



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



Frankie Li, Ken Wong and Ken Ma



ir@dragonadvancetech.com



© Dragon Advance Tech Consulting Company Limited

<https://t.me/learningnets>

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?

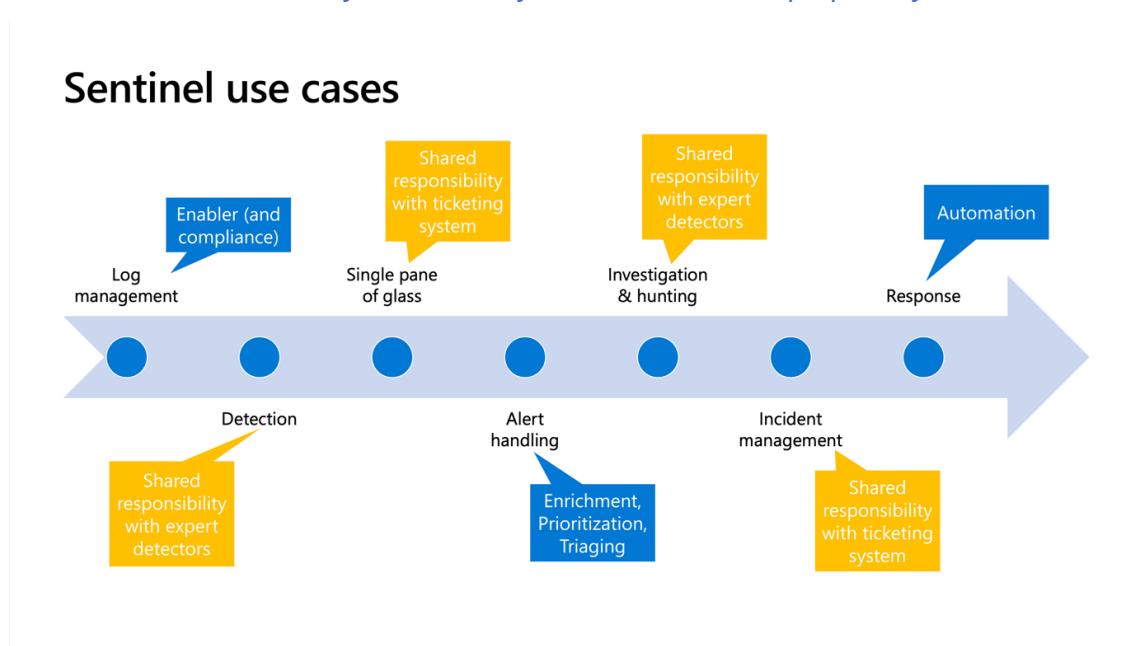
[Microsoft Azure Sentinel](#) is a scalable, [cloud-native](#), security information event management ([SIEM](#)) and security orchestration automated response ([SOAR](#)) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single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

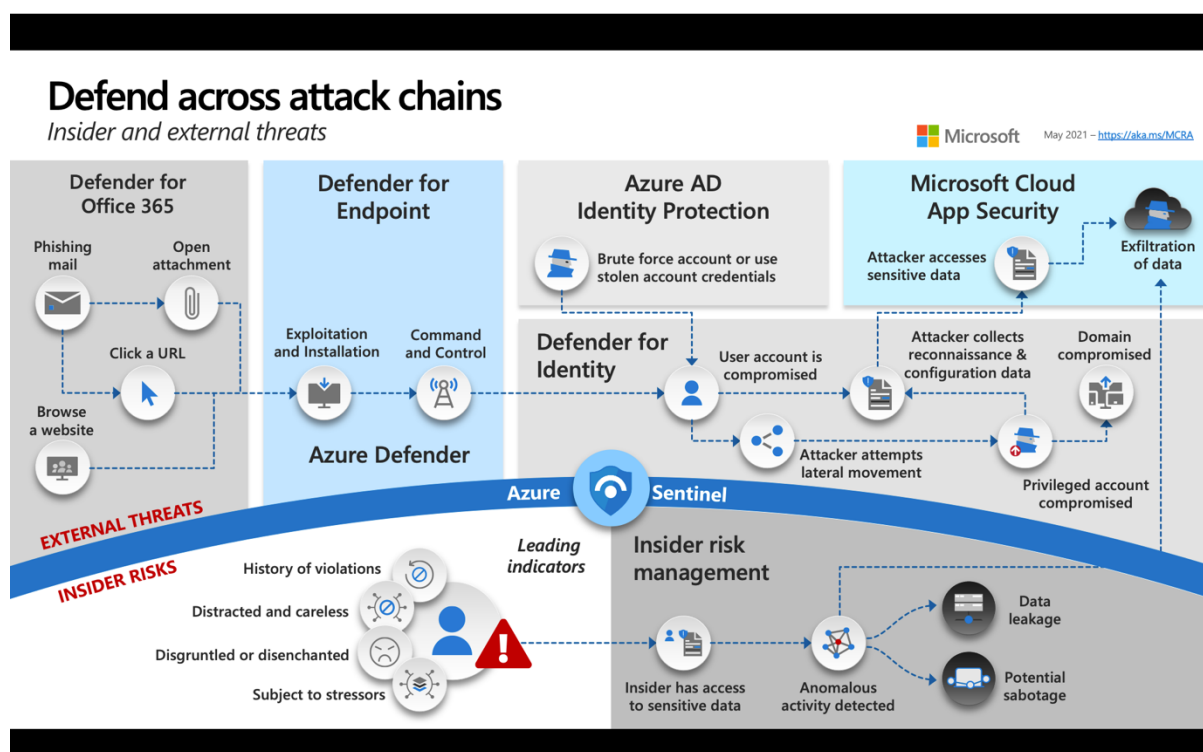
Why using Azure Sentinel?

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 your 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 different 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.

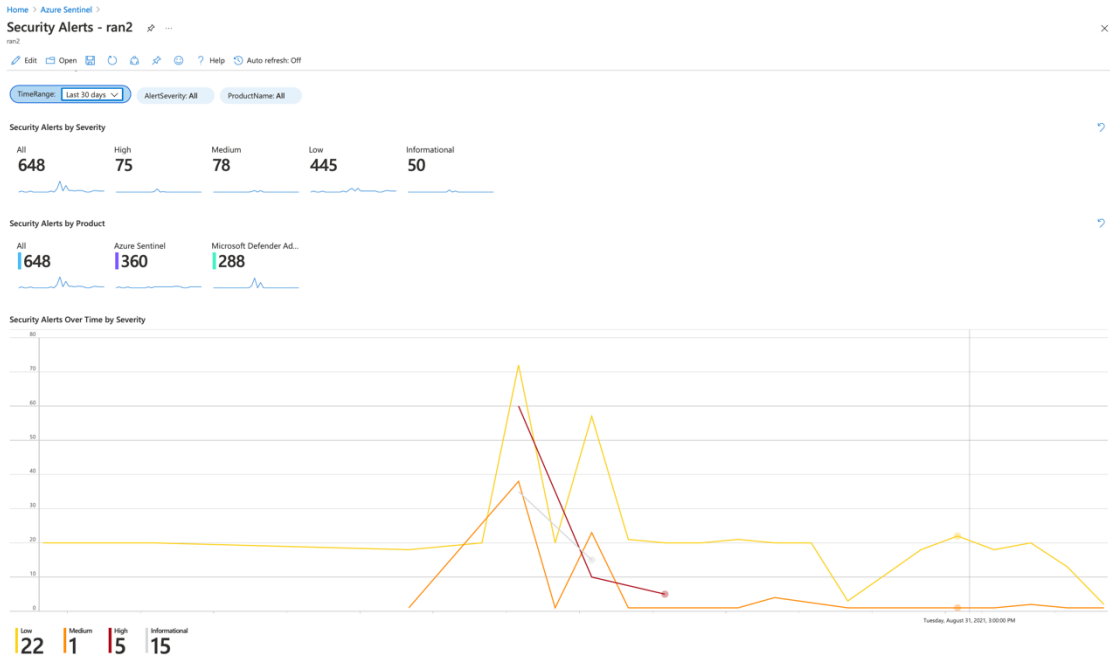
Depends on subscription you bought, your IT team or outsourced vendor (or Help-Desk) should be able to implement suitable features according to your needs by following the [Security Roadmap on Microsoft Defender 365](#) documentation.

