



Lab Manual- Configure Analytics Rules for Azure Sentinel

Prepared for:

Date: 18th Nov 2021

Prepared by:

Document Name: Lab Manual

Document Number AZLabn991

Contributor:

Contents

1.	Introduction.....	3
2.	Lab: Analytics Rules overview	3
2.1	Enable Microsoft Incident Creation Rule.....	7
2.2	Exercise 3: Review Fusion Rule (Advanced Multistage Attack Detection)	10
2.3	Exercise 4: Create Microsoft Sentinel custom analytics rule	12
2.4	Exercise 5: Review resulting security incident	17

1. Introduction

Microsoft Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Defender for Cloud Apps, security alerts from Microsoft Defender for Cloud, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Microsoft Sentinel

In this Lab , we will understand how to create an Azure sentinel workspace and connect with Data source

2. Lab: Analytics Rules overview

1. Open your newly created Microsoft Sentinel instance.
2. On the left menu navigate to analytics and select **Rule template** section
3. Review the analytics rules templates that ship with the product.

The screenshot displays the Microsoft Sentinel Analytics dashboard. The left-hand navigation pane is visible, with the 'Analytics' option highlighted by a red box. The main content area shows the 'Rule templates' section, also highlighted by a red box. At the top, it indicates '55 Active rules' and a 'Rules by severity' breakdown: High (2), Medium (2), and Low (0). Below this, a table lists various rule templates. The first row is marked 'IN USE' and is titled 'Advanced Multistage Attack Detection'. The table columns are 'Severity', 'Name', and 'Rule type'.

Severity	Name	Rule type
High	IN USE Advanced Multistage Attack Detection	Fusion
High	Suspicious application consent similar to O365 Attack Too...	Scheduled
High	SUNBURST and SUPERNOVA backdoor hashes	Scheduled
High	Dev-0228 File Path Hashes November 2021 (ASIM Version)	Scheduled
High	New EXE deployed via Default Domain or Default Domain...	Scheduled
High	Cognni Incidents for Highly Sensitive HR Information	Scheduled
High	Create Incident for XDR Alerts (Medium & Low)	Scheduled
High	Alsld DCShadow	Scheduled
High	Dumping LSASS Process Into a File	Scheduled
High	SOURGUM Actor IOC - July 2021	Scheduled
High	ACTINIUM Actor IOCs - Feb 2022	Scheduled
High	Bulk Changes to Privileged Account Permissions	Scheduled
High	Log4j vulnerability exploit aka Log4Shell IP IOC	Scheduled
High	Vectra AI Detect - Detections with High Severity	Scheduled
High	Known PHOSPHORUS group domains/IP - October 2020	Scheduled
High	Alsld LSASS Memory	Scheduled
High	Azure WAF matching for Log4j vuln(CVE-2021-44228)	Scheduled

4. On the analytics rule filter select **Data sources** and check **security Event**

Active rules

Rule templates

Severity : All

Rule Type : All

Tactics : All

Data Sources : All

Less

Search

SEVERITY ↑↓	NAME ↑↓	DATA SOURCES
High	Create incidents based on Azure	Security Events
High	SUNBU	Microsoft Defender fo...
High	Solorig	Microsoft 365 Defend...
High	THALL	Azure Monitor (... +2 ⓘ)
High	SUPER	DNS (Preview) +4 ⓘ
High	HAFNI	Azure Monitor (IIS)
High	Alsid D	Security Events +1 ⓘ
High	Alsid P	Alsid for Active Direct...
High	Correla	Alsid for Active Direct...
High	Known	Azure Active Directory...
High	Azure	Cisco ASA +2 ⓘ
High	Known	DNS (Preview) +3 ⓘ
High	User Lc	Okta Single Sign-On (...)

Data Sources

Security Events

Select all

Microsoft Defender for Identity (Preview)

Microsoft Defender for Office 365 (Preview)

Office 365

Okta Single Sign-On (Preview)

Palo Alto Networks

Proofpoint On Demand Email Security (Preview)

Proofpoint TAP (Preview)

Pulse Connect Secure (Preview)

Qualys Vulnerability Management (Preview)

Security Events via Le

Sophos XG Firewall (Preview)

5. Review all the analytic rules on the above data source.

■ High (2)

■ Medium (2)

■ Low (0)

■ Informational (51)

