

Microsoft Azure Sentinel

Planning and implementing Microsoft's cloud-native SIEM solution



Yuri Diogenes
Nicholas DiCola
Jonathan Trull

Foreword by Ann Johnson, Corporate Vice President – Cybersecurity Solutions at Microsoft

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Microsoft Azure Sentinel

Planning and implementing
Microsoft's cloud-native SIEM
solution

Yuri Diogenes
Nicholas DiCola
Jonathan Trull

Microsoft Azure Sentinel

Planning and implementing Microsoft's cloud-native SIEM solution

Published with the authorization of Microsoft Corporation by:

Pearson Education, Inc.

Copyright © 2020 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.pearson.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: 978-0-13-648545-2

ISBN-10: 0-13-648545-6

Library of Congress Control Number: 2019957613

ScoutAutomatedPrintCode

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 author(s), 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.

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

Brett Bartow

EXECUTIVE EDITOR

Loretta Yates

DEVELOPMENT EDITOR

Rick Kughen

MANAGING EDITOR

Sandra Schroeder

SENIOR PROJECT EDITOR

Tracey Croom

COPY EDITOR

Rick Kughen

INDEXER

Valerie Perry

PROOFREADER

Vanessa Ta

TECHNICAL EDITOR

Maarten Goet

ASSISTANT SPONSORING
EDITOR

Charvi Arora

EDITORIAL ASSISTANT

Cindy Teeters

COVER DESIGNER

Twist Creative, Seattle

COMPOSITOR

Happenstance Type-O-Rama

Acknowledgments

The authors would like to thank Loretta Yates and the entire Microsoft Press/Pearson team for their support in this project, Ann Johnson for writing the foreword, and also the Azure Sentinel Engineering Team (Eliav Levi, Ofer Shezaf, Koby Koren, Raz Herzberg, Mor Shabi, Laura Machado de Wright, Ben Nick, Julian Gonzalez, and Itay Argoety). Thanks to Ian Hellen for the great work writing Chapter 6. We would also like to thank Maarten Goet (Microsoft MVP) for reviewing this book and thanks to Mike Kassis for writing the Appendix about Kusto Query Language (KQL).

Yuri would also like to thank: my wife and daughters for their endless support; my great God for giving me strength and guiding my path on each step of the way; my co-authors and friends Nicholas DiCola and Jonathan Trull for such great partnership throughout this project. 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. Last, but certainly not least, the entire Azure Sentinel community that keep inspiring us with great content.

Nicholas would also like to thank: my wife and three children for supporting me while working on this book; my co-authors and friends Yuri Diogenes and Jonathan Trull for their hard work on this book. I would also like to thank our Azure Sentinel Engineering team technical reviewers for their support on the book.

Jonathan would also like to thank: God, who is my ultimate teacher and guide; my wife and daughters for their love, encouragement, and endless support; my parents for providing me with the time and resources to pursue my dreams; my extended family for always believing in me; and my co-authors and comrades Yuri Diogenes and Nicholas DiCola. Finally, thanks to Microsoft, the Cybersecurity Solutions Group, and the countless teachers, professors, colleagues, and friends who have taught, counseled, and mentored me over the years.

Contents at a Glance

	<i>Foreword</i>	<i>xii</i>
	<i>Introduction</i>	<i>xv</i>
1	Security challenges for SecOps	1
2	Introduction to Azure Sentinel	13
3	Analytics	33
4	Incident management	51
5	Threat hunting	63
6	Jupyter Notebooks	79
7	Automation with Playbooks	109
8	Data visualization	131
9	Integrating with partners	145
A	Introduction to Kusto Query Language	163
	<i>Index</i>	<i>179</i>

Contents

	<i>Foreword</i>	<i>xiii</i>
	<i>Introduction</i>	<i>xv</i>
Chapter 1	Security challenges for SecOps	1
	Current threat landscape.....	1
	Microsoft Security Intelligence Report	3
	Security challenges for SecOps.....	5
	Resource challenges	7
	Security data challenges	7
	Threat intelligence.....	8
	Cloud-native SIEM.....	11
	Core capabilities	12
Chapter 2	Introduction to Azure Sentinel	13
	Architecture.....	13
	Adoption considerations.....	15
	Enabling Azure Sentinel.....	16
	Data ingestion.....	19
	Ingesting data from Microsoft solutions	21
	Accessing ingested data.....	29
Chapter 3	Analytics	33
	Why use analytics for security?.....	33
	Understanding analytic rules.....	34
	Configuring analytic rules	38
	Types of analytic rules	44
	Creating analytic rules.....	45
	Validating analytic rules.....	49

Chapter 4	Incident management	51
	Introduction to incident management	51
	Security incident in Azure Sentinel	52
	Managing an incident	54
	Investigating an incident	56
	Investigation graph	57
Chapter 5	Threat hunting	63
	Introduction to threat hunting	63
	Hunting threats in Azure Sentinel	64
	Creating new hunting queries and bookmarks	73
Chapter 6	Jupyter Notebooks	79
	Introduction	79
	Why use Jupyter Notebooks?	80
	A word on Python	82
	Different audiences for Jupyter Notebooks	83
	Jupyter environments	83
	Azure Notebooks and Azure Sentinel	84
	Connecting to Azure Sentinel	87
	Using Kqlmagic to query Azure Sentinel data	87
	Notebooks for hunting and investigation	94
	Using Microsoft Threat Intelligence Center toolset	95
	Querying data: The msticpy query library	95
	Event timelines	99
	Looking for suspicious signs in your data	101
	Finding outliers with clustering	103
	Link and display related data sets	105
	Geomapping IP addresses	106
	Summary	107
Chapter 7	Automation with Playbooks	109
	The Importance of SOAR	109
	Real-time automation	110
	Post-incident automation	125

Chapter 8	Data visualization	131
	Azure Sentinel Workbooks	131
	Using built-in Workbooks	133
	Creating custom Workbooks	138
	Creating visualizations in PowerBI and Excel	140
	Creating visualizations in Power BI	141
	Exporting data to Microsoft Excel	143
Chapter 9	Integrating with partners	145
	Connecting with Fortinet	145
	Validating connectivity	148
	Connecting with Amazon Web Services (AWS)	151
	Validating connectivity	156
	Connecting with Palo Alto	158
	Validating connectivity	161
Appendix A	Introduction to Kusto Query Language	163
	The KQL query structure	163
	Data types	166
	Getting, limiting, sorting, and filtering data	167
	Summarizing data	170
	Adding and removing columns	172
	Joining tables	173
	Evaluate	175
	Let statements	176
	Suggested learning resources	177
	<i>Index</i>	179

About the Authors

Yuri Diogenes, MsC

Master of science in cybersecurity intelligence and forensics investigation (UTICA College), Yuri is Senior Program Manager in Microsoft Cxe Security Team, where he primarily helps customers onboard and deploy Azure Security Center and Azure Sentinel. 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 22 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*.

Nicholas DiCola

Nicholas is a Principal Group PM Manager at Microsoft on the Security Customer Experience Engineering (CxE) team, where he leads the Azure Security Get-To-Production team that helps customers with deployments of Azure Security products. He has a Master of Business Administration with a concentration in Information Systems and various industry certifications such as CISSP and CEH. You can follow Nicholas on Twitter at *@mastersejedi*.

Jonathan Trull

Jonathan is Microsoft's Chief Security Strategist. He provides strategic direction on the development of Microsoft products and services and leads a team of security, compliance, and identity advisors who help customers secure their digital transformation initiatives. Jonathan is a seasoned security executive who formally served as the CISO for the State of Colorado and several commercial organizations. He is active in the security community and is helping lead the Cloud Security Alliance's cloud controls matrix working group and is a coach for Carnegie Mellon University's CISO Executive Program. You can follow Jonathan on Twitter at *@jonathantrull* or via LinkedIn at <https://www.linkedin.com/in/jonathantrull/>.

Foreword

Security is—at its' core—a big data problem. Businesses and government entities are producing terabytes of security relevant log data every day and the volumes continue to increase. This data growth is driven by the digitization of business processes and an explosion in the number of intelligent devices being used to power our physical world. Security teams are charged with making sense of this data and spotting the signs of an active attack so that they can respond appropriately.

Azure Sentinel was purpose-built to help address the challenges faced by our customer's security operations teams. It was engineered as a cloud service to automatically scale to the data volumes thrown at it. This allows security teams to focus their time on identifying threats as opposed to administering infrastructure. Azure Sentinel also includes capabilities to automate responses to alerts by triggering playbooks. Playbooks can also collect and add context to existing alerts to speed decision making by SOC analysts.

Yuri, Nicholas, and Jonathan have been working with Azure Sentinel from the beginning of the design and engineering process and have successfully deployed Azure Sentinel for customers large and small. They lay out the foundational aspects of architecting and implementing Azure Sentinel, including connecting data sources; writing custom alerts, workbooks, and playbooks; and using the product to proactively hunt for threats. The authors not only cover the full breadth of product capabilities in the book, but they also offer their practical advice to ensure successful deployment.

Microsoft is fulfilling a mission to develop a robust portfolio of security, compliance, and identity products to meet the needs of our enterprise customers. The security, compliance, and identity solutions are fully integrated and leverage Microsoft's vast threat-intelligence sources to maximize their effectiveness. Azure Sentinel will be a cornerstone of the Microsoft portfolio for years to come and has already been quickly adopted across the globe by customers of all sizes.

