



Dragon Advance Tech

Azure Sentinel:

Use Cases for ATT&CK-based Detection and Mitigations

A field guide for deployment of Azure Sentinel's Log Analytics
and Implementation of Logic Apps as
Automation playbooks for response

Version: Final
Release date: September 2021

Contents

ABOUT THIS WHITEPAPER	2
WHAT IS AZURE SENTINEL?	3
WHY USING AZURE SENTINEL?	4
USE CASE #1:MICROSOFT DEFENDER FOR OFFICE 365	5
USE CASE #2: SYSMON AND POWERSHELL.....	13
USE CASE #3: REMOTE DESKTOP ACTIVITIES	16
APPENDIX I.....	18
APPENDIX II.....	22
APPENDIX III.....	23
APPENDIX IV: SERVICES OFFERED	24

About this whitepaper

This whitepaper is to provide a field guide for deployment of Azure Sentinel's Log Analytics and Implementation of Logic Apps as automation playbooks for security responses which usually will be handled by security analysts. We intend for this guide to serve as reference examples or use cases by applying ATT&CK-based threat detections, mitigations and investigations.

When develop these three use case, we try to use practical scenarios be found in typical Microsoft hybrid-cloud environment. All detection logics and playbooks can be implemented not only on Azure Sentinel but also can be deployed to any commercial SIEM or SOAR solutions.

In preparing these use cases, we assume you have already connected the relevant log sources to Azure Sentinel and have deployed, implemented and configured Azure Sentinel in your organization's Azure tenant. For more information on basic setup and data ingestion, visit the [Azure Sentinel Quick Start Guide](#). For further information on Strategies in data ingestion and incident response, visit [Azure Sentinel Best Practices](#).

What is Azure Sentinel?

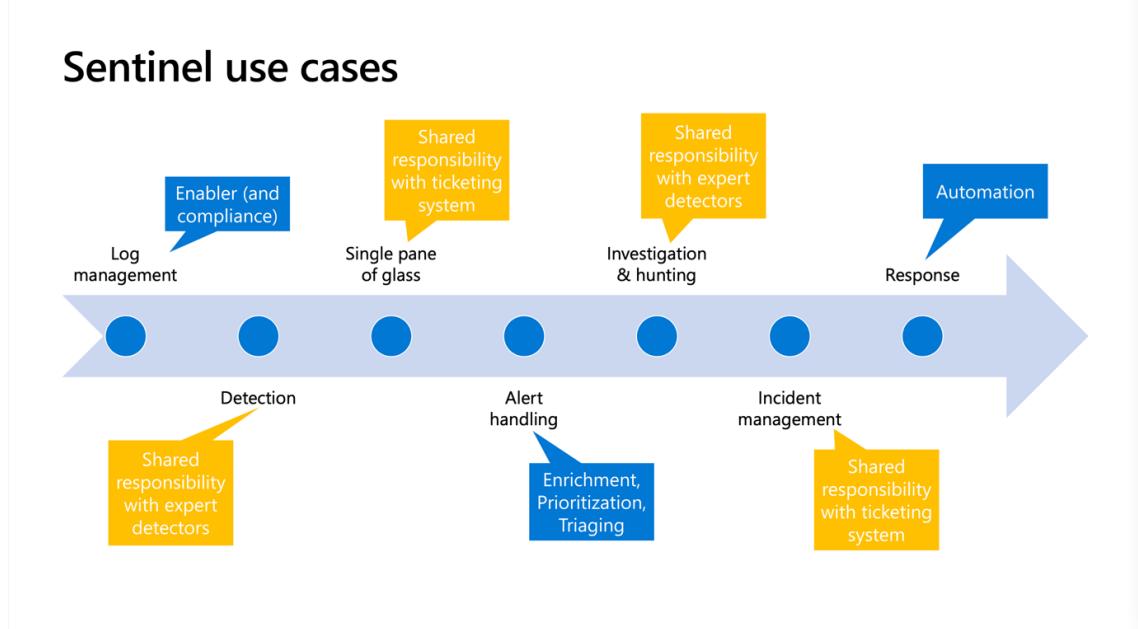
[Microsoft Azure Sentinel](#) is a scalable, [cloud-native](#), security information event management ([SIEM](#)) and security orchestration automated response ([SOAR](#)) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for **alert detection**, **threat visibility**, **proactive hunting**, and **threat response**.

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

- [Collect data](#) at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. Log Analytics workspace is where all ingested data will be stored.
- [Detect](#) previously undetected threats, and minimize false positives using Microsoft's [analytics](#) and unparalleled threat intelligence.
- [Investigate threats](#) with artificial intelligence, and [hunt](#) for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
- [Investigate and respond](#) to incidents rapidly playbooks with built-in orchestration and automation of common tasks.

Building on the full range of existing Azure services, Azure Sentinel natively incorporates proven foundations, like [Log Analytics](#), and [Logic Apps](#) for response playbook execution. Azure Sentinel enriches your investigation and detection with AI, and provides Microsoft's threat intelligence stream and enables you to bring your own threat intelligence.

We prepared this document to provide advices to our clients on making effective use of the security features that are natively provided in the Azure Sentinel. Most of the materials are not our works but extracted from Microsoft. The use cases are prepared for illustration only.



Microsoft©: Steps on defining a use case in Azure Sentinel

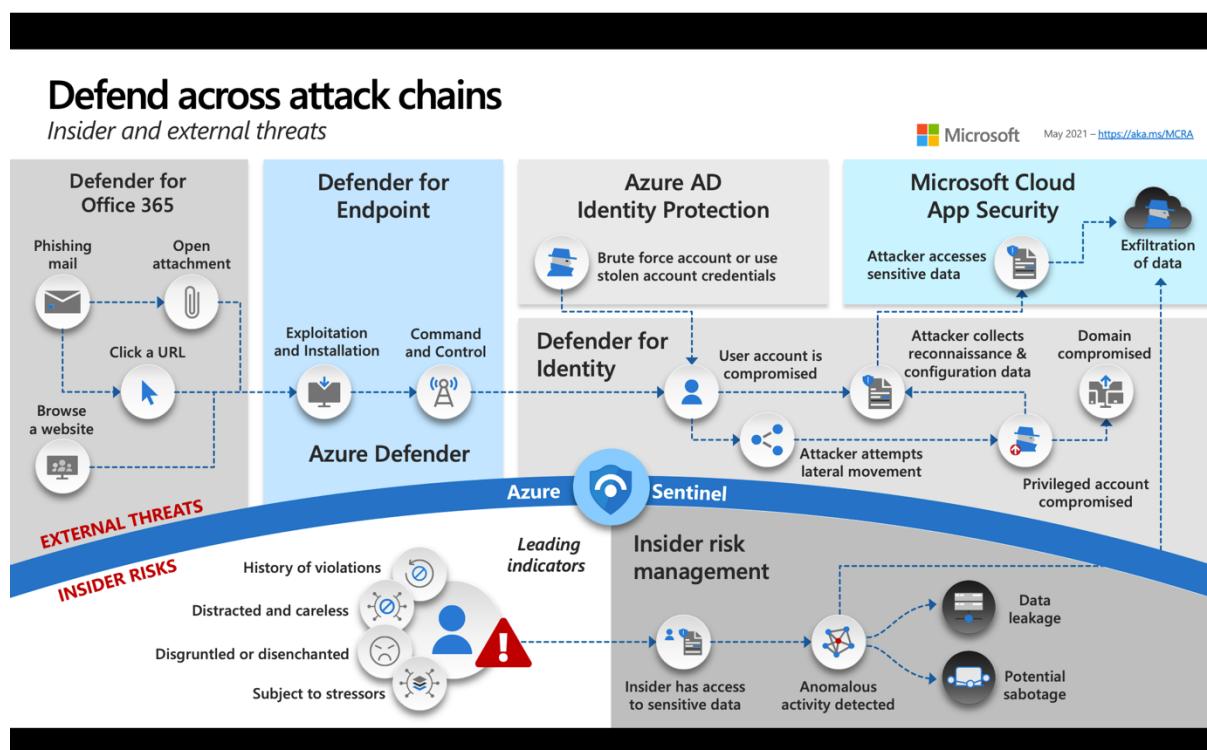
Why using Azure Sentinel?

Your enterprise faces a growing array of increasingly sophisticated security threats.

Detecting and defending against them requires intelligent analytics, effective teamwork, and advanced tools. Microsoft Azure Sentinel meets these needs with a scalable, cloud-native, security information event management ([SIEM](#)) solution that also makes it easier to orchestrate and automate threat responses ([SOAR](#)) security events/alerts.

As a single place for alert detection, threat visibility, [proactive hunting](#), and incident response across the entire enterprise, Azure Sentinel empowers you to perform your regular SOC activities, on the Cloud, on a daily task:

- Review the Incidents to check for new alerts generated by the currently configured analytics rules, and start investigating with advices provided by Microsoft experts.
- Explore results for all built-in queries, and update existing or create new hunting queries and bookmarks.
- Review and enable new applicable analytics rules
- Review the status, date, and time of the last log received from each data connector
- Verify that servers and workstations are actively connected to the workspace
- Verify playbook run statuses and troubleshoot any failures



Microsoft©: Azure Sentinel uses machine learning to profile users, entities, and the environment, detecting attacks that might not be caught using predefined methodologies. This means you can empower Tier 1 analysts to focus their efforts less on sifting through mountains of data and more on highlighting relevant incidents.

