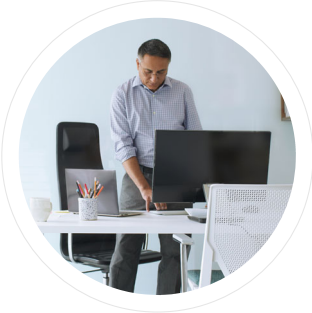
Microsoft Security

SC-200 Microsoft Security Operations Analyst

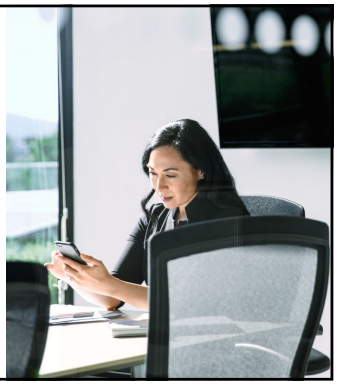
Ben McGee
11/20/2022



1

Microsoft Security

Module 7: Create detections and perform investigations using Microsoft Sentinel



2

Module agenda

- Threat detection with Microsoft Sentinel analytics
- Threat response with Microsoft Sentinel playbooks
- Security incident management in Microsoft Sentinel
- User and entity behavior analytics in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel

3

Lesson 1: Threat detection with Microsoft Sentinel analytics

4

Lesson introduction

After this lesson, you will be able to:

- Explain the importance of Microsoft Sentinel Analytics.
- Explain different types of analytics rules.
- Create rules from templates.
- Create new analytics rules and queries using the analytics rule wizard.
- Manage rules with modifications.

5

Microsoft Sentinel Analytics explained

Overview

Microsoft Sentinel Analytics analyzes data from various sources to identify correlations and anomalies.

By using analytics rules, you can trigger alerts based on the attack techniques that are used by known malicious actors.

You can set up these rules to help ensure your SOC is alerted to potential security incidents in your environment in a timely fashion.

Common security analytics use cases include:

- Identification of compromised accounts
- User behavior analysis to detect potentially suspicious patterns
- Network traffic analysis to locate trends indicating potential attacks
- Detection of data exfiltration by attackers
- Detection of insider threats

6

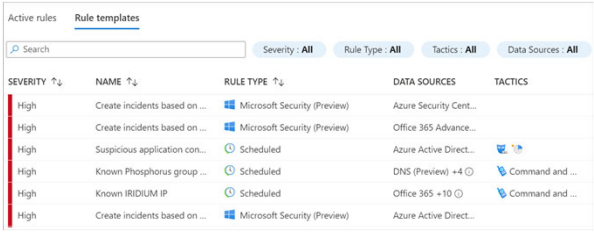
Types of analytics rules

- Microsoft security
- Fusion
- Machine learning (ML) behavioral analytics
- Anomaly (preview)
- Scheduled
- Near-real-time (NRT) (preview)

7

Create an analytics rule from a template

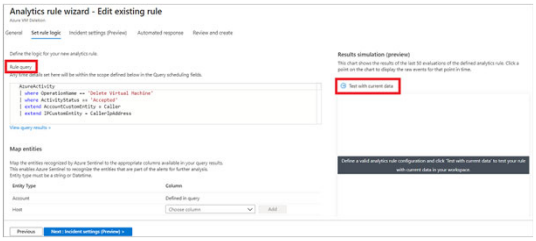
The Analytics section in Microsoft Sentinel contains rule templates that are preloaded from the Microsoft Sentinel GitHub repository. You can use these templates to create a rule to detect security threats.



8

Create an analytics rule from a wizard

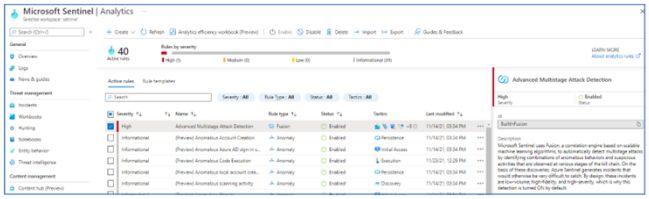
Creating a custom rule from the scheduled query rule type provides you with the highest level of customization. You can define, your own KQL code, set a schedule to run the alerts, or provide an automated action by associating a Microsoft Sentinel Playbook.



9

Manage analytics rules

To adjust the noise and filter the more important threats detected, you should manage the analytics rules on an ongoing basis. This will help ensure that your rules remain useful and efficient in detecting potential security threats.



10

Lesson 3: Security incident management in Microsoft Sentinel

11

Lesson introduction

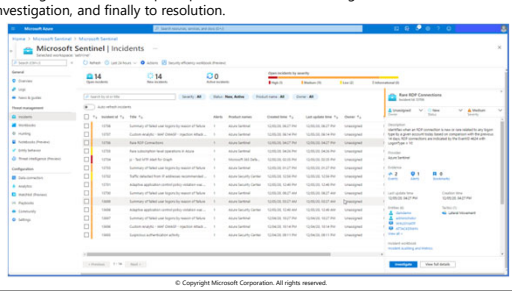
After this lesson, you will be able to:

- Explain Microsoft Sentinel incident management
- Explore Microsoft Sentinel evidence and entity management
- Investigate and manage incident resolution

12

Describe incident management

Incident management is the complete process of incident investigation, from creation, to in-depth investigation, and finally to resolution.



