Microsoft Security

Microsoft Sentinel skill-up training plan

Sameh Younis

Senior Security Solution Architect

Based on Microsoft Learn documentation's skill-up training

Plan Outline

- Part 1: Overview
  - Module 0: Other learning and support options
  - Module 1: Get started with Microsoft Sentinel
  - Module 2: How is Microsoft Sentinel used?
- Part 2: Architecting and deploying
  - Module 3: Workspace and tenant architecture
  - Module 4: Data collection
  - Module 5: Log management
  - Module 6: Enrichment: Threat intelligence, watchlists, and more
  - Module 7: Log transformation
  - Module 8: Migration
  - Module 9: Advanced SIEM information model and normalization
- Part 3: Creating content
  - Module 10: Kusto Query Language
  - Module 11: Analytics
  - Module 12: Implementing SOAR
  - Module 13: Workbooks, reporting, and visualization
  - Module 14: Notebooks
  - Module 15: Use cases and solutions
- Part 4: Operating
  - Module 16: A day in a SOC analyst's life, incident management, and investigation
  - Module 17: Hunting
  - Module 18: User and Entity Behavior Analytics (UEBA)
  - Module 19: Monitoring Microsoft Sentinel's health
- Part 5: Advanced
  - Module 20: Extending and integrating by using the Microsoft Sentinel APIs
  - Module 21: Build-your-own machine learning
- Next Steps: Recommended Content and Certification Readiness

Part 1: Overview

Module 0: Other learning and support options

- This skill-up training is a level-400 training that's based on the Microsoft Sentinel Ninja training. If you don't want to go as deep, or you have a specific issue to resolve, other resources might be more suitable:
- Although the skill-up training is extensive, it naturally has to follow a script and can't expand on every topic. See the referenced documentation for information about each article.
- You can now become certified with the new certification SC-200: Microsoft Security Operations Analyst, which covers Microsoft Sentinel. For a broader, higher-level view of the Microsoft Security suite, you might also want to consider SC-900: Microsoft Security, Compliance, and Identity Fundamentals or AZ-500: Microsoft Azure Security Technologies.
- If you're already skilled up on Microsoft Sentinel, keep track of what's new or join the Microsoft Cloud Security Private Community program for an earlier view into upcoming releases.
- Do you have a feature idea to share with us? Let us know on the Microsoft Sentinel user voice page.
- Are you a premier customer? You might want the on-site or remote, four-day *Microsoft Sentinel Fundamentals Workshop*. Contact your Customer Success Account Manager for more details.
- Do you have a specific issue? Ask (or answer others) on the Microsoft Sentinel Tech Community. Or you can email your question or issue to us at MicrosoftSentinel@microsoft.com.

Module 1: Get started with Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Sentinel delivers security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response. For more information, see What is Microsoft Sentinel?.

If you want to get an initial overview of Microsoft Sentinel's technical capabilities, the latest Ignite presentation is a good starting point. You might also find the Quick Start Guide to Microsoft Sentinel useful (site registration is required). You'll find a more detailed overview in this Microsoft Sentinel webinar: YouTube, MP4, or presentation.

Finally, do you want to try it yourself? The Microsoft Sentinel All-In-One Accelerator (blog, YouTube, MP4, or presentation) offers an easy way to get started. To learn how to get started, review the onboarding documentation, or view Insight's Microsoft Sentinel setup and configuration video.

Learn from other users

Thousands of organizations and service providers are using Microsoft Sentinel. As is usual with security products, most organizations don't go public about it. Still, here are a few who have:

- Find public customer use cases.
- Stuart Gregg, Security Operations Manager at ASOS, posted a much more detailed blog post from the Microsoft Sentinel experience, focusing on hunting.

Learn from analysts

- Azure Sentinel achieves a Leader placement in Forrester Wave, with top ranking in Strategy
- Microsoft named a Visionary in the 2021 Gartner Magic Quadrant for SIEM for Microsoft Sentinel

Module 2: How is Microsoft Sentinel used?

Many organizations use Microsoft Sentinel as their primary SIEM. Most of the modules in this course cover this use case. In this module, we present a few extra ways to use Microsoft Sentinel.

As part of the Microsoft Security stack
Use Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft Defender XDR together to protect your Microsoft workloads, including Windows, Azure, and Office:

- Read more about our comprehensive SIEM+XDR solution combining Microsoft Sentinel and Microsoft Defender XDR.
- Read The Azure Security compass (now Microsoft Security Best Practices) to understand the Microsoft blueprint for your security operations.
- Read and watch how such a setup helps detect and respond to a WebShell attack: blog or video demo.
- View the Better Together webinar "OT and IOT attack detection, investigation, and response."