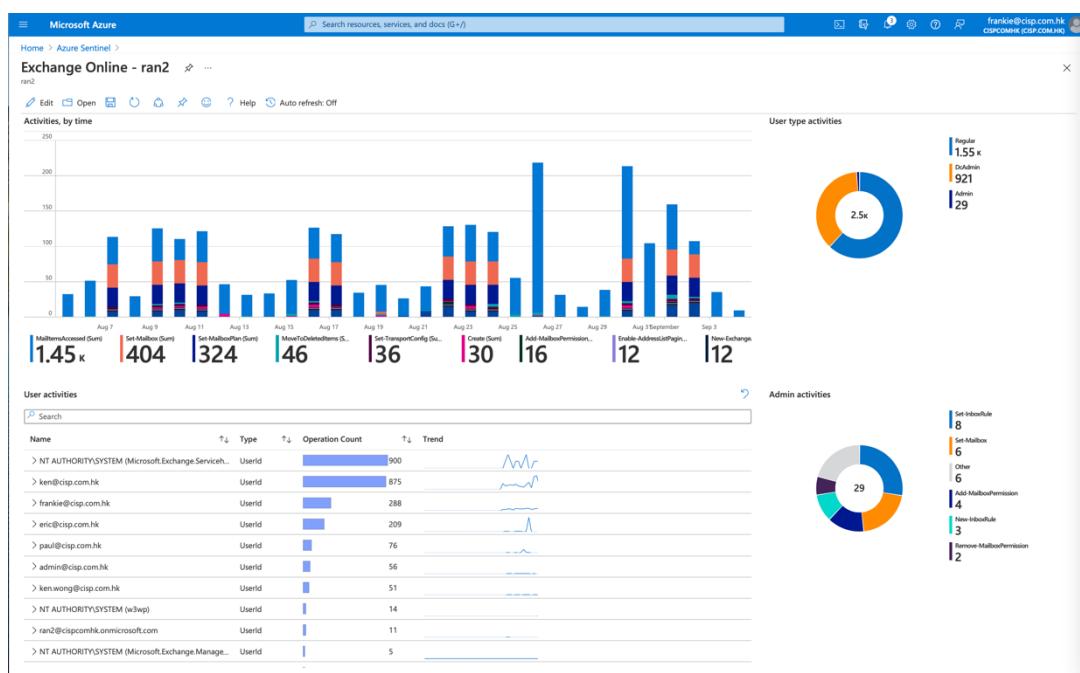
Use Case #1: Microsoft Defender for Office 365

Microsoft Defender 365 (previously named as Microsoft 365 ATP) comes in difference features according to the licenses bought by client. Most of the account and security features are mentioned in the table provided in the Appendix I.

Depends on subscription you bought, your IT team or outsourced vendor (or Help-Desk) should be able to implement suitable features according to your needs by following the [Security Roadmap on Microsoft Defender 365](#) documentation.

Another option is to [Integrate Microsoft 365 Defender with Azure Sentinel](#) for advance detection, monitoring and response on various kind of cyber-attacks. SIEM integration API for detections is the key on ingestion of incidents, entities and security events to Azure Sentinel for this use case. To use Microsoft 365 Defender along with Azure Sentinel, you need Defender for Office 365, Plan 1 or above (i.e. at least Microsoft 365 Business Premium subscription).

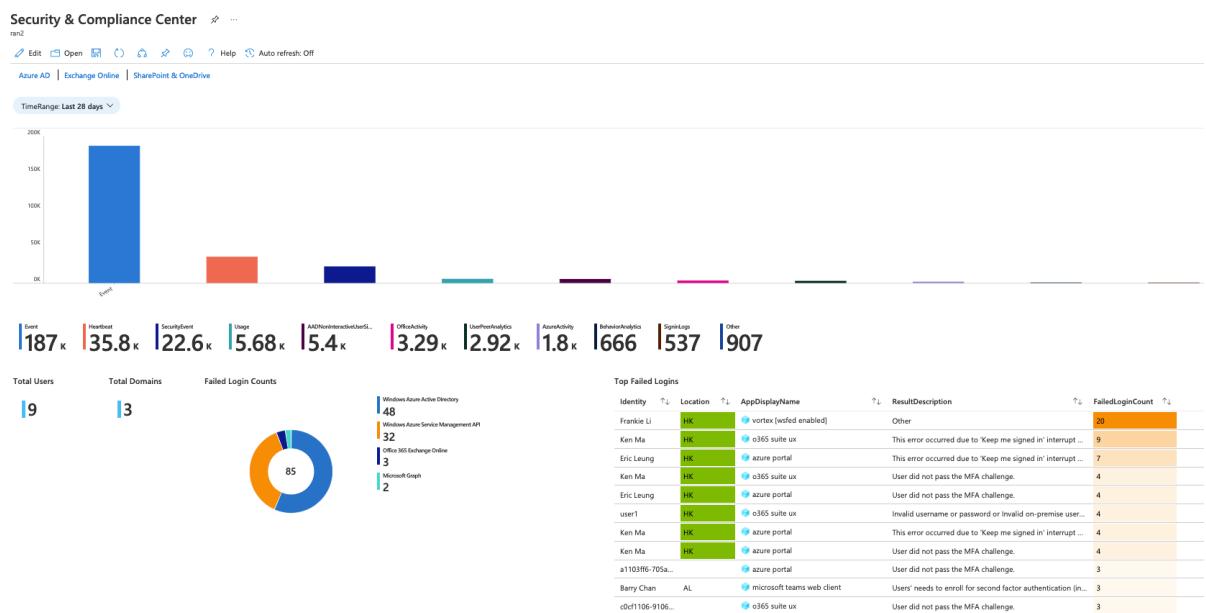
We select Microsoft 365 Defender as a use case because it is fully integrated to Azure Sentinel and Azure Sentinel provides some useful built-in workbook templates out of the box. These templates are designed by Microsoft security experts and analysts based on known threats, common attack vectors, and signature patterns of suspicious activity. They allow you to apply advanced analytics without the need to build your own machine learning models or become a data science expert. By enabling these templates, you will automatically be alerted to anomalies that could indicate an attack.



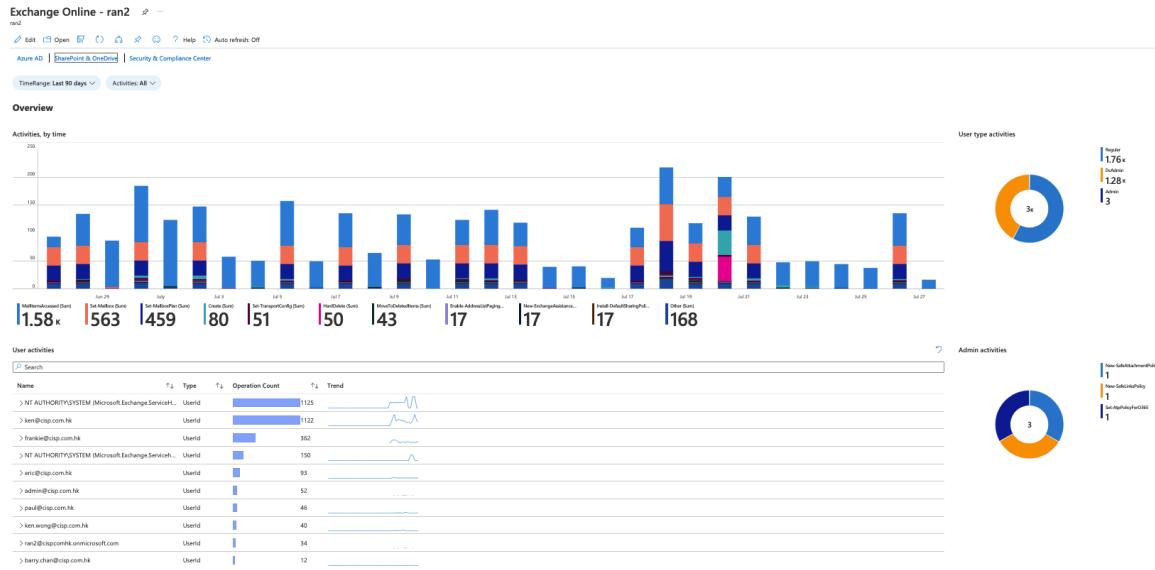


Microsoft©: Azure Sentinel Template - Security Alerts
(Security Alerts dashboard for alerts in your Azure Sentinel environment.)

Other than all the out-of-the-box Workbooks available in Azure Sentinel, we create custom rules and workbooks (dashboards) to monitor and detect security alerts/events of Security & Compliance Centre, Exchange Online, Azure Active Directory and SharePoint & OneDrive

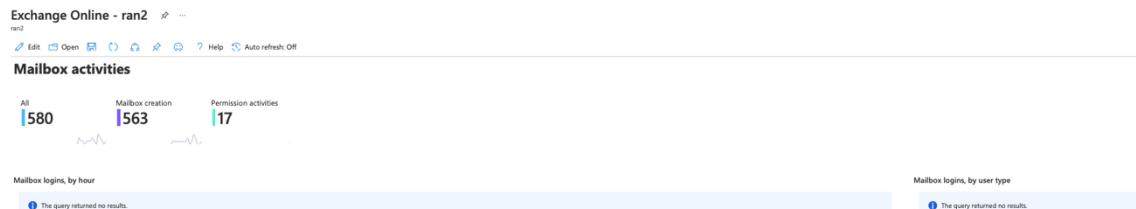


DATC Sentinel Template: Security & Compliance
*(Security & Compliance dashboard for **login alerts** in your Azure Sentinel environment.)*



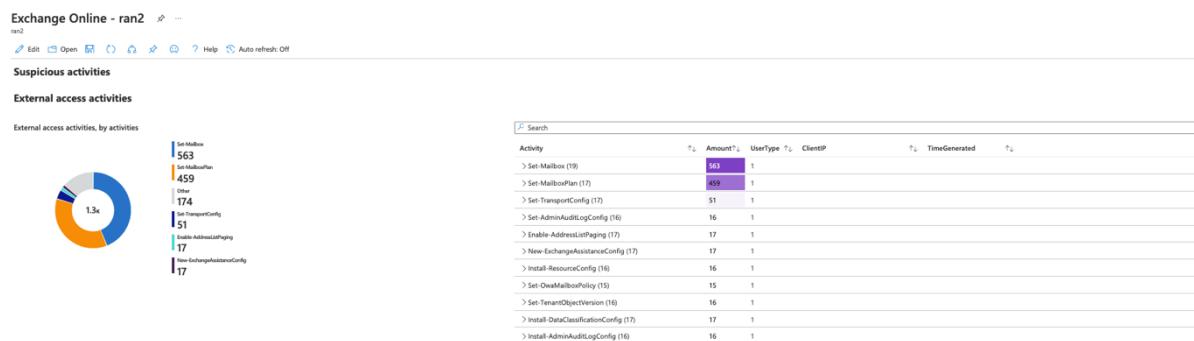
DATC Sentinel Template: Exchange Online

(Exchange Online dashboard an Overview in your Azure Sentinel environment.)



DATC Sentinel Template: Exchange Online

(Exchange Online dashboard for mailbox activities in your Azure Sentinel environment.)