Rule templates

+ Add filter

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics
High	New EXE deployed via Default Domain or Default Domain...	Scheduled	Security Events via Legacy Agent	Tactics
High	Dumping LSASS Process Into a File	Scheduled	Security Events via Legacy Agent	Credential Access
High	SOURGUM Actor IOC - July 2021	Scheduled	DNS (Preview) +14	Persistence
High	ACTINIUM Actor IOCs - Feb 2022	Scheduled	DNS (Preview) +10	Persistence
High	Log4j vulnerability exploit aka Log4Shell IP IOC	Scheduled	Office 365 +13	Command and Control
High	MSHTML vulnerability CVE-2021-40444 attack	Scheduled	Security Events via Legacy Agent +1	Execution
High	Known Barium IP	Scheduled	Amazon Web Services S3 +18	Command and Control
High	DEV-0322 Serv-U related IOCs - July 2021	Scheduled	DNS (Preview) +12	Initial Access
High	HAFNIUM UM Service writing suspicious file	Scheduled	Security Events via Legacy Agent +3	Initial Access
High	Non Domain Controller Active Directory Replication	Scheduled	Security Events via Legacy Agent	Credential Access
High	Credential Dumping Tools - Service Installation	Scheduled	Security Events via Legacy Agent	Credential Access
High	Security Service Registry ACL Modification	Scheduled	Security Events via Legacy Agent +3	Defense Evasion
High	Known ZINC related maldoc hash	Scheduled	Cisco ASA +2	Command and Control
High	Known ZINC Comebacker and Klackring malware hashes	Scheduled	DNS (Preview) +12	Execution
High	New EXE deployed via Default Domain or Default Domain...	Scheduled	Security Events via Legacy Agent	Tactics
High	Exchange OAB Virtual Directory Attribute Containing Pote...	Scheduled	Security Events via Legacy Agent +1	Initial Access
High	Known NICKEL domains and hashes	Scheduled	Squid Proxy (Preview) +11	Command and Control
High	NOBELIUM IOCs related to FoggyWeb backdoor	Scheduled	F5 Networks +11	Collection
High	Credential Dumping Tools - File Artifacts	Scheduled	Security Events via Legacy Agent	Credential Access
High	DSRM Account Abuse	Scheduled	Security Events via Legacy Agent	Persistence
High	Known IRIDIUM IP	Scheduled	Amazon Web Services S3 +19	Command and Control
High	DEV-0586 Actor IOC - January 2022	Scheduled	Cisco ASA +4	Impact
High	Exchange Virtual Directory Attribute Containing Potenti...	Scheduled	Security Events via Legacy Agent +2	Tactics

5. In the rule search bar type **Rare RDP Connections** for the rule name.
6. To review the rule logic and possible configuration options, in the right lower corner press **create rule**.

Create

Refresh

Analytics efficiency workbook (Preview)

Enable

Disable

Delete

Import

Export

Guides & Feedback

55

Active rules

Rules by severity

High (2)

Medium (2)

Low (0)

Informational (51)

LEARN MORE

About analytics rules

Active rules

Rule templates

rare

Data Sources: Security Events via Legacy Agent

Add filter

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics	Techniques
Medium	Rare RDP Connections	Scheduled	Security Events via Legacy Agent +2	Lateral Movement	T1021
Informational	INUSE (Preview) Rare privileged process calls on a daily b...	Anomaly	Security Events via Legacy Agent	Initial Access	T1078

Rare RDP Connections

Medium

Scheduled

Description

Identifies when an RDP connection is new or rare related to any logon type by a given account today based on comparison with the previous 14 days. RDP connections are indicated by the EventID 4624 with LogonType = 10

Data sources

Security Events via Legacy Agent

SecurityEvents --

Windows Security Events via AMA

SecurityEvents --

Windows Forwarded Events (Preview)

WindowsEvents --

Tactics and techniques

Lateral Movement (1)

Rule query

```
let starttime = 14d;
let endtime = 1d;
union isfuzzy=true
  (SecurityEvent
    | where TimeGenerated >= ago(endtime)
    | where EventID == 4624 and LogonType == 10
```

Rule frequency

Run query every 1 day

Rule period

Last 14 days data

Note:

You haven't used this template yet; you can use it to create analytics rules.

One or more data sources used by this rule is missing. This might limit the functionality of the rule.

Create rule

< Previous

Page 1 of 1

Next >

Analytics rule wizard - Create new rule from tem

General Set rule logic Incident settings Automated response Review and

Analytics rule details

Rare RDP Connections

Identifies when an RDP connection is new or rare related to any logon type by a given account today based on comparison with the previous 14 days.
RDP connections are indicated by the EventID 4624 with LogonType = 10