To monitor your multicloud workloads
The cloud is (still) new and often not monitored as extensively as on-premises workloads. Read this presentation to learn how Microsoft Sentinel can help you close the cloud monitoring gap across your clouds.

Side by side with your existing SIEM
For either a transition period or a longer term, if you're using Microsoft Sentinel for your cloud workloads, you might be using Microsoft Sentinel alongside your existing SIEM. You might also be using both with a ticketing system such as Service Now.

For more information about migrating from another SIEM to Microsoft Sentinel, view the migration webinar: YouTube, MP4, or presentation.

Continue module 2 →

Module 2 Continued….

There are three common scenarios for side-by-side deployment:

- If you have a ticketing system in your SOC, a best practice is to send alerts or incidents from both SIEM systems to a ticketing system such as Service Now. Examples include using Microsoft Sentinel incident bi-directional sync with ServiceNow or sending alerts enriched with supporting events from Microsoft Sentinel to third-party SIEMs.
- At least initially, many users send alerts from Microsoft Sentinel to their on-premises SIEM. To learn how, see Send alerts enriched with supporting events from Microsoft Sentinel to third-party SIEMs.
- Over time, as Microsoft Sentinel covers more workloads, you would ordinarily reverse direction and send alerts from your on-premises SIEM to Microsoft Sentinel. To do so:
  - For Splunk, see Send data and notable events from Splunk to Microsoft Sentinel.
  - For QRadar, see Send QRadar offenses to Microsoft Sentinel.
  - For ArcSight, see Common Event Format (CEF) forwarding.

You can also send the alerts from Microsoft Sentinel to your third-party SIEM or ticketing system by using the Graph Security API. This approach is simpler, but it doesn't enable sending other data.

For MSSPs

Because it eliminates the setup cost and is location agnostic, Microsoft Sentinel is a popular choice for providing SIEM as a service. You'll find a list of MISA (Microsoft Intelligent Security Association) member-managed security service providers (MSSPs) that use Microsoft Sentinel. Many other MSSPs, especially regional and smaller ones, use Microsoft Sentinel but aren't MISA members.

To start your journey as an MSSP, read the Microsoft Sentinel Technical Playbooks for MSSPs. More information about MSSP support is included in the next module, which covers cloud architecture and multitenant support.

Part 2: Architecting and deploying

Module 3: Workspace and tenant architecture

A Microsoft Sentinel instance is called a *workspace*. The workspace is the same as a Log Analytics workspace, and it supports any Log Analytics capability. You can think of Microsoft Sentinel as a solution that adds SIEM features on top of a Log Analytics workspace.

Multiple workspaces are often necessary and can act together as a single Microsoft Sentinel system. A special use case is providing a service by using Microsoft Sentinel (for example, by an *MSSP* (Managed Security Service Provider) or by a *Global SOC* in a large organization).

To learn more about using multiple workspaces as one Microsoft Sentinel system, see Extend Microsoft Sentinel across workspaces and tenants or view the webinar: YouTube, MP4, or presentation.

When you're using multiple workspaces, consider the following:

- An important driver for using multiple workspaces is *data residency*. For more information, see Microsoft Sentinel data residency.
- To deploy Microsoft Sentinel and manage content efficiently across multiple workspaces, you could manage Microsoft Sentinel as code by using continuous integration/continuous delivery (CI/CD) technology. A recommended best practice for Microsoft Sentinel is to enable continuous deployment. For more information, see Enable continuous deployment natively with Microsoft Sentinel repositories.
- When you're managing multiple workspaces as an MSSP, you might want to protect MSSP intellectual property in Microsoft Sentinel.

The Microsoft Sentinel Technical Playbook for MSSPs provides detailed guidelines for many of those topics, and it's useful for large organizations, not just for MSSPs.

Module 4: Data collection

The foundation of a SIEM is collecting telemetry: events, alerts, and contextual enrichment information, such as threat intelligence, vulnerability data, and asset information. Here is a list of sources to refer to:

- Read Microsoft Sentinel data connectors.
- Go to Find your Microsoft Sentinel data connector to see all the supported and out-of-the-box data connectors. You'll find links to generic deployment procedures, and extra steps required for specific connectors.
- Data collection scenarios: Learn about collection methods such as Logstash/CEF/WEF. Other common scenarios are permissions restriction to tables, log filtering, collecting logs from Amazon Web Services (AWS) or Google Cloud Platform (GCP), Microsoft 365 raw logs, and so on. All can be found in the "Data Collection Scenarios" webinar: YouTube, MP4, or presentation.