Exchange Online dashboard for Suspicious activities in your Azure Sentinel environment

Azure AD Overview

TimeRange: Last 30 days | Apps All | UserNamePrefix All | UserName All | Category: NonInteractiveUserSignInLogs... | Country All

Summary of top errors

Error Code	Reason	Error Count	Category
500032	Other	19	SignInLogs
500581	Other	9	SignInLogs
501114	Other	6	SignInLogs
50126	Invalid username or password or Invalid on-premise user...	4	SignInLogs
700081	Other	3	NonInteractiveUserSignInLogs
500088	The provided authorization code or refresh token is expir...	2	NonInteractiveUserSignInLogs

Login Failure

Time generated	User	IP Address	Result description	Country or region
7/2/2021, 10:32:12 PM	Paul.Keh	58.176.221.253	Other	HK
7/18/2021, 5:37:47 PM	Paul.Keh	61.93.233.238	Other	HK
7/1/2021, 11:13:23 AM	user1	202.8.241.118	Invalid username or password or Invalid on-premise user...	HK
7/1/2021, 11:13:16 AM	user1	202.8.241.118	Invalid username or password or Invalid on-premise user...	HK
7/1/2021, 11:12:44 AM	user1	202.8.241.118	Invalid username or password or Invalid on-premise user...	HK
7/1/2021, 11:12:10 AM	user1	202.8.241.118	Invalid username or password or Invalid on-premise user...	HK

Sign-ins by Location

Name	Sign-In Count	Trend	Failure Count	Interrupt Count	Category
HK	508	Up	16	16	SignInLogs
US	3	Up	2	0	SignInLogs
HK	508	Up	36	36	SignInLogs
AL	2	Up	0	0	NonInteractiveUserSignInLogs
SG	7	Up	2	0	NonInteractiveUserSignInLogs

Success login out of HK

UserPrincipalName	Country	Count
ken@cip.com.hk	US	723
barry.chan@cip.com.hk	AL	10
eric@cip.com.hk	US	5
eric@cip.com.hk	SG	3

Login Failure out of HK

UserPrincipalName	Country	Count
eric@cip.com.hk	US	4
ken.wong@cip.com.hk	SG	2

MFA Enabled

The query returned no results.

DATC Sentinel Template: Azure Active Directory

(Azure AD dashboard on *Overview* in your Azure Sentinel environment)

Azure AD Overview

TimeRange: Last 30 days | Apps All | UserNamePrefix All | UserName All | Category All | Country All

Success Login by Country

UserPrincipalName	Country	Count
frankie@cip.com.hk	HK	561
ken@cip.com.hk	US	227
eric@cip.com.hk	US	271
ken@cip.com.hk	AL	222
rac@cip.com.hk.comicsoft.com	US	257
paul@cip.com.hk	US	227
ken.wong@cip.com.hk	HK	149
admin@cip.com.hk	US	115
barry.chan@cip.com.hk	AL	73
eric@cip.com.hk	US	10
eric@cip.com.hk	SG	5

Success Login by Country

Hong Kong 5.16x, United States 727, United Kingdom 10, Singapore 7

Success Login via Browser Agent

Success Logins: 698

Failed Login via Browser Agent

Failed Logins: 43

(Azure AD dashboard on *User Login Assessment* in your Azure Sentinel environment)

SharePoint & OneDrive - ran2

TimeRange: Last 30 days | Apps All | UserNamePrefix All | UserName All | Category All | Country All

Sites

Site_Url	Userid	Operation	Numb...
https://cipcomhk.sharepoint.com/sites/cipcomhk/	SHAREPOINT\system	FileVersionsAllDeleted	3
https://cipcomhk.sharepoint.com/sites/Incident6Newexe...	paul@cip.com.hk	FolderCreated	2
https://cipcomhk.sharepoint.com/sites/Incident6Newexe...	paul@cip.com.hk	FileModified	2
https://cipcomhk-my.sharepoint.com/	frankie@cip.com.hk	FileAccessed	1
https://cipcomhk.sharepoint.com/sites/Incident6Newexe...	ken.wong@cip.com.hk	FileAccessed	1
https://cipcomhk.sharepoint.com/sites/cipcomhk/	ken@cip.com.hk	FileAccessed	1

IP addresses

IP Addresses: 34

ClientIP	Userid	Operation	Numb...
175.159.178.58	paul@cip.com.hk	PageViewed	2
175.159.178.58	paul@cip.com.hk	FileAccessed	2
175.159.178.58	paul@cip.com.hk	ListViewed	2
175.159.178.58	paul@cip.com.hk	ListCreated	2
175.159.178.58	paul@cip.com.hk	FileModified	2
20.190.144.171	admin@cip.com.hk	SharingPolicyChanged	2

Sites details

Site_Url	Userid	Operation	Numb...
https://cipcomhk.sharepoint.com/sites/cipcomhk/	SHAREPOINT\system	FileVersionsAllDeleted	3
https://cipcomhk.sharepoint.com/sites/Incident6Newexe...	paul@cip.com.hk	FolderCreated	2
https://cipcomhk.sharepoint.com/sites/Incident6Newexe...	paul@cip.com.hk	FileModified	2
https://cipcomhk-my.sharepoint.com/	frankie@cip.com.hk	FileAccessed	1
https://cipcomhk.sharepoint.com/sites/Incident6Newexe...	ken.wong@cip.com.hk	FileAccessed	1
https://cipcomhk.sharepoint.com/sites/cipcomhk/	ken@cip.com.hk	FileAccessed	1

IP addresses details

ClientIP	Userid	Operation	Numb...
175.159.178.58	paul@cip.com.hk	PageViewed	2
175.159.178.58	paul@cip.com.hk	FileAccessed	2
175.159.178.58	paul@cip.com.hk	ListViewed	2
175.159.178.58	paul@cip.com.hk	ListCreated	2
175.159.178.58	paul@cip.com.hk	FileModified	2
20.190.144.171	admin@cip.com.hk	SharingPolicyChanged	2

DATC Sentinel Template: SharePoint & OneDrive

(SharePoint & OnDrive dashboard on *Sites Access* in your Azure Sentinel environment)

Azure Sentinel also provides out-of-the-box, built-in [threat detection rules](#) to help you analyse and monitor your Office 365 activities. Rule templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that looks suspicious. Many of the rules can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can assign and investigate in your environment. Other than all the out-of-the-box Detection Rules available in Azure Sentinel, DATC create custom rules to detect security events on Exchange Online. (Appendix II)

Results simulation
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data

Threshold: 0

0

Jul 25 August Aug 3 Aug 15 Aug 22 Aug 29 Sep 5

Microsoft©: Azure Sentinel Analytics Rule - Malformed user agent

Results simulation
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

Test with current data

Threshold: 0

1

0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0

Aug 22

Alert enrichment (Preview)

Entity mapping

Map up to five entities recognized by Azure Sentinel from the appropriate fields available in your query results. This enables Azure 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](#)

+ Add new entity

Custom details

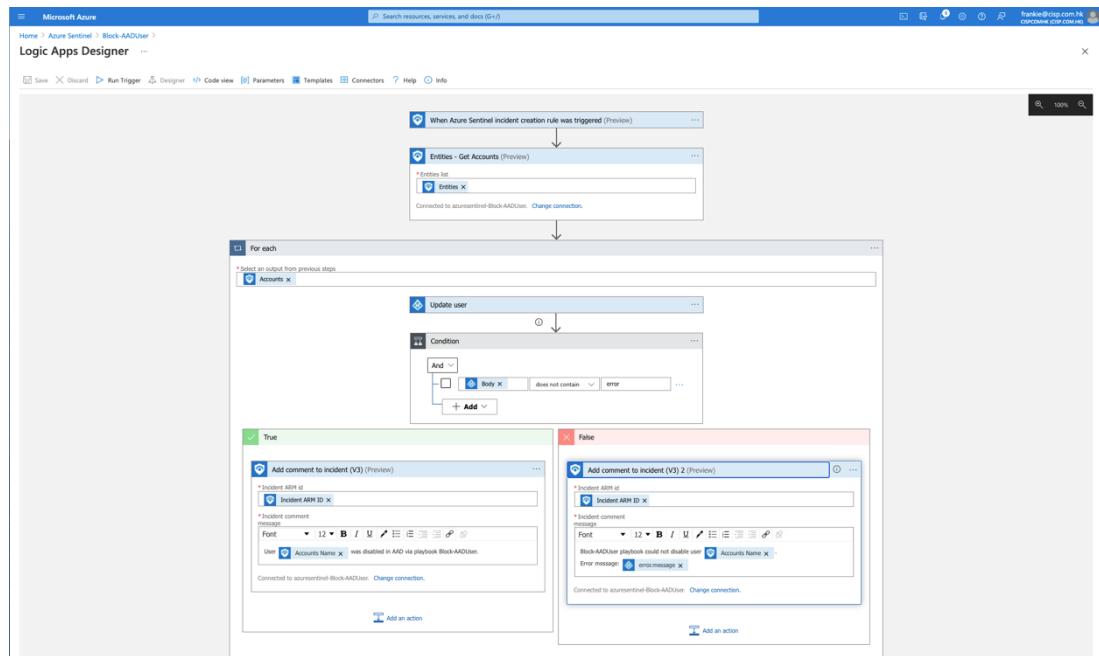
Alert details

Query scheduling

Microsoft©: Azure Sentinel Analytics Rule - Mail redirect via ExO transport rule

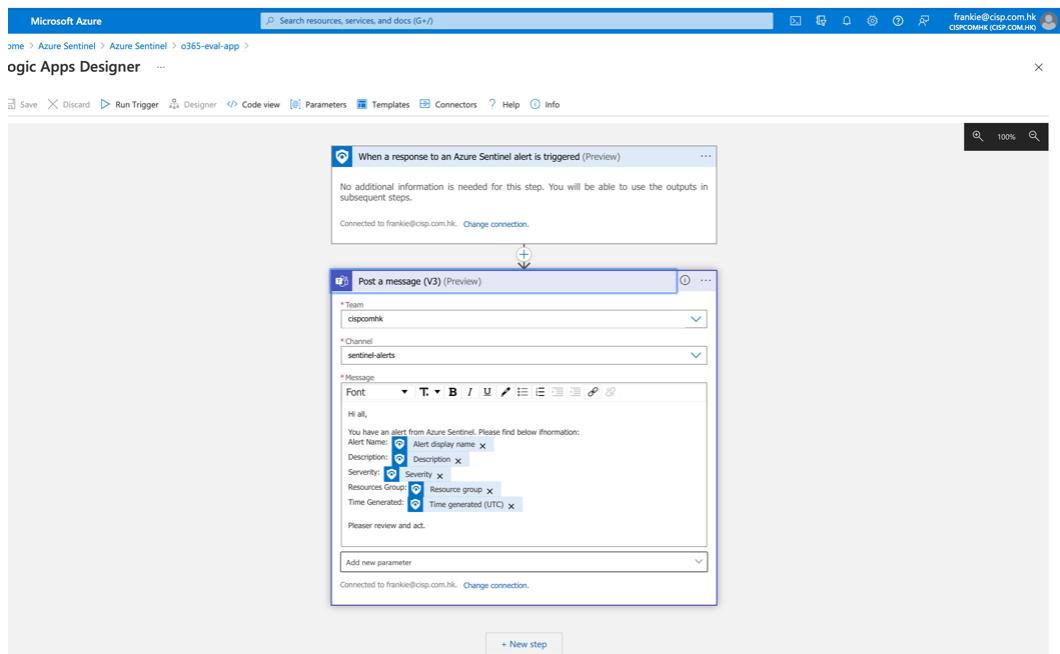
Playbooks are collections of procedures that can be run from Azure Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

