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

Contents

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?

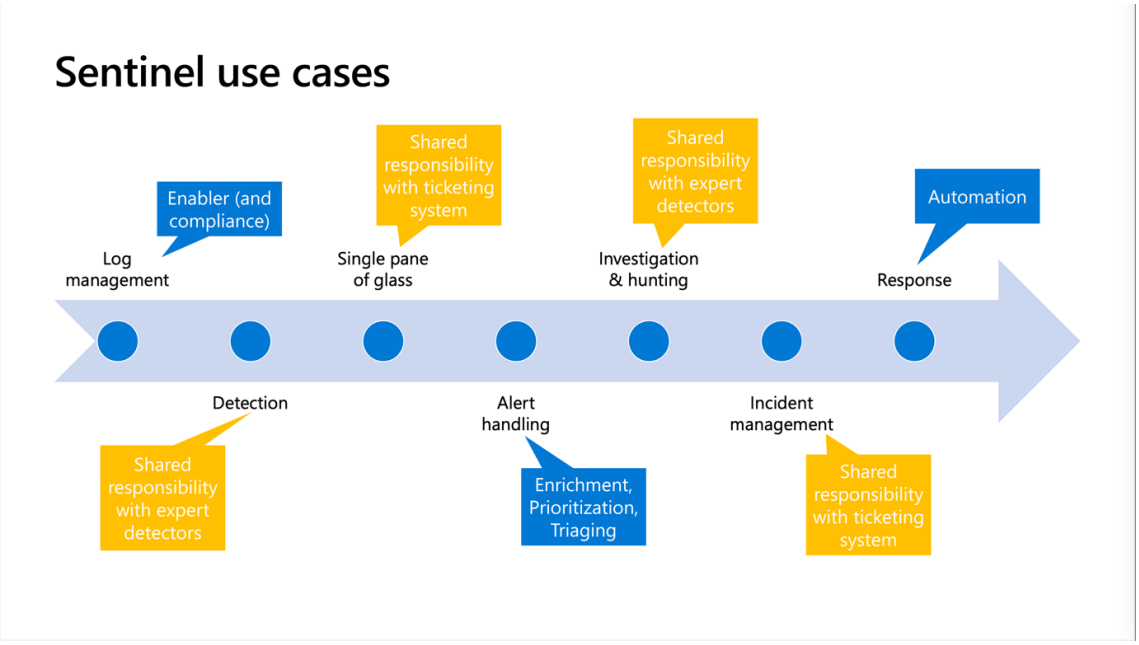
Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert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

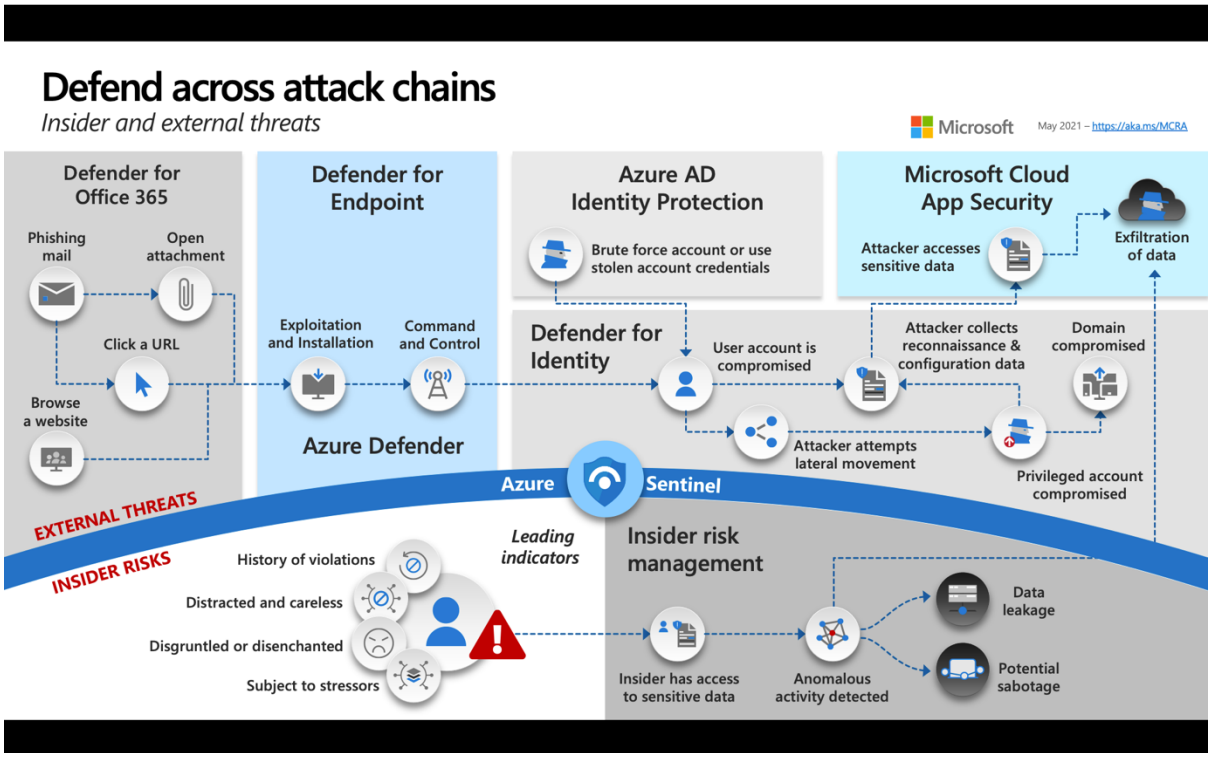
Why using Azure Sentinel?

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.

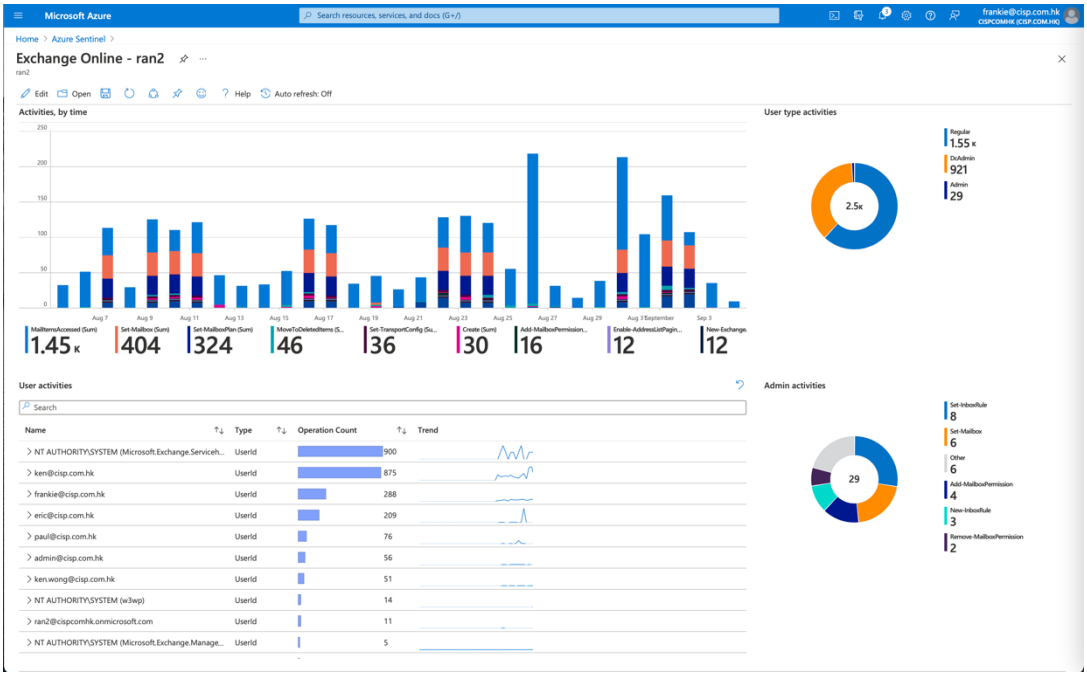
Use Case #1:Microsoft Defender for Office 365

Microsoft Defender 365 (previously named as Microsoft 365 ATP) comes in 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.