The first piece of information you'll see for each connector is its *data ingestion method*. The method that appears there is a link to one of the following generic deployment procedures, which contain most of the information you'll need to connect your data sources to Microsoft Sentinel:

Data ingestion method	Associated article
Azure service-to-service integration	Connect to Azure, Windows, Microsoft, and Amazon services
Common Event Format (CEF) over Syslog	Get CEF-formatted logs from your device or appliance into Microsoft Sentinel
Microsoft Sentinel Data Collector API	Connect your data source to the Microsoft Sentinel Data Collector API to ingest data
Azure Functions and the REST API	Use Azure Functions to connect Microsoft Sentinel to your data source
Syslog	Collect data from Linux-based sources by using Syslog
Custom logs	Collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent

If your source isn't available, you can create a custom connector. Custom connectors use the ingestion API and therefore are similar to direct sources. You most often implement custom connectors by using Azure Logic Apps, which offers a codeless option, or Azure Functions.

Module 5: Log management

The first architecture decision to consider when you're configuring Microsoft Sentinel, is *how many workspaces and which ones to use*. Other key log management architectural decisions to consider include:

- Where and how long to retain data.
- How to best manage access to data and secure it.

Ingest, archive, search, and restore data within Microsoft Sentinel

To get started, view the "Manage your log lifecycle with new methods for ingestion, archival, search, and restoration" webinar.

This suite of features contains:

- **Basic ingestion tier**: A new pricing tier for Azure Monitor Logs that lets you ingest logs at a lower cost. This data is retained in the workspace for only eight days.
- **Archive tier**: Azure Monitor Logs has expanded its retention capability from two years to seven years. With this new tier, you can retain data for up to seven years in a low-cost archived state.
- **Search jobs**: Search tasks that run limited KQL to find and return all relevant logs. These jobs search data across the analytics tier, the basic tier, and archived data.
- **Data restoration**: A new feature that lets you pick a data table and a time range so that you can restore data to the workspace via a restore table.

For more information about these new features, see Ingest, archive, search, and restore data in Microsoft Sentinel.

Continue module 5 →

Continue Module 5

Alternative retention options outside the Microsoft Sentinel platform

If you want to *retain data* for more than two years or *reduce the retention cost*, consider using Azure Data Explorer for long-term retention of Microsoft Sentinel logs. See the webinar slides, webinar recording, or blog.

Want more in-depth information? View the "Improving the breadth and coverage of threat hunting with ADX support, more entity types, and updated MITRE integration" webinar.

If you prefer another long-term retention solution, see Export from Microsoft Sentinel / Log Analytics workspace to Azure Storage and Event Hubs or Move logs to long-term storage by using Azure Logic Apps. The advantage of using Logic Apps is that it can export historical data.

Finally, you can set fine-grained retention periods by using table-level retention settings. For more information, see Configure data retention and archive policies in Azure Monitor Logs (Preview).

Log security

- Use resource role-based access control (RBAC) or table-level RBAC to enable multiple teams to use a single workspace.
- If needed, delete customer content from your workspaces.
- Learn how to audit workspace queries and Microsoft Sentinel use by using alerts workbooks and queries.
- Use private links to ensure that logs never leave your private network.

Dedicated cluster

Use a dedicated workspace cluster if your projected data ingestion is about or more than 500 GB per day. With a dedicated cluster, you can secure resources for your Microsoft Sentinel data, which enables better query performance for large data sets.

Module 6: Enrichment: Threat intelligence, watchlists, and more

One of the important functions of a SIEM is to apply contextual information to the event steam, which enables detection, alert prioritization, and incident investigation. Contextual information includes, for example, threat intelligence, IP intelligence, host and user information, and watchlists. Microsoft Sentinel provides comprehensive tools to import, manage, and use threat intelligence. For other types of contextual information, Microsoft Sentinel provides watchlists and other alternative solutions.

Threat intelligence

Threat intelligence is an important building block of a SIEM. View the "Explore the Power of Threat Intelligence in Microsoft Sentinel" webinar.

In Microsoft Sentinel, you can integrate threat intelligence by using the built-in connectors from TAXII (Trusted Automated eXchange of Indicator Information) servers or through the Microsoft Graph Security API. For more information, see Threat intelligence integration in Microsoft Sentinel.

For more information about importing threat intelligence, see the Module 4: Data collection sections.

After it's imported, threat intelligence is used extensively throughout Microsoft Sentinel. The following features focus on using threat intelligence:

- View and manage the imported threat intelligence in **Logs** in the new **Threat Intelligence** area of Microsoft Sentinel.
- Use the built-in threat intelligence analytics rule templates to generate security alerts and incidents by using your imported threat intelligence.
- Visualize key information about your threat intelligence in Microsoft Sentinel by using the threat intelligence workbook.

View the "Automate Your Microsoft Sentinel Triage Efforts with RiskIQ Threat Intelligence" webinar: YouTube or presentation.