For example, if you want *to stop potentially compromised users from moving around your network and stealing information*, you can create an automated, multifaceted response to incidents generated by rules that detect compromised users. You start by creating a playbook that takes the step to disable the user in Azure AD, like the following:



Microsoft©: Sentinel Playbook: Block-AADUser

Or, we prefer *to send an alert message to Teams channel* to serve as an open ticket for the incident:



DATC Sentinel Playbook: Teams Channel

Teams

Your teams

- cispcomhk
- General
- DATC
- sentinel-alerts**
- Incident 6: New executab...
- DATC

sentinel-alerts Posts Files +

Channel Meet

FL 04/09 6:08 pm

Frankie Li 04/09 6:08 pm
Hi all,

You have an alert from Azure Sentinel. Please find below ifnornation:
Alert Name: UEBA-Logon-HK
Description: User and Entity Behavior Logon from Hong Kong
Severrity: Low
Resources Group:container01
Time Generated: 2021-09-04T10:08:15.8573606Z

Please review and act.

See less

Reply

5 September 2021

FL 05/09 4:07 pm

Frankie Li 05/09 4:07 pm
Hi all,

You have an alert from Azure Sentinel. Please find below ifnornation:
Alert Name: Rare and potentially high-risk Office operations
Description: Identifies Office operations that are typically rare and can provide capabilities useful to attackers.
Severrity: Medium
Resources Group:container01
Time Generated: 2021-09-05T08:07:05.5213557Z

Please review and act.

See less

Reply

Join or create a team

New conversation

Example Sentinel Playbooks: Teams Alerts

The screenshot shows the Microsoft Azure Azure Sentinel | Incidents page. The left sidebar includes sections for General (Overview, Logs, News & guides), Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence (Preview)), Configuration (Data connectors, Analytics, Watchlist, Automation, Solutions (Preview)), Community, and Settings. The main content area displays a summary of incidents: 82 Open incidents, 82 New incidents, and 0 Active incidents. A chart titled "Open incidents by severity" shows the distribution across High (0), Medium (7), Low (55), and Informational (20) levels. Below this, a table lists alerts with columns for Title, Alerts, Product name, Created time, Last update time, and Owner. Each alert row contains a link to its full details. To the right, a detailed view for an alert titled "Rare and potentially high-risk Office operations" is shown, including sections for Description, Alert product names (Azure Sentinel), Evidence (Events 2, Alerts 1, Bookmarks 0), and various metrics like Last update time (09/05/21, 04:07 PM) and Creation time (09/05/21, 04:07 PM). The bottom right corner shows a link to the full incident details.

Example Sentinel Playbooks: Teams Alerts

Azure Sentinel | Automation

Selected workspace: 'ran2'

Automation rules (Preview)

Name	Status	Trigger kind	Subscription	Resource group	Location	Tags
Azure-Sentinel-Alert-To-Team	Enabled	Azure Sentinel Alert	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Block-AADUser	Enabled	Azure Sentinel Incident (Pr...	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Block_IPs_on_MDATP	Enabled	Azure Sentinel Alert	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Change-Incident-Security	Enabled	Azure Sentinel Incident (Pr...	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Comment-OriginAlertURL	Enabled	Using Azure Sentinel Action	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Comment_RemediationSteps	Enabled	Azure Sentinel Incident (Pr...	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Get-geo-from-IP	Disabled	Azure Sentinel Alert	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Get-VirusTotalDomainReport	Enabled	Azure Sentinel Incident (Pr...	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
IdentityProtection-EmailResponse	Enabled	Azure Sentinel Alert	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
o365-eval-app	Enabled	Azure Sentinel Alert	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
OTX-Threat-Intel	Enabled	Other	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security
Triggers	Enabled	Azure Sentinel Incident (Pr...	Pay-As-You-Go	container01	East Asia	LogicAppsCategory: security

Example Sentinel Playbooks: Deployed in our Azure Sentinel

Azure Sentinel | Incidents

Selected workspace: 'ran2'

Open incidents by severity

Severity	Count
High (0)	0
Medium (7)	7
Low (55)	55
Informational (20)	20

Suspicious Process Discovery

Incident ID: 897
Investigate in Microsoft Defender for Endpoint

Evidence

- N/A (0) Events
- 1 Alerts
- 0 Bookmarks

Tags

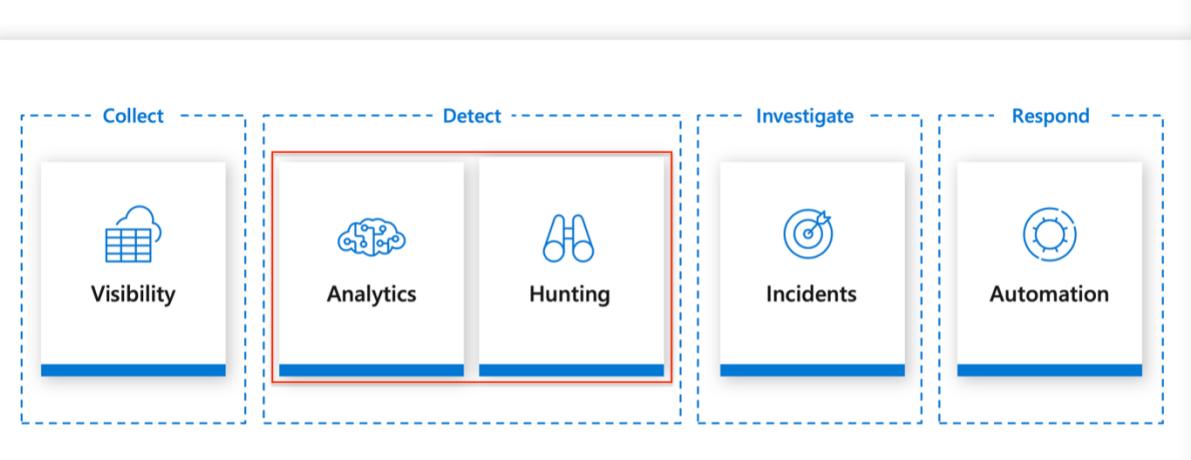
Sentinel Incidents: Alerts found in Azure Sentinel

Use Case #2: Sysmon and PowerShell

Adversaries may abuse [PowerShell](#) commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, for example:

- Download (and execute) malicious payload
- Create a reverse shell
- Perform credential dumping using Mimikatz
- Embed script in an image
- Write a complete ransomware
- Launch fileless attacks
- and more

We take malicious use of PowerShell as a threat indicator and make reference to MITRE ATT&CK Enterprise Matrix Tactic & Technique called: Command and Scripting Interpreter: [PowerShell](#) to build this use case on Azure Sentinel.



Microsoft©: Azure Sentinel: End-to-end solution for security operations

Logging is the key to knowing how the attackers came in and how they got you. There are many ways (such as using Microsoft Defender for Endpoint (MDE) or any EDR solution) to collect the right data for monitoring and detection of malicious use of PowerShell. In this use case, we use Microsoft offered tools for an SME on-premises and cloud logging feature to create analytics for us to monitor the malicious use of PowerShell.

[Sysmon](#) “is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time”.

We gather the possible attackers' TTPs on how PowerShell are used in the attack scenarios from various threat intel sources and some github published red-team frameworks (such as: the [EmpireProject](#) and RedCanary's [AtomicRedTeam](#)).

After installed the Sysmon with appropriate configuration, we collect Windows Event logs from a few selected endpoints and execute a few PowerShell commands. We have to make modification on the Sysmon parser after data connector

Microsoft Azure

Search resources, services, and docs (G+)

frankie@isp.com.hk CSECOMINE ISP.COM.HK

Home > Azure Sentinel > Azure Sentinel

Azure Sentinel < cisprohk (isp.com.hk)

+ Create Manage view ...

Filter for any field... Name: ran2

Azure Sentinel | Incidents Selected workspace: ran2

Search (Cmd+/) Refresh Last 30 days Actions Security efficiency workbook Columns Guides & Feedback

General

522 Open incidents 522 New incidents 0 Active incidents

Open incidents by severity

High (39) Medium (56) Low (383) Informational (44)

Search by ID, title, tags, owner or product Severity: All Status: New, Active More (2)

Incident ID Title Alerts Product names Created time

Wohami Execution 1 Azure Sentinel 09/08/21, 04:13 PM

Wohami Execution 1 Azure Sentinel 09/08/21, 04:12 PM

'Ceprolad' malware was blocked 1 Microsoft Defender ... 09/08/21, 03:15 PM

Suspicious Process Discovery 1 Microsoft Defender ... 09/07/21, 06:45 PM

Suspicious sequence of explorati... 1 Microsoft Defender ... 09/07/21, 06:45 PM

A script with suspicious content... 1 Microsoft Defender ... 09/07/21, 06:45 PM

Rare and potentially high-risk Or... 1 Azure Sentinel 09/05/21, 04:07 PM

UEBA-Logon-HK 1 Azure Sentinel 09/04/21, 06:08 PM

Wohami Execution Incident ID: 900

Unassigned New Status Medium Severity

Description Detects the execution of wohami, which is often used by attackers after exploitation / privilege escalation but rarely used by administrators

Alert product names • Azure Sentinel

Evidence N/A Events 1 Alerts 0 Bookmarks

Last update time 09/08/21, 04:13 PM Creation time 09/08/21, 04:13 PM

Entities (0) Tactics (1) Discovery

Incident workbook Incident Overview

Analytics rule Wohami Execution

Tags

The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alert. Learn more

< Previous Page 1 - 50 Next >

View full details Actions

A simple Sysmon Sentinel detection rule: whoami started from PowerShell

The screenshot shows a Microsoft Teams interface with the following details:

- Left Sidebar:** Activity, Chat, Teams, Calendar, Calls, Files, and Apps.
- Top Bar:** Search bar, Channel, Meet, and other Teams navigation icons.
- Teams Tab:** Shows "Your teams" with entries for "cispcomhk" and "Incident 6: New executab...".
- Alerts:** A list of three alerts from the "sentinel-alerts" channel.
 - Alert 1:** Resources Group: [redacted], Time Generated: [redacted]. Message: "Pleaser review and act." with "See less" and "Reply" options. A reply from "Frankie Li" at 4:13 pm says "Hi all," followed by detailed alert information: Alert Name: Whoami Execution, Description: Detects the execution of whoami, which is often used by attackers after exploitation / privilege escalation but rarely used by administrators, Severity: Medium, Resources Group: container01, Time Generated: 2021-09-08T08:13:02.9533639Z.
 - Alert 2:** Message: "Pleaser review and act." with "See less" and "Reply" options. A reply from "Frankie Li" at 4:13 pm says "Hi all," followed by "You have an alert from Azure Sentinel. Please find below ifnformation: Entities: []".
- Bottom Buttons:** "New conversation" button.