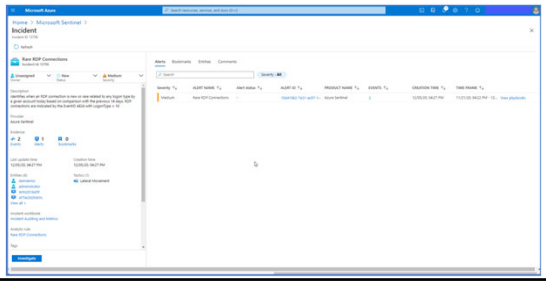
13

Explain evidence and entities

14

Investigate incidents

Incident management is the complete process of incident investigation, from creation, to in-depth investigation, and finally to resolution.



15

Lesson 2: Threat response with Microsoft Sentinel playbooks

16

Lesson introduction

After this lesson, you will be able to:

- Explain Microsoft Sentinel SOAR capabilities
- Explore the Microsoft Sentinel Logic Apps connector
- Create a playbook to automate an incident response
- Run a playbook on demand in response to an incident

17

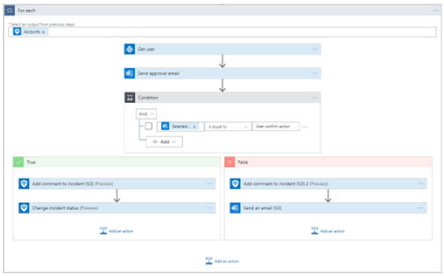
Microsoft Sentinel playbooks explained

Microsoft Sentinel as a SIEM and SOAR solution Security Orchestration, Automation and Response (SOAR) solution	**Microsoft Sentinel playbooks** Security playbooks are collections of procedures based on Azure Logic Apps that run in response to an alert.	**Azure Logic Apps** Azure Logic Apps is a cloud service that automates the operation of your business processes.
Logic Apps Connector A connector is a component that provides an interface to a service.	**Triggers and Actions** A trigger is an event that occurs when a specific set of conditions is satisfied. An action is an operation that performs a task.	**Microsoft Sentinel Logic Apps connector** A Microsoft Sentinel playbook uses a Microsoft Sentinel Logic Apps connector.

18

Create a Logic App

The Logic App Designer provides a design canvas that you use to add a trigger and actions to your workflow.



19

Run a playbook on demand

1. Manually from an Incident
2. Automatically from an Analytics Rule

20

Lesson 4: User and entity behavior analytics in Microsoft Sentinel

21

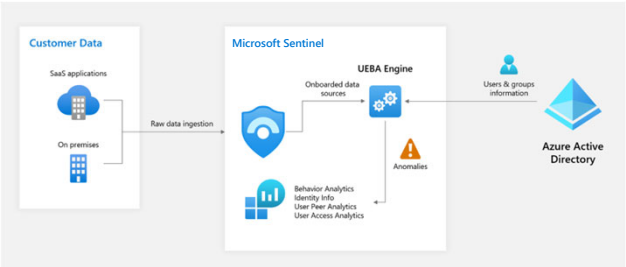
Lesson introduction

After this lesson, you will be able to:

- Explain User and Entity Behavior Analytics in Microsoft Sentinel
- Explore entities in Microsoft Sentinel

22

User and entity behavior analytics explained



23

Explore entity behavior information

The Entity behavior page allows you to search for entities or select from the list of already displayed entities. Once selected the Entity page is displayed with information and timeline of alerts and activities

24

Display entities timeline

25

Lesson 5: Query, visualize, and monitor data in Microsoft Sentinel

26

Lesson introduction

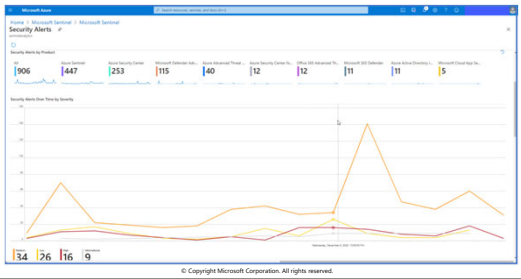
After this lesson, you will be able to:

- Visualize security data using Microsoft Sentinel Workbooks
- Explain Workbook queries
- Explore Workbook capabilities
- Create a Microsoft Sentinel Workbook

27

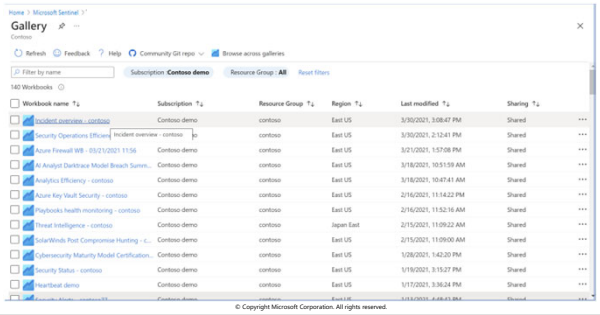
Microsoft Sentinel Workbooks

Workbooks provide a dashboard like interface. There are Workbooks provided by Microsoft Sentinel and the community. You can also create your own Workbooks.



28

Create a new Microsoft Sentinel Workbook



29

Knowledge check

Check your knowledge with the module quiz in your course viewer

30

Lab 01 – Create detections and perform investigations using Microsoft Sentinel

31

Lab Exercises for module 7

1. Activate a Microsoft Security rule
2. Create a playbook
3. Create a scheduled query
4. Understand detection modeling
5. Conduct attacks
6. Create detections
7. Investigate incidents
8. Create workbooks

32

Microsoft Security

33