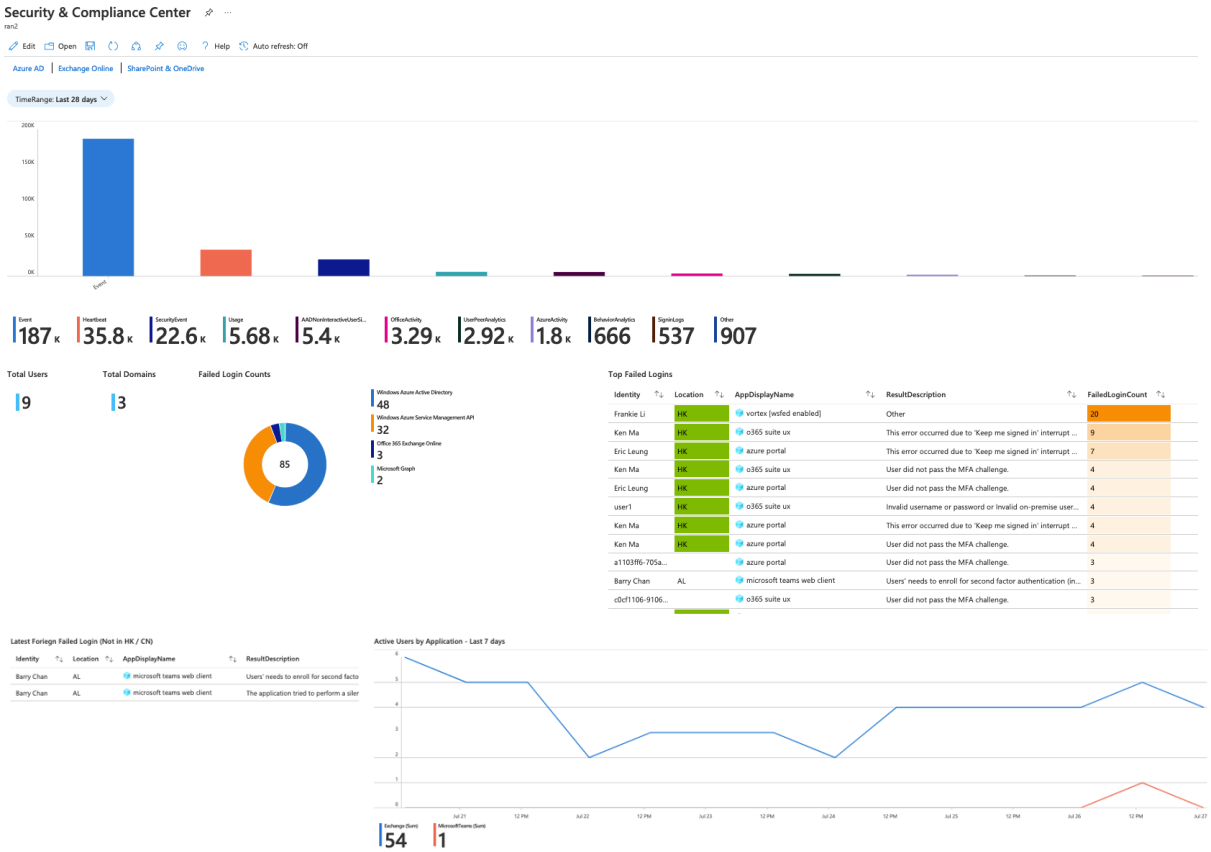
Microsoft©: Azure Sentinel Template - Exchange Online

(Gain insights into MEO by tracing and analyzing all Exchange operations and user activities)

Microsoft©: Azure Sentinel Template - Security Alerts

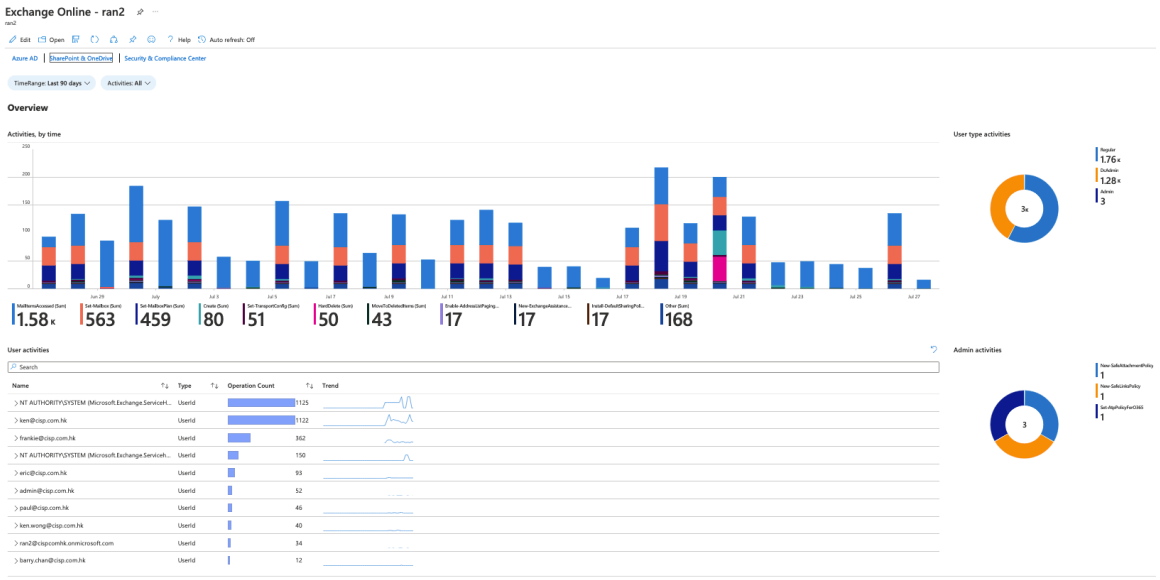
(Security Alerts dashboard for alerts in your Azure Sentinel environment.)

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



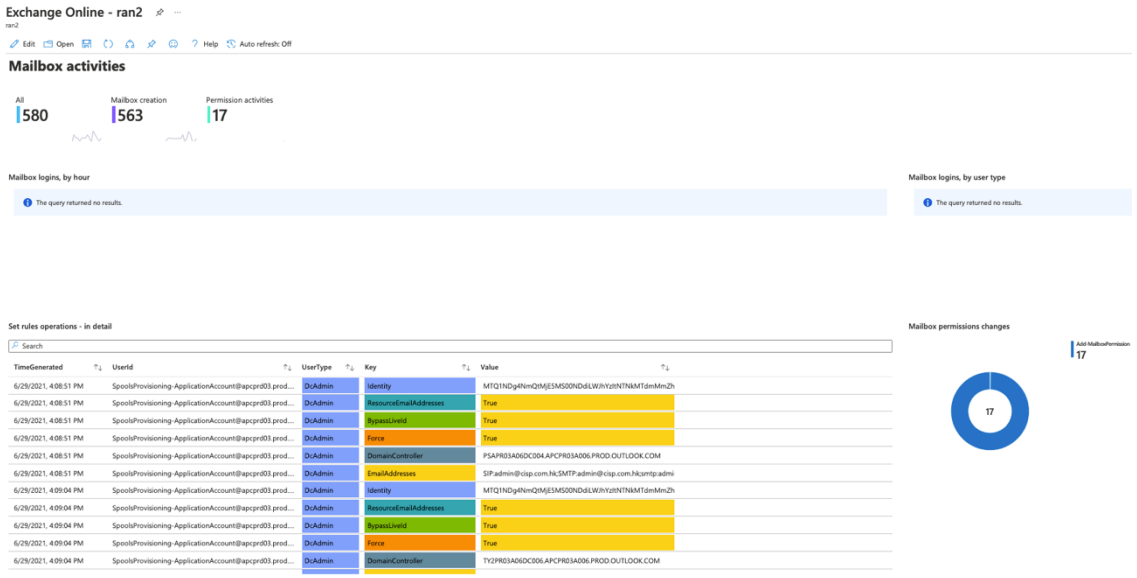
DATC Sentinel Template: Security & Compliance

