Professional Portfolio

Tevin Agtarap

Cybersecurity & Information Assurance

Splunk Engineer | Cloud Security Specialist | SIEM & Compliance Expert

Table of Contents

TEVIN AGTARAP

Mobile: 406.202.8047 | Email: agtaraptevin@gmail.com | LinkedIn: https://www.linkedin.com/in/tevinagtarap/
| Clearance: Top Secret/SCI

PERFORMANCE SUMMARY

Incident Response & SIEM Management – Develop, customize, and maintain SIEM solutions such as Splunk and ePO (Trellix/McAfee) to support organizational security posture and conduct log analysis, threat detection, and response coordination.

Compliance & Security knowledge – Leverage knowledge of frameworks such as NIST, implement and manage security controls that meet compliance requirements. Adept at collaborating within teams or working independently to address dynamic security challenges effectively.

Vulnerability Assessment & Management – Conduct vulnerability assessments of DoD information systems and suggest remediation actions for identified vulnerabilities.

- Security Information & Event Management (SIEM) ■ ePO DLP Management ■ Team Leadership
- Cybersecurity & Risk Management ■ Project Management ■ ACAS Configuration
- IT Infrastructure & Operations ■ Cloud Vulnerability & Solutions ■ eMASS Administration
- SOC & Incident Response ■ Regulatory Compliance ■ Stakeholder Engagement

EDUCATION

Bachelor of Science, Cybersecurity & Information Assurance 2021, Western Governors University, Salt Lake City, UT

Master of Science, Cybersecurity & Information Assurance 2024, Western Governors University, Salt Lake City, UT

CERTIFICATIONS

Splunk – Splunk Core Certified Power User, Splunk Enterprise Certified Admin
CompTIA - A+, Project+, Network+**, Security+, CySA+, Pentest+, CASP+**
AWS – Certified Cloud Practitioner
ISC2 – Certified in Cybersecurity
CIW Web Security Associate ITIL

PROFESSIONAL EXPERIENCE

Applied Research Laboratories, The University of Texas at Austin (ARL: UT) – Austin, TX
Splunk Engineer - 03/2025 - Present *(FULL TIME – 40HRS A WEEK)*

- Design and deploy Splunk Enterprise on Linux/Windows across single and distributed environments.
- Install/configure search heads, indexers, UF/HF, deployment server, cluster manager

- Own data onboarding: inputs.conf, props.conf, transforms.conf
- Develop dashboards for ISSOs/ISSMs and business leaders, visualizing system health, alerts, and compliance posture.
- Train users on SPL, onboarding, dashboards, and best practices
- Evaluate and pilot new Splunk features, apps, and TAs; integrate and operationalize when they add value.

Army Future Command – Austin, TX
Information Assurance Engineer III 10/2/2023 – 03/02/2025 (FULL TIME – 40HRS A WEEK)

- Assist stakeholders in identifying and evaluating technical and operational security risks, threats, weaknesses, and vulnerabilities associated with information systems.
- Monitor DISA STIGs for updates and communicate any changes to stakeholders.
- Conduct research and investigations of cyber events to include those that potentially violate regulatory requirements.
- Assist with ACAS scans on NIPR and SIPR machines. Direct remediation teams to open vulnerabilities that need to be remediated.
- Develop and maintain cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
- Incident response and protection using ePO and Microsoft defender. Physical incident response in identifying asset and securing asset for further investigation and forensics.
- Monitor controls in eMASS to help push assess only and assess and authorize packages through the RMF process.

BAE SYSTEMS – HILL AFB, UT
CYBER ANALYST II (ISSO/ISSM) 03/13/2023 – 9/23/2023 (FULL TIME – 40HRS A WEEK)

- Serve as cybersecurity technical advisor, consultant, and primary point of contact to the Program Manager, Information System Owner, and other stakeholders
- Assessment and analysis of threats, vulnerabilities, and risk for assigned system(s)
- Ensure continuous monitoring (e.g., weekly, monthly, etc.) in accordance with cognizant security authority requirements are being implemented and met.
- Ensure all DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals

- Work with NIST 800-53 and JSIG to insure DoD Risk Management framework best practices
- Interfacing with information assurance managers, including reviewing documentation, such as systems security plans (SSPs), risk assessment reports, accreditation packages, and Plan of Actions and Milestones (POA&Ms)
- Perform or review Security Impact Assessments for configuration changes and facilitate approval or disapproval of changes with the appropriate stakeholders
- Provide mentoring to other team members

DEPARTMENT OF DEFENSE, AIR FORCE – HILL AFB, UT (NH-2210-3) **INFORMATION SYSTEM SECURITY OFFICER,** *08/29/2022 – 03/10/2023 (FULL TIME – 40HRS A WEEK)*

- Support for Special Access Program (SAP) Information Assurance activates
- Review, prepare and update Automated Information System (AIS) authorization packages, perform selfinspections, identify AIS vulnerabilities, and implement countermeasures, prepare reports on the status of security safeguards applied to the computer systems
- Analyze complexities of existing technology, review/revise/develop policy, initiate plans for enhancements, and provide management sufficient technical and cost analysis information, through written documentation and oral briefings
- Work with the ISSM in designing and implementing government regulatory compliance requirements
- Communicate with ISSM and incident response team on any security incidents
- Work with NIST 800-53 and JSIG to insure DoD Risk Management framework best practices
- Coordinate any changes or modifications to hardware, software, or firmware of a system with the ISSM and AO/DAO prior to the change
- Identify cyber security vulnerabilities and assist with the implementation of the countermeasures for them

D.A. DAVIDSON COMPANIES, IT RISK MANAGEMENT TEAM, REMOTE – HELENA, MT **IT SECURITY OPERATIONS SPECIALIST II,** *04/12/ 2021 – 05/27/2022 (FULL TIME – 40HRS A WEEK)*

- Administer the provisioning, de-provisioning, and review of access controls on systems to ensure the principle of least privilege, separation of duties and need to know is being followed in adherence to Davidson policies
- Handling events such as identifying security issues, extensive troubleshooting, and coordinating resolution with various IT groups
- Troubleshoot and resolve hardware/software failures as well as security breaches, threats, and availability issues

- Regularly provide proactive support including security configurations, security policy modification recommendation and diagnostics of remote network security issues

- SME on Vulnerability Management/analysis using enterprise vulnerability scanners. Create, run, analysis and remediate vulnerabilities found on Davidson infrastructure based on critically of vulnerability

- Ensure Davidson is implanting best practice security policies that address business needs while protecting corporate assets

- Whitelisting Host/URL'S in enterprise proxy. Trace I.P addresses using proxy to analyse traffic

- Tools and Programs used: Enterprise proxy, Splunk, Enterprise Vulnerability Scanners, Enterprise SIEM, Ivanti Ticketing system, Project tracking via Jira, Phantom, 0365 – Security and Compliance, SolarWinds, SailPoint, Polarity

STATE OF MONTANA, DEPARTMENT OF ADMINISTRATION SITSD/NTSB, Helena, MT **IT**
System Administrator, *07/01/2017 – 04/09/2021 (Full Time – 40hrs a week)*

- Implement customer service to non-technical clients, management, and stakeholders

- Manage 10-20 daily support tickets through Service Now, responding to Tier 1, 2, 3 and escalating tickets when necessary

- Partner with State of Montana NOC and SOC to troubleshoot network issues, oversee installation of applications and software for state employees, and ensure proper authentication of state network devices using Active Directory

- Leverage Python, C#, Java, and CLI interface with Cisco and Juniper network devices to assist with programming switches, routers, and scripts

- Configure and install voice software, hardware, and network equipment, using AVAYA Manager for voice configurations and Putty/SSH for media gateways, switches, routers, and audio codes

- Partner with CenturyLink now Lumen to implement, troubleshoot and add or disconnect telecommunication services

- Achieved Governor's and Department of Administration's Awards for Excellence in Performance for implementation of state-wide VoIP infrastructure

- Help update and configure Voice Ops servers to work with Carbon Black

- Implement project management skills when deploying and working with State of Montana stake holders to implement Avaya VoIP phones

COMPUSOURCE, INC., Bozeman, MT
Information Technology Specialist, *05/21/2014 – 04/13/2016 (Full Time – 40hrs a week)*

- Managed team of 2-5 employees, including training and project management
- Ensured industry standards and compliance of cabling layouts by utilizing blueprints, spliced fiber optic cable, installed cameras and security systems, and tested cables using Fluke
- Installed Cisco switches into Panduit data racks and patched in Computers, IP Phones, Printers, and Fax Machines, troubleshooting all devices when necessary for hospital staffing 500+
- Designed rack and row layouts to optimize air circulation and functionality, and built out data centers by leveraging proper equipment to pull in fiber and copper cable and ensured achievement of product warranties and standards

STATE OF MONTANA, Helena, MT
Web Developer, *07/01/2013 – 05/01/2014 (Part Time – 30hrs a week)*

- Created, designed, and updated Department of Justice web pages by leveraging Dreamweaver and WordPress CMS to edit HTML/PHP and build and manage site
- Collaborated and effectively communicated with state employees to ensure satisfaction and executed administrative office duties
- Partnered with Lead Web Developer and Department of Justice Security team to ensure safety requirements of website, including multi-factor authentication, Web Application firewalls, proper port usage, and more
- Assisted Lead Web Developer with patching and renewing software and certificates needed for WordPress and server

PROFESSIONAL ORGANIZATIONS

(ISC)2 – International Information Systems Security Certification Consortium, Member **COMMUNITY**

INVOLVEMENT

Vapor Detailing, Owner, Helena Summer Jobs Program Coordinator, & Charity Partner (2016- Present) **AWARDS**

Governor's Award for Excellence in Performance 2018, State of Montana
Governor's Award for Excellence in Performance 2020, State of Montana
Department of Administration Award for Excellence in Performance 2018, State of Montana

Splunk Security Portfolio

Dashboards, SOAR Automation, and Enterprise Deployment

Prepared by Tevin

September 18, 2025

Executive Summary

Hands-on Splunk engineer focused on practical, auditor-friendly security analytics across SIEM dashboards (AU-2), on-prem Splunk SOAR 6.4.x, and Splunk Enterprise deployments.

Skills Matrix

Area	Technologies / Skills	Proficiency	Highlights
Splunk Platform	Splunk Enterprise 9.x–10.x; SH/IDX/CM/HF/UF	Expert	Air-gapped builds; role-based access
Splunk SOAR	SOAR 6.4.x; Apps; Assets; Playbooks	Advanced	On-prem deployment; vault usage
SPL & Dashboards	SPL; Dashboard Studio; tokens; drilldowns	Expert	AU-2 views; exec summaries
Security Analytics	NIST 800-53; MITRE ATT&CK	Advanced	Auditor-friendly searches
Data Onboarding	CIM; TAs; props/transforms; WinEventLog; auditd	Advanced	Normalization & hygiene
Automation	Python; PowerShell; Bash	Advanced	Automation scripts & APIs

SIEM Dashboard Portfolio

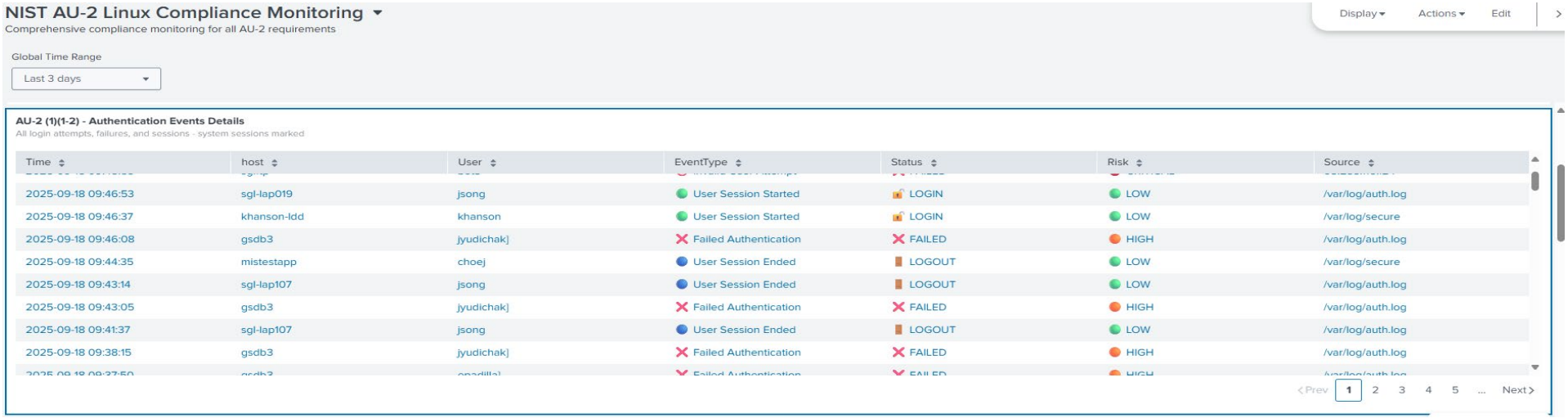
NIST AU-2 Linux and Windows Compliance Monitoring Dashboard's

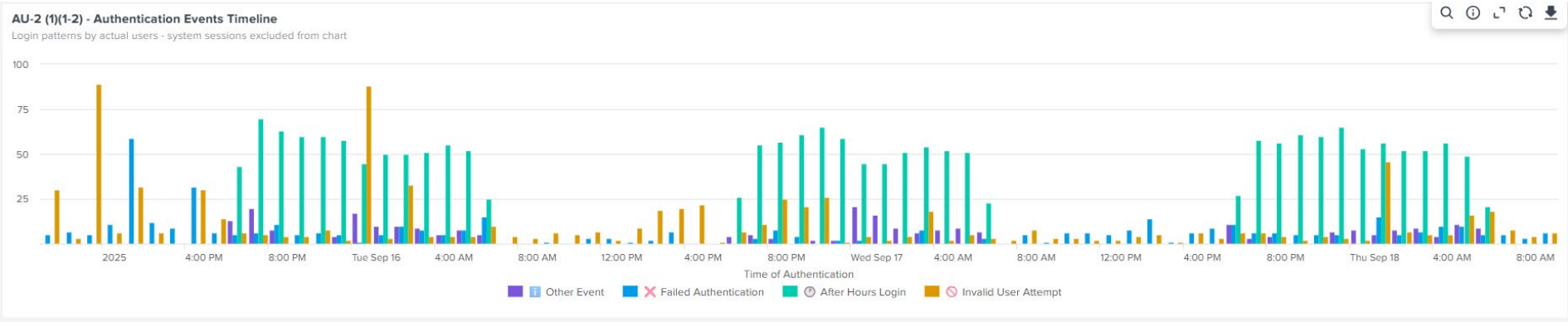
Splunk - Security Information & Event Management (SIEM) Dashboard Portfolio

Linux

NIST AU-2 Authentication Events Details Summary:

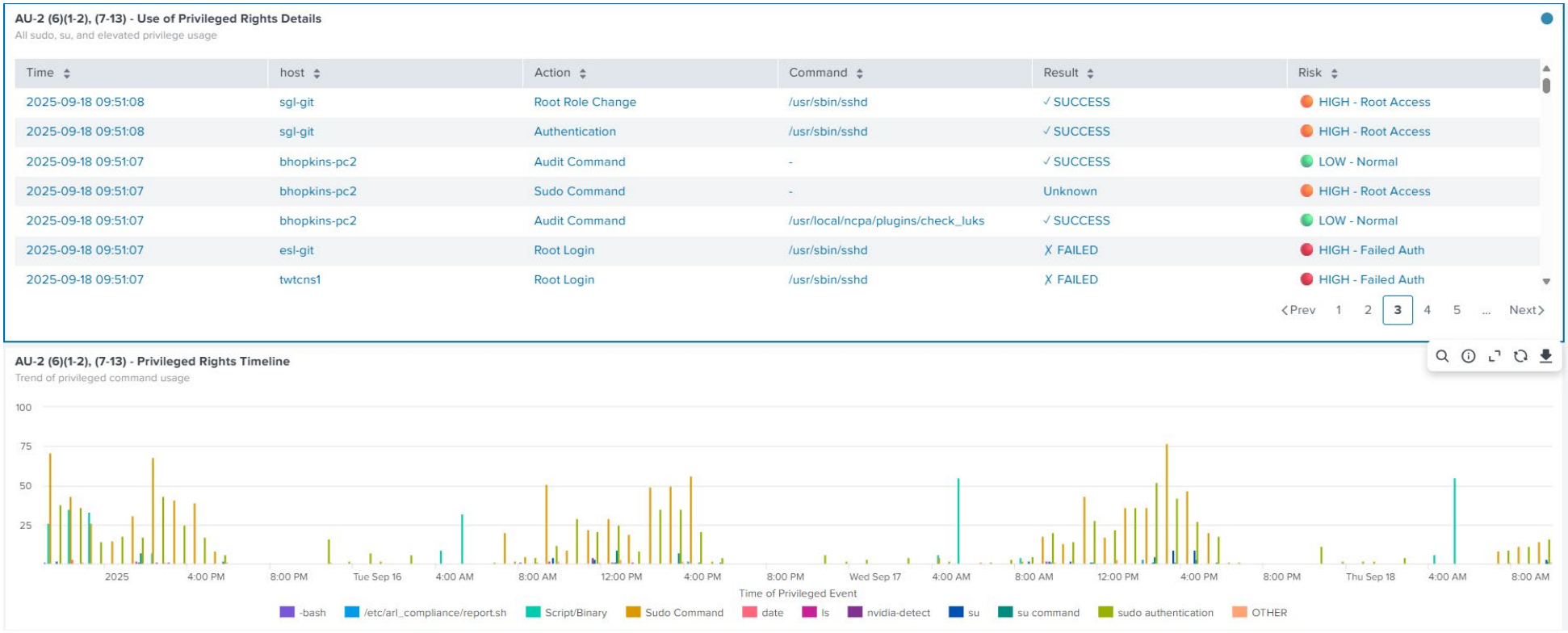
This detailed view displays authentication events from the last 3 days, showing login attempts, failures, and sessions across the system. The log captures various security events including successful user sessions (marked as LOGIN/LOGOUT), failed authentication attempts (marked as FAILED), and their associated risk levels (LOW/HIGH). Each entry provides timestamp, host system, username, event type, status, risk assessment, and source information, enabling granular tracking of user authentication activities and potential security incidents for compliance monitoring.





AU-2 Privileged Rights Usage Details Summary:

This report tracks sudo, su, and elevated privilege usage across systems. The detailed log shows privileged actions including root role changes, authentication attempts, audit commands, and sudo command executions on various hosts. Each entry displays timestamp, host, action type, command executed, result (SUCCESS/FAILED), and risk level (HIGH for root access/failed auth, LOW for normal operations). The timeline graph below visualizes the trend of privileged command usage over time, categorizing events by type (sudo commands, scripts, authentication, etc.) to identify patterns and potential security concerns.



AU-2 User and Group Management Events Summary:

This report monitors user account and group management activities across the system. The log shows user modification events tracking changes to administrative accounts with risk levels ranging from MEDIUM to HIGH. All entries indicate "Admin access modified" in the details, suggesting privilege-level changes. The timeline graph below visualizes the frequency and distribution of user management activities (User Modified, User Deleted, Group Created, User Created, Password Changed) over time, helping identify patterns in account administration and potential unauthorized changes to user privileges.

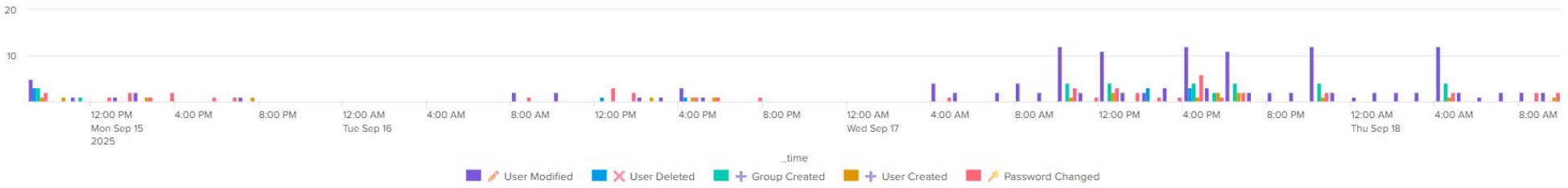
AU-2 (5)(1-2) - User and Group Management Events

Time	host	Action	Target	Risk	Details
2025-09-18 09:05:51	titan2	User Modified	admmike	HIGH	Admin access modified
2025-09-18 09:05:51	titan2	User Modified	desimone	MEDIUM	
2025-09-18 08:05:52	titan2	User Modified	admmike	HIGH	Admin access modified
2025-09-18 08:05:52	titan2	User Modified	desimone	MEDIUM	
2025-09-18 07:05:53	titan2	User Modified	admmike	HIGH	Admin access modified

< Prev 1 2 3 Next >

AU-2 (5)(1-2) - User Management Timeline

User/Group Creation, Modification, and Deletion Events"



AU-2 Security Relevant File and Object Activity Summary:

This report monitors access to critical system files, with all access shown having system flag enabled. The log tracks activities including audit log monitoring events for log collection systems and file activity monitoring for other system files. All recorded actions are performed by root user, with most events marked as automated system processes. Risk levels are classified as LOW for both log collection and other file activities. The timeline graph below visualizes file access patterns and actions performed (accessed, deleted, security events, cron jobs, etc.) to identify potential unauthorized access or unusual file system behavior across the monitoring period.

AU-2 (2)(1-6), (3-4) - Security Relevant File and Object Activity

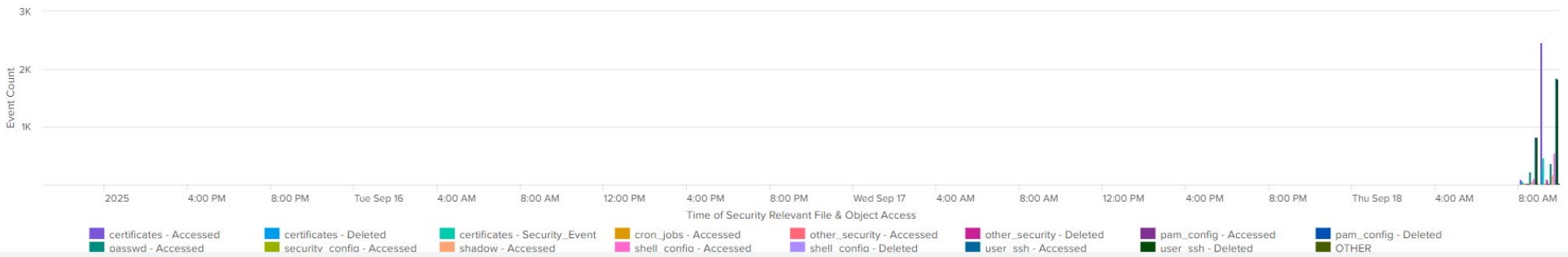
Monitor access to critical system files - all access shown with system flag

Time	Host	File Name	Full Path	What Happened	Risk Level	User	System/Automated
2025-09-18 09:51:30	ndlbwrk4	audit.log	/var/log/audit/audit.log	Audit Log Monitoring (mode: 100600)	LOW - Log Collection System	root	Yes
2025-09-18 09:51:30	ndlbkrb1	audit.log	/var/log/audit/audit.log	Audit Log Monitoring (mode: 100600)	LOW - Log Collection System	root	Yes
2025-09-18 09:51:30	sgl-lap002	wtmp	/var/log/wtmp	File Activity (mode: 100664)	LOW - Other File	root	No
2025-09-18 09:51:30	ndlbkik1	audit.log	/var/log/audit/audit.log	Audit Log Monitoring (mode: 100600)	LOW - Log Collection System	root	Yes

Prev 1 2 3 4 5 ... Next

AU-2 (2)(1-6), (3-4) - File Activity Timeline

Shows which files were accessed and what actions were performed

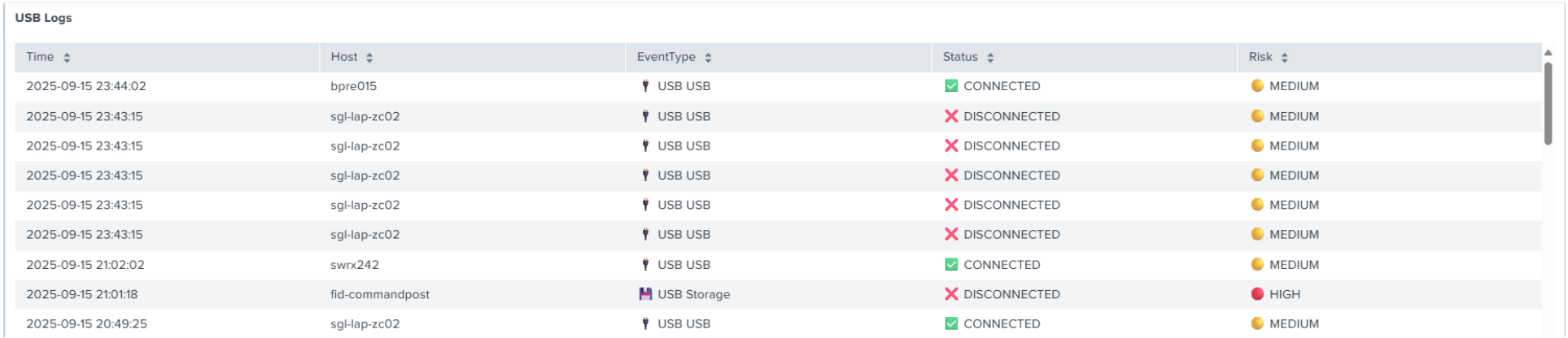


Print Logs Summary:
This report tracks print job activities across network printers. The log shows successfully completed print jobs from various hosts, with all events marked as PRINTED status and MEDIUM risk level. Print jobs are distributed across different printers in the organization, with file sizes ranging from small documents (34.3 KB) to larger files (4935.4 KB). The total pages printed vary from single pages to multi-page documents (up to 16 pages). All print activities are monitored to ensure compliance with document handling policies and to detect potential data exfiltration attempts through physical printing.