2 selected

6. Press **Next: Set rule logic** in the bottom of the page

Home > Microsoft Sentinel > Microsoft Sentinel >

Analytics rule wizard - Create new rule from template

Rare RDP Connections

General **Set rule logic** Incident settings Automated response Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
let starttime = 14d;  
let endtime = 1d;  
(union isfuzzy=true  
(SecurityEvent  
| where TimeGenerated >= ago(endtime)  
| where EventID == 4624 and LogonType == 10  
| extend CustomEntity = if(TimeGenerated >= ago(endtime), SecurityEvent, null()))
```

[View query results >](#)

Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. [Learn more >](#)

Account

FullName

AccountCustomEntity

+ Add identifier

Host

FullName

HostCustomEntity

+ Add identifier

IP

Address

IPCustomEntity

+ Add identifier

+ Add new entity

Custom details

Previous **Next : Incident settings >**

7. in the rule logic screen, you have the ability to create or modify the rule KQL query, control of the entity mapping and define the scheduling and lookback time range.
8. After you reviewed the rule configuration options, close this page and navigate back to the main Microsoft Sentinel Overview screen

2.1 Enable Microsoft Incident Creation Rule

Microsoft Sentinel is a cloud-native SIEM and as such, it acts as single pane of glass for alerts and event correlation. For this purpose, and to be able to ingest and surface alerts from Microsoft Security Products, we create a **Microsoft incident creation rule**. In this exercise, we will review this feature and create one example rule with a filtering option to help the analyst deal with alert fatigue.

1. In Microsoft Sentinel main page press on the **Analytics** section.
2. In the top bar press on **+Create** and select **Microsoft incident creation rule**

Microsoft Sentinel | Analytics ...
Selected workspace: 'sentinaldemo'

Search (Ctrl+/) « **Create** Refresh Analytics efficiency workbook (Preview) Enable Disable Delete Import Export Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics**
- Watchlist
- Automation
- Settings

Scheduled query rule by severity

Microsoft incident creation rule (2) Medium (2) Low (0) Informational (51)

NRT query rule

Active rules Rule templates

Search: rare Data Sources: Security Events via Legacy Agent Add filter

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics	Techniques
Medium	Rare RDP Connections	Scheduled	Security Events via Legacy Agent +2	Lateral Movement	T1021
Informational	IN USE (Preview) Rare privileged process calls on a daily b...	Anomaly	Security Events via Legacy Agent	Initial Access	T1078

High	Vectra AI Detect - Detections with High Severity	Scheduled
High	Known PHOSPHORUS group domains/IP - October 2020	Scheduled
High	Alsld LSASS Memory	Scheduled
High	Azure WAF matching for Log4j vuln(CVE-2021-44228)	Scheduled

3. In the rule name enter "**Azure Defender only medium and high Alerts**"
4. In the **Microsoft security service** dropdown select **Azure Defender**
5. In the **Filter by severity** select **custom** and mark **High** and **Medium**

Analytics rule wizard - Create a new microsoft incident creation rule ...

General Automated response Review and create

Create an analytics rule that creates incidents based on alerts generated in another Microsoft security service.

Analytics rule details

Name *

Azure Defender only medium and high Alerts ✓

Description

Status

Enabled Disabled

Analytics rule logic

Microsoft security service *

Microsoft Defender for Cloud ✓

Filter by severity

☐ Any
☒ Custom

*

High, Medium ✓

- ☒ High
- ☒ Medium
- ☐ Low
- ☐ Informational

Only create incidents from alerts that do not contain the following text in the alert name

+ Add

Next : Automated response >

6. Press **Next: Automated response**

7. In the above "**Automated response**" page you can attach automation rule that can generate automation tasks that can assist your SOC with repetitive tasks, or Security remediation. More in this topic in the SOAR module.

[Home](#) > [Microsoft Sentinel](#) > [Microsoft Sentinel](#) >

Analytics rule wizard - Create a new microsoft incident creation rule ...

General Automated response Review and create

Incident automation

View all automation rules that will be triggered by this analytics rule and create new automation rules. The automation rule will receive the incident as its input, as will any playbooks called by the automation rule. Only playbooks configured with the incident trigger can be called by automation rules.

+ Add new

Order

Automation rule name

No automation rules

8. Press **Next: Review** and **create** in the next page.



Azure Sentinel | Analytics

Selected workspace: 'sentinellabws'

» + Create ▾ ↻ Refresh Analytics efficiency workbook (Preview) | ⏻ Enable ⏻ Disable 🗑️ D



4

Active rules

Rules by severity

■ High (3) ■ Medium (1) ■ Low (0) ■ Informational (0)

Active rules

Rule templates

Severity : All

Rule Type : All

▾ More (2)

<input type="checkbox"/> SEVERITY ↑↓	NAME ↑↓	RULE TYPE ↑↓
<input type="checkbox"/> High	Advanced Multistage Attack Detection	Fusion
<input type="checkbox"/> High	Solorigate Network Beacon	Scheduled
<input type="checkbox"/> High	Azure Defender only medium and high Alerts	Microsoft Security
<input type="checkbox"/> Medium	Sign-ins from IPs that attempt sign-ins to disabled accounts	Scheduled

2.2 Exercise 3: Review Fusion Rule (Advanced Multistage Attack Detection)

Fusion rule is a unique kind of detection rule. With Fusion rule, Microsoft Sentinel can automatically detect multistage attacks by identifying combinations of anomalous behaviors and suspicious activities That are observed at various stages of the kill-chain.

In this exercise we will learn how to distinguish and review **Fusion rule** in Microsoft Sentinel.

1. In the analytics page rule template tab, use the **Rule Type** filter and select **Fusion**

Active rules Rule templates

Severity : All

Rule Type : All

Tactics : All

Data Sources : All


SEVERITY ↑↓	NAME ↑↓			
High	IN USE TEARDROP memory-only dropper			
High	Alsid Password Guessing			
High	IN USE Solorigate Named Pipe			