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



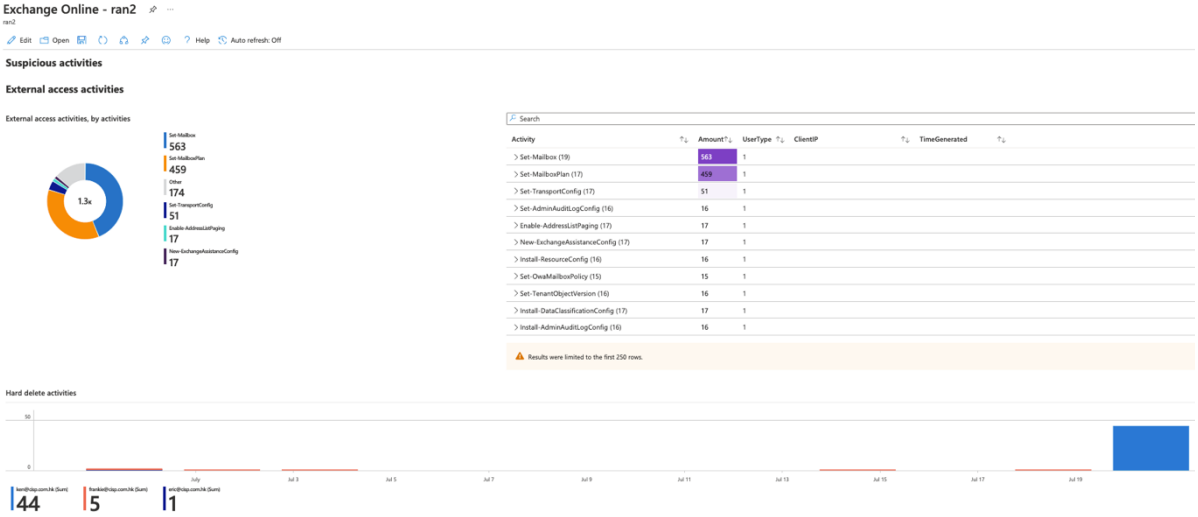
DATC Sentinel Template: Exchange Online

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

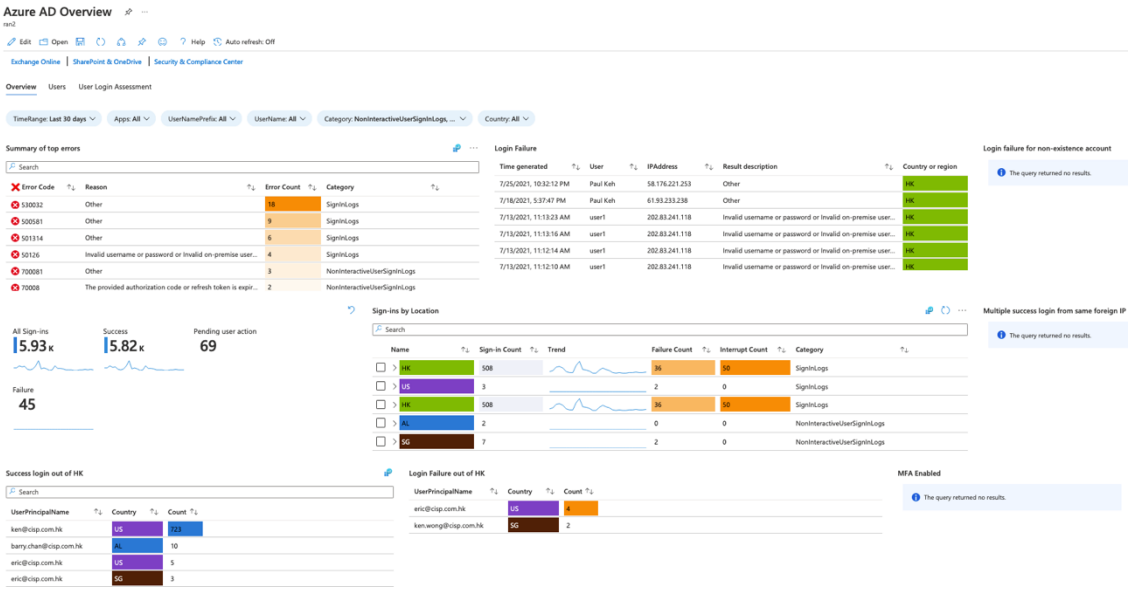


DATC Sentinel Template: Exchange Online

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

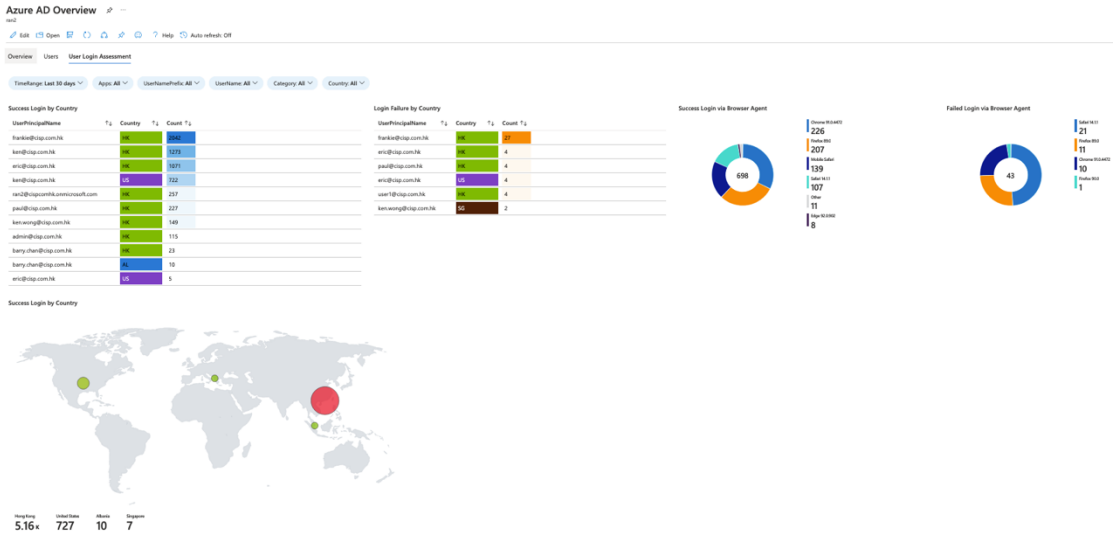


Exchange Online dashboard for Suspicious activities in your Azure Sentinel environment)

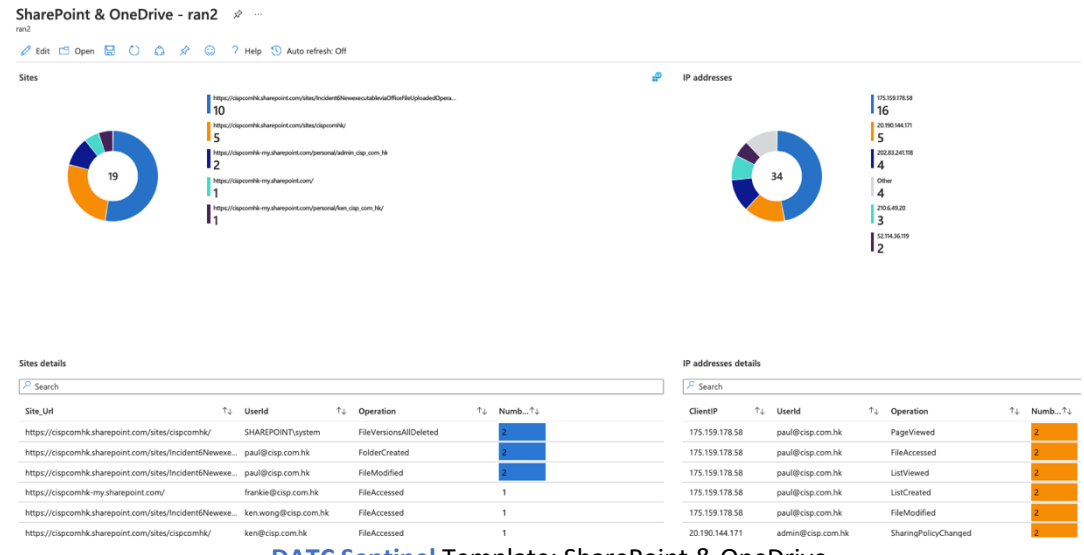


DATC Sentinel Template: Azure Active Directory

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



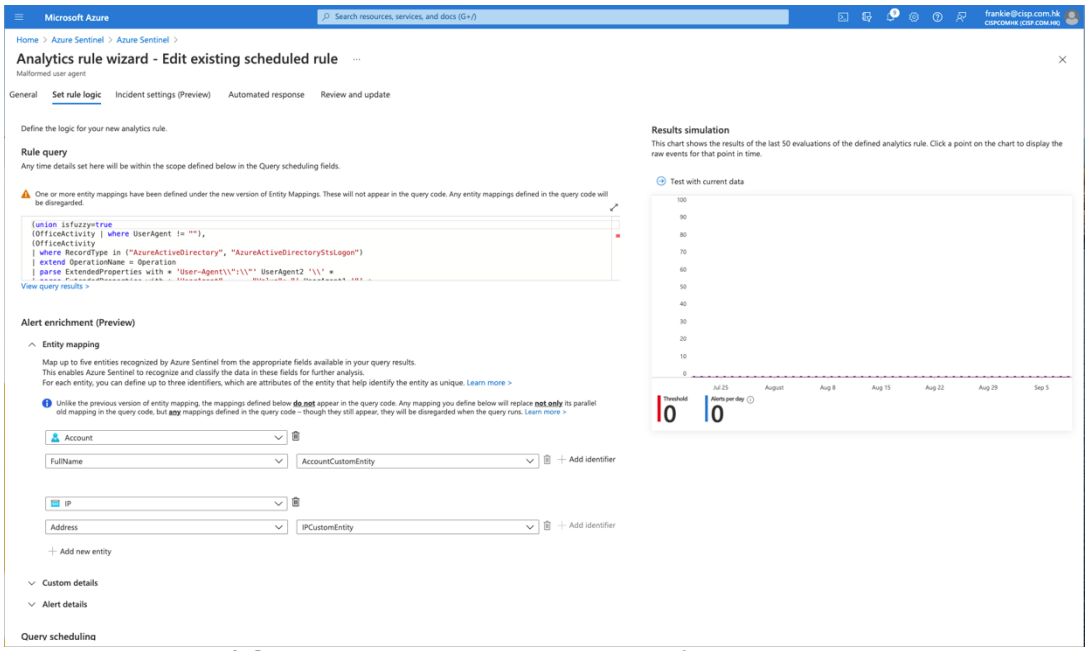
(Azure AD dashboard on User Login Assessment in your Azure Sentinel environment)



