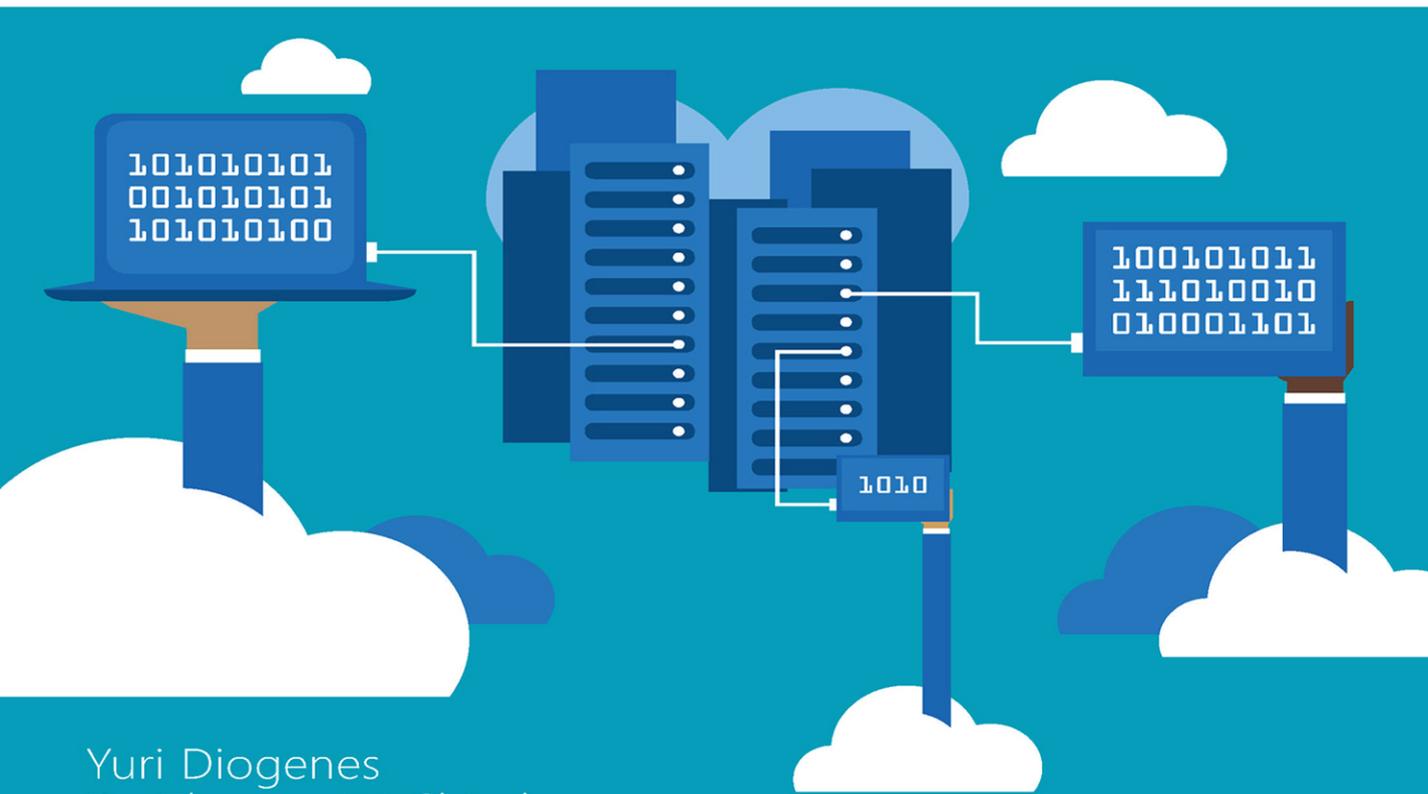


Microsoft Azure Security Center



Yuri Diogenes
Dr. Thomas W. Shinder

Foreword by Hayden Hainsworth, Principal Group Program Manager, Microsoft C+E Security Engineering

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Microsoft Azure Security Center

Yuri Diogenes
Dr. Thomas W. Shinder

Microsoft Azure Security Center

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

Copyright © 2018 by Pearson Education, Inc.

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 www.pearsoned.com/permissions/. 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.

ISBN-13: 978-1-5093-0703-6

ISBN-10: 1-5093-0703-6

Library of Congress Control Number: 2018938489

1 18

TRADEMARKS

Microsoft and the trademarks listed at <http://www.microsoft.com> on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

WARNING AND DISCLAIMER

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 provided is on an "as is" basis. The authors, the publisher, and Microsoft Corporation 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 CD or programs accompanying it.

SPECIAL SALES

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corp-sales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

CREDITS

EDITOR-IN-CHIEF

Greg Wiegand

EXECUTIVE EDITOR

Laura Norman

DEVELOPMENT EDITOR

Kate Shoup/Polymath
Publishing

MANAGING EDITOR

Sandra Schroder

SENIOR PROJECT EDITOR

Tracey Croom

COPY EDITOR

Scout Festa

INDEXER

Valerie Perry

PROOFREADER

Elizabeth Welch

TECHNICAL EDITOR

Mike Martin

EDITORIAL ASSISTANT

Cindy J. Teeters

COVER DESIGNER

Twist Creative, Seattle

COMPOSITOR

Jeff Lytle, Happenstance
Type-O-Rama

GRAPHICS

Vived Graphics

Contents

| | |
|---|-----------|
| <i>Foreword</i> | <i>ix</i> |
| <i>Introduction</i> | <i>xi</i> |
| Chapter 1 The threat landscape | 1 |
| Understanding cybercrime | 1 |
| Understanding the cyber kill chain | 2 |
| Common threats | 4 |
| Building a security posture | 5 |
| Adopting an assume-breach mentality | 6 |
| Cloud threats and security | 7 |
| Compliance | 8 |
| Risk management | 9 |
| Identity and access management | 9 |
| Operational security | 9 |
| Endpoint protection | 10 |
| Data protection | 10 |
| Azure Security | 11 |
| Host protection | 12 |
| Network protection | 12 |
| Storage protection | 14 |
| Chapter 2 Introduction to Azure Security Center | 17 |
| Understanding Security Center | 17 |
| Security Center architecture | 18 |
| Security Center dashboard | 21 |
| Considerations before adoption | 22 |
| Role-based access control | 22 |
| Security policy | 23 |
| Storage | 23 |
| Recommendations | 23 |
| Incorporating Security Center into your security operations | 24 |

| | | |
|------------------|---|-----------|
| | Onboarding resources | 25 |
| | Initial assessment | 30 |
| Chapter 3 | Policy management | 33 |
| | Legacy Azure Security Center security policy | 33 |
| | Next-generation Azure Security Center security policy | 38 |
| | The Data Collection blade | 38 |
| | The Policy Management blade | 40 |
| | The Email Notifications blade | 41 |
| | The Pricing Tier blade | 42 |
| | Azure Policy | 43 |
| | Policy definitions and assignments | 44 |
| | Initiative definitions and assignments | 44 |
| | Exploring Azure Policy | 45 |
| | Customizing your Security Center security policies | 49 |
| | Azure Security Center RBAC and permissions | 49 |
| Chapter 4 | Mitigating security issues | 51 |
| | Compute recommendations | 51 |
| | Setting up endpoint protection | 52 |
| | Remediate Security Configurations | 56 |
| | Networking recommendations | 58 |
| | NSGs on subnets not enabled | 59 |
| | Restrict access through internet-facing endpoint | 61 |
| | Storage and data | 63 |
| | Server auditing and threat detection not enabled | 64 |
| | Storage encryption not enabled | 66 |
| | Applications | 68 |
| | Web application firewall not installed | 68 |
| Chapter 5 | Using Security Center for incident response | 73 |
| | Understanding security alerts | 73 |
| | Detection scenarios | 75 |
| | Detecting spam activity | 75 |
| | Crash-dump analysis | 76 |

| | |
|--|------------|
| Accessing security alerts | 77 |
| Security incidents | 79 |
| Custom alerts | 81 |
| Investigating a security issue | 84 |
| Responding to a security alert | 89 |
| Creating a playbook | 89 |
| Building the workflow | 91 |
| Executing a playbook | 94 |
| Auditing playbook execution | 95 |
| Chapter 6 Advanced cloud defense | 99 |
| Threat prevention versus threat detection | 99 |
| Methods of threat detection | 100 |
| Atomic detection | 101 |
| Threat-intelligence feeds and integrated security solutions | 102 |
| Behavioral analysis | 104 |
| Anomaly detection | 106 |
| The cyber kill chain and fusion alerts | 108 |
| Application whitelisting: adaptive application controls | 111 |
| Just-in-time VM access | 114 |
| Chapter 7 Security incident and event management (SIEM) integration with Splunk | 121 |
| Integrating SIEM solutions | 122 |
| Splunk integration with Azure Security Center | 123 |
| Confirming accessible logs in Azure Monitor | 124 |
| Configuring the subscription for the Splunk SIEM pipe | 124 |
| Creating and configuring a resource group for the Splunk SIEM pipe | 124 |
| Setting up an Azure AD application to provide an access control identity | 125 |
| Creating an Azure key vault | 127 |
| Copying the app password into Key Vault | 130 |
| Making an event hub | 131 |
| Creating a shared access key for event hub access control | 133 |

| | | |
|-------------------|---|------------|
| | Placing the event hub shared access key in Azure Key Vault | 134 |
| | Hooking up the event hub to Azure Monitor | 136 |
| | Spinning up the virtual machine that hosts the Splunk enterprise VM | 138 |
| | Installing and configuring the Azure Monitor add-on for Splunk | 139 |
| Chapter 8 | Monitoring identity and access | 141 |
| | Monitoring identity-related activities | 141 |
| | Identity posture | 143 |
| | Failed logons | 144 |
| | Logons over time | 147 |
| | Integrating Security Center with Azure Active Directory Identity Protection | 148 |
| | Customizing your search | 149 |
| Chapter 9 | Using threat intelligence to identify security issues | 153 |
| | What is threat intelligence and why use it? | 153 |
| | Using threat intelligence reports in Security Center | 155 |
| | Using the Threat Intelligence dashboard in Security Center | 157 |
| | Hunting security issues in Security Center | 159 |
| | Virtual Analyst | 163 |
| Appendix A | Using multiple workspaces in Security Center | 164 |
| | Creating a new workspace | 164 |
| | Moving computers and VMs to a new workspace | 165 |
| Appendix B | Customizing your operating system security baseline assessment | 168 |
| | General considerations | 168 |
| | Customizing operating system configuration | 169 |
| | Downloading the JSON file | 169 |
| | Editing the JSON file | 170 |
| | Uploading the new rule | 173 |
| | <i>Index</i> | 174 |

Acknowledgments

The authors would like to thank Laura Norman and the entire Microsoft Press team for their support in this project, Hayden Hainsworth for writing the foreword of this book, and also other Microsoft colleagues that contributed by writing a sidebar for this book: Laura Hunter, Nicholas DiCola, Koby Koren, Sarah Fender, Tomer Teller, Miri Landau, Ben Kliger, Ajeet Prakash, and John Kemnetz. We would also like to thank Mike Martin (Microsoft MVP) for reviewing this book.

