

Configuration Manual

MSc Research Project
MSc Cybersecurity

Amruta Pandhare
Student ID: x23269227

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name: Amruta Anant Pandhare
Student ID: x23269227
Programme: MSc Cybersecurity **Year:** 2024-2025
Module: MSc Research Project
Lecturer: Kamil Mahajan
Submission Due Date: 01/09/2025
Project Title: THRIVE: A Structured, CTI-Prioritised Threat Hunting Methodology for Security Operations Centres (SOCs)
Word Count: 2052 **Page Count:** 39

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Amruta Anant Pandhare

Date: 01/09/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Amruta Pandhare
Student ID: x23269227

This configuration manual provides a step-by-step guide for implementing the THRIVE threat hunting methodology in a Security Operations Centre (SOC) or lab environment. Due to confidentiality restrictions, specific organisational data cannot be disclosed. To ensure reproducibility, a functionally equivalent environment was replicated using an Azure student subscription. This configuration manual includes setup instructions, tool configurations, and workflow steps with screenshots so that the process can be replicated for training, evaluation, or operational deployment.

Section 1: Environment Setup

1.1. Azure Environment

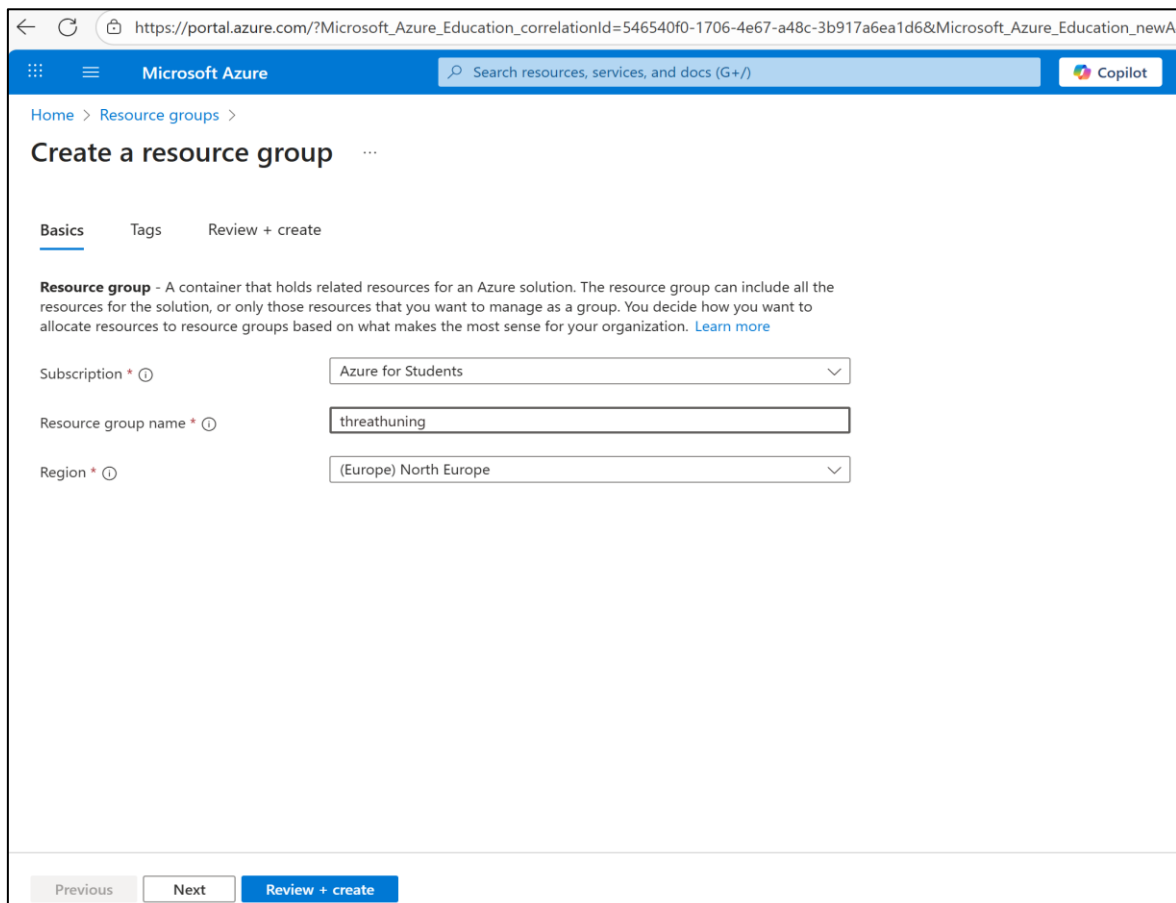


Figure 1. Create Azure resource group in an appropriate region.

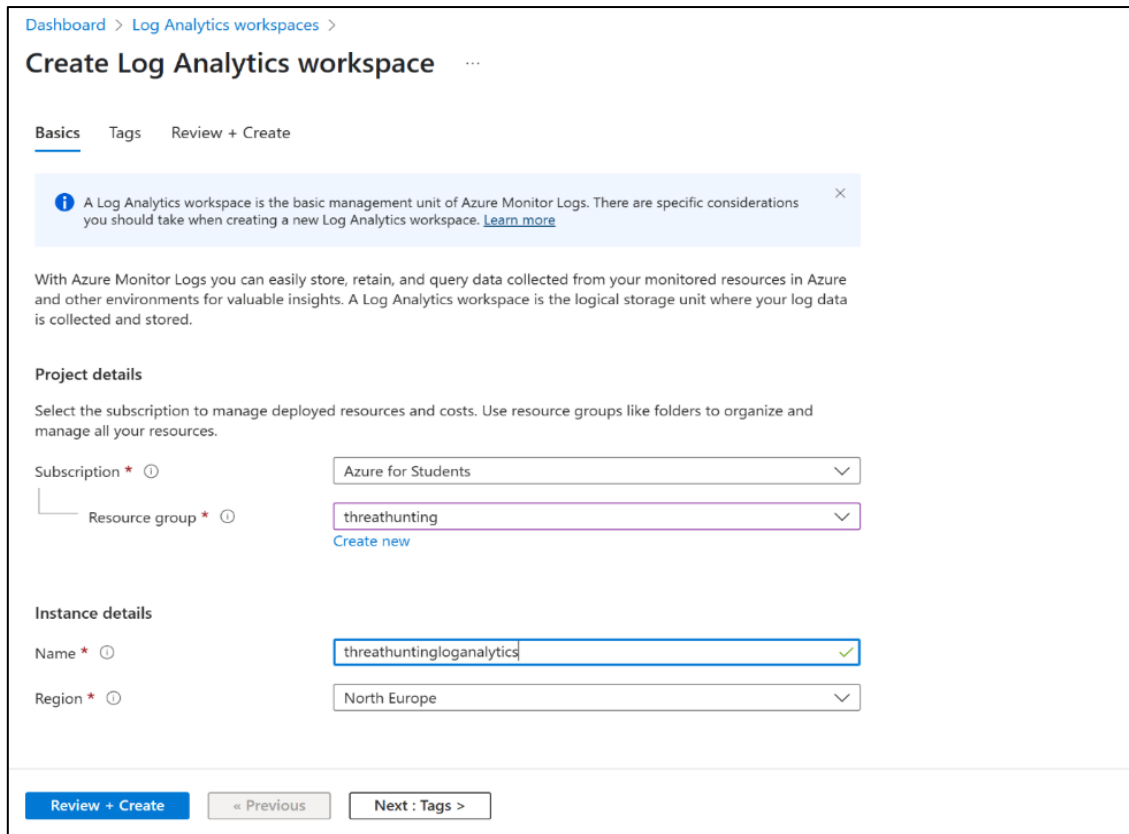


Figure 2: Create log analytics workspace in the resource group and region.

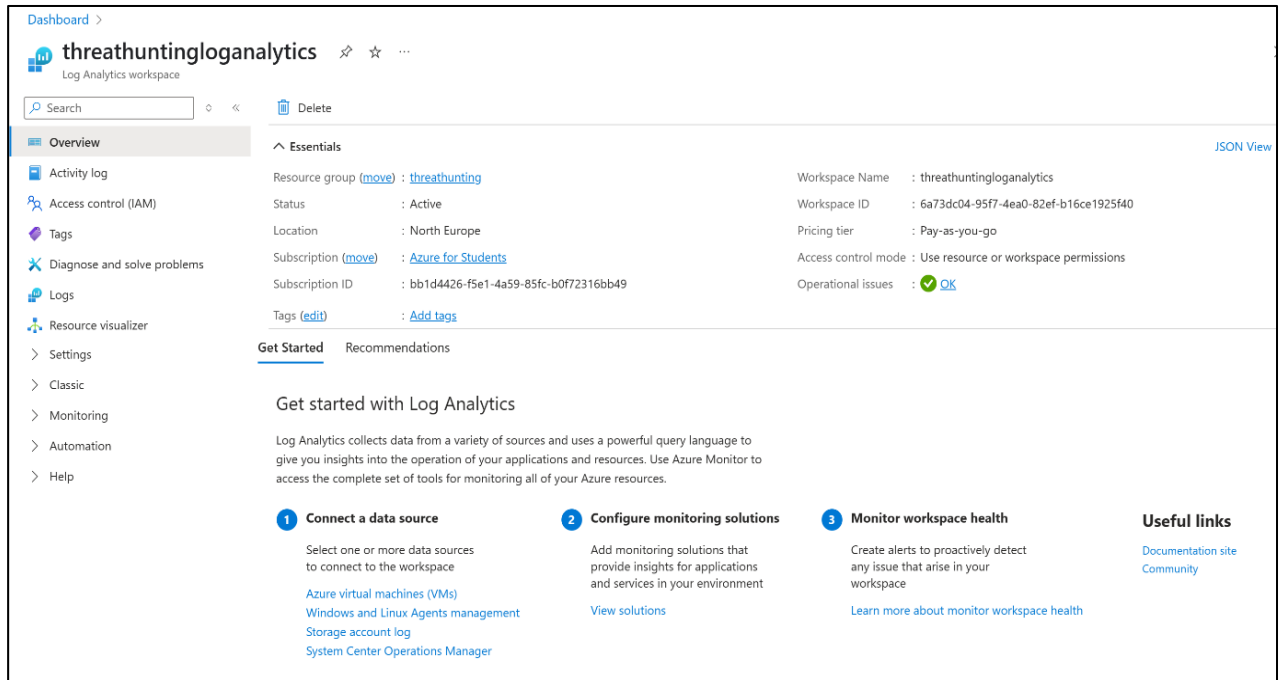


Figure 3. Workspace overview showing workspace name and ID.

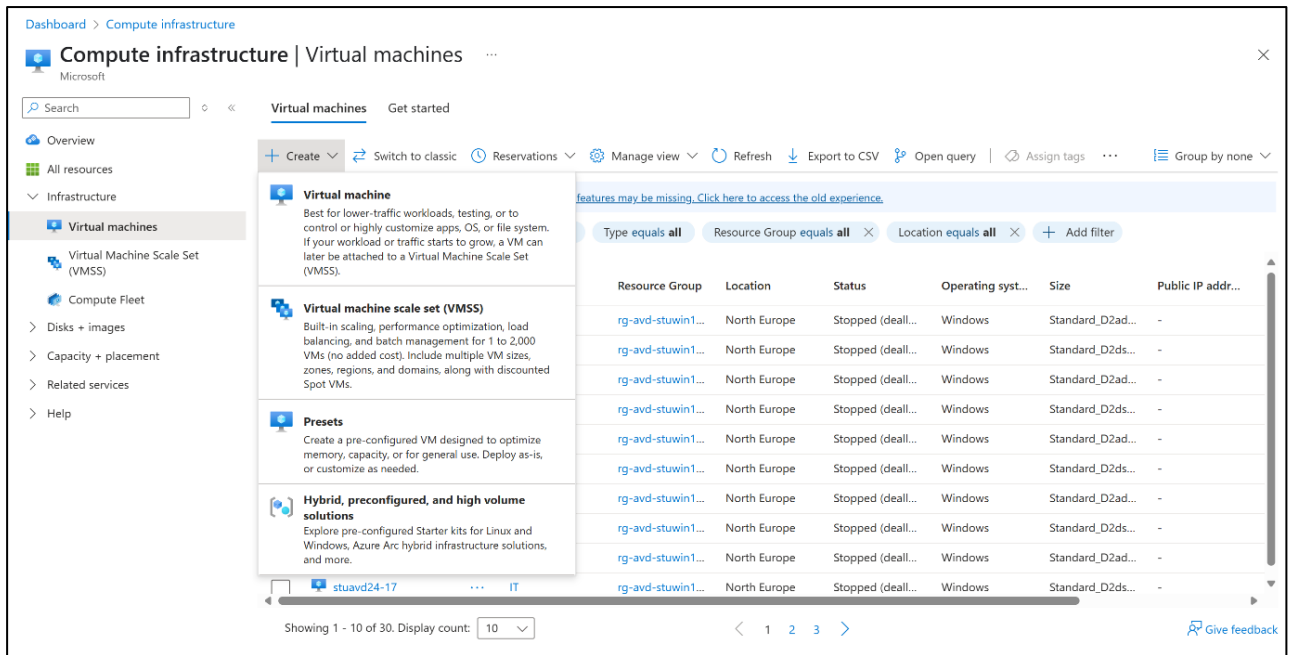


Figure 4. Create virtual machine for log ingestion.

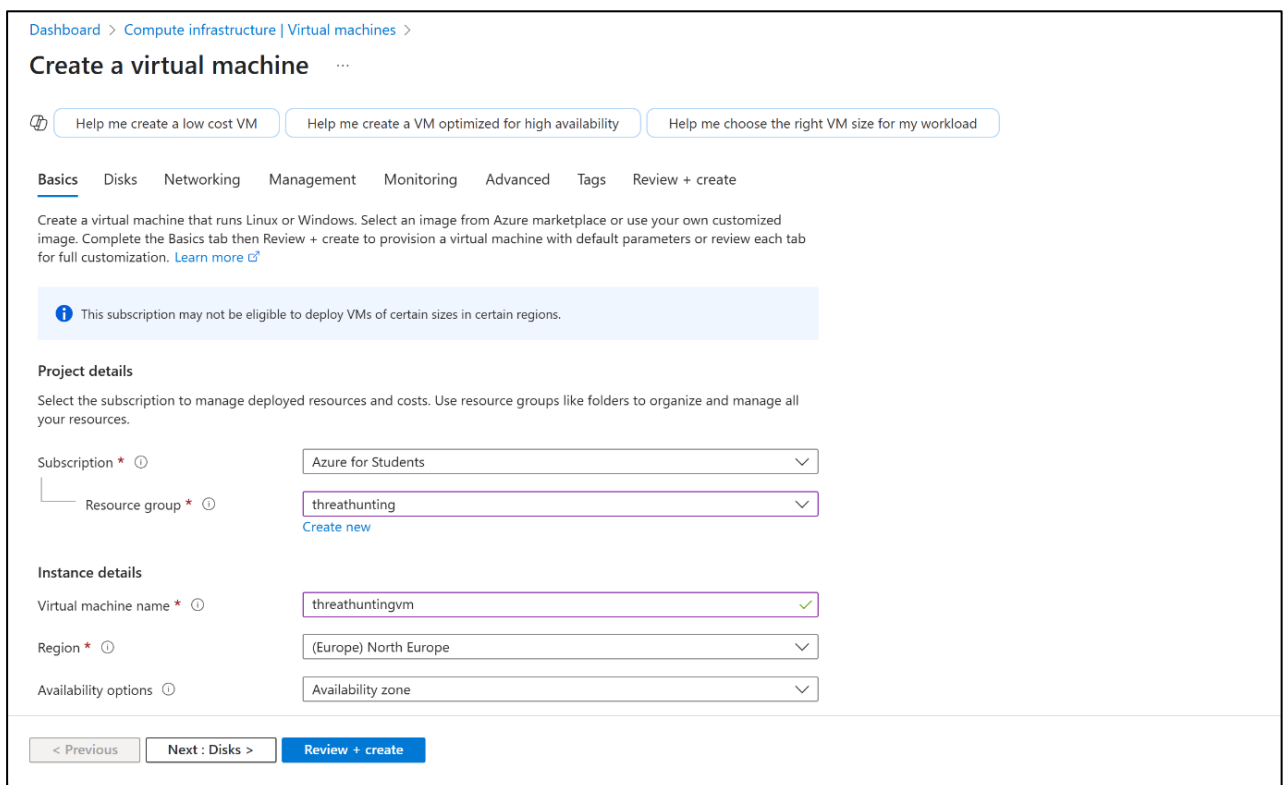


Figure 5. Create Windows 10 virtual machine in the same region and virtual network.

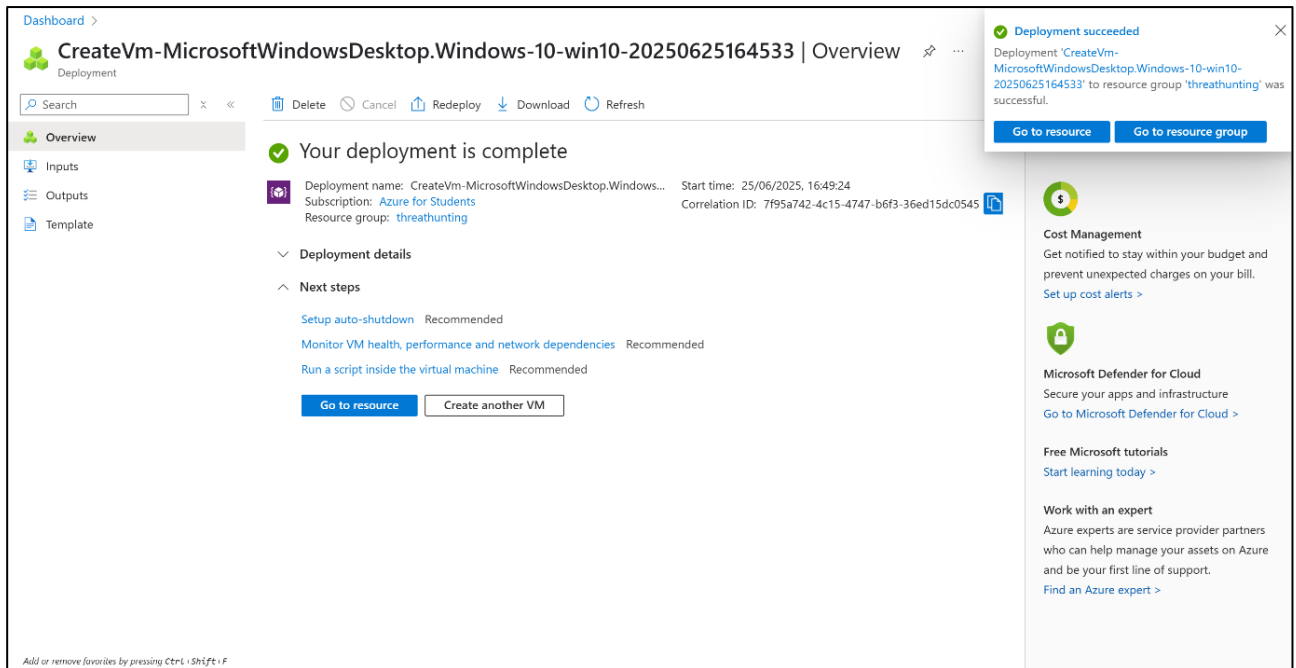


Figure 6. Successfully deploy virtual machine

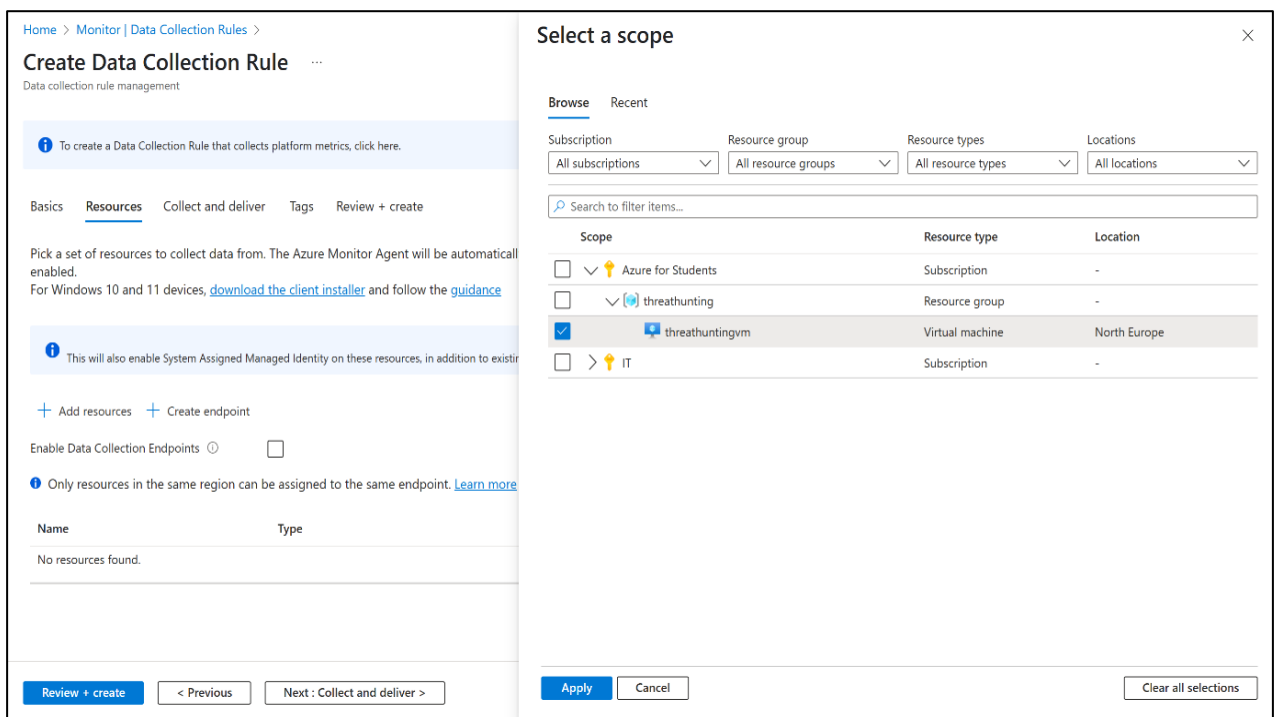


Figure 7. Create data collection rule for log onboarding.

