 money mules, 357–358
 monitoring, constant, 306
 MS-CHAPv2 downgrade attack,
 278–280
 MTDD (Mean Time to Detect), 133
 MTTR (Mean Time to Respond), 133
 Mueller, Robert, 1
 mule managers, 358, 359
 mules, 357–358
 multifactor authentication (MFA), 77
 Musk, Elon, 46

N

NAC (network access control), 67,
 470–471
 National Cyber Security Centre, 14
 nation-state cyber operations, 91–92,
 109–110
 nation-state exploitation, 14
 nation-state-backed ransomware
 attacks, 27–28, 29–30
 NDR (network detection and
 response), 67, 754, 762–765
 negligent insiders, 45
 NetFlow, 754–762
 network access control (NAC), 67
 network detection and response
 (NDR), 67
 network security assessments,
 151–155
 strategic zero trust readiness
 assessment, 155–157

case study, 193–196
environment analyze phase,
203–245
execute phase, 253–256
five-phase security lifecycle, 198
interview process based on
control areas, 161–162
mapping business flows to
Cisco SAFE, 167–168,
183–185
mapping network to technical
domains, 171–173
mapping SAFE capabilities to
core components, 185–188
mapping technical domain
risks to MITRE ATT&CK
TTPs, 166–167
mapping technical domains
to zero trust frameworks,
173–177
mapping to technical domains,
155–157
mapping to technical domains
to security frameworks and
methodologies, 159–161
maturity level and risk severity
evaluation, 177–183
measure phase, 257–259
process details, 169–171
recommend phase, 249–253
roadmap, 168–169
scope and methodology,
196–198
security baseline phase,
198–203
technical domain maturity
level, 162–164
technical domain risk and
severity evaluation, 164–166
 ZTA (Zero Trust Architecture), 151

network segmentation, Cisco ISE, 545–554

network visibility and segmentation, 119

NIST 800–207 tenets, Zero Trust, 374–376

NIST Cybersecurity Framework (CSF), 117

NIST SP 800–30, risk severity evaluations, 180–181

NIST SP 800–207 zones, Purdue Model architecture, 649–668

node distribution and redundancy, PSNs, 488–491

north-south defense. *see* macrosegmentation

NotPetya attack, 101

O

observability, 120

Observability domain, Zero Trust Architecture (ZTA), 213, 231–232, 243–244, 248

on-path attacks, Generation 7, 361–366

on-path attacks with fraudulent devices, 61–67

Open Web Application Security Project (OWASP), 118

open-source hacking tools, 84–85

open-source intelligence (OSINT) tools, 75–76

operational resilience, strengthening, 115

operators, cybercrime group organizations, 58

OSINT (open-source intelligence) tools, 75–76

OT (operational technology)