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.

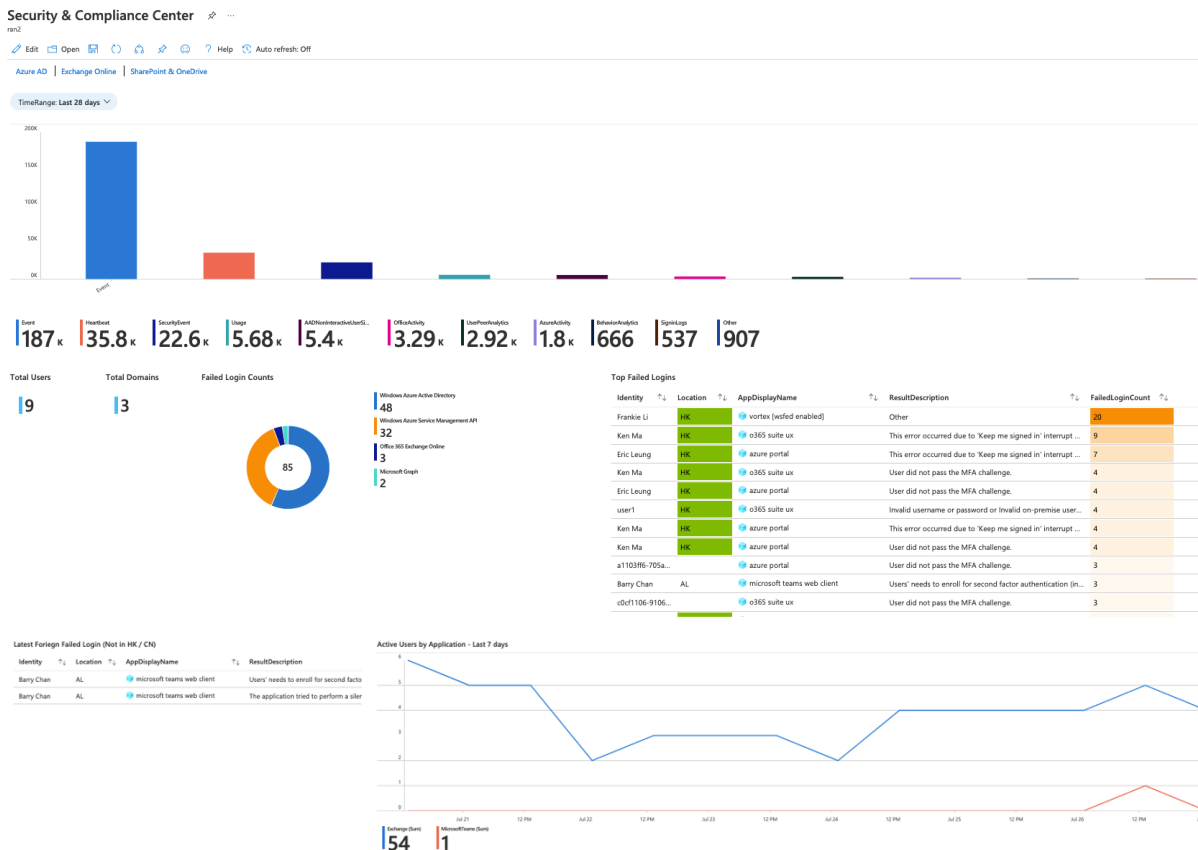


Microsoft©: Azure Sentinel Template - Exchange Online
(Gain insights into MEO by tracing and analyzing all Exchange operations and user activities)

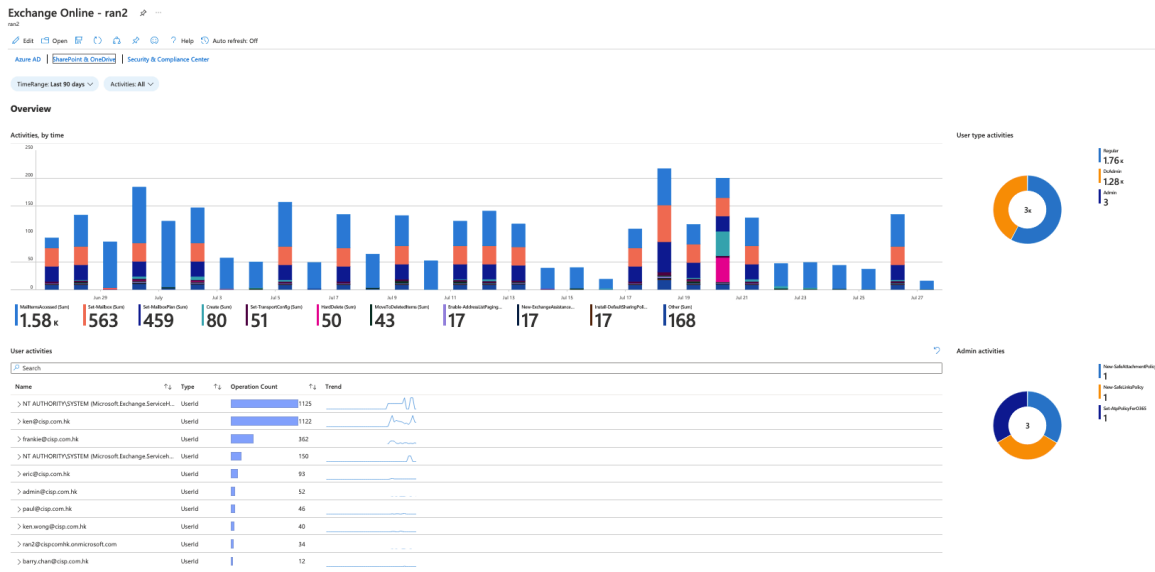


Microsoft©: Azure Sentinel Template - Security Alerts
(Security Alerts dashboard for alerts in your Azure Sentinel environment.)