Short on time? View the Ignite session (28 minutes).

Want more in-depth information? View the "Deep dive on threat intelligence" webinar: YouTube, MP4, or presentation.

Continue module 6 →

Continue Module 6....

Watchlists and other lookup mechanisms

To import and manage any type of contextual information, Microsoft Sentinel provides watchlists. By using watchlists, you can upload data tables in CSV format and use them in your KQL queries. For more information, see Use watchlists in Microsoft Sentinel, or view the "Use watchlists to manage alerts, reduce alert fatigue, and improve SOC efficiency" webinar: YouTube or presentation.

Use watchlists to help you with following scenarios:

- **Investigate threats and respond to incidents quickly**: Rapidly import IP addresses, file hashes, and other data from CSV files. After you import the data, use watchlist name-value pairs for joins and filters in alert rules, threat hunting, workbooks, notebooks, and general queries.
- **Import business data as a watchlist**: For example, import lists of users with privileged system access, or terminated employees. Then, use the watchlist to create allowlists and blocklists to detect or prevent those users from logging in to the network.
- **Reduce alert fatigue**: Create allowlists to suppress alerts from a group of users, such as users from authorized IP addresses who perform tasks that would normally trigger the alert. Prevent benign events from becoming alerts.
- **Enrich event data**: Use watchlists to enrich your event data with name-value combinations that are derived from external data sources.

In addition to watchlists, you can use the KQL external-data operator, custom logs, and KQL functions to manage and query context information. Each of the four methods has its pros and cons, and you can read more about the comparisons between them in the blog post "Implementing lookups in Microsoft Sentinel." Although each method is different, using the resulting information in your queries is similar and enables easy switching between them.

For ideas about using watchlists outside analytic rules, see Utilize watchlists to drive efficiency during Microsoft Sentinel investigations.

View the "Use watchlists to manage alerts, reduce alert fatigue, and improve SOC efficiency" webinar: YouTube or presentation.

Module 7: Log transformation

Microsoft Sentinel supports two new features for data ingestion and transformation. These features, provided by Log Analytics, act on your data even before it's stored in your workspace. The features are:

- **Logs ingestion API**: Use it to send custom-format logs from any data source to your Log Analytics workspace and then store those logs either in certain specific standard tables, or in custom-formatted tables that you create. You can perform the actual ingestion of these logs by using direct API calls. You can use Azure Monitor data collection rules to define and configure these workflows.

- **Workspace data transformations for standard logs**: It uses data collection rules to filter out irrelevant data, to enrich or tag your data, or to hide sensitive or personal information. You can configure data transformation at ingestion time for the following types of built-in data connectors:
    - Azure Monitor agent (AMA)-based data connectors (based on the new Azure Monitor agent)
    - Microsoft Monitoring agent (MMA)-based data connectors (based on the legacy Azure Monitor Logs Agent)
    - Data connectors that use diagnostics settings
    - Service-to-service data connectors

For more information, see:

- Transform or customize data at ingestion time in Microsoft Sentinel
- Find your Microsoft Sentinel data connector

Module 8: Migration

In many (if not most) cases, you already have a SIEM and need to migrate to Microsoft Sentinel. Although it might be a good time to start over and rethink your SIEM implementation, it makes sense to utilize some of the assets you've already built in your current implementation. View the "Best practices for converting detection rules" (from Splunk, QRadar, and ArcSight to Azure Microsoft Sentinel) webinar: YouTube, MP4, presentation, or blog.

You might also be interested in the following resources:

- Splunk Search Processing Language (SPL) to KQL mappings
- ArcSight and QRadar rule mapping samples

Module 9: Advanced SIEM information model and normalization

Working with varied data types and tables together can present a challenge. You must become familiar with those data types and schemas as you're writing and using a unique set of analytics rules, workbooks, and hunting queries. Correlating among the data types that are necessary for investigation and hunting can also be tricky.

The Advanced SIEM information model (ASIM) provides a seamless experience for handling various sources in uniform, normalized views. ASIM aligns with the Open-Source Security Events Metadata (OSSEM) common information model, promoting vendor-agnostic, industry-wide normalization. View the "Advanced SIEM information model (ASIM): Now built into Microsoft Sentinel" webinar: YouTube or presentation.

The current implementation is based on query time normalization, which uses KQL functions:

- **Normalized schemas** cover standard sets of predictable event types that are easy to work with and build unified capabilities. The schema defines which fields should represent an event, a normalized column naming convention, and a standard format for the field values.
  - View the "Understanding normalization in Microsoft Sentinel" webinar: YouTube or presentation.
  - View the "Deep Dive into Microsoft Sentinel normalizing parsers and normalized content" webinar: YouTube, MP3, or presentation.