Add data source ✕

*** Data source** Destination

Select which data source type and the data to collect for your resource(s).

Data source type *

Windows Event Logs ▼

i If using Sentinel, use [the connector configuration](#) for collecting Windows Security events to **avoid unexpected increase in storage cost.** [Learn More](#)

Choose Basic to enable collection of event logs. Choose Custom if you want more control over which event logs are collected.

None Basic **Custom**

Use XPath queries to filter event logs and limit data collection. [Learn more about event logs and XPath syntax](#)

Add

Event logs

Application!*[System[(Level=1 or Level=2)]]	✕
Security!*[System[(band(Keywords,13510798882111488)]]]	✕
System!*[System[(Level=1 or Level=2)]]	✕

Add data source
Next : Destination >
Cancel

Figure 8. Add data sources (Windows Events Logs).

Add data source ✕

*** Data source** Destination

Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. [Learn more about pricing.](#)

+ Add destination

* Destination type	Subscription	Destination Details
Azure Monitor Logs ▼	Azure for Students ▼	threathuntingloganalytics (threat... ▼ ✕

Figure 9. Add log analytics workspace as destination.

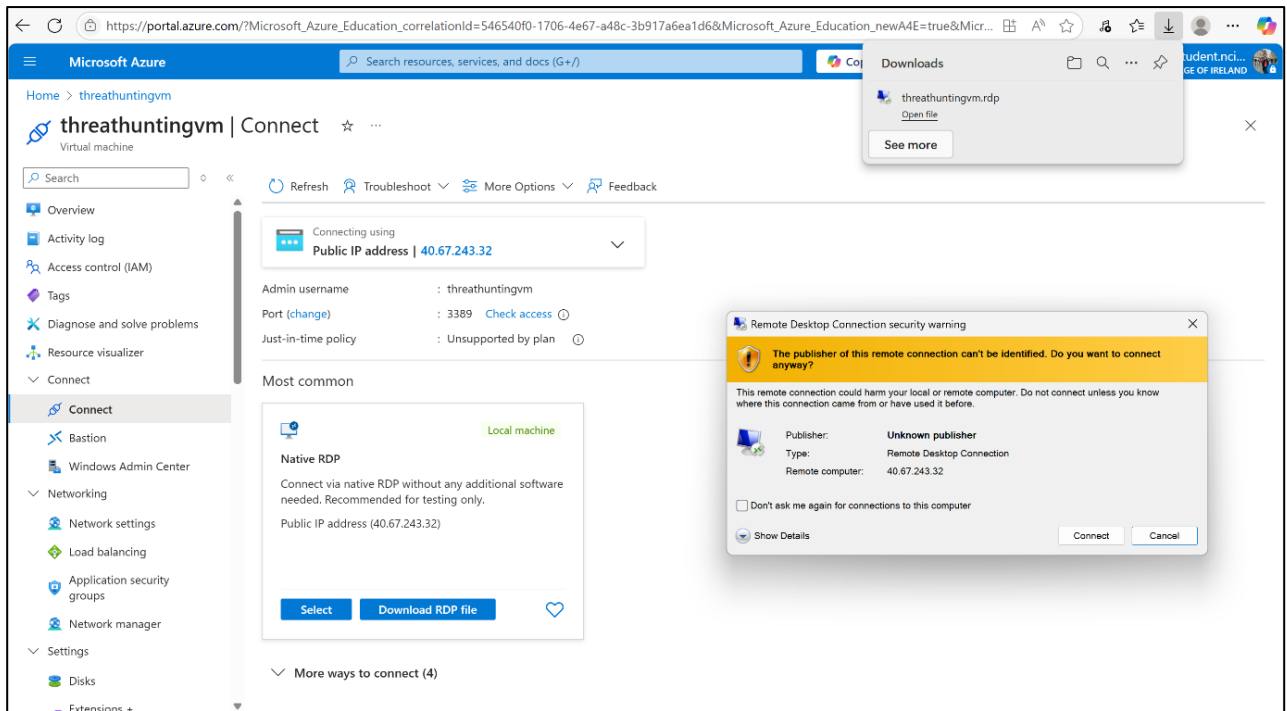


Figure 10. Download RDP file to connect to the virtual machine.

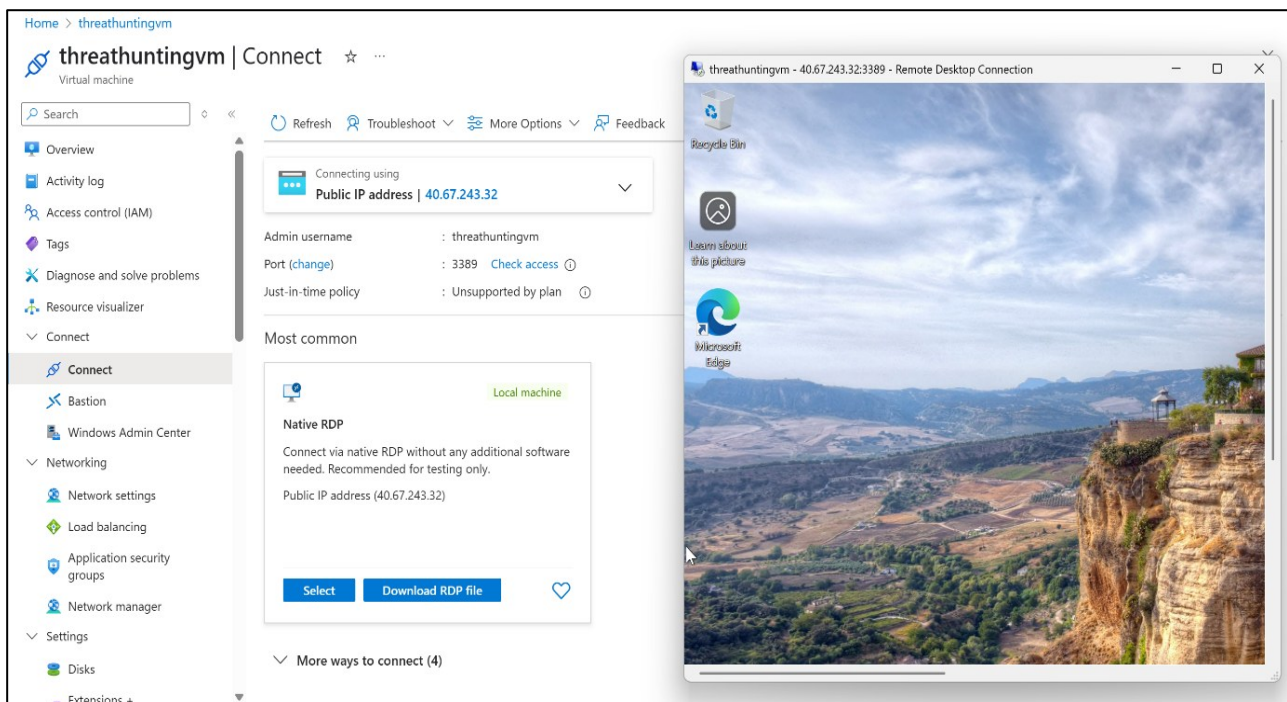


Figure 11. Connect to the virtual machine & perform some activities to generate logs.

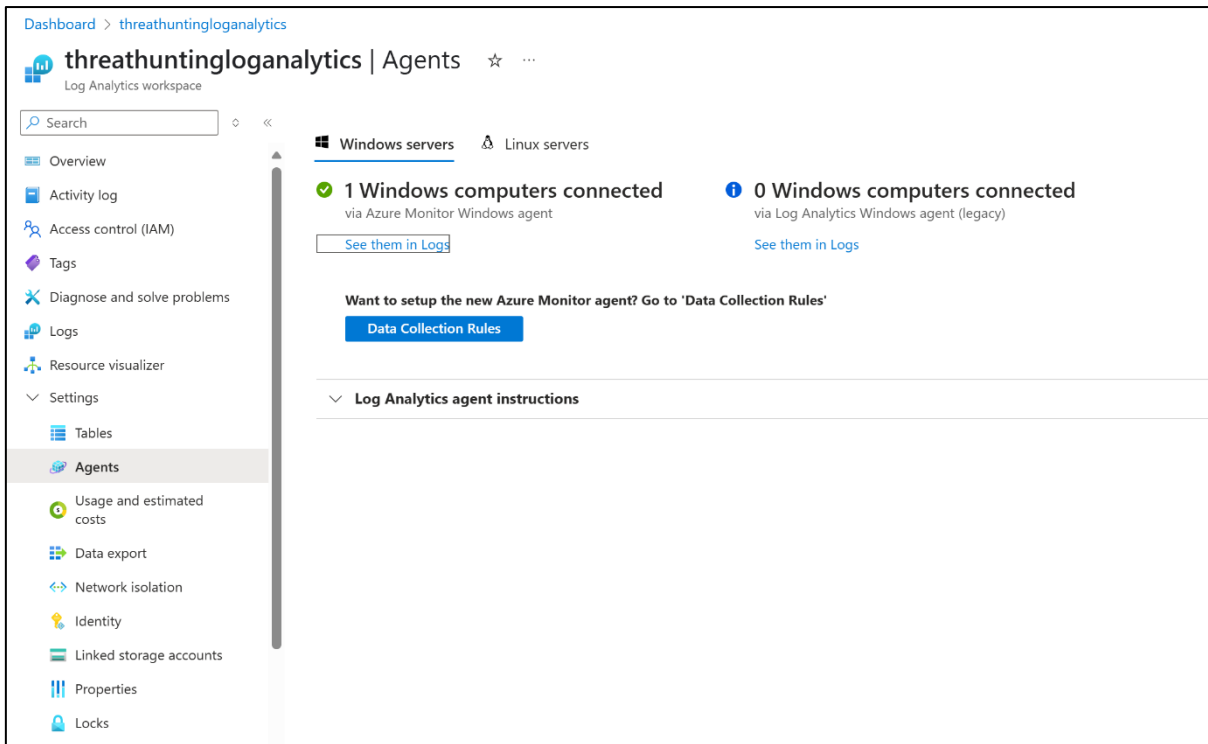


Figure 12. Workspace Agents view confirming the VM is connected.

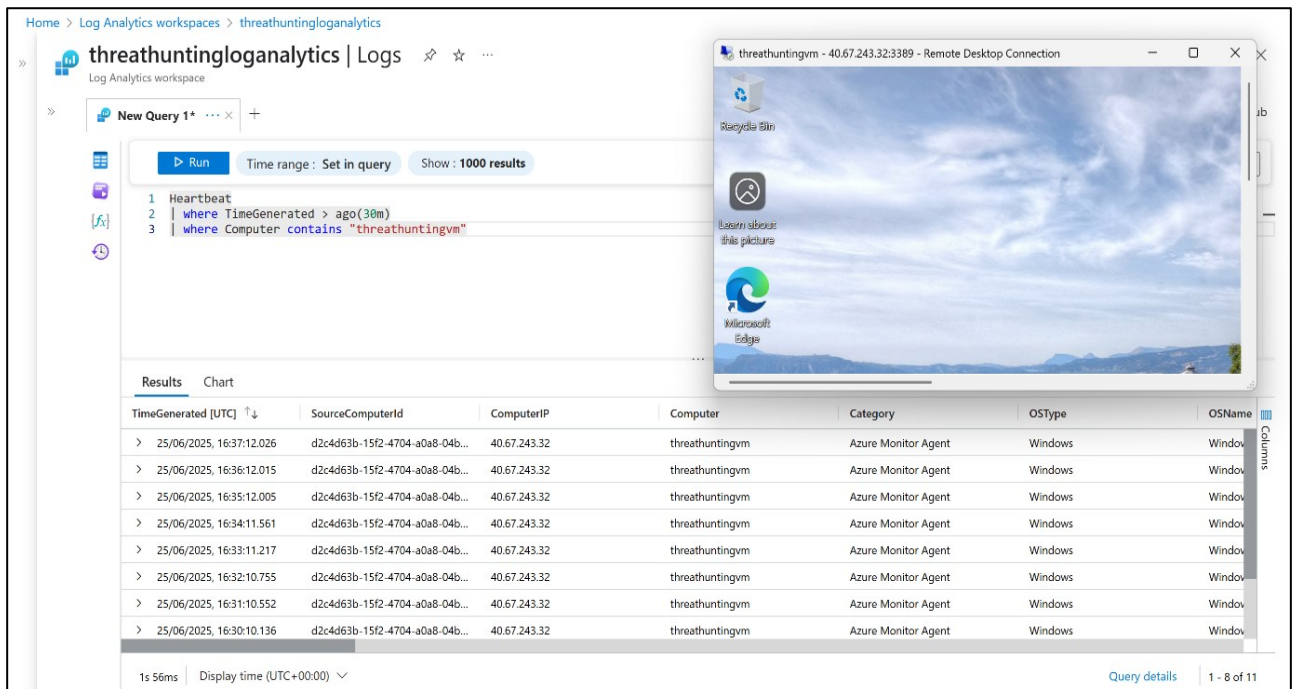


Figure 13. Workspace logs query confirming heartbeat from the VM.

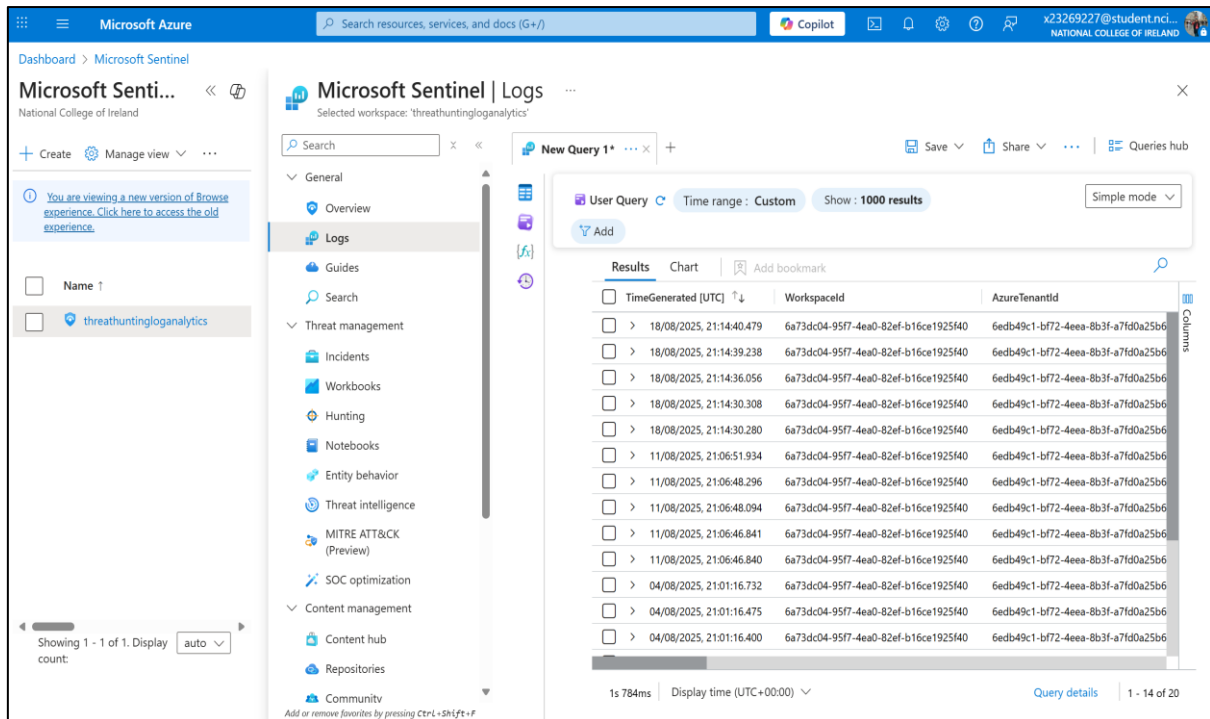


Figure 14. Enable Microsoft Sentinel on the Log Analytics workspace.

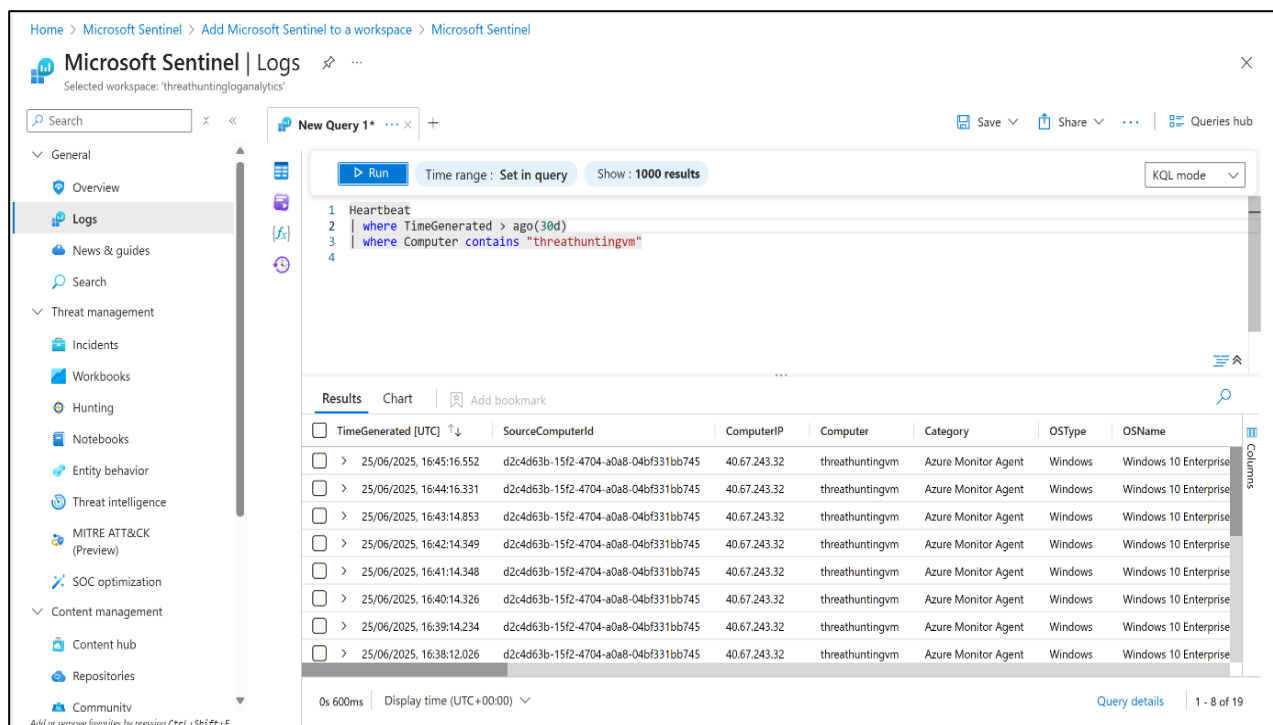


Figure 15. Sentinel logs query confirming logs from the VM.