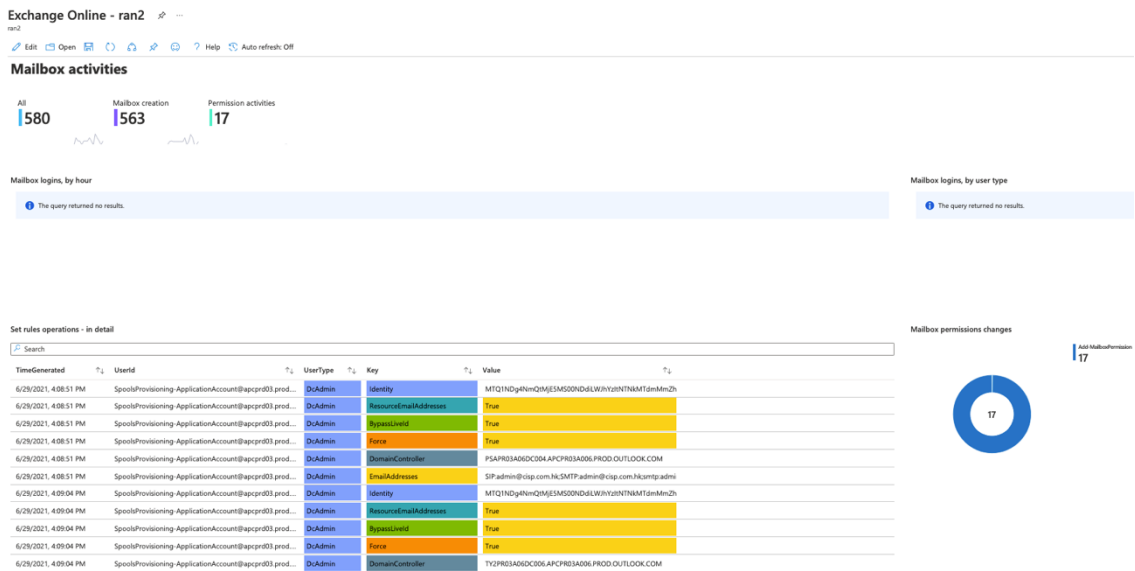
Other than all the out-of-the-box Workbooks available in Azure Sentinel, we create custom rules and workbooks (dashboards) to monitor and detect security alerts/events of Security & Compliance Centre, Exchange Online, Azure Active Directory and SharePoint & OneDrive



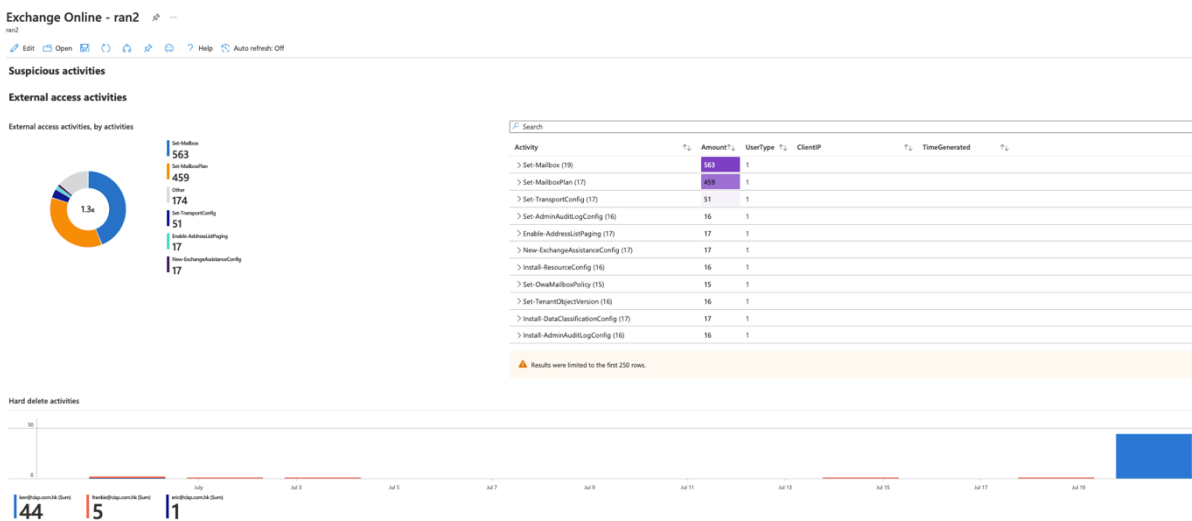
DATC Sentinel Template: Security & Compliance
(Security & Compliance dashboard for login alerts in your Azure Sentinel environment.)



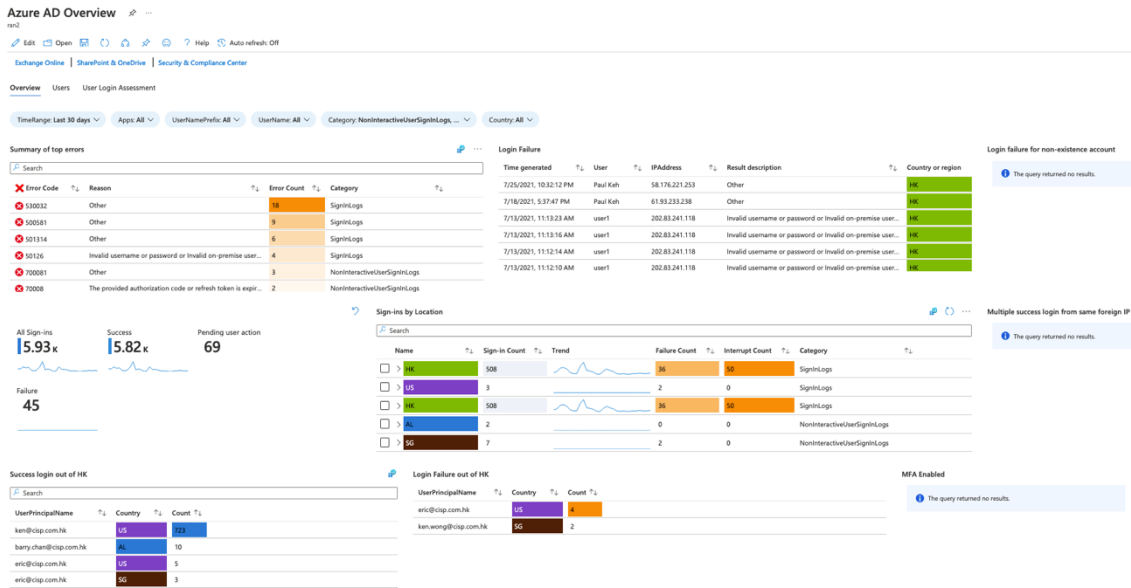
DATC Sentinel Template: Exchange Online
(Exchange Online dashboard an Overview in your Azure Sentinel environment.)



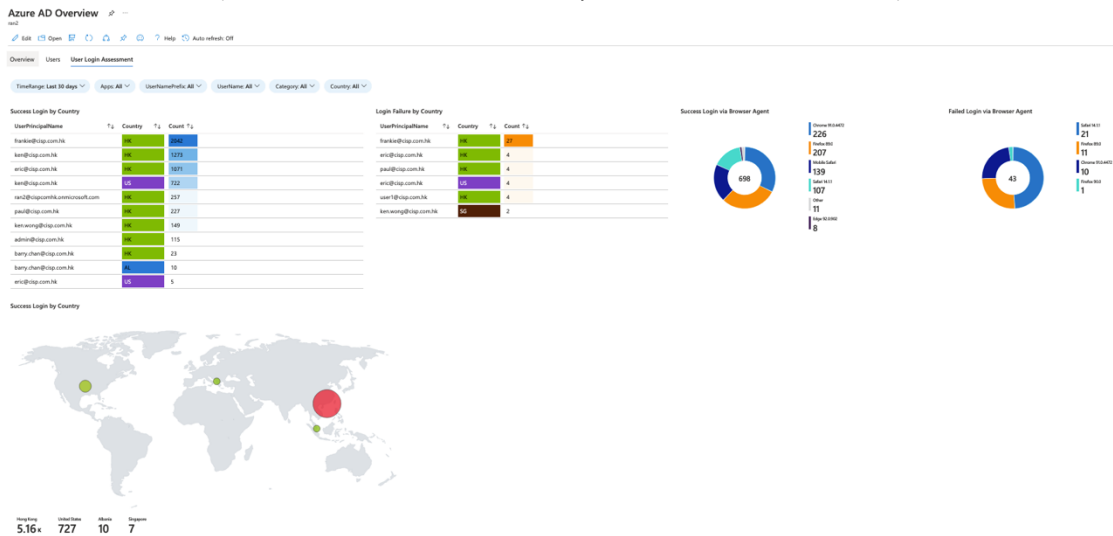
DATC Sentinel Template: Exchange Online
(Exchange Online dashboard for mailbox activities in your Azure Sentinel environment.)