Yuri would also like to thank: my wife and daughters for their endless support and understanding; my great God for giving me strength and guiding my path on each step of the way; my great friend and co-author Tom Shinder for another awesome partnership; and Adwait Joshi (AJ) and the entire Azure Security Center Team, especially all the Security Center PMs at Microsoft Israel for their ongoing collaboration and contribution. Thanks to my manager, Nicholas DiCola, and my coworkers Laura Hunter, Ty Balascio, Andrew Harris, Marie Groove, Gershon Levitz, and Yoann Mallet for inspiring me to do more. Last but not least, thanks to my parents for working hard to give me an education, which is the foundation I use every day to keep moving forward in my career.

Tom would also like to thank: so many people that it's very difficult to name them all in the space allocated. Probably most important is Yuri Diogenes, who motivated me to partner up on another book with him. I don't know why he asks me, because I know I drive him crazy each time we write a book together. Nevertheless, Yuri is a blessing to me and all those around him, and he keeps me from resting on my prodigious laurels. I want to thank David Cross, who brought me into Azure Security Engineering and all the fascinating opportunities it's offered; while David is now with Google, he's still an inspiration. I also want to give major props to Avi Ben-Menahem and Ramesh Chinta, both of whom have always been supportive of my efforts, and who are models of the best that Microsoft has to offer. And of course, the entire Azure Security Engineering PM team—the dedication, diligence, intelligence, and number of hours worked per week by this team is unmatched, and the results of these attributes show in the fact that Azure is the most secure public cloud service platform in the industry. Finally, eternal thanks to my wife—my lifetime love, partner, and confidant—and to God, who has given me much more in life than I deserve.

About the authors

Yuri Diogenes, MsC

With a master of science in cybersecurity intelligence and forensics investigation (UTICA College), Yuri is senior program manager in Microsoft CxP Security Team, where he primarily helps customers onboard and incorporate Azure Security Center as part of their security operations/incident response. Yuri has been working for Microsoft since 2006 in different positions, including five years as senior support escalation engineer in CSS Forefront Edge Team, and from 2011 to 2017 in the content development team, where he also helped create the Azure Security Center content experience since its launch in 2016. Yuri has published a total of 20 books, mostly around information security and Microsoft technologies. Yuri also holds an MBA and many IT/Security industry certifications, such as CISSP, E|CND, E|CEH, E|CSA, E|CHFI, CompTIA Security+, CySA+, Cloud Essentials Certified, Mobility+, Network+, CASP, CyberSec First Responder, MCSE, and MCTS. You can follow Yuri on Twitter at @yuridiogenes or read his articles at his personal blog: <http://aka.ms/yuridio>.

Tom Shinder

Tom Shinder is a cloud security program manager in Azure Security Engineering. He is responsible for security technical content and education, customer engagements, and competitive analysis. He has presented at many of the largest security industry conferences on topics related to both on-premises and public cloud security and architecture. Tom earned a bachelor's degree in neuropsychobiology from the University of California, Berkeley, and an MD from the University of Illinois, Chicago. He was a practicing neurologist prior to changing careers in the 1990s. He has written over 30 books on OS, network, and cloud security, including *Microsoft Azure Security Infrastructure* and *Microsoft Azure Security Center* (IT Best Practices series, Microsoft Press). Tom can be found hugging his Azure console when he's not busy hiding his keys and secrets in Azure Key Vault.

Foreword

I was so pleased to hear that Yuri and Tom were teaming up to write another book on security. I found their first book about Azure core security, *Microsoft Azure Security Infrastructure*, riveting—I read it cover to cover twice, recommending it to anyone interested in learning more about security in Azure.

This book extends that work. It will teach you all you want to know about how to use Azure Security Center—the security solution to get visibility and control and prevent and detect threats in your Azure subscriptions. Security Center is a critical solution for protecting a cloud workload, and, as indicated by Gartner in their Cloud Workload Protection (CWP) Magic Quadrant, modern hybrid datacenters require a unique protection strategy. And since the classic security perimeter we relied upon is gone with the migration of datacenter workloads into public clouds, a new security paradigm is required. Moreover, with the integration with Log Analytics, and as long as the monitoring agent is installed on your machines, Azure Security Center can be used for your machines on-premises, in a private datacenter, or in another cloud as well. This will simplify your life and I trust you'll come to rely on Azure Security Center as your primary dashboard and alerting engine for years to come.

No industry is immune to cyberattacks. This book is relevant for everyone around the world. Given the cybersecurity landscape as it exists today and the criticality of the information digital age, we need to assume breach as a mindset and think about what capabilities we need to detect adversarial activity or malicious insiders inside our networks rather than over-relying on thwarting attackers at the front door. Gone are the days when it was acceptable to turn a blind eye to risk. If you don't know what you don't know, it's impossible to take action. Prevention is of the utmost importance, true. However, the ability to detect and control is paramount. Simple, intuitive, and intelligent investigation capabilities are a must to support SecOps teams flooded in a sea of alerts, as well as to support incident response teams.

This book will help you plan, onboard, and learn how to effectively use Security Center to detect and investigate threats in your Azure subscriptions (or in your datacenter workloads). You'll also learn how to integrate with other solutions, like Azure Active Directory Identity Protection Center, and export your logs to a security information and event management system should you choose to do so. I sincerely hope that you get energy from the capabilities the authors outline in this book, and that it will spur you to action to follow their best practices and recommendations while gaining confidence in the solution.

After reading this book, you will have a better understanding of what Security Center is and how to incorporate it into your security operations center. Yuri and Tom were inspired to write this book because many customers would like to have

one place to go to understand what Security Center is, what its requirements are, and how to operate it. You'll find the material to be technical. It is written with security analysts, architects, and cloud operators in mind, along with any IT professional who wants to understand more about Security Center.

If you've read Tom's work, you'll know he's a long-term experienced and seasoned security veteran and author. He's also a senior program manager in the Azure Security Engineering team. Follow him on Twitter. Read his blogs if you'd like to learn more. He has a wealth of knowledge and wisdom from his days working on-premises and his journey to the cloud.

Yuri is a well-established writer in his own right, publishing document after document in his former role as a content writer for Azure Security. He's recently joined my team as a senior program manager to support customers' and partners' success using Microsoft's Cloud and Enterprise Security products and services. He has a wealth of information and excels at simplifying the complex.

Dig in.

Hayden Hainsworth
Principal Group Program Manager
Microsoft C+E Security Engineering

Introduction

Welcome to *Azure Security Center*, a book that was developed together with the Azure Security Center product group to provide in-depth information about Azure Security Center and to demonstrate best practices based on real-life experience with the product in different environments.

The purpose of this book is to introduce the wide array of security features and capabilities available in Azure Security Center. After being introduced to all of these security options, you will dig in to see how they can be used in a number of operational security scenarios so that you can get the most out of the protect, detect, and respond skills provided only by Azure Security Center.

Who is this book for?

Azure Security Center is for anyone interested in Azure security: security administrators, support professionals, developers, and engineers.

Azure Security Center is designed to be useful for the entire spectrum of Azure users. You can have no security experience, some experience, or be a security expert and will get value from Azure Security Center. This book provides introductory, intermediate and advanced coverage on a large swath of security issues that are addressed by Azure Security Center.

The approach is a unique mix of didactic, narrative, and experiential instruction. Didactic covers the core introductions to the services. The narrative leverages what you already understand and we bridge your current understanding with new concepts introduced in the book.

Finally, the experience component is presented in two ways— we share our experiences with Azure Security Center and how to get the most out of it by showing in a stepwise, guided fashion how to configure Azure Security Center to gain all the benefits it has to offer,

In this book you will learn:

- How to secure your Azure assets no matter what your level of security experience
- How to save hours, days and weeks of time by removing the trial and error
- How to protect, detect, and respond to security threats better than ever by knowing how to get the most out of Azure Security Center

System requirements

- Anyone with access to a Microsoft Azure subscription can use the information in this book.

Errata, updates & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

<https://aka.ms/AzureSecurityCenter/errata>

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *<http://support.microsoft.com>*.

Stay in touch

Let's keep the conversation going! We're on Twitter: *<http://twitter.com/MicrosoftPress>*.

Using Security Center for incident response

In the previous chapter, you learned how to address security recommendations using Azure Security Center, which is part of the overall enhancement of your security posture. However, protection is just one of the pillars of your security posture. You also need to enhance your detection and response.

On the detection front, Security Center constantly monitors your assets. When it identifies suspicious activities, it raises an alert. Importantly, it also reduces false positives, which is very important for your security operations.

In this chapter, you will learn how to use Security Center to detect threats against your environment, and how to investigate security issues as part of your incident-response process.

Understanding security alerts

The information gathered by Security Center in conjunction with network data and feeds from connected partners is used to detect threats and suspicious activities. Security Center analyzes this information by correlating the data from these sources to identify threats. Security alerts are prioritized in Security Center along with recommendations on how to remediate the threat.

IMPORTANT Security alerts are not available in the free tier version of Security Center; the standard tier is required.

Security Center uses advanced security analytics and machine-learning technologies to evaluate events across the entire cloud fabric. The security analytics include data from multiple sources, including Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds. Security Center also applies known patterns to discover malicious behavior, which is called behavioral analysis.

Security Center uses statistical profiling to build a historical baseline, which is called anomaly detection. This triggers alerts when it detects deviations from established baselines that conform to a potential attack vector.