To simplify our task in preparing the first set of detection rules for immediate use, we import [Sigma Rule to Azure Sentinel](#) for this demonstration. Using this approach, you can easily have more than 1,000 high quality MITRE ATT&CK ready detection rules, including PowerShell related rules, readily for your Azure Sentinel use.

We provided a few of our Sysmon & PowerShell Analytics rules in Appendix III.

We also created a KQL rule to detect Empire PowerShell invocation for detection of suspicious parameters on the latest cyber threats.

General Information

Analysis ID: 334401

Score: 56

Range: 0 - 100

Whitelisted: false

Confidence: 100%

Detection

SIGNS

- MALICIOUS
- SUSPICIOUS
- CLEAN
- UNKNOWN

Signatures

- Sigma detected: Powershell launch wmic ...
- Suspicious command line found
- Suspicious powershell command line found
- Contains long sleeps (> 3 min)
- Creates a process in suspended mode (LI...)
- Enables debug privileges
- Found a high number of Window / User s...
- May sleep (evasive loops) to hinder dyna...
- Monitors certain registry keys / values for ...
- Queries the volume information (name, se...
- Very long cmdline option found, this is ver...

Classification

A circular heatmap diagram with concentric rings and various threat indicators like Malware, Exploit, Persistence, and Network.

Malware Configuration

No configs have been found

DATC: A Windows PowerShell threat found on 3 September 2021

Active rules

SEVERITY	NAME	RULE TYPE	STATUS	TACTICS	LAST MODIFIED
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled	Lateral Movement	08/19/21, 01:40 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled	Lateral Movement	09/05/21, 05:10 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled	Lateral Movement	06/11/21, 03:12 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled	Lateral Movement	09/05/21, 05:11 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled	Lateral Movement	09/05/21, 05:13 PM
High	CVE-2021-1675 Print Spooler Exploitation IPC A...	Scheduled	Enabled	Lateral Movement	07/07/21, 04:21 PM
High	Empire Shell Launch Parameters	Scheduled	Enabled	Lateral Movement	09/08/21, 12:26 PM
High	Known Manganeze IP and User-Agent activity	Scheduled	Enabled	Malware	09/05/21, 05:25 PM
Medium	Anomalous login followed by Teams action	Scheduled	Enabled	Malware	06/12/21, 06:47 PM
Medium	Brute force attack against Azure Portal	Scheduled	Enabled	Credential Access	06/27/21, 10:44 PM
Medium	Exchange AuditLog disabled	Scheduled	Enabled	Defense Evasion	06/13/21, 04:09 PM
Medium	Mail redirect via ExO Transport rule	Scheduled	Enabled	Exfiltration	06/13/21, 04:14 PM
Medium	Malformed user agent	Scheduled	Disabled	Impact	06/13/21, 04:15 PM
Medium	Malicious Inbox Rule	Scheduled	Enabled	Impact	06/13/21, 03:07 PM
Medium	Multiple users email forwarded to same destinat...	Scheduled	Enabled	Impact	06/13/21, 04:16 PM
Medium	New executable via Office FileUploaded Operatio...	Scheduled	Enabled	Command and Control	06/13/21, 04:06 PM
Medium	Office policy tampering	Scheduled	Disabled	Impact	06/13/21, 04:16 PM
Medium	Rare and potentially high-risk Office operations	Scheduled	Enabled	Impact	06/13/21, 04:06 PM
Medium	RDP session from Non jump host IP	Scheduled	Enabled	Impact	09/03/21, 10:52 AM
Medium	SharePointFileOperation via previously unseen IPs	Scheduled	Enabled	Exfiltration	06/13/21, 04:05 PM
Medium	(Preview) TI map IP entity to OfficeActivity	Scheduled	Enabled	Impact	06/11/21, 03:17 PM

Rule details for Empire PowerShell Launch Parameters

Rule query:

```
#!/from the sigma\rules\windows.process_creation
// title: Empire PowerShell Launch Parameters
// https://github.com/Nerd32d/signature-base/blob/main/rules/windows/process_creation.yaml
// https://github.com/RedTeam-Playground/Windows-Shell-Exploit-Signature-Base/blob/main/rules/windows/process_creation.yaml
```

Rule frequency: Run query every 6 hours

Rule period: Last 6 hours data

Rule threshold: Trigger alert if query returns more than 0 results

Event grouping: Group all events into a single alert

Suppression: Not configured

Create incidents from this rule: Enabled

Alert grouping: Disabled

DATC: Detects PowerShell invocation with suspicious parameters

Use Case #3: Remote Desktop Activities

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the [Remote Desktop Protocol \(RDP\)](#) as Remote Desktop Services (RDS).

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the Accessibility Features technique for Persistence.

In our previous ransomware investigation cases, after gaining access to the IT infrastructure through vulnerable VPN solution, we found adversaries used lots of RDP to perform their lateral movement activities.

User and Entity Behaviour Analytic (UEBA) highlights the anomalies. Using RDP activities as example, the company's policy required users use jump host machine to connect to critical asset. Azure sentinel Analytic and Watchlist allow us to spot out if anyone violate the policy.

The screenshot shows the Azure Sentinel Analytics interface. At the top, there is a code editor window containing the following PowerShell-like query:

```
1 let jumphost = (_GetWatchlist('jumphost') | project IPAddress);
2 RDP
3 |where EventID == 21 or EventID == 22 or EventID == 25
4 |where RemoteHost !in~ (jumphost)
5 |where RemoteHost!="LOCAL"
6 |project TimeGenerated, Computer, RemoteHost, User, Session, RenderedDescription;
```

Below the code editor is a results table with the following data:

TimeGenerated [UTC]	Computer	RemoteHost	User	Session
9/8/2021, 8:48:42.923 AM	dc.windomain.local	192.168.38.104	WINDOMAIN\ vagr...	2

Generating alert and send notification to Teams

The screenshot shows the Microsoft Defender XDR incident view for an alert from dc.windomain.local. The alert details are as follows:

- Alert from dc.windomain.local**
Incident ID: 901
- Status:** New
- Severity:** Medium
- Description:** 2021-09-08T08:48:42.923000Z From Remote IP: 192.168.38.104 User: WINDOMAIN\ vagrant
- Alert product names:** Azure Sentinel
- Evidence:** 1 Events, 1 Alerts, 0 Bookmarks
- Timeline:** Sept 8, 16:48 - Alert from dc.windomain.local (Medium | Detected by Azure Sentinel | Tactics: --)

You have an alert from Azure Sentinel. Please find below information:

Alert Name: Alert from DESKTOP-F7NIGP1 - RDP policy violation connect from non jumphost IP

Description: 2021-09-09T02:09:31.487000Z From Remote IP: 192.168.22.196 User: DESKTOP-F7NIGP1\Forensic

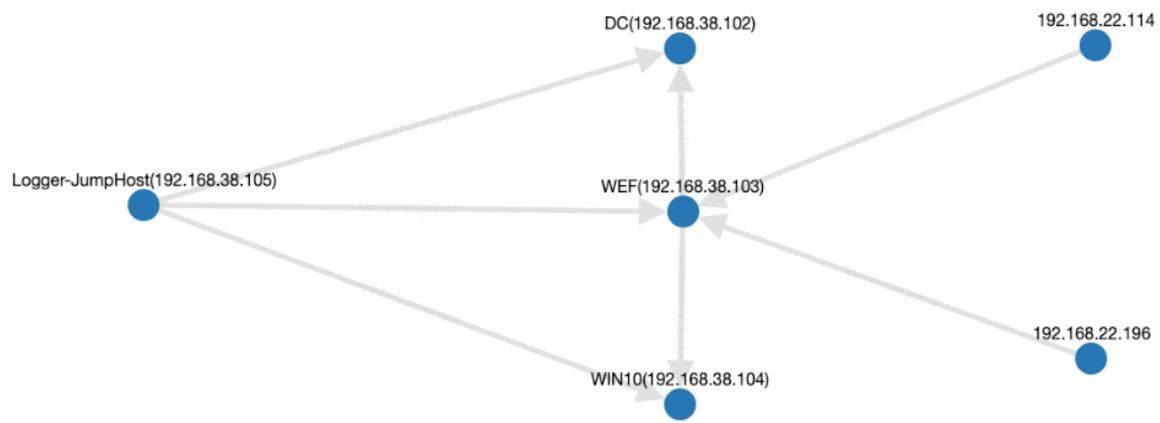
Severity: Medium

Resources Group:container01

Time Generated: 2021-09-09T02:16:31.0241718Z

Please review and act.

Furthermore, a more intuitive view of the UEBA when applying link analysis. See the example of DRP activities below.