High	IN USE Modified domain federation trust settings			
High	IN USE Create incidents based on Azure Active Directory			
High	IN USE First access credential added to Application or Ser			

Rule Type

☒ Select all
☐ Scheduled
☒ Fusion
☐ Microsoft Security
☐ ML Behavior Analytics

2. In the template screen notice the tag **IN USE** as this rule template enabled by default.

3. Press on the rule and review the data sources in the rule right pane.

 **Advanced Multistage Attack Detection**

High Severity	Fusion Rule Type
<p>Description</p> <p>Using Fusion technology based on machine learning, Azure Sentinel automatically detects multistage attacks by identifying combinations of anomalous behaviors and suspicious activities observed at various stages of the kill chain. On the basis of these discoveries, Azure Sentinel generates incidents that would otherwise be very difficult to catch. By design, these incidents are low-volume, high-fidelity, and high-severity, which is why this detection is turned ON by default.</p> <p>There are a total of 90 Fusion incident types detected by Azure Sentinel.</p> <p>To detect these multistage attacks, the following data connectors must be configured:</p> <ul style="list-style-type: none">• Azure Active Directory Identity Protection.• Microsoft Cloud App Security.• Microsoft Defender for Endpoint.• Azure Defender.• Palo Alto Networks. <p>For a full list and description of each scenario that is supported for these multistage attacks, go to https://aka.ms/SentinelFusion.</p>	

As Fusion rules produce security incidents with high fidelity and simulation can be challenging, we are adding an example of an incident that was created from fusion detection.

In the below example we are seeing 2 low severity alerts from **Azure Active Directory Identity Protection** and **Microsoft Cloud App Security** that stich together into high severity incidence:

Home > Azure Sentinel > Azure Sentinel >

Incident ...

Incident ID: 18399

Refresh Create automation rule (Preview)

Sign-in from an unfamiliar location leading to Mass ...

Incident ID: 18399

Unassigned Owner New Status High Severity

Description

This is an indication of a sign in by 40bab4f8-5536-4bcb-97a0-51b01bb39fa2 from (Dublin,Leinster, IE), an unfamiliar location. Next, The user JeffL@seccxp.ninja deleted more than 9,448 unique objects in a single session. Additional risks in this user session: This user uploaded 1540 unique objects in a single session. This user impersonated 3 different accounts in a single session. For more information about this detection, please see <https://docs.microsoft.com/en-us/azure/sentinel/fusion>.

Alert product names

- Azure Active Directory Identity Protection
- Microsoft Cloud App Security

Evidence

N/A 2 Alerts 0 Bookmarks

Last update time: 05/02/21, 01:44 AM Creation time: 05/02/21, 01:44 AM

Entities (2)

JeffL@seccxp.ninja 52.210.179.58 View full details >

Incident workbook

Incident Overview

Analytics rule

Advanced Multistage Attack Detection

Tags

Investigate

Timeline (Preview) Alerts Bookmarks Entities Comments

Search

Timeline content: All Severity: All Tactics: All

May 1 3:29 PM **Mass delete** Low | Detected by Microsoft Cloud App Security | Tactics: -- View playbooks

May 1 2:55 PM **UnfamiliarLocation** Low | Detected by Azure Active Directory Identity Protection | Tactics: -- View playbooks

2.3 Exercise 4: Create Microsoft Sentinel custom analytics rule

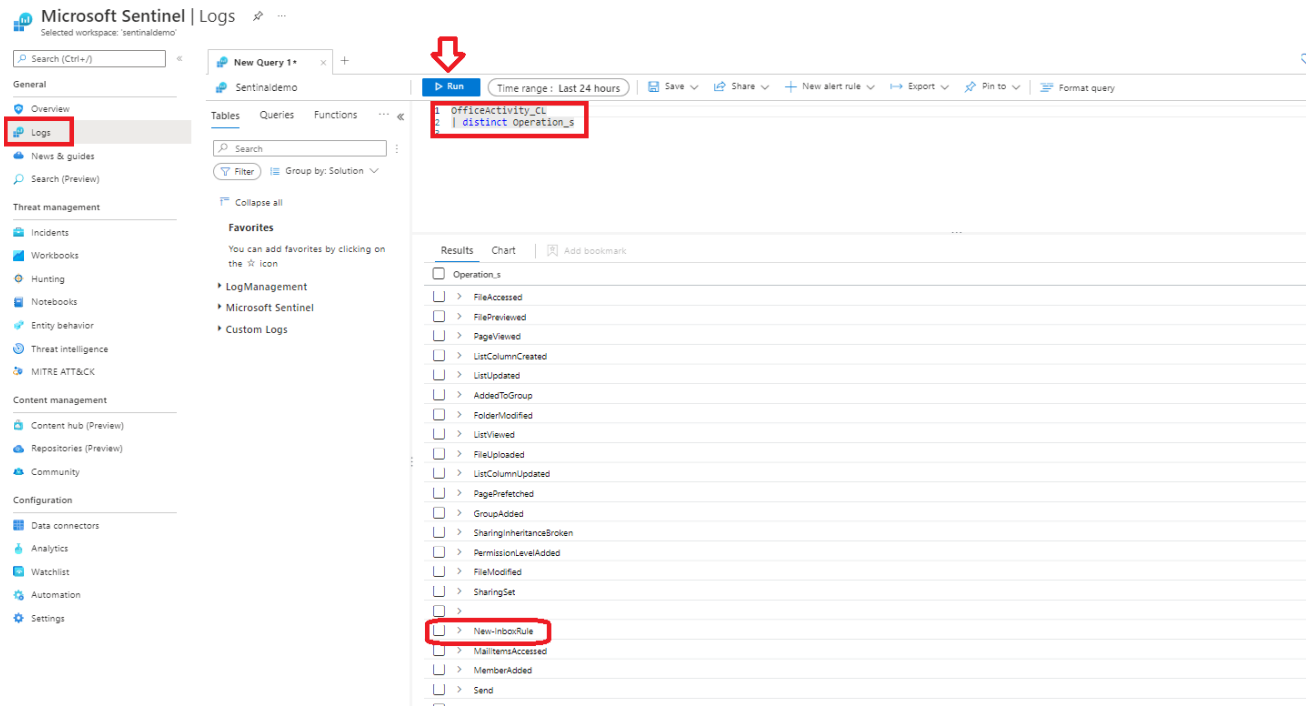
Your Security consult notify you about this thread

https://www.reddit.com/r/sysadmin/comments/7kyp0a/recent_phishing_attempts_my_experience_and_what/ Base on the attack vector and the organization risk he recommend you to create detection rule for this malicious activity. In this exercise you will use Microsoft Sentinel analytics rule wizard to create new detection.

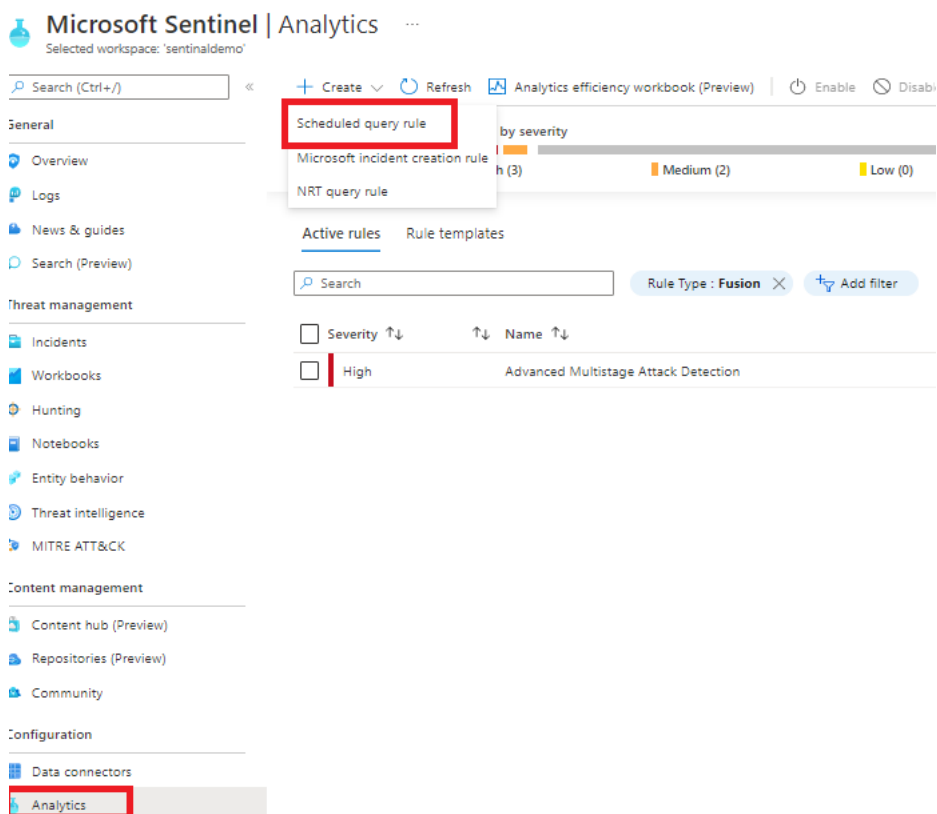
1. Review the article in the above link and understand what is the data source that will be part of the detection.
2. Check if this operation are capture as part of your collection strategy:
 - In the left menu press on the **Logs** and navigate to the search canvas

important note: in this lab we are using custom logs that replace the Out-of-the-box tables

- Run the search query below to see the list of activities Microsoft Sentinel captured in the last 24hr
- OfficeActivity_CL
| distinct Operation_s
- As you can see the **New-InboxRule** operation is indeed captured in your logs.



3. In the analytics rule page, in the top bar press on **+Create** and select **scheduled query Rule**



4. In this screen we will add general information regarding this rule.
5. In the **Name** type "**Malicious Inbox Rule - custom**".
6. In the rule **Description** add **This rule is detecting on delete all traces of phishing email from user mailboxes**.
7. In the **Tactics** select **Persistence** and **Defense Evasion**.

Analytics rule wizard - Create a new scheduled rule

General Set rule logic Incident settings Automated response Review and create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *

Malicious Inbox Rule - custom ✓

Description

This rule is detecting on delete all traces of phishing email from user mailboxes. ✓

Tactics and techniques

2 selected

- ☐ Reconnaissance
- ☐ Resource Development
- ☐ Initial Access
- ☐ Execution
- ☒ Persistence
- ☐ T1098 - Account Manipulation
- ☐ T1197 - BITS Jobs
- ☐ T1547 - Boot or Logon Autostart Execution
- ☐ T1037 - Boot or Logon Initialization Scripts
- ☐ T1176 - Browser Extensions
- ☐ T1554 - Compromise Client Software Binary
- ☐ T1136 - Create Account
- ☐ T1543 - Create or Modify System Process
- ☐ T1546 - Event Triggered Execution
- ☐ T1133 - External Remote Services
- ☐ T1574 - Hijack Execution Flow
- ☐ T1525 - Implant Internal Image
- ☐ T1556 - Modify Authentication Process
- ☐ T1137 - Office Application Startup
- ☐ T1542 - Pre-OS Boot
- ☐ T1053 - Scheduled Task/Job
- ☐ T1505 - Server Software Component

Next: Set rule logic >

8. In the rule **severity** select **medium**.
9. Press **Next: SET rule logic**.
10. In the **Rule logic** page, review and copy the above query