Microsoft Azure Sentinel is the authoritative source for implementing Microsoft's hottest new security solution. It was a pleasure to review for Yuri, Nicholas, and Jonathan. Pick up your copy today!

Ann Johnson
Corporate Vice President
Cybersecurity Solutions Group

Introduction

Welcome to Azure Sentinel. This book was developed together with the Azure Sentinel product group to provide in-depth information about Microsoft's new cloud-based security information and event management (SIEM) system, Azure Sentinel, 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 capabilities available in Azure Sentinel. After being introduced to the main use case scenarios to use Azure Sentinel, you will dig in to see how to deploy and operationalize Azure Sentinel for data collection, analytics, incident management, threat detection, and response.

Who is this book for?

Azure Sentinel is for anyone interested in security operations in general: cybersecurity analysts, security administrators, threat hunters, support professionals, and engineers.

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

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 Sentinel and how to get the most out of it by showing in a stepwise, guided fashion how to configure Azure Sentinel to gain all the benefits it has to offer.

In this book you will learn:

- How to connect different data sources to Azure Sentinel
- How to create security analytics
- How to investigate a security incident in Azure Sentinel
- 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:

MicrosoftPressStore.com/AzureSentinel/errata

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

For additional book support and information, please visit
<http://www.MicrosoftPressStore.com/Support>.

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>*.

Introduction to Azure Sentinel

Given the threat landscape presented in Chapter 1, there is a clear need for a system that can collect data from different sources, perform data correlation, and present this data in a single dashboard.

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Azure Sentinel natively incorporates proven foundation services from Azure, such as Log Analytics and Logic Apps. Also, Azure Sentinel enriches your investigation and detection with Artificial Intelligence (AI) in conjunction with Microsoft's threat intelligence stream.

In this chapter, you will learn more about the architecture, design considerations, and initial configuration of Azure Sentinel.

Architecture

Because Azure Sentinel is part of Azure, the first prerequisite to deployment is to have an active Azure subscription. As with any other security information and event management (SIEM), Azure Sentinel needs to store the data that it will collect from the different data sources that you configure. Azure Sentinel will store this data in your preferred Log Analytics workspace. You can create a new workspace or use an existing one. However, it is recommended that you have a dedicated workspace for Azure Sentinel because alert rules and investigations do not work across workspaces. Keep in mind that you need at least contributor permission for the subscription in which the workspace resides.

TIP All the data you stream to Azure Sentinel is stored in the geographic location of the workspace you selected.

To help you to better understand Azure Sentinel's architecture, you need to first understand the different components of the solution. Figure 2-1 shows a diagram of the major Azure Sentinel components.

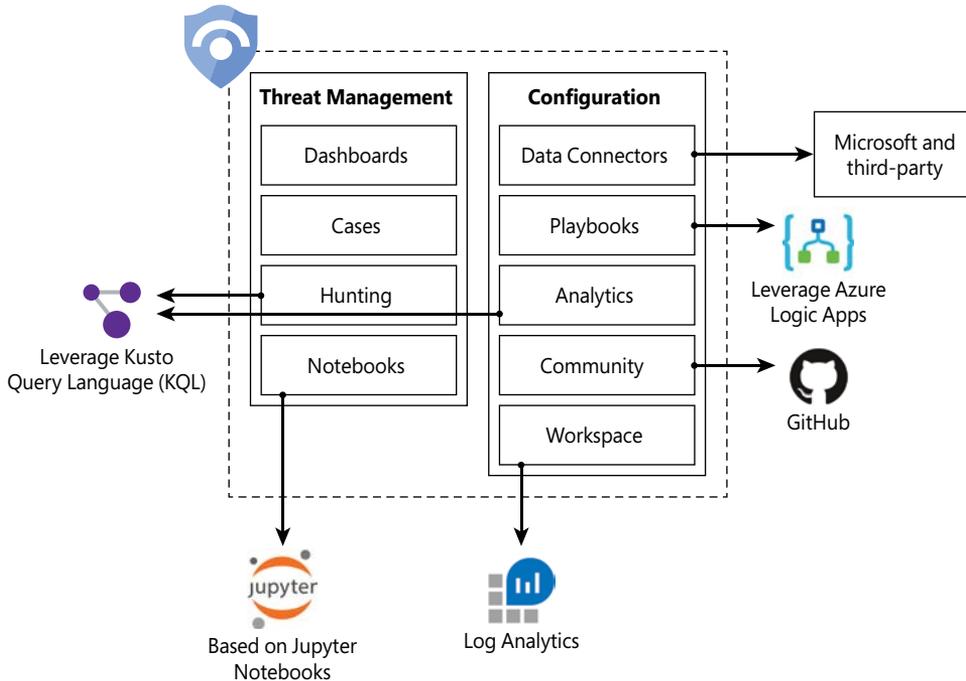


FIGURE 2-1 Major components of Azure Sentinel

The components shown in Figure 2-1 are presented in more detail below:

- **Dashboards:** Built-in dashboards provide data visualization for your connected data sources, which enables you to deep dive into the events generated by those services. You will learn more about dashboards in Chapter 8, “Data visualization.”
- **Cases:** A case is an aggregation of all the relevant evidence for a specific investigation. It can contain one or multiple alerts, which are based on the analytics that you define. You will learn more about cases in Chapter 4, “Case management.”
- **Hunting:** This is a powerful tool for investigators and security analysts who need to proactively look for security threats. The searching capability is powered by Kusto Query Language (KQL). You will learn more about hunting in Chapter 5, “Hunting.”
- **Notebooks:** By integrating with Jupyter notebooks, Azure Sentinel extends the scope of what you can do with the data that was collected. The notebooks feature combines full programmability with a collection of libraries for machine learning, visualization, and data analysis. You will learn more about notebooks in Chapter 6, “Notebooks.”
- **Data Connectors:** Built-in connectors are available to facilitate data ingestion from Microsoft and partner solutions. You will learn more data connectors later in this chapter.
- **Playbooks:** A Playbook is a collection of procedures that can be automatically executed upon an alert triggered by Azure Sentinel. Playbooks leverage Azure Logic Apps, which help you automate and orchestrate tasks/workflows. You will learn more about playbooks in Chapter 7, Automation with Playbooks.”

- **Analytics:** Analytics enable you to create custom alerts using Kusto Query Language (KQL). You will learn more about analytics in Chapter 3, “Analytics.”
- **Community:** The Azure Sentinel Community page is located on GitHub, and it contains Detections based on different types of data sources that you can leverage in order to create alerts and respond to threats in your environment. The Azure Sentinel Community page also contains hunting query samples, playbooks, and other artifacts. You will learn more about community in Chapter 3, “Analytics.”
- **Workspace:** Essentially, a Log Analytics workspace is a container that includes data and configuration information. Azure Sentinel uses this container to store the data that you collect from the different data sources. You will learn more about workspace configuration later in this chapter.

Adoption considerations

Although Azure Sentinel is a cloud-based SIEM, there are some initial design considerations that you must be aware of. When planning Azure Sentinel adoption, use the following list of questions as the foundation for your initial assessment. This will help you to identify the areas from which you need to obtain more details before deploying Azure Sentinel:

1. Who has permission to deploy Azure Sentinel in my tenant?

- Azure Sentinel uses a Role-Based Access Control model and enables you to set granular levels of permissions for different needs. There are three built-in roles available for Azure Sentinel, they are:
 - Azure Sentinel reader: enable the user to view incidents and data but cannot make changes.
 - Azure Sentinel responder: enable the user to read and perform some actions on incidents, such as assign to another user or change the incident’s severity.
 - Azure Sentinel contributor: enable the user to read, perform some actions on incidents and create or delete analytic rules.

To deploy Azure Sentinel on your tenant you need contributor permissions to the subscription in which the Azure Sentinel workspace resides.

Note: All Azure Sentinel built-in roles grant read access to the data in your Azure Sentinel workspace.

2. What permissions do the team members require to do their jobs using Azure Sentinel?

- It is important to plan who will have access to the Azure Sentinel Dashboard. Depending on how the organization is structured, you may have different teams handling different areas of Azure Sentinel. For example, the SecOps team might be actively looking at new alerts, while the Threat Hunting Team might be performing proactive hunting. Again, leverage the RBAC model to assign granular permissions to different groups.
- Consider the different scenarios, such as creating cases, closing cases, creating new analytics, using hunting queries, and writing playbooks.

3. Am I going to deploy Azure Sentinel in a single or multitenant scenario?

- Azure Sentinel can be deployed in both scenarios. In a multitenant scenario, you can deploy Azure Sentinel on each tenant and use Azure Lighthouse to have a multitenant visualization of all tenants.

4. What are the data sources from which I want to ingest data?

- That's probably one of the most critical questions to ask in the beginning of the project. By having a list of data sources that you want to connect to Azure Sentinel, you can evaluate whether there are built-in connectors for the target system or whether you will need to use another method to connect. Here, you should also define whether you are going to ingest data only from cloud resources or if you also plan to collect data from on-premises resources.
- Make sure to prioritize the data sources that are more important for your business. If you are just performing a proof-of-concept, ensure that you connect to the primary Microsoft services that are used by your organization and at least a couple of on-premises resources that will be utilized in production.