Appendix I

Office 365 security builds on the core protections offered by EOP. In Office 365 security, there are three main security services (or products) tied to your subscription type:

1. Exchange Online Protection (EOP)
2. Microsoft Defender for Office 365 Plan 1 (Defender for Office P1)
3. Microsoft Defender for Office 365 Plan 2 (Defender for Office P2)

Exchange Online Protection (EOP)

Prevent/Detect	Investigate	Respond
<ul style="list-style-type: none"> • Spam, phish • malware • bulk mail, spoof intelligence • impersonation detection • Admin Quarantine • Admin and user submissions of False Positives and False Negatives • Allow/Block for URLs and Files 	<ul style="list-style-type: none"> • Audit log search • Message Trace (part of the reporting features) 	<ul style="list-style-type: none"> • Zero-hour Auto-Purge (ZAP) • Refinement and testing of Allow and Block lists

Defender for Office 365, Plan 1 (Included in Microsoft 365 Business Premium)

Prevent/Detect	Investigate	Respond
<p>Technologies include everything in EOP plus:</p> <ul style="list-style-type: none"> • Safe Attachments • Safe Links • Microsoft Defender for Office 365 protection for workloads (ex. SharePoint Online, Teams, OneDrive for Business) • Time-of-click protection in email, Office clients, and Teams • Anti-phishing protection in Defender for Office 365 • User and domain impersonation protection • Alerts, and SIEM integration API for alerts 	<ul style="list-style-type: none"> • SIEM integration API for detections • Real-time detections tool • URL trace (view Safe Links actions) 	<ul style="list-style-type: none"> • Same

Defender for Office 365, Plan 2 (which expands on the investigation and response side of the house, and adds a new hunting strength. Office 365 E5 and Microsoft 365 E5)

Prevent/Detect	Investigate	Respond
<p>Technologies include everything in EOP, and Microsoft Defender for Office 365 P1 plus:</p> <ul style="list-style-type: none"> • Safe Documents (not included in Office 365 E5) 	<ul style="list-style-type: none"> • Threat Explorer • Threat Trackers • Campaign views 	<ul style="list-style-type: none"> • Automated investigation and response (AIR) • AIR from Threat Explorer • AIR for compromised users • SIEM Integration API for Automated Investigations • Attack simulation training



Transform your enterprise with Microsoft solutions

Connect, protect, and empower every employee, from the office to the frontline worker, with a Microsoft solution that enhances productivity and drives innovation.

Microsoft 365 Stay connected and get more done with intelligent apps and experiences, integrated cloud services, and built-in security.	Office 365 Create, share, edit, and collaborate in real time from anywhere on any device with a cloud-based suite of productivity apps and services.	Microsoft Enterprise Mobility + Security (EMS) Protect and secure your organization and empower your employees to work in new and flexible ways with an intelligent mobility management and security platform.	Windows 10 Benefit from a highly secure and manageable productivity platform that runs on a wide variety of hardware devices or in the cloud.
---	--	--	---

Jump to section:

Microsoft 365 Apps	Knowledge, insights, and content	Endpoint and app management	Information governance
Email, calendar, and scheduling	Analytics	Threat protection	eDiscovery and auditing
Meetings, calling, and chat	Project and task management	Identity and access management	Insider risk management
Social, intranet, and storage	Automation, app building, and chatbots	Information protection	Windows

Information Worker Plans										Frontline Worker Plans							
Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10			Microsoft 365				Office 365	
E3	E5	ES Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security Add-on	F5 Compliance Add-on	F5 Sec + Comp Add-on	F3
USD ERP per user per month	\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80	\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4
Microsoft 365 Apps	•	•			•	•											
Desktop client apps ¹	•	•			•	•	•					Read only	• ³				• ³
Office Mobile apps ¹	•	•			•	•	•					Read only	•			•	
Office for the web	•	•			•	•	•					• ⁴				• ⁴	
Install apps on up to 5 PCs/Mac + 5 tablets + 5 smartphones	•	•			• ⁴	•	•										
Microsoft Editor premium features	•	•				•	•										
Multilingual user interface for Office applications	•	•				•	•										

¹Includes Word, Excel, PowerPoint, OneNote, Outlook, Access (PC only), and Publisher (PC only)

²Includes Word, Excel, PowerPoint, Outlook, and OneNote mobile Apps

³Limited to devices with integrated screens smaller than 10.1"

⁴Mobile app only

Email, calendar, and scheduling				Information Worker Plans				Frontline Worker Plans							
Exchange	Plan 2	Plan 2		Plan 1	Plan 2	Plan 2		See footnote 1	Kiosk			Kiosk			
Mailbox size	100 GB	100 GB		50 GB	100 GB	100 GB			2 GB			2 GB			
Calendar	•	•		•	•	•			•	•		•			•
Outlook desktop client	•	•		•	•	•									
Email archiving	•	•		• ²	•	•									
Exchange Online Protection	•	•		•	•	•									
Public folder mailboxes	•	•		•	•	•									
Resource mailboxes	•	•		•	•	•									
Inactive mailboxes	•	•		•	•	•									
Microsoft Shifts	•	•		•	•	•									
Microsoft Bookings	•	•		•	•	•									

¹Microsoft 365 F1 includes the Exchange Kiosk service plan to enable Teams calendar only. It does not include mailbox rights.

²250 GB limit

Page 1 of 5

Information Worker Plans										Frontline Worker Plans							
Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10			Microsoft 365				Office 365	
E3	E5	ES Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security Add-on	F5 Compliance Add-on	F5 Sec + Comp Add-on	F3
USD ERP per user per month	\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80	\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4
Meetings, calling, and chat	•	•			•	•	•			•	•	•	•	•	•	•	•
Microsoft Teams	•	•			•	•	•			•	•	•	•	•	•	•	•
Unlimited chat	•	•			•	•	•			•	•	•	•	•	•	•	•
Online meetings	•	•			•	•	•			•	•	•	•	•	•	•	•
Live Events	•	•			•	•	•			•	•	•	•	•	•	•	•
Webinars	•	•			•	•	•			•	•	•	•	•	•	•	•
Screen sharing and custom backgrounds	•	•			•	•	•			•	•	•	•	•	•	•	•
Record meetings	•	•			•	•	•			•	•	•	•	•	•	•	•
Priority notifications	•	•			•	•	•			•	•	•	•	•	•	•	•
Phone System	•	•				•											
Audio Conferencing	•	•				•											

¹Check country and region availability at <https://docs.microsoft.com/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans>

²Cannot be administrators. No site mailbox. No personal site.

³In addition to 1TB storage provided per organization.

⁴Microsoft will provide an initial 5 TB of OneDrive storage per user. Customers who want additional OneDrive storage can request it as needed by contacting Microsoft support. Subscriptions for fewer than five users receive 1 TB OneDrive storage per user.

⁵OneDrive personal storage is included in the Microsoft 365 plan.

⁶OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁷OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁸OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁹OneDrive Personal storage is included in the Microsoft 365 plan.

¹⁰OneDrive Business Premium storage is included in the Microsoft 365 plan.

¹¹OneDrive Business Standard storage is included in the Microsoft 365 plan.

¹²OneDrive Business Basic storage is included in the Microsoft 365 plan.

¹³OneDrive Personal storage is included in the Microsoft 365 plan.

¹⁴OneDrive Business Premium storage is included in the Microsoft 365 plan.

¹⁵OneDrive Business Standard storage is included in the Microsoft 365 plan.

¹⁶OneDrive Business Basic storage is included in the Microsoft 365 plan.

¹⁷OneDrive Personal storage is included in the Microsoft 365 plan.

¹⁸OneDrive Business Premium storage is included in the Microsoft 365 plan.

¹⁹OneDrive Business Standard storage is included in the Microsoft 365 plan.

²⁰OneDrive Business Basic storage is included in the Microsoft 365 plan.

²¹OneDrive Personal storage is included in the Microsoft 365 plan.

²²OneDrive Business Premium storage is included in the Microsoft 365 plan.

²³OneDrive Business Standard storage is included in the Microsoft 365 plan.

²⁴OneDrive Business Basic storage is included in the Microsoft 365 plan.

²⁵OneDrive Personal storage is included in the Microsoft 365 plan.

²⁶OneDrive Business Premium storage is included in the Microsoft 365 plan.

²⁷OneDrive Business Standard storage is included in the Microsoft 365 plan.

²⁸OneDrive Business Basic storage is included in the Microsoft 365 plan.

²⁹OneDrive Personal storage is included in the Microsoft 365 plan.

³⁰OneDrive Business Premium storage is included in the Microsoft 365 plan.

³¹OneDrive Business Standard storage is included in the Microsoft 365 plan.

³²OneDrive Business Basic storage is included in the Microsoft 365 plan.

³³OneDrive Personal storage is included in the Microsoft 365 plan.

³⁴OneDrive Business Premium storage is included in the Microsoft 365 plan.

³⁵OneDrive Business Standard storage is included in the Microsoft 365 plan.

³⁶OneDrive Business Basic storage is included in the Microsoft 365 plan.

³⁷OneDrive Personal storage is included in the Microsoft 365 plan.

³⁸OneDrive Business Premium storage is included in the Microsoft 365 plan.

³⁹OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁴⁰OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁴¹OneDrive Personal storage is included in the Microsoft 365 plan.

⁴²OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁴³OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁴⁴OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁴⁵OneDrive Personal storage is included in the Microsoft 365 plan.

⁴⁶OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁴⁷OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁴⁸OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁴⁹OneDrive Personal storage is included in the Microsoft 365 plan.

⁵⁰OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁵¹OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁵²OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁵³OneDrive Personal storage is included in the Microsoft 365 plan.

⁵⁴OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁵⁵OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁵⁶OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁵⁷OneDrive Personal storage is included in the Microsoft 365 plan.

⁵⁸OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁵⁹OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁶⁰OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁶¹OneDrive Personal storage is included in the Microsoft 365 plan.

⁶²OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁶³OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁶⁴OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁶⁵OneDrive Personal storage is included in the Microsoft 365 plan.

⁶⁶OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁶⁷OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁶⁸OneDrive Business Basic storage is included in the Microsoft 365 plan.

⁶⁹OneDrive Personal storage is included in the Microsoft 365 plan.

⁷⁰OneDrive Business Premium storage is included in the Microsoft 365 plan.

⁷¹OneDrive Business Standard storage is included in the Microsoft 365 plan.

⁷²OneDrive Business Basic storage is included in the Microsoft 365 plan.