```
let Keywords = dynamic(["helpdesk", " alert", " suspicious", "fake", "malicious",
"phishing", "spam", "do not click", "do not open", "hijacked", "Fatal"]);
OfficeActivity_CL
| where Operation_s =~ "New-InboxRule"
| where Parameters_s has "Deleted Items" or Parameters_s has "Junk Email"
| extend Events=todynamic(Parameters_s)
| parse Events with * "SubjectContainsWords" SubjectContainsWords '*'
| parse Events with * "BodyContainsWords" BodyContainsWords '*'
| parse Events with * "SubjectOrBodyContainsWords" SubjectOrBodyContainsWords '*'
| where SubjectContainsWords has_any (Keywords)
or BodyContainsWords has_any (Keywords)
or SubjectOrBodyContainsWords has_any (Keywords)
| extend ClientIPAddress = case( ClientIP_s has ".", tostring(split(ClientIP_s,":")[0]),
ClientIP_s has "[", tostring(trim_start(@['['],tostring(split(ClientIP_s,"") [0]))),
ClientIP_s )
| extend Keyword = iff(isnotempty(SubjectContainsWords), SubjectContainsWords,
(iff(isnotempty(BodyContainsWords),BodyContainsWords,SubjectOrBodyContainsWords )))
| extend RuleDetail = case(OfficeObjectId_s contains '/',
tostring(split(OfficeObjectId_s, '/')[-1]) , tostring(split(OfficeObjectId_s, '\\')[-
1]))
```