1.2. AWS WorkSpaces Setup (for Red/Blue team testing)

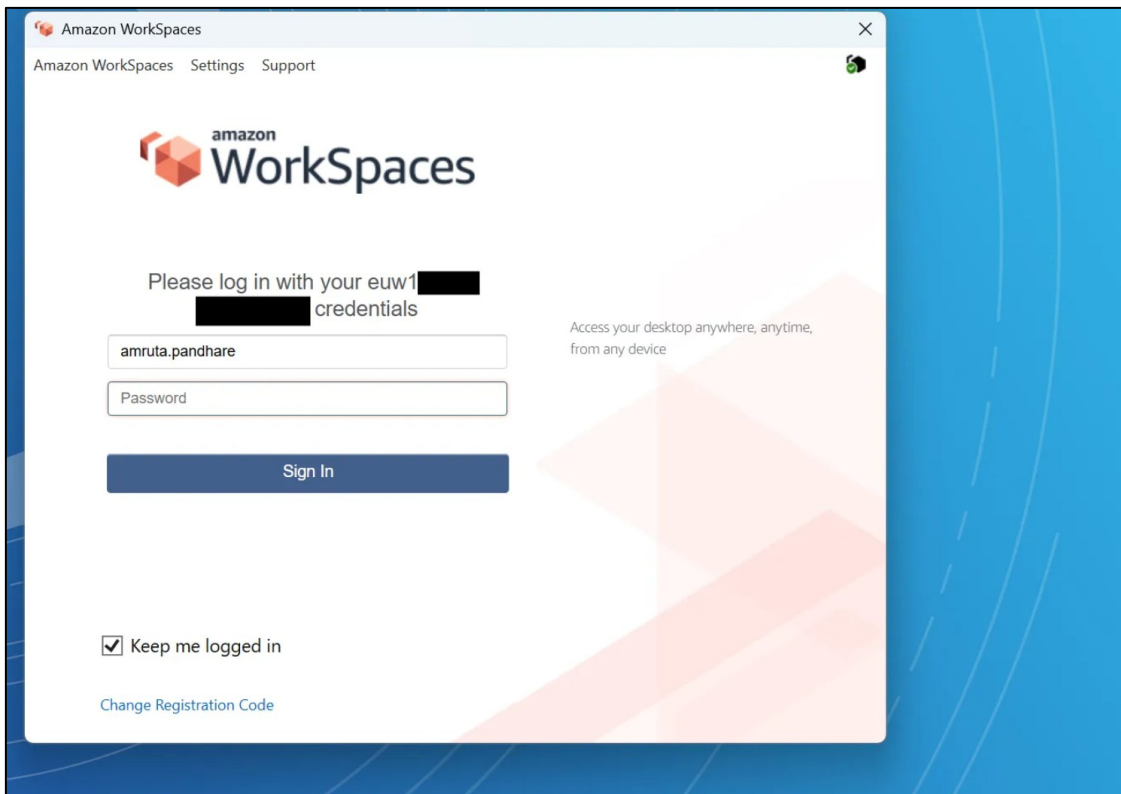


Figure 16. Amazon workspaces test machine for red/blue team testing.

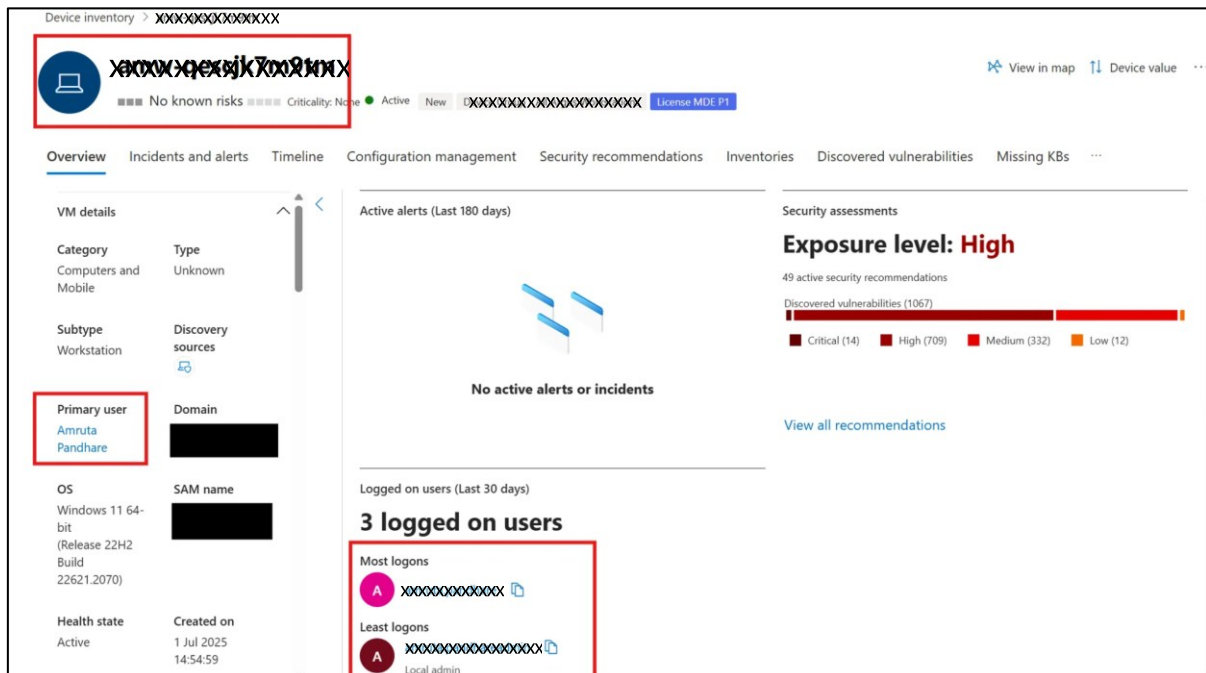


Figure 17. Defender device inventory showing the AWS WorkSpace onboarded.

Section 2: Hunting Maturity Model (HMM) self-assessment

Maturity Level Assessment (Sqrrl Hunting Maturity Model)			
HMM Level	Characteristics	Indicators	Questions to Ask
HM0 - Initial	No formal threat hunting. Security is reactive, based only on alerts and incidents. No dedicated threat hunters.	No hunting logs, no hypotheses, no tools beyond basic SIEM alerts	Do we ever perform hunts proactively, or only after alerts/incidents?
HM1 - Minimal	Threat hunting happens occasionally by skilled analysts using intuition. No consistent process, documentation, or tool use.	Isolated hunting examples, no playbooks, no team collaboration	Do analysts ever explore threats manually, even if unstructured?
HM2 - Procedural	Hunting occurs more regularly. Basic procedures exist. CTI may be used, but hypothesis creation is limited or informal.	Uses Sentinel or EDRs to query logs, creates basic hypotheses, semi-regular hunts	Do we document our hunts and use CTI or TTPs to guide them?
HM3 - Innovative	Well-defined hunting program. CTI informs structured hypotheses. Regular documentation, tracking, and some automation.	Tracks hunts, review queries, documents outcomes, builds detection rules	Do we have a repeatable process to move from CTI to detection rules?
HM4 - Leading	Threat hunting is fully integrated with detection engineering. Hypotheses are hypothesis- and TTP-driven, backed by strong metrics, automation, and red teaming.	Uses dashboards, MITRE ATT&CK mapping, red/blue validation, contributes to CTI sharing	Do we measure hunt effectiveness and improve based on lessons learned?

Figure 18. Hunting Maturity Model self-assessment.

Section 3: Threat Intelligence Ingestion & Prioritisation

3.1. Automating IOC Ingestion with Logic Apps

Authenticate for API access | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated. [Read here for more info](#)

THREAT fox from ABUSE.ch | SPANNAUS
[Browse IOCs](#) [Share IOCs](#) [IOC Requests](#) [Access Data](#) [FAQ](#) [About](#) [Login](#)

🕒 Expiration of IOCs

Since 2025-05-01, we are expiring IOCs that are older than 6 months. We are doing so to avoid false positives, mostly happening on cloud based infrastructure where assets (e.g. IP addresses) are changing customers quickly. Expired IOCs are not exposed on the ThreatFox API and data Export. However, they are still visible and searchable through the ThreatFox UI, but flagged to be expired.

Obtain an Auth-Key (Required)

In order to interact with the ThreatFox API, you need to obtain an **Auth-Key** first. If you don't have one you can get one for free here:

- [abuse.ch Authentication Portal](#)

Whenever you interact with the ThreatFox API, you must include the HTTP header **Auth-Key** with your Auth-Key. Example `curl` command:

```
curl -H "Auth-Key: YOUR-AUTH-KEY" -X POST https://threatfox-api.abuse.ch/api/v1/ -d '{"query": "get_iocs", "days": 1}'
```

Query recent IOCs

You can obtain a copy of the current IOC dataset from ThreatFox by sending an HTTP POST request to the Threatfox API as documented below:

Figure 19. ThreatFox platform - IOC source.

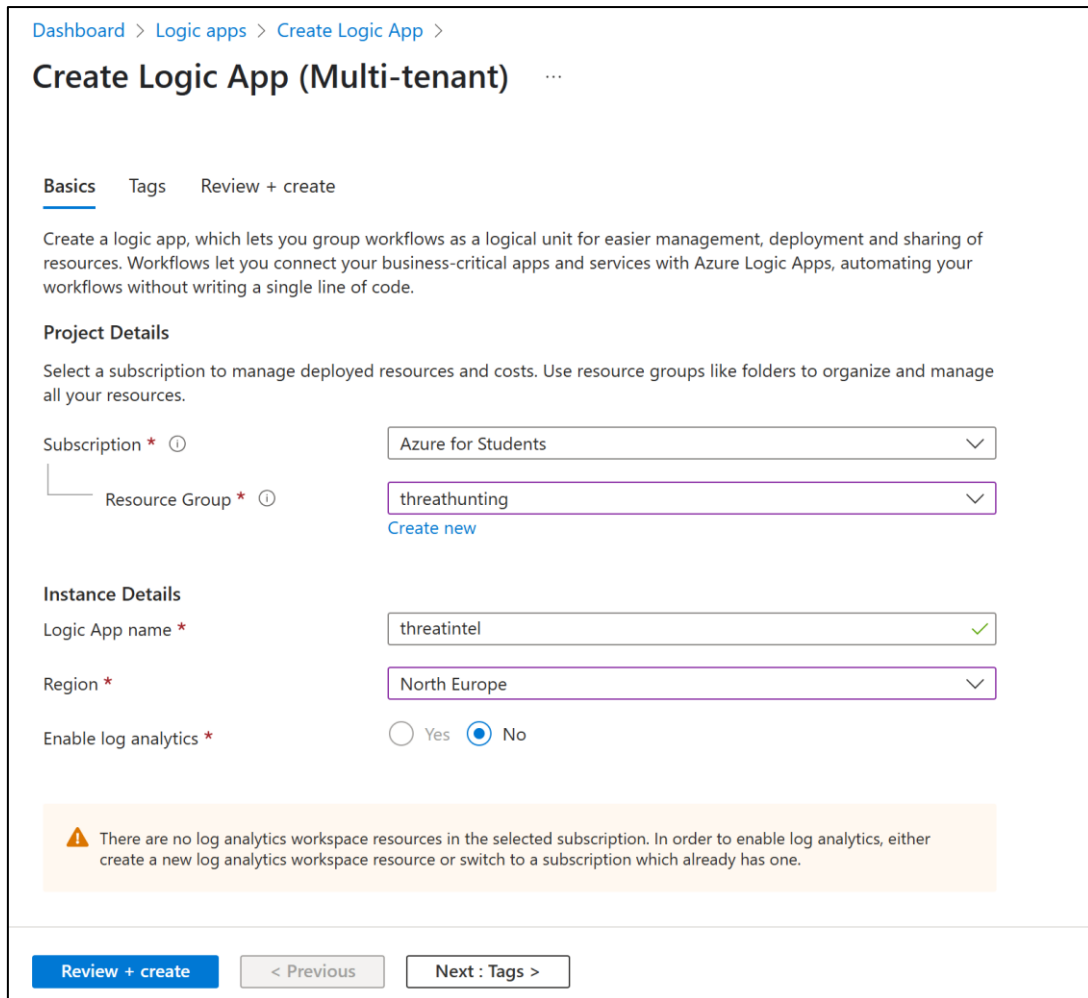


Figure 20. Create logic app for IOC ingestion in the same resource group.

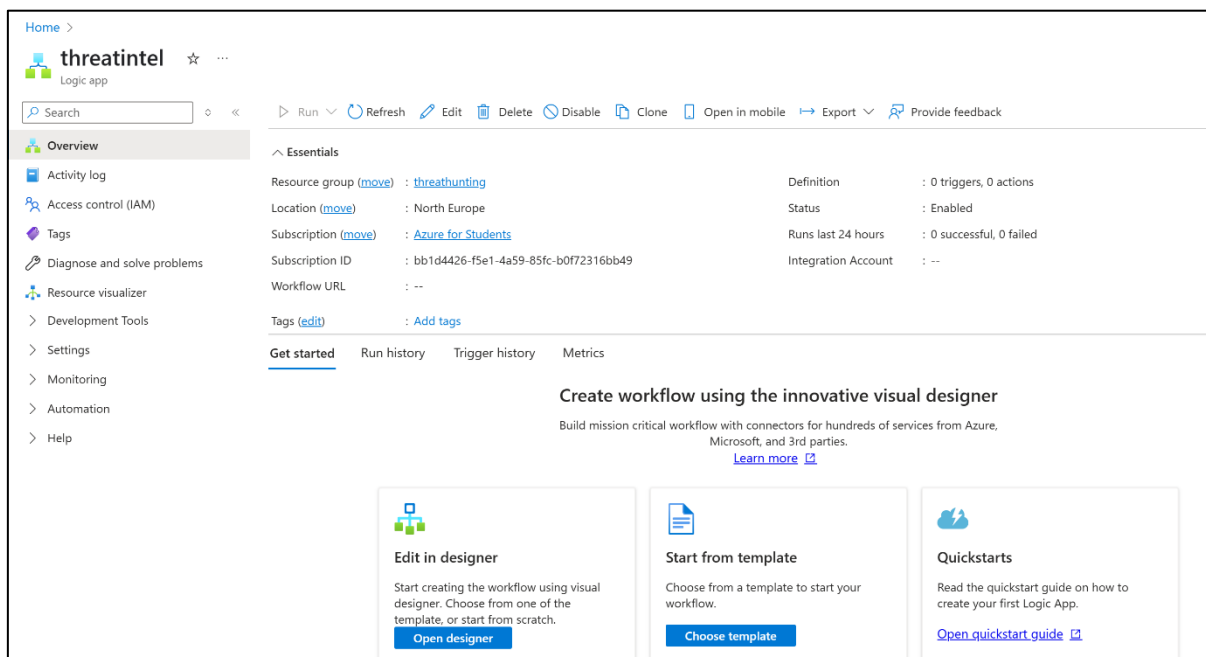


Figure 21. Create workflow using visual designer.

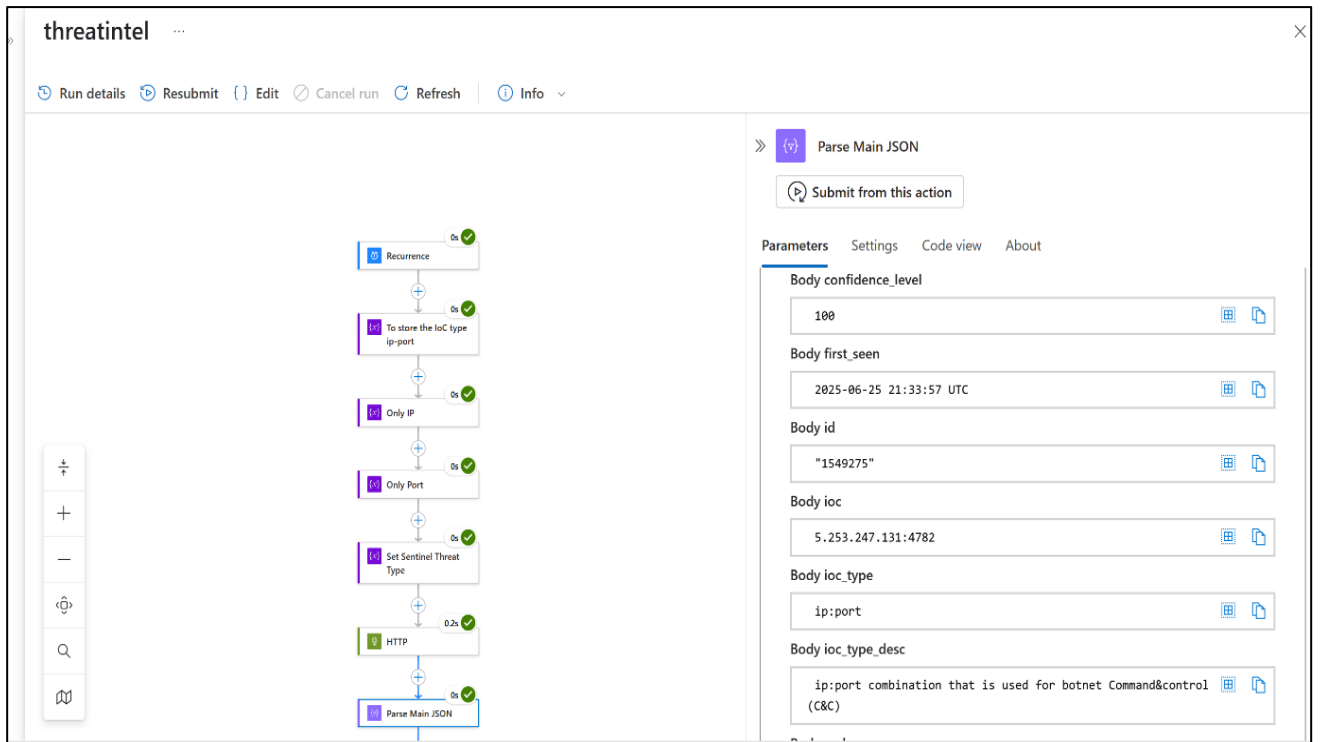


Figure 22. Parse IOC's before pushing it to Sentinel.

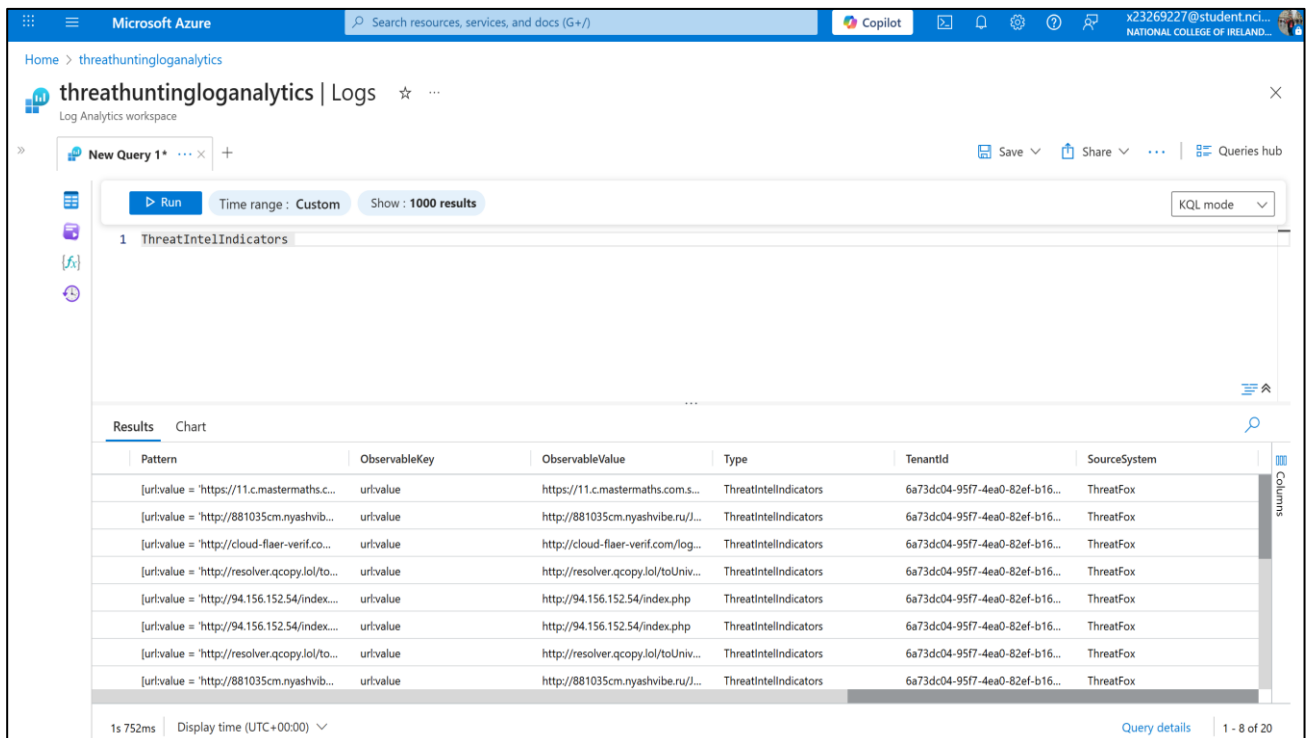


Figure 23. ThreatIntelligenceIndicator table showing ingested IOCs.

3.2. RSS Feeds Integration

Connectors for "Threat Intel Alerts" channel in "Threat Intel Alerts" team ×

Office 365 Connectors within Teams will be retired soon. The Workflows app provides similar functionality with more scalability and security. [Learn More](#).
Note: To manage existing connections, please open Connectors page in [Teams web client](#).

Search All Sort by Popularity

MANAGE

Configured

My Accounts

CATEGORY

All

Analytics

CRM

Customer Support

Developer Tools

HR

Marketing

News & Social

Project Management

Others

Connectors for your team

- RSS**
Get RSS feeds for your group. [Configure](#)
- Forms**
Easily create surveys, quizzes, and polls. [Configure](#)

All connectors

- Azure DevOps**
Collaborate on and manage software projects online. [Add](#)
- Incoming Webhook**
Send data from a service to your Office 365 group in real time. [Add](#)
- Jira Cloud**
Gather, organize, and assign issues detected in your software. [Add](#)
- Engage** Updated
Receive updates from your Engage network. [Add](#)

Figure 24. Create RSS connections to post blogs on team's channel.