Print Logs

Time	Host	EventType	Status	Risk	Printer	TotalPages	Size_KB
2025-09-18 09:55:51	bpre034	Print Job	PRINTED	MEDIUM	SGL_BW_Mailroom	16	4935.4
2025-09-18 09:08:15	pre039	Print Job	PRINTED	MEDIUM	SGL_Color_Penrod3rd	1	34.3
2025-09-18 08:43:45	bpre037	Print Job	PRINTED	MEDIUM	SGL_Color_T500	1	83.3
2025-09-18 08:43:24	bpre037	Print Job	PRINTED	MEDIUM	SGL_Color_T500	4	433.5
2025-09-18 08:27:30	pre055	Print Job	PRINTED	MEDIUM	SGL_BW_Mailroom	1	63.1
2025-09-18 08:23:23	bpre037	Print Job	PRINTED	MEDIUM	SGL_BW_Mailroom	1	83.1
2025-09-18 08:23:14	bpre037	Print Job	PRINTED	MEDIUM	SGL_BW_Mailroom	4	433.3
2025-09-18 08:16:36	bpre037	Print Job	PRINTED	MEDIUM	SGL_Color_Mailroom	4	433.2
2025-09-18 08:16:26	pre055	Print Job	PRINTED	MEDIUM	SGL_BW_Mailroom	1	93.0
2025-09-18 08:16:25	bpre037	Print Job	PRINTED	MEDIUM	SGL_Color_Mailroom	1	83.2
2025-09-18 08:14:43	pre055	Print Job	PRINTED	MEDIUM	SGL_BW_Mailroom	3	288.4

USB Logs Summary:
This report monitors USB device connections and disconnections across the network. The log tracks both standard USB devices and USB storage devices, with events showing CONNECTED and DISCONNECTED statuses. Most USB activities are classified as MEDIUM risk, with USB storage disconnection events marked as HIGH risk due to potential data exfiltration concerns. Multiple disconnection events from the same host suggest repeated USB device removal or potential security policy violations. The monitoring helps detect unauthorized USB usage and potential data transfer attempts through removable media.



USB Logs

Time	Host	EventType	Status	Risk
2025-09-15 23:44:02	bpre015	USB USB	CONNECTED	MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	USB USB	DISCONNECTED	MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	USB USB	DISCONNECTED	MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	USB USB	DISCONNECTED	MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	USB USB	DISCONNECTED	MEDIUM
2025-09-15 23:43:15	sgl-lap-zc02	USB USB	DISCONNECTED	MEDIUM
2025-09-15 21:02:02	swrx242	USB USB	CONNECTED	MEDIUM
2025-09-15 21:01:18	fid-commandpost	USB Storage	DISCONNECTED	HIGH
2025-09-15 20:49:25	sgl-lap-zc02	USB USB	CONNECTED	MEDIUM

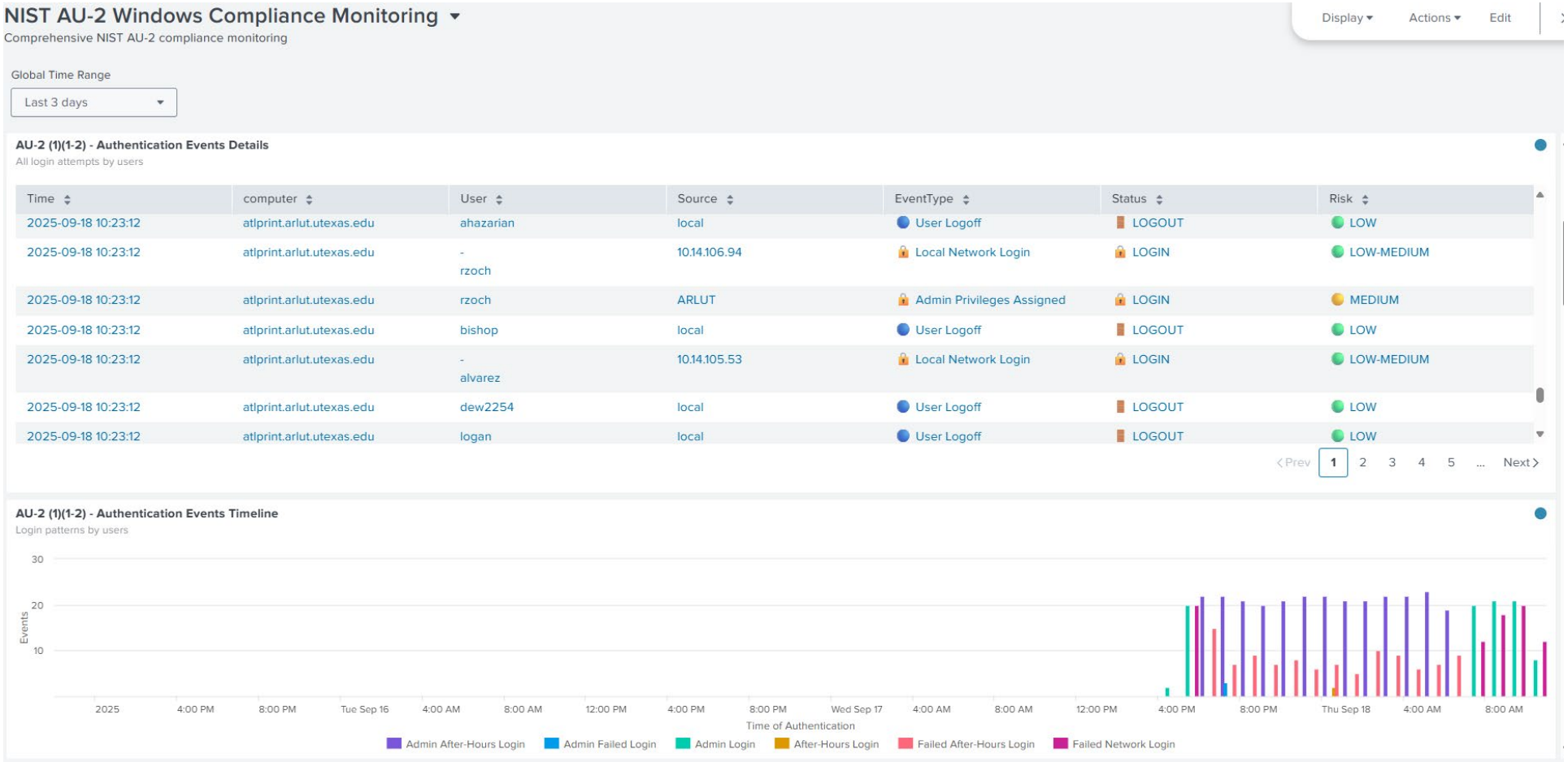
USB/CD/Burn Activity Summary:

This report monitors removable media and optical disc activities across the network. The log tracks multiple event types including unknown audio devices (USB headsets), CD/DVD burning operations, and CD/DVD device detections. All events are system-initiated with varied risk levels - HIGH risk for unknown audio devices and active CD/DVD burning operations (potential data exfiltration), and MEDIUM risk for standard CD/DVD device detection. Notable activities include mounted CD/DVD burning sessions with specific file references and multiple audio device connections via USB. The monitoring helps identify unauthorized media usage and potential data transfer attempts through optical media or unauthorized peripheral connections

USB/CD/Burn Activity

Time	Host	User	EventType	Status	Risk	DeviceDetails
2025-09-17 13:59:37	sgl-lap053	[System]	AUDIO DEVICE	DETECTED	HIGH - UNKNOWN AUDIO	Audio Device ()
2025-09-17 13:59:37	sgl-lap053	[System]	AUDIO DEVICE	DETECTED	HIGH - UNKNOWN AUDIO	Audio Device (Logi USB Headset)
2025-09-17 11:02:56	pre038	[System]	CD/DVD BURNING	DETECTED	HIGH - CD/DVD BURNING	brasero
2025-09-17 11:02:56	pre038	[System]	CD/DVD BURNING	DETECTED	HIGH - CD/DVD BURNING	brasero
2025-09-17 11:02:52	pre038	[System]	CD/DVD BURNING	DETECTED	HIGH - CD/DVD BURNING	brasero
2025-09-17 10:30:43	pre024	[System]	AUDIO DEVICE	DETECTED	HIGH - UNKNOWN AUDIO	Audio Device ()
2025-09-17 10:30:43	pre024	[System]	AUDIO DEVICE	CONNECTED	HIGH - UNKNOWN AUDIO	Audio Device ()
2025-09-17 10:30:43	pre024	[System]	AUDIO DEVICE	DETECTED	HIGH - UNKNOWN AUDIO	Audio Device (Logitech USB Headset)
2025-09-17 09:53:46	filo-pc	filo	CD/DVD BURNING	MOUNTED	HIGH - CD/DVD BURNING	User: filo, Disc: K3b (UID: 14015)
2025-09-17 08:30:28	filo-pc	[System]	CD/DVD DEVICE	DETECTED	MEDIUM - CD/DVD ACTIVITY	CD/DVD Activity
2025-09-17 07:40:06	pre038	[System]	CD/DVD BURNING	DETECTED	HIGH - CD/DVD BURNING	brasero

Windows


NIST AU-2 Windows Compliance Monitoring
Comprehensive NIST AU-2 compliance monitoring
Display
Actions
Edit
Global Time Range
Last 3 days
AU-2 (1)(1-2) - Authentication Events Details
All login attempts by users
Time
computer
User
Source
EventType
Status
Risk
2025-09-18 10:23:12 atlprint.arlut.utexas.edu ahazarian local User Logoff LOGOUT LOW
2025-09-18 10:23:12 atlprint.arlut.utexas.edu - rzoch 10.14.106.94 Local Network Login LOGIN LOW-MEDIUM
2025-09-18 10:23:12 atlprint.arlut.utexas.edu rzoch ARLUT Admin Privileges Assigned LOGIN MEDIUM
2025-09-18 10:23:12 atlprint.arlut.utexas.edu bishop local User Logoff LOGOUT LOW
2025-09-18 10:23:12 atlprint.arlut.utexas.edu - alvarez 10.14.105.53 Local Network Login LOGIN LOW-MEDIUM
2025-09-18 10:23:12 atlprint.arlut.utexas.edu dew2254 local User Logoff LOGOUT LOW
2025-09-18 10:23:12 atlprint.arlut.utexas.edu logan local User Logoff LOGOUT LOW
Prev
1
2
3
4
5
...
Next
AU-2 (1)(1-2) - Authentication Events Timeline
Login patterns by users
30
20
10
Events
2025
4:00 PM
8:00 PM
Tue Sep 16
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
Wed Sep 17
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
Thu Sep 18
4:00 AM
8:00 AM
Time of Authentication
Admin After-Hours Login
Admin Failed Login
Admin Login
After-Hours Login
Failed After-Hours Login
Failed Network Login

AU-2 (6)(1-2), (7-13) - Use of Privileged Rights Details

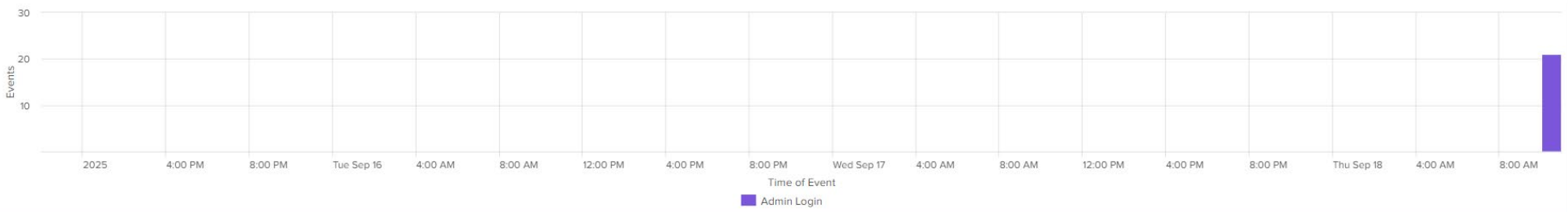
User privileged actions

Time	computer	Action	User	What Happened	Risk
2025-09-18 10:20:31	gtorres-wl.arlut.utexas.edu	Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:20:23	prod-wd.arlut.utexas.edu	Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:20:06	mcleod-wl2.arlut.utexas.edu	Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:19:59	gtorres-wl.arlut.utexas.edu	Ownership Privilege Used	sndsc-prod	Ownership privilege - can take control of any object	CRITICAL
2025-09-18 10:19:57	SPTEST.arlut.utexas.edu	Admin Login	- sptestadmin	Admin account logged in	HIGH

Prev 1 2 3 4 5 Next

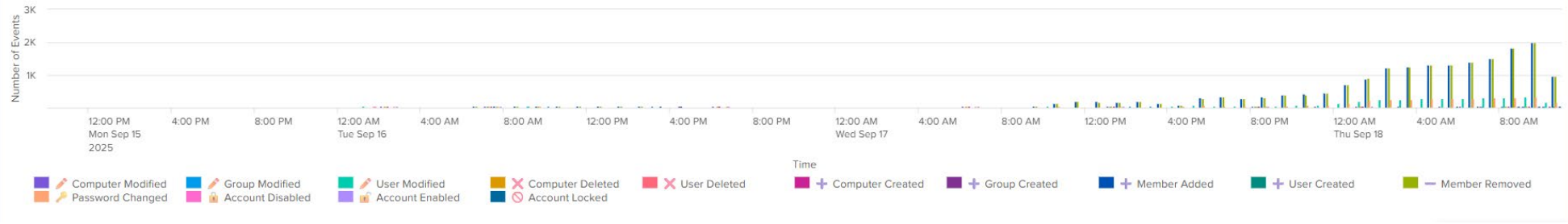
AU-2 (6)(1-2), (7-13) - Privileged Rights Timeline

User privileged actions



AU-2 (5)(1-2) - User Management Timeline

Trend of user management activities



AU-2 (2)(1-6), (3-4) - Security File and Object Activity

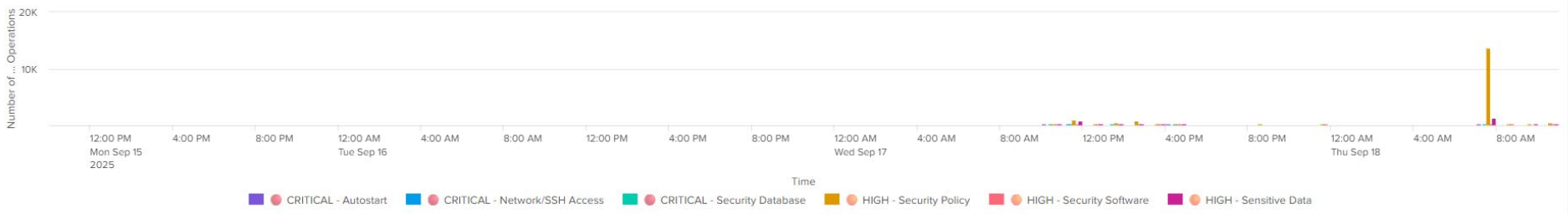
Security file access by users

Time	Computer	User	File Name	What Happened	Risk Level	Process
2025-09-18 10:23:05	sccmits.arlut.utexas.edu	SQLServerReportingServices	rsreportserver.config	File Read	MEDIUM - Configuration	I:\Program Files\Microsoft SQL Server Reporting Services\SSRS\RSHostingService\RSHostingService.exe
2025-09-18 10:23:05	sccmits.arlut.utexas.edu	SQLServerReportingServices	config.json	File Read	MEDIUM - Configuration	I:\Program Files\Microsoft SQL Server Reporting Services\SSRS\RSHostingService\RSHostingService.exe
2025-09-18 10:23:05	sccmits.arlut.utexas.edu	SQLServerReportingServi	Microsoft.BIServer.Management.WebApi.dll	File Read	MEDIUM - Executable	I:\Program Files\Microsoft

< Prev 1 2 3 4 5 Next >

AU-2 (2)(1-6), (3-4) - Security File Activity Timeline

Security file access by users



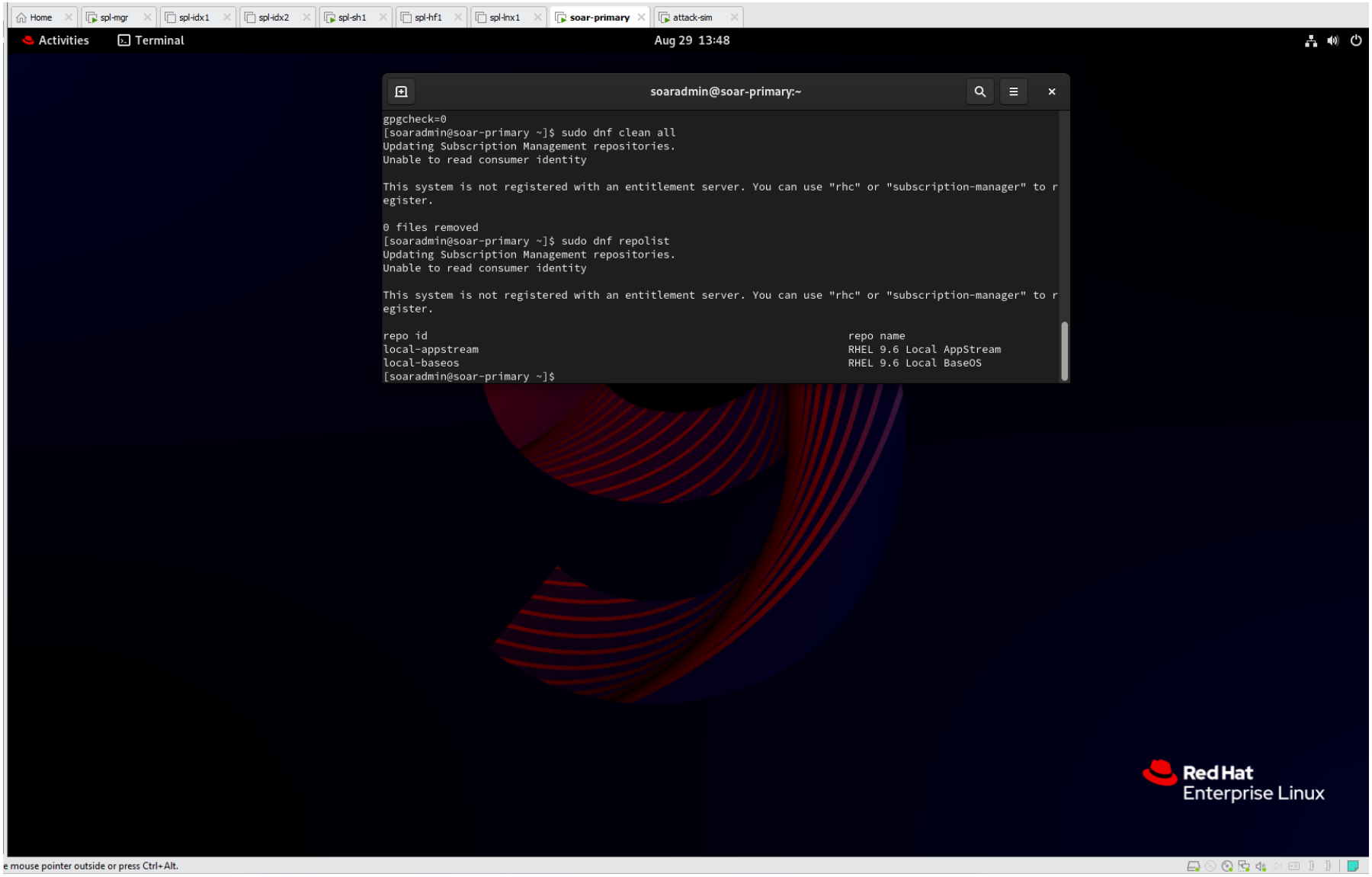
USB/CD/BURN

Time	Host	User	EventType	Status	Risk	DeviceDetails	FileDirection	FileName
2025-09-18 10:22:19	cliffhanger.arlut.utexas.edu	dclifton	FILE TRANSFER	BULK TRANSFER (5 files)	HIGH - FILE TRANSFER	File: 8748459.SLDDRW	FROM REMOVABLE (Bulk 5 files)	8748370.SLDDRW, 8748378.SLDDRW, 8748417.SLDDRW, 8748418.SLDDRW, 8748459.SLDDRW
2025-09-18 10:11:38	atl-docs-wv.arlut.utexas.edu	cperez	FILE TRANSFER	BULK TRANSFER (3 files)	HIGH - FILE TRANSFER	File: WAS 2025-SEPTEMBER.xls	FROM REMOVABLE (Bulk 3 files)	WAS 2025-SEPTEMBER.xls, control-flow-ex-2.png, control-flow-ex.png
2025-09-18 10:10:40	atl-docs-wv.arlut.utexas.edu	cperez	FILE TRANSFER	BULK TRANSFER (3 files)	HIGH - FILE TRANSFER	File: WAS 2025-SEPTEMBER.xls	FROM REMOVABLE (Bulk 3 files)	WAS 2025-SEPTEMBER.xls, control-flow-ex-2.png, control-flow-ex.png
2025-09-18 10:08:31	aspd-wind-wv.arlut.utexas.edu	sndsc-prod	FILE TRANSFER	FILE ACCESSED	HIGH - FILE TRANSFER	File: bin	FROM REMOVABLE (Inbound)	bin

Created by Tevin Agtarap on 9/18/2025

Splunk SOAR Deployment and Demonstration

Install REHL Linux 9.6 (Compatible with Splunk Soar) – soar-primary VM



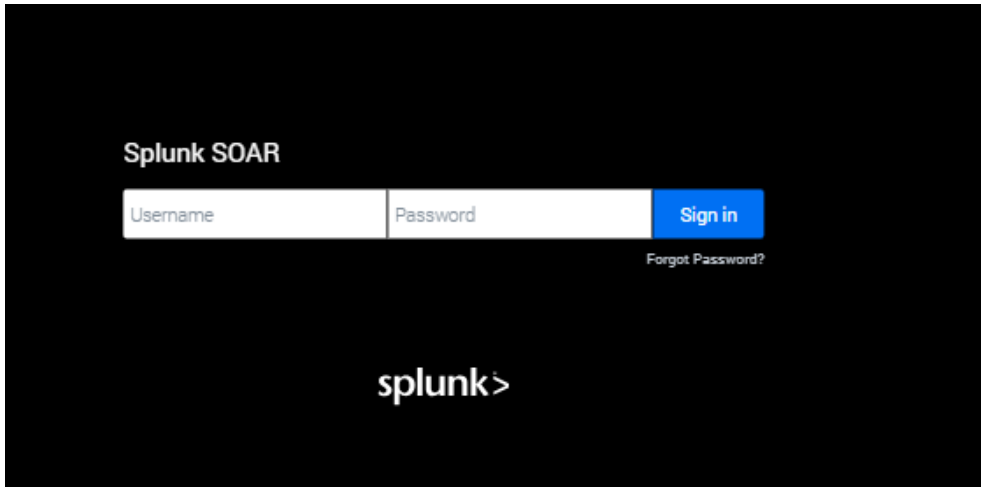
Install Splunk SOAR

```
C:\windows\System32\OpenSSH\scp.exe: stat local "splunk-soar-6.3.0.718-4c6c4889-el8-x86_64.tgz": No such file or directory
PS C:\Users\agtarap\Documents\SplunkLabFiles> scp splunk_soar-unpriv-6.4.1.361-bea76553-el8-x86_64.tgz soaradmin@192.168.221.60:/tmp/
>>
soaradmin@192.168.221.60's password:
splunk_soar-unpriv-6.4.1.361-bea76553-el8-x86_64.tgz                                    33%  546MB 102.3MB/s   00:10 ETA
```

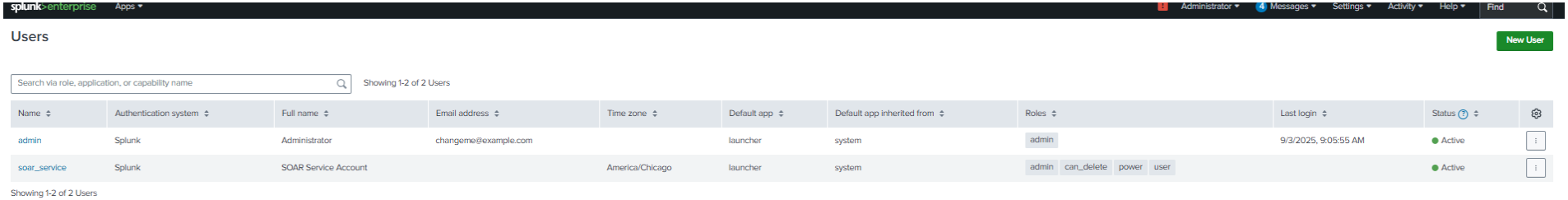
```
[soaradmin@soar-primary ~]$ ls -la /tmp/*.tgz
-rw-rw-r--. 1 soaradmin soaradmin 1698174673 Aug 28 07:51 /tmp/splunk_soar-unpriv-6.4.1.361-bea76553-el8-x86_64.tgz
[soaradmin@soar-primary ~]$
```