Detection capabilities in Azure Security Center

The Azure Security Center Threat Detection module helps identify active threats targeting your Microsoft Azure resources or on-premises computers and provides you with the insights needed to respond quickly.

The detection engine collects data from multiple data sources including but not limited to endpoint logs, network traffic, and cloud services activity, and applies atomic, behavioral, and machine learning-based logic to detect active threats.

Customers can extend the capabilities of the detection engine by authoring their own custom alert rules using a powerful search language. When a threat is detected, an alert is generated and undergoes a series of enrichment stations. These include the following:

- **Comparing against threat intelligence feeds**
- **Using an innovative confidence score and reasoning system**
- **Using a sophisticated fusion engine that correlates alerts into incidents**

To help triage the alerts, Security Center provides advanced incident-response tools that help customers investigate the threat scope and apply custom playbooks to remediate them automatically.

Tomer Teller, Principal Security Program Manager, Azure Security

Regardless of which capability Security Center uses to identify a threat, the result will be externalized in the dashboard via a security alert. A security alert contains valuable information about what triggered the alert, the resources targeted, the source of the attack, and suggestions to remediate the threat.

Security alerts are divided in four categories:

- **Virtual Machine Behavioral Analysis (VMBA)** This type of alert uses behavioral analytics to identify compromised resources based on an analysis of the virtual machine (VM) event logs, such as process creation events and login events.
- **Network analysis** This type of alert collects security information from your Azure Internet Protocol Flow Information Export (IPFIX) traffic and analyzes it to identify threats. An example of an alert that belongs to this category is the Suspicious Incoming RDP Network Activity from Multiple Sources alert.
- **Resource analysis** This analyzes your Platform as a Service (PaaS) services, such as Azure SQL, and triggers alerts based on this analysis. An example of an alert that belongs to this category is the *Potential SQL Injection* alert.
- **Contextual information** This provides extra context to reach a verdict about the nature of the threat and how to mitigate it.

TIP Because the list of alerts is constantly evolving, we recommend that you visit <https://aka.ms/ASCAAlerts> to obtain the latest list of security alerts.

Detection scenarios

There are many scenarios in which Security Center will rapidly warn you about a suspicious activity. The following sections cover a couple of important scenarios to give you an idea of how powerful Security Center detections are and the advantage of using multiple data sources to enhance the confidence level of an alert.

Detecting spam activity

In this detection scenario, the attacker compromises an Azure VM and uses it to send spam emails. Using machine learning, Security Center can detect a spike in SMTP traffic. It then queries other data sources to make sure this spike is due to malicious behavior. Finally, it correlates this traffic with the Office 365 spam database to determine whether it is legitimate traffic. If the result of this correlation is that the traffic is suspicious, Security Center triggers the alert shown in Figure 5-1. In this scenario, Security Center uses built-in analytics, machine learning, and threat intelligence from Office 365. Performing these three steps provides not only more precise detection but also a higher level of confidence in the alert.

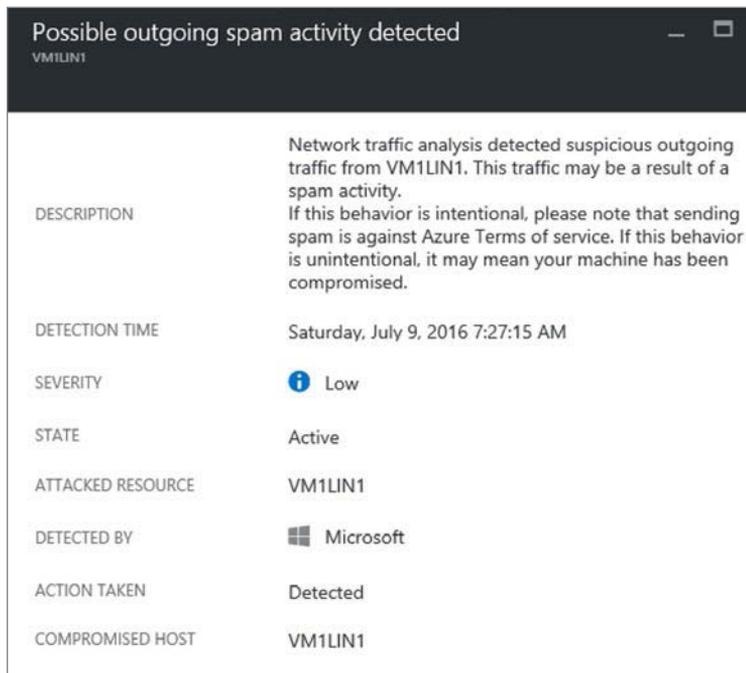


FIGURE 5-1 Spam alert in Security Center.

Crash-dump analysis

In this scenario, the attacker compromises an Azure VM and installs malware that goes undetected by the antimalware installed on the VM. This malware causes a crash in a legitimate program. When a crash occurs in a Windows system, Windows Error Reporting (WER) generates a user-mode memory crash dump (.dmp file), which by default is located under %LOCALAPPDATA%\CrashDumps. Security Center collects an ephemeral copy of the crash dump file and scans it for evidence of exploits and compromises.

If Security Center finds such evidence, it generates an alert like the one shown in Figure 5-2. This alert indicates that the crash-dump analysis has detected executable code that exhibits behavior that is commonly performed by malicious payloads. Although non-malicious software may perform this behavior, it is not a typical development practice. Follow the remediation steps to investigate this issue further.

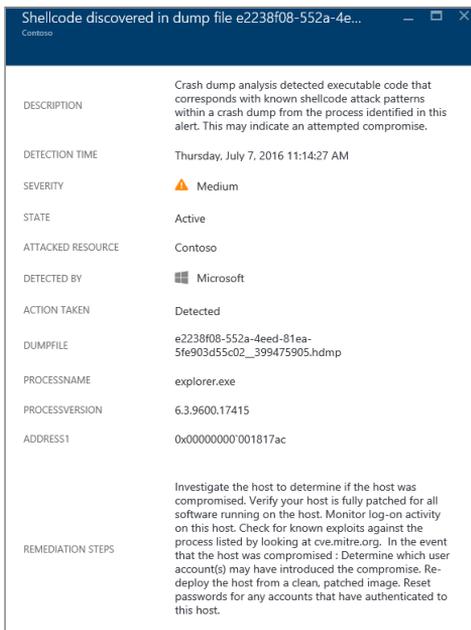


FIGURE 5-2 Crash-dump analysis alert.

Accessing security alerts

The number of security alerts you see in the Security Center dashboard may vary depending on the amount of resources that you are monitoring with Security Center and the business itself. Some organizations receive more attacks than others, and as a result have more security alerts.

If you don't have any security alerts in your environment, simulate one by following the procedures in the following article: <https://aka.ms/ASCAAlertValidation>. Once you have an alert, follow these steps to access it:

1. Open the **Azure Portal** and sign in as a user who has **Security Admin** privileges.
2. In the left pane, click **Security Center**.
3. In the left pane of the Security Center window, under **Detection**, click **Security Alerts**. The Security Alerts dashboard appears. (See Figure 5-3.)



FIGURE 5-3 The Security Alerts dashboard.

4. The Security Alerts dashboard lists current alerts, organized by severity (with high-severity alerts listed first), and a bar graph showing the distribution of high-, medium-, and low-severity alerts. Click an alert type to open a new blade showing resources that have been flagged with the alert. (See Figure 5-4.)

| ATTACKED RESOURCE | COUNT | DETECTION TIME | ENVIRONMENT | STATE | SEVERITY |
|-------------------|-------|----------------|-------------|--------|----------|
| vm1 | 1 | 08:01:00 PM | Azure | Active | High |

FIGURE 5-4 A list of attacked resources.

The list contains the following information about each attacked resource:

- The name of the attacked resource
 - The number of times the resource was attacked
 - The time at which the attack was detected
 - The environment in which that the resource resides
 - The state of the alert
 - The severity of the alert
5. Click an attacked resource to see details about the attack, including the following. (See Figure 5-5. Note that the subscription ID has been intentionally obscured in this figure.)
 - A clear description of the attack
 - Attack-specific information, such as the source IP and the software used by the attacker
 - A list of steps to remediate the issue
 6. Return to the main **Security Center** dashboard.

TIP You can use the Azure Activity Log to query security alerts originated by Azure Security Center. For more information, see <https://aka.ms/ASCActivityLog>. You can also use the Alert API to obtain these alerts; see <https://aka.ms/ASCAlertAPI> for details.

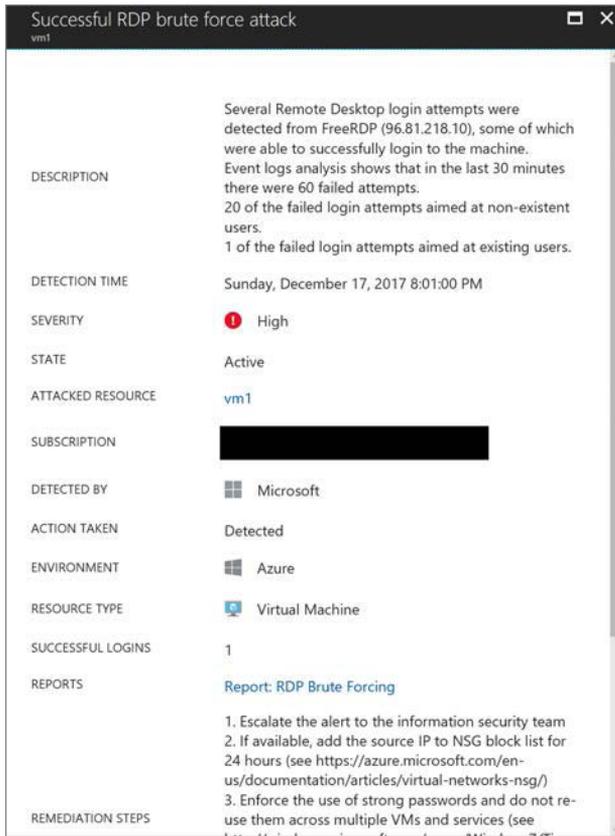


FIGURE 5-5 Details of a security alert.