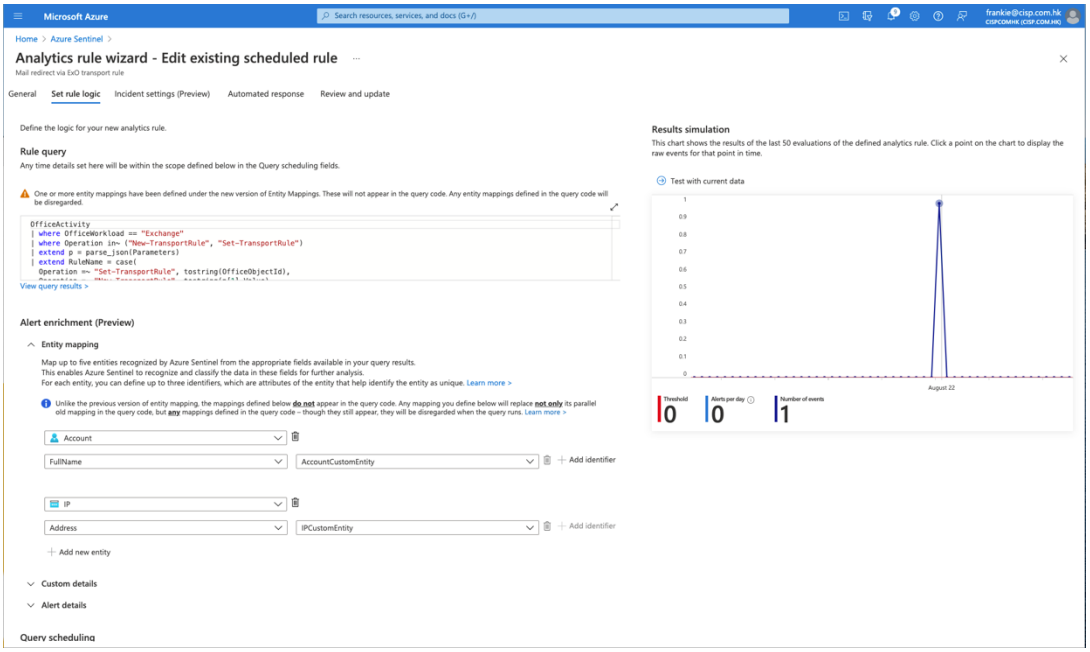
DATC Sentinel Template: SharePoint & OneDrive

(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)



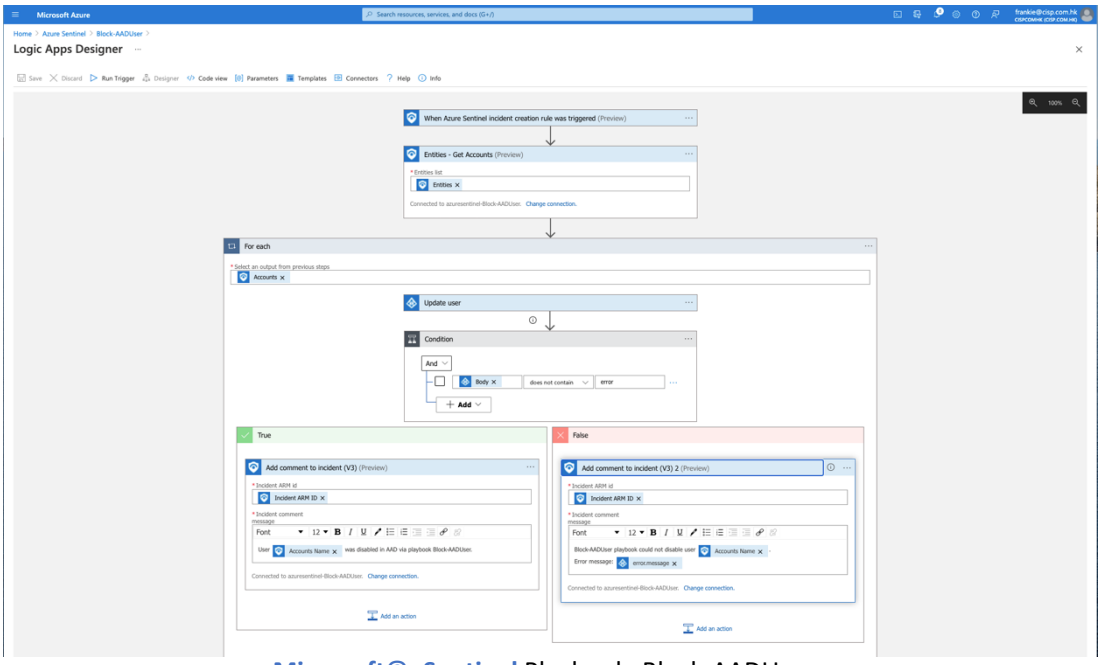
Microsoft©: Azure Sentinel Analytics Rule - Malformed user agent



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

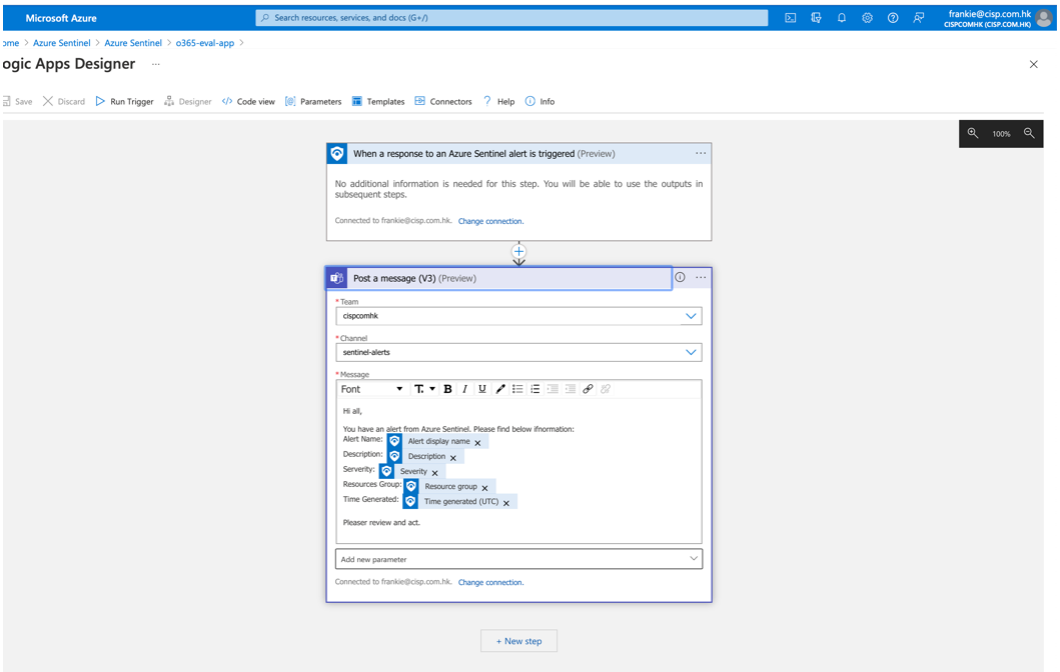
Playbooks are collections of procedures that can be run from Azure Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an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