Install Splunk Soar on soar-primary VM

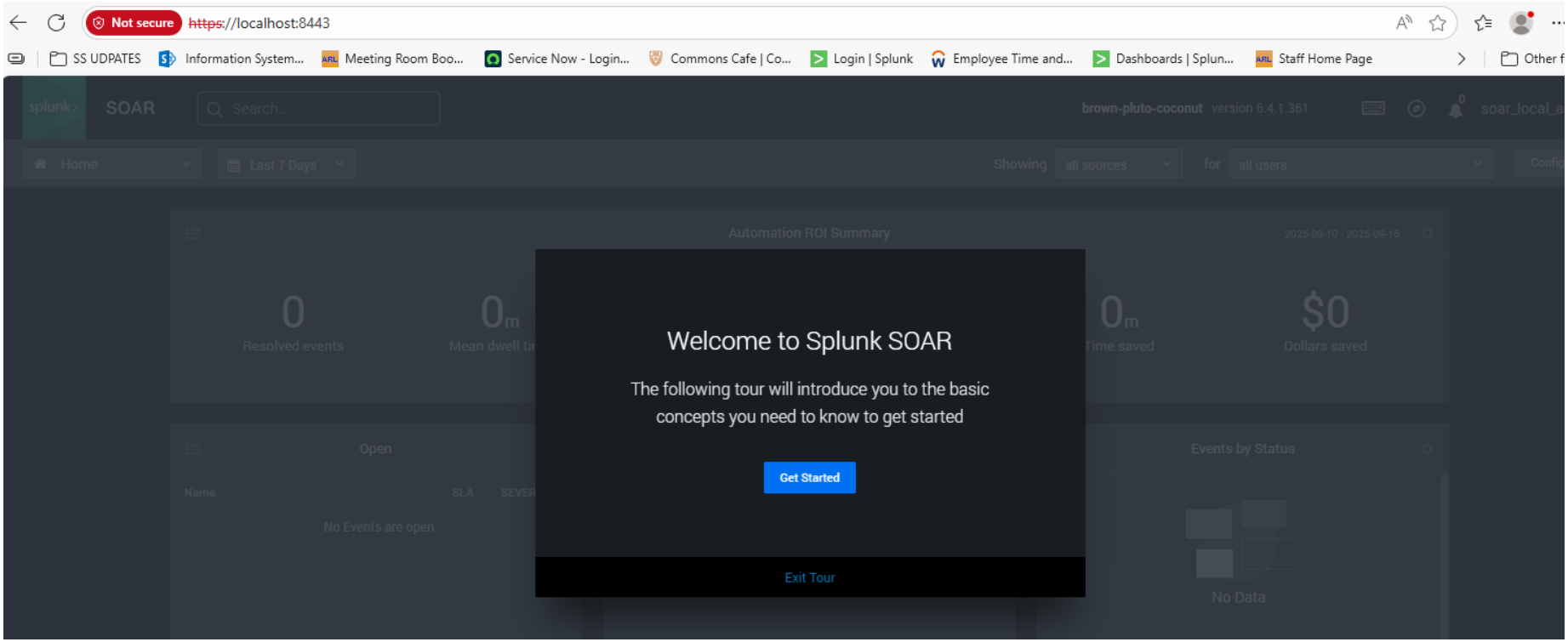
```
[soaradmin@soar-primary ~]$ sudo -u phantom /opt/phantom/bin/start_phantom.sh
Starting all Splunk SOAR services
Starting Connection pooler (PgBouncer):                    [  OK  ]
Checking database connectivity:                            [  OK  ]
Checking external database version:                        [  OK  ]
Checking component versions:                               [  OK  ]
Starting Supervisord:                                      [  OK  ]
Starting Splunk SOAR daemons:                              [  OK  ]
Checking Supervisord processes:                            [  OK  ]
Starting Web application server (uwsgi):                   [  OK  ]
Starting Web server (nginx):                               [  OK  ]
Starting Embedded Universal Forwarder:                     [  OK  ]
Starting Watchdog daemon:                                  [  OK  ]
Splunk SOAR startup successful
```



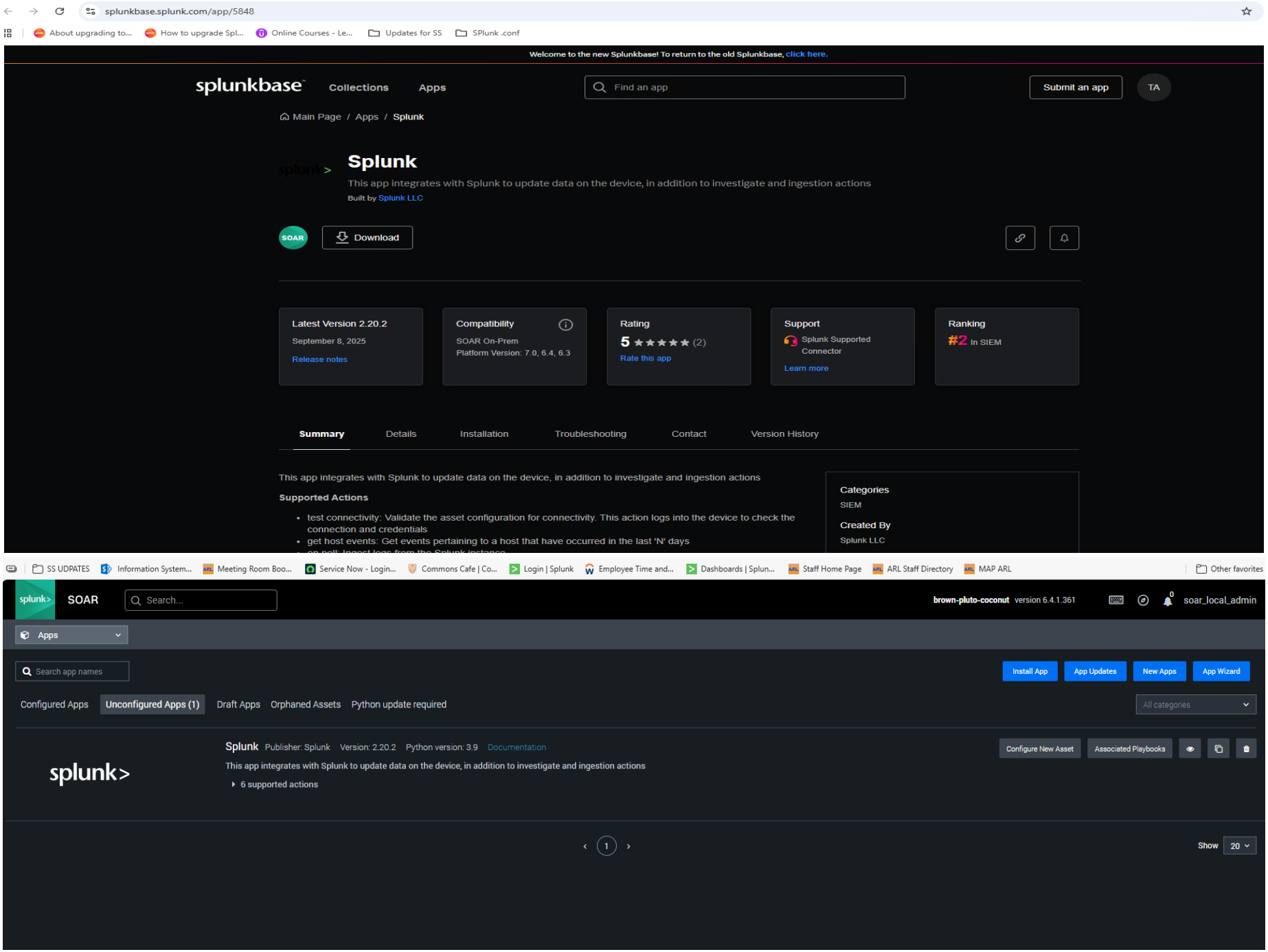
Create soare_service account in Splunk



Finishing configuring Splunk SOAR

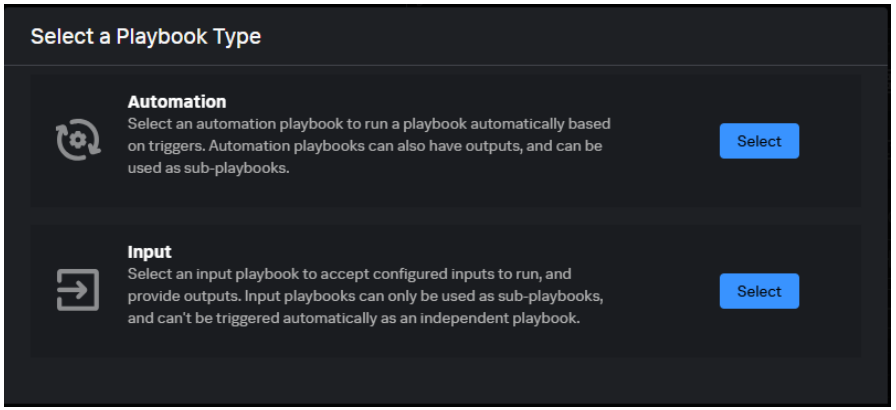


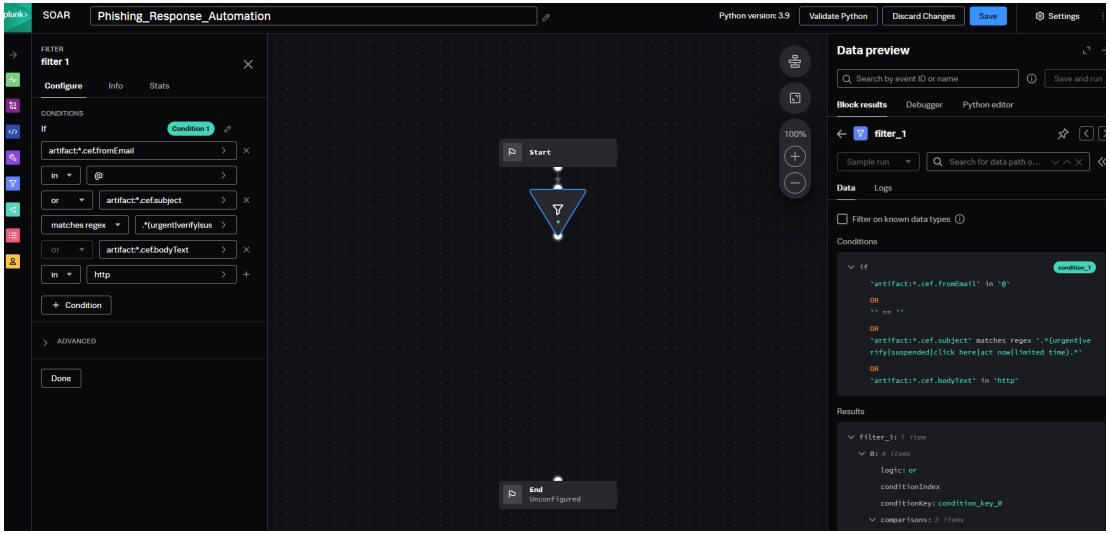
Install Connector



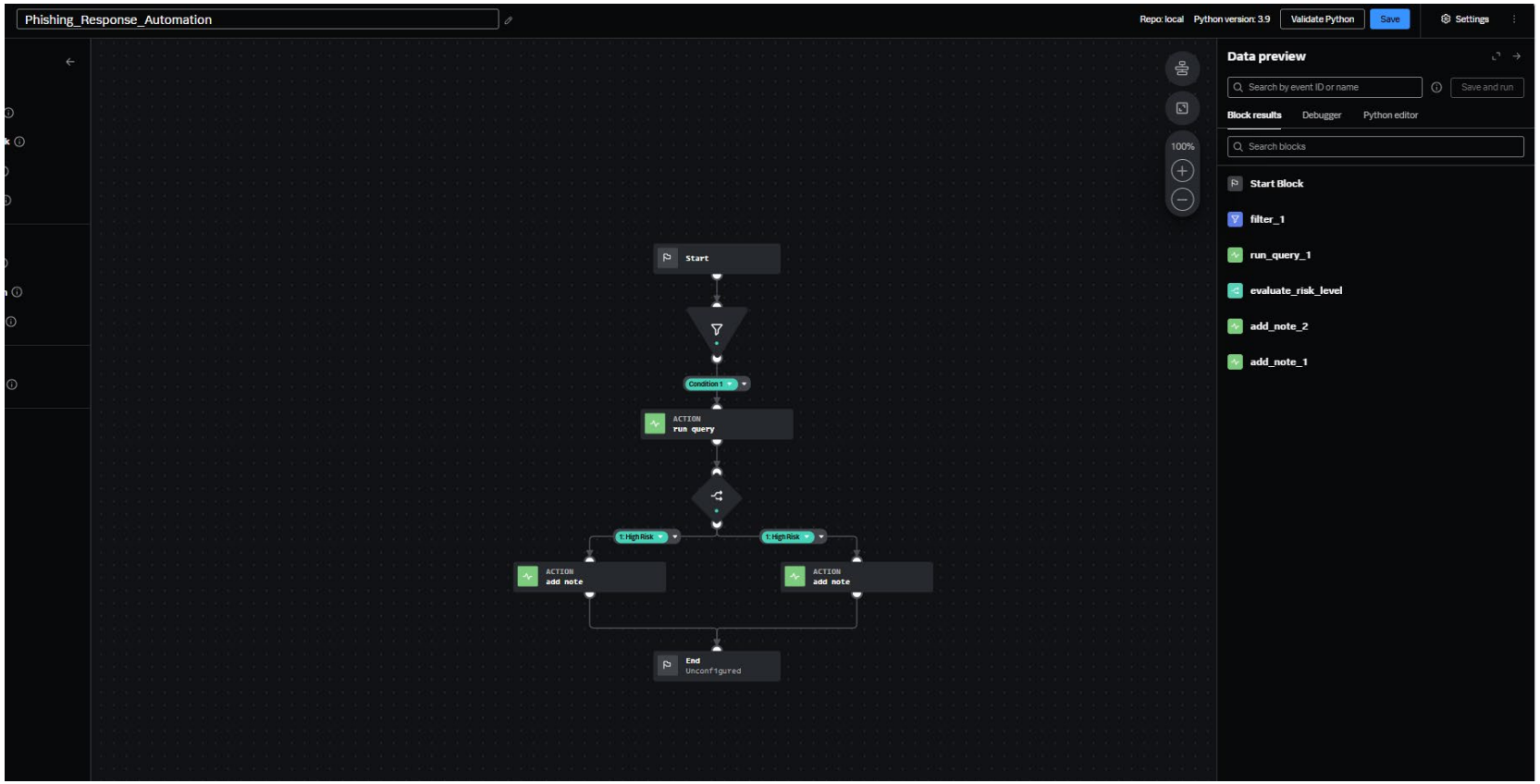
Testing Connectivity to Splunk Enterprise

Creating SOAR Playbooks!

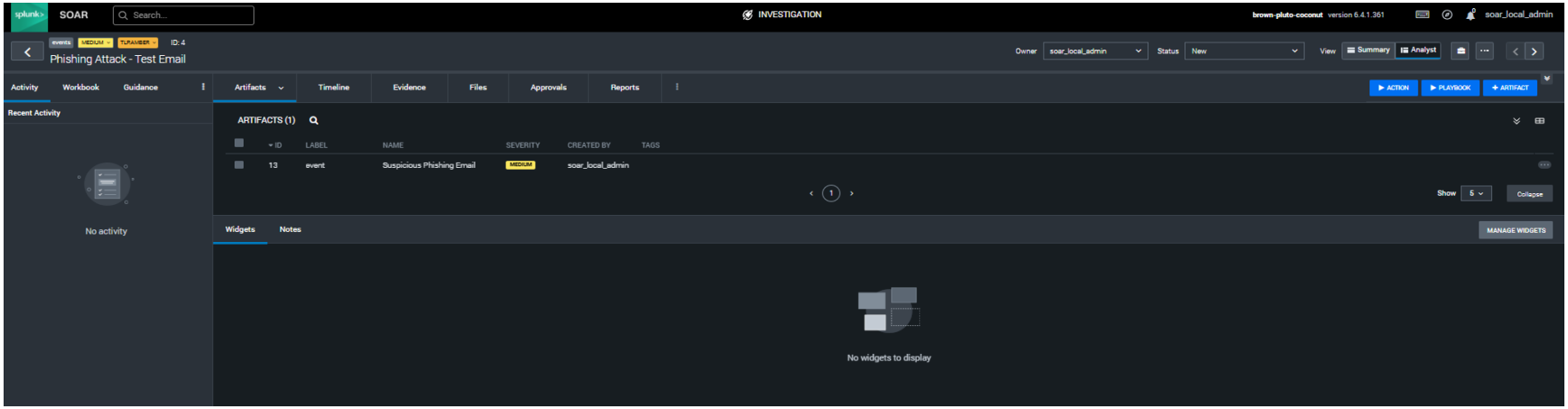




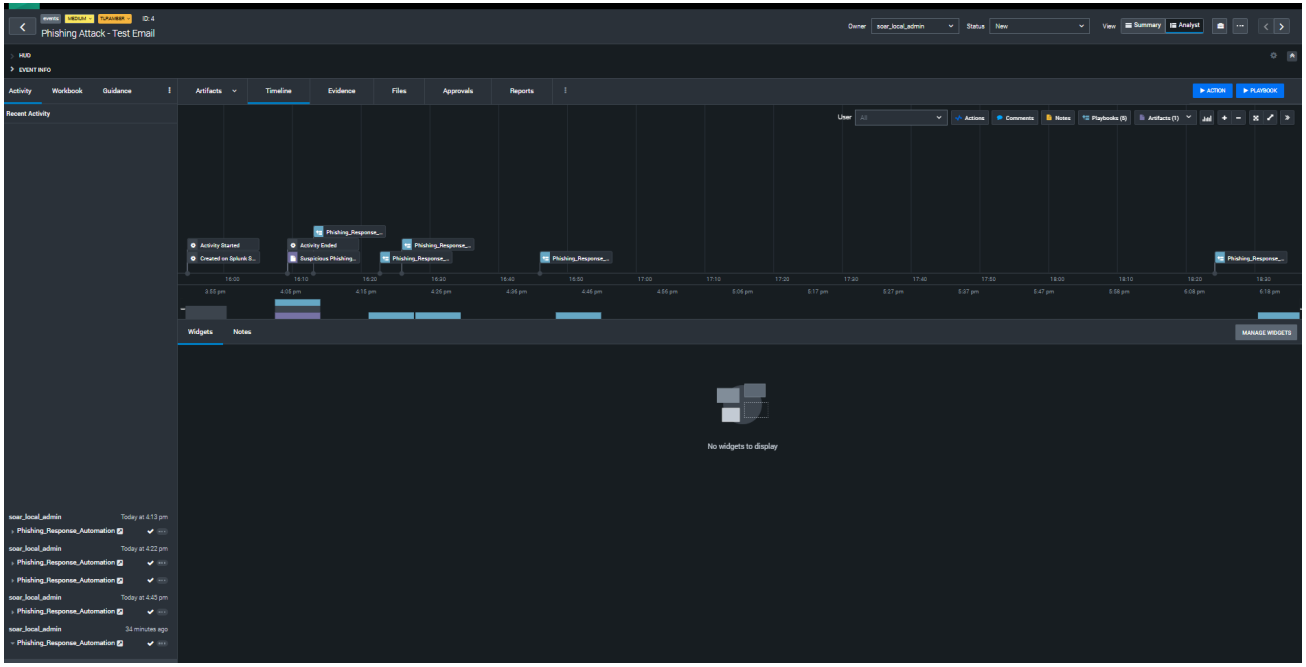
Full playbook built out



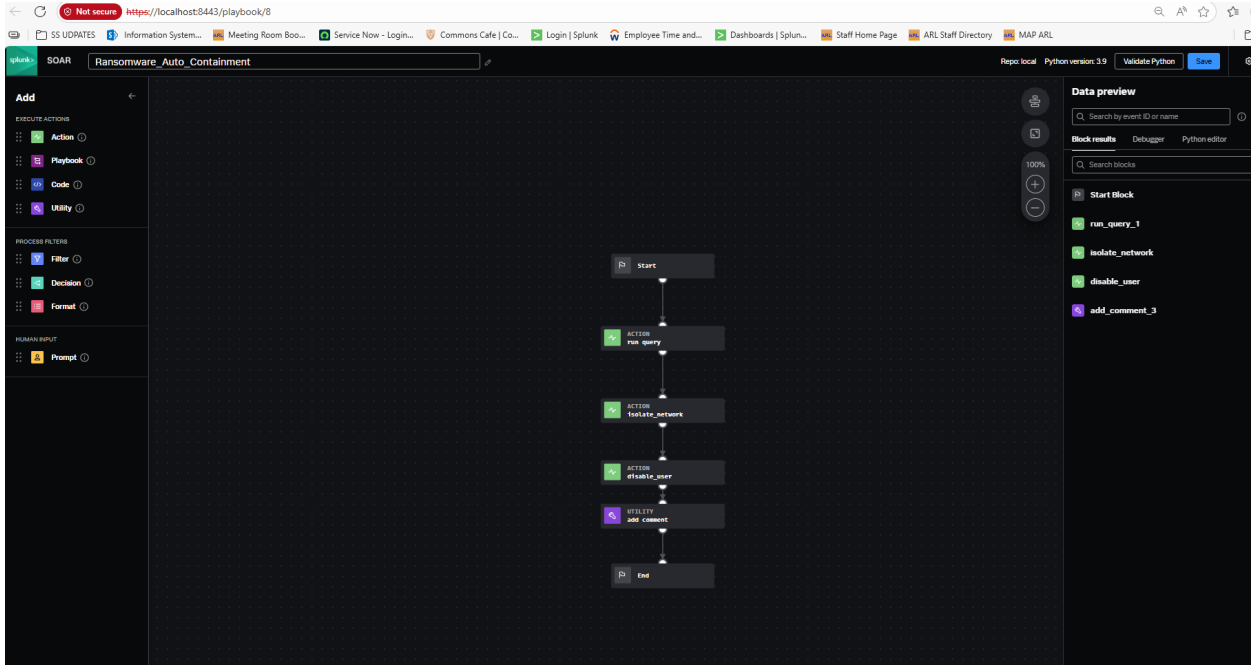
Build out simulated phishing email to test SOAR playbook



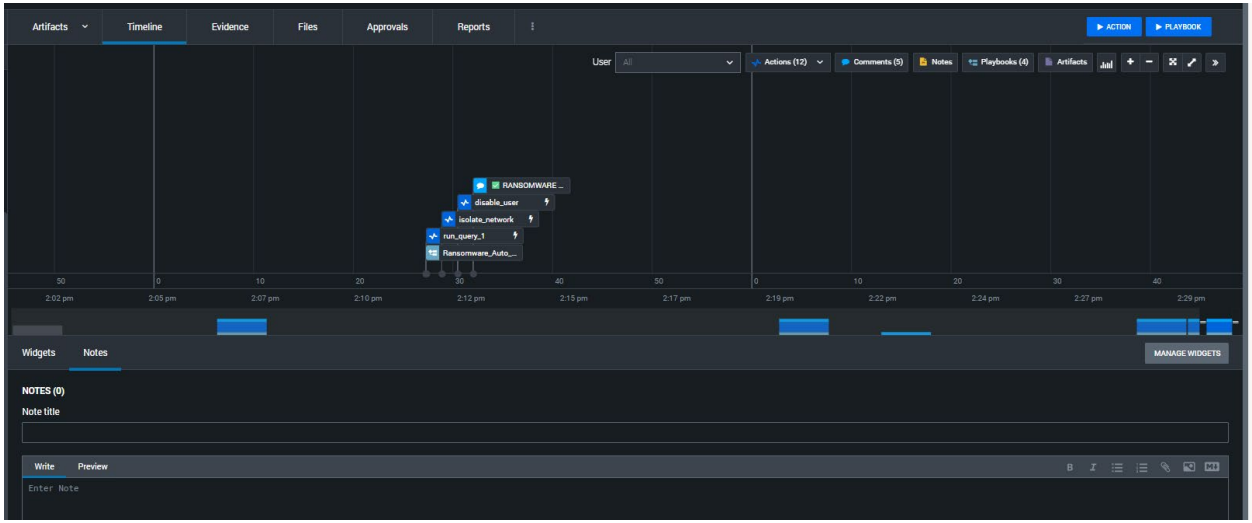
Playbook ran successfully

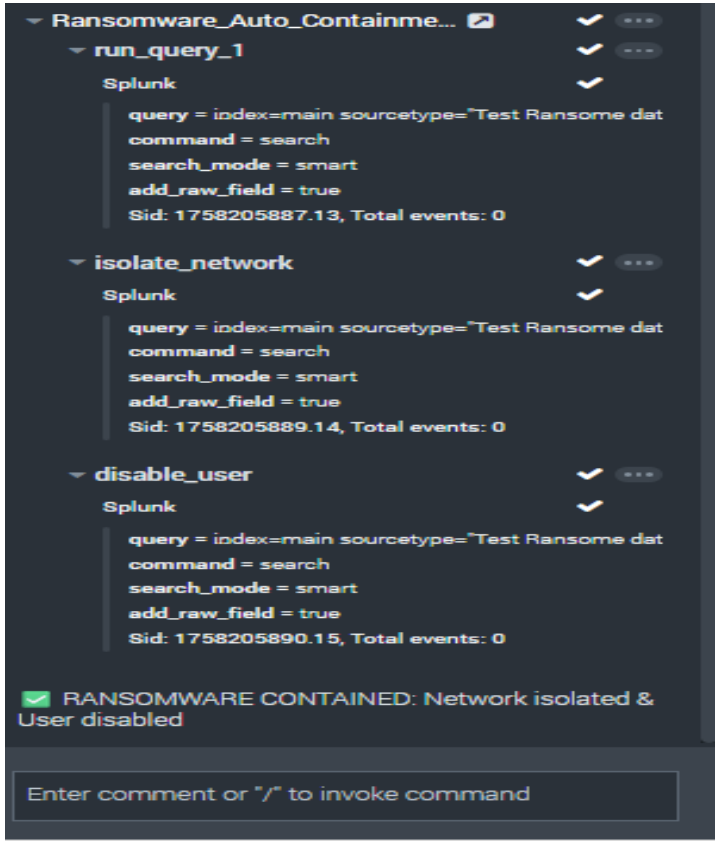


Ransomware Auto Containment



Add Ransomware Attack Event in SOAR and Run Playbook





Container (RANSOMWARE-WIN-VICTIM01)

[Start] → Provides container context

[run_query_1] → Queries Splunk → Finds host="WIN-VICTIM01"