- **Parsers** map existing data to the normalized schemas. You implement parsers by using KQL functions. View the "Extend and manage ASIM: Developing, testing and deploying parsers" webinar: YouTube or presentation.

- **Content** for each normalized schema includes analytics rules, workbooks, and hunting queries. This content works on any normalized data without the need to create source-specific content.

Continue module 9 →

Continue Module 9 ….

Using ASIM provides the following benefits:

- **Cross source detection**: Normalized analytic rules work across sources on-premises and in the cloud. The rules detect attacks, such as brute force, or impossible travel across systems, including Okta, AWS, and Azure.
- **Allows source agnostic content**: Covering built-in and custom content by using ASIM automatically expands to any source that supports ASIM, even if the source was added after the content was created. For example, process event analytics support any source that a customer might use to bring in the data, including Microsoft Defender for Endpoint, Windows Events, and Sysmon. We're ready to add Sysmon for Linux and WEF when it has been released.
- **Support for your custom sources in built-in analytics**
- **Ease of use**: Analysts who learn ASIM find it much simpler to write queries because the field names are always the same.

Learn more about ASIM

Take advantage of these resources:

- View the "Understanding normalization in Azure Sentinel" overview webinar: YouTube or presentation.
- View the "Deep dive into Microsoft Sentinel normalizing parsers and normalized content" webinar: YouTube, MP3, or presentation.
- View the "Turbocharge ASIM: Make sure normalization helps performance rather than impact it" webinar: YouTube, MP4, or presentation.
- Read the ASIM documentation.

Continue module 9 →

Continue Module 9 ....

Deploy ASIM

- Deploy the parsers from the folders, starting with “ASIM*” in the *parsers* folder on GitHub.
- Activate analytic rules that use ASIM. Search for **normal** in the template gallery to find some of them. To get the full list, use this GitHub search.

Use ASIM

- Use the ASIM hunting queries from GitHub.
- Use ASIM queries when you're using KQL on the log screen.
- Write your own analytics rules by using ASIM, or convert existing rules.
- Write parsers for your custom sources to make them ASIM-compatible, and take part in built-in analytics.

Part 3: Creating content

What is Microsoft Sentinel content?

The value of Microsoft Sentinel security is a combination of its built-in capabilities and your ability to create custom capabilities and customize the built-in ones. Among built-in capabilities, there are User and Entity Behavior Analytics (UEBA), machine learning, or out-of-box analytics rules. Customized capabilities are often referred to as "content" and include analytic rules, hunting queries, workbooks, playbooks, and so on.

In this section, we grouped the modules that help you learn how to create such content or modify built-in-content to your needs. We start with KQL, the lingua franca of Azure Microsoft Sentinel. The following modules discuss one of the content building blocks such as rules, playbooks, and workbooks. They wrap up by discussing use cases, which encompass elements of different types that address specific security goals, such as threat detection, hunting, or governance.

Module 10: Kusto Query Language

Most Microsoft Sentinel capabilities use Kusto Query Language (KQL). When you search in your logs, write rules, create hunting queries, or design workbooks, you use KQL.

The next section on writing rules explains how to use KQL in the specific context of SIEM rules.

The recommended journey for learning Microsoft Sentinel KQL

- Pluralsight KQL course: Gives you the basics
- Must Learn KQL: A 20-part KQL series that walks you through the basics of creating your first analytics rule (includes an assessment and certificate)
- The Microsoft Sentinel KQL Lab: An interactive lab that teaches KQL with a focus on what you need for Microsoft Sentinel:
    - Learning module (SC-200 part 4)
    - Presentation or lab URL
    - A Jupyter notebooks version that lets you test the queries within the notebook
    - Learning webinar: YouTube or MP4
    - Reviewing lab solutions webinar: YouTube or MP4
- Pluralsight advanced KQL course
- "Optimizing Azure Microsoft Sentinel KQL queries performance" webinar: YouTube, MP4, or presentation
- "Using ASIM in your KQL queries": YouTube or presentation
- "KQL framework for Microsoft Sentinel: Empowering you to become KQL-savvy" webinar: YouTube or presentation

As you learn KQL, you might also find the following references useful:

- The KQL Cheat Sheet
- Query optimization best practices

Module 11: Analytics

Writing scheduled analytics rules

With Microsoft Sentinel, you can use built-in rule templates, customize the templates for your environment, or create custom rules. The core of the rules is a KQL query; however, there's much more than that to configure in a rule.

To learn the procedure for creating rules, see Create custom analytics rules to detect threats. To learn how to write rules (that is, what should go into a rule, focusing on KQL for rules), view the webinar: YouTube, MP4, or presentation.