```
| summarize count(), StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated)
by Operation_s, UserId_s, ClientIPAddress, ResultStatus_s, Keyword,
OriginatingServer_s, OfficeObjectId_s, RuleDetail
```

11. we can view the rule creation estimatin by pressing **Test with current data** in the right side and see the number of hits.

Analytics rule wizard - Create a new scheduled rule ...

General

Set rule logic

Incident settings

Automated response

Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```

| extend ClientIPAddress = case( ClientIP_s_has '-', toString(split(ClientIP_s, '-')[0]), ClientIP_s_has '[', toString(trim_start('@', toString(split(ClientIP_s, '[')[0]))),
ClientIP_s )
| extend Keyword = iff(isnotempty(subjectcontainswords), subjectcontainswords, (iff(isnotempty(bodycontainswords), bodycontainswords, subjectorbodycontainswords )))
| extend RuleDetail = case(officeobjectid_s_contains '/', toString(split(officeobjectid_s, '/')[-1]), toString(split(officeobjectid_s, '\\')[-1]))
| summarize count(), StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated) by Operation_s, UserId_s, ClientIPAddress, ResultStatus_s, Keyword, OriginatingServer_s,
OfficeObjectId_s, RuleDetail

```

[View query results >](#)

Alert enrichment

- Entity mapping
- Custom details
- Alert details

Query scheduling

Run query every * Hours

Lookup data from the last * Hours

Alert threshold

Generate alert when number of query results is greater than

Event grouping

☒ Alert per event limit is going to be increased soon.