[isolate_network] → Uses host data → Simulates network isolation

[disable_user] → Uses event data → Simulates account disable

[add_comment] → Documents all actions taken

[End] → Playbook complete

Splunk Enterprise Deployment Walkthrough

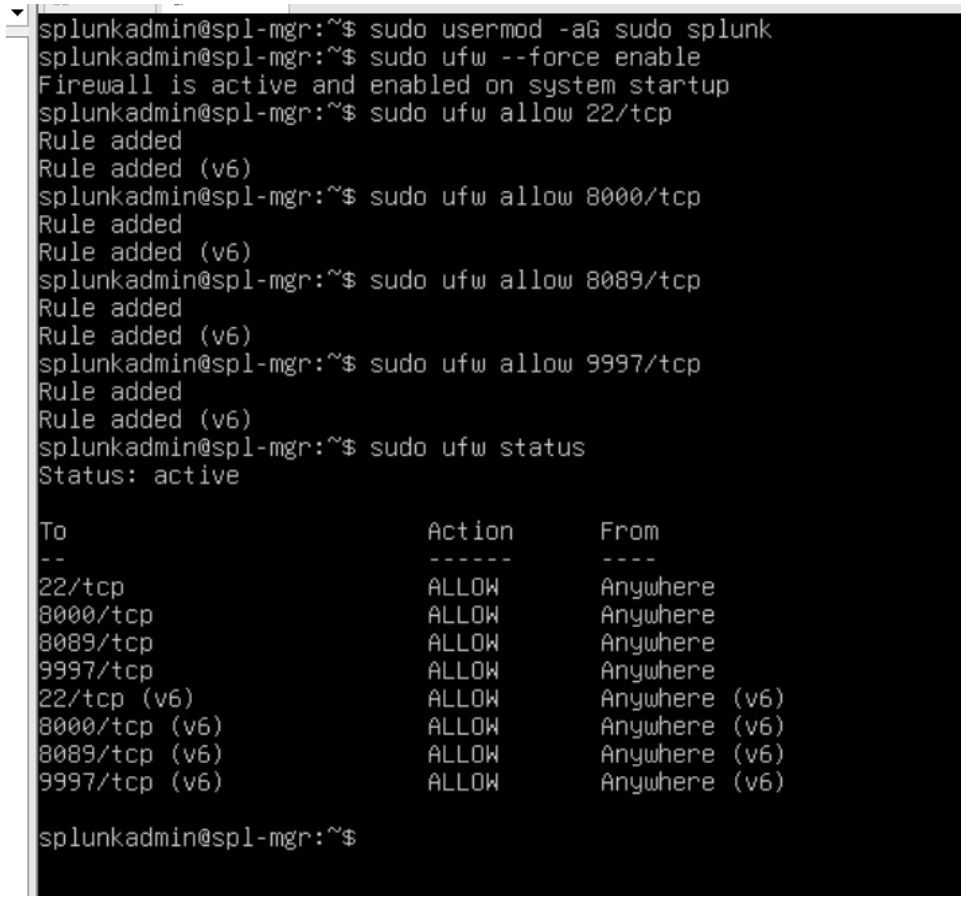
Splunk Deployment!

```
splunkadmin@spl-mgr:~$ ls /mnt/hgfs/
SplunkLabFiles
splunkadmin@spl-mgr:~$ ls -la ~/*.tgz
ls: cannot access '/home/splunkadmin/*.tgz': No such file or directory
splunkadmin@spl-mgr:~$ ls SplunkLabFiles
ls: cannot access 'SplunkLabFiles': No such file or directory
splunkadmin@spl-mgr:~$ sudo ls SplunkLabFiles
ls: cannot access 'SplunkLabFiles': No such file or directory
splunkadmin@spl-mgr:~$ sudo mkdir -p /mnt/shared
splunkadmin@spl-mgr:~$ sudo mount -t fuse.vmhgfs-fuse .host:/SplunkLabFiles /mnt/shared -o allow_other
splunkadmin@spl-mgr:~$ ls -la /mnt/shared/
total 4616711
drwxrwxrwx 1 root root       4096 Aug 21 17:49 .
drwxr-xr-x 4 root root       4096 Aug 22 12:37 ..
-rwxrwxrwx 1 root root 1353162564 Aug 21 17:44 splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
-rwxrwxrwx 1 root root   70895806 Aug 21 17:48 splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.deb
-rwxrwxrwx 1 root root 3303444480 Aug 21 17:37 ubuntu-24.04.3-live-server-amd64.iso
splunkadmin@spl-mgr:~$ cp /mnt/shared/splunk*.deb ~/
splunkadmin@spl-mgr:~$ ls -la ~/*.deb
-rwxrwxr-x 1 splunkadmin splunkadmin 1353162564 Aug 22 12:39 /home/splunkadmin/splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
-rwxrwxr-x 1 splunkadmin splunkadmin   70895806 Aug 22 12:39 /home/splunkadmin/splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.deb
splunkadmin@spl-mgr:~$
```

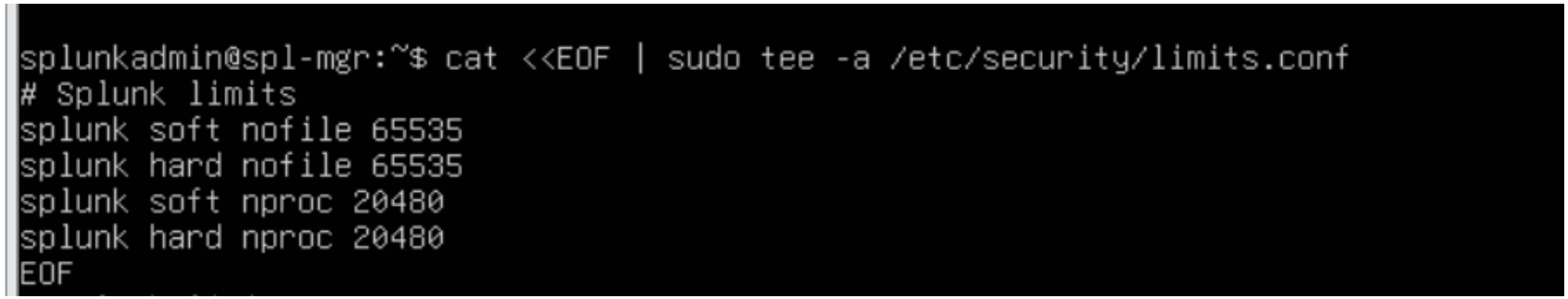
Updating Splunk User password

```
splunkadmin@spl-mgr:~$ sudo passwd splunk
New password:
Retype new password:
passwd: password updated successfully
splunkadmin@spl-mgr:~$
```

Configuring Firewall/ports



System Limits Configuration



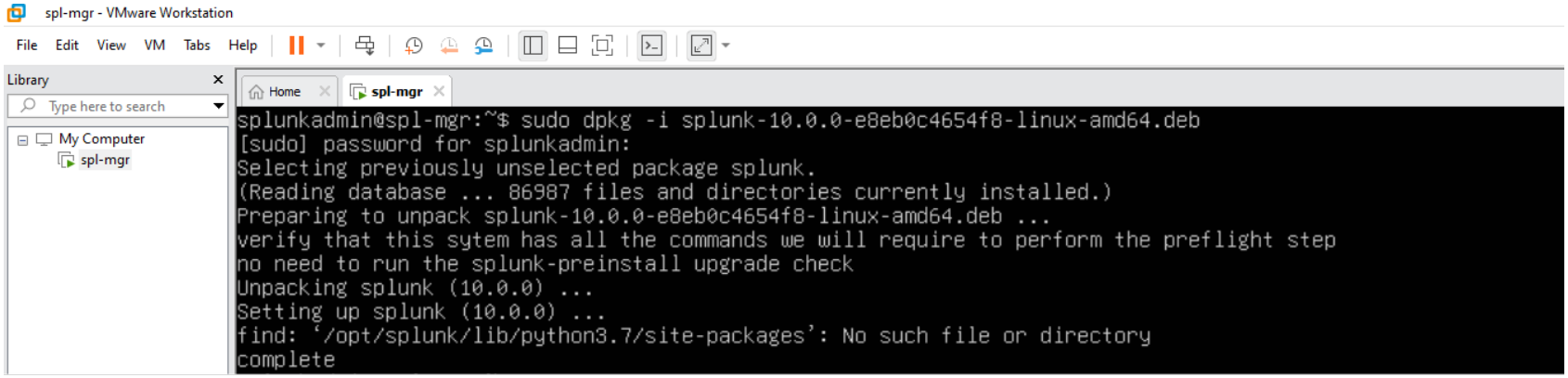
Disable Transparent Huge Pages (THP)

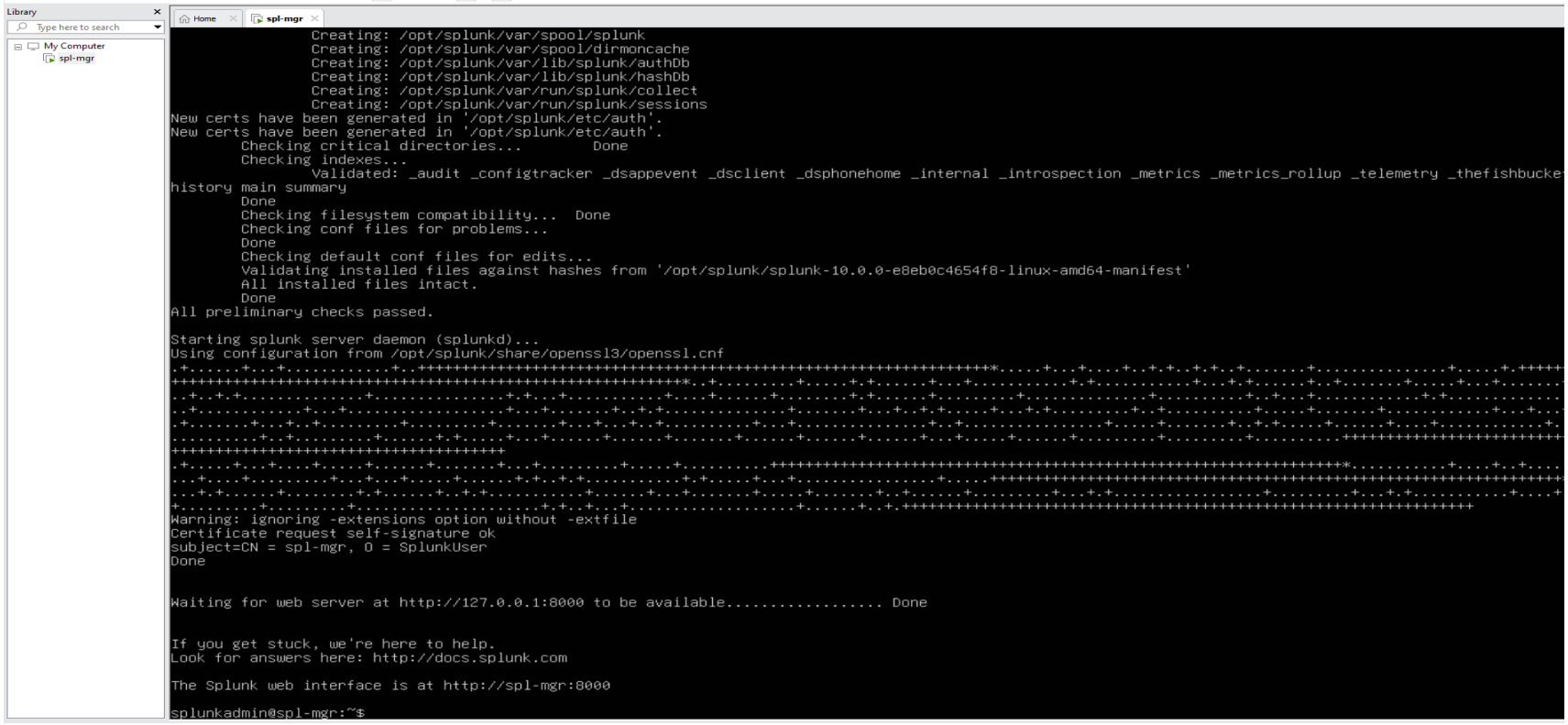
```
splunkadmin@spl-mgr:~$ echo never | sudo tee /sys/kernel/mm/transparent_hugepage/enabled
never
```

```
splunkadmin@spl-mgr:~$ echo never | sudo tee /sys/kernel/mm/transparent_hugepage/defrag
never
splunkadmin@spl-mgr:~$
```

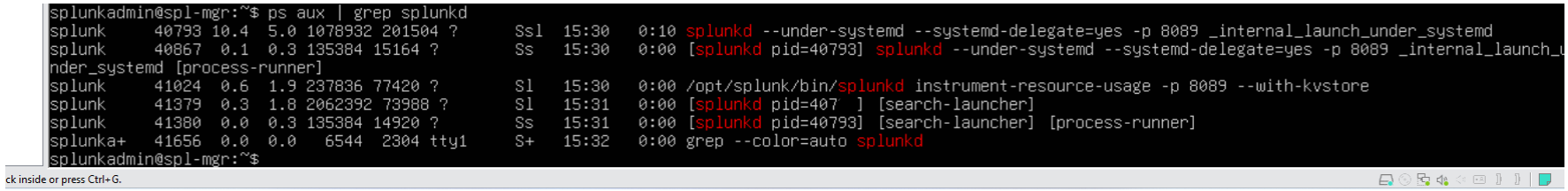
```
splunkadmin@spl-mgr:~$ cat << 'EOF' | sudo tee /etc/systemd/system/disable-thp.service
> [Unit]
> Description=Disable Transparent Huge Pages
>
> [Service]
> Type=simple
> ExecStart=/bin/sh -c "echo never > /sys/kernel/mm/transparent_hugepage/enabled && echo never > /sys/kernel/mm/transparent_hugepage/defrag"
>
> [Install]
> WantedBy=multi-user.target
> EOF
[sudo] password for splunkadmin:
[Unit]
Description=Disable Transparent Huge Pages

[Service]
Type=simple
ExecStart=/bin/sh -c "echo never > /sys/kernel/mm/transparent_hugepage/enabled && echo never > /sys/kernel/mm/transparent_hugepage/defrag"

[Install]
WantedBy=multi-user.target
splunkadmin@spl-mgr:~$ sudo systemctl daemon-reload
splunkadmin@spl-mgr:~$ sudo systemctl enable disable-thp
Created symlink /etc/systemd/system/multi-user.target.wants/disable-thp.service → /etc/systemd/system/disable-thp.service.
splunkadmin@spl-mgr:~$ sudo systemctl start disable-thp
splunkadmin@spl-mgr:~$ cat /sys/kernel/mm/transparent_hugepage/enabled
always madvise [never]
```

Install Splunk Enterprise 10.0.0

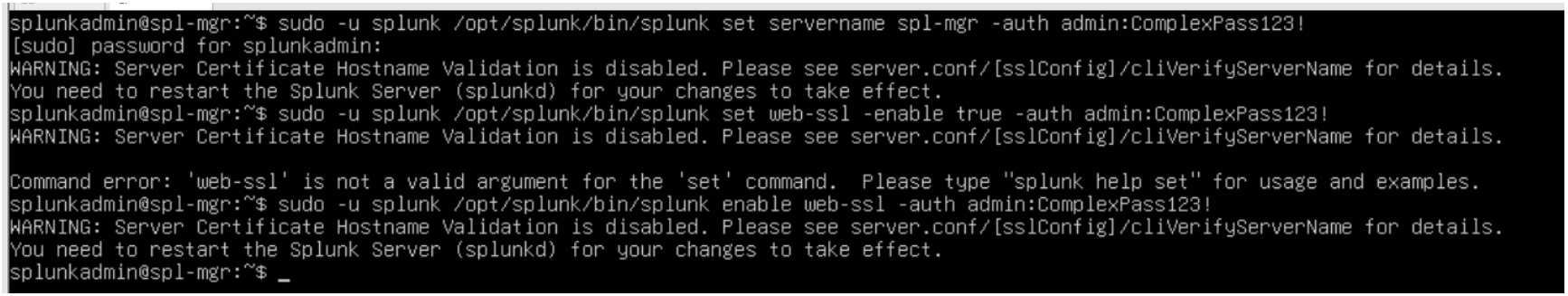




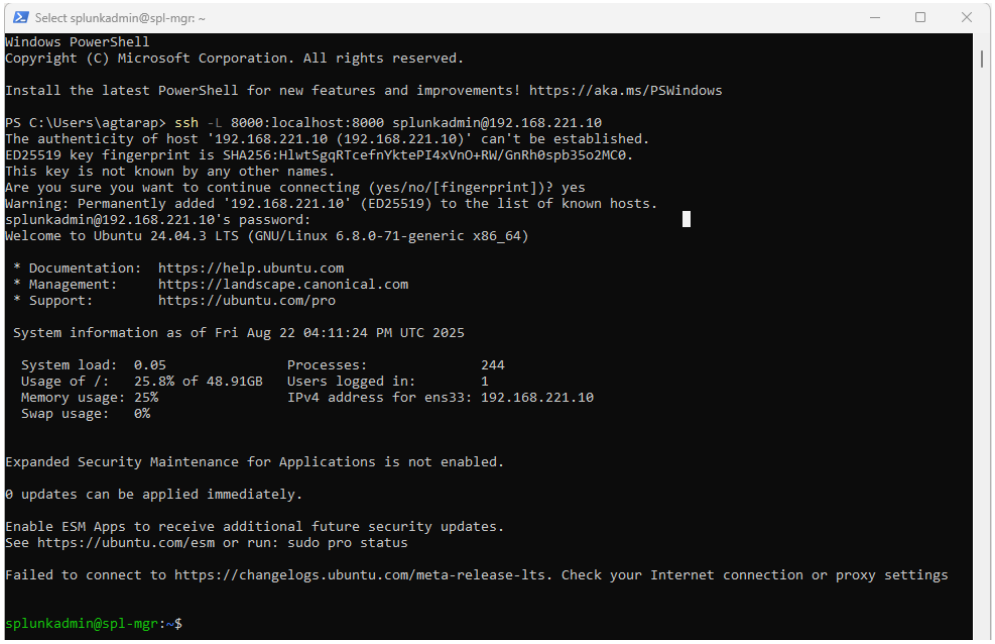
Enable Boot Start



Enable HTTPS



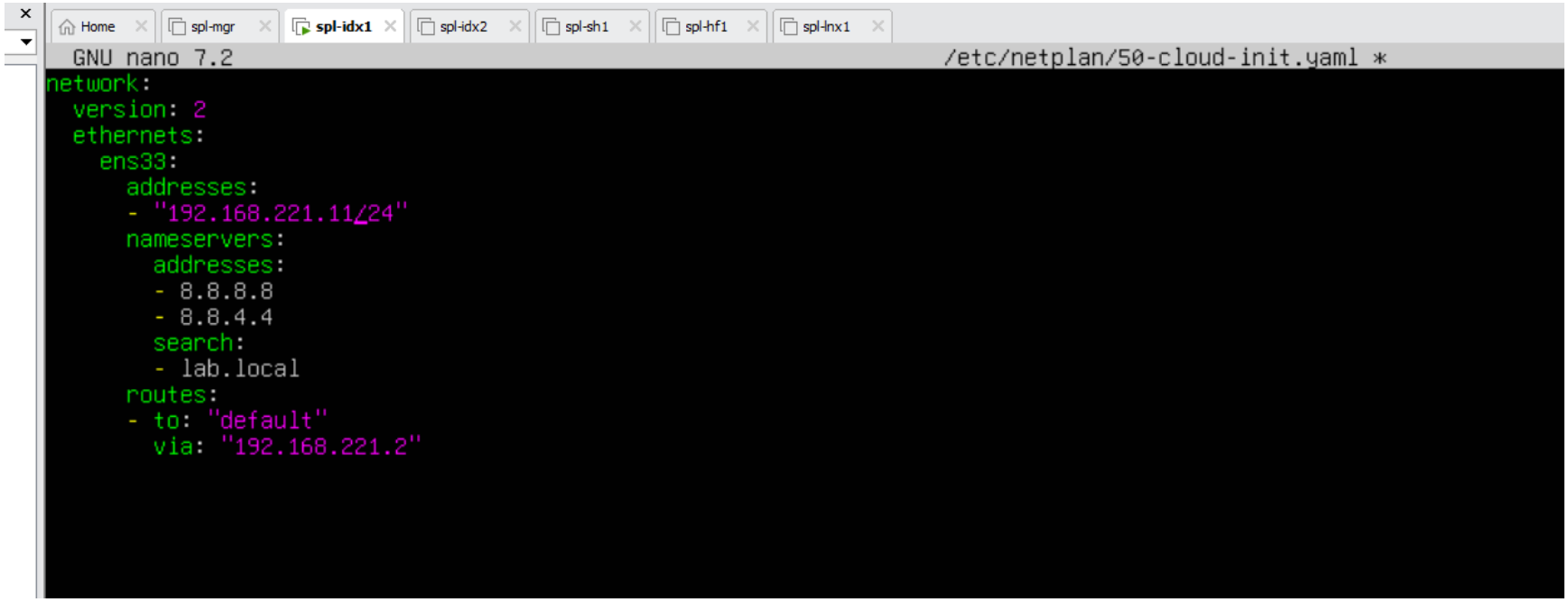
SSH Port Forwarding (Tunneling)



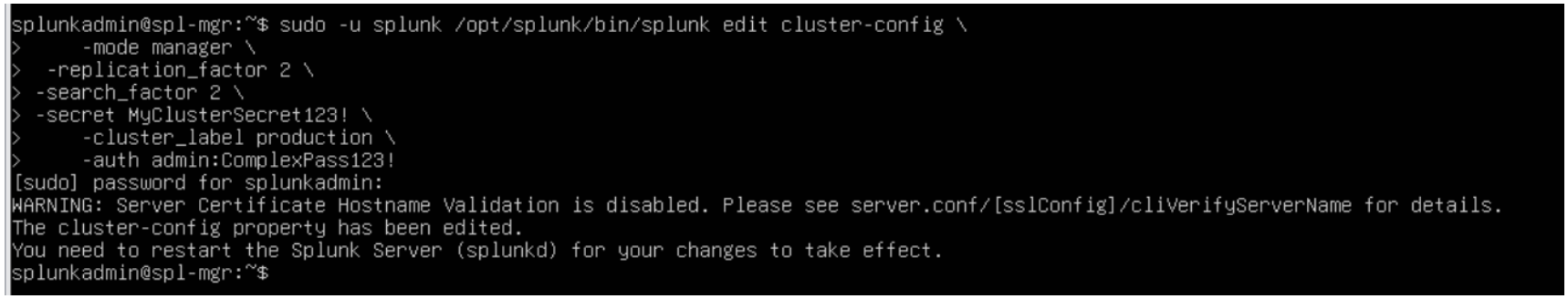
Build all VM's

VM Name	Role	RAM	CPU	Purpose
spl-idx1	Indexer 1	8GB	4	First indexer peer
spl-idx2	Indexer 2	8GB	4	Second indexer peer
spl-sh1	Search Head	6GB	4	Search interface
spl-hf1	Heavy Forwarder	4GB	2	Data collection hub
spl-lnx1	Linux UF	2GB	1	Linux endpoint

Configure VMS



Cluster Configuration

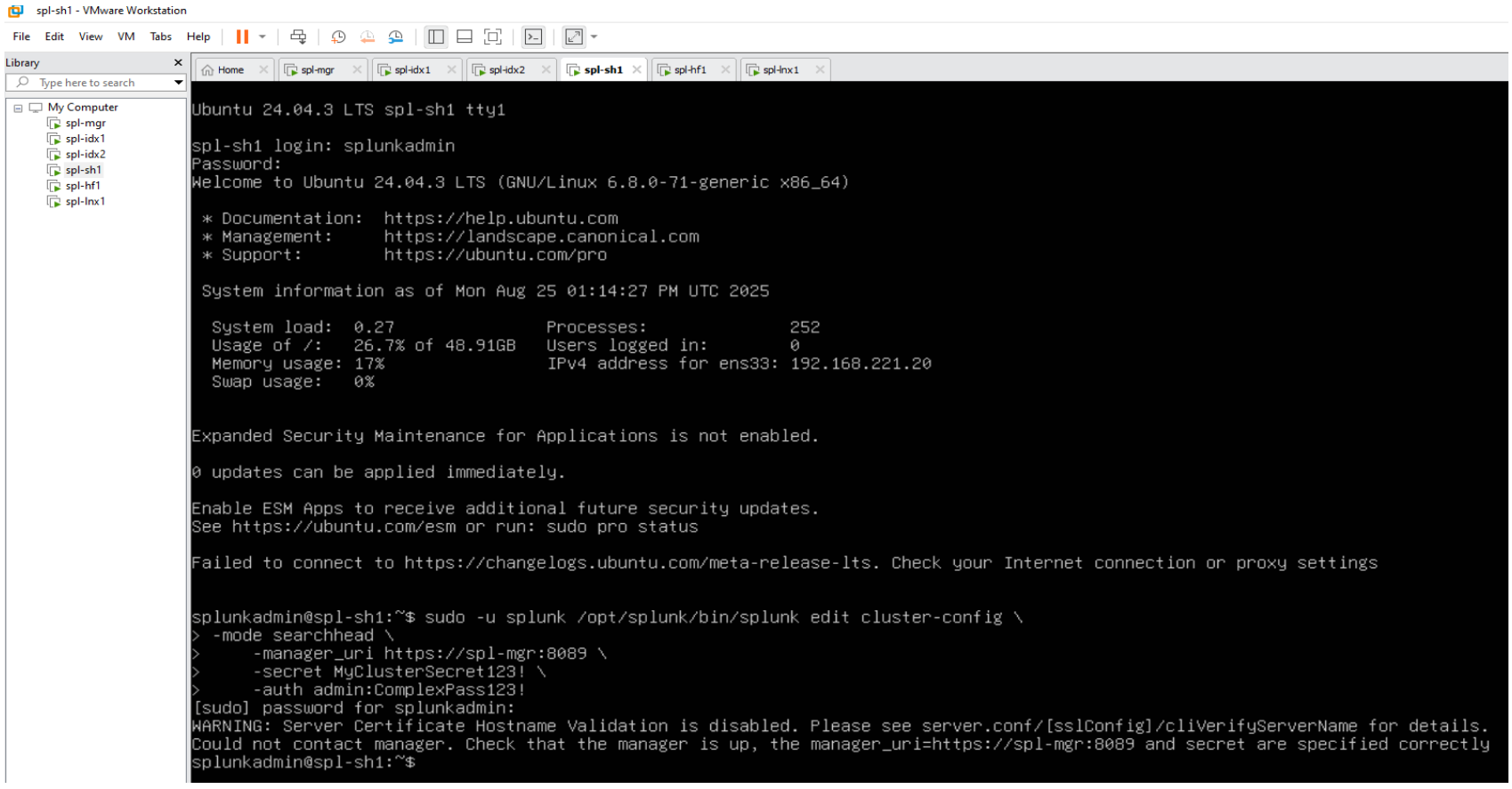


Index Configuration's

```
splunkadmin@spl-idx1:~$ sudo -u splunk /opt/splunk/bin/splunk edit cluster-config \
> -mode peer \
>     -manager_uri https://spl-mgr:8089 \
>     -replication_port 9887 \
>     -secret MyClusterSecret123! \
>     -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Could not contact manager. Check that the manager is up, the manager_uri=https://spl-mgr:8089 and secret are specified correctly
splunkadmin@spl-idx1:~$ sudo systemctl restart Splunkd
```

nside or press Ctrl+G.