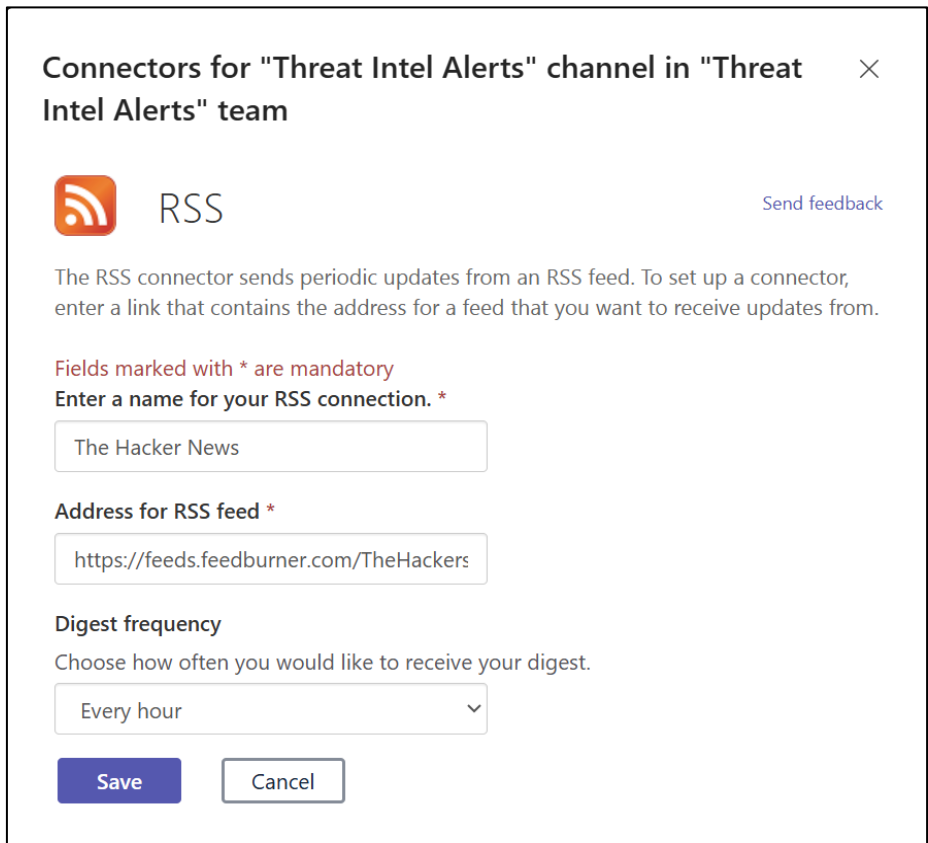


Figure 25. RSS connector configuration.

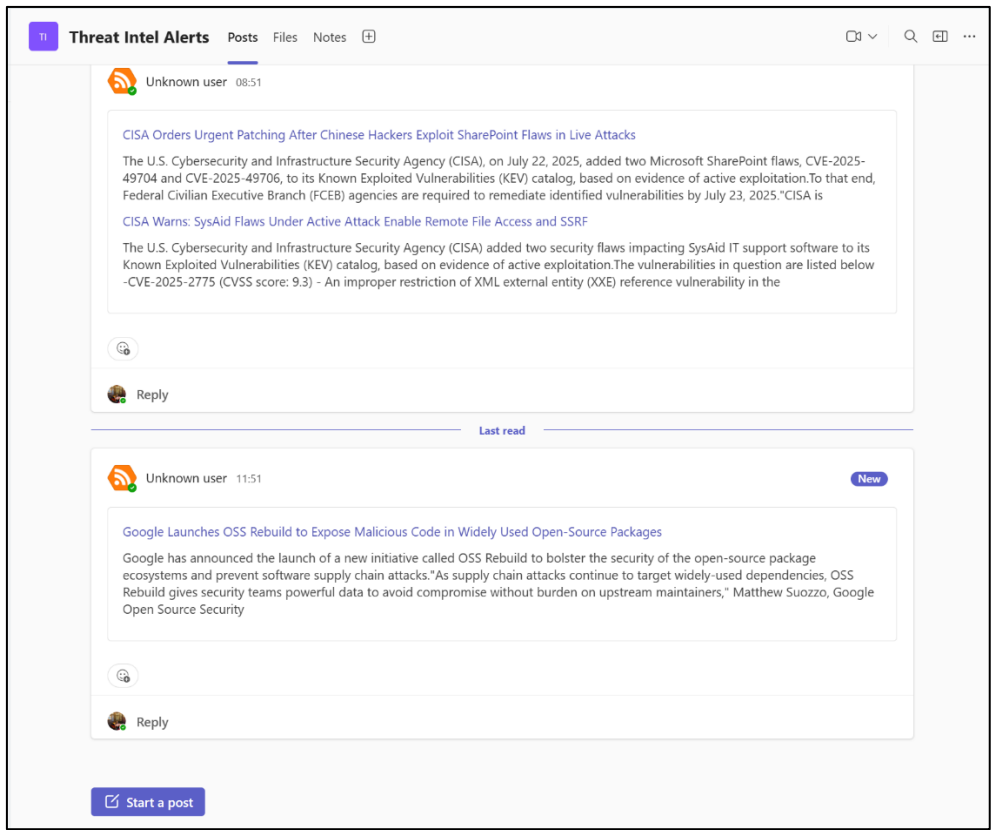


Figure 26. Channel posts triggered by RSS connector.

3.3. CTI Prioritisation Matrix

CTI Scoring Matrix: Criteria + Weights				
Criterion	Description	Score Range	Weight	Scoring Guide
TTP Alignment	Does the CTI reference TTPs relevant to past internal incidents or alerts?	0-3	High	3 = seen in past incident, 2 = plausible TTP, 1 = generic, 0 = none
Industry Targeted	Is the threat specific to your org's sector or geo?	0-2	Medium	2 = same sector, 1 = same region, 0 = no match
Recency	Is the threat/event reported in last 30 days?	0-2	Medium	2 = <7 days, 1 = <30 days, 0 = older
Confidence Score (IOC/Feed)	Confidence as per feed (ThreatFox, MISIP, etc.)	0-2	Medium	2 = >80%, 1 = 50-80%, 0 = <50% or not given
Evasion Capability	Does the threat involve stealthy, dual-use or evasive techniques?	0-1	Low	1 = yes (e.g., T1027, T1055), 0 = no
Detection Readiness	Can it be detected with existing tools/logs (Sentinel, Defender, Sysmon)?	0-1	High	1 = yes (log source available), 0 = no
Scoring Formula				
Total Score = TTP + Industry + Recency + Confidence + Evasion + Detection				
Priority Thresholds				
Total Score (Simple)		Priority	Recommended Action	
8-11		High	Build hypothesis, start hunt immediately	
5-7		Medium	Correlate with logs; schedule for review	
0-4		Low	Archive or pass to CTI-only channels	

Figure 27. CTI Prioritisation Matrix.

Section 4: Hypothesis Creation & Query Formulation

4.1. FileFix-Style Browser-Launched Command Execution

Hunt ID	TH001
Title	FileFix-Style Browser-Launched Command Execution
Objective	Detect browsers spawning suspicious binaries with obfuscation/payload flags, aligned with FileFix-style attacks.
CTI Reference	Triggered by recent articles and LinkedIn posts detailing the FileFix social-engineering attack chain. CTI from sources like mrd0x.com and LinkedIn technical writeups.
MITRE ATT&CK Mapping	T1059.001 (Command and Scripting Interpreter: PowerShell)
Hypothesis	Adversaries may exploit browsers or File Explorer to execute obfuscated commands by tricking users into pasting them into the address bar.
KQL Query	let MonitoredCommands = dynamic(["powershell", "pwsh", "regsvr32", "bitsadmin", "certutil", "mshta"]); let ParentProcessList = dynamic(["chrome", "msedge", "firefox", "brave",

	<pre> "explorer"]); DeviceProcessEvents where Timestamp > ago(30d) where FileName has _any(MonitoredCommands) where InitiatingProcessFileName has _any(ParentProcessList) where ProcessCommandLine has _any ("-EncodedCommand", "-enc", "-nop", "-NoProfile", "-w hidden", "-WindowStyle Hidden", "-ExecutionPolicy Bypass", "bypass", "Invoke-WebRequest", "iwr", "DownloadString", "iex", "Invoke-Expression", "Invoke-Obfuscation", "Add-MpPreference", "Start-Process") project Timestamp, DeviceName, FileName, ProcessCommandLine, InitiatingProcessFileName, InitiatingProcessCommandLine, AccountName order by Timestamp desc </pre>
Data Sources	DeviceProcessEvents

Figure 28. Hypothesis & query for FileFix-Style Browser-Launched Command Execution.

Advanced hunting Selected workspace: null Help resources

Phishing URL Clicks × Common Queries × New query × New query × New query × Port Scanning App Detected × New query ×

Run query Set in query Save Share link Manage rules

```

24
25 let MonitoredCommands = dynamic(["powershell.exe", "pwsh.exe", "regsvr32.exe", "bitsadmin.exe", "certutil.exe", "mshta.exe"]);
26 let BrowserList = dynamic(["chrome.exe", "msedge.exe", "firefox.exe", "brave.exe"]);
27 DeviceProcessEvents
28 | where Timestamp > ago(30d)
29 | where FileName in~ (MonitoredCommands)
30 | and InitiatingProcessFileName in~ (BrowserList)
31 | and ProcessCommandLine has_any ("-EncodedCommand", "-nop", "-NoProfile", "-w hidden", "-WindowStyle Hidden")
32
33
34

```

Getting started Results Query history

Export Show empty columns 2 items Search 00:01.588 Low Chart type Full screen

TimeGenerated	Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath
	10.0.26100.3323					
	POWERSHELL					
	PowerShell.EXE					
	Windows PowerShell					
	9688					
					"powershell.exe -NoProfile -WindowStyle Hidden -Command "echo FileFix Simulation > %env:TEMP%filefix.txt"	

Figure 29. Execution of query for FileFix-Style Browser-Launched Command Execution.

4.2. Potential Data Exfiltration (Insider Threat)

Hunt ID	TH002
Title	Potential Data Exfiltration (Insider Threat)
Objective	Identify emails with attachments sent to personal domains by users shortly before their account was disabled.
CTI Reference	Internal incident history related to intellectual property theft by leavers. Prior CTI reports highlighting insider threats targeting IP via personal emails.
MITRE ATT&CK Mapping	T1537 (Exfiltration Over Alternative Protocol)
Hypothesis	Users who were disabled recently may have sent sensitive data to personal email accounts shortly before their departure.
KQL Query	<pre>// Define personal email domains let personalDomains = dynamic(["gmail.com", "yahoo.com", "outlook.com", "hotmail.com", "aol.com", "icloud.com", "protonmail.com"]); // Step 1: Get latest disable event per user let latestDisables = AuditLogs where OperationName =~ "Disable account" mv-expand TargetResources extend AccountUPN = tostring(TargetResources.userPrincipalName) where isnotempty(AccountUPN) summarize DisabledTime = max(TimeGenerated) by AccountUPN; // Step 2: Get last sign-in time per user let lastSignIns = SigninLogs summarize LastSignIn = max(TimeGenerated) by UserPrincipalName; // Step 3: Join to keep only users who signed in on the same day as being disabled let validDisables = latestDisables join kind=inner (lastSignIns) on \$left.AccountUPN == \$right.UserPrincipalName where startofday(DisabledTime) == startofday(LastSignIn) project AccountUPN, DisabledTime, LastSignIn; // Step 4: Correlate outbound emails to personal domains within 30 days of disable EmailEvents where EmailDirection == "Outbound" extend RecipientDomain = tostring(split(RecipientEmailAddress, "@")[1]) where RecipientDomain in~ (personalDomains) join kind=inner (validDisables) on \$left.SenderFromAddress == \$right.AccountUPN where TimeGenerated between (DisabledTime -30d .. DisabledTime) extend DaysBeforeDisable = datetime_diff('day', DisabledTime,</pre>

	TimeGenerated) summarize AttachmentsSent = countif(AttachmentCount > 0), TotalEmailsSent = count(), FirstSeen = min(TimeGenerated), LastSeen = max(TimeGenerated), ActiveDays = dcount(bin(TimeGenerated, 1d)), PersonalDomainsContacted = make_set(RecipientDomain) by UserPrincipalName = SenderFromAddress, DisabledTime, LastSignIn extend DaysBeforeDisableStart = datetime_diff('day', DisabledTime, FirstSeen), ActivityDurationDays = datetime_diff('day', LastSeen, FirstSeen) where AttachmentsSent > 0 sort by TotalEmailsSent desc
Data Sources	AuditLogs SigninLogs EmailEvents

Figure 30. Hypothesis & query for Potential Data Exfiltration (Insider Threat)

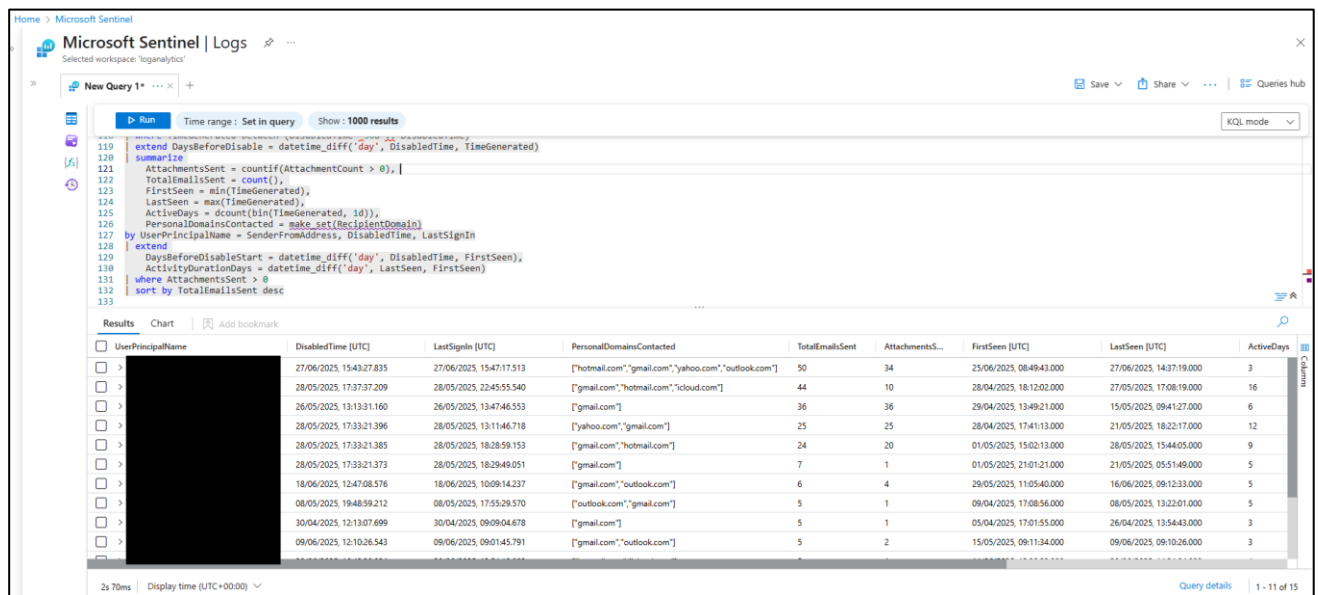


Figure 31. Execution of query for Potential Data Exfiltration (Insider Threat).

4.3 Potentially Malicious Browser Extensions

Hunt ID	TH003
Title	Potentially Malicious Browser Extensions
Objective	Detect installation of browser extensions known to be involved in spyware and user tracking campaigns via Chrome/Edge Web Store.
CTI Reference	Initiated in response to recent reports of 18 malicious browser extensions with millions of downloads, highlighted by Dark Reading, Koi Security, and Forbes.

MITRE ATT&CK Mapping	T1176 (Software Extensions: Browser Extensions)
Hypothesis	Users may unknowingly install browser extensions from trusted web stores that contain spyware capabilities or leak sensitive activity.
KQL Query	<pre>// Inline list of known-bad Chrome extensions let MaliciousExtensions = datatable(extension_id:string, extension_name:string)["kgmeffmlnkfnjjpgmdndcklfigfhajen", "Emoji keyboard online — copy & paste your emoji", "dpdibkjgbaadnnjhkmmnenkmbnhpobj", "Free Weather Forecast", "gaiceihehajjahakcglkhmddclbnlf", "Video Speed Controller — Video manager", "mlgbkfnjdmaoldgagamcnommbbnhfnhf", "Unlock Discord — VPN Proxy to Unblock Discord Anywhere", "eckokfcjbjbgjifpcbdmengnabecdakp", "Dark Theme — Dark Reader for Chrome", "mgbhdehiapbjamfgekfpemhmmcmemg", "Volume Max — Ultimate Sound Booster", "cbajickflblmpjodnjoldpiicfmeemif", "Unblock TikTok — One-Click Proxy", "pdbfnhlobhoahcamoefbfodpmlkgmjm", "Unlock YouTube VPN", "eokjikchkppnkdiplibggnmlkahcdkikp", "Color Picker Eyedropper — Geco colorpick", "ihbiedpeaicgipncdnnkikeehnjiddck", "Weather", "jjdajogomggcjifnjgkpgheijgkbcjdi", "Unlock TikTok", "mmcnmppeeghenglmidpmjkaiamcacmgm", "Volume Booster — Increase your sound", "ojdkklpgpaccicaobnhankbalkkgaafp", "Web Sound Equalizer", "lodeighbngipjjedfelnboplhgediclp", "Header Value", "hkjagicdaogfdifaklcajmgfjllmd", "Flash Player — games emulator", "gflkbgebojohihfnnplhbdakoipdbpdm", "YouTube Unblocked", "kpilmncnoafddjpnbhhepaiilgkdcieaf", "SearchGPT — ChatGPT for Search Engine", "caibdnkmpnjhjdfnomfhijhmebigcelo", "Unlock Discord"]; // Detect .crx installs in the last 30 days DeviceFileEvents where Timestamp > ago(30d) where ActionType in ("FileCreated", "FileModified") where FileName endswith ".crx" extend VersionedID = tostring(split(FileName, '.')[0]) extend ExtensionID = tolower(split(VersionedID, '_')[0])</pre>

	summarize LastSeen = max(TimeGenerated) by DeviceName, ExtensionID join kind=inner MaliciousExtensions on \$left.ExtensionID == \$right.extension_id
Data Sources	DeviceFileEvents

Figure 32. Hypothesis & query for Potentially Malicious Browser Extensions.

The screenshot shows the 'Advanced hunting' interface in Microsoft Sentinel. A query is displayed in the editor, and the results are shown below. The query filters for file creation events on .crx files within the last 30 days. The results table shows one entry for a file named 'EOKJKCHKPPNKDIPBIGGNMLKAHCDKIP_1_0_12_0.crx' created on 8 Jul 2025 08:33:46.

```

4 DeviceFileEvents
5 | where Timestamp > ago(30d)
6 | where ActionType == "FileCreated" or ActionType == "FileModified"
7 | where FileName endswith ".crx"
8 | extend ExtensionIDVersion = tostring(split(FileName, '.') [0])
9 | extend ExtensionID = tolower(split(ExtensionIDVersion, '-') [0])
10 | summarize avg_max(TimeGenerated, *) by DeviceName, ExtensionID
11 | join KoiSecurity on $left.ExtensionID == $right.extension_id
12 | project Timestamp, DeviceName, InitiatingProcessAccountUpn, extension_id, extension_name, ActionType, FileName
  
```

Timestamp	DeviceName	InitiatingProcessAccountUpn	extension_id	extension_name	ActionType	FileName
8 Jul 2025 08:33:46	[REDACTED]	[REDACTED]	eokjkchkppnkdiplibggnmlkahcdkikp	Color Picker Eyedropper — Geco colorpick	FileCreated	EOKJKCHKPPNKDIPBIGGNMLKAHCDKIP_1_0_12_0.crx

Figure 33. Execution of query Potentially Malicious Browser Extensions.

The screenshot shows the 'Hunting' section of the Microsoft Sentinel interface. Three hunt queries are listed in a table, all with a 'Validated' hypothesis and 'New' status.

Hunt name	Status	Hypothesis	Owner	Created time	Last update time
File-Style Browser-Launched Command Execution	New	Validated	Admin Amruta Pandhare	22/07/2025, 14:52	22/07/2025, 14:52
Potential Data Exfiltration (Insider Threat)	New	Validated	Admin Amruta Pandhare	22/07/2025, 13:47	22/07/2025, 14:27
Potentially Malicious Browser Extensions	New	Validated	Admin Amruta Pandhare	22/07/2025, 14:26	22/07/2025, 14:26

Figure 34. All three hunt queries created.

Section 5: Peer Review Process

Create a new repository [Try the new experience](#)

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository.](#)

Required fields are marked with an asterisk (*).

Owner * / Repository name *

threat-hunting-queries is available.