Security incidents

Some attacks may happen in a completely isolated way. Others will be coordinated—that is, part of the same attack campaign. Security Center can identify correlations among these types of attacks and create a security incident that contains two or more related security alerts. To see how this works, follow these steps:

1. In the left pane of the Security Center window, under **Detection**, click **Security Alerts**. If Security Center has identified a security incident in your environment, it will create an alert marked by a different icon. (See the first two alerts in Figure 5-6.)

| DESCRIPTION | COUNT | DETECTED BY | ENVIRONME... | DATE | STATE | SEVERITY |
|--|-------|-------------|--------------|----------|--------|----------|
| Security incident with shared process detected | 1 | Microsoft | Azure | 10/19/17 | Active | High |
| Security incident with shared process detected | 1 | Microsoft | Azure | 10/10/17 | Active | High |
| Potential SQL Injection | 1 | Microsoft | Azure | 12/21/17 | Active | High |
| Modified system binary discovered in dump... | 1 | Microsoft | Azure | 12/18/17 | Active | High |

FIGURE 5-6 Security incidents appear in the Security Alert dashboard with a different icon.

- Click a security incident. A new blade opens with more details about the incident. In the blade shown in Figure 5-7, the incident contains two alerts and two notable events. These notable events are contextual information that can help you during an investigation. (Note that the subscription ID and attacked resources have been intentionally hidden in the figure.)

Security incident with shared process detected

The incident which started on 2017-10-19 10:30:40 UTC and recently detected on 2017-10-24 20:16:45 UTC indicates that an attacker has abused resource in your resource [REDACTED]

DESCRIPTION

DETECTION TIME Thursday, October 19, 2017 4:30:40 AM

SEVERITY High

STATE Active

ATTACKED RESOURCE [REDACTED]

SUBSCRIPTION [REDACTED]

DETECTED BY Microsoft

ENVIRONMENT Azure

Alerts included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE | SEVERITY |
|--|-------|-------------------|-------------------|----------|
| Local Administrators group members were... | 1 | 10/19/17 04:30 AM | [REDACTED] | Medium |
| Local Administrators group members were... | 1 | 10/24/17 05:52 AM | [REDACTED] | Medium |

Notable events included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE |
|--|-------|-------------------|-------------------|
| Potentially suspect behaviour reported as extra... | 3 | 10/24/17 06:31 AM | [REDACTED] |
| Rare SVCHOST service group executed | 1 | 10/24/17 06:33 AM | [REDACTED] |

Investigation not available

FIGURE 5-7 Details about a security incident.

NOTE The advantage of using the Security Incident blade is that it tells you which alerts are related. This can help you to track down the perpetrator and identify compromised systems.

- Click an alert to see details about the alert. The details will be similar to those shown in Figure 5-5.
- Click a notable event. This opens a page containing contextual data about the event. (See Figure 5-8.) This page shows the suspicious process name and the command

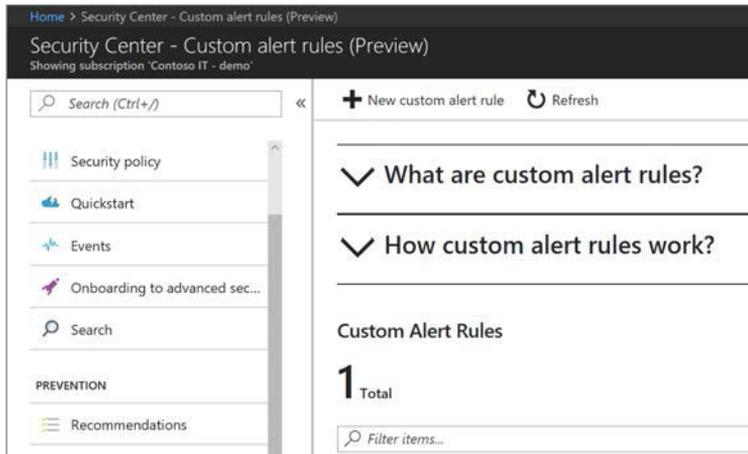


FIGURE 5-9 Creating a custom alert.

2. Click the **New Custom Alert Rule** button. The **Create a Custom Alert Rule** blade appears. (See Figure 5-10.)

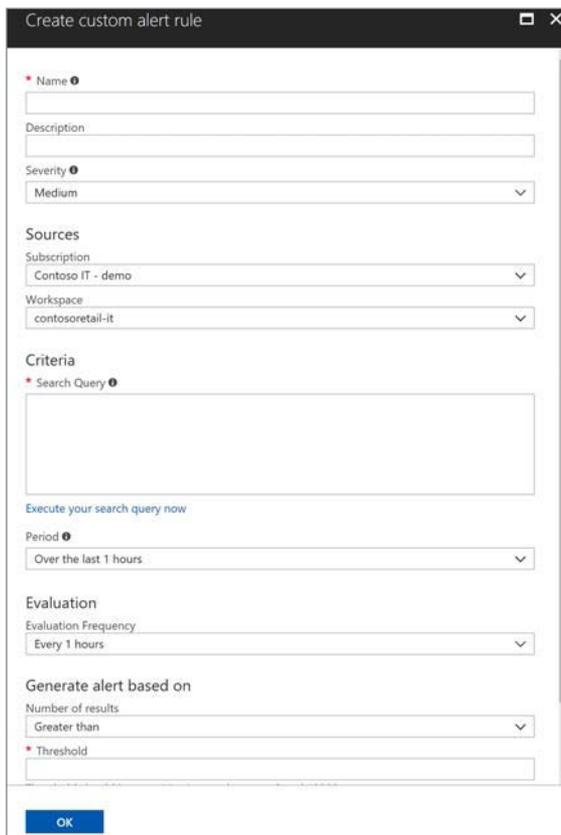


FIGURE 5-10 The Create Custom Alert Rule blade.

3. In the **Name** field, type the name for this rule.
4. In the **Description** field, type a brief description of the rule's intent.
5. In the **Severity** drop-down list, select the severity level—High, Medium, or Low. Choose a level that reflects the priority of this alert for your security operations team.
6. In the **Sources** section, open the **Subscription** drop-down list and select the subscription that will be used by this custom rule.
7. Open the **Workspace** drop-down list and choose the workspace against which this rule should be running.
8. In the **Search Query** box in the **Criteria** section, search for the event you want to monitor. For example, if you want to monitor all security events whose identifier is *4688* and whose command line contains the word *diskpart*, type the following query and click the **Execute Your Search Query Now** link:

SecurityEvent | where EventID==4688 and CommandLine contains "diskpart"

TIP The query language used for this search is the Log Analytics language. For more information about this language, and for more examples, see <https://aka.ms/laquerylan>.

9. In the **Period** drop-down list, select the time interval that should be used for this query. (By default, it will test over the last hour.)
10. In the **Evaluation** section, open the **Evaluation Frequency** drop-down list and specify how frequently this custom rule should be executed.
11. The **Generate Alert Based On** section contains two settings that are directly correlated: **Number of Results** and **Threshold**. Open the **Number of Results** drop-down list and choose **Greater Than**. Then, in the **Threshold** box, type **2**. The alert will be triggered if the result for the query is greater than 2.
12. Select the **Enable Suppress Alerts** option if you want to set a time to wait before Security Center sends another alert for this rule.
13. Click **OK** to create the new rule. It will appear in the **Custom Alert Rules** section of the **Custom Alert** blade. (See Figure 5-11.)

| Custom Alert Rules | |
|--------------------|-------------------------------|
| 1 Total | |
| Filter items... | |
| ALERT NAME | DESCRIPTION |
| ASCBook | Testing Rule for the ASC Book |

FIGURE 5-11 The new custom rule.

- Now that you've created the new rule, alerts pertaining to this rule will appear with other alerts in the **Security Alerts** dashboard. (See Figure 5-12.)

| DESCRIPTION | COUNT | DETECTED BY | ENVIRONME... | DATE | STATE | SEVERITY |
|--------------------------|-------|-------------|--------------|----------|--------|----------|
| NEW ASCBook | 1 | Alert Rule | Azure | 12/25/17 | Active | Medium |

FIGURE 5-12 A new security alert based on the custom rule that was created.

Investigating a security issue

In some scenarios, the information you obtain from a security alert can be enough for your incident-response team to conduct an investigation and identify the root cause of the issue. However, in some circumstances, you may need more details to understand the correlation between alerts and how the attack was performed. In Security Center, you can use the **Investigation** feature to obtain this information. Follow these steps:

- In the left pane of the Security Center window, under **Detection**, click **Security Alerts**.
- In the **Security Alerts** dashboard, click the security alert that you want to investigate.
- Select the attacked resource you want to investigate. Then click the **Investigate** option at the bottom of the security alert page. (After you click the Investigate option for an alert, it changes to a **Continue an Investigation** option.) The **Investigation** dashboard appears. (See Figure 5-13.)



FIGURE 5-13 The Investigation dashboard with a security incident selected.

On the left side of the Investigation dashboard is the **investigation path** and **map**. The relevant entities (security alerts, computer, users, and security incidents) appear correlated in the map, and the timeline shows the current data interval for this investigation. On the right side are the attributes for the selected entity in the map. For example, Figure 5-14 shows the attributes for the entity selected in Figure 5-13.

Failed RDP Brute Force Attack

Related ▼
 TO INCIDENT

Medium
 PRIORITY

ASC
 DETECTED BY

▼ **General Information**

| | |
|----------------|--|
| DESCRIPTION | Several Remote Desktop login attempts were detected from IP Address: 201.244.154.112, none of them succeeded. Event logs analysis shows that in the last hour there were 230 failed attempts. Some of the failed login attempts aimed at 1 existing user(s). |
| ALERT ID | 2518880795999999999_8069927e-4999-42fe-9437-9c9ee993dffe |
| TIME GENERATED | 12/25/2017 1:34:43.000 PM |
| START TIME | 12/25/2017 11:00:00.000 AM |
| END TIME | 12/25/2017 11:00:00.000 AM |

FIGURE 5-14 Security incident detected attributes.

The approach you take when investigating a security issue may vary depending on the attack, the amount of information available, and what you already know about the attack. For this example, one option would be to analyze the information available from the resource that was attacked—in this case, *contosoweb1*.

4. In the investigation map, click **contosoweb1** to see more details about it. Notice that the investigation map also changes. (See Figure 5-15.) As you can see, there are more than 45 alerts on this server, and there have been anonymous login attempts from the *contosoretail* domain.



FIGURE 5-15 The investigation map reflects the selected entity.