Search Head Configuration




```
splunkadmin@spl-sh1:~$ sudo -u splunk /opt/splunk/bin/splunk add search-server https://spl-idx1:8089 \
>     -auth admin:ComplexPass123! -remoteUsername admin -remotePassword ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Peer added
splunkadmin@spl-sh1:~$
```

Heavy Forwarder Setup

```
splunkadmin@spl-hf1:~$ sudo -u splunk /opt/splunk/bin/splunk enable listen 9997 -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Listening for Splunk data on TCP port 9997.
splunkadmin@spl-hf1:~$ _
```

```
splunkadmin@spl-hf1:~$ cat << 'EOF' | sudo tee /opt/splunk/etc/system/local/outputs.conf
> [tcpout]
u> defaultGroup = indexer_cluster
>
> [tcpout:indexer_cluster]
> server = spl-idx1:9997,spl-idx2:9997
> useACK = true
> autoLB = true
> compressed = true
> EOF
[tcpout]
defaultGroup = indexer_cluster

[tcpout:indexer_cluster]
server = spl-idx1:9997,spl-idx2:9997
useACK = true
autoLB = true
compressed = true
splunkadmin@spl-hf1:~$
```

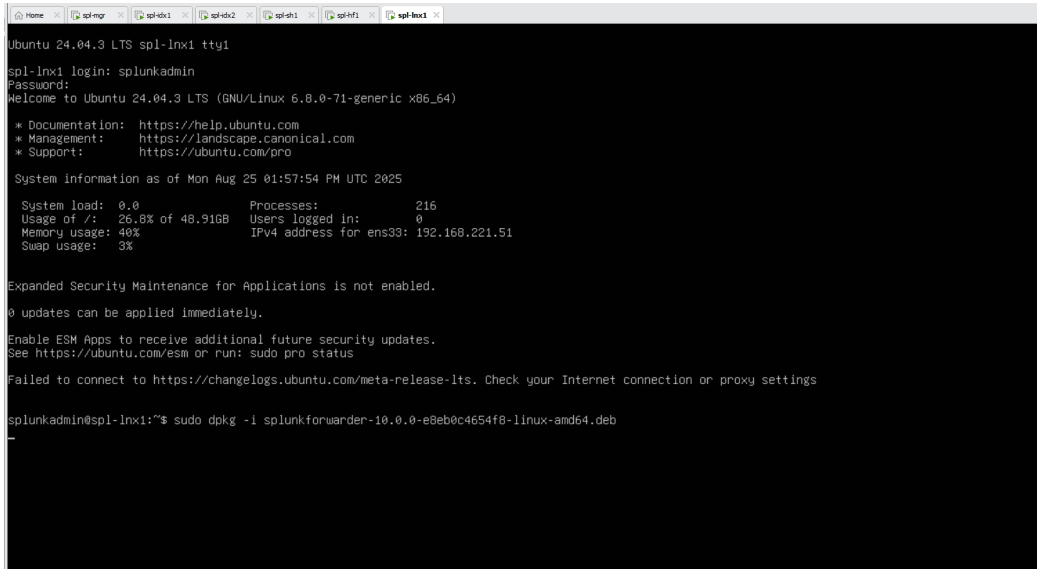
side or press Ctrl+G.

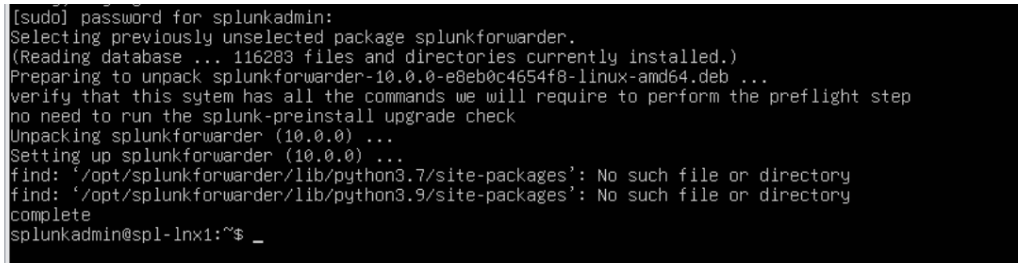
Deployment Server

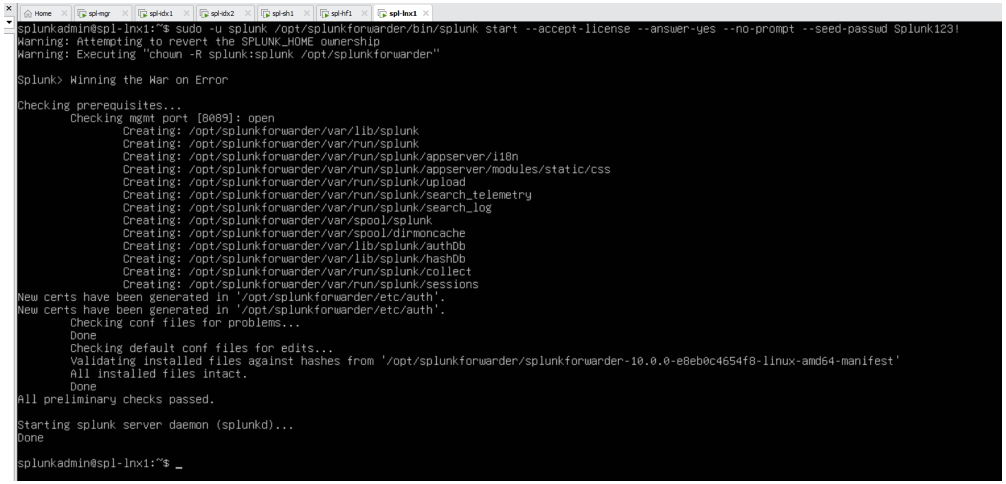
Home | spl-mgr | spl-idx1 | spl-idx2 | spl-sh1 | spl-hf1 | spl-lnx1

```
splunkadmin@spl-mgr:~$ sudo -u splunk mkdir -p /opt/splunk/etc/deployment-apps/TA_base_outputs/local
splunkadmin@spl-mgr:~$ cat << 'EOF' | sudo tee /opt/splunk/etc/deployment-apps/TA_base_outputs/local/outputs.conf
> [tcpout]
> defaultGroup = heavy_forwarder
>
> [tcpout:heavy_forwarder]
> server = spl-hf1:9997
> compressed = true
> EOF
[tcpout]
defaultGroup = heavy_forwarder

[tcpout:heavy_forwarder]
server = spl-hf1:9997
compressed = true
splunkadmin@spl-mgr:~$ sudo chown -R splunk:splunk /opt/splunk/etc/deployment-apps/
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk reload deploy-server -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Reloading serverclass(es).
splunkadmin@spl-mgr:~$ _
```

Universal Forwarder (spl-lnx1)







Verify UF configured correctly

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk list deploy-clients -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Deployment client: 5EEC24CA-82DA-45D3-895E-76830D0CA339
                averagePhoneHomeInterval:       60
                build:       e8eb0c4654f8
                clientName:       5EEC24CA-82DA-45D3-895E-76830D0CA339
                dns:       192.168.221.51
                guid:       5EEC24CA-82DA-45D3-895E-76830D0CA339
                hostname:       spl-lnx1
                id:       connection_192.168.221.51_8089_192.168.221.51_spl-lnx1_linux-x86%64_5EEC24CA-82DA-45D3-895E-76830D0CA339_5EEC24CA-82DA-45D3-895E
0D0CA339
                instanceId:       5EEC24CA-82DA-45D3-895E-76830D0CA339
                instanceName:       spl-lnx1
                ip:       192.168.221.51
                lastPhoneHomeTime:       1756135362
                mgmt:       8089
                name:       5EEC24CA-82DA-45D3-895E-76830D0CA339
                package:       universal_forwarder
                packageType:       deb
                serverClasses:       None
                splunkVersion:       10.0.0
                utsname:       linux-x86_64
splunkadmin@spl-mgr:~$
```

Verify Cluster Health

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk show cluster-manager-status -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Command error: 'cluster-manager-status' is not a valid argument for the 'show' command.  Please type "splunk help show" for usage and examples.
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk show cluster-status -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

 Replication factor met
 Search factor met
 All data is searchable
 Indexing Ready YES
 HA Mode: Disabled

 spl-idx2        B32D5E91-4703-40D3-9A13-8240217D378D    default
         Searchable YES
         Status  Up
         Bucket Count=12

 spl-idx1        B6E895B9-606E-4336-A449-463AA4A6E240    default
         Searchable YES
         Status  Up
         Bucket Count=13
splunkadmin@spl-mgr:~$
```

Check Search Head Connectivity

```
splunkadmin@spl-sh1:~$ sudo -u splunk /opt/splunk/bin/splunk list search-server -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Server at URI "192.168.221.11:8089" with status as "Up"
Server at URI "192.168.221.12:8089" with status as "Up"
splunkadmin@spl-sh1:~$ _
```

Check Universal Forwarder

```
splunkadmin@spl-lnx1:~$ sudo -u splunk /opt/splunkforwarder/bin/splunk show deploy-poll -auth admin:Splunk123!
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Deployment Server URI is set to "spl-mgr:8089".
splunkadmin@spl-lnx1:~$
```

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk list deploy-clients -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

Deployment client: 4EAF7940-C890-4799-A7F9-06CB27083623
                averagePhoneHomeInterval:       60
                build:          e8eb0c4654f8
                clientName:         4EAF7940-C890-4799-A7F9-06CB27083623
                dns:        192.168.221.51
                guid:         4EAF7940-C890-4799-A7F9-06CB27083623
                hostname:         spl-lnx1
                id:         connection_192.168.221.51_8089_192.168.221.51_spl-lnx1_linux-x86%64_4EAF7940-C890-4799-A7F9-06CB27083623_4EAF7940-C890-4799-A7F9-06CB
27083623
                instanceId:         4EAF7940-C890-4799-A7F9-06CB27083623
                instanceName:         spl-lnx1
                ip:         192.168.221.51
                lastPhoneHomeTime:         1756238167
                mgmt:         8089
                name:         4EAF7940-C890-4799-A7F9-06CB27083623
                package:        universal_forwarder
                packageType:        deb
                serverClasses:        None
                splunkVersion:        10.0.0
                utsname:        linux-x86_64
splunkadmin@spl-mgr:~$
```

Splunk Deployment Complete Validation & Testing

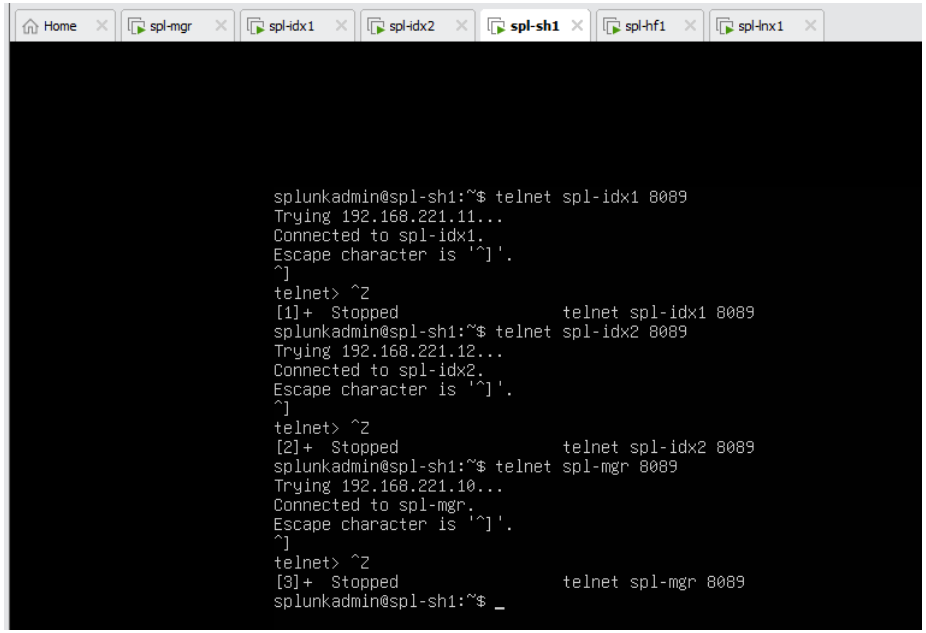
[Data Sources] → [Universal Forwarder] → [Heavy Forwarder] → [Indexer Cluster] → [Search Head]

Verify Network Connectivity

```
splunkadmin@spl-lnx1:~$ telnet spl-hf1 9997
Trying 192.168.221.30...
Connected to spl-hf1.
Escape character is '^]'.

^]
telnet>
```

```
splunkadmin@spl-lnx1:~$ telnet spl-mgr 8089
Trying 192.168.221.10...
Connected to spl-mgr.
Escape character is '^]'.
^]
telnet>
```

```
splunkadmin@spl-hf1:~$ sudo -u splunk /opt/splunk/bin/splunk list forward-server -auth admin:ComplexPass123!
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Active forwards:
        spl-idx1:9997
        spl-idx2:9997
Configured but inactive forwards:
        None
splunkadmin@spl-hf1:~$ _
```



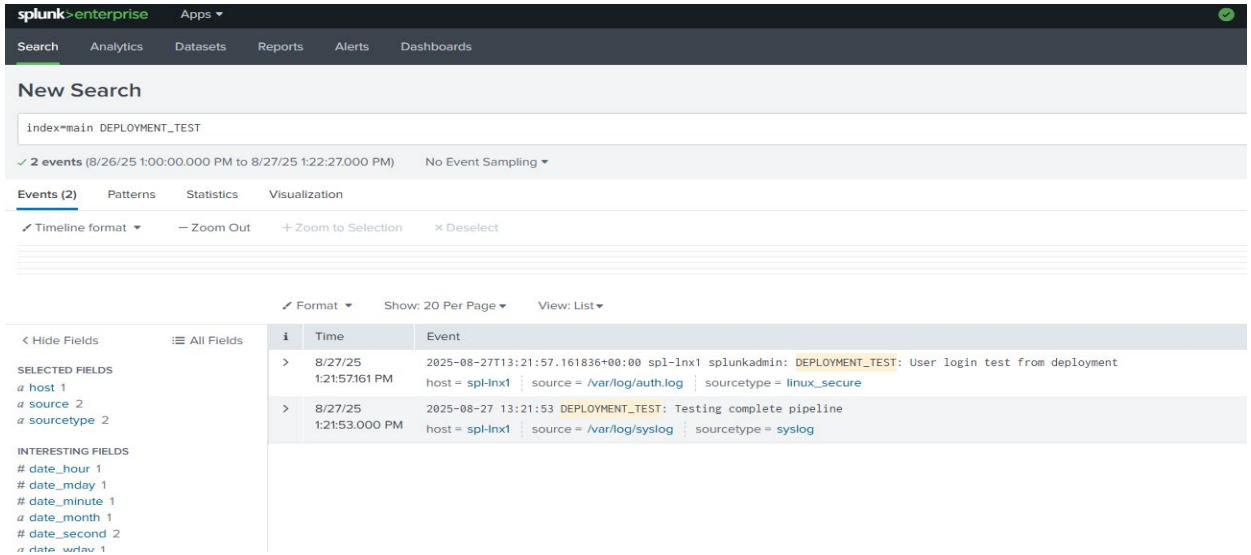

```
splunkadmin@spl-mgr:~$ sudo -u splunk /opt/splunk/bin/splunk show cluster-status -auth admin:ComplexPass123!
[sudo] password for splunkadmin:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.

 Replication factor met
 Search factor met
 All data is searchable
 Indexing Ready YES
 HA Mode: Disabled

 spl-idx2        B32D5E91-4703-40D3-9A13-8240217D378D    default
         Searchable YES
         Status  Up
         Bucket Count=14

 spl-idx1        B6E895B9-606E-4336-A449-463AA4A6E240    default
         Searchable YES
         Status  Up
         Bucket Count=15
splunkadmin@spl-mgr:~$
```

Test Universal Forwarder → Heavy Forwarder

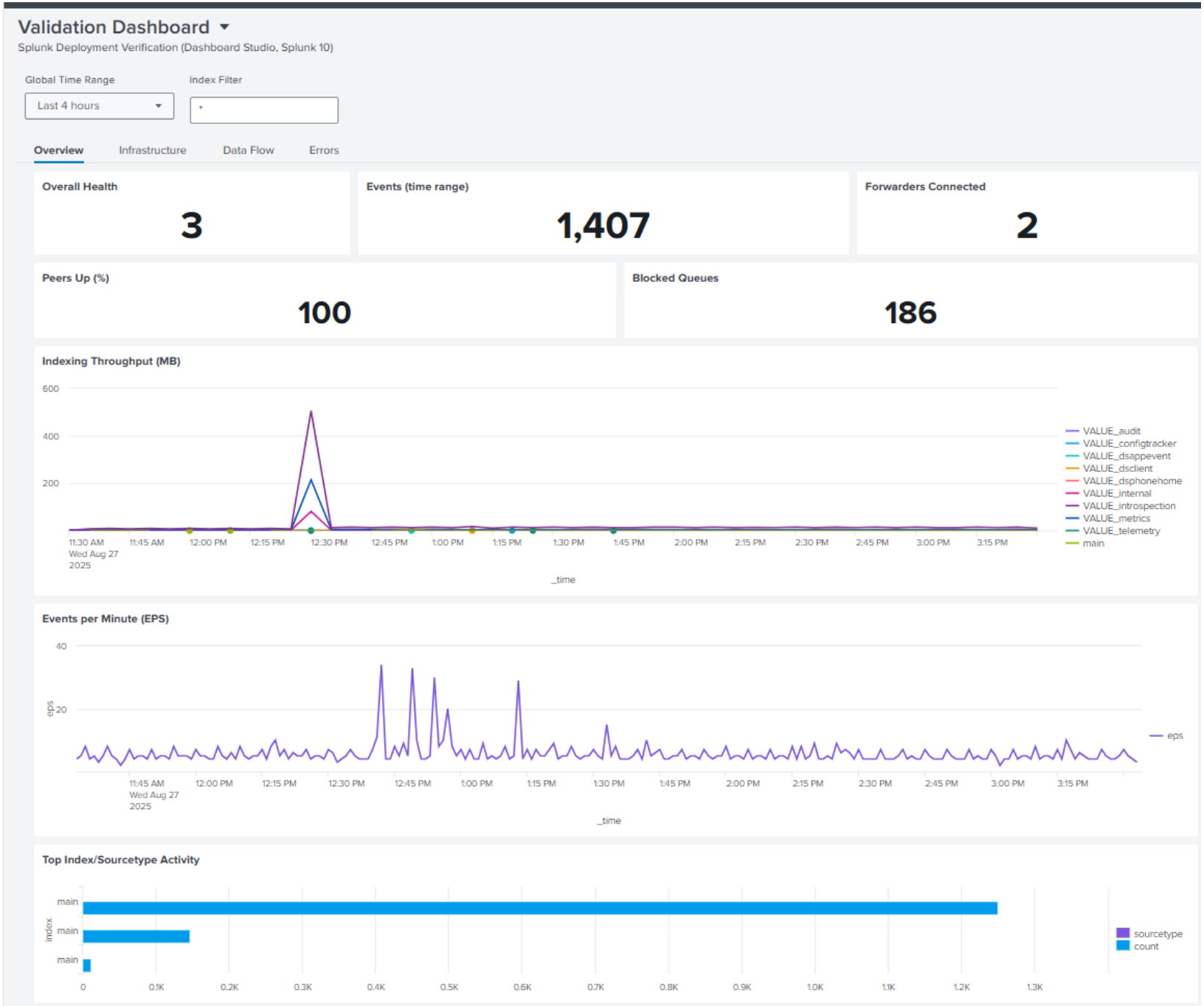
```
splunkadmin@spl-lnx1:~$ echo "$(date '+%Y-%m-%d %H:%M:%S') TEST_MARKER_UF: Universal Forwarder test event $$" | sudo tee -a /var/log/test_uf.log
[sudo] password for splunkadmin:
2025-08-27 12:41:19 TEST_MARKER_UF: Universal Forwarder test event 1325
splunkadmin@spl-lnx1:~$ sudo -u splunk /opt/splunkforwarder/bin/splunk add monitor /var/log/test_uf.log \
>     -index main -sourcetype test_uf -auth admin:Splunk123!
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk:splunk /opt/splunkforwarder"
Added monitor of '/var/log/test_uf.log'.
splunkadmin@spl-lnx1:~$ for i in {1..10}; do
>     echo "$(date '+%Y-%m-%d %H:%M:%S') TEST_MARKER_UF: Event $i from $(hostname) PID=$$ Time=$(date +%s)" | sudo tee -a /var/log/test_uf.log
>     sleep 1
> done
2025-08-27 12:42:06 TEST_MARKER_UF: Event 1 from spl-lnx1 PID=1325 Time=1756298526
2025-08-27 12:42:07 TEST_MARKER_UF: Event 2 from spl-lnx1 PID=1325 Time=1756298527
2025-08-27 12:42:08 TEST_MARKER_UF: Event 3 from spl-lnx1 PID=1325 Time=1756298528
2025-08-27 12:42:09 TEST_MARKER_UF: Event 4 from spl-lnx1 PID=1325 Time=1756298529
2025-08-27 12:42:10 TEST_MARKER_UF: Event 5 from spl-lnx1 PID=1325 Time=1756298530
2025-08-27 12:42:11 TEST_MARKER_UF: Event 6 from spl-lnx1 PID=1325 Time=1756298531
2025-08-27 12:42:12 TEST_MARKER_UF: Event 7 from spl-lnx1 PID=1325 Time=1756298532
2025-08-27 12:42:13 TEST_MARKER_UF: Event 8 from spl-lnx1 PID=1325 Time=1756298533
2025-08-27 12:42:14 TEST_MARKER_UF: Event 9 from spl-lnx1 PID=1325 Time=1756298534
2025-08-27 12:42:15 TEST_MARKER_UF: Event 10 from spl-lnx1 PID=1325 Time=1756298535
splunkadmin@spl-lnx1:~$ _
```