microsegmentation, Industry 4.0, 668–671

segmentation, Zero Trust, 647–671

OT networking, 117

overconfidence bias, 10

OWASP (Open Web Application Security Project), 118

P

packet injection, 280–285

PANs, sizing, 476

patch management, 414

path management strategy, 417–418

patient data, exposure, 19

Payment Card Industry Data Security Standard (PCI DSS), 118

PCI DSS (Payment Card Industry Data Security Standard), 118

PDI (Plan, Design, and Implement) methodology, 582–583

Zero Trust, 582–584

design phase, 587–602

implementation phase, 602–622

planning phase, 584–587

PEAP downgrade attack, 278–280

penetration testers, cybercrime group organizations, 58

PERA (Purdue Enterprise Reference Architecture), 650

persistence techniques, 76–77, 109

PhaaS (phishing-as-a-service), 86

phases

Cisco SAFE, 379–390

cyber kill chain model, 99–102

cyberattacks, 56–57

outcome-driven security assessment, 170–171

- zero trust readiness assessment
 - environment analyze phase*, 203–245
 - five-phase security lifecycle*, 198
 - security baseline phase*, 198–203
- phishing, 5, 49
 - AI, 42
 - PhaaS (phishing-as-a-service), 86
- phishing emails, 100
- phishing experts, cybercrime group organizations, 58
- PINs (SAFE), versus technical domains, 158
- planning phase, PDI (Plan, Design, and Implement) methodology, 584–587
- Plato, 193
- policies
 - TrustSec
 - distribution*, 581
 - enforcement validation*, 622–623
 - matrix*, 581
- port forwarding, enabling in hotspot mode, 324–326
- post-quantum threats, preparing, 115
- pre-deployment, MACsec, 633–634
- privilege escalation, cyberattacks, 57
- proactive threat defense, 749–753
 - advanced lateral movement, 771–772
 - interface authentication state, validation, 858
 - IPFIX (IP Flow Information Export), 754–762
 - LTR-SMB (Little Red SMB), 772–844
 - MACsec
 - implementation validation*, 859–860
 - L.U.M.A. (Layer 2 Undetected Mobile Access)*, 860–889
 - MKA (MACsec Key Agreement)*, 859
 - session state validation*, 859
 - NDR (network detection and response), 754, 762–765
 - NetFlow, 754–762
 - remote access techniques, 771–772
 - SIEM (security information and event management), 754, 767–770
 - XDR (extended detection and response), 754, 765–767
- process injection, 80
- Project Glasswing, 398–410
- project managers, cybercrime group organizations, 58
- protocol exposure, 277–280
- PSNs
 - commercial strategy, 488
 - node distribution and redundancy, 488–491
 - sizing, 481–482
 - per country*, 484–488
- publicly disclosed CVEs, 409–410
- public-private partnerships, law enforcement, 70
- Purdue Model architecture
 - ISA/IEC 62443 zones, 649–668
 - NIST SP 800–207 zones, 649–668
 - Zero Trust, OT (operational technology) segmentation, 647–671
- pxGrids, sizing, 477–481
- Python Flask application, creating, 428–429

Q

quantum computing, 32
 quarantine devices, use cases,
 510–511
 questionnaire, interview process, 205

R

RaaS (ransomware-as-a-service), 55
 RaaS (ransomware-as-a-service),
 13–14, 85–86
 RADIUS, TPS (transactions per
 second), 473
 ransomware, 49–51
 AI-driven, 27–29, 32–35
 defense strategies, 35–38
 attack vectors, 48–49
 Colonial Pipeline ransomware attack,
 14–16
 defense strategies, 31–32
 economic impact, 46–48
 governmental entities, 23–27
 *Argentina National Directorate
 of Migration*, 25–26
 Atlanta city government, 23–24
 Baltimore city government, 25
 *Washington, D.C. police
 department attack*, 26–27
 healthcare sector, 18–23
 *disabling of medical devices
 and hospital networks*, 19
 *disruption of electronic health
 records (EHRs)*, 19
 *exposure of sensitive patient
 data*, 19
 *Springhill Medical Center
 attack*, 21–23
 *Universal Health Services
 (UHS) attack*, 20–21
 WannaCry, 19–20
 insider threats, 44–46
 IoT ecosystems, 30–31
 MLML (machine learning model
 lockout), 31
 motivations, 48–49
 nation-state-backed attacks, 27–28,
 29–30
 RaaS (ransomware-as-a-service),
 13–14, 55, 85–86
 smart cities, 30–31
 supply chain exploitation, 43–44
 rapid detection, 306
 RE&ACT framework, 105–107
 Reagan, Ronald, 467
 reciprocity principle, 10
 recommend phase, strategic zero trust
 readiness assessment, 249–253
 reconnaissance, cybersecurity, 75–76
 reconnaissance phase, cyberattacks, 56
 recruitment, insider threats,
 263–267
 red team operators, cybercrime group
 organizations, 58
 reducing risks, 115
 regulatory compliance, cybersecurity
 strategies, 135–137
 regulatory responses, 96–97
 remote access techniques, 771–772
 remote kill switches, 81
 remote tunnel access, gaining,
 341–343
 replay protection gaps, 275
 Republic, 193
 requirements, security, translating
 into risk, 130–131