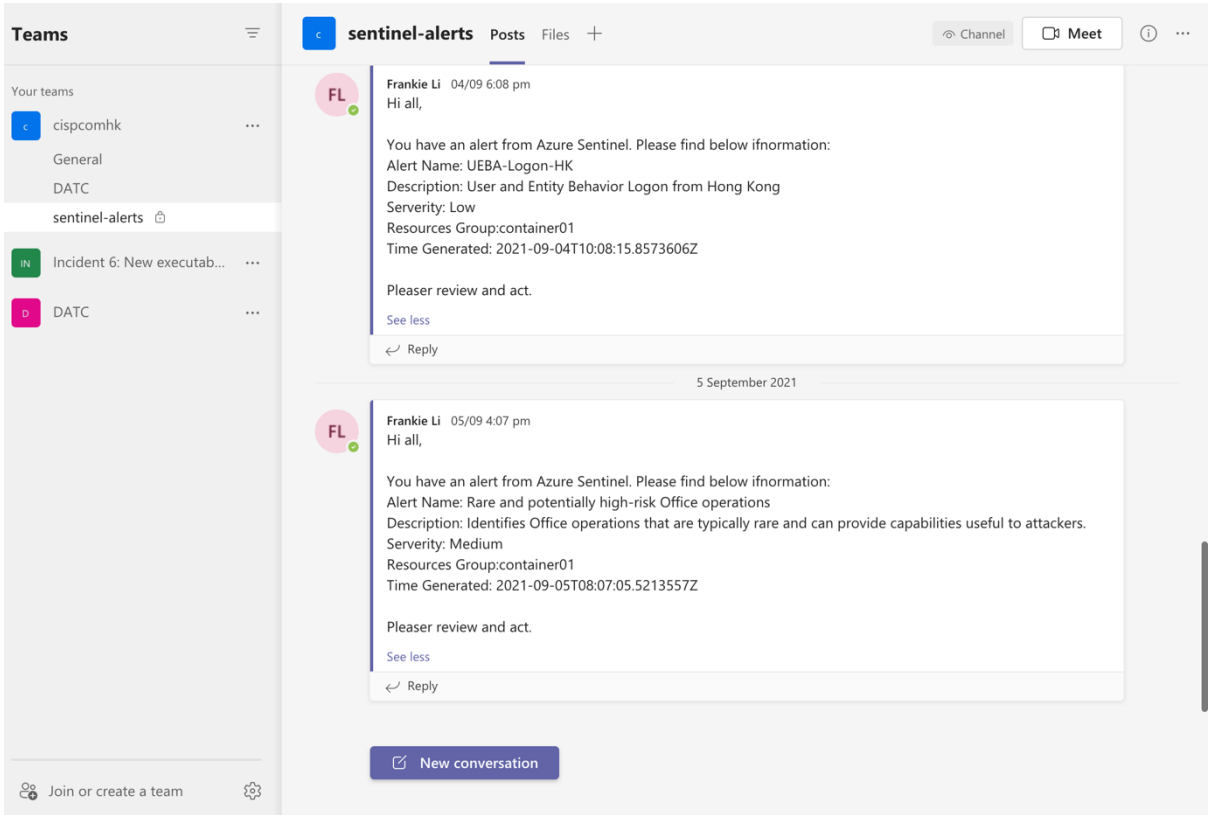


Microsoft©: Sentinel Playbook: Block-AADUser

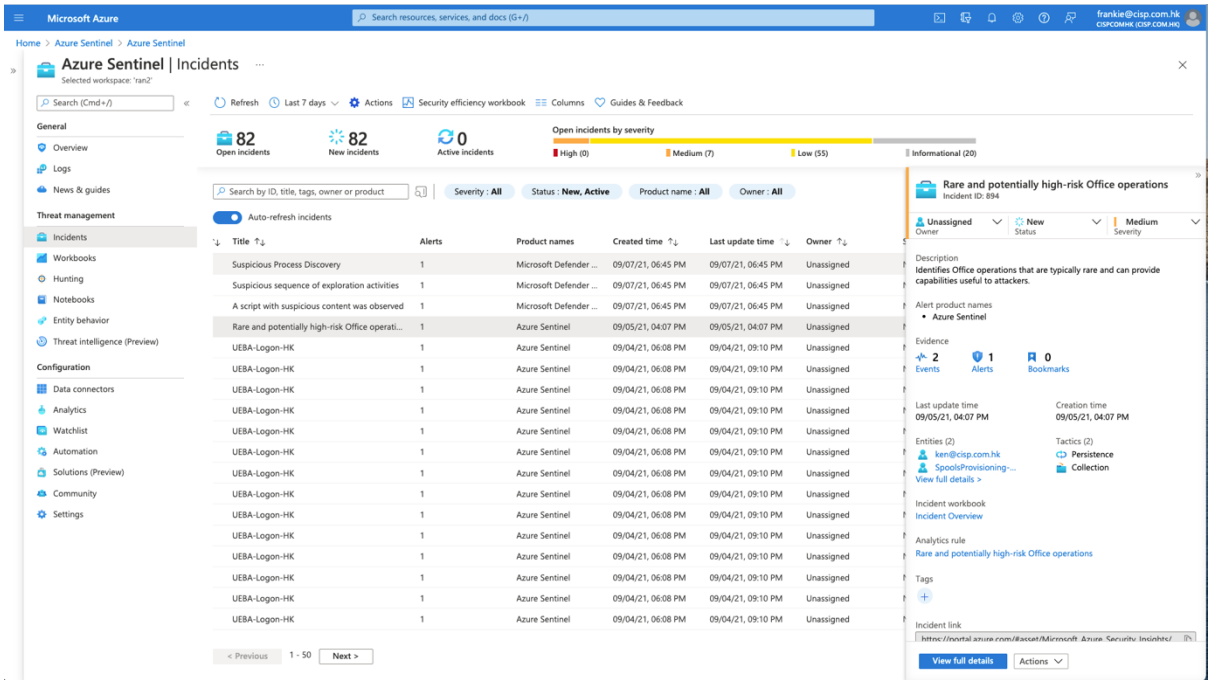
Or, we prefer *to send an alert message to Teams channel* to serve as an open ticket for the incident:



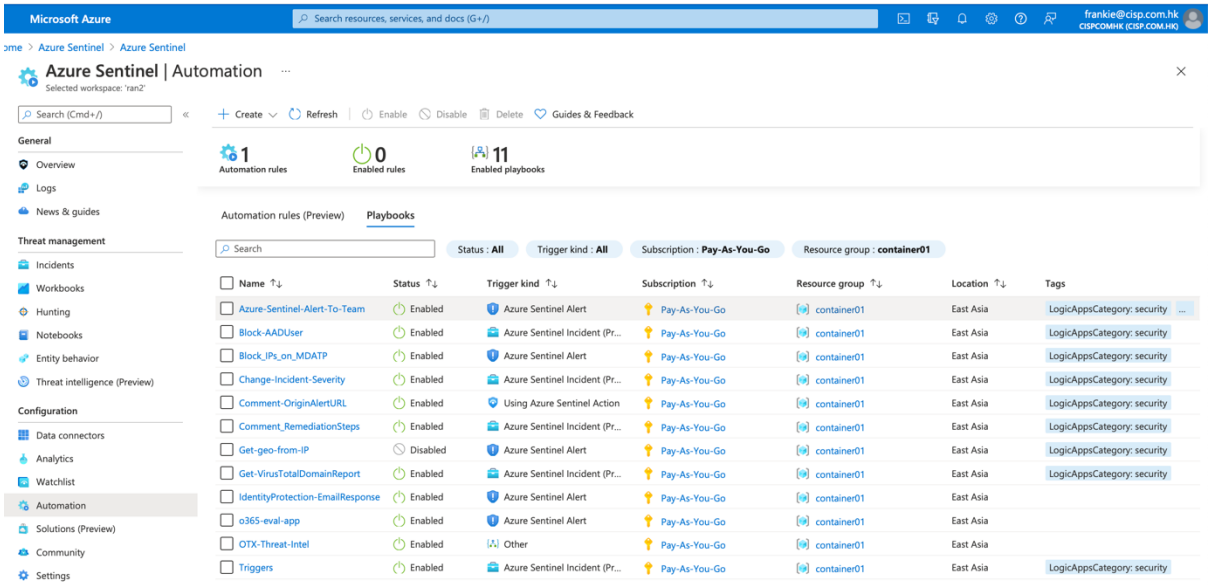
DATC Sentinel Playbook: Teams Channel



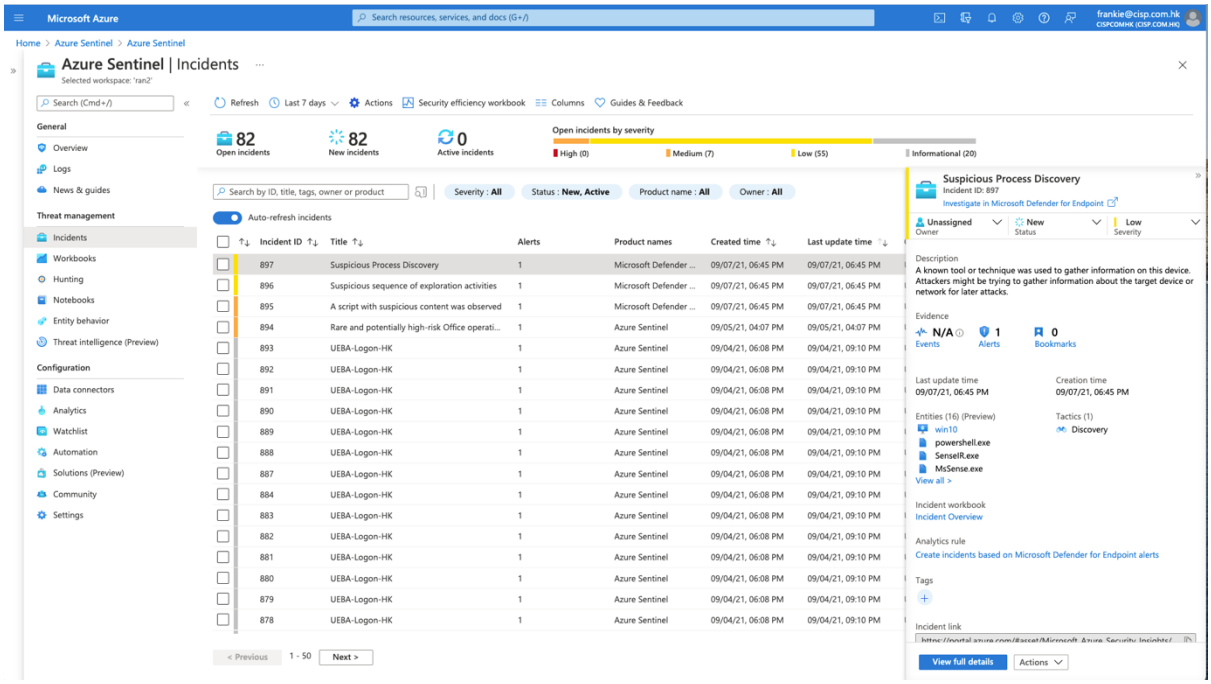
Example Sentinel Playbooks: Teams Alerts