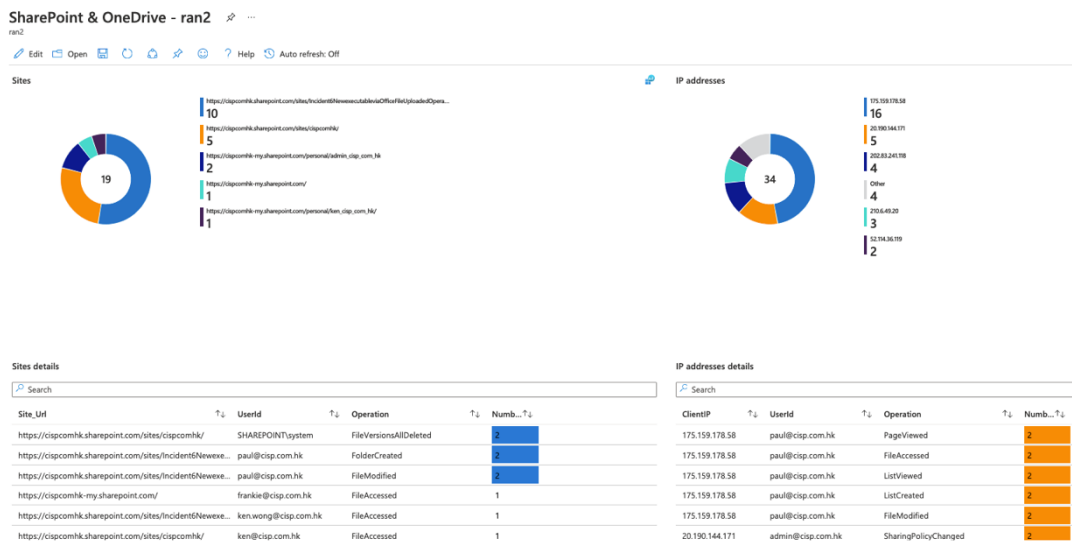
Exchange Online dashboard for Suspicious activities in your Azure Sentinel environment)



DATC Sentinel Template: Azure Active Directory
(Azure AD dashboard on Overview in your Azure Sentinel environment)



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



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)

Microsoft Azure - Analytics rule wizard - Edit existing scheduled rule

Malformed user agent

General **Set rule logic** Incident settings (Preview) Automated response Review and update

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 lon isfuzztrue (OfficeActivity | where UserAgent != ""); (OfficeActivity | where RecordType in ("AzureActiveDirectory", "AzureActiveDirectoryStigLog")) | extend OperationName = Operation | parse ExtendedProperties with * "User-Agent\\\" UserAgent2 '\\\" *
```

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 mappings, 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 (Full Name, AccountCustomEntity)
- IP (Address, IPCustomEntity)

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: 10 | Alerts per day: 10 | Number of events: 10

Microsoft©: Azure Sentinel Analytics Rule - Malformed user agent

Microsoft Azure - Analytics rule wizard - Edit existing scheduled rule

Mail redirect via ExO transport rule

General **Set rule logic** Incident settings (Preview) Automated response Review and update

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.