Resilience and High Availability domain, Zero Trust Architecture (ZTA), 214–215, 234–236, 244–245, 248

REvil ransomware group, 43

Riley, Steve, 288

hub bypass, 273–274

Rio2016 Olympic Games, hacker campaign, 68–69

risk heat matrix, risk severity evaluations, 180–181

risk severity evaluations, 177–183

risks

heat map calculation, 181–183

reducing, 115

severities, evaluation, 180–181

technical domains

evaluation, 164–166

mapping to MITRE ATT&CK TTPs, 166–167

Zero Trust Architecture (ZTA), severity evaluations, 245–249

Robbins, Chuck, 38, 74

RobinHood ransomware attack, 25

ROI (return on investment), cybersecurity, 137–142

roles, cybercrime, 57–60

ROSI (return on security investment), 130, 147

RouterOS

configuring

admin user, 311

APN, 327

attack BVI, 319

default route, 328

initial, 309

IP address, 312

IP pool, 331

L2TP server, 334

loopback, 329

LTE interface, 327

MAC address, 312

management BVI, 316

NAT (Network Address Translation), 314

profile, 332

route, 313

user credentials, 333

LTE interface status, 326, 327

Ryan, Gabriel, 281, 289

breaking MACsec immunity, 282–284

S

sabotage, 102

SAFE. *see* Cisco SAFE

SASE/SSE access, 116, 120

scam artists, cybercrime group organizations, 58

Schneier, Bruce, 301

secure analytics, 119

security. *see* cybersecurity;
network security assessments,
awareness, 306

security operations, automating, 115

security operations centers (SOCs),
38, 115

security segmentation, enabling, 115

security-specialized LLMs, 457–459

segmentation

enabling, 115

macro, 677–699

architecture, 700–715

macrosegmentation, 727–745

rule order, 699–700

- Zero Trust control layer*, 716–727
- micro, 575–579, 582
 - MACsec*, 629–630, 631–634
 - PDI (Plan, Design, and Implement) methodology*, 582–583
 - PDI (Plan, Design, and Implement) methodology with ZeroTrust*, 582–629
- TrustSec, 580–581
- Zero Trust, 414, 420
 - OT (operational technology)*, 647–671
- self-destructing malware, 81
- services, mapping security to, 120–122
- services as resources, 374
- session hijacking, 7
- severities
 - risks
 - technical domains*, 164–166
 - Zero Trust Architecture (ZTA)*, 245–249
- SGT (security group tag), TrustSec, 580–581
- SIEM (security information and event management), 754, 767–770
- Sinclair, Robbie, 151
- sizing calculation, Cisco ISE (Identity Services Engine), 471–488
- smart cities, ransomware attacks, 30–31
- Smart Licensing, Cisco ISE, 504
- SMEs (subject matter experts), 162
- social engineering, 8, 49
 - psychology, 9–10
- social engineers, cybercrime group organizations, 58
- SOCs (security operations centers), 38, 115
 - operations, 457–459
- software EOL (end-of-life), 419
- software inventory processes, 414, 417
- software lifecycle management, 414
- SolarWinds attack, 43
- solution sizing calculation, Cisco ISE (Identity Services Engine), 471–488
- source address manipulation, 80–81
- SP networking, 117
- spear phishing, 5
- Springhill Medical Center
 - ransomware attack, 21–23
- SQL injection
 - administrative search functions, 432–433
 - audit logging, 436–437
 - authentication, 429–430
- static trust, 306
- stolen data integration, 7
- strategic zero trust readiness
 - assessment, 155–157
 - case study, 193–196
 - environment analyze phase, 203–245
 - execute phase, 253–256
 - five-phase security lifecycle, 198
 - interview process based on control areas, 161–162
 - mapping business flows to Cisco SAFE, 167–168, 183–185
 - mapping network to technical domains, 171–173
 - mapping SAFE capabilities to core components, 185–188
 - mapping technical domain risks to MITRE ATT&CK TTPs, 166–167