Information Worker Plans												Frontline Worker Plans							
Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10		Microsoft 365				Office 365				
E3	E5	E5 Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security Add-on	F5 Compliance Sec+Comp Add-on	F3			
USD ERP per user per month	\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80	\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4		
Identity and access management																			
Azure Active Directory Premium	Plan 1	Plan 2	Plan 2						Plan 1	Plan 2				Plan 1	Plan 2	Plan 2	Plan 2	Plan 2	Plan 2
User Provisioning	•	•	•		•	•	•	•	•	•			•	•	•	•	•	•	•
Self Service Password Reset	•	•	•		•	•	•	•					•	•	•	•	•	•	•
Advanced Security Reports	•	•	•										•	•	•	•	•	•	•
Multi Factor Authentication	•	•	•		•	•	•	•					•	•	•	•	•	•	•
Conditional Access	•	•	•		•	•	•	•					•	•	•	•	•	•	•
Risk Based Conditional Access / Identity Protection	•	•	•										•		•	•	•	•	•
Privileged Identity Management	•	•	•										•	•	•	•	•	•	•
Access Reviews	•	•	•										•	•	•	•	•	•	•
Entitlement Management	•	•	•										•	•	•	•	•	•	•
Microsoft 365 Groups	•	•	•		•	•	•	•					•	•	•	•	•	•	•
On-premises Active Directory sync for SSO	•	•	•		•	•	•	•					•	•	•	•	•	•	•
DirectAccess supported	•	•	•										•	•	•	•	•	•	•
Windows Hello for Business	•	•	•										•	•	•	•	•	•	•
Microsoft Advanced Threat Analytics	•	•	•										•	•	•	•	•	•	•
Windows Store Access Management	•	•	•										•	•	•	•	•	•	•
Cloud Access Security Broker																			
Cloud App Security Discover	•	•											•	•	•	•	•	•	•
Office 365 Cloud App Security	•	•											•	•	•	•	•	•	•
Microsoft Cloud App Security	•	•	•	•	•	•	•	•					•	•	•	•	•	•	•
Information protection																			
Azure Information Protection	Plan 1	Plan 2		Plan 2					AIP for O365	AIP for O365	Plan 1	Plan 2				Plan 1	Plan 1	Plan 2	Plan 2
Manual sensitivity labels	•	•		•					•	•	•	•				•	•	•	•
Automatic sensitivity labels	•	•		•					•	•	•	•				•	•	•	•
Machine Learning-based sensitivity labels	•	•		•					•	•						•	•	•	•
Office 365 Data Loss Prevention (DLP) for emails and files	•	•							•	•						•	•	•	•
Communication DLP (Teams chat)	•	•		•					•	•						•	•	•	•
Endpoint DLP	•	•		•					•	•						•	•	•	•
Basic Office Message Encryption	•	•		•					•	•	•	•				•	•	•	•
Advanced Office Message Encryption	•	•		•					•	•						•	•	•	•
Customer Key for Office 365	•	•		•					•	•						•	•	•	•

Page 4 of 5

Information Worker Plans												Frontline Worker Plans							
Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10		Microsoft 365				Office 365				
E3	E5	E5 Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security Add-on	F5 Compliance Sec+Comp Add-on	F3			
USD ERP per user per month	\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80	\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4		
Automation, app building, and chatbots																			
Power Apps for Microsoft 365 ¹	•	•			•	•	•	•				•	•	•	•	•	•	•	•
Power Automate for Microsoft 365 ¹	•	•			• ²	• ²	• ²	• ²				• ³	• ³	•	•	•	•	•	•
Power Virtual Agent for Teams ¹	•	•			•	•	•	•				•	•	•	•	•	•	•	•
Dataaverse for Teams ¹	•	•			•	•	•	•				•	•	•	•	•	•	•	•
¹ Refer to the licensing FAQs and Licensing Guide at https://docs.microsoft.com/power-platform/admin/powerapps-flow/licensing-faq for details including functionality limits.																			
² Cloud flows only.																			
³ Desktop flows only.																			
Endpoint and app management																			
Microsoft Intune	•	•							•	•	•	•	•	•	•	•	•	•	•
Mobile Device Management	•	•			•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Microsoft Endpoint Manager	•	•							•	•	•	•	•	•	•	•	•	•	•
Mobile application management	•	•							•	•	•	•	•	•	•	•	•	•	•
Windows AutoPilot	•	•							•	•	•	•	•	•	•	•	•	•	•
Windows Hello for Business	•	•							•	•	•	•	•	•	•	•	•	•	•
Group Policy support	•	•							•	•	•	•	•	•	•	•	•	•	•
Shared computer activation for Microsoft 365 Apps	•	•							•	•	•	•	•	•	•	•	•	•	•
Endpoint Analytics	•	•							•	•	•	•	•	•	•	•	•	•	•
Cortana management	•	•							•	•	•	•	•	•	•	•	•	•	•
Threat protection																			
Microsoft Defender Antimalware	•	•										•	•	•	•	•	•	•	•
Microsoft Defender Firewall	•	•										•	•	•	•	•	•	•	•
Microsoft Defender Exploit Guard	•	•										•	•	•	•	•	•	•	•
Microsoft Defender Credential Guard	•	•										•	•	•	•	•	•	•	•
BitLocker and BitLocker To Go	•	•										•	•	•	•	•	•	•	•
Windows Information Protection	•	•										•	•	•	•	•	•	•	•
Microsoft Defender for Endpoint	•	•										•	•	•	•	•	•	•	•
Microsoft Defender for Identity	•	•										•	•	•	•	•	•	•	•
Microsoft Defender for Office 365	Plan 2	Plan 2							Plan 2							Plan 2	Plan 2		
Application Guard for Office 365	•	•										•	•	•	•	•	•	•	•
Safe Documents	•	•										•	•	•	•	•	•	•	•

Page 3 of 5



Information Worker Plans								Frontline Worker Plans								
Microsoft 365				Office 365			Enterprise Mobility + Security		Windows 10			Microsoft 365				Office 365
E3	E5	E5 Security Add-on	E5 Compliance Add-on	E1	E3	E5	E3	E5	Pro (for reference)	Enterprise E3	Enterprise E5	F1	F3	F5 Security Add-on	F5 Compliance Sec+Comp Add-on	F3
USD ERP per user per month	\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80	\$5	\$10	\$2.25	\$8	\$8	\$8	\$4
Information governance																
Manual retention labels	•	•			•	•	•	•	•			•	•			•
Basic org-wide or location-wide retention policies	•	•				•	•							•	•	
Rules-based automatic retention policies	•	•		•			•							•	•	
Machine Learning-based retention														•	•	
Teams message retention policies	•	•			• ¹	•	•	•	•			• ¹	• ¹			• ¹
Records Management	•	•			•		•							•	•	
<small>¹30-day minimum retention period.</small>																
eDiscovery and auditing																
Content Search	•	•			•	•	•	•	•			•	•	•	•	•
Core eDiscovery (including Hold and Export)	•	•			•	•								•	•	•
Litigation Hold	•	•				•	•	•	•					•	•	•
Advanced eDiscovery														•	•	
Basic Audit	•	•			•	•	•	•	•			•	•	•	•	•
Advanced Audit	•	•			•	•	•	•	•			•	•	•	•	•
Insider risk management																
Insider Risk Management	•	•			•									•	•	
Communication Compliance	•	•												•	•	
Information Barriers	•	•			•									•	•	
Customer Lockbox	•	•												•	•	
Privileged Access Management	•	•			•		•						•	•	•	
Windows																
Windows 10 Edition	Enterprise	Enterprise								Professional	Enterprise	Enterprise		Enterprise		
Windows Virtual Desktop (WVD)	•	•								•	•	•		•		
Universal Print	•	•								•	•	•		•		

©2021 Microsoft Corporation. All rights reserved. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.
Publish date: JULY 26, 2021

Appendix II

#	Rule Name	Description	Log Source	Severity	MITRE ATT&CK	Threat Intel
1	Known Manganese IP and UserAgent activity	Matches IP plus UserAgent IOCs in OfficeActivity data, along with IP plus Connection string information in the CommonSecurityLog data related to Manganese group activity	Office 365 OfficeActivity	High	Execution Privilege Escalation Command and Control	APTS Manganese Lookup
2	SharePointFileOperation via devices with previously unseen user agents	Identifies if the number of documents uploaded or downloaded from device(s) associated with a previously unseen user agent exceeds a threshold (default is 5)	Office 365 OfficeActivity	Medium	Exfiltration	
3	Exchange workflow MailItemsAccessed operation anomaly	Identifies anomalous increases in Exchange mail items accessed operations. The query leverages KQL built-in anomaly detection algorithms to find large deviations from baseline patterns. Sudden increases in execution frequency of sensitive actions should be further investigated for malicious activity. Manually change scorethreshold from 1.5 to 3 or higher to reduce the noise based on outliers flagged from the query criteria	Office 365 OfficeActivity	Medium	Collection	Solorigate NOBELIUM
4	Exchange AuditLog disabled	Identifies when the exchange audit logging has been disabled which may be an adversary attempt to evade detection or avoid other defenses	Office 365 OfficeActivity	Medium	DefenseEvasion	
5	Malicious Inbox Rule	Often times after the initial compromise the attackers create inbox rules to delete emails that contain certain keywords. This is done so as to limit ability to warn compromised users that they've been compromised	Office 365 OfficeActivity	Medium	Persistence DefenseEvasion	
6	Office policy tampering	Identifies if any tampering is done to either auditing, ATP Safelink, SafeAttachment, AntiPhish or Dlp policy. An adversary may use this technique to evade detection or avoid other policy based defenses	Office 365 OfficeActivity	Medium	Persistence DefenseEvasion	
7	Mail redirect via ExO transport rule	Identifies when Exchange Online transport rule configured to forward emails. This could be an adversary mailbox configured to collect mail from multiple user accounts	Office 365 OfficeActivity	Medium	Collection Exfiltration	
8	SharePointFileOperation via previously unseen ips	Identifies when the volume of documents uploaded to or downloaded from Sharepoint by new IP addresses exceeds a threshold (default is 50)	Office 365 OfficeActivity	Medium	Exfiltration	
9	Multiple users email forwarded to same destination	Identifies when multiple (more than one) users mailboxes are configured to forward to the same destination. This could be an attacker-controlled destination mailbox configured to collect mail from multiple compromised user accounts	Office 365 OfficeActivity	Medium	Collection Exfiltration	Data Theft
10	External user added and removed in short timeframe	This detection flags the occurrences of external user accounts that are added to a Team and then removed within one hour	Office 365 OfficeActivity	Low	Persistence	
11	Possible STRONTIUM attempted credential harvesting - Sept 2020	Surface potential STRONTIUM group Office365 credential harvesting attempts within OfficeActivity Logon events	Office 365 OfficeActivity	Low	CredentialAccess	
12	New executable via Office FileUploaded Operation	Identifies when executable file types are uploaded to Office services such as SharePoint and OneDrive. List currently includes ".exe", ".inf", ".gip", ".cmd", ".bat" file extensions. Additionally, identifies when a given user is uploading these files to another user's workspace. This may be indication of a staging location for malware or other malicious activity	Office 365 OfficeActivity	Low	CommandAndControl	
13						

Microsoft©: Azure Sentinel Detection Rules – Office 365 Activity

(*Security Detection Rules for your Azure Sentinel environment.*)