```
OfficeActivity | where OfficeWorkload == "Exchange" | where Operation in ("New-TransportRule", "Set-TransportRule") | extend p = parse_json(Parameters) | extend fuRelease = case( Operation == "Set-TransportRule", tostring(OfficeObjectId),
```

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 mappings, 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 (Full Name, AccountCustomEntity)
- IP (Address, IPCustomEntity)

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.

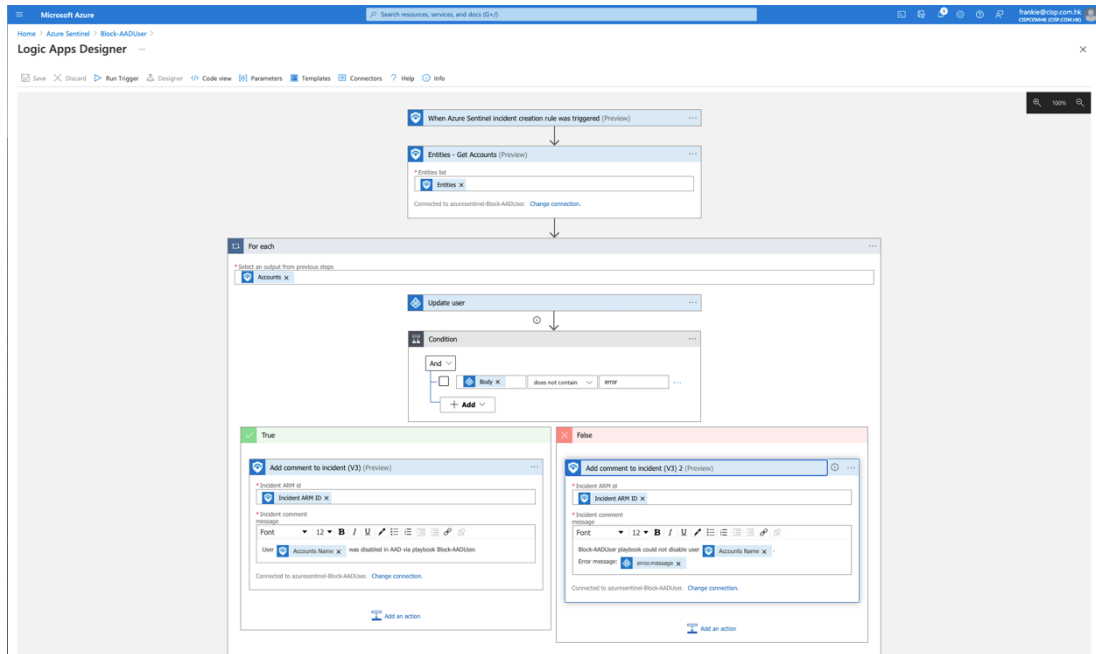
Test with current data

Threshold: 10 | Alerts per day: 10 | Number of events: 11

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

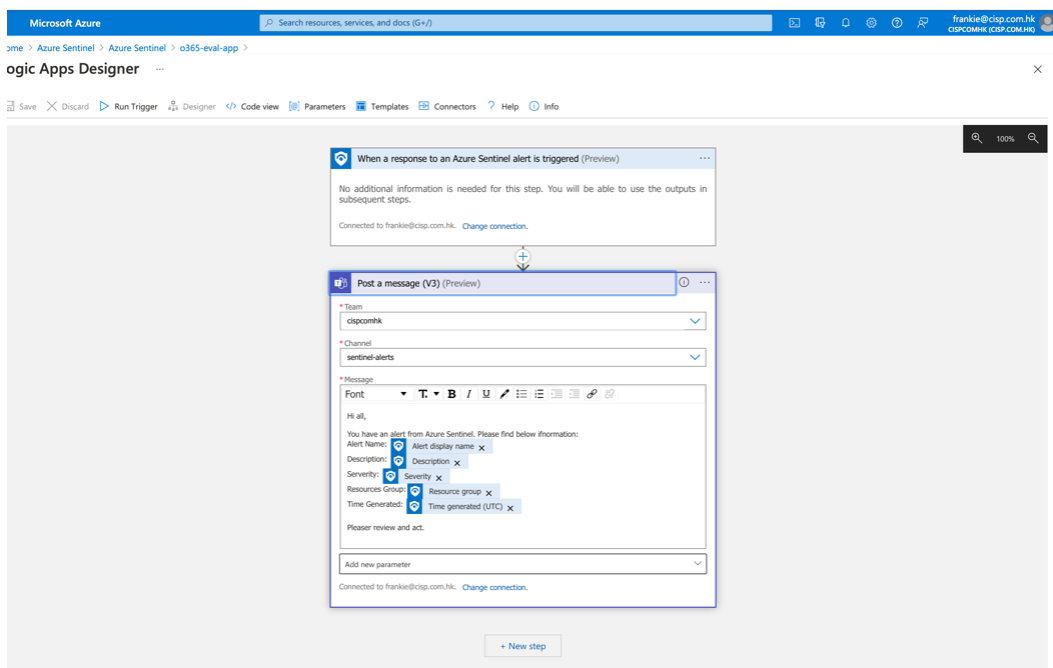
Playbooks are collections of procedures that can be run from Azure Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an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

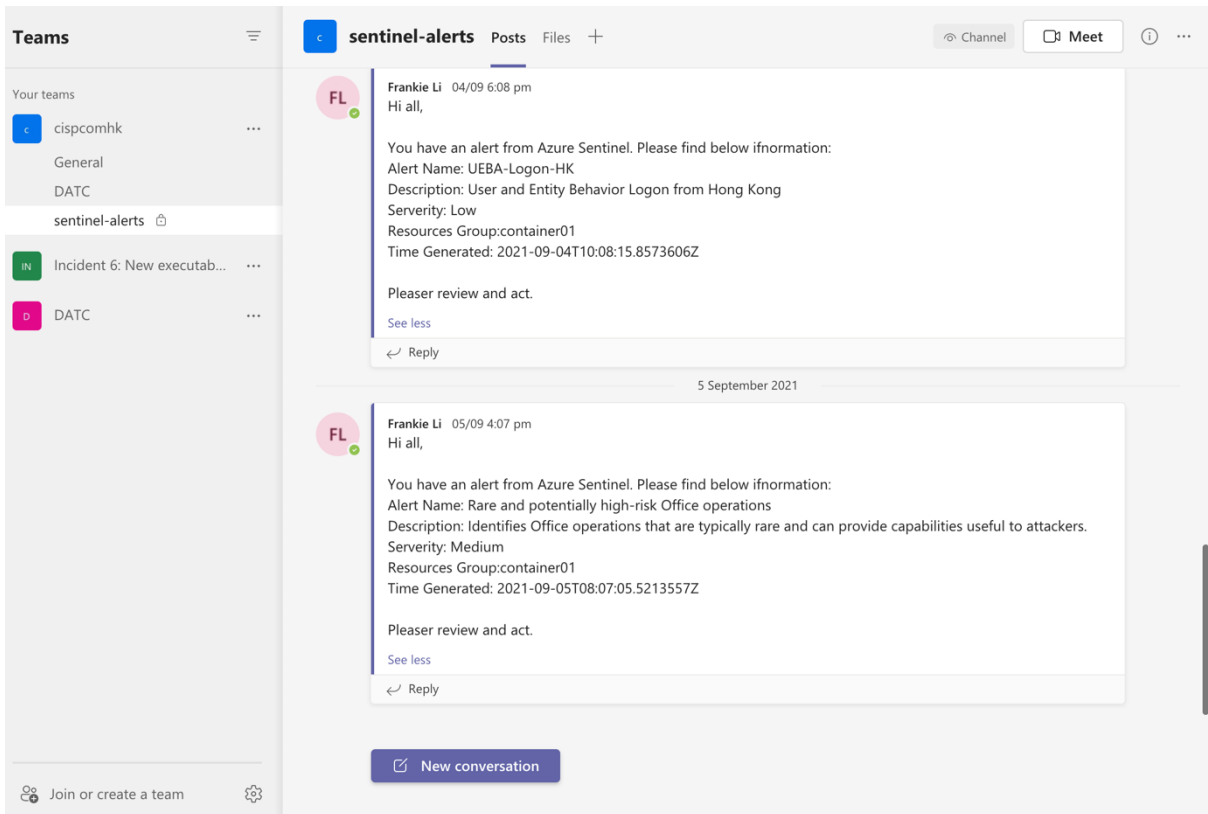


Microsoft©: Sentinel Playbook: Block-AADUser

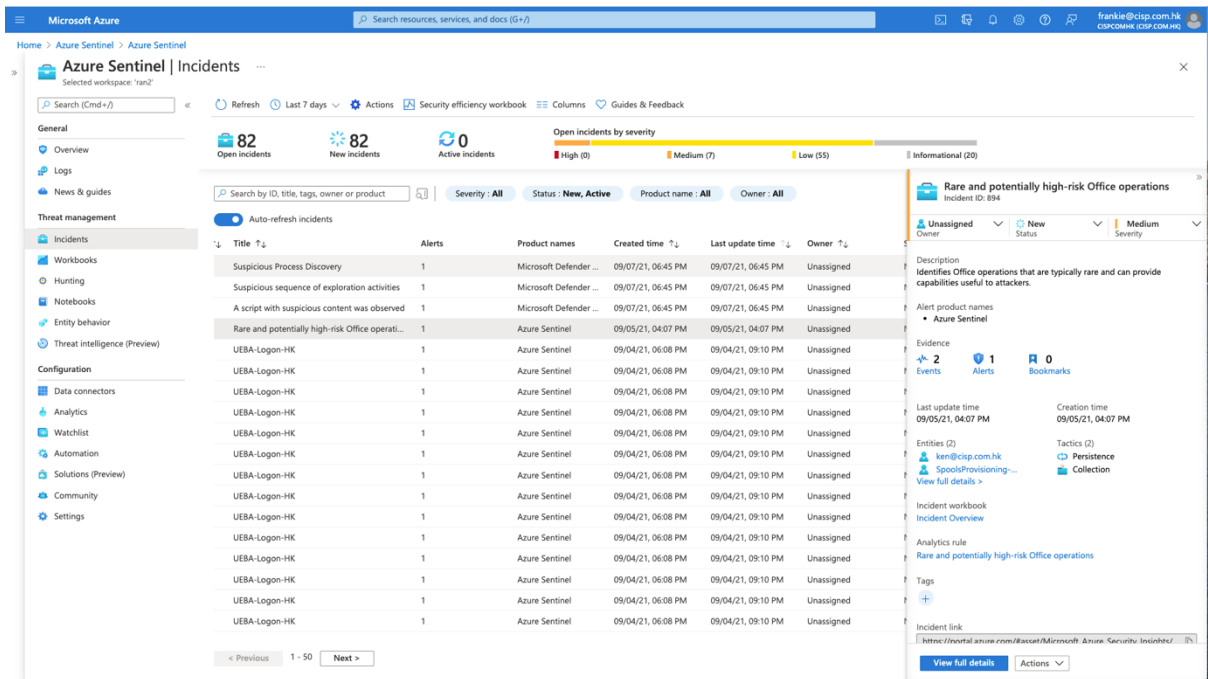
Or, we prefer *to send an alert message to Teams channel* to serve as an open ticket for the incident:



DATC Sentinel Playbook: Teams Channel



Example Sentinel Playbooks: Teams Alerts



Example Sentinel Playbooks: Teams Alerts

Microsoft Azure | Azure Sentinel | Automation

Automation rules (Preview) | Playbooks

Automation rules: 1, Enabled rules: 0, Enabled playbooks: 11

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-Severity	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

Microsoft Azure | Azure Sentinel | Incidents

Open incidents by severity: High (0), Medium (7), Low (55), Informational (20)

Incident ID	Title	Alerts	Product names	Created time	Last update time
897	Suspicious Process Discovery	1	Microsoft Defender ...	09/07/21, 06:45 PM	09/07/21, 06:45 PM
896	Suspicious sequence of exploration activities	1	Microsoft Defender ...	09/07/21, 06:45 PM	09/07/21, 06:45 PM
895	A script with suspicious content was observed	1	Microsoft Defender ...	09/07/21, 06:45 PM	09/07/21, 06:45 PM
894	Rare and potentially high-risk Office operati...	1	Azure Sentinel	09/05/21, 04:07 PM	09/05/21, 04:07 PM
893	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
892	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
891	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
890	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
889	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
888	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
887	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
884	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
883	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
882	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
881	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
880	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
879	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM
878	UEBA-Logon-HK	1	Azure Sentinel	09/04/21, 06:08 PM	09/04/21, 09:10 PM

Suspicious Process Discovery
Incident ID: 897

Description: A known tool or technique was used to gather information on this device. Attackers might be trying to gather information about the target device or network for later attacks.

Evidence: 1 Alerts, 0 Bookmarks

Entities (10) (Preview): win10, powershell.exe, SenseI.exe, MsSense.exe

Incident link: https://portal.azure.com/#blade/MicrosoftAzureSentinel/IncidentOverview

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.