Configure how rule query results are grouped into alerts

☒ Group all events into a single alert

☐ Trigger an alert for each event

Suppression

[Previous](#) [Next - Incident settings >](#)

Results simulation

This chart shows the results of the last 50 evaluations of the defin

[Test with current data](#)

12. Under the **Alert enrichment (Preview)**, expand the entity mapping section that will allow us to map our fields to well-known categories:

- In the **Entity type** open the supported list of entities and select **Account** in the identifier select **FullName** and map it to **UserId_s**
- Press **+ Add new entity** and this time select **Host** entity in the identifier select **FullName** and map it to **OriginatingServer_s**
- Press **+ Add new entity**, select **IP** entity, in the identifier select **Address** and map it to **ClientIPAddress** value.

Your mapping should look like the above:

Analytics rule wizard - Create a new scheduled rule

General **Set rule logic** Incident settings Automated response Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

⚠ One or more entity mappings have been defined under the new version of Entity Mappings. These will not appear in the query code. Any entity mappings defined in the query code will be disregarded.

```
extend ClientIPAddress = case( ClientIP_s has ".", tostring(split(ClientIP_s, ".")[0]), ClientIP_s has "[", tostring(trim_start('@'[1], tostring(split(ClientIP_s, "[")[0])
ClientIP_s )
extend Keyword = iff(isnotempty(SubjectContainsWords), SubjectContainsWords, (iff(isnotempty(BodyContainsWords), BodyContainsWords, SubjectOrBodyContainsWords )))
extend RuleDetail = case(OfficeObjectId_s contains '/', tostring(split(OfficeObjectId_s, '/')[-1]), tostring(split(OfficeObjectId_s, '\\')[-1]))
summarize count(), StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated) by Operation_s, UserId_s, ClientIPAddress, ResultStatus_s, Keyword, OriginatingServer_s, RuleDetail
```

[View query results >](#)

Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results.

This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis.

For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

ⓘ Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code, though they still appear, they will be disregarded when the query runs. [Learn more >](#)

Account	
FullName	UserId_s
Host	
FullName	OriginatingServer_s
IP	
Address	ClientIPAddress

+ Add new entity

Custom details

Alert details

Query scheduling

Previous **Next: Incident settings >**

To make your SOC more productive, save analyst time and effectively triage newly created incidents, your SOC analyst ask you to add the affected user from the search results as part of the alert title.

- For applying this request, we will use the **Alert details** feature and create custom **Alert Name Format**
 - In the **Alert Name Format** copy the above dynamic title "**Malicious Inbox Rule, affected user {{UserId_s}}**"
- In the **Query scheduling** set the **run query every** to **5 minutes** and the **Lookup data to last 12 Hours** (This scheduling might not be ideal for production environment and should be tune). If you deployed the lab more than 12 hours ago, you will need to change the lookback period.
- In the **Suppression** leave it on **Off**
- Press the **Next: Incident settings(Preview)**
- As your SOC is under stress, we want to reduce the number of alerts and be sure that when analyst handle a specific incident, he/she will see all related events or other incidents related to the same attack story. For that we will **implement Alert grouping** feature. To do so, follow the steps below:
 - In the **Incident settings (Preview)** under **Alert grouping** change it to **Enabled**.
 - Modify the **Limit the group to alerts created within the selected time frame** to **12 hours**.

- Select the **Grouping alerts into a single incident if the selected entity types and details matches** and select the Account.

Analytics rule wizard - Create a new scheduled rule ...

General Set rule logic Incident settings Automated response Review and create

Incident settings

Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

Enabled Disabled

Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Enabled Disabled

i Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.

Limit the group to alerts created within the selected time frame *

12 Hours

Group alerts triggered by this analytics rule into a single incident by

- ☒ Grouping alerts into a single incident if all the entities match (recommended)
- ☐ Grouping all alerts triggered by this rule into a single incident
- ☐ Grouping alerts into a single incident if the selected entity types and details match:

Select entities

Select details

⚠ Entity-based alert grouping can make use **only** of entities mapped using the new version, if any exist. Entities mapped with the old version (that appear in the query code) will be available for grouping **only** if there are no mappings defined using the new version.

Re-open closed matching incidents

Enabled **Disabled**

Previous

Next : Automated response >

8. Press the **Next: Automated response** and also press **Next:Review** and create this newly analytics rule.

2.4 Exercise 5: Review resulting security incident

After we created the custom analytics rule that detect us for malicious inbox rule rules. Let's review the incident that was created from this analytics rule.

1. On the main Microsoft Sentinel main page, select **incidents** and review the incident page
2. Locate a new incident with title "**Malicious Inbox Rule, affected user AdeleV@contoso.OnMicrosoft.com**" notice that the name adapt and the effected user name added to the incident name.