Example Sentinel Playbooks: Teams Alerts



Example Sentinel Playbooks: Deployed in our Azure Sentinel



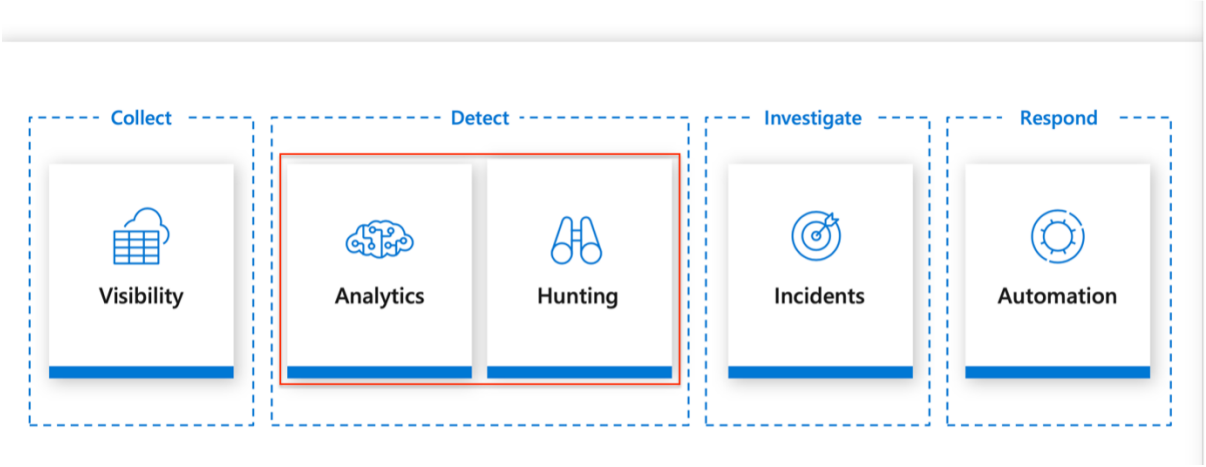
Sentinel Incidents: Alerts found in Azure Sentinel

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.



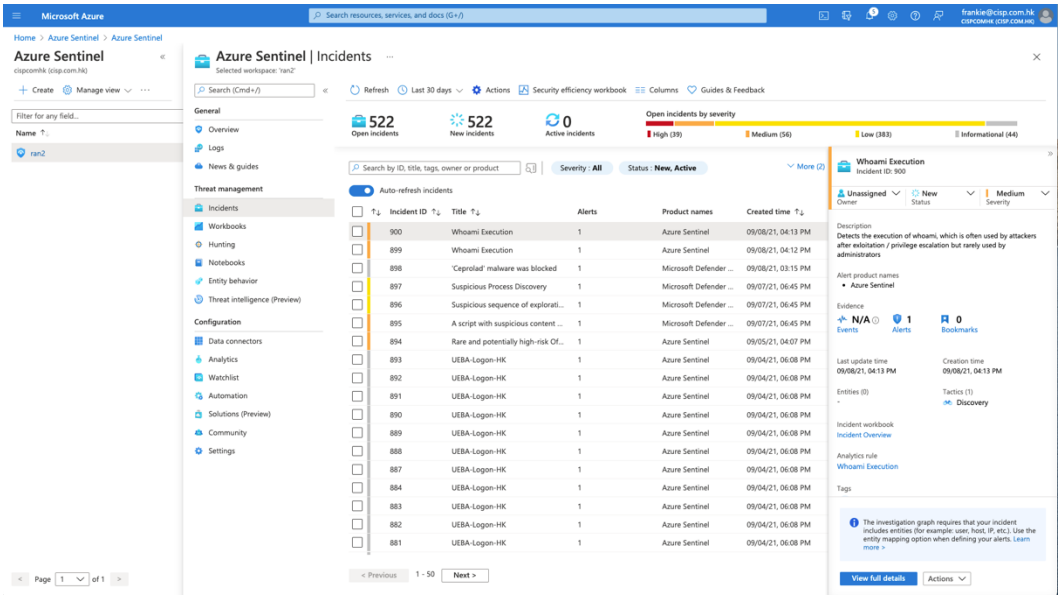
Microsoft©: Azure Sentinel: End-to-end solution for security operations

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.

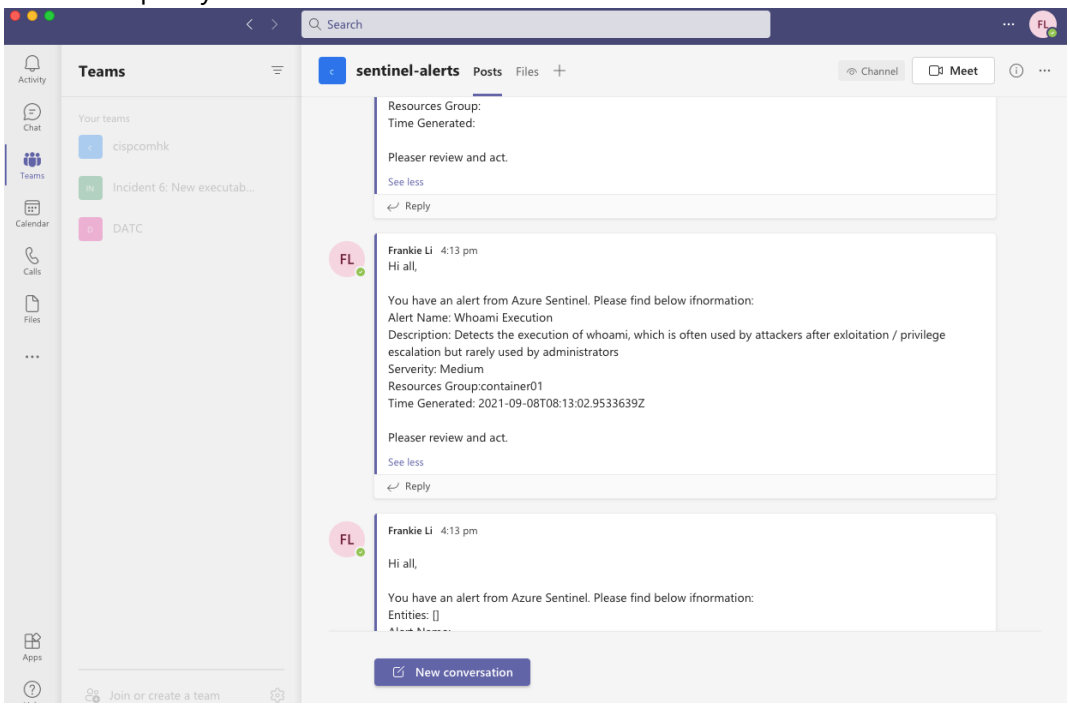
Sysmon "is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time".

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



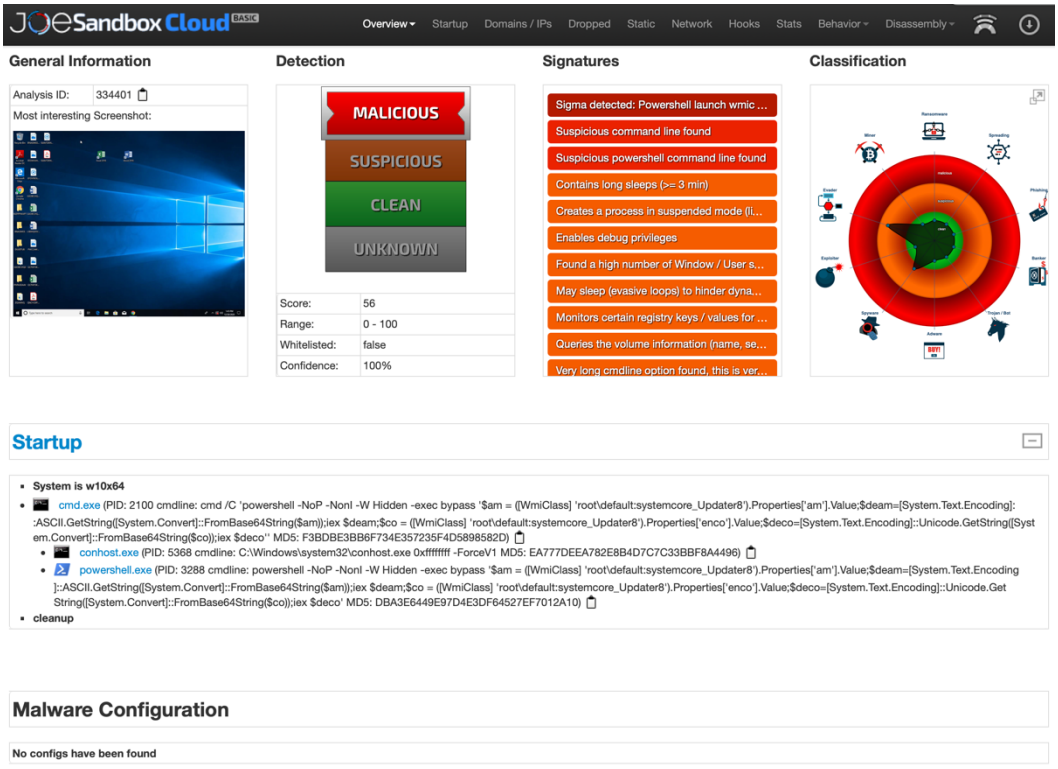
A simple Sysmon Sentinel detection rule: whoami started from PowerShell