SIEM analytics rules have specific patterns. Learn how to implement rules and write KQL for those patterns:

- **Correlation rules**: See Using lists and the "in" operator or using the "join" operator
- **Aggregation**: See Using lists and the "in" operator, or a more advanced pattern handling sliding windows
- **Lookups**: Regular, or approximate, partial and combined lookups
- **Handling false positives**
- **Delayed events:** A fact of life in any SIEM, and they're hard to tackle. Microsoft Sentinel can help you mitigate delays in your rules.
- **Use KQL functions as *building blocks***: Enrich Windows Security Events with parameterized functions.

The blog post "Blob and File storage investigations" provides a step-by-step example of writing a useful analytic rule.

Continue module 11 →

Continue Module 11 ...

Using built-in analytics

Before you embark on your own rule writing, consider taking advantage of the built-in analytics capabilities. They don't require much from you, but it's worthwhile learning about them:

- Use the built-in scheduled rule templates. You can tune those templates by modifying them the same way to edit any scheduled rule. Be sure to deploy the templates for the data connectors you connect, which are listed in the data connector **Next steps** tab.
- Learn more about Microsoft Sentinel machine learning capabilities: YouTube, MP4, or presentation.
- Get the list of Microsoft Sentinel advanced, multi-stage attack detections (Fusion), which are enabled by default.
- View the "Fusion machine learning detections with scheduled analytics rules" webinar: YouTube, MP4, or presentation.
- Learn more about Microsoft Sentinel built-in SOC-machine learning anomalies.
- View the "Customized SOC-machine learning anomalies and how to use them" webinar: YouTube, MP4, or presentation.
- View the "Fusion machine learning detections for emerging threats and configuration UI" webinar: YouTube or presentation.

Module 12: Implementing SOAR

In modern SIEMs, such as Microsoft Sentinel, SOAR makes up the entire process from the moment an incident is triggered until it's resolved. This process starts with an incident investigation and continues with an automated response. The blog post "How to use Microsoft Sentinel for Incident Response, Orchestration and Automation" provides an overview of common use cases for SOAR.

Automation rules are the starting point for Microsoft Sentinel automation. They provide a lightweight method of centralized, automated handling of incidents, including suppression, false-positive handling, and automatic assignment.

To provide robust workflow-based automation capabilities, automation rules use Logic Apps playbooks. To learn more:

- View the "Unleash the automation Jedi tricks and build Logic Apps playbooks like a boss" webinar: YouTube, MP4, or presentation.
- Read about Logic Apps, which is the core technology that drives Microsoft Sentinel playbooks.
- See The Microsoft Sentinel Logic Apps connector, the link between Logic Apps and Microsoft Sentinel.

You'll find dozens of useful playbooks in the *Playbooks* folder on Microsoft Sentinel GitHub site, or read A playbook using a watchlist to inform a subscription owner about an alert for a playbook walkthrough.

Module 13: Workbooks, reporting, and visualization

Workbooks

As the nerve center of your SOC, Microsoft Sentinel is required for visualizing the information it collects and produces. Use workbooks to visualize data in Microsoft Sentinel.

- To learn how to create workbooks, read the Azure Workbooks documentation or watch Billy York's Workbooks training (and accompanying text).
- The mentioned resources aren't Microsoft Sentinel-specific. They apply to workbooks in general. To learn more about workbooks in Microsoft Sentinel, view the webinar: YouTube, MP4, or presentation. Read the documentation.

Workbooks can be interactive and enable much more than just charting. With workbooks, you can create apps or extension modules for Microsoft Sentinel to complement its built-in functionality. You can also use workbooks to extend the features of Microsoft Sentinel. Here are a few examples of such apps:

- The Investigation Insights Workbook provides an alternative approach to investigating incidents.
- Graph visualization of external Teams collaborations enables hunting for risky Teams use.
- The users' travel map workbook allows you to investigate geo-location alerts.
- The Microsoft Sentinel insecure protocols workbook implementation guide, recent enhancements, and overview video) helps you identify the use of insecure protocols in your network.
- Finally, learn how to integrate information from any source by using API calls in a workbook.

You'll find dozens of workbooks in the *Workbooks* folder in the Microsoft Sentinel GitHub. Some of them are available in the Microsoft Sentinel workbooks gallery as well.

Continue module 13 →

Module 13: Workbooks, reporting, and visualization

Reporting and other visualization options

Workbooks can serve for reporting. For more advanced reporting capabilities, such as reports scheduling and distribution or pivot tables, you might want to use:

- Power BI, which natively integrates with Azure Monitor Logs and Microsoft Sentinel.
- Excel, which can use Azure Monitor Logs and Microsoft Sentinel as the data source, and view the "Integrate Azure Monitor Logs and Excel with Azure Monitor" video.
- Jupyter notebooks, a topic that's covered later in the hunting module, are also a great visualization tool.