5. Do I already have Azure Security Center deployed and monitoring my servers?

- If you already have Azure Security Center deployed and you are using the default workspace created by Security Center, you need to be aware that you can't enable Azure Sentinel on this default workspace. However, if you are using a custom workspace in Azure Security Center, you can enable Azure Sentinel on this workspace. You will find more details about workspace design in "Enabling Azure Sentinel," later in this chapter.

These are key questions that you must answer before you start configuring Azure Sentinel. Once you answer these questions—and others that may be very specific to your type of organization—you are ready to enable Azure Sentinel in your Azure subscription.

Enabling Azure Sentinel

Azure Sentinel is available in Azure Portal, and to enable it, you need a Log Analytics workspace. A Log Analytics workspace provides:

- A geographic location for data storage.
- Data isolation by granting different users access rights following the Log Analytics' recommended design strategies for workspaces; these recommendations can be found at <http://aka.ms/asbook/workspacedesign>.
- A scope for configuration of settings, such as pricing tier, retention, and data capping.

Although Azure Sentinel supports multiple workspaces for some scenarios, it is recommended that you use a centralized workspace because alert rules and investigations do not function across workspaces.

NOTE To learn more about workspace design consideration and Role-Based Access Control (RBAC) for workspaces, visit <http://aka.ms/asbook/workspaces> and <http://aka.ms/asbook/workspacesbp>.

The following steps assume that you don't have a workspace and that you will create one as part of the Azure Sentinel deployment:

6. Open **Azure Portal** and sign in with a user who has contributor privileges in the subscription in which the Azure Sentinel workspace resides.
7. Under **All services**, type *Sentinel* and click **Azure Sentinel**, as shown in Figure 2-2.

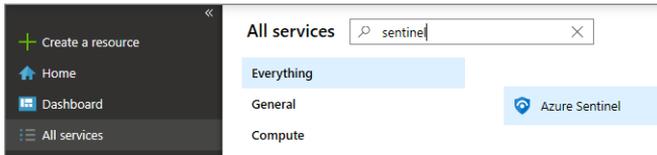


FIGURE 2-2 Accessing Azure Sentinel in Azure Portal

8. When Azure Sentinel launches for the first time, there is no workspace associated to it; the initial blade will look similar to Figure 2-3.

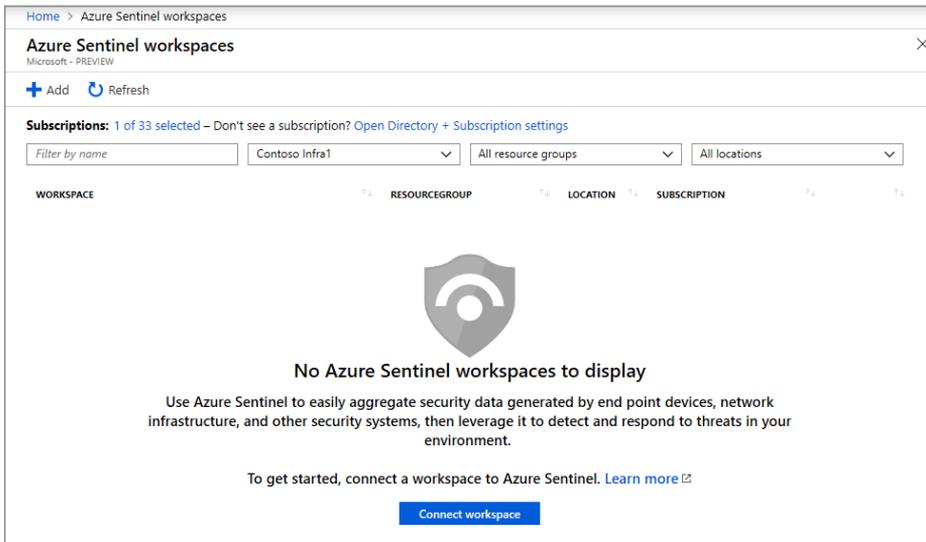


FIGURE 2-3 Azure Sentinel workspace selection page

9. At this point, you can either click the **Add** button or click the **Connect Workspace** button. Both options will lead you to the **Choose a workspace to add to azure sentinel** page, as shown in Figure 2-4.

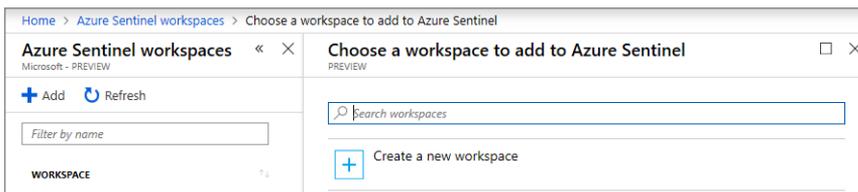


FIGURE 2-4 Adding a new workspace to Azure Sentinel

10. Click the **Create a new workspace** option; the **Log analytics workspace** page appears, as shown in Figure 2-5.

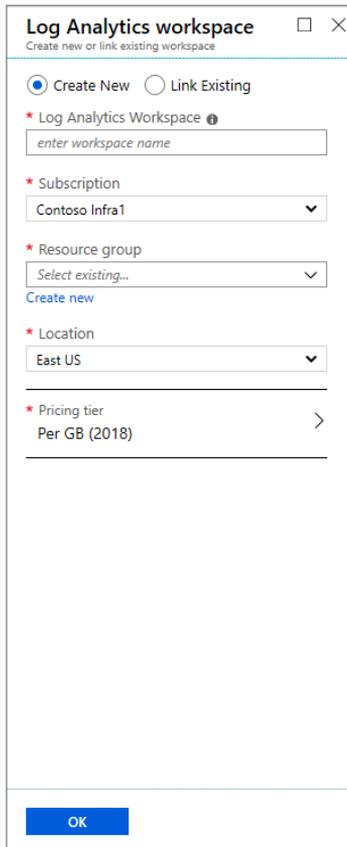


FIGURE 2-5 Creating a new workspace to be used by Azure Sentinel

11. In the **Log Analytics Workspace** field, type a name for the workspace.
12. In the **Subscription** field, select the subscription that you want to use.
13. From the **Resource group** drop-down menu, select the resource group you want to use.
14. From the **Location** drop-down menu, select the location where the workspace will reside.
15. For the **Pricing tier**, select **Per GB**.
16. After completing those fields, click the **OK** button.
17. On the **Choose a workspace to add to Azure Sentinel** page, select the workspace that you just created and click the **Add Azure Sentinel** button; the initial **Azure Sentinel** dashboard appears, as shown in Figure 2-6.

Now that you have your workspace configured, you are ready to start ingesting data from different sources. We'll cover that in the next section.

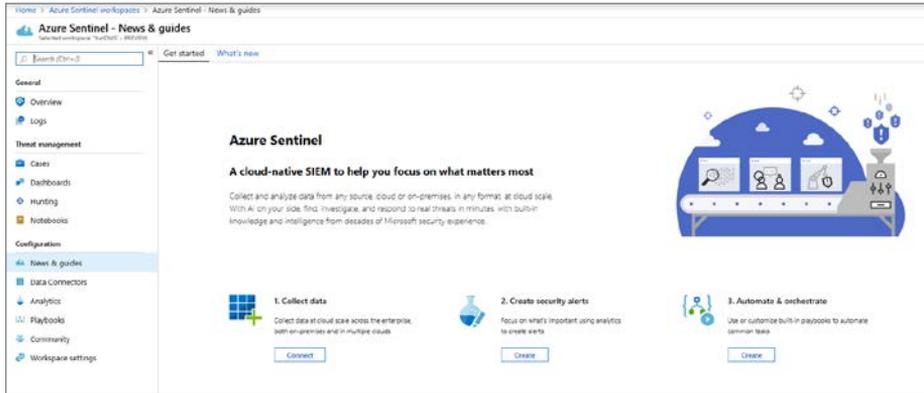


FIGURE 2-6 Initial Azure Sentinel page

Data ingestion

Azure Sentinel enables you to use data connectors to configure connections with different Microsoft services, partner solutions, and other resources. There are several out-of-the-box data connectors available in Azure Sentinel, and there are different ways to ingest data when a connector is not available. Figure 2-7 shows a diagram of the available options.