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: sentineldemo

Search (Ctrl+F)

Refresh Last 24 hours Actions Security efficiency workbook Columns Guides & Feedback

General

Overview

Logs

News & guides

Search (Preview)

Incident management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK

Content management

Content hub (Preview)

Open incidents by severity

Open incidents: 3 New incidents: 3 Active incidents: 0

High (1) Medium (2) Low (0) Informational (0)

Search by ID, title, tags, owner or product

Severity: All Status: 2 selected Product name: All Owner: All

Auto-refresh incidents

Severity	Incident ID	Title	Alerts	Product names	Created time	Last update time	Owner	Status	Tags
Medium	3	Sign-ins from IPs that attempt sign-ins to disabled accounts	6	Microsoft Sentinel	04/14/22, 06:12 PM	04/14/22, 06:37 PM	Unassigned	New	
Medium	2	Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com	6	Microsoft Sentinel	04/14/22, 06:12 PM	04/14/22, 06:37 PM	Unassigned	New	
High	1	Soloigate Network Beacon	6	Microsoft Sentinel	04/14/22, 06:12 PM	04/14/22, 06:37 PM	Unassigned	New	

Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com

Incident ID: 2

Unassigned Owner New Status Medium Severity

Description

This rule is detecting on delete all traces of phishing email from user mailboxes

Alert product names

- Microsoft Sentinel

Evidence

6 Events 6 Alerts 0 Bookmarks

Last update time: 04/14/22, 06:37 PM

Creation time: 04/14/22, 06:12 PM

Entities (1)

- AdeleV@contoso.O...

View full details >

Tactics and techniques

- Defense Evasion (0)
- Persistence (0)

Incident workbook

Incident Overview

Analytics rule

Malicious Inbox Rule - custom

Tags

Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...

Last comment (Total: 0)

Write a comment...

3. In the right pane we can review the incident preview, this view will give us high level overview on the incident and the entity that related to it.

4. Press on the "view full details"

Incident

Incident ID 2

Refresh

Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com

Incident ID: 2

Unassigned Owner New Status Medium Severity

Description

This rule is detecting on delete all traces of phishing email from user mailboxes

Alert product names

- Microsoft Sentinel

Evidence

6 Events 6 Alerts 0 Bookmarks

Last update time: 04/14/22, 06:37 PM

Creation time: 04/14/22, 06:12 PM

Entities (1)

- AdeleV@contoso.O...

View full details >

Tactics and techniques

- Defense Evasion (0)
- Persistence (0)

Incident workbook

Incident Overview

Analytics rule

Malicious Inbox Rule - custom

Tags

Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...

Last comment (Total: 0)

Write a comment...

Timeline Alerts Bookmarks Entities Comments

Search

Timeline content: All Severity: All Tactics: All

Apr 14 6:01 PM Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com Medium | Detected by Microsoft Sentinel | Tactics: [icon]

Apr 14 5:56 PM Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com Medium | Detected by Microsoft Sentinel | Tactics: [icon]

Apr 14 5:51 PM Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com Medium | Detected by Microsoft Sentinel | Tactics: [icon]

Apr 14 5:46 PM Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com Medium | Detected by Microsoft Sentinel | Tactics: [icon]

Apr 14 5:41 PM Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com Medium | Detected by Microsoft Sentinel | Tactics: [icon]

Apr 14 5:36 PM Malicious Inbox Rule, affected user AdeleV@contoso.onmicrosoft.com Medium | Detected by Microsoft Sentinel | Tactics: [icon]



Malicious Inbox Rule, affected user AdeleV@contoso...

Incident ID: 5



Unassigned
Owner



New
Status



Medium
Severity



Description

This rule is detecting on delete all traces of phishing email from user mailboxes

Alert product names

- Azure Sentinel

Evidence



1
Events



1
Alerts



0
Bookmarks

Last update time

05/02/21, 10:01 PM

Creation time

05/02/21, 10:01 PM

Entities (1)



adelev@contoso.on...
[View full details >](#)

Tactics (2)



Persistence



Defense Evasion

Incident workbook

[Incident Overview](#)

Analytics rule

[Malicious Inbox Rule - custom](#)

Tags



Incident link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Insights/...



Last comment

(Total: 0)

Write a comment...



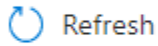
[View full details](#)

Actions

5. In the incident full details page you are able to see alert timeline (effective when you have more than one alert in a given incident)
6. Check the top level tabs and press on the entity tab, this section will expose all the mapped entities that related to this incident.

Incident ...

Incident ID 5



Refresh

>>

Timeline (Preview)

Alerts

Bookmarks

Entities

Comments

View entities full details [here](#)

Search

Entities : **All**

Name ↑↓

Type ↑↓

[adelev@contoso.onmicrosoft.com](#)

Account

7. press on the entity "[AdeleV@contoso.OnMicrosoft.com](#)" this action will navigate us to the user entity page, this page will give us holistic view on the user entity, with all its activity and related alerts.