- mapping technical domains to zero trust frameworks, 173–177
- mapping to technical domains, 157–158
- mapping to technical domains to security frameworks and methodologies, 159–161
- maturity level and risk severity evaluation, 177–183
- measure phase, 257–259
- process details, 169–171
- recommend phase, 249–253
- roadmap, 168–169
- scope and methodology, 196–198
- security baseline phase, 198–203
- technical domain maturity level, 162–164
- technical domain risk and severity evaluation, 164–166
- strategies**
 - cybersecurity
 - alignment*, 135–137
 - executive interpretation*, 145–146
 - executive sponsorship*, 132–134
 - living*, 134–135
 - regulatory compliance*, 135–137
- Stuxnet attack, 91–92
- Stuxnet worm, 100–101
- subject matter experts (SMEs), 162
- Success Tracks, 122
- Sun Tzu, 55, 111
- SUNBURST malware, 78–79
- supply chain exploitation, 49
 - ransomware, 43–44
- surfaces, networks, protecting, 157–158

- switches, attacks, 348–352
- synthetic identity fraud, 6–7

T

targets

- endpoint network addresses, 344–345
- identification, 341–348
- IP and MAC addresses, cloning, 346–348

technical domains

- versus Cisco SAFE PINs, 158
- election, 159
- identifying, 116–117
- mapping networks to, 157–158, 171–173
- mapping networks to security frameworks and methodologies, 159–161
- mapping risks to MITRE ATT&CK TTPs, 166–167
- mapping to zero trust frameworks, 173–177
- maturity level, 162–164
- risks and severities evaluation, 164–166

Zero Trust Architecture (ZTA)

- Corporate Computers*, 207–208, 217–218, 240, 246
- Data Center Firewall*, 210–211, 224–226, 242, 247
- Device Admin Control-AAA*, 213–214, 232–234, 244, 248
- Email Security*, 207, 215–216, 240, 246
- Observability*, 213, 231–232, 243–244, 248
- Resilience and High Availability*, 214–215, 234–236, 244–245, 248

Threat Detection and Response, 212–213, 229–231, 243, 247
Virtual Servers (VMs), 211–212, 226–229, 242–243, 247
VPN Remote Access, 209–210, 221–224, 241–242, 247
Wired and Wireless LAN, 208–209, 218–221, 241, 246
 technical environments, 118–120, 147
 technical KPIs, 124–126
 Tesla, insider attacks, 46
 third-party insiders, 45
 third-party vendor exploitation, 101
 Threat Detection and Response
 domain, Zero Trust Architecture (ZTA), 212–213, 229–231, 243, 247
 threat response, accelerating, 115
 threat visibility, improving, 115
 threats. *see also* attacks
 machine speed, defending against, 411–425
 time-based expiration, malware, 81
 Timestomp, 80
 tools
 hackers, 84, 108–109
 black market, 85
 CaaS (Cybercrime-as-a-Service), 85–86
 dark web, 85
 legal and ethical issues, 86–89
 open-source, 84–85
 topologies, fraudulent device attacks, requirements, 308–309
 TPS (transactions per second), RADIUS, 473
 transparent bridge bypass, 276–277
 triple extortion models, 13
 Triton/Trisis cyberattack, 17–18

TrustSec, 574
 architecture, 581
 control plane integration, 581
 enforcement mechanisms, 581
 inline tagging, MTU, 623–629
 matrix, policy definition, 581
 policies, enforcement validation, 622–623
 policy distribution, 581
 segmentation, 580–581
 SGT (security group tag), 580–581
 standard-based authentication, 580