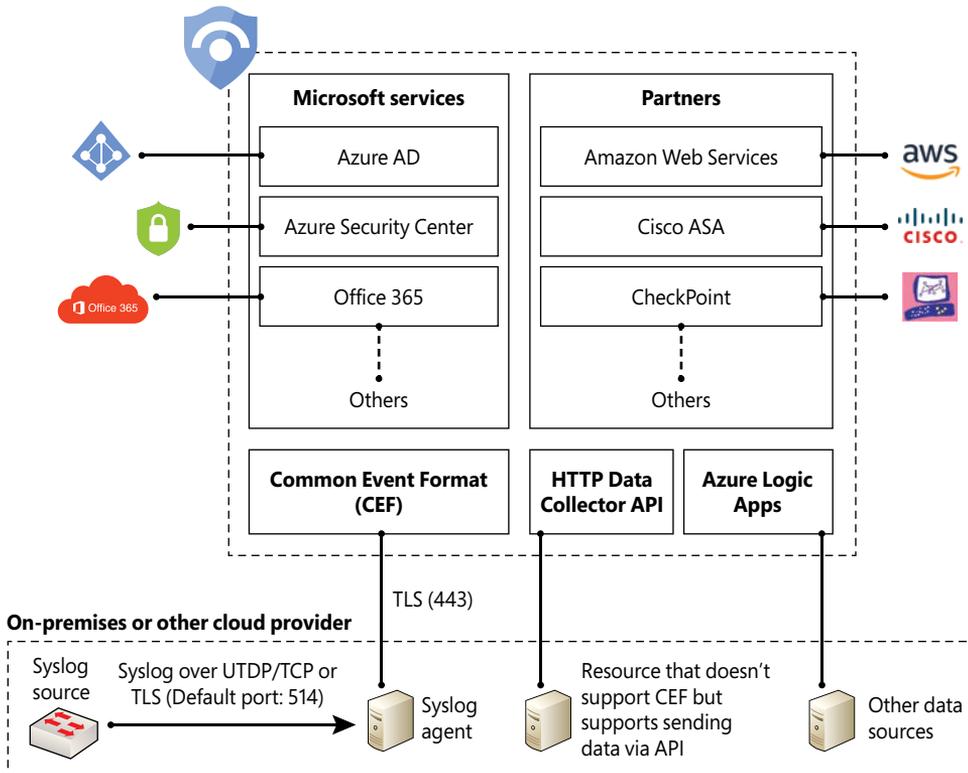


FIGURE 2-7 Different methods to ingest data into Azure Sentinel

Figure 2-7 only shows a small subset of Microsoft services. At the time this chapter was written, Azure Sentinel provided support for the following Microsoft services:

- Azure AD
- Office 365
- Cloud App Security
- Azure Activity Log
- Azure AD Identity Protection
- Azure Information Protection
- Azure ATP
- Azure Security Center
- Domain Name Server
- Microsoft Defender ATP
- Microsoft Web Application Firewall
- Windows Firewall
- Windows Security Events

The diagram also shows a subset of partners' connectors. The number of connectors may change over time as Microsoft continues to encourage other vendors to partner and create new connectors. At the time this chapter was written, the following external connectors were available:

- Amazon Web Services (AWS)
- Barracuda
- Check Point
- Palo Alto Networks
- Fortinet
- F5
- Symantec ICDX

If an external solution is not on the data connector list, but your appliance supports saving logs as Syslog Common Event Format (CEF), the integration with Azure Sentinel is available via CEF Connector. If CEF support is not available on your appliance, but it supports calls to a REST API, you can use the HTTP Data Collector API to send log data to the workspace on which Azure Sentinel is enabled. Data ingestion from some of these connectors requires a license, while some others are free. To see an updated pricing list for the connectors, visit <http://aka.ms/asbook/dataconnectors>.

TIP To learn how to use the HTTP Data Collector API to send log data to a workspace from a REST API client, visit <http://aka.ms/asbook/datacollectorapi>.

Utilize a cloud-native SIEM to reduce integration costs and free up resources

Ease of integration with telemetry sources is key to SIEM success. I often encounter security operations teams that spend too much effort on connecting data sources and maintaining event flow, which reduces the time they spend delivering security value. The cloud environment enables Azure Sentinel to offer a resilient and straightforward way to connect to data sources; this is done by abstracting servers and networks and by offering service-based serverless computing.

For example, with just a few clicks, you can connect Sentinel to Office 365, Azure AD, or Azure WAF and start receiving events immediately and get populated dashboards in minutes. Now that you are connected, there is no need to worry about connectivity health. No collector machine can fail or be choked with an event spike.

If an Office 365 customer is struggling with the implementation of detection use cases to address auditor concerns, they will find that a month-long project using a legacy SIEM can be implemented in less than a day by onboarding Azure Sentinel, connecting it to Office 365, and implementing the required use cases.

You may think that this is true only for collecting from Microsoft sources; however, Azure Sentinel AWS CloudTrail connector, which is based on serverless cloud-to-cloud connection, provides the same benefits. Connect in a few clicks and never worry about a failing VM or event spike.

Collecting from on-premises systems tends to require legacy collection methods such as Syslog. However, vendors such as F5, Symantec, and Barracuda offer native integration of their systems to Azure Sentinel providing the cloud-native collection benefits to on-premises equipment.

Ofer Shezaf, Principal Program Manager, Azure Sentinel Team

Ingesting data from Microsoft solutions

One way to quickly start validating Azure Sentinel's data ingestion is to start the configuration by using Microsoft built-in connectors. To visualize data from the subscription-level events that have occurred in Azure—which includes data ranging from Azure Resource Manager (ARM)

operational data to updates on service health events—you can start with Azure Activity Log. Follow the steps below to connect with Azure Activity Log:

1. Open **Azure Portal** and sign in with a user who has contributor privileges for the workspace on which Azure Sentinel will be enabled and the resource group.
2. Under the **All services** option, type *Sentinel* and click **Azure Sentinel** when it appears at the lower right, as shown in Figure 2-8.

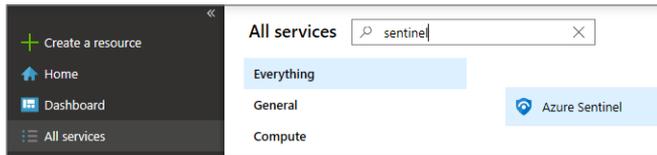


FIGURE 2-8 Accessing Azure Sentinel in Azure Portal

3. Click in the workspace that was created in the “Enabling Azure Sentinel” section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. From the list of connectors, click **AzureActivity**; the **AzureActivity** page will appear, as shown in Figure 2-9.

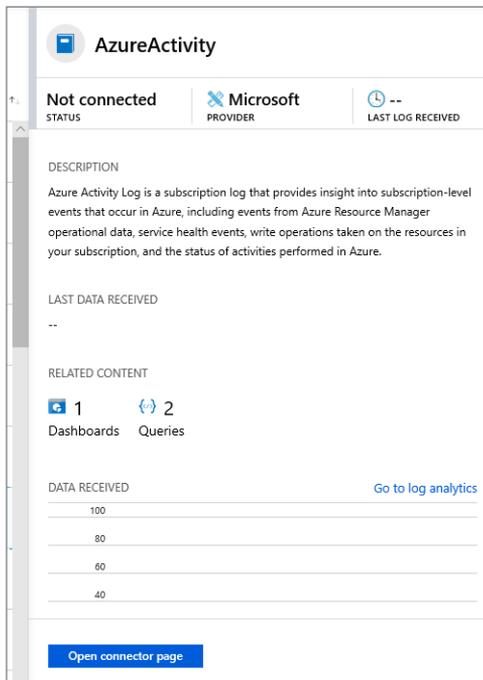


FIGURE 2-9 Azure Activity Log connector blade

6. Click the **Open Connector Page** button, and you will see the **Instructions** tab, as shown in Figure 2-10.

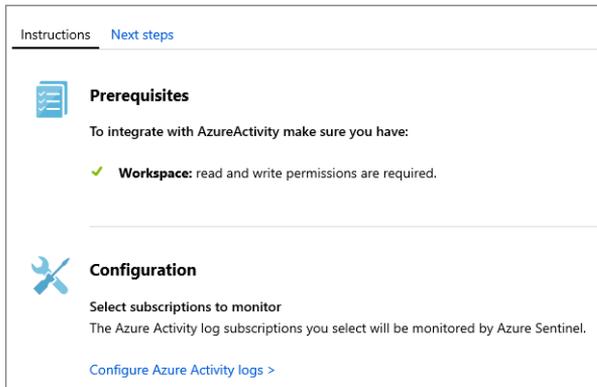


FIGURE 2-10 Instructions tab with more details about prerequisites and configuration

7. Click the **Configure Azure Activity logs** option, and the Azure Activity Log page appears. Click the subscription to which you want to connect and click the **Connect** button.
8. Wait until you see a notification indicating the subscription was successfully connected and click the **Refresh** button. Ensure that the status has changed to Connected and close each blade until you see the main **Data Connectors** page.
9. Click **Overview** under **General** in the left navigation pane.
10. On the **Overview** page, you will see that there is no activity yet; this is expected because you just initiated the ingestion of Azure Activity Logs. Now you will generate some activity, and at the end of this chapter, you will check how the data flowed to Azure Sentinel. Create a new Virtual Machine with the following specifications:
 - **Operating System:** Windows Server 2016.
 - **Resource Group:** Use the same resource group that you created for the workspace in the “Enabling Azure Sentinel” section, earlier in this chapter.
 - **Remote Desktop Connection:** Enabled.

Connecting to Azure Security Center

If you have Azure Security Center enabled in your subscription, you can start ingesting the Security Alerts generated by Security Center, which provides a rich set of threat detections. Security Center will generate alerts according to the different resource types:

- Infrastructure as a Service (IaaS), Virtual Machines (VMs), and non-Azure servers
- Native compute
- Data services

You need the Azure Security Center standard tier in order to connect with Azure Sentinel. Follow the steps below to connect to Security Center and start streaming security alerts to Azure Sentinel:

1. Open **Azure Portal** and sign in with a user who has contributor privileges for the workspace on which Azure Sentinel will be enabled as well as the resource group.
2. Under the **All services** option, type *Sentinel*, and click **Azure Sentinel**, as shown in Figure 2-11.