Great repository names are short and memorable. Need inspiration? How about [symmetrical-pancake](#) ?

Description (optional)

Public
Anyone on the internet can see this repository. You choose who can commit.

Private
You choose who can see and commit to this repository.

Initialize this repository with:
 Add a README file
This is where you can write a long description for your project. [Learn more about READMEs.](#)

Add .gitignore

Choose which files not to track from a list of templates. [Learn more about ignoring files.](#)

Choose a license

A license tells others what they can and can't do with your code. [Learn more about licenses.](#)

This will set `main` as the default branch. Change the default name in your [settings](#).

You are creating a public repository in your personal account.

[Create repository](#)

Figure 35. Create a new GitHub repository.

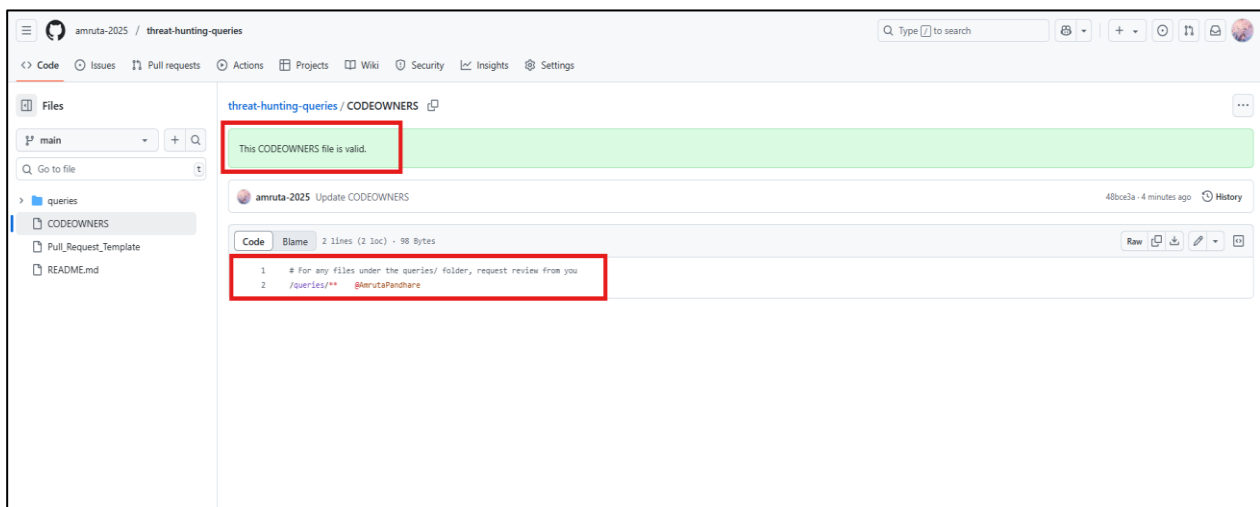


Figure 36. Create CODEOWNERS file for queries.

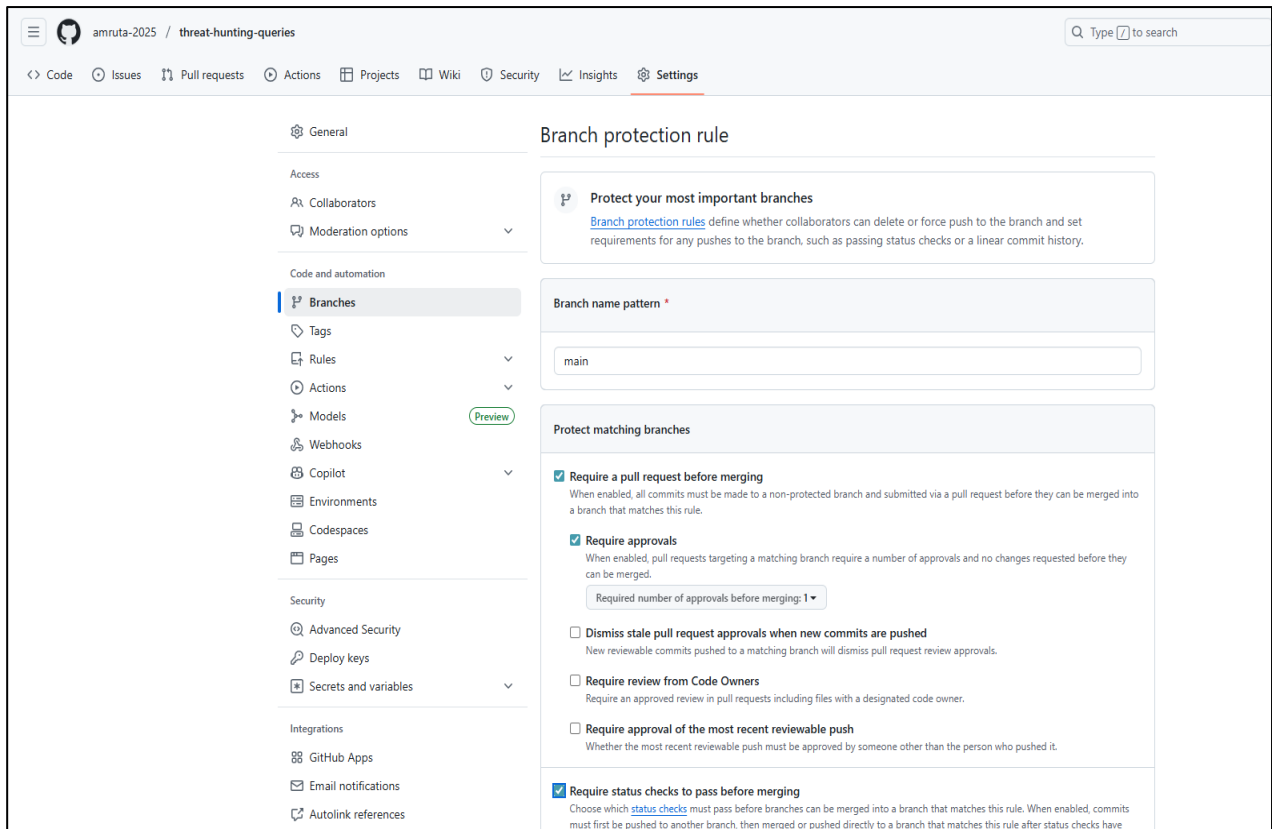


Figure 37. Create new branch protection rule.

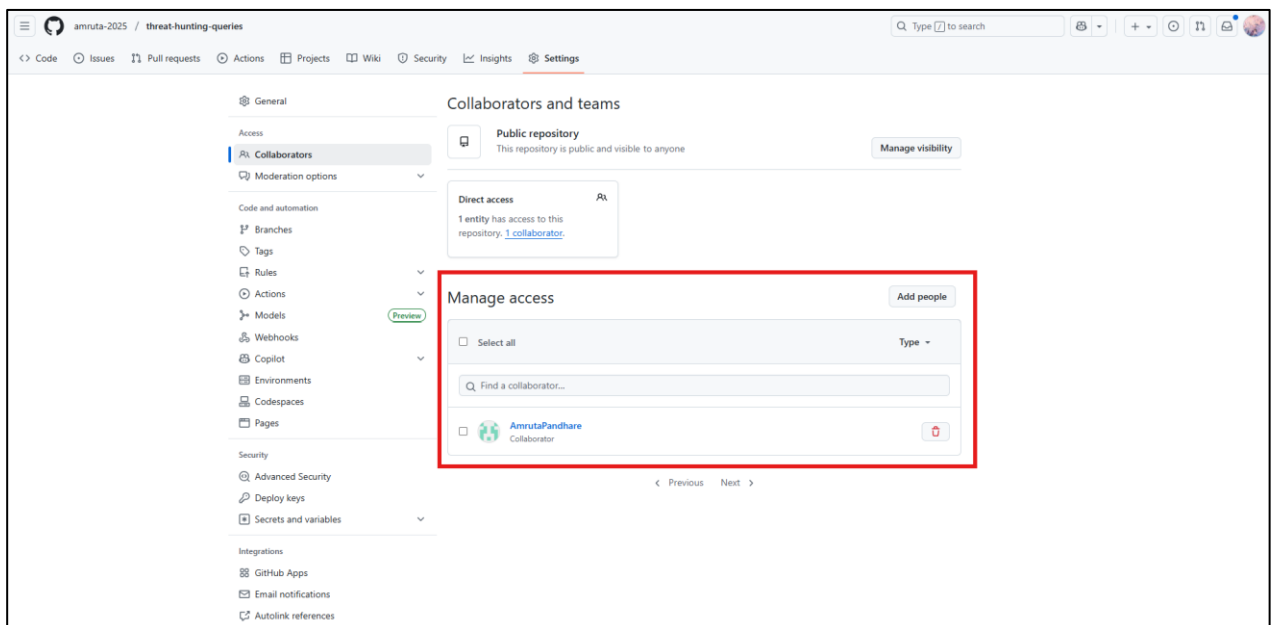


Figure 38. Invite collaborators for peer review.

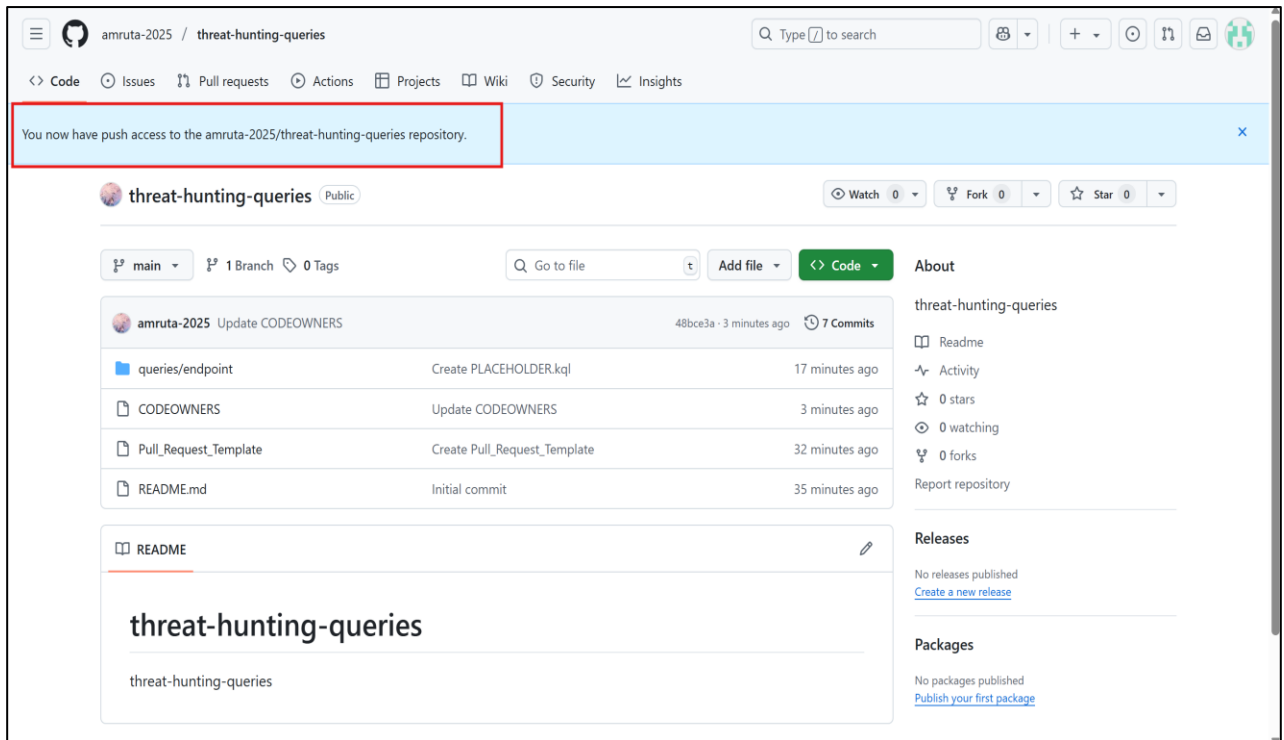


Figure 39. Granted push access to the collaborators.

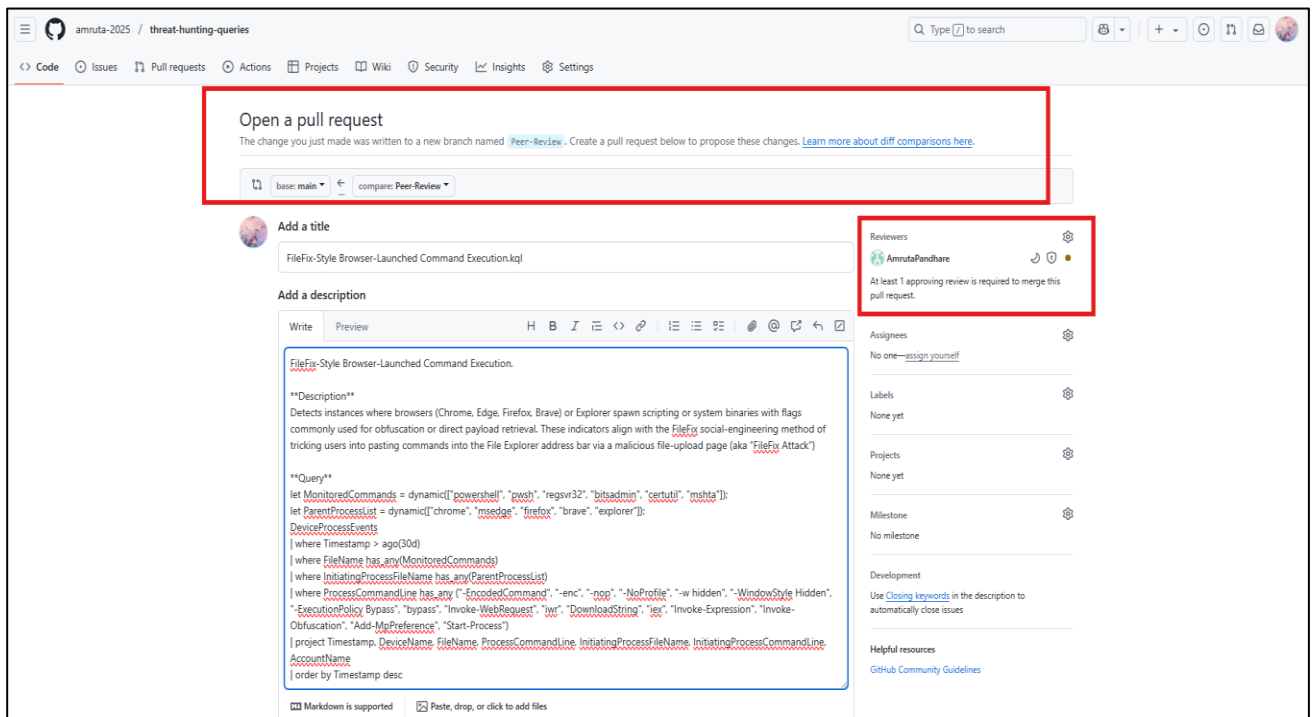


Figure 40. Create a new pull request with hunting data.

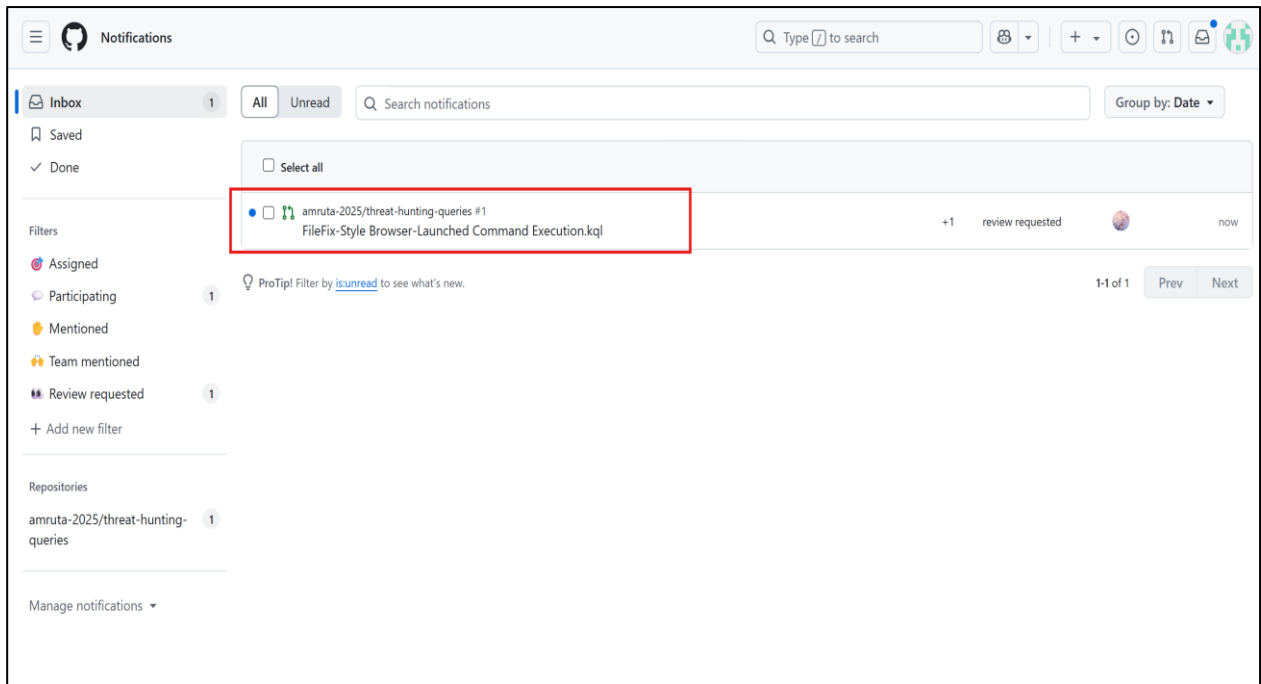


Figure 41. Collaborator will receive that pull request for review.

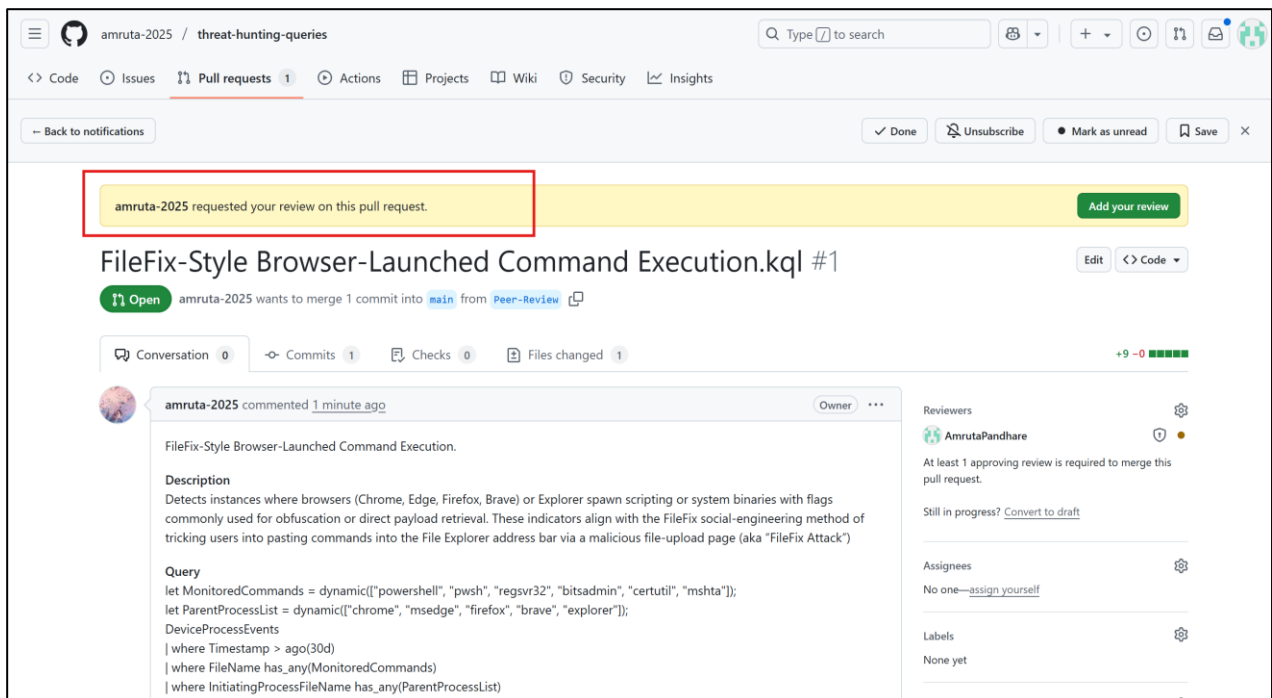


Figure 42. Requested pull request for review.