Module 14: Notebooks

Jupyter notebooks are fully integrated with Microsoft Sentinel. Although considered an important tool in the hunter's tool chest and discussed the webinars in the hunting section below, their value is much broader. Notebooks can serve for advanced visualization, as an investigation guide, and for sophisticated automation.

To understand notebooks better, view the Introduction to notebooks video. Get started using the notebooks webinar (YouTube, MP4, or presentation) or read the documentation. The Microsoft Sentinel Notebooks Ninja series is an ongoing training series to upskill you in notebooks.

An important part of the integration is implemented by MSTICPy, which is a Python library developed by our research team to be used with Jupyter notebooks. It adds Microsoft Sentinel interfaces and sophisticated security capabilities to your notebooks.

- MSTICPy Fundamentals to Build Your Own Notebooks
- MSTICPy Intermediate to Build Your Own Notebooks

Module 15: Use cases and solutions

With connectors, rules, playbooks, and workbooks, you can implement *use cases*, which is the SIEM term for a content pack that's intended to detect and respond to a threat. You can deploy Microsoft Sentinel built-in use cases by activating the suggested rules when you're connecting each connector. A *solution* is a group of use cases that address a specific threat domain.

The "Tackling Identity" webinar (YouTube, MP4, or presentation) explains what a use case is and how to approach its design, and it presents several use cases that collectively address identity threats.

Another relevant solution area is *protecting remote work*. View our Ignite session on protecting remote work, and read more about the following specific use cases:

- Microsoft Teams hunting use cases and Graph visualization of external Microsoft Teams collaborations
- Monitoring Zoom with Microsoft Sentinel: custom connectors, analytic rules, and hunting queries.
- Monitoring Azure Virtual Desktop with Microsoft Sentinel: use Windows Security Events, Microsoft Entra sign-in logs, Microsoft Defender XDR for Endpoints, and Azure Virtual Desktop diagnostics logs to detect and hunt for Azure Virtual Desktop threats.
- Monitor Microsoft Intune using queries and workbooks.

And finally, focusing on recent attacks, learn how to monitor the software supply chain with Microsoft Sentinel.

Microsoft Sentinel solutions provide in-product discoverability, single-step deployment, and enablement of end-to-end product, domain, and/or vertical scenarios in Microsoft Sentinel. For more information, see About Microsoft Sentinel content and solutions, and view the "Create your own Microsoft Sentinel solutions" webinar: YouTube or presentation.

Part 4: Operating

Module 16: Handling incidents

After you build your SOC, you need to start using it. The "day in an SOC analyst's life" webinar (YouTube, MP4, or presentation) walks you through using Microsoft Sentinel in the SOC to *triage*, *investigate*, and *respond* to incidents.

To help enable your teams to collaborate seamlessly across the organization and with external stakeholders, see Integrating with Microsoft Teams directly from Microsoft Sentinel. And view the "Decrease your SOC's MTTR (Mean Time to Respond) by integrating Microsoft Sentinel with Microsoft Teams" webinar.

You might also want to read the documentation article on incident investigation. As part of the investigation, you'll also use the entity pages to get more information about entities related to your incident or identified as part of your investigation.

Incident investigation in Microsoft Sentinel extends beyond the core incident investigation functionality. You can build additional investigation tools by using workbooks and notebooks, Notebooks are discussed in the next section, Module 17: Hunting. You can also build more investigation tools or modify existing ones to your specific needs. Examples include:

- The Investigation Insights Workbook provides an alternative approach to investigating incidents.
- Notebooks enhance the investigation experience. Read Why use Jupyter for security investigations?, and learn how to investigate by using Microsoft Sentinel and Jupyter notebooks:
  - Part 1
  - Part 2
  - Part 3

Module 17: Hunting

Although most of the discussion so far has focused on detection and incident management, *hunting* is another important use case for Microsoft Sentinel. Hunting is a **proactive search for threats** rather than a reactive response to alerts.

The hunting dashboard is constantly updated. It shows all the queries that were written by the Microsoft team of security analysts and any extra queries that you've created or modified. Each query provides a description of what it's hunting for, and what kind of data it runs on. These templates are grouped by their various tactics. The icons at the right categorize the type of threat, such as initial access, persistence, and exfiltration. For more information, see Hunt for threats with Microsoft Sentinel.

To understand more about what hunting is and how Microsoft Sentinel supports it, view the introductory "Threat hunting" webinar: YouTube, MP4, or presentation. The webinar starts with an update on new features. To learn about hunting, start at slide 12. The YouTube video is already set to start there.