U

Ukrainian power grid attacks, 16–17
 UNC5176 hacking groups, 61
 undercover operations, 68–69
 underground economy, cybercrime, 92–96, 109
 undetected mobile access attacks, 285–287
 Universal Health Services (UHS)
 attack, 20–21
 URSA Trojan, 61
 user protection, 119
 user safety, protecting, 115

V

validation
 interface authentication state, 858
 MACsec session state, 859
 victims. *see* targets
 video deepfakes, 6
 Virtual Servers (VMs) domain, Zero Trust Architecture (ZTA), 211–212, 226–229, 242–243, 247

voice deepfakes, 6

VPN Remote Access domain,
Zero Trust Architecture
(ZTA), 209–210, 221–224,
241–242, 247

VPNs (virtual private networks)

configuring

client connections, 342–343

PPTP client, 341–343

L2TP, configuring, 328–334

W

WannaCry ransomware attack,
19–20

Washington, D.C. police department
attack, 26–27

Williams, Darren, 60

Wired and Wireless LAN domain,
Zero Trust Architecture (ZTA),
208–209, 218–221, 241, 246

wired corporate LANs, weakness
exploitation, insider threats, 270

wireless bridge bypass, 290–292

WLANs (Wireless Local Area
Networks), 802.1X attacks,
bypasses, 271–274

X

XDR (extended detection and
response), 754, 765–767

Z

Zero Trust

assumptions, 376–377

behavioral analytics, 414, 420

continuous monitoring, 375

counterattacks, NIST 800–207
tenets, 374–376

dynamic authentication and
authorization, 376

dynamic policy, 375

identity control, 414, 420

intelligence-driven feedback, 376

macrosegmentation, control layer,
716–727

PDI (Plan, Design, and Implement)
methodology, 582–584

design phase, 587–602

implementation phase, 602–622

planning phase, 584–587

segmentation, 414, 420

OT (operational technology),
647–671

Zero Trust Architecture (ZTA), 118,
127–128

key findings and gaps, evaluating,
239–245

maturity, applying control area
reviews, 215–236

maturity levels, evaluating current,
236–239

risk severity evaluations, 245–249

technical domains

Corporate Computers, 207–208,
217–218, 240, 246

Data Center Firewall, 210–211,
224–226, 242, 247

Device Admin Control-AAA,
213–214, 232–234, 244, 248

Email Security, 207, 215–216,
240, 246

Observability, 213, 231–232,
243–244, 248

*Resilience and High
Availability*, 214–215,
234–236, 244–245, 248

- Threat Detection and Response*, 212–213, 229–231, 243, 247
- Virtual Servers (VMs)*, 211–212, 226–229, 242–243, 247
- VPN Remote Access*, 209–210, 221–224, 241–242, 247
- Wired and Wireless LAN*, 208–209, 218–221, 241, 246
- zero trust readiness assessment**, 155–157
 - case study, 193–196
 - environment analyze phase, 203–245
 - execute phase, 253–256
 - five-phase security lifecycle, 198
 - interview process based on control areas, 161–162
 - mapping business flows to Cisco SAFE, 167–168, 183–185
 - mapping network to technical domains, 171–173
 - mapping SAFE capabilities to core components, 185–188
 - mapping technical domain risks to MITRE ATT&CK TTPs, 166–167
 - mapping technical domains to zero trust frameworks, 173–177
 - mapping to technical domains, 157–158
 - mapping to technical domains to security frameworks and methodologies, 159–161
 - maturity level and risk severity evaluation, 177–183
 - measure phase, 257–259
 - process details, 169–171
 - recommend phase, 249–253
 - roadmap, 168–169
 - scope and methodology, 196–198
 - security baseline phase, 198–203
 - technical domain maturity level, 162–164
 - technical domain risk and severity evaluation, 164–166
- ZTA (Zero Trust Architecture)**. *see* **Zero Trust Architecture (ZTA)**, 118, 127–128
- ZTE LTE 4G/5G modem**, 321