```
splunkadmin@spl-hf1:~$ sudo lsof -i :9997 | grep spl-lnx1
[sudo] password for splunkadmin:
splunkd 41780      splunk  120u  IPv4 422380      0t0  TCP spl-hf1:9997->spl-lnx1:42808 (ESTABLISHED)
splunkadmin@spl-hf1:~$
```

Confirming the entire pipeline works: UF (spl-lnx1) → HF (spl-hf1) → Indexers (spl-idx1, spl-idx2) → Search Head (spl-sh1)



Custom Built Splunk Deployment Verification Dashboard using JSON



Validation Dashboard

Splunk Deployment Verification (Dashboard Studio, Splunk 10)

Global Time Range: Last 4 hours

Index Filter: *

Overview | **Infrastructure** | Data Flow | Errors

Server Info

splunk_server	version	os_name	product_type
spl-mgr	10.0.0	Linux	enterprise
spl-idx1	10.0.0	Linux	enterprise
spl-idx2	10.0.0	Linux	enterprise

Distributed Search Peers

peerName	status	build	version
spl-idx1	Up	e8eb0c4654f8	10.0.0
spl-idx2	Up	e8eb0c4654f8	10.0.0

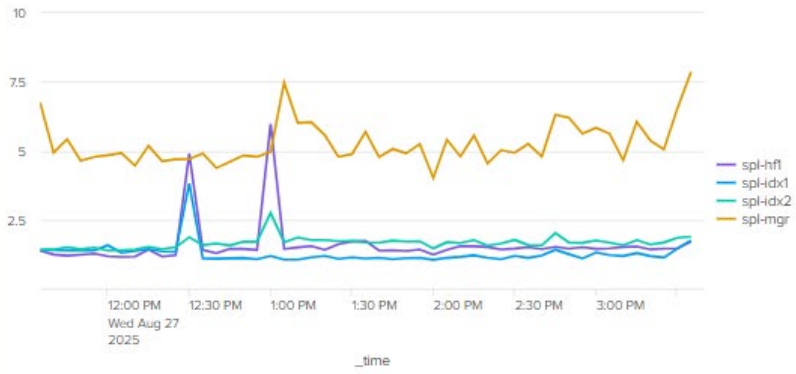
Cluster Manager Info

mode	service_read...	indexing_rea...	replication_f...	search_factor
	1	1		

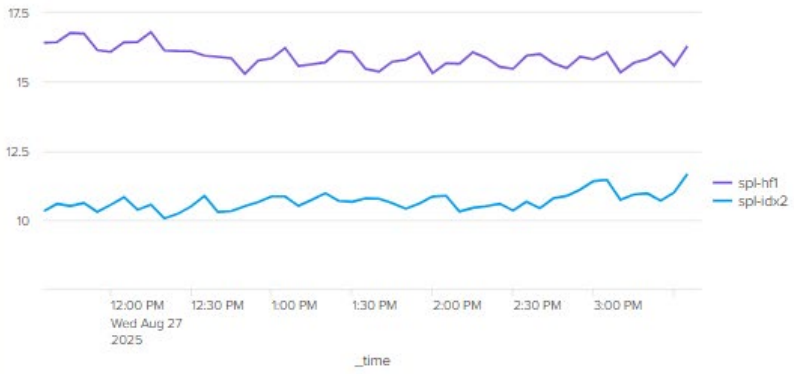
Indexer Cluster Peers

label	status	buckets_db	consistent
spl-idx2	Up		
spl-idx1	Up		

CPU %, by Host (_introspection)



Memory %, by Host (_introspection)



Deployment Clients

0

HEC Tokens (enabled/total)

0

Validation Dashboard

Splunk Deployment Verification (Dashboard Studio, Splunk 10)

Global Time Range: Last 4 hours

Index Filter: *

Overview | Infrastructure | **Data Flow** | Errors

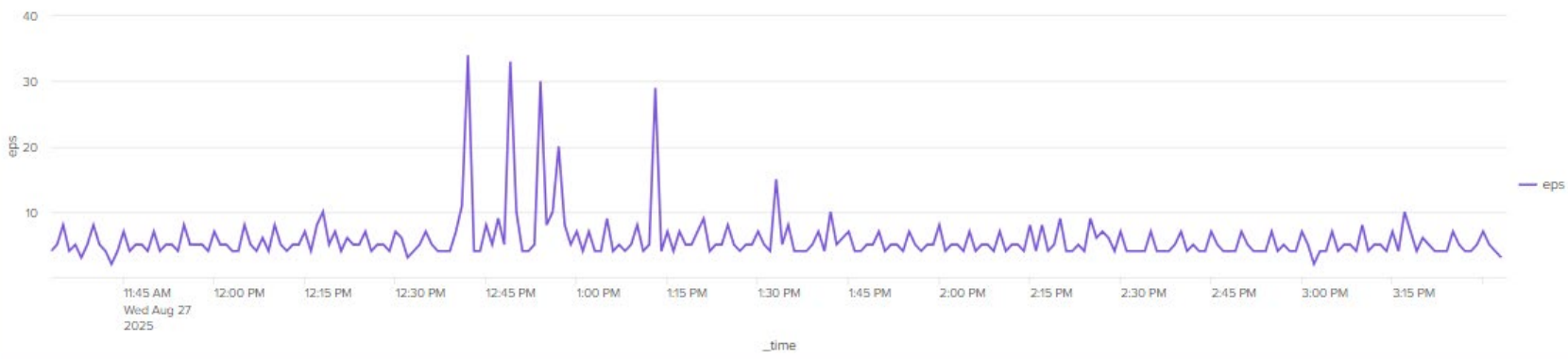
Forwarder Connections (eps, KBps)

sourceHost	KBps	eps
192.168.221.30	16.78	11.97
192.168.221.51	0.17	0.88

Test Marker Events

test_type	sourcetype	host	count
HF	test_hf	spl-hf1	11

Events / 1m for *



AWS - Cloud Security & Vulnerability Management Portfolio

Phase 1: Security Foundation

IAM & Access Control - Implemented multi-factor authentication with Duo, created IAM user 'portfolio-admin' with AdministratorAccess policy via security group, enforced password complexity requiring uppercase, lowercase, numbers, and symbols.

Audit & Monitoring - Deployed CloudTrail named 'portfolio-audit-trail' with multi-region coverage, KMS encryption enabled, capturing all management events while excluding data events for cost optimization.

Budget Controls - Created $5 monthly budget with 80% threshold alerts to maintain cost awareness throughout testing.

Phase 2: Infrastructure with Intentional Vulnerabilities

VPC Architecture - Built 'portfolio-vpc' (10.0.0.0/16) with 2 public and 2 private subnets across availability zones, configured route tables and internet gateway.

S3 Bucket Issues - Created 'portfolio-test-bucket-918689' with deliberate misconfigurations: public access allowed, no encryption, no versioning, missing SSL-only policy.

EC2 Security Gaps - Deployed 'portfolio-web-server' (t2.micro) with vulnerable security group 'portfolio-web-sg' having SSH open to 0.0.0.0/0, unencrypted EBS volumes.

Phase 3: Detection & Compliance

AWS Config - Configured 10 compliance rules, detected 6 non-compliant resources including public S3, missing encryption, open SSH, achieving initial 40% compliance score.

S3 Remediation - Blocked all public access settings, enabled SSE-S3 encryption, activated versioning, implemented SSL-only bucket policy, achieved 90% compliance in <30 minutes.

Security Group Fixes - Restricted SSH from 0.0.0.0/0 to specific IP only, removed unnecessary ICMP rules, enabled EBS encryption by default for future volumes.

Phase 4: Incident Response & Automation

Compromised Key Simulation - Created 'test-developer' IAM user, simulated unauthorized API calls, detected activity via CloudTrail within 5 minutes, disabled compromised keys.

Lambda Auto-Remediation - Built Python function 'S3SecurityAutoFix' that automatically enables encryption and versioning on non-compliant buckets, tested successful execution.