- To explore further, click the **Exploration** option in the right pane. (See Figure 5-16.)

The screenshot shows the Security Center interface for the entity contosoeb1.contosoretail.com. The main area displays a list of issues on the computer:

| Issue | Count | Action |
|---|-------|--------|
| Missing security updates | 3 | Search |
| Rarely used processed often employed by attackers | 6 | Search |
| Accounts failed to log on | 8K | Search |
| Distinct processes executed on the machine | 72 | Search |
| Number of accounts logged on to the machine | 10 | Search |

The right pane shows navigation options: Info, Entities, Search, and Exploration (highlighted).

FIGURE 5-16 Exploring more options for the selected entity.

6. Review all the events in the **Exploration** page. These will be very important for your investigation and can help you understand how the attack took place.
7. Repeat steps 4–6 for each relevant entity in the investigation map. As the map redraws itself, it will become clearer how the attack took place and which systems were compromised. As you click each entity, the options available to you may change depending on the entity type.
8. To see all entities correlated with the entity you've selected on the map, click the **Entities** option. The example shown in Figure 5-17 displays two entities (Alerts and Computers) that are correlated with the selected user on the map.

abbybecker_contoso.europedemo.onmicrosoft.co...

Alerts 1

| TITLE | TIME GENERATED | SEVERITY |
|-------------------------------------|---------------------------|----------|
| Sign-in from an unfamiliar location | 11/28/2017 9:13:28.000 AM | Medium |

Computers 2

NAME

contosowebbe2.contoso.europe.com

FIGURE 5-17 Entities correlation.

9. To visualize events correlated with the selected entity, click the **Search** option. The example in Figure 5-18 shows the events correlated with a server.

contosowebfe1.contoso.europe.com

You have the following logs on computer 'contosowebfe1.contoso.europe.com':

| NAME | COUNT |
|-------------------------|-------|
| SecurityEvent | 45K |
| Heartbeat | 18.7K |
| Update | 6.1K |
| SecurityBaseline | 1.7K |
| Usage | 1.2K |
| ProtectionStatus | 312 |
| UpdateSummary | 47 |
| SecurityBaselineSummary | 13 |
| SecurityDetection | 4 |

FIGURE 5-18 Events correlated with the selected entity.

10. Click one of the events. The **Log Search** dashboard from **Log Analytics** opens and shows all records.

As you continue to investigate each entity, you may find that Security Center will flag an entity as **unrelated** to the incident. (See Figure 5-19.)

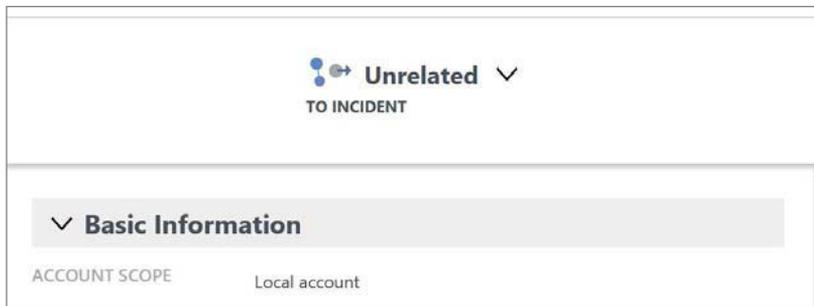


FIGURE 5-19 Security Center may flag an entity as unrelated to the incident.

Usually, this determination is accurate. However, in some scenarios, you may find that a correlation between that entity and the incident does exist. In that case, you'll want to manually change that flag.

11. To change the flag, click the drop-down arrow next to the **Unrelated** heading, select **Related**, and choose a reason in the drop-down list. (See Figure 5-20.)

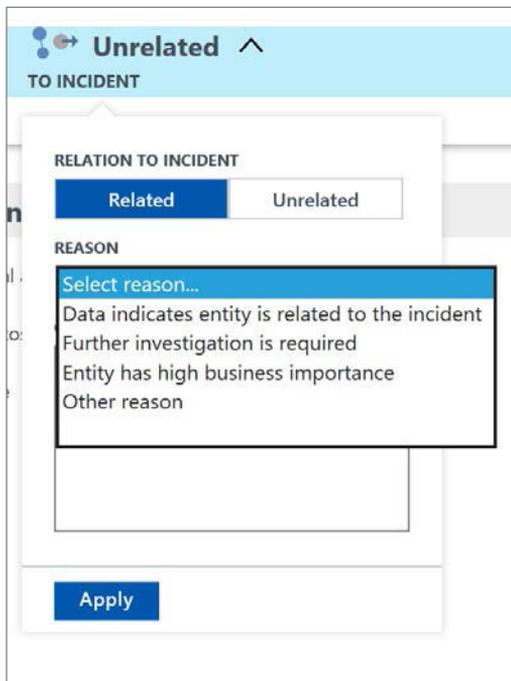


FIGURE 5-20 Changing the entity relation with the incident.

Responding to a security alert

Now that you know how to use Security Center to detect an alert and how to investigate a security issue, you can move to the next phase: responding to a security alert. To aid you in this, Security Center supports a feature called security playbook. Security playbooks enable you to create a collection of procedures that can be executed from Security Center when a certain security alert is triggered. Azure Logic Apps is the automation mechanism behind security playbooks.

Before creating a playbook, you should have in mind what you want to automate. Before implementing this feature, answer the following questions:

- For which security alert should I automate a response?
- What steps should be automated if the conditions for this alert are true?
- What steps should be automated if the conditions for this alert are false?

NOTE This is only a sampling of questions to get you started. As you start creating security playbooks, other questions may be raised.

Creating a playbook

In this example, the goal is to create a security playbook that sends an email anytime a high alert is triggered. Follow these steps:

1. In the left pane of the Security Center window, under **Automation & Orchestration**, click **Playbooks**. The Playbook dashboard opens. Assuming this is the first time you've created a playbook, the dashboard will be empty, as shown in Figure 5-21.

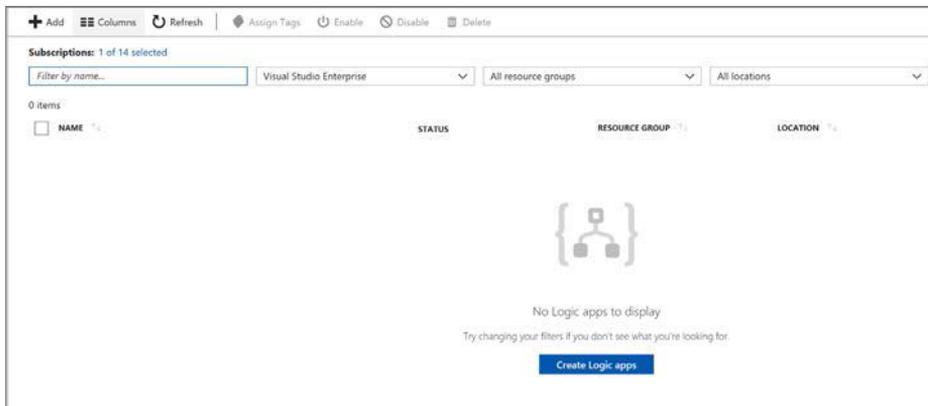


FIGURE 5-21 Creating a new security playbook.

2. Click the **Create Logic App** button. The **Create Logic App** blade appears. (See Figure 5-22.)

The screenshot shows the 'Create logic app' blade with the following fields and options:

- Name:** A text input field.
- Subscription:** A dropdown menu with 'Visual Studio Enterprise' selected.
- Resource group:** Radio buttons for 'Create new' (selected) and 'Use existing', with a text input field below.
- Location:** A dropdown menu with 'North Central US' selected.
- Log Analytics:** 'On' and 'Off' buttons.
- Information box:** A blue 'i' icon and text: 'You can add triggers and actions ... your Logic App after creation.'
- Pin to dashboard:** A checkbox.
- Buttons:** A blue 'Create' button and a link for 'Automation options'.

FIGURE 5-22 Creating a new logic app.

3. In the **Name** box, type a name for this playbook.
4. In the **Subscription** drop-down list, select your subscription type.
5. In the **Resource Group** section, select either the **Create New** or the **Use Existing** option. If you select the latter, type the name of the existing group in the box below the option buttons.
6. Select a location from the **Location** drop-down list.
7. If you want to monitor your workflow using Log Analytics, you can click the **On** button in the **Log Analytics** section. For this example, leave it **Off**, which is the default.

8. Click the **Create** button. The new playbook will appear in the list in the Playbook dashboard. (See Figure 5-23.) If you don't see it, click **Refresh**.

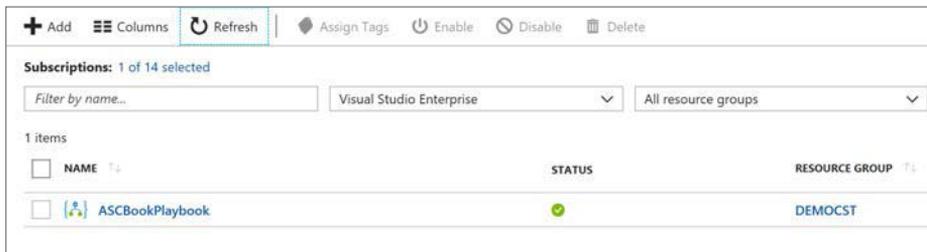


FIGURE 5-23 New playbook successfully created.

Building the workflow

You've created a playbook, but it doesn't contain any procedures yet. Your next step is to build the workflow for the playbook. Follow these steps:

1. Click the playbook you just created to edit it.
2. Under **Templates**, click **Blank Logic App**. The **Logic Apps Designer** dashboard appears.
3. In the **Search** box, type **Security Center**. (See Figure 5-24.)