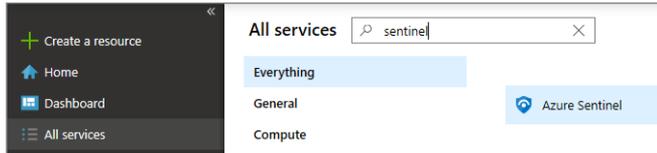


FIGURE 2-11 Accessing Azure Sentinel in Azure Portal

3. Click in the workspace that was created in the “Enabling Azure Sentinel” section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. Click **Azure Security Center**, and a new pane appears on the right side, as shown in Figure 2-12.

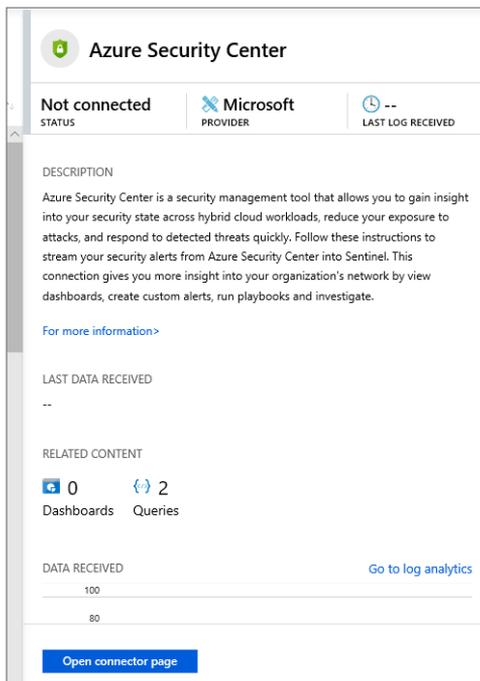


FIGURE 2-12 Azure Security Center connector

6. Click **Open Connector Page** button and the full Azure Security Center connector page appears, as shown in Figure 2-13.

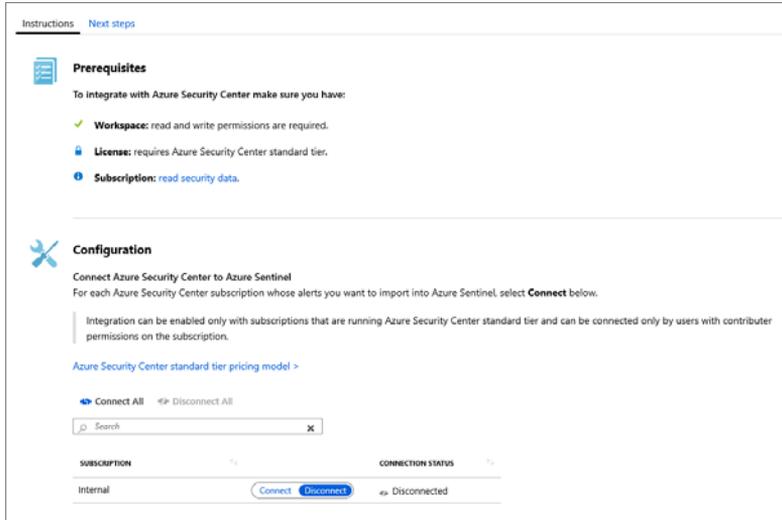


FIGURE 2-13 Azure Security Center connector page

7. Under the **Configuration** section, next to the subscription that has the Azure Security Center standard tier enabled, click **Connect**.
8. The **Connection Status** will temporarily appear as Connecting, and once it is finished, it will appear as Connected.
9. After confirming that it is connected, close the Azure Security Center page, and on the **Data Connectors** page, click **Refresh**; you will see that the Azure Security Center connector status appears as Connected, as shown in Figure 2-14.



FIGURE 2-14 Azure Security Center connector fully connected

10. Click the **Overview** option in the left pane to return to the main dashboard.

TIP If you want to generate some alerts in Azure Security Center, you can use the set of instructions available in the Security Center playbooks at <http://aka.ms/ascpaybooks>.

Connecting to Azure Active Directory

Azure Active Directory (Azure AD) is the identity and access-management service in the cloud. Each Azure tenant has a dedicated and trusted Azure AD directory. The Azure AD directory includes the tenant's users, groups, and apps, and it is used to perform identity and access-

management functions for tenant resources. If you want to export sign-in data from Active Directory to Azure Sentinel, you must have an Azure AD P1 or P2 license.

To connect Azure Sentinel with Azure AD, follow these steps:

1. Open **Azure Portal** and sign in with a user who has global administrator or security administrator permissions. You also need to have read permission to access Azure AD diagnostic logs if you want to see connection status.
2. Choose the **All services** option, type *Sentinel* in the search box, and click **Azure Sentinel**, as shown in Figure 2-15.

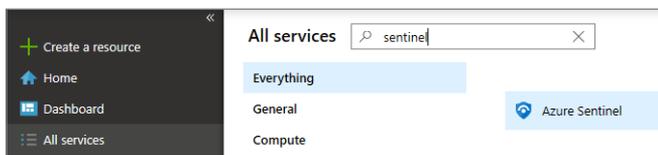


FIGURE 2-15 Accessing Azure Sentinel in Azure Portal

3. Click the workspace that was created in the “*Enabling Azure Sentinel*” section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. Click **Azure Active Directory**, and a new pane appears on the right side, as shown in Figure 2-16.

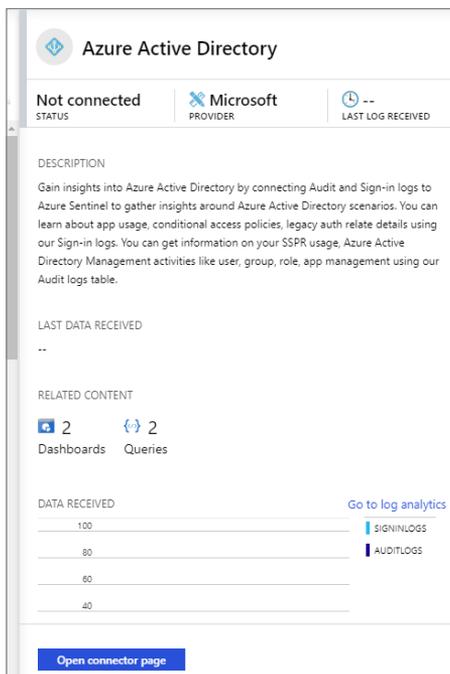


FIGURE 2-16 Azure Active Directory connector

6. Click **Open Connector Page** button, and the full Azure Active Directory connector page appears, as shown in Figure 2-17.

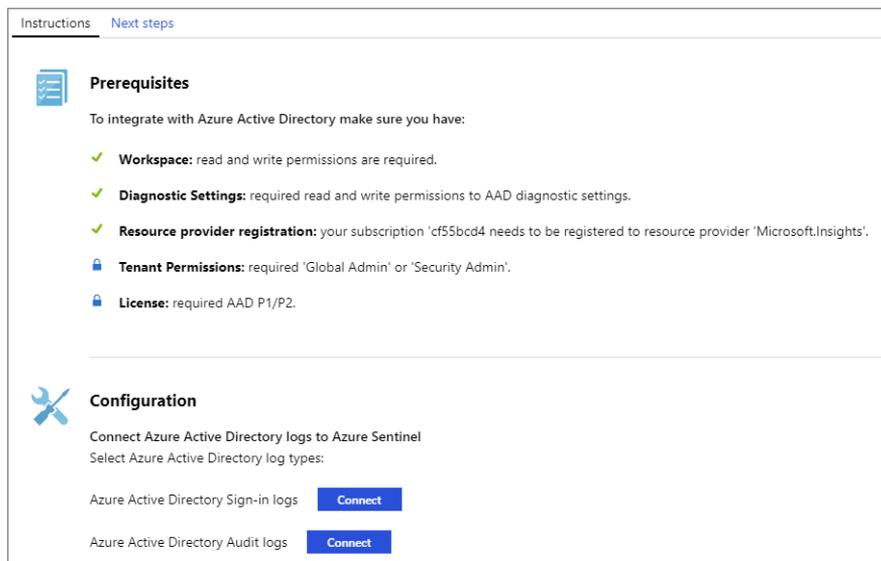


FIGURE 2-17 Azure Active Directory connector page

7. In the **Configuration** section, you have the option to connect to Azure AD sign-in logs and audit logs. Ideally, you should connect with both because it provides a broader visibility of your identity related activities. For this example, click both **Connect** buttons.
8. Once you finish connecting, both buttons will change to **Disconnect**.
9. Close this page and click the **Overview** option in the left pane to return to the main dashboard.

Connecting to Azure Active Directory Identity Protection

Azure Active Directory Identity Protection helps to protect your organization's identities by enabling you to configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached. To perform the integration of Azure Active Directory Identity Protection with Azure Sentinel, you must have an Azure Active Directory Premium P1 or P2 license.