Although the introductory webinar focuses on tools, hunting is all about security. Our security research team webinar (YouTube, MP4, or presentation) focuses on how to actually hunt.

The follow-up webinar, "AWS threat hunting by using Microsoft Sentinel" (YouTube, MP4, or presentation) drives the point by showing an end-to-end hunting scenario on a high-value target environment.

Finally, you can learn how to do SolarWinds post-compromise hunting with Microsoft Sentinel and WebShell hunting, motivated by the latest recent vulnerabilities in on-premises Microsoft Exchange servers.

Module 18: User and Entity Behavior Analytics (UEBA)

The newly introduced Microsoft Sentinel User and Entity Behavior Analytics (UEBA) module enables you to identify and investigate threats inside your organization and their potential impact, whether they come from a compromised entity or a malicious insider.

As Microsoft Sentinel collects logs and alerts from all its connected data sources, it analyzes them and builds baseline behavioral profiles of your organization's entities (such as *users*, *hosts*, *IP addresses*, and *applications*) across time and peer-group horizon. Through various techniques and machine learning capabilities, Microsoft Sentinel can then identify anomalous activity and help you determine whether an asset has been compromised. Not only that, but it can also figure out the relative sensitivity of particular assets, identify peer groups of assets, and evaluate the potential impact of any given compromised asset (its "blast radius"). Armed with this information, you can effectively prioritize your investigation and incident handling.

Learn more about UEBA by viewing the webinar (YouTube, MP4, or presentation), and read about using UEBA for investigations in your SOC.

To learn about the most recent updates, view the "Future of Users Entity Behavioral Analytics in Microsoft Sentinel" webinar.

Module 19: Monitoring Microsoft Sentinel's health

Part of operating a SIEM is making sure that it works smoothly and is an evolving area in Azure Microsoft Sentinel. Use the following to monitor Microsoft Sentinel's health:

- Measure the efficiency of your Security operations (video).

- The Microsoft Sentinel Health data table provides insights on health drifts, such as latest failure events per connector, or connectors with changes from success to failure states, which you can use to create alerts and other automated actions. For more information, see Monitor the health of your data connectors. View the "Data Connectors Health Monitoring Workbook" video. And get notifications on anomalies.

- Monitor agents by using the agents' health solution (Windows only) and the Heartbeat table (Linux and Windows).

- Monitor your Log Analytics workspace: YouTube, MP4, or presentation, including query execution and ingestion health.

- Cost management is also an important operational procedure in the SOC. Use the Ingestion Cost Alert Playbook to ensure that you're always aware of any cost increases.

Part 5: Advanced

Module 20: Extending and integrating by using the Microsoft Sentinel APIs

As a cloud-native SIEM, Microsoft Sentinel is an API-first system. Every feature can be configured and used through an API, enabling easy integration with other systems and extending Microsoft Sentinel with your own code. If API sounds intimidating to you, don't worry. Whatever is available by using the API is also available by using PowerShell.

To learn more about the Microsoft Sentinel APIs, view the short introductory video and read the blog post. For a deeper dive, view the "Extending and integrating Sentinel (APIs)" webinar (YouTube, MP4, or presentation), and read the blog post Extending Microsoft Sentinel: APIs, integration, and management automation.

Module 21: Build-your-own machine learning

Microsoft Sentinel provides a great platform for implementing your own machine learning algorithms. We call it the *Build-your-own machine learning model*, or BYO ML. BYO ML is intended for advanced users. If you're looking for built-in behavioral analytics, use our machine learning analytics rules or UEBA module, or write your own behavioral analytics KQL-based analytics rules.

To start with bringing your own machine learning to Microsoft Sentinel, view the "Build-your-own machine learning model" video, and read the Build-your-own machine learning model detections in the AI-immersed Azure Sentinel SIEM blog post. You might also want to refer to the BYO ML documentation.

Next Steps, Recommended Content and Certification Readiness

Next steps

- Pre-deployment activities and prerequisites for deploying Microsoft Sentinel
- Quickstart: Onboard Microsoft Sentinel
- What's new in Microsoft Sentinel

Recommended content

- Best practices for Microsoft Sentinel
- Microsoft Sentinel sample workspace designs
- Plan costs and understand Microsoft Sentinel pricing and billing
- Roles and permissions in Microsoft Sentinel
- Deploy Microsoft Sentinel side-by-side with an existing SIEM

Microsoft Learn and Certification

- Microsoft Sentinel formal learning path
- Certification: Microsoft Certified: Security Operations Analyst Associate
- Exam: SC-200: Microsoft Security Operations Analyst – Study Guide
- Exam: SC-200: Practice Assessment
- Exam: SC-200: EXAM SANDBOX demo experience
- Exam SC-200: prep video

Thank You