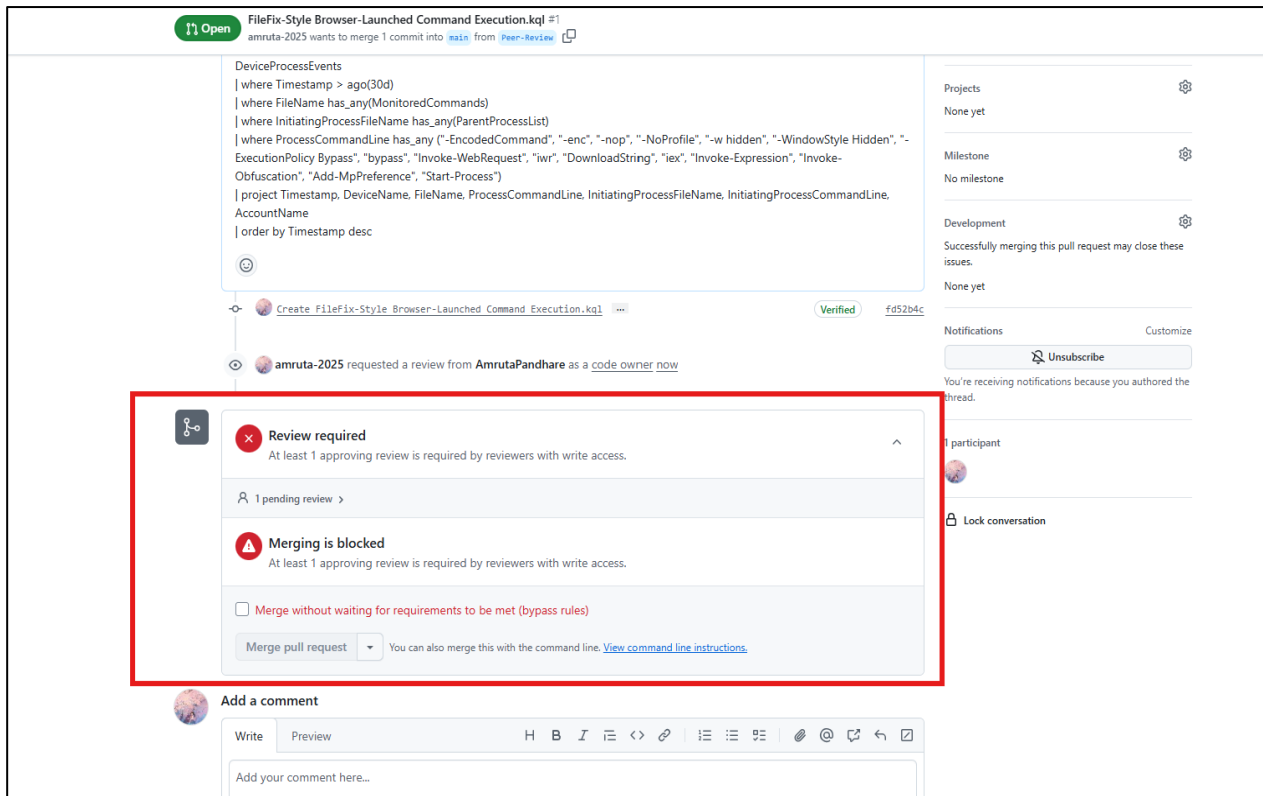


Figure 43. At least 1 approval is required by collaborators.

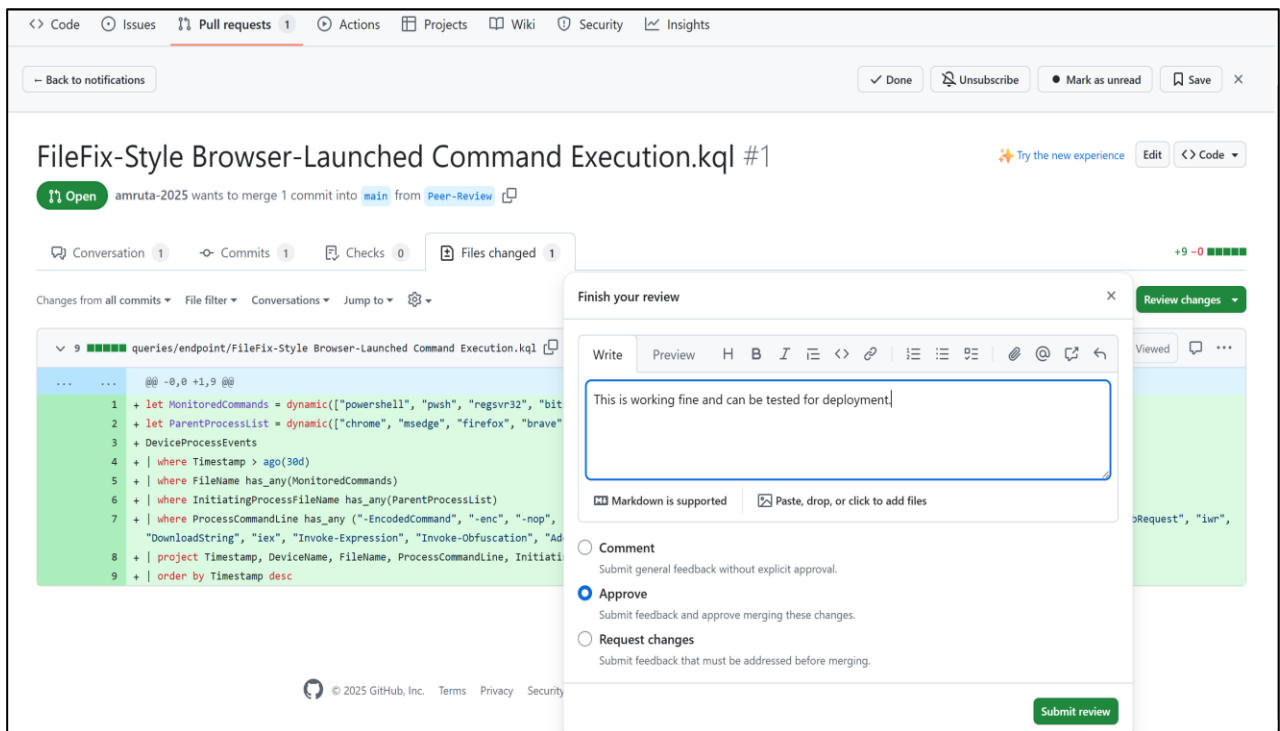


Figure 44. Add review comments.

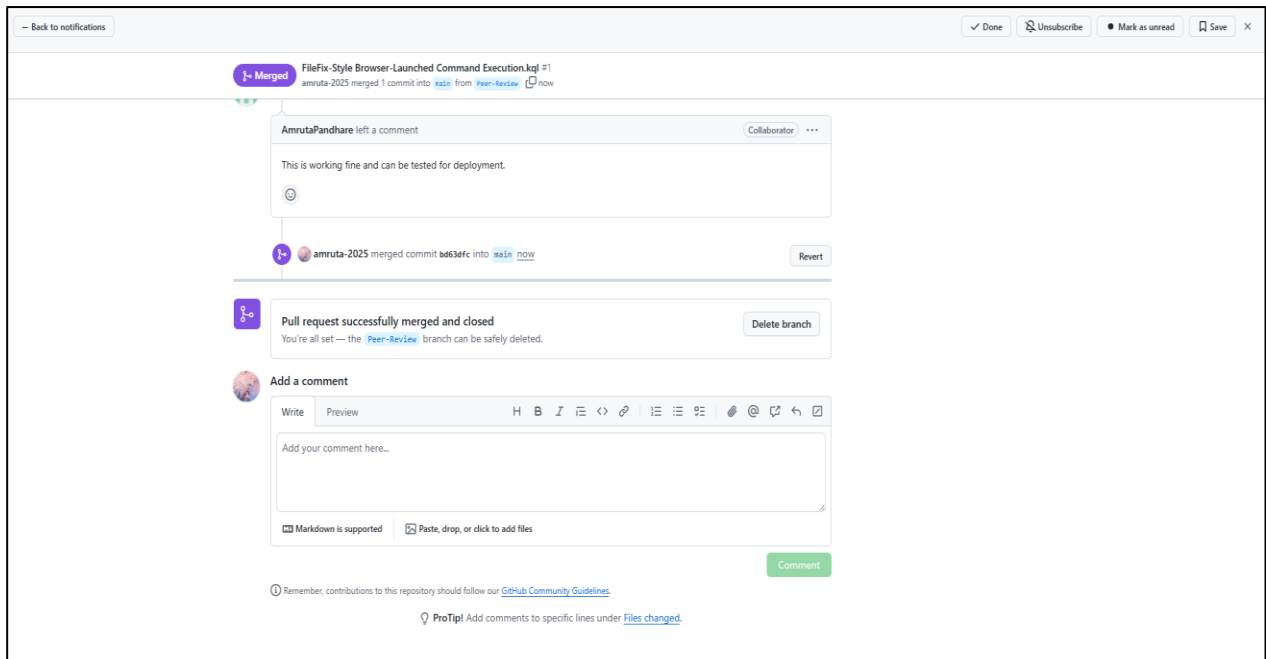


Figure 45. Merge it to the main branch if validated.

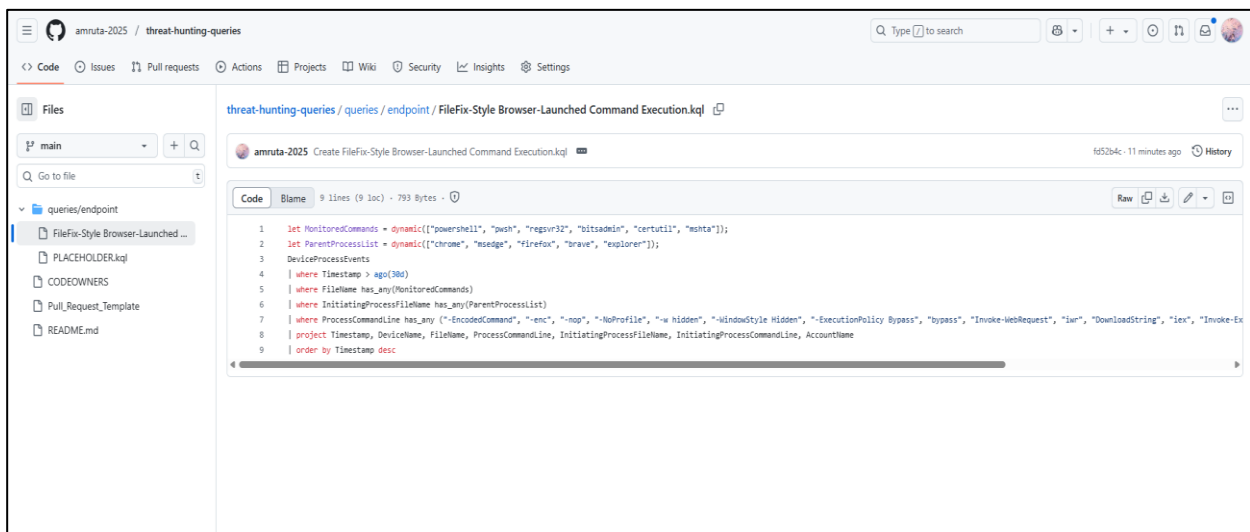


Figure 46. GitHub repository with approved threat hunting queries.

Section 6: Hypothesis Validation (Red/Blue Testing)

6.1. FileFix-Style Browser-Launched Command Execution

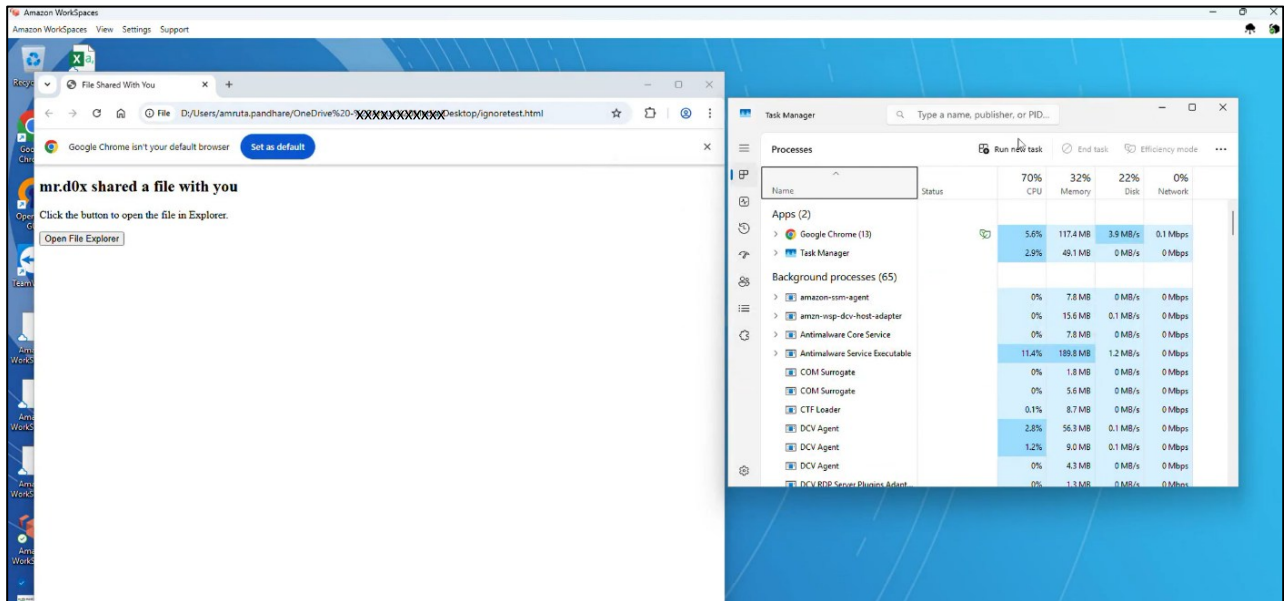


Figure 47. Phishing payload creation.

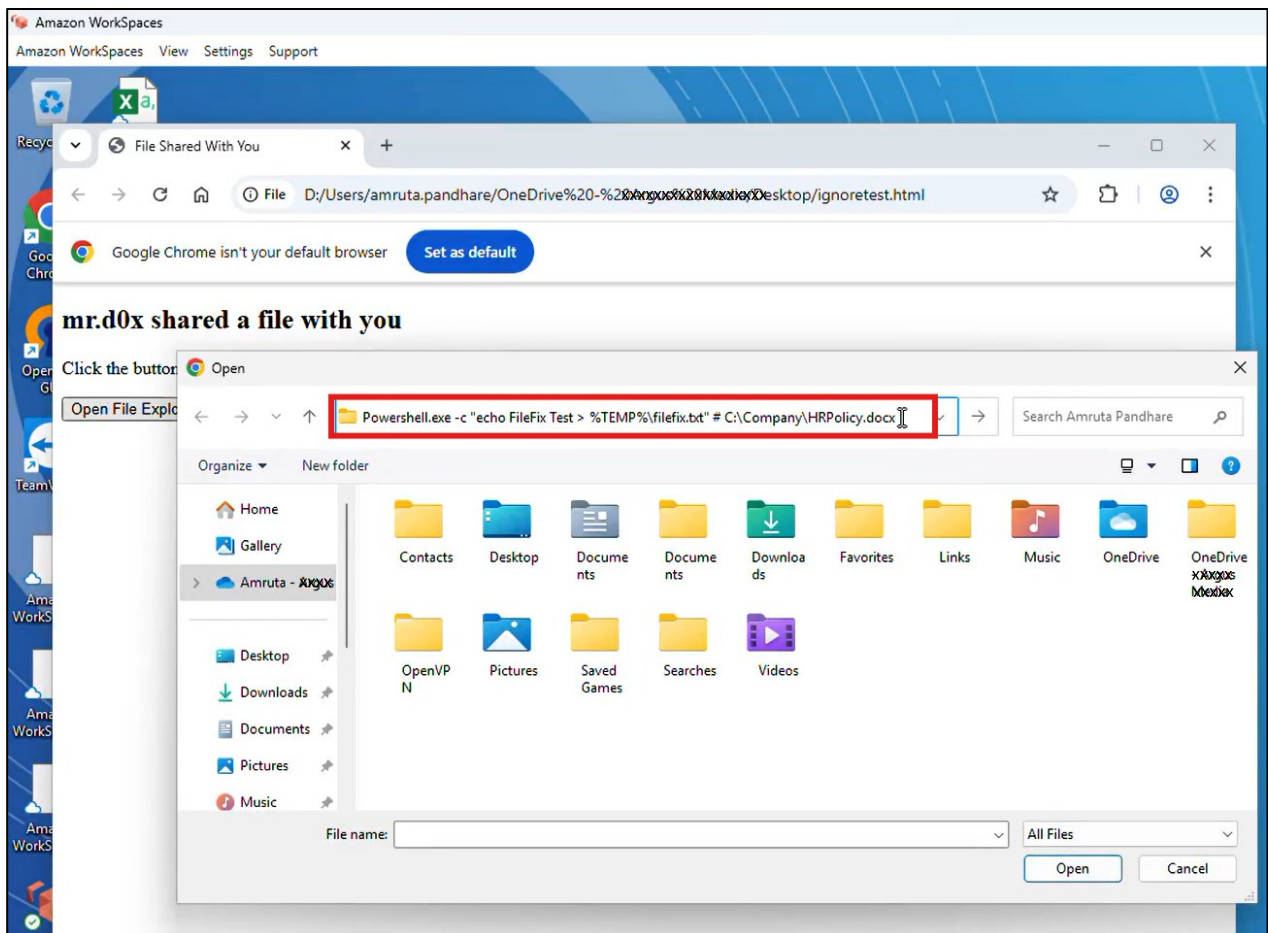


Figure 48. FileFix Style malicious command execution.

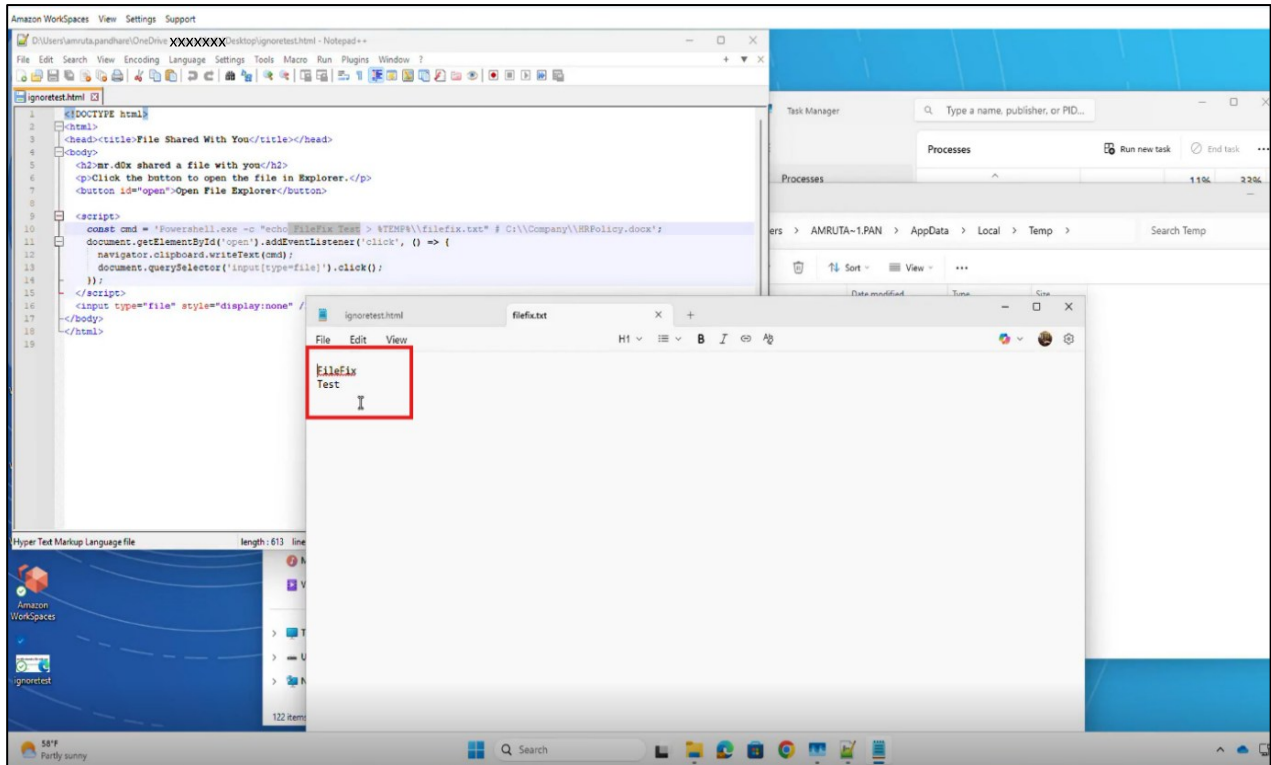


Figure 49. Malicious payload code & output.