To connect Azure Sentinel with Azure Active Directory Identity Protection, follow these steps:

1. Open **Azure Portal** and sign in with a user who has global administrator or security administrator permissions.

2. In the **All services** text box, type *Sentinel*, and click **Azure Sentinel** when it appears as the lower right, as shown in Figure 2-18.

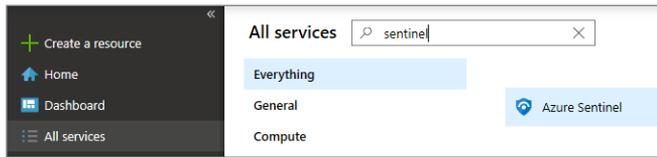


FIGURE 2-18 Accessing Azure Sentinel in Azure Portal

3. Click the workspace that was created in the *"Enabling Azure Sentinel"* section, earlier in this chapter.
4. When the **Azure Sentinel** dashboard opens, click **Data Connectors** under **Configuration** in the left navigation pane.
5. Click **Azure Active Directory Identity Protection**, and a new pane appears on the right side, as shown in Figure 2-19.

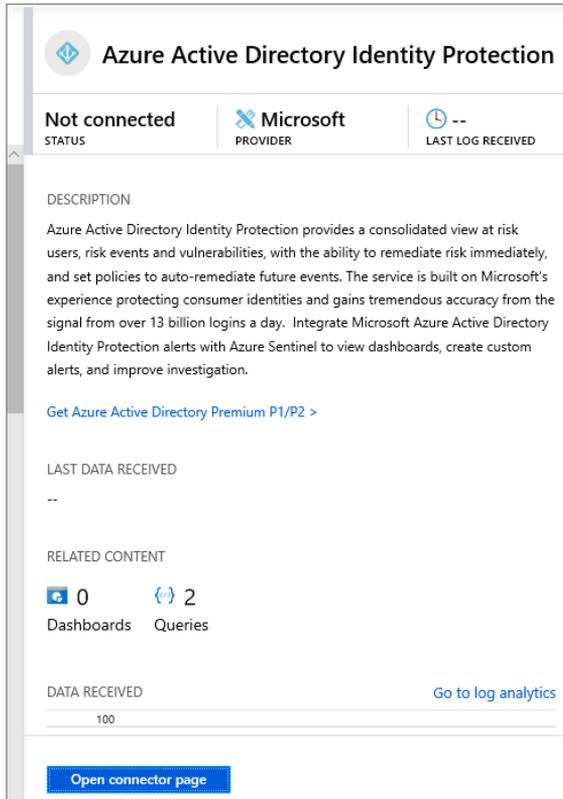


FIGURE 2-19 Azure Active Directory Identity Protection connector

6. Click the **Open Connector Page** button and the full Azure Active Directory Identity Protection connector page appears, as shown in Figure 2-20.

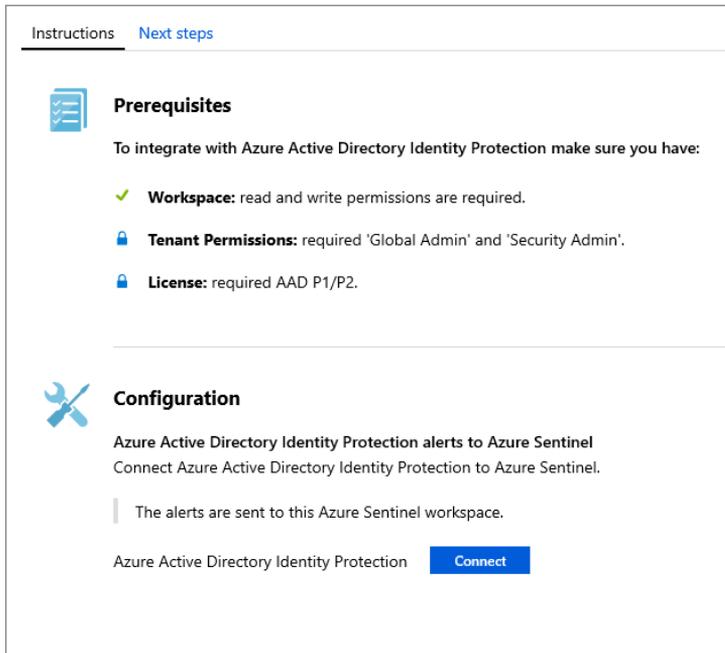


FIGURE 2-20 Azure Active Directory Identity Protection connector

7. Under **Configuration**, click the **Connect** button.
8. Once you finish connecting, the button will change to **Disconnect**.
9. Close this page and click the **Overview** option in the left pane to return to the main dashboard.

There are many more connectors for other Microsoft Solutions, and most of them follow the same flow as the solutions explained so far. The only thing you need to be aware of are the prerequisites for each solution. Make sure to visit the product's webpage to better understand what permissions are necessary to connect to the target data set. In Chapter 9, "Integrating with partners," you will learn how to connect with some partners' solutions.

Accessing ingested data

After connecting with the data sources that you need, you can start validating the connection flow to ensure the data is being saved in the workspace. To perform this validation, you need to access the workspace from Azure Sentinel and perform some queries using Kusto Query Language (KQL).

A Kusto query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read, author, and automate. The query uses schema entities that are organized in a hierarchy similar to SQL's databases, tables, and columns.

Follow these steps to access the workspace from Azure Sentinel and perform the validation for Azure Activity Log, which was the first data source that you connected in this chapter:

1. Open **Azure Portal** and sign in with a user who has contributor privileges for the workspace in which Azure Sentinel will be enabled as well as contributor privileges for the resource group.
2. Select the **All services** option, type *Sentinel*, and click **Azure Sentinel**, as shown in Figure 2-21.

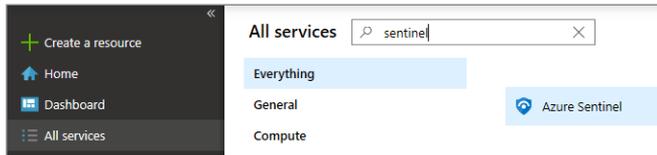


FIGURE 2-21 Accessing Azure Sentinel in Azure Portal

3. Click in the workspace that was created in the “*Enabling Azure Sentinel*” section, earlier in this chapter, and the **Azure Sentinel** main dashboard appears.
4. Under **General**, click **Logs**.
5. On the Logs page, type *AzureActivity* and click the **Run** button. You should see all activities that were performed and collected in the last 24 hours (which is the default time-frame). The result should look similar to Figure 2-22.

TimeGenerated [UTC]	OperationName	OperationNameValue	Level	ActivityStatus	ActivityStatus
> 2019-08-12T01:20:09.836	Microsoft.Authorization/policies/audit/action	Microsoft.Authorization/policies/audit/action	Warning	Succeeded	Succeeded
> 2019-08-12T01:20:09.995	Microsoft.Authorization/policies/audit/action	Microsoft.Authorization/policies/audit/action	Warning	Succeeded	Succeeded
> 2019-08-12T01:20:10.360	Microsoft.Authorization/policies/audit/action	Microsoft.Authorization/policies/audit/action	Warning	Succeeded	Succeeded
> 2019-08-12T01:20:11.350	Microsoft.Authorization/policies/audit/action	Microsoft.Authorization/policies/audit/action	Warning	Succeeded	Succeeded

FIGURE 2-22 Azure Sentinel workspace results

As you can see, the logs are flowing, and you can obtain all results with a single query. However, in a real scenario, you want to narrow the results. An easy way to learn KQL while performing queries is to leverage the context-sensitive IntelliSense capability. To do that, write the query and IntelliSense will open a drop-down menu showing the available options, as shown in Figure 2-23.

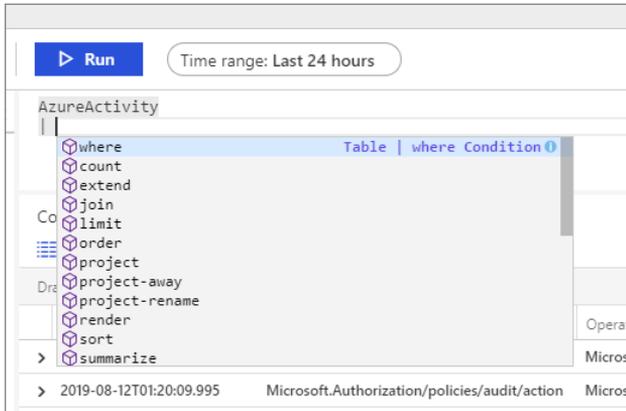


FIGURE 2-23 Using the context-sensitive IntelliSense capability

To narrow the search to look only for activities that are related to VM creation (which was the task you did in the beginning of this chapter), type the query below and click **Run**.

AzureActivity

| where OperationName contains "Create or Update Virtual Machine"

The results should be similar to Figure 2-24, unless you have done other activities where the operation name refers to the VM creation or an update to the VM.