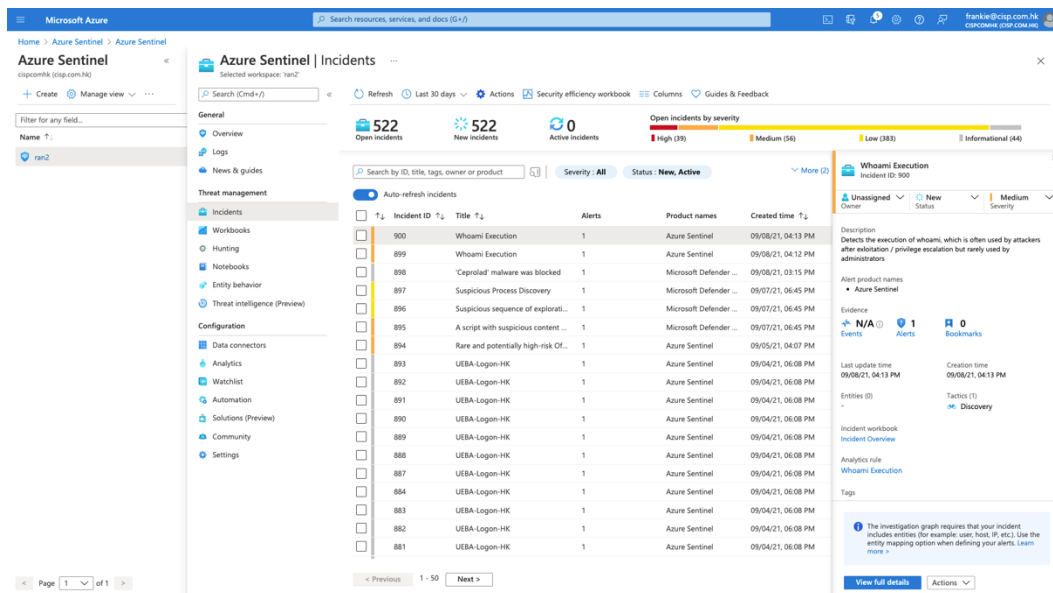
Microsoft©: Azure Sentinel: End-to-end solution for security operations

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.

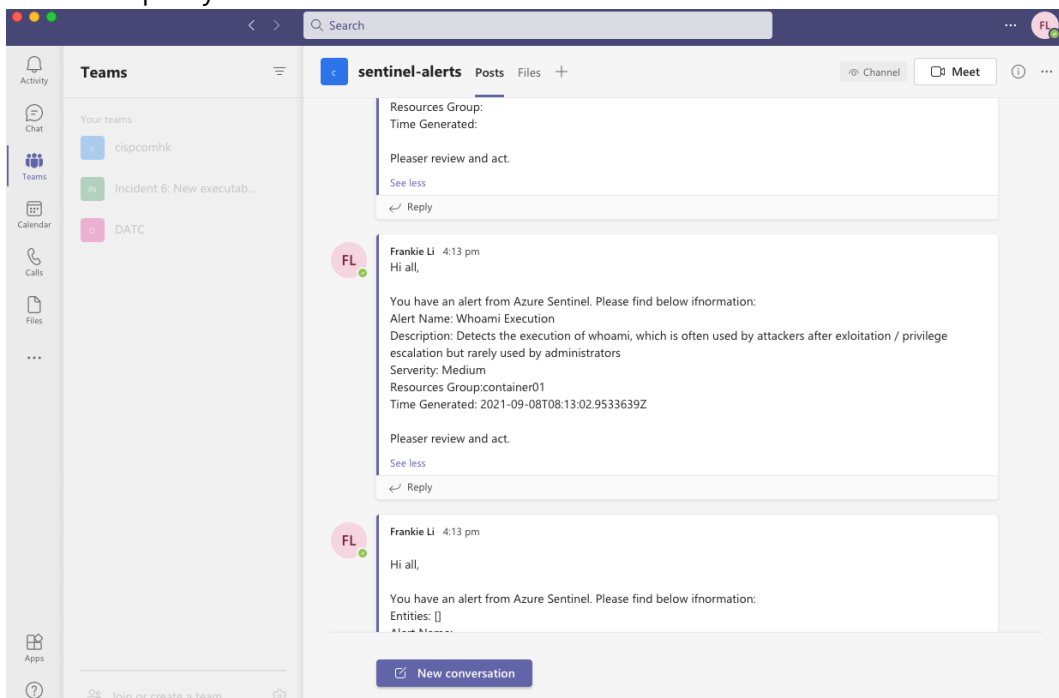
[Sysmon](#) “is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation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



A simple Sysmon Sentinel detection rule: whoami started from PowerShell



To simply 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 innovation for detection of suspicious parameters on the latest cyber threats.

The screenshot shows the JoeSandbox Cloud interface with the following sections:

- General Information:** Analysis ID: 334401. Most Interesting Screenshot: A Windows desktop environment.
- Detection:** A vertical bar indicates the detection level: MALICIOUS (red), SUSPICIOUS (orange), CLEAN (green), and UNKNOWN (grey). Score: 56, Range: 0 - 100, Whitelisted: false, Confidence: 100%.
- Signatures:** A list of detected signatures including:
 - 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 (jil...)
 - 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 radar chart showing various threat indicators.
- Startup:** A list of system processes and commands, including powershell.exe and conhost.exe.
- Malware Configuration:** A section stating "No configs have been found".

DATC: A Windows PowerShell threat found on 3 September 2021

The screenshot shows the Azure Sentinel Analytics console with the following details:

- Active Rules Summary:** 57 Active rules. Severity breakdown: High (8), Medium (3), Low (1), Informational (35).
- Active Rules Table:**

SEVERITY	NAME	RULE TYPE	STATUS	TACTICS	LAST MODIFIED
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled		08/19/21, 01:40 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled		09/05/21, 05:10 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled		06/11/21, 03:12 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled		09/05/21, 05:11 PM
High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled		09/05/21, 05:13 PM
High	CVE-2021-1675 Print Spooler Exploitation IPC A...	Scheduled	Enabled	Lateral Move...	07/07/21, 04:21 PM
High	Empire PowerShell Launch Parameters	Scheduled	Enabled		09/08/21, 12:26 PM
High	Known Manganese IP and UserAgent activity	Scheduled	Enabled		09/05/21, 05:25 PM
Medium	Anomalous login followed by Teams action	Scheduled	Enabled		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		06/13/21, 04:14 PM
Medium	Malformed user agent	Scheduled	Disabled		06/13/21, 04:15 PM
Medium	Malicious Inbox Rule	Scheduled	Enabled		06/13/21, 03:07 PM
Medium	Multiple users email forwarded to same destinat...	Scheduled	Enabled		06/13/21, 04:16 PM
Medium	New executable via Office FileUploaded Operati...	Scheduled	Enabled	Command and ...	06/13/21, 04:06 PM
Medium	Office policy tampering	Scheduled	Disabled		06/13/21, 04:16 PM
Medium	Rare and potentially high-risk Office operations	Scheduled	Enabled		06/13/21, 04:06 PM
Medium	RDP session from Non jump host IP	Scheduled	Enabled		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
- Empire PowerShell Launch Parameters Rule Detail:**
 - Id:** 411bcbf12-5a9a-419f-b33f-2f36ab0128a5
 - Description:** Detects PowerShell invocation with suspicious parameters. @ItsReallyNick: *0/59 on static engines. Sort of expected given it just launches local PowerShell script. Payload detection reminder: this doesn't use
 - Rule query:**