6.2. Potential Data Exfiltration (Insider Threat)

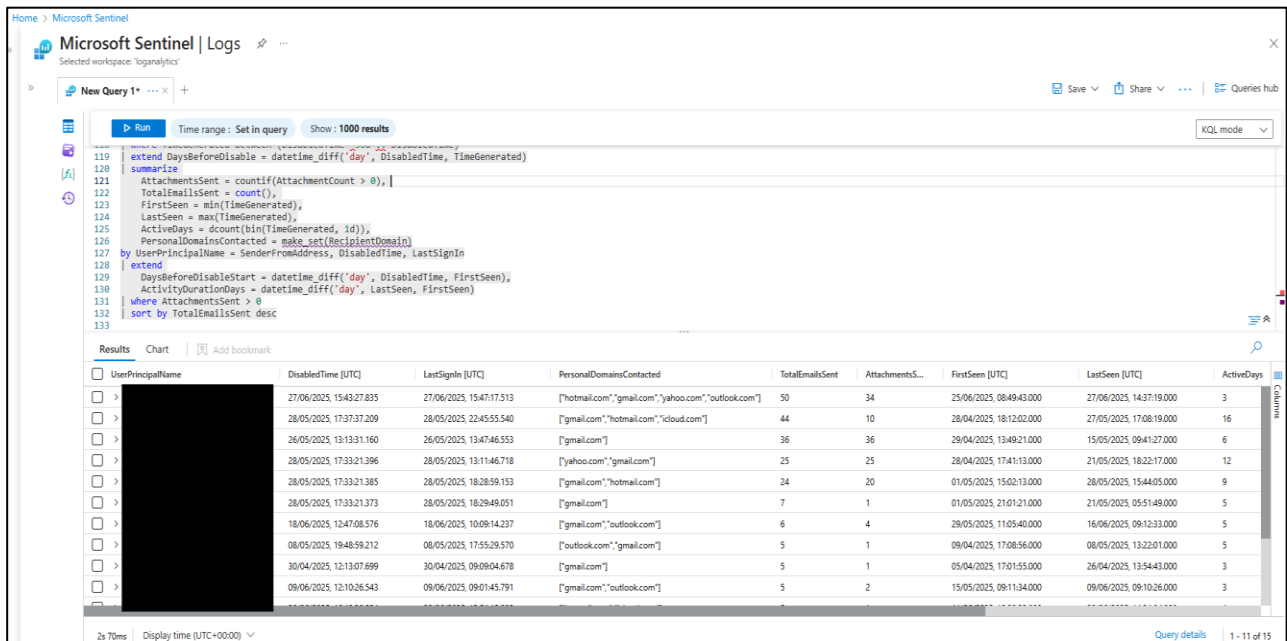


Figure 50. Email events SOC telemetry.

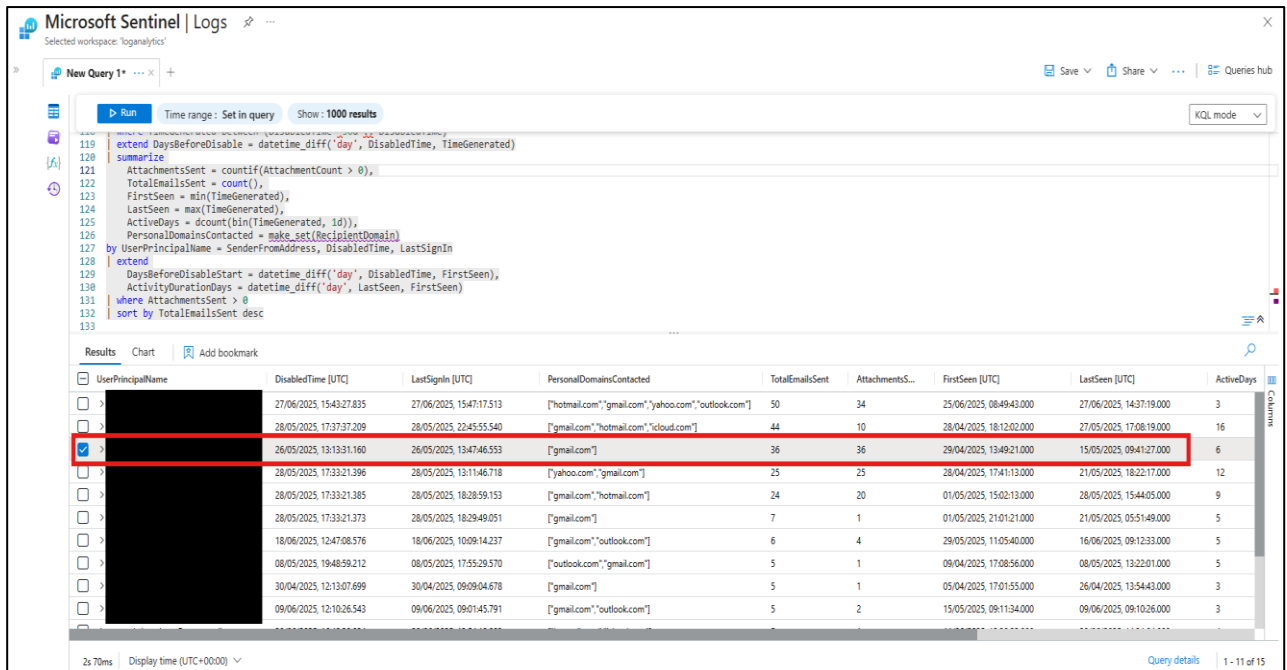


Figure 51. Suspicious data exfiltration by departing employee.

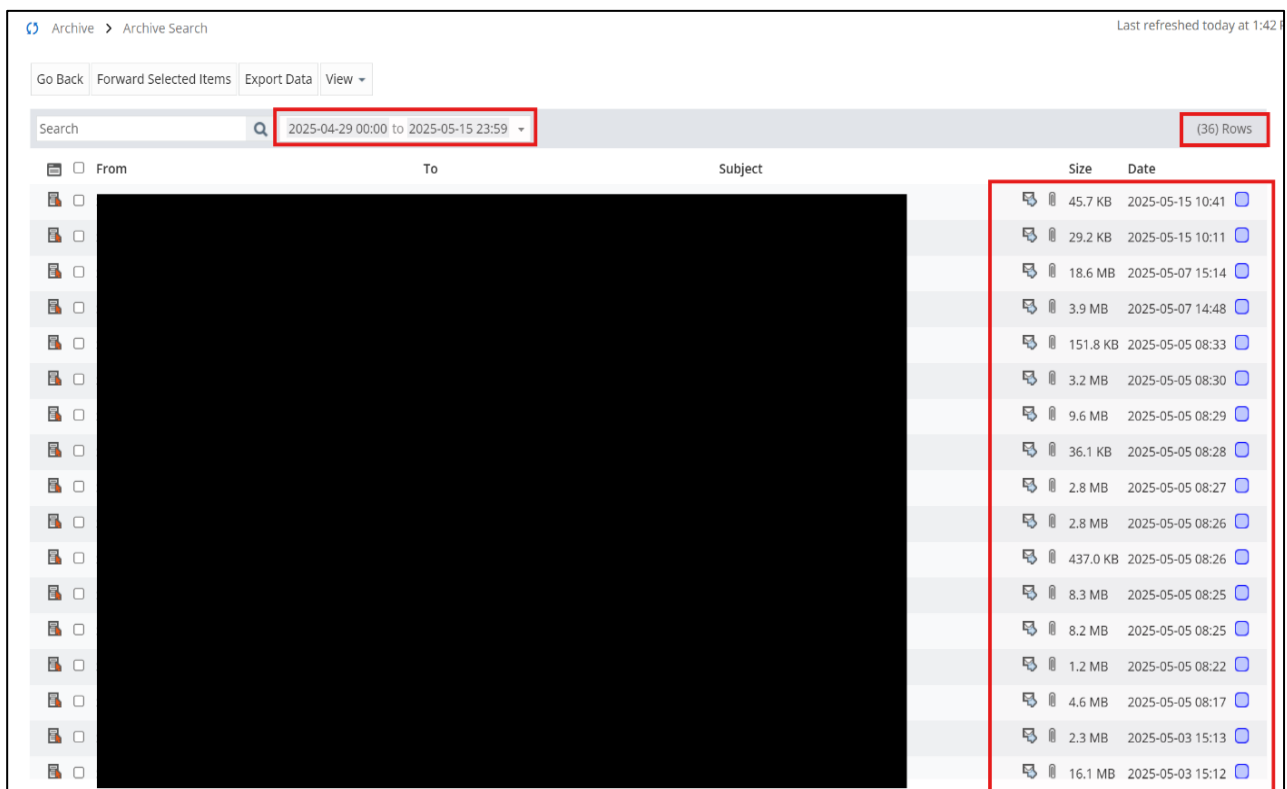


Figure 52. Validated Mimecast logs for data exfiltration for the same departing user.

6.3. Potentially Malicious Browser Extensions

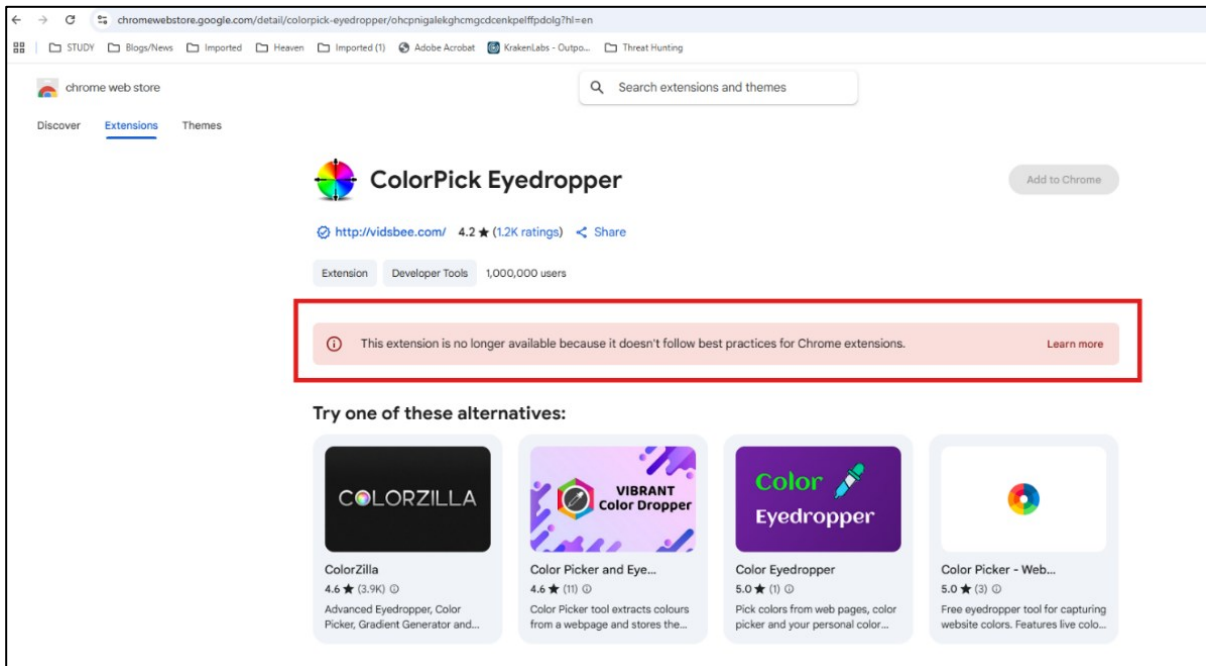


Figure 53. Malicious browser extension removed by chrome web store.

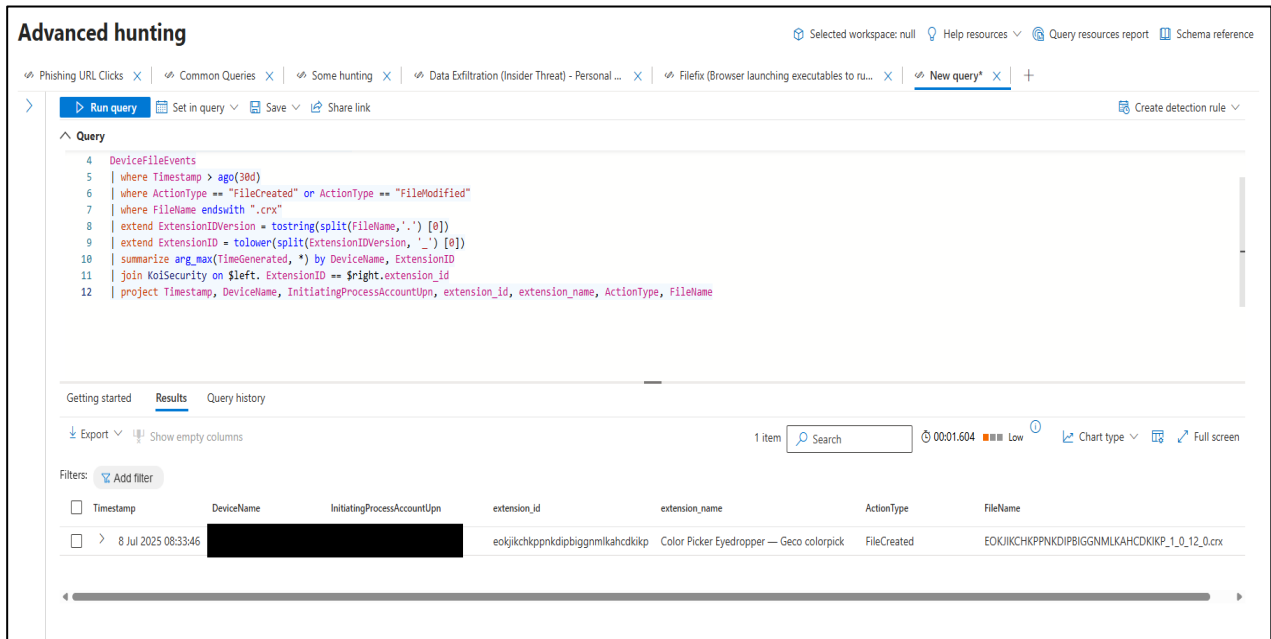


Figure 54. Malicious browser extension installed on user's device.

Section 7: Detection Rule & Playbook Creation

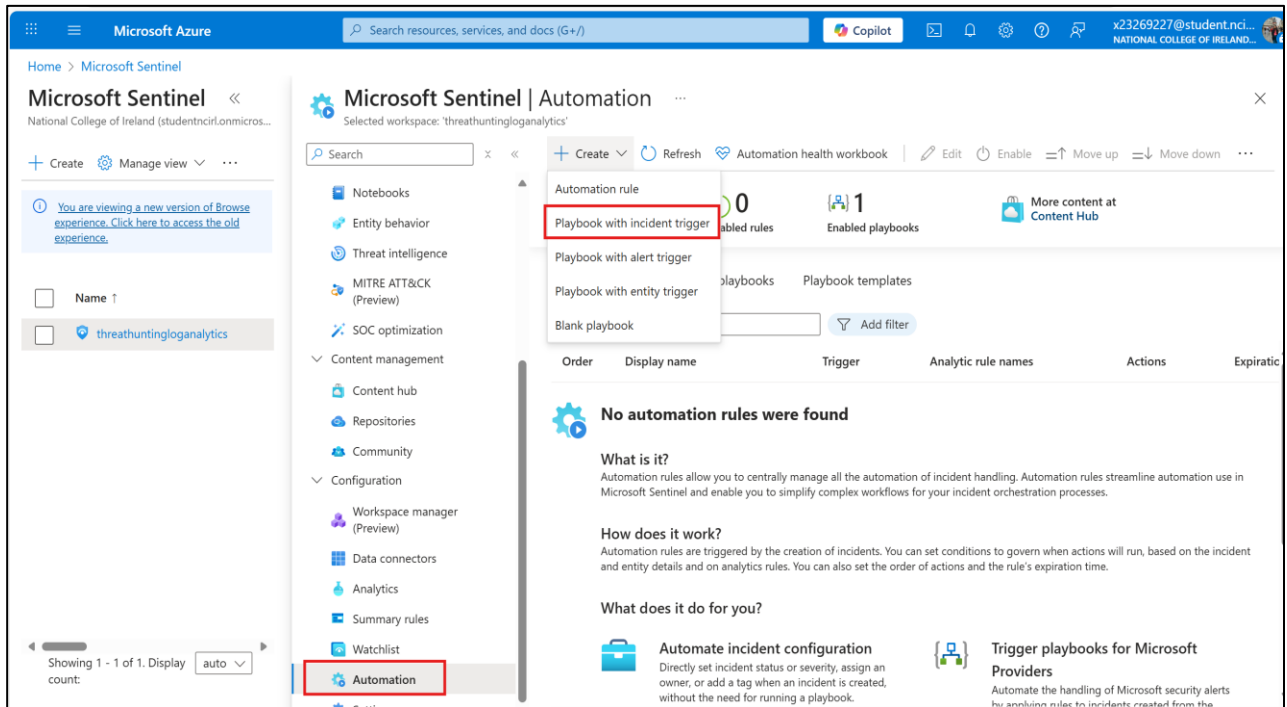


Figure 55. Example of playbook creation for detection rule.

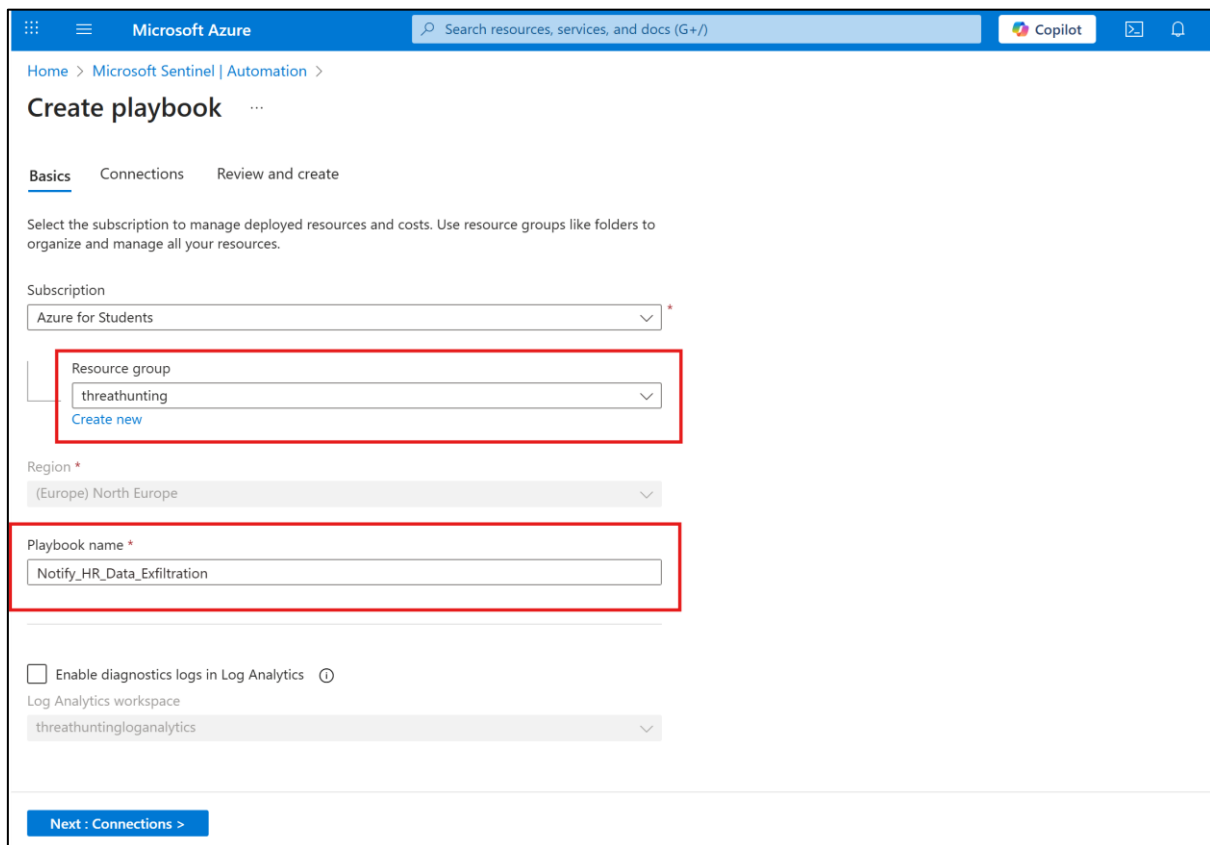


Figure 56. Create a playbook to notify HR about data exfiltration.