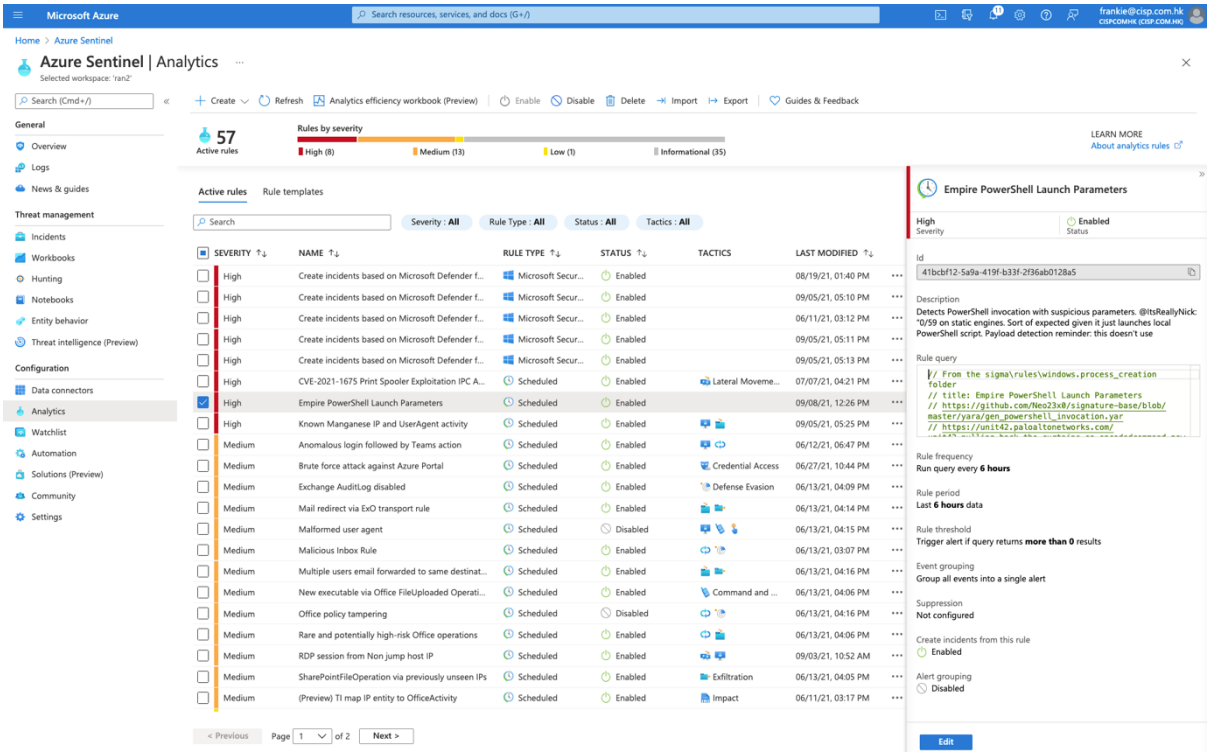
To simply our task in preparing the first set of detection rules for immediate use, we import [Sigma Rule to Azure Sentinel] for this demonstration. Using this approach, you can easily have more than 1,000 high quality MITRE ATT&CK ready detection rules, including PowerShell related rules, readily for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



DATC: A Windows PowerShell threat found on 3 September 2021



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.

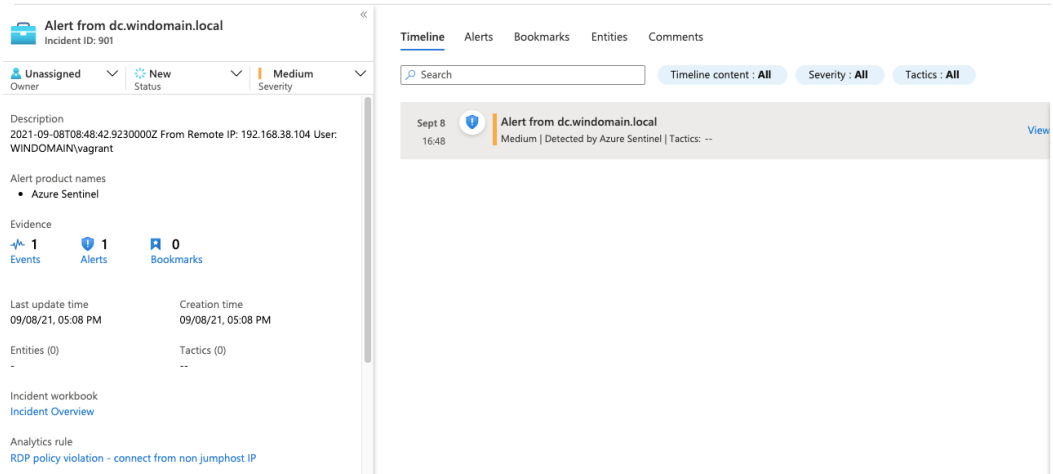
```
let jumphost = (_GetWatchlist('jumphost') | project IPAddress);
RDP
|where EventID == 21 or EventID == 22 or EventID == 25
|where RemoteHost !in~ (jumphost)
|where RemoteHost!="LOCAL"
|project TimeGenerated, Computer, RemoteHost, User, Session, RenderedDescription;
```

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

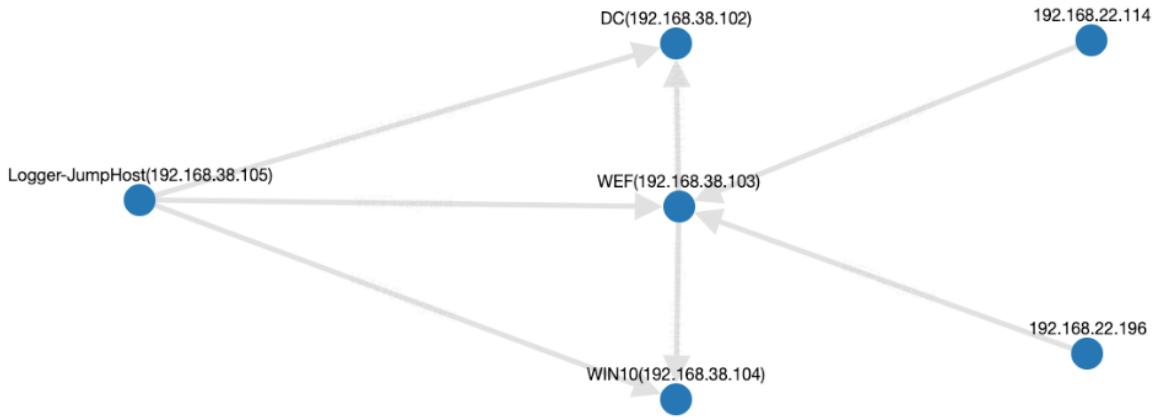
Generating alert and send notification to Teams



You have an alert from Azure Sentinel. Please find below ifnormation:
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
Serverity: Medium
Resources Group:container01
Time Generated: 2021-09-09T02:16:31.0241718Z

Pleaser 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
• 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	• Audit log search • Message Trace (part of the reporting features)	• 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
Technologies include everything in EOP plus: • 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	• SIEM integration API for detections • Real-time detections tool • URL trace (view Safe Links actions)	• 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
Technologies include everything in EOP, and Microsoft Defender for Office 365 P1 plus: • Safe Documents (not included in Office 365 E5)	• Threat Explorer • Threat Trackers • Campaign views	• Automated investigation and response (AIR) • AIR from Threat Explorer • AIR for compromised users • SIEM Integration API for Automated Investigations • Attack simulation training

Microsoft

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

	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																		
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]	•	•							•[4]				•[4]
Microsoft Editor premium features	•	•				•	•											
Multilingual user interface for Office applications	•	•				•	•											

[1]Includes Word, Excel, PowerPoint, OneNote, Outlook, Access (PC only), and Publisher (PC only)
[2]Includes Word, Excel, PowerPoint, Outlook, and OneNote mobile Apps
[3]Limited to devices with integrated screens smaller than 10.1"
[4]Mobile apps only

Email, calendar, and scheduling																		
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	•	•				•	•						•	•				•

[1]Microsoft 365 F1 includes the Exchange Kiosk service plan to enable Teams calendar only. It does not include mailbox rights.
[2]50 GB limit