Drag a column header and drop it here to group by that column						
TimeGenerated [UTC]	OperationName	OperationNameValue	Level	ActivityStatus	ActivityStatusValue	
> 2019-08-11T12:40:25.374	Create or Update Virtual Machine	Microsoft.Compute/virtualMachines/write	Informational	Started	Started	
> 2019-08-11T12:40:26.254	Create or Update Virtual Machine	Microsoft.Compute/virtualMachines/write	Informational	Accepted	Accepted	
> 2019-08-11T12:42:35.429	Create or Update Virtual Machine	Microsoft.Compute/virtualMachines/write	Informational	Succeeded	Succeeded	

FIGURE 2-24 Results of a more specific query

To validate the other data sources that were ingested in this chapter, you can use the following sample queries:

- **Azure Active Directory**

- Query: *SignInLogs*

- Use this query to visualize all Azure AD sign-in logs.

- Query: *AuditLogs*

- Use this query to visualize all Azure AD audit logs.

- **Azure Active Directory Identity Protection**

- Query: *SecurityAlert | where ProviderName == "IPC"*
 - Azure AD Identity Protection alerts are located under the *SecurityAlert* table, and the way to identify alerts coming from this provider is by using the keyword "IPC" on the *ProviderName* field. This query will list all alerts generated by Azure AD Identity Protection.

- **Azure Security Center**

- Query: *SecurityAlert | where AlertName contains "suspicious"*
 - This query will list all alerts generated by Security Center where the alert name contains the keyword "suspicious".

Index

SYMBOLS

- + (Add) operator, KQL, 169
- / (Divide) operator, KQL, 169
- (Equals) operator, KQL, 169–170
- > (Greater) operator, KQL, 169
- >= (Greater or Equal) operator, KQL, 169–170
- < (Less) operator, KQL, 169
- <= (Less or Equal) operator, KQL, 169
- % (Modulo) operator, KQL, 169
- * (Multiply) operator, KQL, 169
- != (Not equals) operator, KQL, 169
- lin (Not equals to any of the elements) operator, KQL, 169
- (Subtract) operator, KQL, 169

A

- AAD user, Logic Apps, 115
- access control, 15
- Activity Workbook, 133–137
- Add (+) operator, KQL, 169
- adversaries, knowledge of, 8
- aggregation reference, KQL (Kusto Query Language), 172
- alerts
 - and bookmarks, 97
 - listing in dashboard, 56–61
- analysts
 - “single pane of glass,” 7
 - SOC (security operations center), 5
- analytic rules
 - configuring, 38–44
 - creating, 45–49
 - types, 44–45
 - validating, 49–50
- analytics
 - component, 15
 - justification for usage, 33–34
- Analytics dashboard, accessing, 34–37
- any() function, KQL, 172
- Apache Struts, vulnerability in, 2
- architecture, Azure Sentinel, 13–15
- arg_max() function, KQL, 172
- arg_min() function, KQL, 172
- “assume breach” mindset, 2–3
- attack timeline with alerts, 61
- attrib* tool, use with WannaCry, 34
- Audit Logs hunting queries, 70
- automation
 - post-incident, 125–130
 - real-time, 110–125
- avg() function, KQL, 172
- AWS (Amazon Web Services), connecting with, 151–157
- AWS CloudTrail hunting queries, 70

- Azure Active Directory Identity Protection, 25–29
- Azure Activity hunting queries, 70
- Azure Activity Log, 22–23. *See also* log data
- Azure Logic Apps, 43
- Azure Notebooks, 84–87
- Azure Security Center, connecting to, 23–25
- Azure Sentinel
 - accessing in Azure Portal, 52
 - accessing ingested data, 29–32
 - addressing SecOps challenges, 11
 - adoption considerations, 15–16
 - analytics, 15
 - architecture, 13–15
 - cases, 14
 - Community, 15, 45
 - components, 14
 - connecting to, 88–94
 - core capabilities, 12
 - dashboards, 14
 - data collection, 12
 - data connectors, 14
 - data ingestion, 19–29
 - documentation, 11
 - enabling, 16–19
 - GitHub repository, 56, 107
 - hunting, 14
 - incidents page, 53
 - investigation of threats, 12
 - Log Analytics workspace, 15–16
 - notebooks, 14
 - overview, 1
 - Playbooks, 14
 - querying data, 87–94
 - rapid response, 12
 - security incidents, 52–55
 - Technical Community blogs, 107
 - threat detection, 12

B

- Base64-encoded contents, decoding, 103
- Bitcoin ransom
 - coin-mining malware, 4
 - paying via Petya, 1
- black box rules, 44
- bokeh* library, 99
- bookmarks. *See also* queries
 - and alerts, 97
 - and hunting queries, 73–78
 - using with incidents, 56, 67–69
- `bool` type, KQL, 166
- `buildschema()` function, KQL, 172

C

- cases, 14
- CDF collector, installing, 146–147
- CDOC (Cyber Defense Operations Center), 6
- CEF (Common Event Format), 20, 160
- CISOs (Chief Information Security Officers), 1, 7
- cloud-native SIEM, 11–12, 21
- clustering, finding outliers with, 103–104
- coin-mining malware, 4
- Collection, ATT&CK Matrix, 66
- columns, adding and removing in
 - KQL, 172–173
- Command And Control, ATT&CK Matrix, 66
- comments, using with incidents, 56
- Community page, 15, 45
- community-based hunting queries, 77–78
- comparison operators, KQL (Kusto Query Language), 169
- connecting
 - with AWS (Amazon Web Services), 151–157
 - to Azure Sentinel, 88–94
 - with Fortinet, 145–151
 - with Palo Alto, 158–162

Consumer Interview System, 3
 Containment, incident management, 51–52
 count() function, KQL, 172
 countif() function, KQL, 172
 Credential Access, ATT&CK Matrix, 66
 CTI (cyberthreat intelligence), 8
 Custom Deployment blade, post-incident automation, 126
 CVE-2017-0145 critical vulnerability, 33
 CVE-2017-5638 critical vulnerability, 2–3
 cyberattacks in Europe, 1
 cyberdefense operations, fusion center model, 6

D

DART (Detection and Response Team), Microsoft, 3–5
 dashboards, 14
 data
 exporting to Excel, 143
 summarizing in KQL, 170–172
 suspicious signs in, 101–103
 data collection, 12, 20
 data connectors, 14
 data ingestion, 19–29
 data sets, linking/displaying, 105
 data sources, considering, 16
 data types, KQL, 166–167
 data visualization
 Azure Sentinel workbooks, 131–132
 built-in workbooks, 133–137
 custom workbooks, 138–140
 Excel, 143
 PowerBI, 141–142
DataFrame, using with pandas, 92, 95, 105
 datetime type, KQL, 166

DBScan algorithm, using to cluster processes, 104
 dcount() function, KQL, 172
 decimal type, KQL, 166
 decoding obfuscated data, Notebooks, 103
 Defender Advanced Threat Protection, Microsoft, 3–4
 Defense Evasion, ATT&CK Matrix, 66
 deployment considerations, 16
 Detection and Analysis, incident management, 51–52
 Discovery, ATT&CK Matrix, 66
 Divide (/) operator, KQL, 169
 DNS Events hunting queries, 71
DNS Proxies incident, 56
 documentation, Azure Sentinel, 11
 DSVM (Data Science Virtual Machine), 87
 dynamic type, KQL, 166

E

Edit API Connection blade, post-incident automation, 127
 Edit Template blade, post-incident automation, 126
 email messages, scanning by Office 365, 4
 entities, using with incidents, 56, 59
 Enumeration of users and groups, hunting query, 68
 Equals (==) operator, KQL, 169–170
 Equals to one of the elements (in) operator, KQL, 169
 Equifax network, 3
 Eradication, incident management, 51–52
 Europe, cyberattacks in, 1
evaluate operator, KQL (Kusto Query Language), 175–176

event timelines

event timelines, Notebooks, 99–100. *See also*
Timeline
evidence, 14
Excel, exporting data to, 143
Execution, ATT&CK Matrix, 65
Exfiltration, ATT&CK Matrix, 66
Exploration Notebooks, 94
exploration queries, 61. *See also* queries
exporting data to Microsoft Excel, 143
extend, KQL (Kusto Query Language), 173

F

finding outliers with clustering,
Notebooks, 103–104
forensics analysts, 5
Fortinet, connecting with, 145–151
fullouter join, KQL, 175
fusion center model, cyberdefense
operations, 6

G

geomapping IP addresses, Notebooks, 106
GitHub repository, 70, 85–86, 107
Greater (>) operator, KQL, 169
Greater or Equal (>=) operator, KQL, 169–170
guid type, KQL, 166–167

H

Hellen, Ian, 79
HTTP Data Collector API, 20
hunting, 14
hunting and investigation, notebooks, 94–106
Hunting dashboard, accessing, 64–68

hunting queries. *See also* threat hunting
availability, 70–73
and bookmarks, 73–78
community-based, 77–78

I

identity protection, 27–29
Impact, ATT&CK Matrix, 66
in (Equals to one of the elements) operator,
KQL, 169
lin (Not equals to any of the elements)
operator, KQL, 169
incident management. *See also* security
incidents
Azure Sentinel, 52–55
investigation, 56–61
overview, 51–52
ingesting data, 19–32
Initial Access, ATT&CK Matrix, 65
inner join, KQL, 175
innerunique join, KQL, 175
int type, KQL, 166
integration costs, reducing, 21
IntelliSense capability, using, 31
investigation
graph, 57–61
of threats, 12
Tier 2, 5
IOA (indicators of attack), 34
IOCs (indicators of compromise), 33, 101–102
IP addresses
geomapping, 106
looking up, 102
IPython, 79, 96
ipywidgets, Jupyter Notebooks, 98, 105