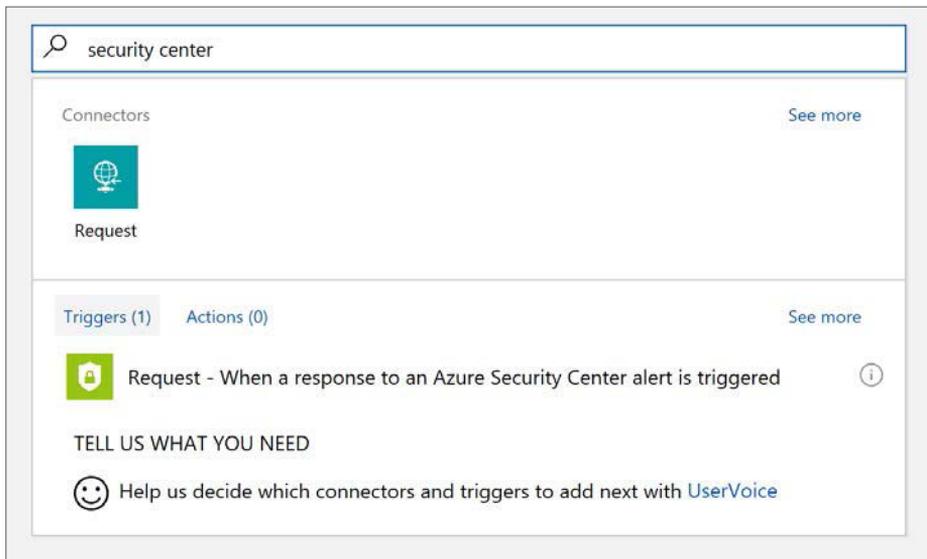


FIGURE 5-24 Using the Security Center template in Logic Apps.

4. Click the **Request – When a Response to an Azure Security Center Alert Is Triggered** option.

5. Click the **New Step** button. The options shown in Figure 5-25 appear.

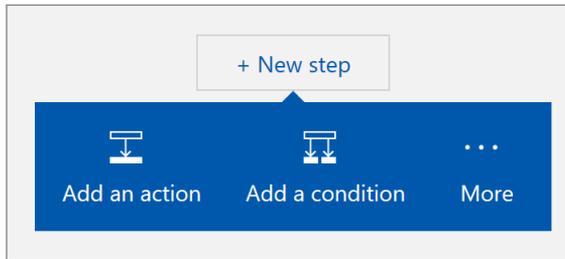


FIGURE 5-25 Adding a new step to the workflow.

6. Click **Add a Condition**. The options shown in Figure 5-26 appear.

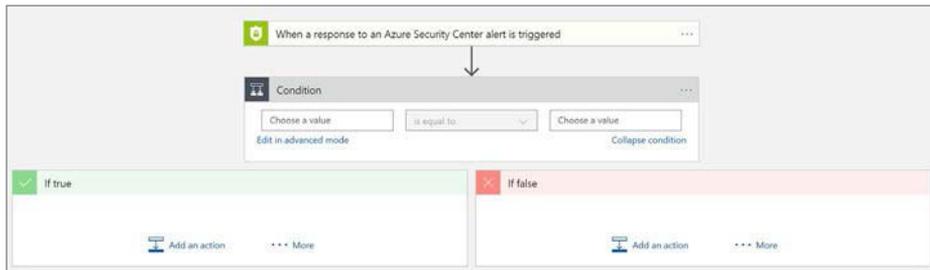


FIGURE 5-26 Adding a new condition to the workflow.

7. Under **Condition**, click the first box, and select **Alert Severity** from the drop-down list that appears. Then click the gray area outside the Condition settings to hide the drop-down list.
8. Leave the second box with the default option (**Is Equal To**).
9. Click in the third box and type **Medium**.
10. In the **If True** section, click **Add an Action**, and choose **Office 365 Outlook** from the drop-down list that appears.
11. Open the **All Actions** drop-down list and choose **Office 365 Outlook – Send an Email**.
12. Sign in with your Office 365 or corporate Outlook account. This is the email address that will be used to send the email when this condition is met. You should see a dialog box like the one shown in Figure 5-27.

NOTE In a real-world scenario, you could use a custom account—for example, `incident@contoso.com` or `support@contoso.com`—instead of a user email address.

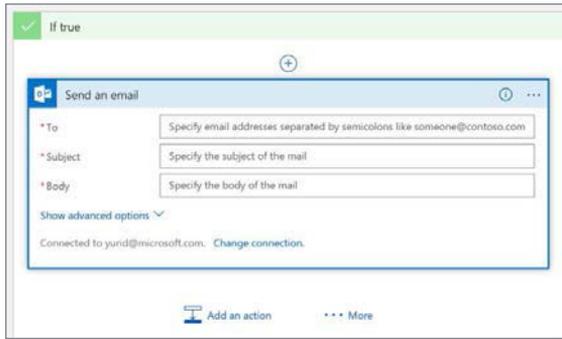


FIGURE 5-27 Email parameters.

13. Type the destination address in the **To** field. This is the mailbox that will receive the alert. If you want to send the alert to more than one mailbox, separate each address with a semicolon.
14. In the **Subject** field, type a brief message that reflects the intent of the email—for example, **High Severity Alert Detected**.
15. In the **Body** field, type a generic message, and concatenate it with the variables that appear in the drop-down list next to the **Send an Email** box. (See Figure 5-28.)

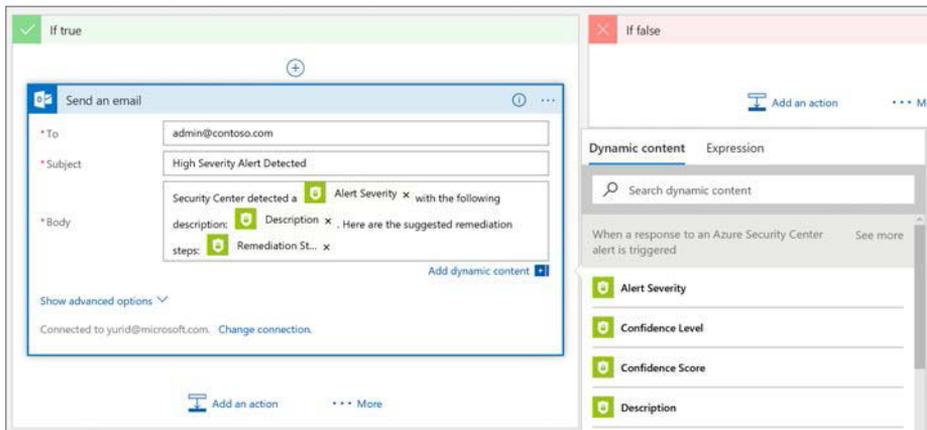


FIGURE 5-28 Description using fixed text and variables.

16. If you want to trigger an action if the alert is not a high priority, repeat steps 10–15 in the **If False** section.
17. Click **Save** in the upper-left corner of the **Logic Apps Designer** dashboard.
18. Click **Close** in the **Logic Apps Designer** dashboard and in the playbook's properties.

Executing a playbook

Now that the playbook contains a workflow, you can execute the playbook. You can do so from two locations: the **Security Alerts** dashboard or the **Investigation** dashboard. The following steps demonstrate the execution from the **Security Alerts** dashboard.

NOTE As of this writing, the playbook feature is on preview and is a manual process.

1. In the left pane of the Security Center window, under **Detection**, click **Security Alerts**.
2. The playbook you created applies to high-severity alerts. To meet this condition, click a high-priority alert.
3. Click the attacked resource that corresponds to the high-priority alert. A blade for the attacked resource opens.
4. Click the **Run Playbooks** button. The Playbooks blade appears. (See Figure 5-29.)

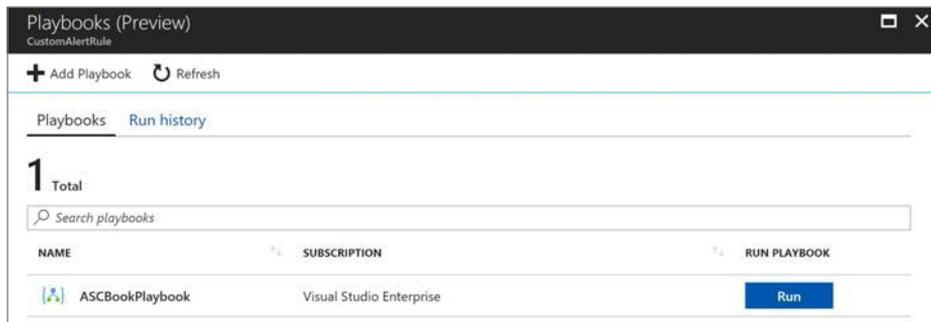


FIGURE 5-29 The Playbooks blade with the playbook you just created.

5. Click **Run**. The security playbook runs.
6. To confirm that the playbook ran correctly, click the **Run History** tab, click the **Refresh** button, and check the result. (See Figure 5-30.)



FIGURE 5-30 The Run History tab shows a history of every execution of this playbook.

7. Check the mailbox you set as the destination for the email generated by the playbook. You should have received an email from Security Center about the alert based on the parameters you set when you created the workflow.

When you click **Run History**, the log you see pertains only to the execution of the playbook against the alert you selected. Let's call it Alert A. If you run the same playbook on a different alert—Alert B—you won't see an entry for that operation in the history for Alert A. Instead, it will appear in a separate history, for Alert B.

Auditing playbook execution

As noted, you can check whether a playbook was executed against a particular alert by viewing its history. However, this won't show you whether the playbook was executed against *all* relevant alerts. For that, you should audit the playbook's execution. That way, you see its full execution log. Follow these steps to perform this operation:

1. In the left pane of the Security Center window, under **Automation & Orchestration**, click **Playbooks**.
2. Click the playbook you want to audit.
3. The playbook's properties cite the details of all executions, including the date, start time, and duration. You can also filter by date and time. (See Figure 5-31.)

The screenshot displays two panels: 'Runs history' and 'Trigger History'.

Runs history

Filters: All, Start ti..., Pick a date, Pick a time

Specify the run identifier to open monitor view directly (→)

| STATUS | START TIME | IDENTIFIER | DURATION |
|-----------|-------------------|------------------|---------------|
| ✓ Succ... | 12/26/2017 4:2... | 0858687279503... | 2.13 Seco... |
| ✓ Succ... | 12/26/2017 4:2... | 0858687280075... | 543 Millis... |

Trigger History

Filters: All, Start ti..., Pick a date, Pick a time

manual

Callback url [POST]
<https://prod-03.eastus.logic.azure.com:443/workflows/...>

| STATUS | START... | FIRED |
|-----------|----------|-------|
| ✓ Succ... | 12/26... | Fired |
| ✓ Succ... | 12/26... | Fired |

FIGURE 5-31 Complete history of executions for this playbook.