#	Rule Name	Description	Log Source	Severity	MITRE ATT&CK	Threat Intel
21	Office 365 Anonymous SharePoint Link used	This alert detects when an anonymous link created in Sharepoint has been used. The anonymous link allow access to the shared document without any credentials.	Office 365 OfficeActivity	Informational	Initial Access Execution	Elevation of Privilege
22	Non owner Office 365 mailbox login activity	This will help you determine if mailbox access observed with Admin/Delegate LogonType. The logon type indicates mailbox accessed from non-owner user. Exchange allows Admin and delegate permissions to access other user's inbox.	Office 365 OfficeActivity	Medium	Initial Access	Elevation of Priviledge
23	New Office 365 admin activity detected	This will help you discover any new admin account activity which was seen and were not seen historically. Any new accounts seen in the results can be validated and investigated for any suspicious activities. Please note that this use case is very noisy and it is recommended to tune it regularly.	Office 365 OfficeActivity	Informational	Credential Access	Unauthorized activity
24	Powershell mailbox login activity in Office 365	This will help you determine if mailbox login was done from Exchange Powershell session. By default, all accounts you create in Office 365 are allowed to use Exchange Online PowerShell. Administrators can use Exchange Online PowerShell to enable or disable a user's ability to connect to Exchange Online PowerShell.	Office 365 OfficeActivity	Medium	Initial Access Execution	Improper Usage
25	Malware detected in a Office 365 repository	This alert triggers when Office 365 antivirus engine detects malware in a file hosted in Sharepoint or OneDrive.	Office 365 OfficeActivity	High	Execution Command and Control	Malicious Content
26	Rare and potentially high risk Office 365 operations	This will help you identify Office operations that are typically rare and can provide capabilities useful to attackers.	Office 365 OfficeActivity	Low	Persistence Collection	Improper Usage
27	Office 365 policy tampering	Identifies if any tampering is done to either auditlog, ATP Safelink, SafeAttachment, AntiPhish or Dlp policy. An adversary may use this technique to evade detection or avoid other policy based defenses.	Office 365 OfficeActivity	Medium	Persistence Credential Access	Improper Usage
28	Office 365 connections from malicious IP addresses (Managed Sentinel Threat Intelligence)	Indicates Office 365 activities recorded from IP addresses listed in Managed Sentinel Threat Intelligence Feed. Recommended score level to be setup for 75 and higher.	Office 365 OfficeActivity	Medium	Initial Access Exfiltration	External attacker
29	Office 365 Anonymous SharePoint Link Created	This alert detects when an anonymous link was created in Sharepoint. The anonymous link allow access to the shared document without any credentials.	Office 365 OfficeActivity	Informational	Initial Access Exfiltration	Elevation of Privilege
30	Office 365 inactive user accounts	This alert will trigger for users that have been active in last 90 days, but not in the last 60 days	Office 365 OfficeActivity	Informational	N/A	N/A
31	A malicious IP address accessing an Office 365 resource	This alert triggers when a success connection is established to O365 resources from a malicious IP address	Office 365 OfficeActivity	Medium	Initial Access Command and Control Exfiltration	Compromised Accounts
32	Office 365 Mailbox Added or Removed	This alert identifies administrative operations for mailbox creation and removal. This is an operational alert.	Office 365 OfficeActivity	Informational	N/A	N/A
33	Silent OfficeActivity Workload	This alert is triggered when an Office 365 workload such as Exchange, SharePoint, OneDrive, etc. has not generated logs in the last 1 hour. Version 1.0	Office 365 OfficeActivity	Informational	Execution	System monitoring impact

DATC Sentinel Detection Rules – Office 365 Activity

(*Security Detection Rules for your Azure Sentinel environment.*)

Appendix III

Sentinel Analytic Rules for PowerShell - Sep 6 2021

©2021 Analytic Rules for PowerShell. All rights reserved. This document is for informational purposes only. DATC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. Some information relates to pre-released product which may be substantially modified before it's commercially released.

#	Rule Name	Description	Author	Condition	falsepositives	MITRE ATT&CK	Severity	Query Reference	Reference
1	Alternate PowerShell Hosts	Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe	Roberto Rodriguez @Cyb3rWard0g	selection and not filter	Programs using PowerShell directly without invocation of a dedicated interpreter	attack.execution attack.t1059.001	medium	Event where ((EventID == 4103 and ContextInfo contains "I") and not (ContextInfo contains "powershell.exe")) Event where ((EventID == 400 and HostApplication contains "I") and not (HostApplication endswith 'powershell.exe'))	https://github.com/Cyb3rWard0g/ThreatHunter-Playbook/tree/master/playbooks/windows/02_execution/t1086_powershell/alternate
2	Silence.EDA Detection	Detects Silence empireDNSagent	Alina Stepenkova, Group-IB, oscd.community	empire and dnsat	attack.execution attack.t1059.001 attack.t1066 attack.command_and_control attack.t1071.004 attack.t1071 attack.t1572 attack.impact attack.t1529 attack.g0991 attack.t0363	critical	Event where (ScriptBlockText contains '\$System.Diagnostics.Process' and ScriptBlockText contains 'Stop-Computer') and ScriptBlockText contains 'Restart-Computer' and ScriptBlockText contains 'Exception in execution' and ScriptBlockText contains '\$cmdargs' and ScriptBlockText contains 'Close-DnsatTurner' and ScriptBlockText contains 'Set type=LookupType 'nserv' and ScriptBlockText contains 'Command nslookup 2-8 Out-String' and ScriptBlockText contains 'New-RandomDNSSField' and ScriptBlockText contains '[Convert]::ToString(\$,\$(NOPTIONS, 16)) and ScriptBlockText contains '\$Session.Dead = \$True' and ScriptBlockText contains '@'\$Session'\Driver\''-eq')		
4	PowerShell ADRecon Execution	Detects execution of ADRecon.ps1 for AD reconnaissance which has been reported to be actively used FIN7	Bhavesh Raj	selection	attack.discovery attack.execution attack.t1059.001	high	Event where (EventID == 4104 and (ScriptBlockText contains 'Function Get-ADReconComObj' or ScriptBlockText contains 'ADRecon-Report.xlsx'))	https://github.com/sense-of-security/ADRecon https://bi-zone.medium.com/rom-pent-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23ca7e319	
5	Automated Collection Command PowerShell	Detects collection established within a system or network, an adversary may use automated techniques for exfiltrating internal data.	frack113	all of them	attack.collection attack.t1119	medium	Event where (EventID == 4104 and (ScriptBlockText contains 'doc' or ScriptBlockText contains 'dot' or ScriptBlockText contains 'xsl' or ScriptBlockText contains 'xslc' or ScriptBlockText contains 'ppt' or ScriptBlockText contains 'ppsx' or ScriptBlockText contains 'rtf' or ScriptBlockText contains 'pdf' or ScriptBlockText contains 'xlt' and ScriptBlockText contains 'Get-ChildItem' and ScriptBlockText contains '-Recurse' and ScriptBlockText contains '-Include')	https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1119/T1119.r	
6	Bad Opsec Powershell Code Artifacts	Detects trivial artifacts observed in variants of prevalent offensive ps1 payloads, including Cobalt Strike Beacon, PoshC2, Powerview, Letmein, Empire, Powersploit, and other attack payloads that often undergo minimal changes by attackers due to bad opsec.	ok @securonix invrep_de, oscd.community	selection_4104 or selection_4103	Moderate-to-low. Despite the shorter length, lower entropy for some of these, because of high specificity, fp appears to be fairly limited in many environments.	attack.execution attack.t1059.001 attack.t1086	critical	Event where (EventID == 4104 and (ScriptBlockText contains '\$Obit' or ScriptBlockText contains 'harmi\$Obit' or ScriptBlockText contains 'mattification' or ScriptBlockText contains 'RastaMouse' or ScriptBlockText contains 'tifikin.' or ScriptBlockText contains '0xdeadbeef')) or (EventID == 4103 and (Payload contains '\$Obit' or Payload contains 'harmi\$Obit' or Payload contains 'mattification' or Payload contains 'RastaMouse' or Payload contains 'tifikin.' or Payload contains '0xdeadbeef'))	https://newtonpaul.com/analysing-fileless-malware-cobalt-strike-beacon/ https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-file-for-high-value-targets/ https://www.msfeditor.pl/pl/pg8t
7	Execution via CL_Invocation.ps1	Detects Execution via SyncInvoke in CL_Invocation.ps1 module	oscd.community, Natalia Shornikova	selection		attack.defense_evasion attack.t1216	high	Event where (EventID == 4104 and ScriptBlockText contains 'CL_Invocation.ps1' and ScriptBlockText contains 'SyncInvoke')	https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSScripts/CLInvocation.yml https://twitter.com/b0h0ps/status/94065991012327424
8	Execution via CL_Mutexverifiers.ps1	Detects Execution via runAfterCancelProcess in CL_Mutexverifiers.ps1 module	oscd.community, Natalia Shornikova	selection		attack.defense_evasion attack.t1216	high	Event where (EventID == 4104 and ScriptBlockText contains 'CL_Mutexverifiers.ps1' and ScriptBlockText contains 'runAfterCancelProcess')	https://github.com/LOLBAS-Project/LOLBAS/blob/master/yml/OSScripts/CL_Mutexverifi.yml https://twitter.com/gabrielekj/status/99311115447577600
9	Clear PowerShell History	Detects keywords that could indicate clearing PowerShell history	Ilyas Ochkov, Jonathan Ribeiro, Danill Yugayevskiy, oscd.community	selection_1 and (selection_2 or selection_3) or selection_4 and (selection_5 or selection_6)	Legitimate PowerShell scripts	attack.defense_evasion attack.t1070.003 attack.t1146	medium	Event where (EventID == 4104 and ((ScriptBlockText contains 'del' or ScriptBlockText contains 'Remove-Item' or ScriptBlockText contains 'rm') and ScriptBlockText contains '(Get-PSReadLineOption).HistorySavePath')) or (ScriptBlockText contains 'Set-PSReadLineOption' and ScriptBlockText contains 'HistorySaveStyle' and ScriptBlockText contains 'SaveNothing')) or (EventID == 4103 and ((Payload contains 'del' or Payload contains 'Remove-Item' or Payload contains 'rm') and Payload contains '(Get-PSReadLineOption).HistorySavePath') or (Payload contains 'Set-PSReadLineOption' and Payload contains 'HistorySaveStyle' and Payload contains 'SaveNothing'))))	https://gist.github.com/hook-s3c/7363a856c3dbadeb71085147f0421a
10	PowerShell Create Local User	Detects creation of a local user via PowerShell	@ROXPinTeddy	selection	Legitimate user creation	attack.execution attack.t1059.001 attack.t1096 attack.persistence attack.t1136.001	medium	Event where (EventID == 4104 and ScriptBlockText contains 'New-LocalUser')	https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1136/T1136.r