EKS Deployment - Installed eksctl in CloudShell, created 'portfolio-cluster' with proper IAM roles (ClusterRole and NodeRole), verified kubectl connectivity.

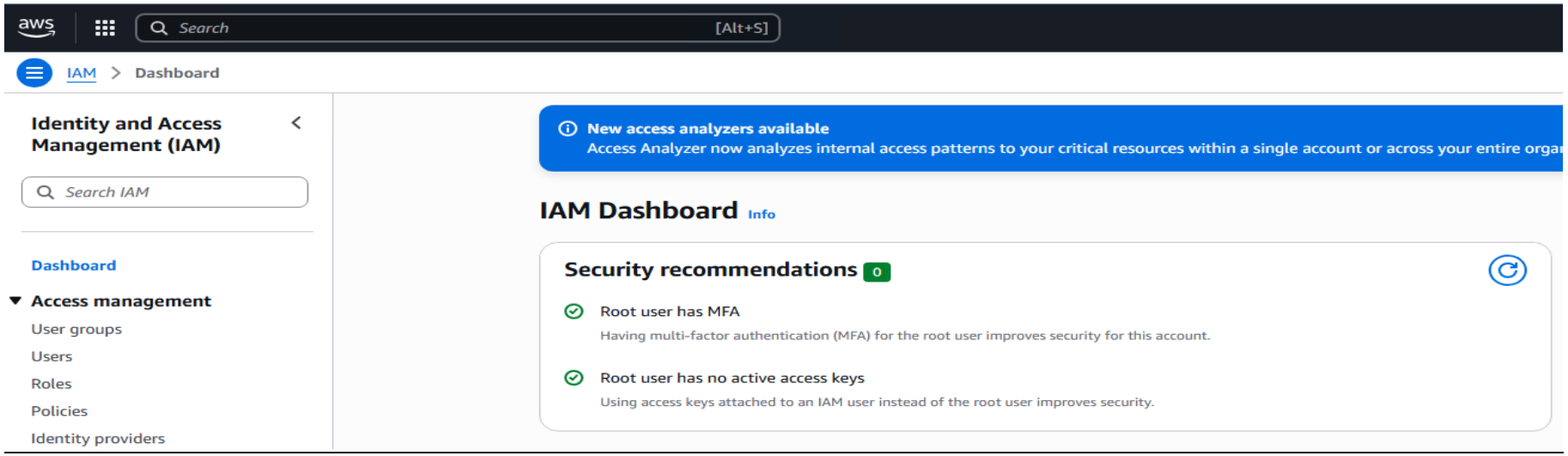
Phase 5: Advanced Security Tools

Amazon Inspector - Activated scanning, created Ubuntu instance 'i-0887dfece8721dded', detected 101 package vulnerabilities including CVE-2025-21919 (CVSS 7.8) with no available patch.

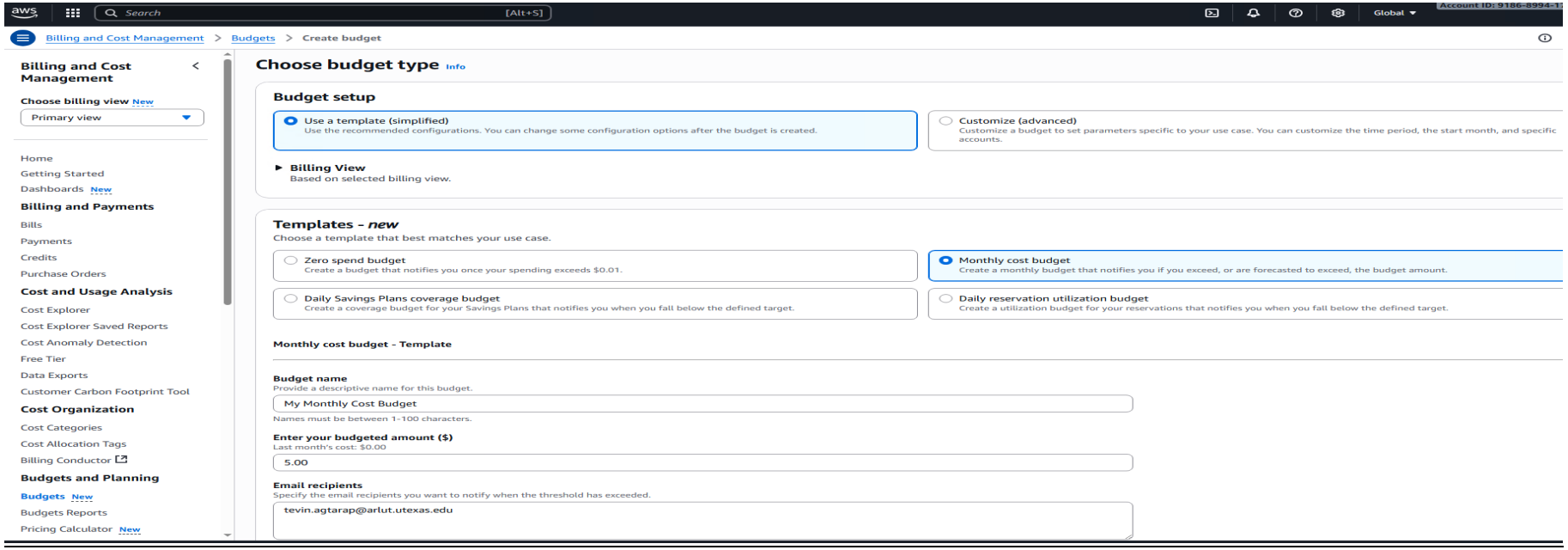
Zero-Day Management - Verified patch unavailable ("work in progress" per Ubuntu), implemented compensating controls, terminated vulnerable instance as risk mitigation.

Amazon GuardDuty - Enabled threat detection (detector ID: 7eccb8b03cff3a081bf7dc7204c9a55c), generated sample findings including cryptocurrency mining and SSH brute force attacks.

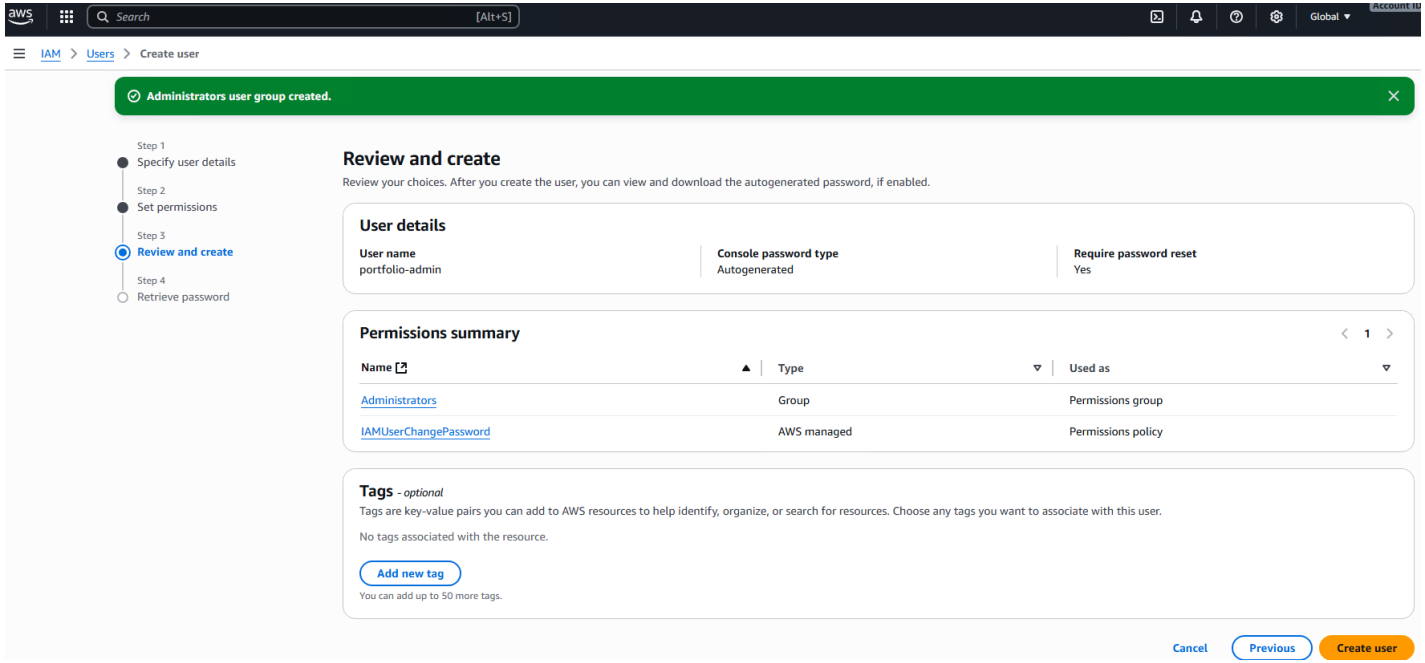
Add multifactor authentication using the DUO APP



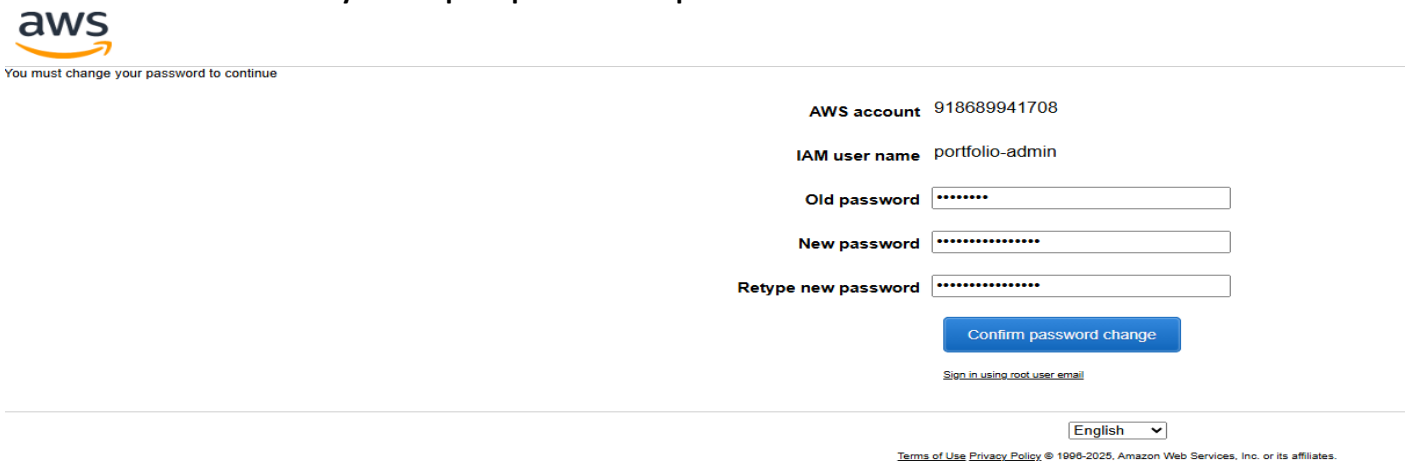
Create a budget



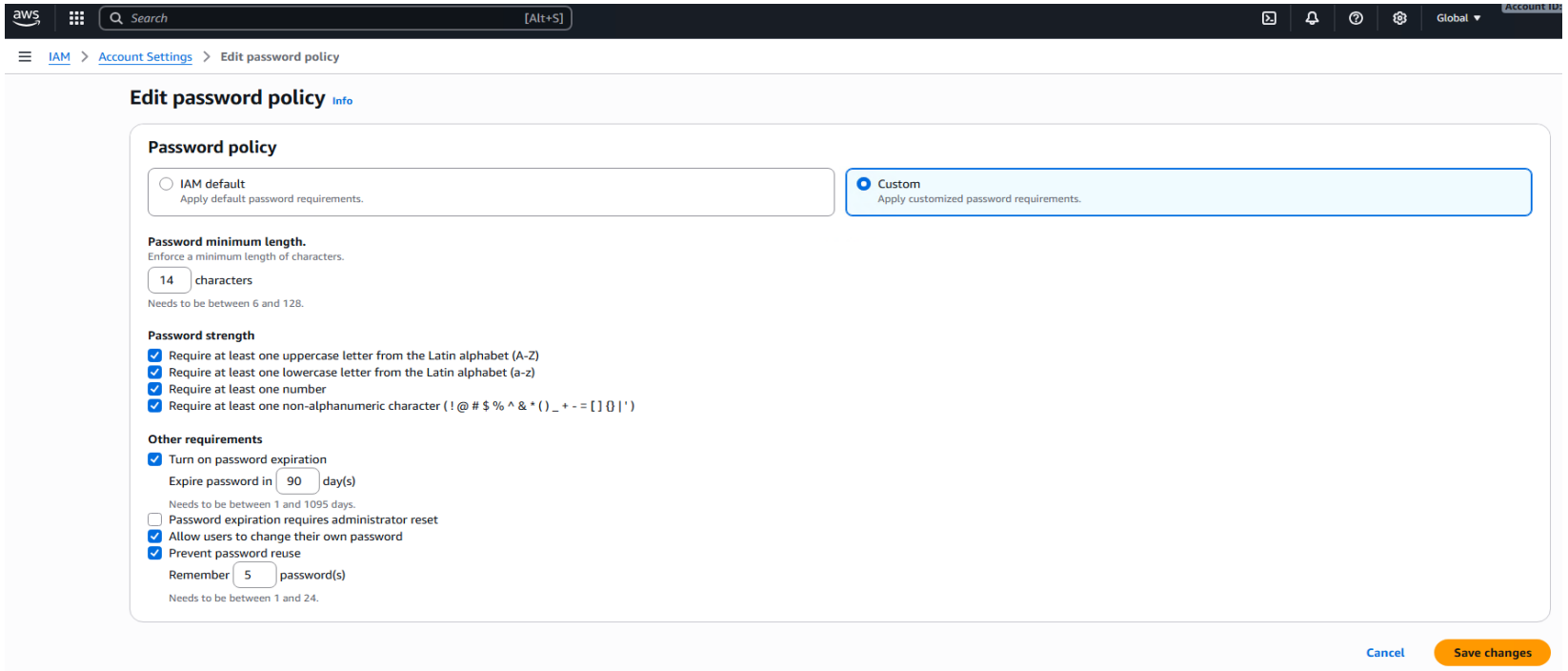
For this portfolio lab, I used AWS's AdministratorAccess managed policy to ensure full access for security testing and configuration. In production, I would implement least-privilege custom policies based on actual job functions.



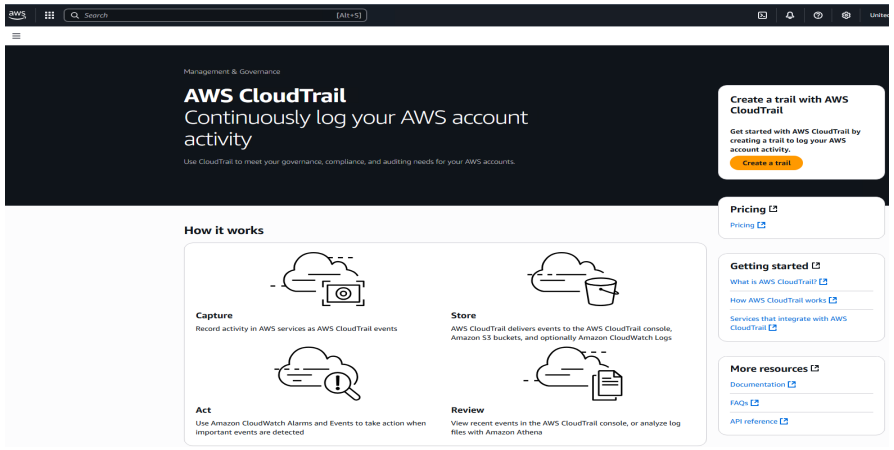
After account creation verify user is prompted for new password



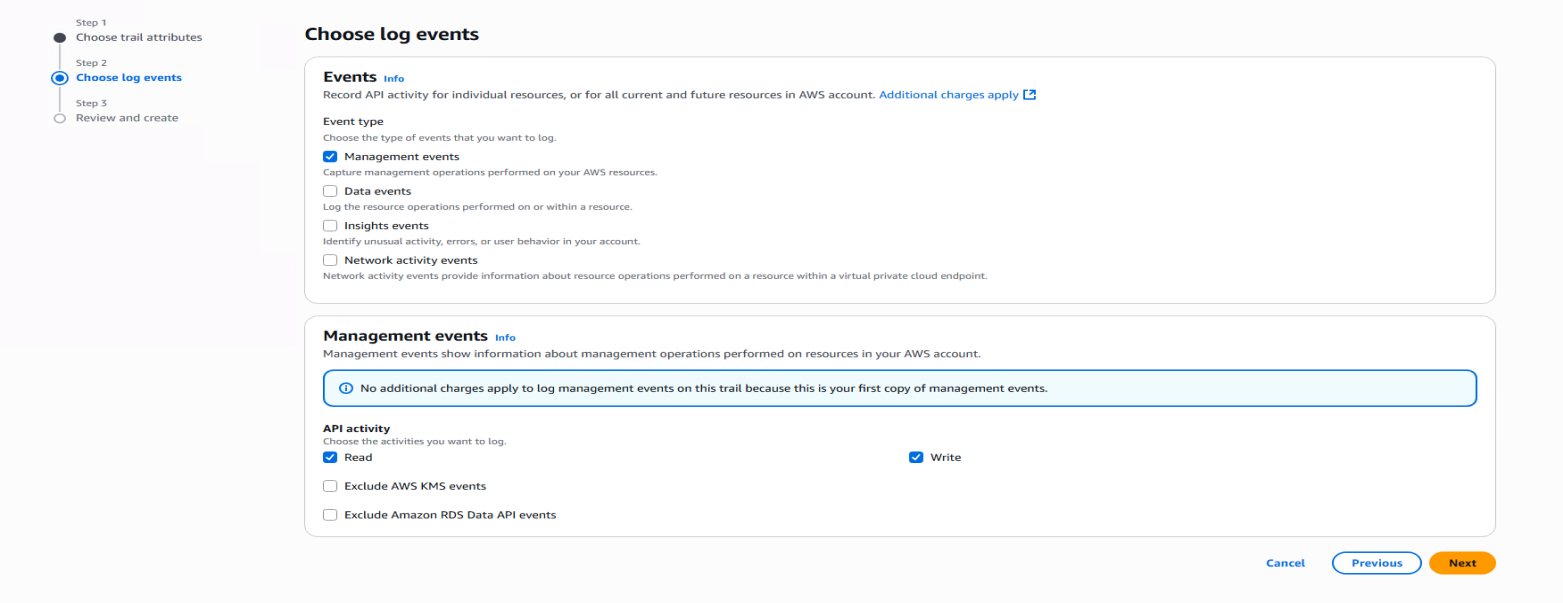
Update AWS Password Security Policy to reflect industry standards



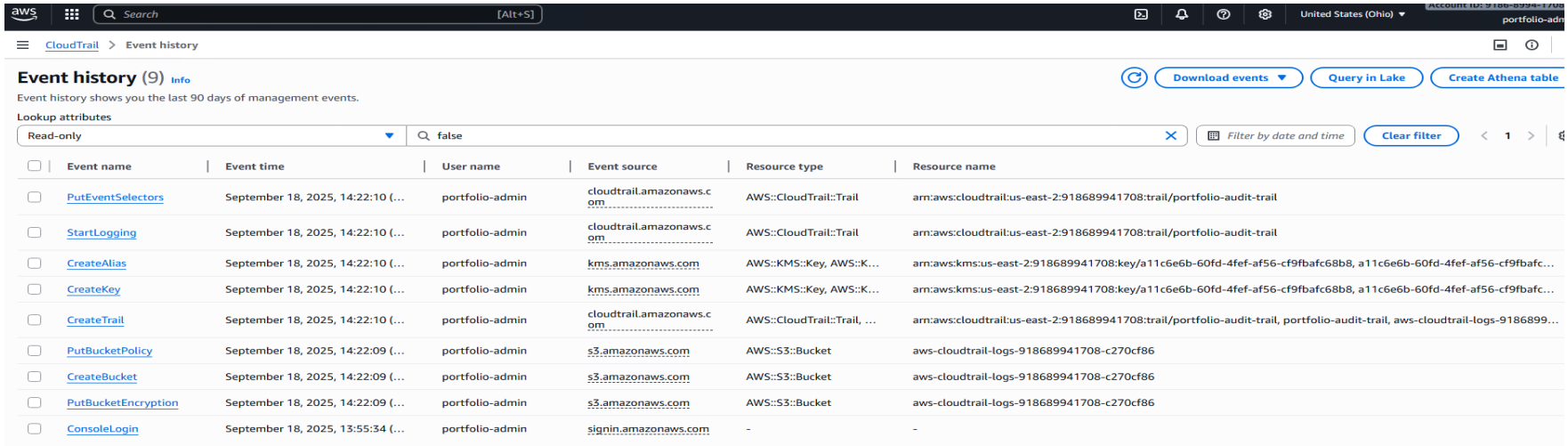
Create AWS CloudTrail - Complete audit log of all API calls - Evidence of security monitoring - Compliance with best practices



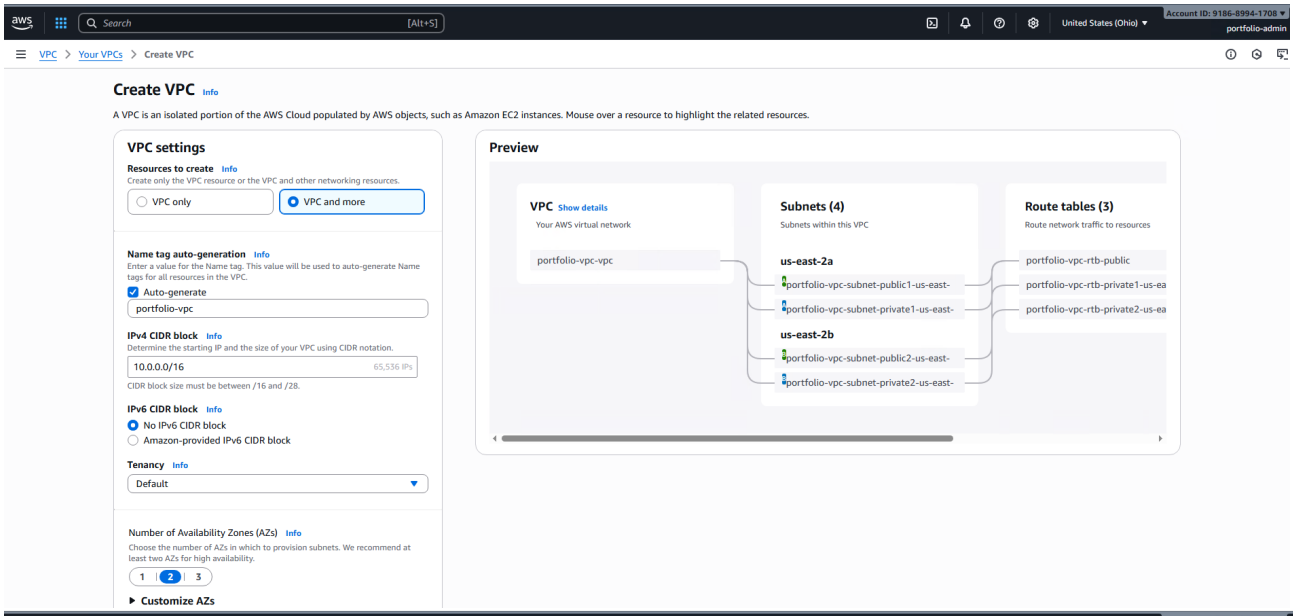
For my portfolio, I configured CloudTrail to capture all management events while optimizing costs by excluding data events. This provides complete visibility into configuration changes and user activities without incurring charges. In production, I would selectively enable data events for sensitive buckets based on data classification.

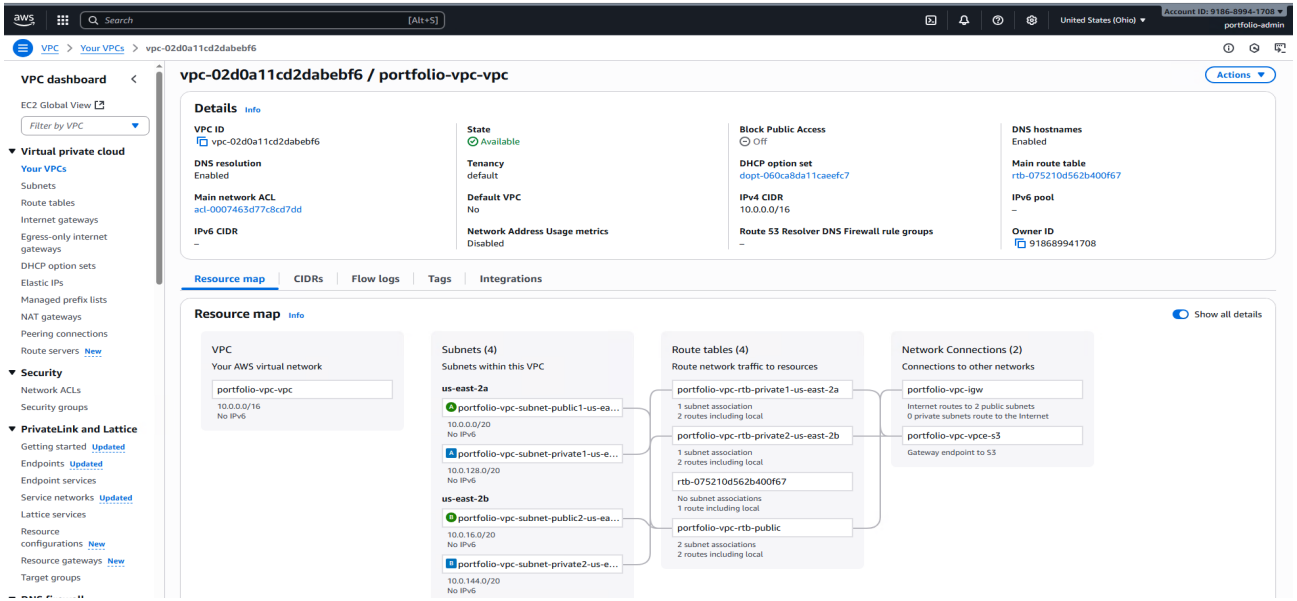


CloudTrail up and running and monitoring logs

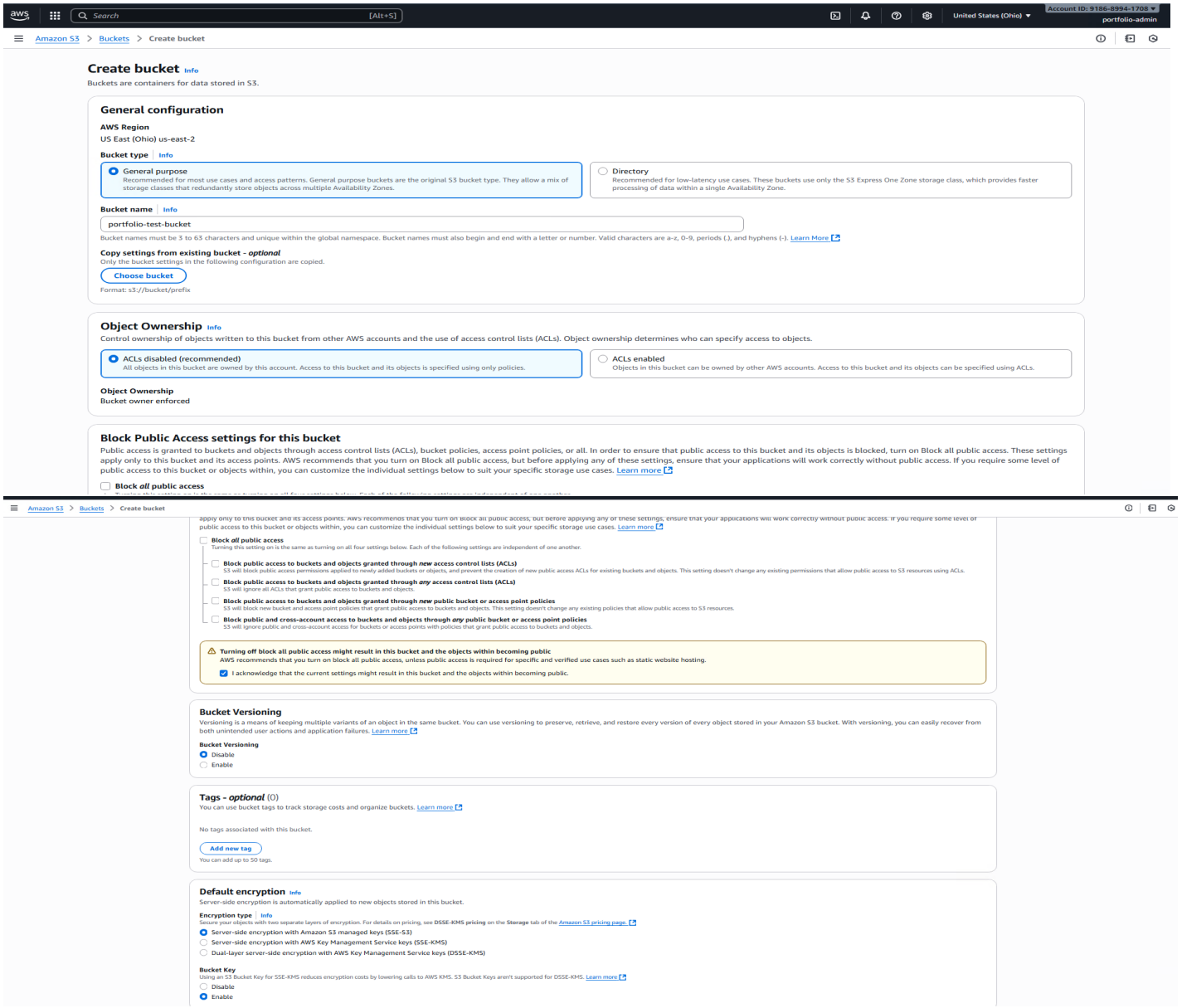


AWS Infrastructure Setup – Create VPC

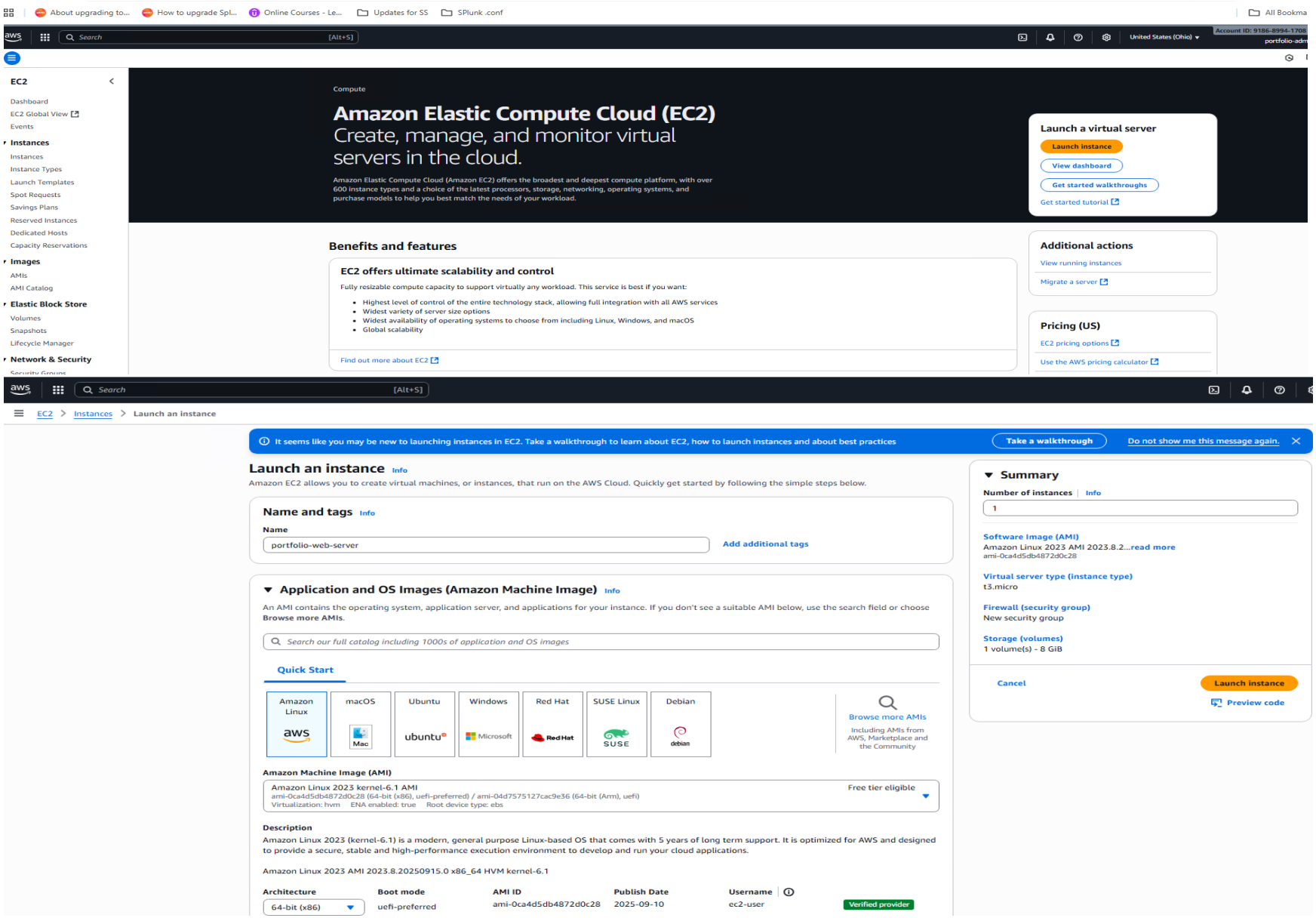




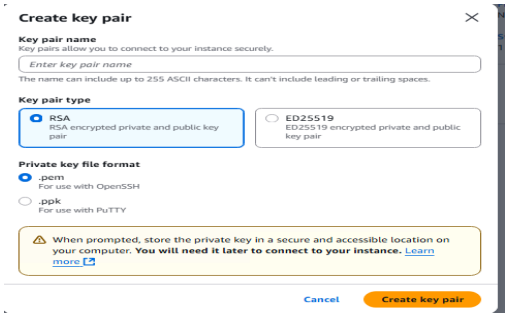
Create S3 Bucket <u>with Security Issues!</u> – Build with deliberate security problems that our scanning tools will detect and that I will remediate.



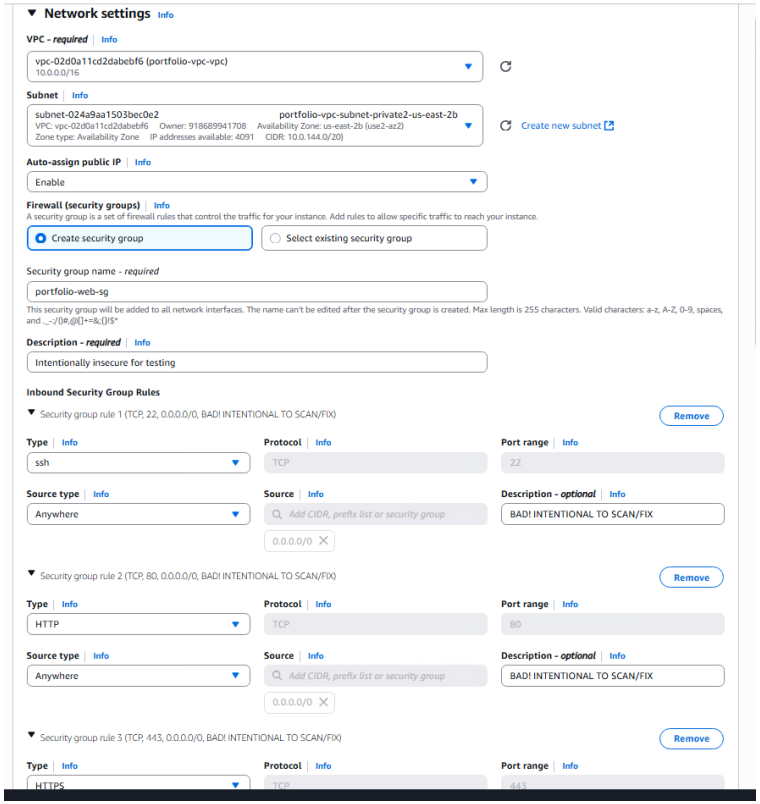
Create EC2 Instance with Security Issues! -

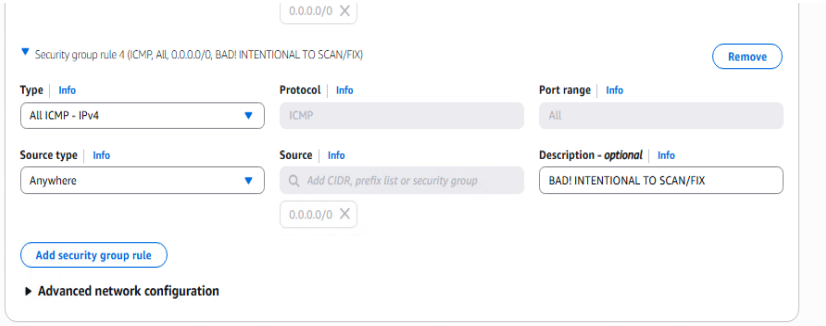


Generate key pair

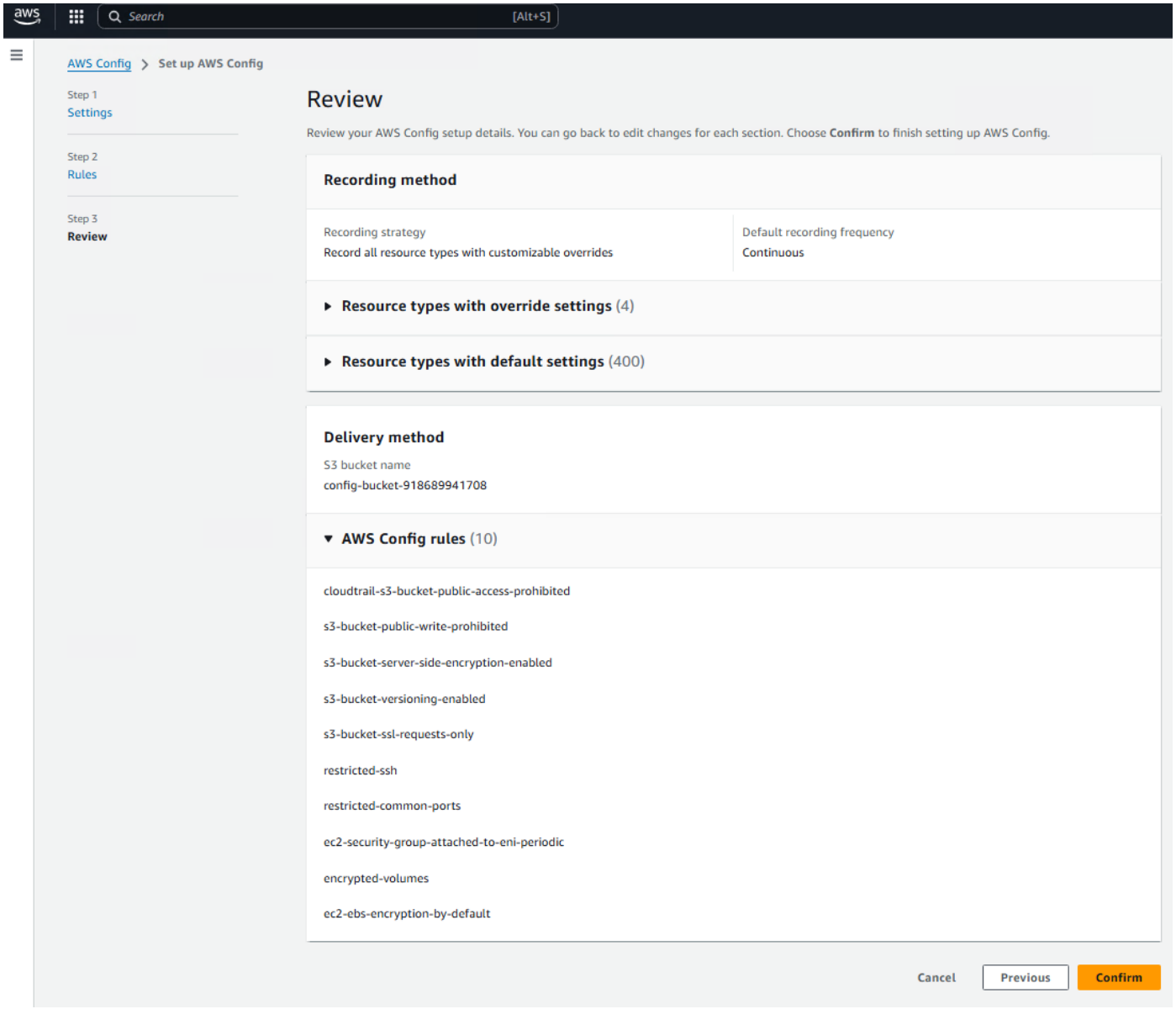


Network settings - BAD! INTENTIONAL TO SCAN/FIX

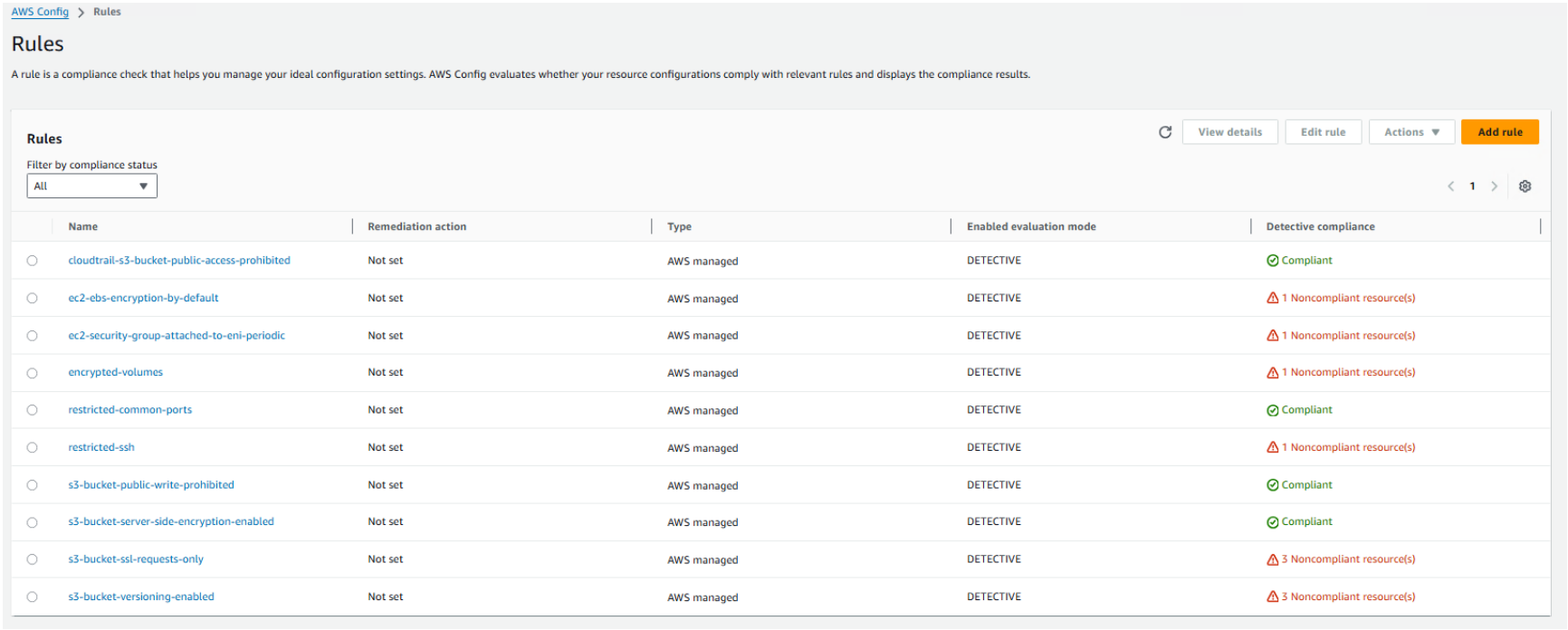




Detect infrastructure issues via AWS Config



AWS Config found our Noncompliant resources



AWS Config > Rules

Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules

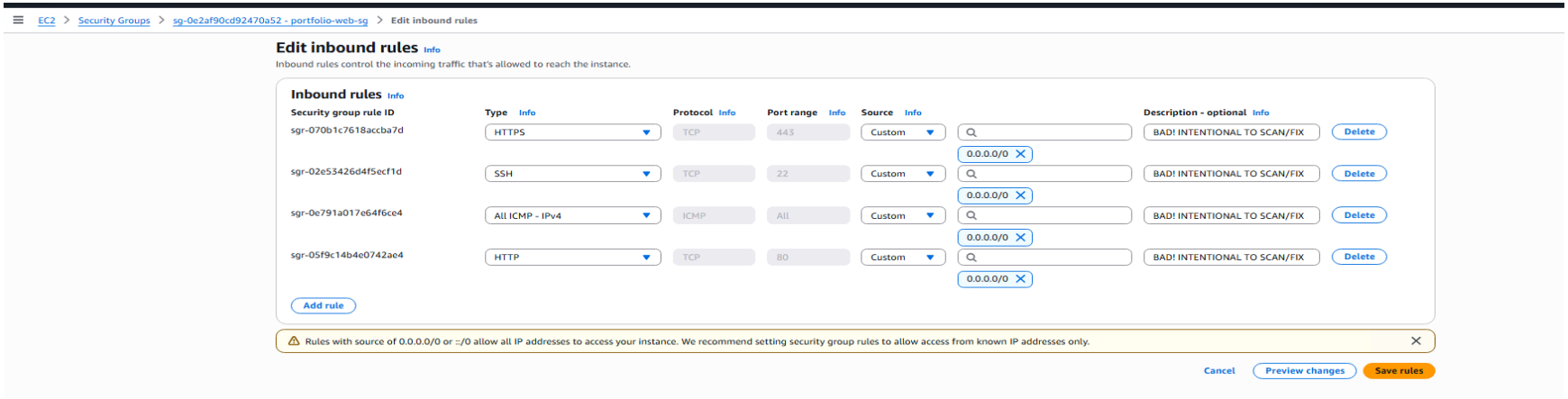
View details | Edit rule | Actions | Add rule

Filter by compliance status: All

1

Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
cloudtrail-s3-bucket-public-access-prohibited	Not set	AWS managed	DETECTIVE	Compliant
ec2-ebs-encryption-by-default	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)
ec2-security-group-attached-to-eni-periodic	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)
encrypted-volumes	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)
restricted-common-ports	Not set	AWS managed	DETECTIVE	Compliant
restricted-ssh	Not set	AWS managed	DETECTIVE	1 Noncompliant resource(s)
s3-bucket-public-write-prohibited	Not set	AWS managed	DETECTIVE	Compliant
s3-bucket-server-side-encryption-enabled	Not set	AWS managed	DETECTIVE	Compliant
s3-bucket-ssl-requests-only	Not set	AWS managed	DETECTIVE	3 Noncompliant resource(s)
s3-bucket-versioning-enabled	Not set	AWS managed	DETECTIVE	3 Noncompliant resource(s)

Time to remediate!