4. For more details on a particular execution, click the execution line. The **Run History** blade opens with the **Logic App Run** dashboard displayed. (See Figure 5-32.)

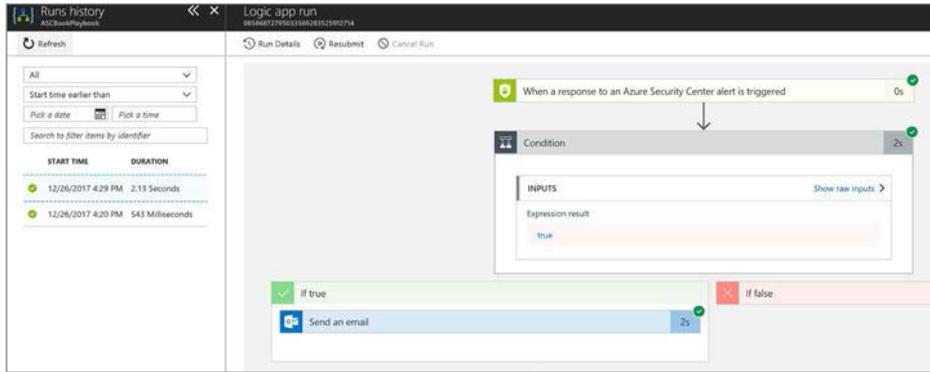


FIGURE 5-32 More details about a particular execution.

Notice that in the workflow, a small green check mark appears in the upper-right corner of each box. This indicates the successful execution of that particular step.

5. If you don't see a green check mark, click the step to view the raw data and troubleshoot. For example, if you click the **When a Response to an Azure Security Center Alert Is Triggered** option, you will see the raw input and output received by the Logic App. (See Figure 5-33.)

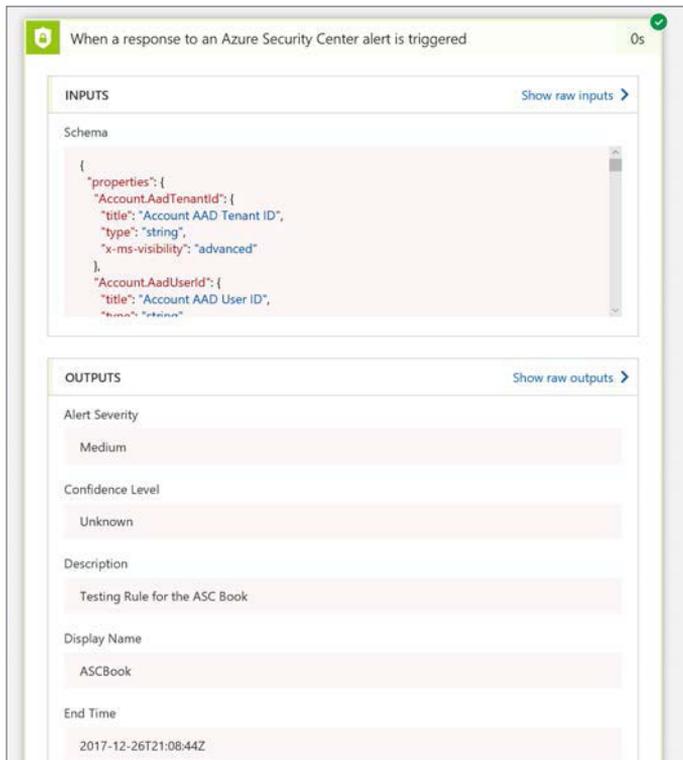


FIGURE 5-33 Raw input and output.

6. Click **Close** in the Logic App Run page and in the playbook's properties.

You can integrate the playbook with solutions from certain partners. For example, you can integrate it with Service Now to create a service ticket when an incident is detected.

TIP The following presentation, delivered by co-author Yuri Diogenes at Ignite 2017, shows how to integrate playbook with Slack: <https://youtu.be/e8iFCz5RM4g>.

Index

A

- AAD (Azure Active Directory), 125–127
- access and identity
 - activities, 141–142
 - Failed Logons, 144–147
 - Identity Posture, 143–144
 - Logons Over Time, 147–148
 - management, 9
 - restricting, 61–63
- Access Control (IAM), 22
- ACLs (access control lists), 12
- Activity Log, 78
- AD Identity Protection,
 - integration with ASC, 148–149
- Adaptive Application Controls, 38, 111–114
- agents
 - installing, 26–30
 - missing and not responding, 52
 - removing, 35
- Amazon EC2 keys, theft, 7
- analytics. *See* Log Analytics
- anomaly detection, 20, 106–108
- Antimalware installation, 55
- application controls, 111–114
- application whitelisting, 111–114
- applications. *See also* logic app
 - firewalls, 68–71
 - as malware, 5
- ASC (Azure Security Center).
 - See also* security; SIEM (Security Incident and Event Management); Splunk
 - integration solution
 - access control, 22
 - analytics, 20
 - architecture, 18–21
 - assessment, 30–32
 - connectivity, 18
 - considerations, 22–24
 - dashboard, 21–22, 142
 - detection capabilities, 20–21
 - event evaluation, 20
 - Failed Logons, 144–147
 - features, 15–16
 - Identity Posture, 143–144
 - incorporating, 24–25
 - intelligence resources, 104
 - JIT VIM access
 - feature, 115–119
 - Logons Over Time, 147–148
 - Monitoring Agent, 19
 - next-generation
 - policy, 38–43
 - onboarding resources, 25–30
 - overview, 17–18
 - permissions, 49–50
 - RBAC (role-based access control), 22–23d
 - recommendations, 23–24
 - security operations, 24–25
 - security policy, 23
 - storage, 23
 - subscription, 17–18
 - tiers, 17–18
 - assume-breach mentality, 6. *See also* attacks
 - atomic detection, 101–102
 - ATP (Advanced Threat Protection), 155
 - attack vectors, identifying, 2–3
 - attacked resources, listing, 77–78
 - attacks. *See also* assume-breach mentality; detection capabilities; Trojans
 - brute force, 85
 - drive-by download sites, 4
 - IP addresses, 7
 - local privilege escalation, 3
 - RDP brute force, 114
 - SSH brute-force, 114
 - attributes, obtaining
 - for VMs, 167
 - authentication-related issues, investigating, 152
 - Azure AD Identity Protection
 - customizing search, 149–152
 - integration, 148–149
 - Azure Automation and PowerShell, 30
 - Azure Log Analytics
 - customizing searches, 149–152
 - IntelliSense, 152
 - query language, 83

- query result, 158
- website, 19
- Azure Monitor add-on
 - accessible logs, 124
 - event-hub connection, 136–138
 - and Splunk, 139
- Azure Policy. *See also* policies; security policies
 - customizing, 49
 - definitions and assignments, 44, 48
 - elements, 47
 - exploring, 45–48
 - initiative definitions and assignments, 44–45
 - JSON configuration, 48
 - overview, 43–44
 - scope, 44
- Azure Portal, 11–12
- Azure security. *See also* security
 - Disk Encryption, 14
 - host protection, 12
 - network protection, 12–13
 - overview, 11–12
 - storage protection, 14

B

- behavioral analytics, 20, 104–105
- blades, security policies, 35–36
- BLOBs (binary large objects), 37
- botnets, defined, 2
- breaches. *See* assume-breach mentality; attacks
- brute-force attacks, 85

C

- C2 (command and control) servers, 4
- CAV (counter-antivirus) services, 2
- CCE (Common Configuration Enumeration), 25, 52, 56–58

- cloud defense
 - cyber kill chain, 108–111
 - fusion alerts, 108–111
 - JIT VM access, 114–119
 - threat detection, 100–108
 - threat prevention vs. detection, 99–100
- cloud security, rethinking, 31–32
- cloud threats
 - access management, 9
 - compliance, 8–9
 - data protection, 10
 - endpoint protection, 10
 - identity management, 9
 - and machine learning, 105–106
 - operational security, 9
 - overview, 7–8
 - risk management, 9
- compliance, 8–9
- compute recommendations
 - CCE (Common Configuration Enumeration), 56–58
 - endpoint protection, 52–56
 - overview, 51–52
 - security configurations, 56
- compute recommendations, accessing, 30–31
- configuration flaws, 7
- contextual information alerts, 74
- crash-dump analysis, 76
- CSPs (cloud solution providers), 8–9
- cyber kill chain, 2–4, 108–111
- cybercrime, 1–2

D

- data and storage
 - encryption, 66–67
 - overview, 63–64
 - protection, 10
 - server auditing, 64–66
 - threat detection, 64–66
- Data Collection blade, 38–40

- database auditing, 64
- DCU (Digital Crimes Unit), 153
- defense layers, 11
- detect, security posture, 5–6
- detection capabilities, 74, 154–155. *See also* attacks
- DevOps, 7
- DiCola, Nicholas, 71
- Disk Encryption policy, 37, 52
- domain dominance, 3
- drive-by download sites, 4

E

- Email Notifications blade, 41–42
- encryption, 14. *See also* Storage Encryption policy
- Endpoint Protection policy, 10, 37, 52–56
- entities and incidents, 87–88
- error codes, website, 173. *See also* WER (Windows Error Reporting)
- ETW (Event Tracking for Windows), 19
- Event 4625, 145–147
- event hub
 - connecting to Azure Monitor, 136–138
 - creating for SIEM, 122, 131–132
 - shared access key, 133–136
- events. *See also* notable events
 - correlating with entities, 87
 - evaluating, 20
 - filtering, 39

F

- Failed Logons section, 144–147
- Fender, Sarah, 31–32
- financial losses, 1
- firewalls, 58, 68–70

G

GitHub public secret attack, 7–8

H

Healthy Databases, 64
 host protection, 12
 Hunter, Laura E., 15–16
 hunting security issues, 159–162
 Hyper-V virtualization solution, 12