J

join, KQL (Kusto Query Language), 174–175
 Jupyter Notebooks. *See also* Notebooks
 audiences, 83
 complexity guidelines, 80–81
 data persistence, repeatability,
 backtracking, 81
 data processing, 82
 environments, 83–84
 interactive display environment, 81–82
 ipywidgets, 98
 joining to external data, 82
 machine learning, 82
 magic command, 89–90
 overview, 79–84
 scripting and programming, 81
 use cases, 83
 visualization, 82
 Jupyter server options, Azure
 Notebooks, 86–87
 JupyterHub, 87

K

Kassis, Mike, 163
 Koren, Koby, 110
 KQL (Kusto Query Language)
 accessing ingested data, 29–32
 adding and removing columns, 172–173
 aggregation reference, 172
 comparison operators, 169
 data types, 166–167
 evaluate operator, 175–176
 extend, 173
 filtering data, 169–170
 getting data, 167–168

join, 174–175
 joining tables, 173–175
 learning resources, 177
let statements, 176–177
 limiting data, 168
 numerical operators, 169
 PowerShell, 164–166
project and *project-away*
 statements, 172–173
 sorting data, 168
 SQL, 164
 string operators, 169–170
 structure, 163–166
 summarizing data, 170–172
take operator, 168
union, 174
 workspace data, 39–40

KQL queries
 Palo Alto Networks firewalls, 161–162
 substituting Python variables in, 93–94
 Kqlmagic. *See also* queries
 and *QueryProvider*, 96
 using to query data, 87–94

L

Lateral Movement, ATT&CK Matrix, 66
leftanti join, KQL, 175
leftouter join, KQL, 175
leftsemi join, KQL, 175
 Less (<) operator, KQL, 169
 Less or Equal (<=) operator, KQL, 169
let statements, KQL, 176–177
 linking/displaying related data sets,
 Notebooks, 105
 Log Analytics workspace, 15–16, 157
 log data ingestion time, 49

log data

log data, sending to workspaces, 20. *See also*
Azure Activity Log
Logic Apps, 109, 111–115, 121
logon information, querying, 98–99
long type, KQL, 166

M

magic command, Jupyter, 89–90
`make_bag()` function, KQL, 172
`make_list()` function, KQL, 172
`make_set()` function, KQL, 172
malicious URL STIX object, 9–10
malware
 coin-mining, 4
 Petya and NotPetya, 1–2
`max()` function, KQL, 172
Maxmind GeoLite, 106
M.E.Doc tax accounting software, 2
Microsoft Excel, exporting data to, 143
Microsoft
 black box rules, 44
 Defender Advanced Threat Protection, 3–4
 Detection and Response Team (DART), 3–5
 GitHub repository, 70, 85–86
 Security Intelligence Report, 3–5
 services, 20
 solutions, 44–45
 vendors/partners' connectors, 20
`min()` function, KQL, 172
Mitre, definition of SOC, 5
MITRE ATT&CK knowledge base, 34, 65–66
ML (machine learning) technique, 103
Modulo (%) operator, KQL, 169
MSTIC (Microsoft Threat Intelligence Center),
 Notebooks, 95

msticpy query library, Notebooks, 95–97
Multiple Data Sources hunting queries, 71
Multiply (*) operator, KQL, 169

N

NIST (National Institute of Standards and
Technology), 51
Not equals (!-) operator, KQL, 169
Not equals to any of the elements (!in)
operator, KQL, 169
Notebooks. *See also* Jupyter Notebooks
 alerts and bookmarks, 97
 benefits, 107
 decoding obfuscated data, 103
 diagram, 14
 event timelines, 99–100
 finding outliers with clustering, 103–104
 geomapping IP addresses, 106
 hunting and investigation, 94–106
 IoCs and threat intelligence, 101–102
 linking/displaying related data sets, 105
MSTIC (Microsoft Threat Intelligence
Center), 95
 msticpy query library, 95–97
 msticpy query library, 95–97
 querying process/logon
 information, 98–99
 suspicious signs in data, 101–103
 types, 94
NotPetya malware, 1–2
NSG (Network Security Group), 145
numerical operators, KQL (Kusto Query
Language), 169

O

obfuscated data, decoding, 103
 Office 365 action, adding for Playbook, 116
 Office 365 Activity hunting queries, 71
 Office 365, email messages scanned by, 4
 Operation WilySupply, 3
 operational CTI, 8
order operator, KQL (Kusto Query Language), 168

P

Palo Alto Networks firewalls, connecting with, 158–162
 pandas dataframes, 92, 105
 percentiles() function, KQL, 172
 permissions, considering, 15
 Persistence, ATT&CK Matrix, 66
 Petya ransomware, 1
 phishing, 4
 pie charts, adding to Workbooks, 139
 Playbooks
 diagram, 14
 post-incident automation, 125–128
 real-time automation, 110–125
 SOAR (Security Orchestration, Automation and Response), 109–110
 post-incident automation, 125–130
 Power BI, visualizations, 141–142
 PowerShell and KQL, 164–166
 Privilege Escalation, ATT&CK Matrix, 66
 process information, querying, 98–99
 procedures. *See* Playbooks
project and *project-away* statements, KQL (Kusto Query Language), 172–173

protection, automating, 12
 Python, 82–83, 92–94

Q

queries. *See also* bookmarks; exploration queries; KQL (Kusto Query Language); Kqlmagic
 and bookmarks, 67
 process and logon information, 98–99
 validating data sources, 31–32
 Query Language Reference, 40
 querying process/logon information, Notebooks, 98–99
 QueryProvider library, *msticpy*, 95–96

R

ransomware
 Petya, 1
 WannaCry, 33–34
 RBAC (Role-Based Access Control), 15–16
 real type, KQL, 166
 real-time automation, 110–125
 reference operational model, SOC (Security Operations Center), 9
 Remediation, incident management, 51–52
 remediation analysts, 5
 reports. *See* Workbooks
 resources, freeing up, 21
 REST API client, 20
rightanti join, KQL, 175
rightouter join, KQL, 175
rightsemi join, KQL, 175
 Rule Templates tab, 36

S

Sample Notebooks, 94

SecOps (Security Operations)

- addressing challenges, 11
- cloud-native SIEM, 11–12
- intelligence report, 3–5
- resource challenges, 7
- security challenges, 5–8
- threat intelligence, 8–10
- threat landscape, 1–3

Security Alert hunting queries, 71

security data challenges, 7–8

Security Event hunting queries, 72

security incidents, 52–55. *See also* incident management

Security Intelligence Report, Microsoft, 3–5

Shezaf, Ofer, 21

SIEM (Security Incident and Event Management), 1

- cloud-native, 11–12, 21

Sign-in Logs hunting queries, 72–73

“single pane of glass,” analysts, 7

SMB (Server Message Block), 2

SOAR (Security Orchestration, Automation and Response), 11

- overview, 109–110

SOC (Security Operations Center), 1

- reference operational model, 9
- resource challenges, 7
- and SecOps, 5–6
- threat hunting, 63–64

software supply chains, targeting, 3

SQL and KQL, 164

stdev() function, KQL, 172

STIX object, malicious URL, 9–10

strategic CTI, 8

string operators, KQL (Kusto Query Language), 169

string type, KQL, 166

Subtract (-) operator, KQL, 169

sum() function, KQL, 172

summarize statement, KQL, 170–172

support engineers, SOC (security operations center), 6

suspicious signs in data, Notebooks, 101–103

SYSLOG CEF messages, 145, 159

Syslog Common Event Format, 20

Syslog daemon, configuring for Palo Alto, 158–159

Syslog hunting queries, 73

T

tables, joining in KQL, 173–175

tactical CTI, 8

take operator, KQL (Kusto Query Language), 168

TAXII (Trusted Automated Exchange of Intelligence Information), 10

Technical Community blogs, 107

threat collection, 12

threat hunting. *See also* hunting queries

- implementing, 64–73
- overview, 63–64
- queries and bookmarks, 73–78

threat intelligence, 8–10, 73

threat landscape, 1–5

TI (Threat Intelligence) indicators, 101–102

Tier 1-Tier 3 analysts, SecOps, 5–7

time charts, adding to Workbooks, 140

Timeline, listing for incident alerts, 59–60. *See also* event timelines

timespan type, KQL, 166–167

TTPs (tactics, techniques, procedures), 1, 8

U

Ukraine, infections in, 1–2
union, KQL (Kusto Query Language), 174
URL. *See* malicious URL STIX object

V

`variance()` function, KQL, 172
visualizations, Power BI, 141–142
VM (virtual machine)
 isolating, 52
 Palo Alto Networks firewalls, 159
 for testing real-time automation, 122–125
vulnerabilities, targeting, 2

W

W3C IIS Log hunting queries, 73
WannaCry ransomware, 33–34
“web shells,” dropping, 3
where operator, KQL (Kusto Query Language), 169–170
Wire Data hunting queries, 73
Workbooks
 action menu, 136
 customizing, 138–140
 editing, 138
 pie charts, 139
 templates, 132, 134–135
 time charts, 140
 using, 131, 133–137
workspace design consideration, 16–18