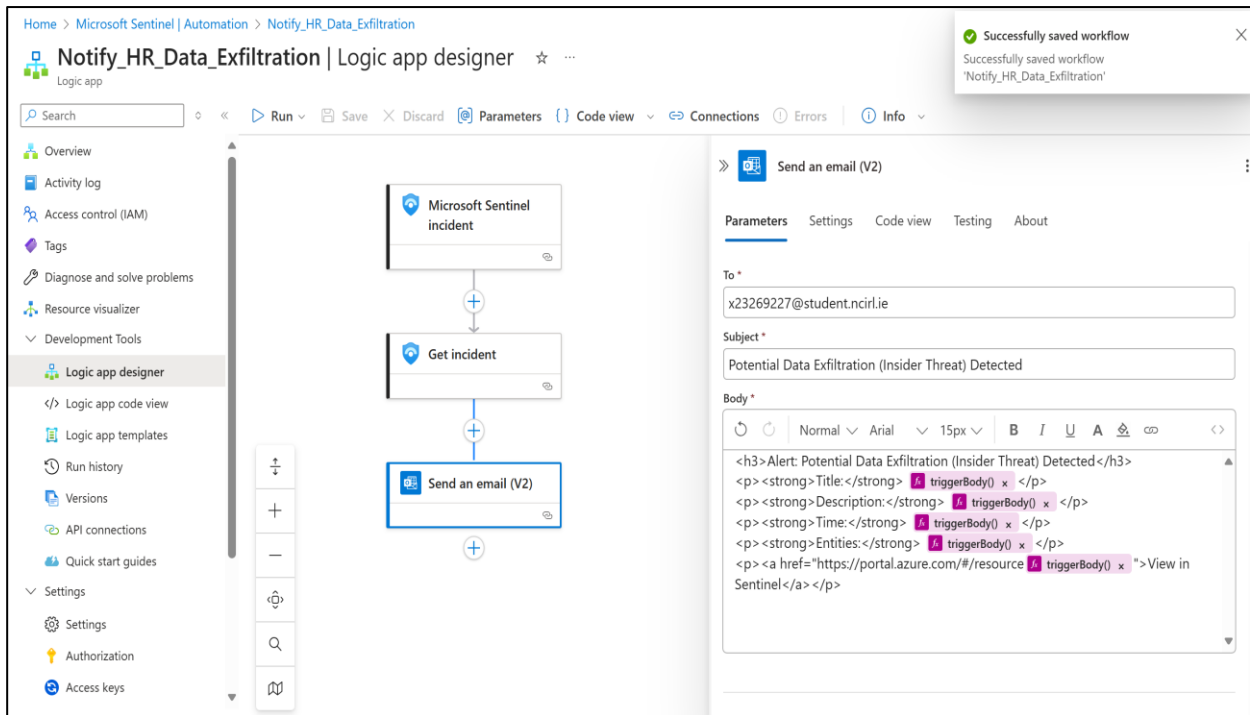


Figure 57. Create a logic flow to send email on incident trigger.

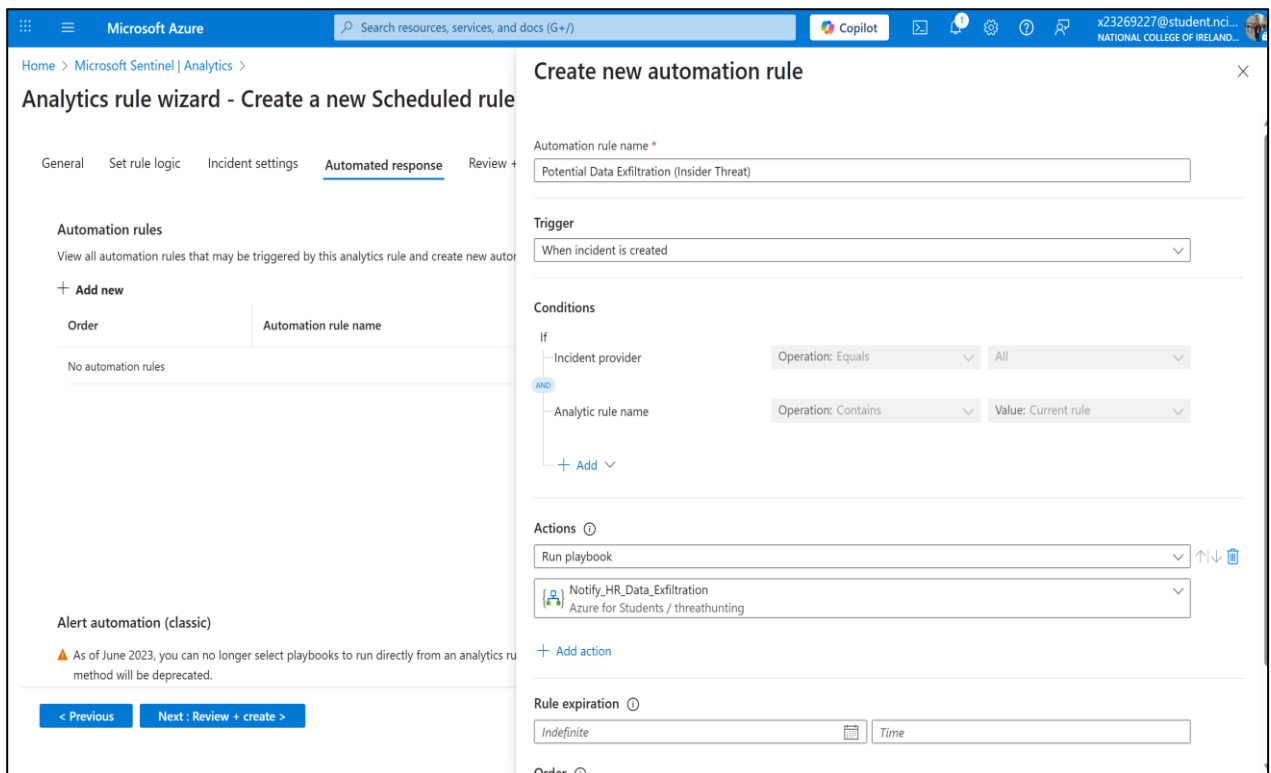


Figure 58. Add created playbook to detection rule for automated response.

Section 8: Documentation & Knowledge Formalisation

	A	B	C
1	Threat Hunting Template		
2	Hunt ID	TH001	
3	Title	FileFix-Style Browser-Launched Command Execution	
4	Objective	Detect browsers spawning suspicious binaries with obfuscation/payload flags, aligned with FileFix-style attacks.	
5	CTI Reference	Triggered by recent articles and LinkedIn posts detailing the FileFix social-engineering attack chain. CTI from sources like mrd0x.com and LinkedIn technical writeups.	
6	MITRE ATT&CK Mapping	T1059.001 (Command and Scripting Interpreter: PowerShell)	
7	Hypothesis	Adversaries may exploit browsers or File Explorer to execute obfuscated commands by tricking users into pasting them into the address bar.	
8	KQL Query	<pre>let MonitoredCommands = dynamic(["powershell", "pwsh", "regsvr32", "bitsadmin", "certutil", "mshta"]); let ParentProcessList = dynamic(["chrome", "msedge", "firefox", "brave", "explorer"]); DeviceProcessEvents where Timestamp > ago(30d) where FileName has _any(MonitoredCommands) where InitiatingProcessFileName has _any(ParentProcessList) where ProcessCommandLine has _any ("-EncodedCommand", "-enc", "-nop", "-NoProfile", "-w hidden", "-WindowStyle Hidden", "-ExecutionPolicy Bypass", "bypass", "Invoke-WebRequest", "iwr", "DownloadString", "iex", "Invoke-Expression", "Invoke-Obfuscation", "Add-MpPreference", "Start-Process") project Timestamp, DeviceName, FileName, ProcessCommandLine, InitiatingProcessFileName, InitiatingProcessCommandLine, AccountName order by Timestamp desc</pre>	

< > ☰ Maturity Level Assessment CTI Prioritization SOP Template 1 SOP Template 2 SOP Template 3 +

Figure 59. Detailed documentation of threat hunting SOPs

Section 9: Retrospective & Metrics Dashboard

The screenshot displays the Amazon QuickSight interface. On the left, a navigation sidebar includes options like Favorites, Recent, My folders, Shared folders, Dashboards, Data stories, Analyses, **Datasets** (highlighted), Community, and Topics. The main area shows a table of datasets:

Name	Owner	Last Modified
[Redacted]	SPICE Me	8 months ago
[Redacted]	SPICE Me	a month ago
[Redacted]	SPICE Me	7 days ago
Thrive Hunt Summary.csv	SPICE Me	2 days ago
Thrive CTI Scoring.csv	SPICE Me	2 days ago
THRIVE HMM Progress.csv	SPICE Me	2 days ago
[Redacted]	SPICE Me	2 days ago
[Redacted]	SPICE Me	a day ago
Thrive TTPS.xlsx	SPICE Me	16 hours ago
Thrive TTPS.xlsx	SPICE Me	16 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	12 hours ago
[Redacted]	SPICE Me	2 hours ago

In the top right corner, a 'NEW DATASET' button is highlighted with a red box. The 'Datasets' menu item in the left sidebar is also highlighted with a red box.

Figure 60. Create a dashboard using Amazon QuickSight.

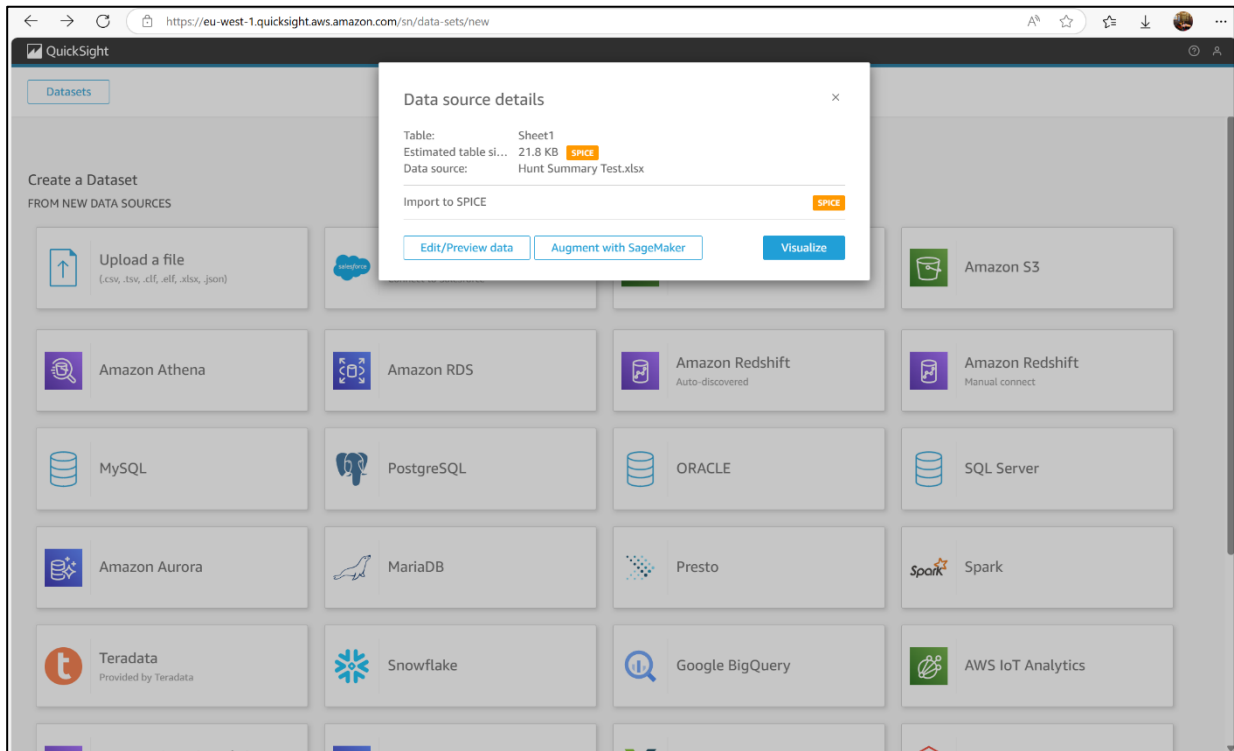


Figure 61. Upload threat hunting data including all the details.

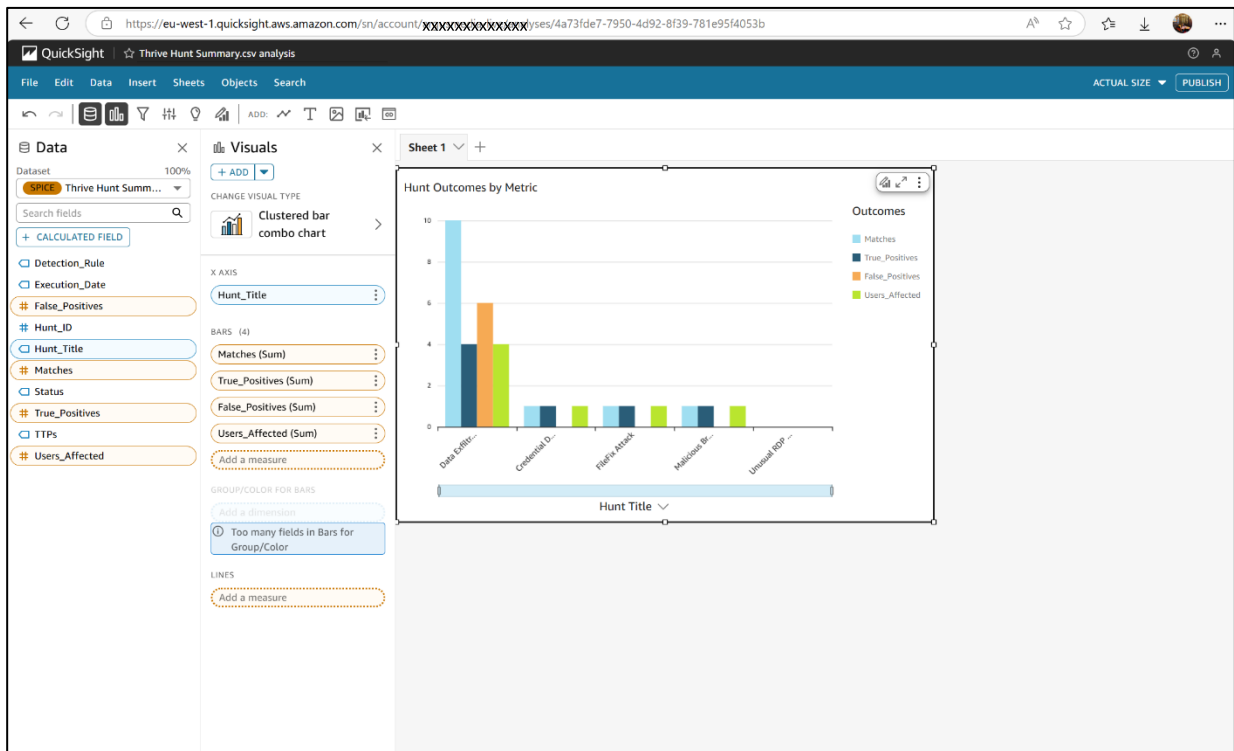


Figure 62. Create dashboard using QuickSight visualization.

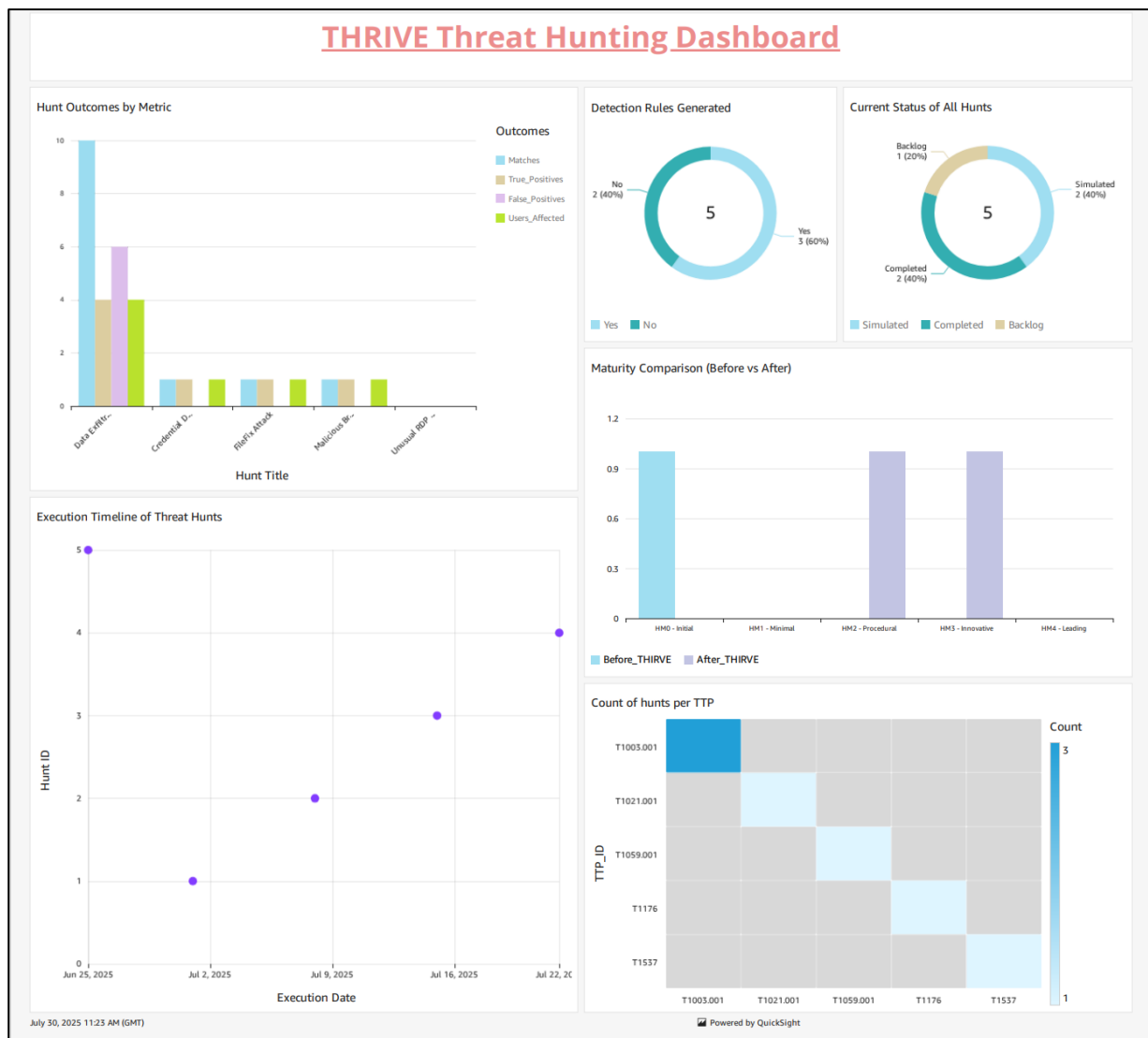


Figure 63. Threat hunting dashboard.

Section 10: References

Microsoft Learn (2024). *Create Log Analytics workspaces - Azure Monitor*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace?tabs=azure-portal> [Accessed 03 Aug. 2025].

Microsoft Learn (2025). *Onboard to Microsoft Sentinel*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/sentinel/quickstart-onboard?tabs=defender-portal> [Accessed 03 Aug. 2025].

Microsoft Learn (2025). *Quickstart - Create a Windows VM in the Azure portal - Azure Virtual Machines*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal> [Accessed 03 Aug. 2025].

Microsoft Learn (2025). *Find your Microsoft Sentinel data connector*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/sentinel/data-connectors-reference> [Accessed 03 Aug. 2025].

Amazon.com. (2025). *Create a WorkSpace in WorkSpaces Personal - Amazon WorkSpaces*. [online] Available at: <https://docs.aws.amazon.com/workspaces/latest/adminguide/create-workspaces-personal.html> [Accessed 03 Aug. 2025].

Abuse.ch. (2025). *ThreatFox | Export*. [online] Available at: <https://threatfox.abuse.ch/export/#csv> [Accessed 03 Aug. 2025].

Microsoft Learn (2025). *Create example Consumption workflow in Azure portal - Azure Logic Apps*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/logic-apps/quickstart-create-example-consumption-workflow> [Accessed 08 Aug. 2025].

Microsoft Learn (2025). *Reference for functions in workflow expressions - Azure Logic Apps*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/logic-apps/expression-functions-reference> [Accessed 08 Aug. 2025].

Microsoft Learn (2024). *Manage Microsoft 365 connectors and custom connectors - Microsoft Teams*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/microsoftteams/m365-custom-connectors> [Accessed 08 Aug. 2025].

Microsoft Learn (2024). *Hunting capabilities in Microsoft Sentinel*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/sentinel/hunting?tabs=defender-portal> [Accessed 13 Aug. 2025].

Microsoft Learn (2025). *Create custom hunting queries in Microsoft Sentinel - Microsoft Sentinel*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/sentinel/hunts-custom-queries?tabs=defender-portal> [Accessed 13 Aug. 2025].

Microsoft Learn (2025). *Kusto Query Language (KQL) overview - Kusto*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/kusto/query/?view=microsoft-fabric> [Accessed 13 Aug. 2025].

GitHub Docs. (2025). *Pull requests documentation - GitHub Docs*. [online] Available at: <https://docs.github.com/en/pull-requests> [Accessed 15 Aug. 2025].

Mrd0x.com. (2025). Available at: <https://mrd0x.com/filefix-clickfix-alternative/> [Accessed 15 Aug. 2025].

Toulas, B. (2025). *Malicious Chrome extensions with 1.7M installs found on Web Store*. [online] BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/malicious-chrome-extensions-with-17m-installs-found-on-web-store/> [Accessed 15 Aug. 2025].

Microsoft Learn (2025). *Create scheduled analytics rules in Microsoft Sentinel*. [online] Microsoft.com. Available at: <https://learn.microsoft.com/en-us/azure/sentinel/create-analytics-rules?tabs=defender-portal> [Accessed 15 Aug. 2025].

Amazon.com. (2025). *Tutorial: Create an Amazon QuickSight dashboard using sample data - Amazon QuickSight*. [online] Available at: <https://docs.aws.amazon.com/quicksight/latest/user/example-analysis.html> [Accessed 15 Aug. 2025].