Microsoft

	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																		
Microsoft Teams	•	•			•	•	•						•	•				•
Unlimited chat	•	•			•	•	•						•	•				•
Online meetings	•	•			•	•	•						•	•				•
Live Events	•	•			•	•	•											
Webinars	•	•			•	•	•											
Screen sharing and custom backgrounds	•	•			•	•	•						•	•				•
Record meetings	•	•			•	•	•						•	•				•
Priority notifications	•	•			•	•	•						•	•				•
Phone System		•					•											
Audio Conferencing		•					•											

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

Social, intranet, and storage																		
SharePoint	Plan 2	Plan 2			Plan 1	Plan 2	Plan 2						Kiosk[1]	Kiosk[1]				Kiosk[1]
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]

[1]Cannot be administrators. No site mailbox. No personal site.
[2]In addition to 1TB storage provided per organization.
[3]Microsoft 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																		
Microsoft Graph API	•	•			•	•	•						•	•				•
Microsoft Search	•	•			•	•	•						•	•				•
Microsoft Stream	•	•			•	•	•						•[1]	•[1]				•[1]
Microsoft Forms[2]	•	•			•	•	•							•				•
Microsoft Lists	•	•			•	•	•						•	•				•
Delve	•	•			•	•	•											

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

Analytics																		
Productivity Score	•	•			•	•	•						•	•				•
Secure Score	•	•			•	•	•				•	•	•	•				•
Compliance Management	•	•			•	•	•						•	•				•
MyAnalytics (full)		•					•											
Insights by MyAnalytics	•	•			•	•	•											
Power BI Pro		•					•											

Project and task management																		
Microsoft Planner	•	•			•	•	•						•	•				•
Microsoft To-Do	•	•			•	•	•							•				•
Briefing Email	•	•			•	•	•											

Microsoft

	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
Identity and access management																		
Azure Active Directory Premium	Plan 1	Plan 2	Plan 2					Plan 1	Plan 2				Plan 1	Plan 1	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 Discovery	•	•						•	•				•	•				
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		•		•			•									•	•	

Microsoft

	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
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]	•	•			•	•	•							•				•

[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		•	•												•		•	

Microsoft

	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
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		•		•			•									•	•	
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	•	•								•	•	•		•				

[1]30-day minimum retention period.

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 Priviledge Escalation Command and Control	APT5 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 occurances 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

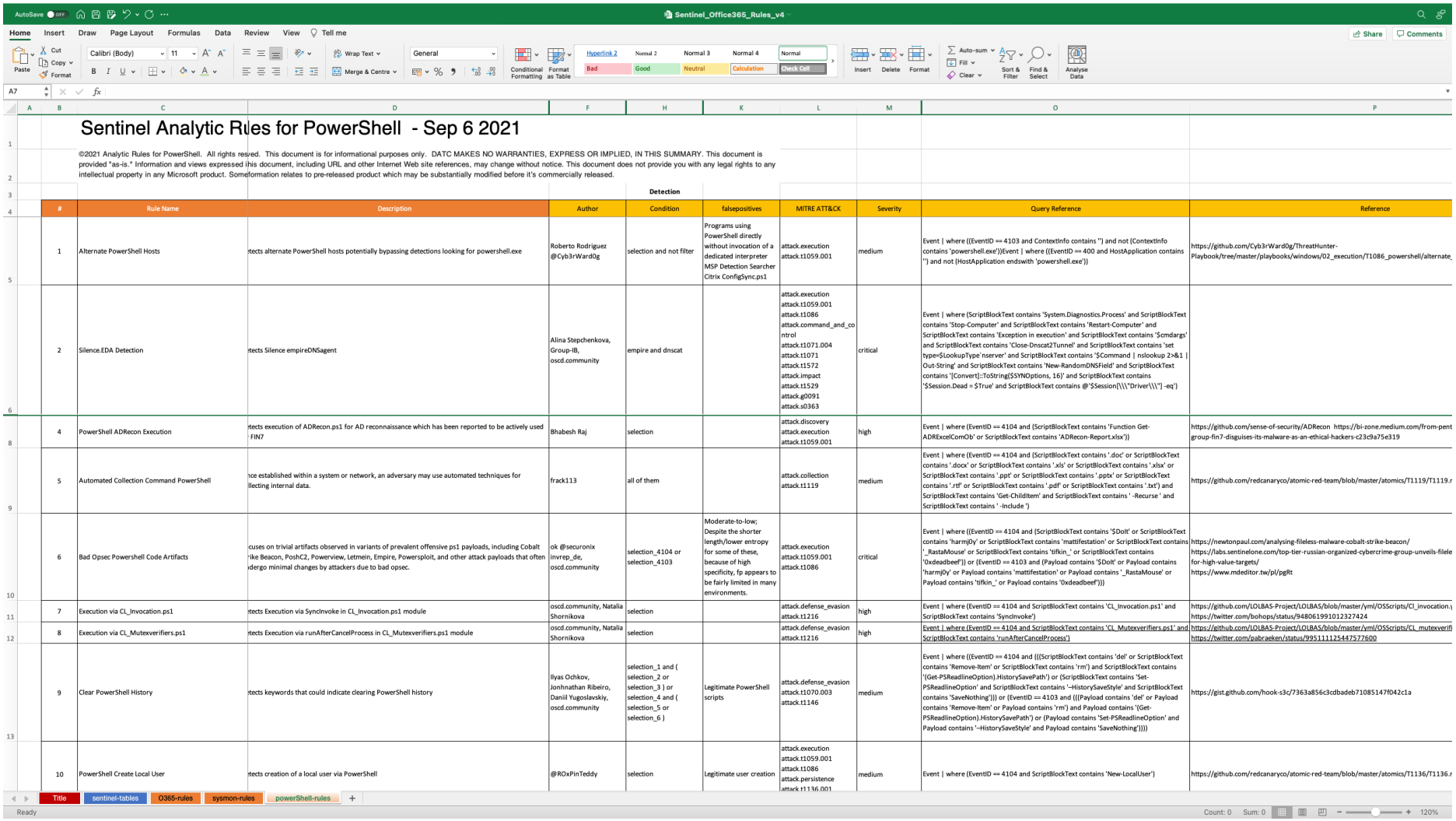
(Security Detection Rules for your Azure Sentinel environment.)

#	Rule Name	Description	Log Source	Severity	MITRE ATT&CK	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 Priviledge
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 Analytic Rules for PowerShell - Sep 6 2021

				Detection					
#	Rule Name	Description	Author	Condition	falsepositives	MITRE ATT&CK	Severity	Query Reference	Reference
1	Alternate PowerShell Hosts	tects 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 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/Cyb3rWard0g/ThreatHunter-Playbook/tree/master/playbooks/windows/02_execution/T1086_powershell/alternate_
2	Silence.EDA Detection	tects Silence empireDNSagent	Alina Stepchenkova, 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.t1529 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 '$cmdargs' and ScriptBlockText contains 'Close-Dnscat2Tunnel' and ScriptBlockText contains 'set type=$LookupTypeˋnserver' 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	tects execution of ADRecon.ps1 for AD reconnaissance which has been reported to be actively used FIN7	Bhabesh Raj	selection		attack.discovery attack.execution attack.t1059.001	high	Event | where (EventID == 4104 and (ScriptBlockText contains 'Function Get-ADRExcelComOb' or ScriptBlockText contains 'ADRecon-Report.xlsx'))	https://github.com/sense-of-security/ADRecon https://bi-zone.medium.com/from-pentest-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319
5	Automated Collection Command PowerShell	nce established within a system or network, an adversary may use automated techniques for llecting 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-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	cuses on trivial artifacts observed in variants of prevalent offensive ps1 payloads, including Cobalt rike Beacon, PoshC2, Powerview, Letmein, Empire, Powersploit, and other attack payloads that often dergo 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 '$Doit' or ScriptBlockText contains 'harmj0y' or ScriptBlockText contains 'mattifestation' or ScriptBlockText contains '_RastaMouse' or ScriptBlockText contains 'tifkin_' or ScriptBlockText contains '0xdeadbeef')) or (EventID == 4103 and (Payload contains '$Doit' or Payload contains 'harmj0y' or Payload contains 'mattifestation' or Payload contains '_RastaMouse' or Payload contains 'tifkin_' or Payload contains '0xdeadbeef')))	https://newtonpaul.com/analysing-fileless-malware-cobalt-strike-beacon/ https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-filele for-high-value-targets/ https://www.mdeditor.tw/pl/pgRt
7	Execution via CL_Invocation.ps1	tects 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/Cl_invocation.y https://twitter.com/bohops/status/948061991012327424
8	Execution via CL_Mutexverifiers.ps1	tects 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 https://twitter.com/pabraeken/status/995111125447577600
9	Clear PowerShell History	tects keywords that could indicate clearing PowerShell history	Ilyas Ochkov, 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/7363a856c3cdbadeb71085147f042c1a
10	PowerShell Create Local User	tects 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/T1136/T1136.r