```

// From the sigma/rules/windows_process_creation
folder
// title: Empire PowerShell Launch Parameters
// https://github.com/Neo23x0/signature-base/blob/master/yara/gen_powershell_invocation.yar
// https://unit42.paloaltonetworks.com/...

```
 - 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.

```
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;
```

Results | Chart | Columns | Add bookmark | Display time (UTC+00:00)

Completed. Showing results from the last 4 hours. 00:01.4 1 records

	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 Azure Sentinel interface. On the left, an alert is displayed with the following details:

- Alert from dc.windomain.local** (Incident ID: 901)
- Status: Unassigned
- Severity: Medium
- Description: 2021-09-08T08:48:42.9230000Z From Remote IP: 192.168.38.104 User: WINDOMAIN\vagrant
- Alert product names: Azure Sentinel
- Evidence: 1 Events, 1 Alerts, 0 Bookmarks
- Last update time: 09/08/21, 05:08 PM
- Creation time: 09/08/21, 05:08 PM
- Entities (0): -
- Tactics (0): --
- Incident workbook: Incident Overview
- Analytics rule: RDP policy violation - connect from non jumphost IP

On the right, the Timeline view shows a single alert entry:

- 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

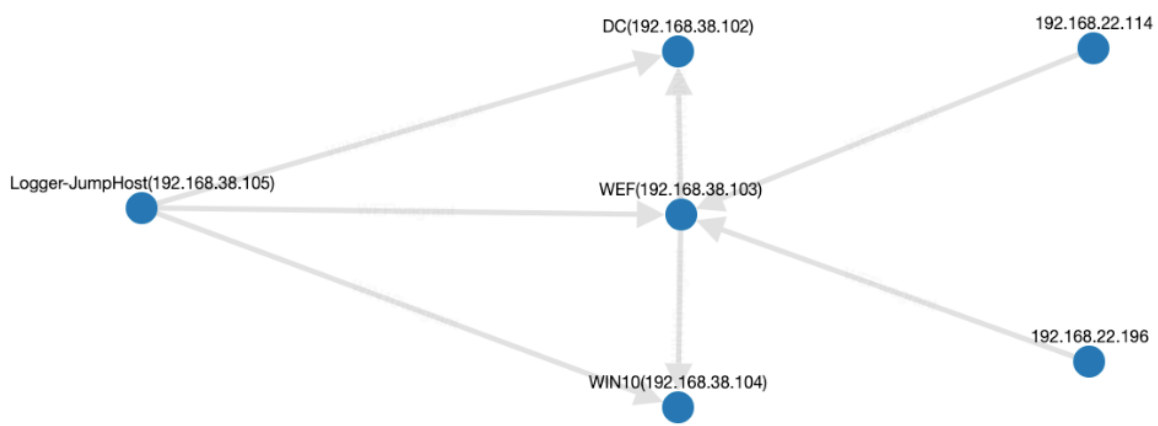
Description: 2021-09-09T02:09:31.4870000Z From Remote IP: 192.168.22.196 User: DESKTOP-F7NIGP1\Forensic
Severity: Medium

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](#)
- [Email, calendar, and scheduling](#)
- [Meetings, calling, and chat](#)
- [Social, intranet, and storage](#)
- [Knowledge, insights, and content](#)
- [Analytics](#)
- [Project and task management](#)
- [Automation, app building, and chatbots](#)
- [Endpoint and app management](#)
- [Threat protection](#)
- [Identity and access management](#)
- [Information protection](#)
- [Information governance](#)
- [eDiscovery and auditing](#)
- [Insider risk management](#)
- [Windows](#)

	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 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

	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 Add-on	F5 Sec + Comp Add-on	F3	
Desktop client apps ¹	•	•				•	•												
Office Mobile apps ²	•	•			•	•	•						Read only	• ³					• ³
Office for the web	•	•			•	•	•						Read only	•					•
Install apps on up to 5 PCs/Mac + 5 tablets + 5 smartphones	•	•			• ⁴	•	•							• ¹					• 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 apps only

Email, calendar, and scheduling

	Plan 2	Plan 2		Plan 1	Plan 2	Plan 2				See footnote 1	Kiosk								Kiosk
Exchange 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.
²50 GB limit

	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 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

	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 Add-on	F5 Sec + Comp Add-on	F3	
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>

Social, intranet, and storage

	Plan 2	Plan 2		Plan 1	Plan 2	Plan 2				Kiosk ¹	Kiosk ¹								Kiosk ¹
SharePoint Additional storage per license ²	10GB	10GB		10GB	10GB	10GB													
OneDrive personal storage	Unlimited ³	Unlimited ³		1 TB	Unlimited ³	Unlimited ³							2GB	2GB					2 GB
Yammer Enterprise	•	•		•	•	•							• ¹	• ¹					• ¹

¹Cannot be administrators. No site mailbox. No personal site.
²In addition to 1TB storage provided per organization.
³Microsoft 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.

Knowledge, insights, and content

	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 Add-on	F5 Sec + Comp Add-on	F3	
Microsoft Graph API	•	•			•	•	•						•	•					•
Microsoft Search	•	•			•	•	•												•
Microsoft Stream	•	•			•	•	•						• ¹	• ¹					• ¹
Microsoft Forms ²	•	•			•	•	•												•
Microsoft Lists	•	•			•	•	•												•
Delve	•	•			•	•	•												•

¹Users can record meetings and consume Stream content but cannot publish to Stream.
²Licensed users can create/share/manage forms. Completing/responding does not require a Forms license.

Analytics

	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 Add-on	F5 Sec + Comp Add-on	F3	
Productivity Score	•	•			•	•	•						•	•					•
Secure Score	•	•			•	•	•						•	•					•
Compliance Management	•	•			•	•	•						•	•					•
MyAnalytics (full)	•	•			•	•	•												
Insights by MyAnalytics	•	•			•	•	•												
Power BI Pro	•	•			•	•	•												

Project and task management

	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 Add-on	F5 Sec + Comp Add-on	F3	
Microsoft Planner	•	•			•	•	•						•	•					•
Microsoft To-Do	•	•			•	•	•												•
Briefing Email	•	•			•	•	•												•

Information Worker Plans

Frontline Worker Plans

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 Add-on	F5 Security + Compliance Add-on	F3
\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80		\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4

USD ERP per user per month

Identity and access management

	Plan 1	Plan 2	Plan 2					Plan 1	Plan 2			Plan 1	Plan 1	Plan 2		Plan 2	
Azure Active Directory Premium																	
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 Discovery	•	•						•	•			•	•				
Office 365 Cloud App Security	•	•						•	•			•	•				
Microsoft Cloud App Security	•	•	•					•	•			•	•				

Information protection

	Plan 1	Plan 2	Plan 2		AP for O365	AP for O365	Plan 1	Plan 2			Plan 1	Plan 1	Plan 2	Plan 2	
Azure Information Protection															
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	•	•			•	•	•	•			•	•		•	•

Information Worker Plans

Frontline Worker Plans

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 Add-on	F5 Security + Compliance Add-on	F3
\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80		\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4

USD ERP per user per month

Automation, app building, and chatbots

Power Apps for Microsoft 365 ¹	•	•			•	•	•					•	•				•
Power Automate for Microsoft 365 ¹	•	•			• ²	• ²	• ²			• ³	• ³			•			• ²
Power Virtual Agent for Teams ¹	•	•			•	•	•							•			•
Dataverse for Teams ¹	•	•			•	•	•							•			•

¹Refer to the licensing FAQs and Licensing Guide at <https://docs.microsoft.com/power-platform/admin/powerapps-flow-licensing-faq> for details including functionality limits.

²Cloud flows only.

³Desktop 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		•	•											•		•	

Information Worker Plans

Frontline Worker Plans

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 Add-on	F5 Security + Comp Add-on	F3