I

IaaS (Infrastructure as a Service), 17
 IAM (Access Control), 22
 IC3 (Internet Crime Complaint Center), 1–2
 Identity & Access, customizing search, 149–152
 identity and access
 activities, 141–142
 Failed Logons, 144–147
 Identity Posture, 143–144
 Logons Over Time, 147–148
 management, 9
 restricting, 61–63
 Identity Posture section, 143–144
 IExpress self-extractor, 29
 inbound security rules, 62–63
 Incident Playbook, 162. *See also* playbooks
 incident response. *See* security incidents
 crash-dump analysis, 76
 detection scenarios, 75–76
 security alerts, 73–75
 spam activity, 75
 InfoSec Institute, lurking statistic, 5
 initiative definitions and assignments, 44–45

install and exploit, 109–110
 intel, obtaining, 3
 IntelliSense, Log Analytics, 152
 internet-facing endpoints,
 59, 61–63
 Investigation feature, using, 84–88
 IP addresses, attacks, 7
 IPFIX (Internet Protocol Flow Information Export), 74
 IT assets, securing, 99–100

J

JIT Network Access, 37–38, 52
 JSON configuration
 OS customization, 169–172
 policies, 48
 Just-in-Time VM access, 114–119.
 See also VMs (Virtual Machines)

K

Kemnetz, John, 122
 Key Vault blade
 app password, 130–131
 creating, 127–130
 Kliger, Ben, 106
 Koren, Koby, 142

L

Landau, Miri, 169
 legacy security policy, 33–38
 Linux agents, installing, 27
 local privilege escalation attack, 3
 Log Analytics
 customizing searches, 149–152
 IntelliSense, 152
 query language, 83
 query result, 158
 website, 19

log search, customizing, 150
 logic app, creating, 90. *See also* applications
 logon failures, reasons for, 144
 Logons Over Time
 section, 147–148
 lurking statistic, 5

M

machine learning and
 cloud, 105–106
 malware
 Antimalware installation, 55
 apps as, 5
 Microsoft
 Antimalware installation, 55
 Monitoring Agent, 19
 Security Intelligence Report/
 IP-address attacks, 7
 Missing Disk Encryption, 52
 Missing Scan Data, 52
 Missing System Updates, 52
 Monitoring Agent, 19
 MSRC (Microsoft Security Response Center), 153
 MSTIC (Microsoft Threat Intelligence Center), 153

N

network analysis alerts, 74
 network protection, 12–13
 network recommendations
 internet-facing
 endpoints, 61–63
 NSGs on subnets not
 enabled, 59–61
 overview, 58–59
 restricting access, 61–63
 NGFW (Next-Generation Firewall) policy, 37, 58
 Nitol botnet, 2

notable events, 162. *See also* events

Notepad++, downloading, 170
 NSGs (network security groups),
 12, 37, 59–61,

O

omsagent daemon, 19
 onboarding resources, 25–30
 operational security, 9
 OS hardening, rules, 169, 172–173
 OS security configuration
 considerations, 168–169
 customizing, 169–173
 JSON file, 169–172
 uploading rule, 173
 OS Version Not Updated, 52
 OWASP documentation for
 cyberattacks, 68

P

permissions
 and OS customization, 168
 and RBAC, 49–50
 Petya ransomware, 1
 playbooks. *See also* Incident
 Playbook; security alerts
 auditing execution, 95–97
 creating, 89–91
 executing, 94–95
 website, 162
 workflows, 91–93
 policies. *See* Azure Policy;
 security policies
 Policy Management blade, 40–41
 post breach, 109–110
 Potential SQL Injection alert, 74.
See also SQL databases

PowerShell, script to obtain VM's
 attribute, 167
 Prakash, Ajeet, 155
 prevention, importance of, 71
 Pricing Tier blade, 42–43
 Privileged Access Workstations, 10
 protect, security posture, 5–6
 public key secret, 7

Q

QKSee
 installation, 3
 Trojan, 4

R

ransomware
 complaints, 1
 financial loss, 1
 Petya, 1
 WannaCry, 1
 RBAC (role-based access
 control), 11, 22–23, 49–50
 RDP brute-force attacks, 114
 recon, internal and external, 3
 red/blue team simulations, 6
 Remediate Security
 Configurations, 52, 56–58
 removing agents, 35
 reports, linking to security
 alerts, 156
 resource analysis alerts, 74
 resources, onboarding, 25–30
 respond, security posture, 5–6
 Restart Pending, 52
 risk management, 9
 rules, OS hardening, 169, 172–173

S

scan data, 52
 SDL (Security Development
 Lifecycle), 68
 SecOps (security operations), 24
 securing IT assets, 99–100
 security. *See also* ASC (Azure
 Security Center)
 cloud threats, 7–11
 incidents, 79–81
 resources, 12
 security admin role, 22
 security alerts. *See also* playbooks
 accessing, 77–84
 categories, 74
 customizing, 81–84
 displaying, 160–161
 linking to reports, 156
 overview, 73–74
 responding to, 89
 security assessments,
 customizing, 169
 Security Center
 access control, 22
 analytics, 20
 architecture, 18–21
 assessment, 30–32
 connectivity, 18
 considerations, 22–24
 dashboards, 21–22, 142
 detection capabilities, 20–21
 event evaluation, 20
 Failed Logons, 144–147
 features, 15–16
 Identity Posture, 143–144
 incorporating, 24–25
 intelligence resources, 104
 JIT VIM access feature, 115–119
 Logons Over Time, 147–148
 Monitoring Agent, 19
 next-generation policy, 38–43

- onboarding resources, 25–30
- overview, 17–18
- permissions, 49–50
- RBAC (role-based access control), 22–23
- recommendations, 23–24
- security operations, 24–25
- security policy, 23
- storage, 23
- subscription, 17–18
- tiers, 17–18
- Security Configurations policy, 36
- security data, analyzing, 149–152
- security incidents, 110, 160–161.
 - See incident response
- security issues
 - hunting, 159–162
 - investigating, 84–88
- security playbooks. *See also* Incident Playbook; security alerts
 - auditing execution, 95–97
 - creating, 89–91
 - executing, 94–95
 - website, 162
 - workflows, 91–93
- security policies. *See* Azure Policy; policies
 - blades, 35–36
 - customizing, 49
 - legacy, 33–38
 - overview, 23
- security posture, 5–6
- security reader role, 22
- security rules, 62–63
- server auditing, 64–66
- SIEM (Security Incident and Event Management), 121–123.
 - See *also* Splunk integration solution
- Slack, integrating playbooks, 97
- social engineering, 3
- spam activity, detecting, 75
- Splunk integration solution.
 - See *also* ASC (Azure Security Center); SIEM (Security Incident and Event Management)
 - app password for Key Vault, 130–131
 - Azure AD application, 125–127
 - Azure Key Vault, 127–130, 134–135
 - Azure Monitor add-on, 139
 - confirming accessible logs, 124
 - event hub and Azure Monitor, 131–132, 136–138
 - processes, 123
 - shared access key, 133–134
 - Splunk SIEM pipe, 124
 - VM (Virtual Machine), 138–139
- SQL Auditing & Threat Detection, 38
- SQL databases, threat detection, 66. *See also* Potential SQL Injection alert
- SQL Encryption, 38
- SSE (Storage Service Encryption), 14
- SSH brute-force attacks, 114
- storage
 - considering, 23
 - encryption, 66–67
- storage and data
 - encryption, 66–67
 - overview, 63–64
 - protection, 10
 - server auditing, 64–66
 - threat detection, 64–66
- Storage Encryption policy, 37.
 - See *also* encryption
- storage protection, 14
- streaming logs, 122
- suspicious process executed alert, 161
- System Updates policy, 36, 52

T

- target and attack, 109–110
- TDE (Transparent Data Encryption), 64
- Teller, Tomer, 74
- threat detection
 - anomaly detection, 106–108
 - atomic, 101–102
 - behavioral analytics, 104–105
 - methods, 101
 - vs. prevention, 64, 99–100
 - threat-intelligence feeds, 102–104
- threat intelligence
 - dashboard in Security Center, 157–159
 - hunting security issues, 159–162
 - integration, 20
 - overview, 153–155
 - reports in Security Center, 155–156
 - VA (Virtual Analyst), 163
- threats, 4–5
- TLS (Transport Layer Security), 10
- Trojans, 1, 4. *See also* attacks

V

- VA (Virtual Analyst), threat intelligence, 163
- VAs (vulnerability assessments), 36–37
- VHD (virtual hard disk), 63
- VM Agent Is Missing or Not Responding, 52
- VMBA (Virtual Machine Behavioral Analysis) alerts, 74
- VMs (Virtual Machines). *See also*
 - Just-in-Time VM access
 - Azure Portal, 12–13
 - cloud-weaponization, 7

- moving to workspaces, 165–167
- obtaining attributes, 167
- operations, 12
- Splunk enterprise, 138–139
- VMware virtualization solution, 12
- VNets (virtual networks), 12
- vulnerabilities, identifying and mitigating, 57, 71
- Vulnerability Assessment Not Installed, 52

W

- WAF (Web Application Firewall)
 - policy, 37
- web applications, 68–70
- websites
 - Activity Log for security
 - alerts, 78
 - agent installation, 29
 - application whitelisting, 114
 - ASC detection capabilities, 21
 - ASC pricing, 18
 - Azure AD Identity Protection, 149
 - Azure network security, 13
 - Azure Policy, 48

- Azure Storage security, 14
- CCE rules, 25, 58
- cloud threats, 7
- compliance, 9
- compute recommendations, 51
- computer security, 12
- cybercrime, 2
- Data Collection blade, 39
- Disk Encryption, 37
- endpoint protection, 53
- error codes, 173
- event hub for SIEM, 122
- IC3 (Internet Crime Complaint Center), 1
- IExpress self-extractor, 29
- Incident Playbook, 162
- Linux agents, 27
- Log Analytics, 83
- Log Analytics workspaces, 19
- Nitol botnet, 2
- Notepad++, 170
- OWASP documentation for cyberattacks, 68
- playbook integration with Slack, 97
- Privileged Access Workstations, 10

- RBAC (role-based access control), 23
- SDL (Security Development Lifecycle), 68
- security alerts, 75, 77
- Splunk integration solution, 139
- SQL database threat detection, 66
- threat intelligence map, 159
- VAs (vulnerability assessments), 36
- Welcome to Azure Policy blade, 46
- WER (Windows Error Reporting), 19. *See also* error codes
- whitelisting, 111–114
- WinZipper Trojan, 4
- workflows, creating for playbooks, 91–94
- workspaces
 - changing defaults, 166
 - computers and VMs, 165–167
 - creating, 19, 164–165
 - data retention, 23 and data storage, 19
 - ID and primary key, 29
 - monitoring, 141