\$32	\$57	\$12	\$12	\$8	\$20	\$35	\$8.80	\$14.80		\$5	\$10	\$2.25	\$8	\$8	\$8	\$13	\$4

USD ERP per user per month

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	•	•		•			•	•							•	•	

¹30-day minimum retention period.

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 ATTACK	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 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 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	Surfaces 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', 'gzip', 'cmd', 'bat' file extensions. Additionally, identifies when a given user is uploading these files to another users workspace. This may be indication of a staging location for malware or other malicious activity	Office 365 OfficeActivity	Low	CommandAndControl	

Microsoft©: Azure Sentinel Detection Rules – Office 365 Activity
(Security Detection Rules for your Azure Sentinel environment.)

#	Rule Name	Description	Log Source	Severity	MITRE ATTACK	Threat Intel
20	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
21	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 Privilege
22	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
23	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
24	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
25	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
26	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
27	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
28	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
29	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
30	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
31	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
32	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 Office365_Rules_v4

Home Insert Draw Page Layout Formulas Data Review View Tell me

Calibri (Body) 11

General

Hyperlink 2 Normal 2 Normal 3 Normal 4 Normal

Bad Good Neutral Calculation Check Cell

Share Comments

A7

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	Detection 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 @Cy3rWard0g	selection and not filter	Programs using PowerShell directly without invocation of a dedicated interpreter MSP Detection Searcher Citrix ConfigSync.ps1	attack.execution attack.t1059.001	medium	Event where ((EventID == 4103 and ContextInfo contains *) and not (ContextInfo contains 'powershell.exe'))[Event] where ((EventID == 400 and HostApplication contains *) and not (HostApplication endswith 'powershell.exe'))	https://github.com/Cy3rWard0g/ThreatHunter-Playbook/tree/master/playbooks/windows/O2_execution/11086_powershell/alternate
2	Silence.EDA Detection	Detects Silence empire eDNSagent	Alina Stephenkova, Group-IB, oscd.community	empire and dnscat		attack.execution attack.t1059.001 attack.t1086 attack.command_and_control attack.t1071.004 attack.t1071 attack.t1572 attack.impact attack.t1519 attack.g0091 attack.s0363	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-Dnscat2Tunnel' and ScriptBlockText contains 'set type=\$LookupType' nserver' and ScriptBlockText contains '\$Command nslookup 2&1 Out-String' and ScriptBlockText contains 'New-RandomDNSField' and ScriptBlockText contains '[Convert]::ToString(\$SYNOptions, 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	Bhadesh Raj	selection		attack.discovery attack.execution attack.t1059.001	high	Event where (EventID == 4104 and (ScriptBlockText contains 'Function Get-ADReconComOb' or ScriptBlockText contains 'ADRecon-Report.xlsx'))	https://github.com/sense-of-security/ADRecon https://bi-zone.medium.com/from-pent-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319
5	Automated Collection Command PowerShell	Tool established within a system or network, an adversary may use automated techniques for collecting internal data.	frack113	all of them		attack.collection attack.t1119	medium	Event where (EventID == 4104 and (ScriptBlockText contains '.doc' or ScriptBlockText contains '.docx' or ScriptBlockText contains '.xls' or ScriptBlockText contains '.xlsx' or ScriptBlockText contains '.ppt' or ScriptBlockText contains '.pptx' or ScriptBlockText contains '.rtf' or ScriptBlockText contains '.pdf' or ScriptBlockText contains '.txt') and ScriptBlockText contains 'Get-Children' and ScriptBlockText contains '-Recurse' and ScriptBlockText contains '-Include')	https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/11119/11119.r
6	Bad Opsec Powershell Code Artifacts	Focuses on trivial artifacts observed in variants of prevalent offensive ps1 payloads, including Cobalt like 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, it appears to be fairly limited in many environments.	attack.execution attack.t1059.001 attack.t1086	critical	Event where ((EventID == 4104 and (ScriptBlockText contains '\$DoIt' or ScriptBlockText contains 'harmj0n' or ScriptBlockText contains 'mattifestation' or ScriptBlockText contains 'RastaMouse' or ScriptBlockText contains 'lflkin_' or ScriptBlockText contains '\$Dedebeef')) or (EventID == 4103 and (Payload contains '\$DoIt' or Payload contains 'harmj0n' or Payload contains 'mattifestation' or Payload contains 'RastaMouse' or Payload contains 'lflkin_' or Payload contains '\$Dedebeef'))	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.mdeditor.tw/pl/pgft
7	Execution via CL_Invocation.ps1	Detects Execution via Synchvoke 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 'Synchvoke')	https://github.com/LOLBAS-Project/LOLBAS/blob/master/vml/OSScripts/CL_Invocation.v https://twitter.com/bohops/status/948061991012327424
8	Execution via CL_Mutueverifiers.ps1	Detects Execution via runAfterCancelProcess in CL_Mutueverifiers.ps1 module	oscd.community, Natalia Shornikova	selection		attack.defense_evasion attack.t1216	high	Event where (EventID == 4104 and ScriptBlockText contains 'CL_Mutueverifiers.ps1' and ScriptBlockText contains 'runAfterCancelProcess')	https://github.com/LOLBAS-Project/LOLBAS/blob/master/vml/OSScripts/CL_muteverifi https://twitter.com/pabrakeon/status/99511125447577600
9	Clear PowerShell History	Detects keywords that could indicate clearing PowerShell history	Ilyas Oshkov, Jonhnathan Ribeiro, Daniil Yugoslavskiy, 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/7363a856c3cbadeb71085147f042c1a
10	PowerShell Create Local User	Detects creation of a local user via PowerShell	@ROXPinTeddy	selection	Legitimate user creation	attack.execution attack.t1059.001 attack.t1086 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/11136/11136.r

Ready

Count: 0 Sum: 0

120%