EC2 > Security Groups > sg-0e2af90cd92470a52 - portfolio-web-sg > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-070b1c7618accba7d	HTTPS	TCP	443	Custom	0.0.0.0/0	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-02e53426d4f5ecf1d	SSH	TCP	22	Custom	0.0.0.0/0	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-0e791a017e64f6ce4	All ICMP - IPv4	ICMP	All	Custom	0.0.0.0/0	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-05f9c14b4e0742ae4	HTTP	TCP	80	Custom	0.0.0.0/0	BAD! INTENTIONAL TO SCAN/FIX	Delete

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel | Preview changes | Save rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-070b1c7618accba7d	HTTPS	TCP	443	Custom	0.0.0.0/0	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-02e53426d4f5ecf1d	SSH	TCP	22	My IP	146.6.208.24/32	BAD! INTENTIONAL TO SCAN/FIX	Delete
sgr-05f9c14b4e0742ae4	HTTP	TCP	80	Custom	0.0.0.0/0	BAD! INTENTIONAL TO SCAN/FIX	Delete

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel | Preview changes | Save rules

Edit Block public access (bucket settings) Info

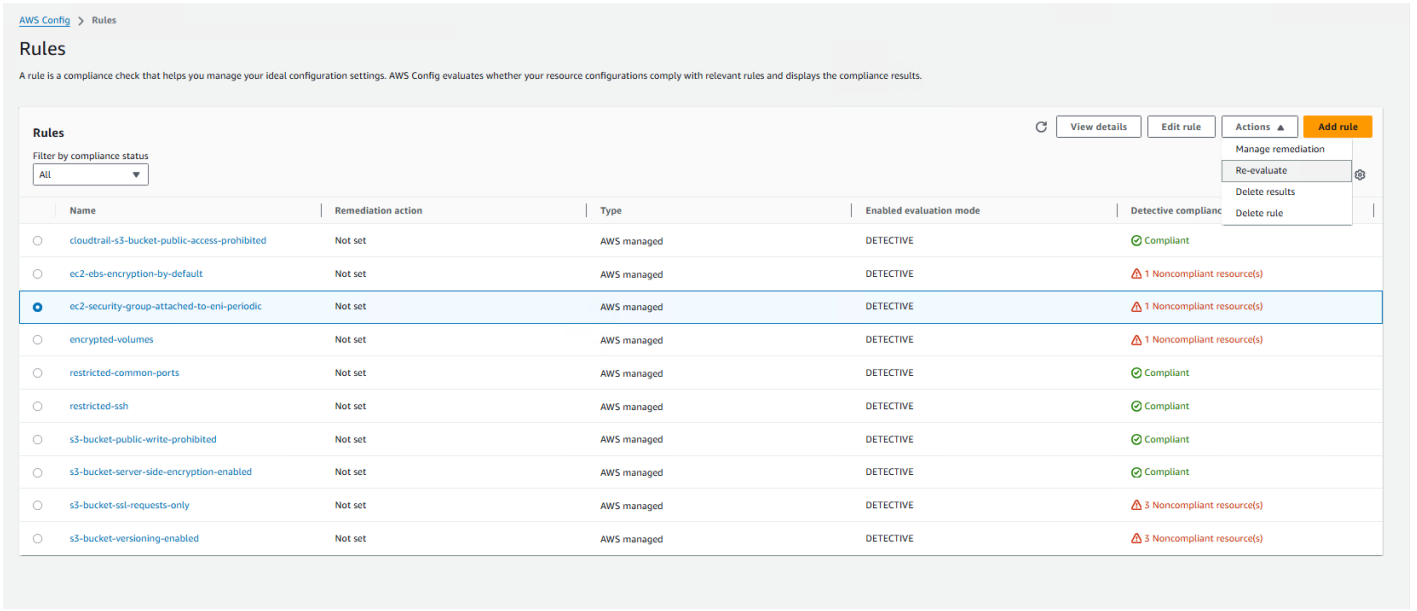
Block public access (bucket settings)

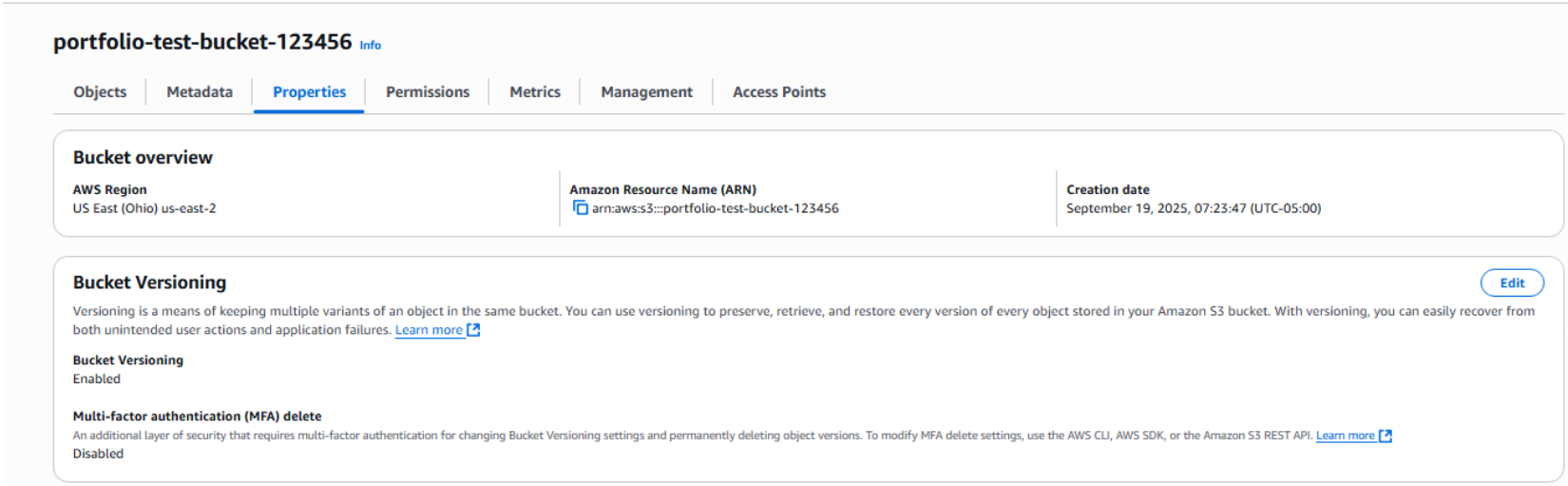
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

- **Block *all* public access**
  Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
  - **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
    S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
    S3 will ignore all ACLs that grant public access to buckets and objects.
  - **Block public access to buckets and objects granted through *new* public bucket or access point policies**
    S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
  - **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
    S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

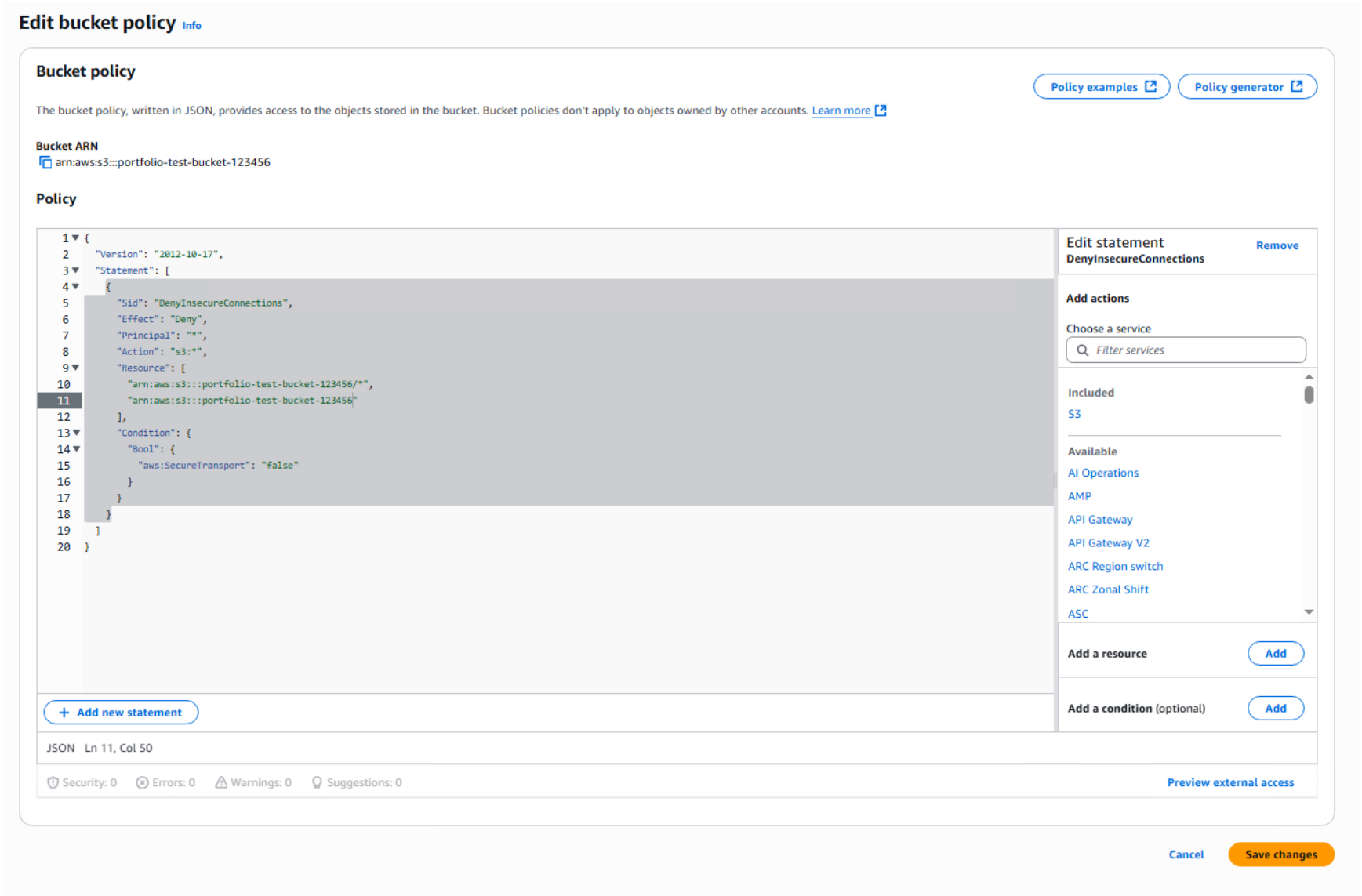
Cancel | Save changes

Issues Remediated now let's Re-evaluate rules.

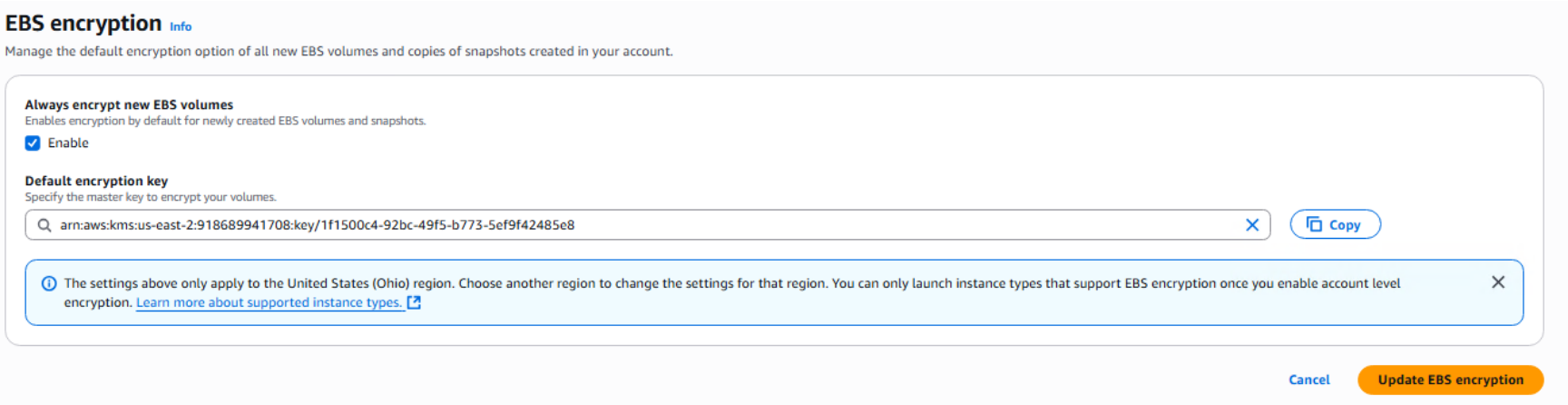

AWS Config > Rules
Rules
A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.
Rules
View details
Edit rule
Actions
Add rule
Manage remediation
Re-evaluate
Delete results
Delete rule
Filter by compliance status
All
Name
Remediation action
Type
Enabled evaluation mode
Detective compliance
cloudtrail-s3-bucket-public-access-prohibited
Not set
AWS managed
DETECTIVE
Compliant
ec2-ebs-encryption-by-default
Not set
AWS managed
DETECTIVE
1 Noncompliant resource(s)
ec2-security-group-attached-to-eni-periodic
Not set
AWS managed
DETECTIVE
1 Noncompliant resource(s)
encrypted-volumes
Not set
AWS managed
DETECTIVE
1 Noncompliant resource(s)
restricted-common-ports
Not set
AWS managed
DETECTIVE
Compliant
restricted-ssh
Not set
AWS managed
DETECTIVE
Compliant
s3-bucket-public-write-prohibited
Not set
AWS managed
DETECTIVE
Compliant
s3-bucket-server-side-encryption-enabled
Not set
AWS managed
DETECTIVE
Compliant
s3-bucket-ssl-requests-only
Not set
AWS managed
DETECTIVE
3 Noncompliant resource(s)
s3-bucket-versioning-enabled
Not set
AWS managed
DETECTIVE
3 Noncompliant resource(s)


portfolio-test-bucket-123456 Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
US East (Ohio) us-east-2
Amazon Resource Name (ARN)
arn:aws:s3:::portfolio-test-bucket-123456
Creation date
September 19, 2025, 07:23:47 (UTC-05:00)
Bucket Versioning
Edit
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Enabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

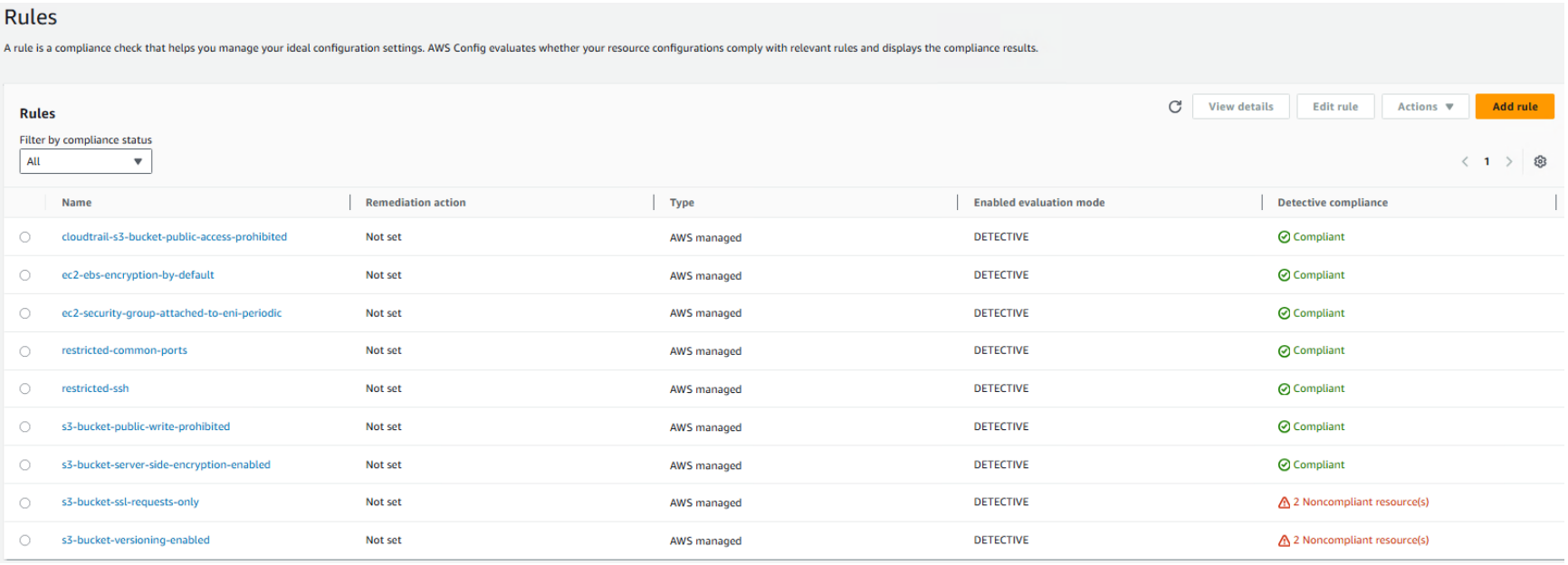
Fix S3 SSL Requests Only



Fix EBS Encryption Default

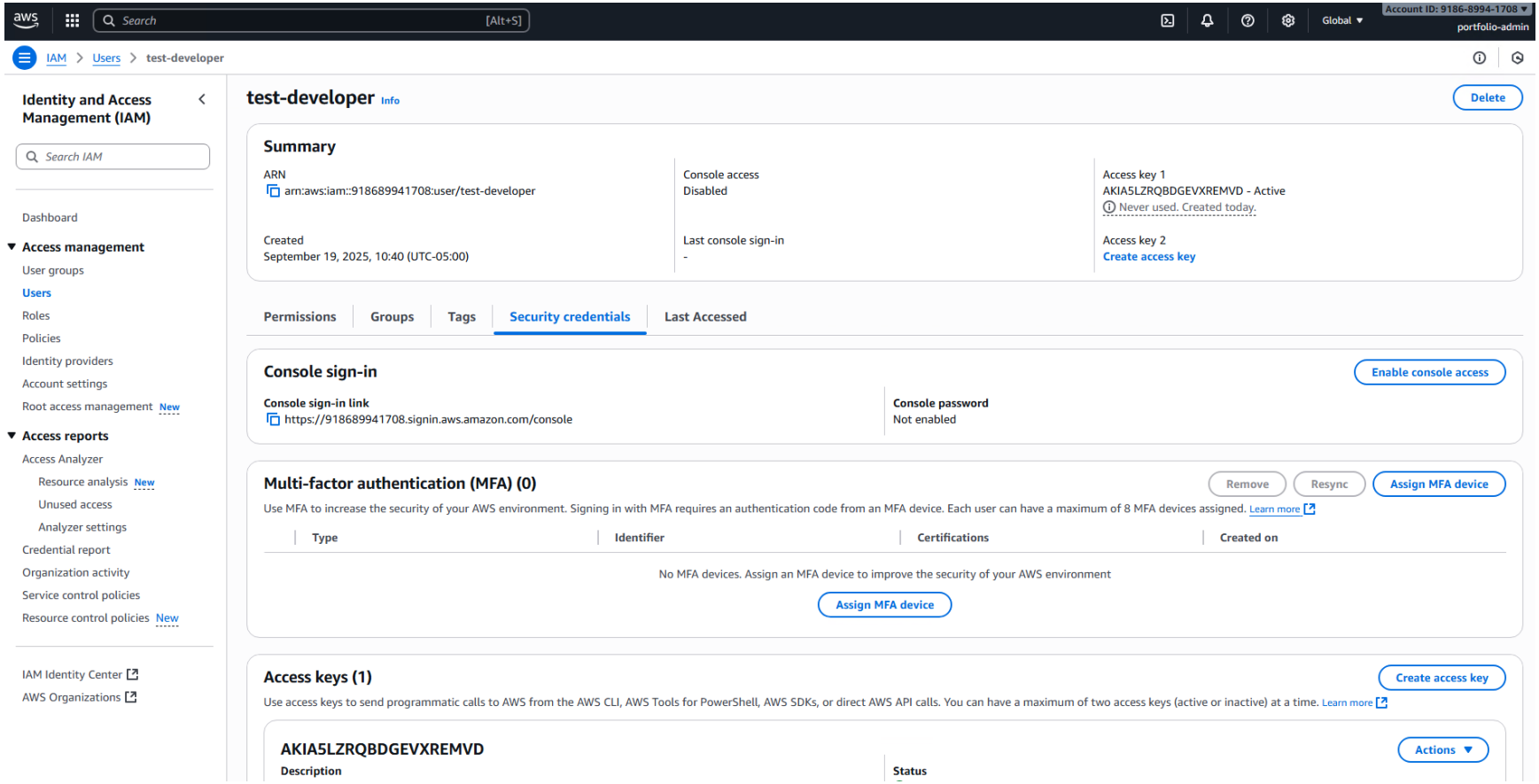


All Noncompliant resources fix on our bucket. The 2 Noncompliant are on the buckets AWS provides. All resources remediated!

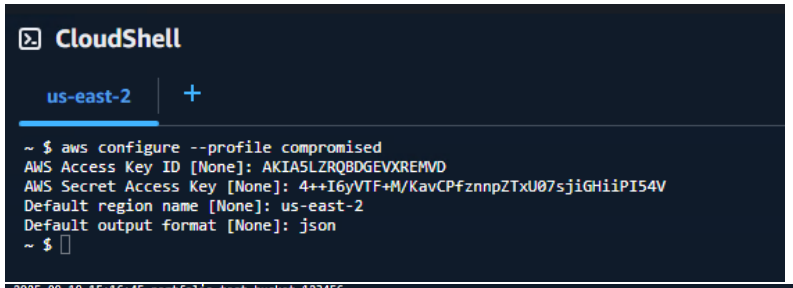


Incident Response Simulation - Compromised IAM Access Keys

Let's create a test IAM user with access keys that we'll "compromise”!

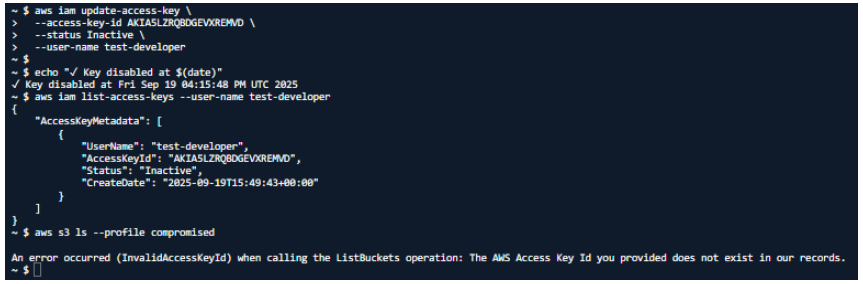


Simulate Attack – Configure compromised credentials via CloudShell

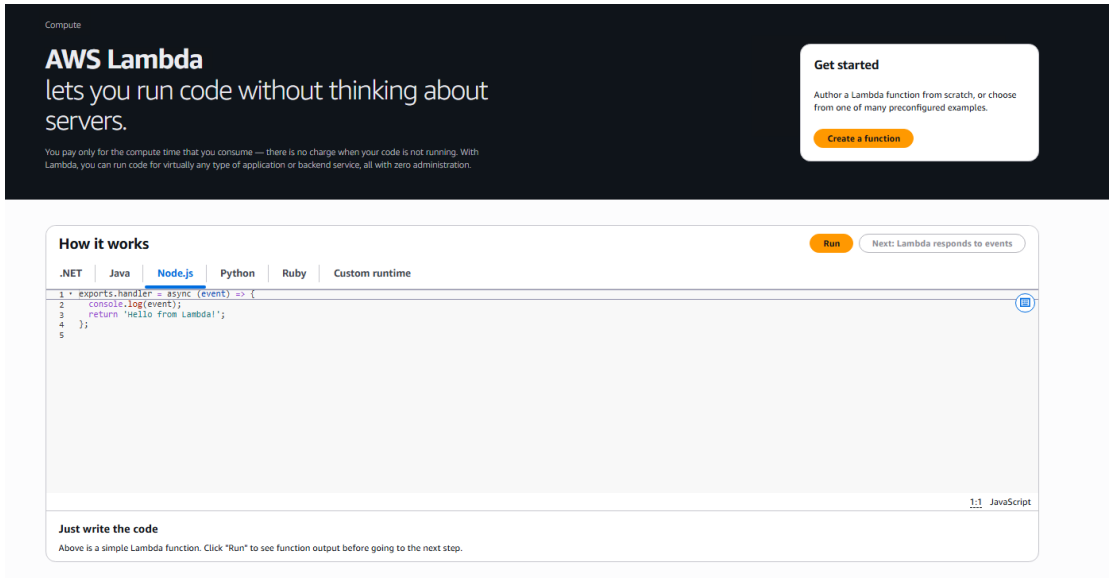


Now let's investigate simulated attack via CloudTrail!

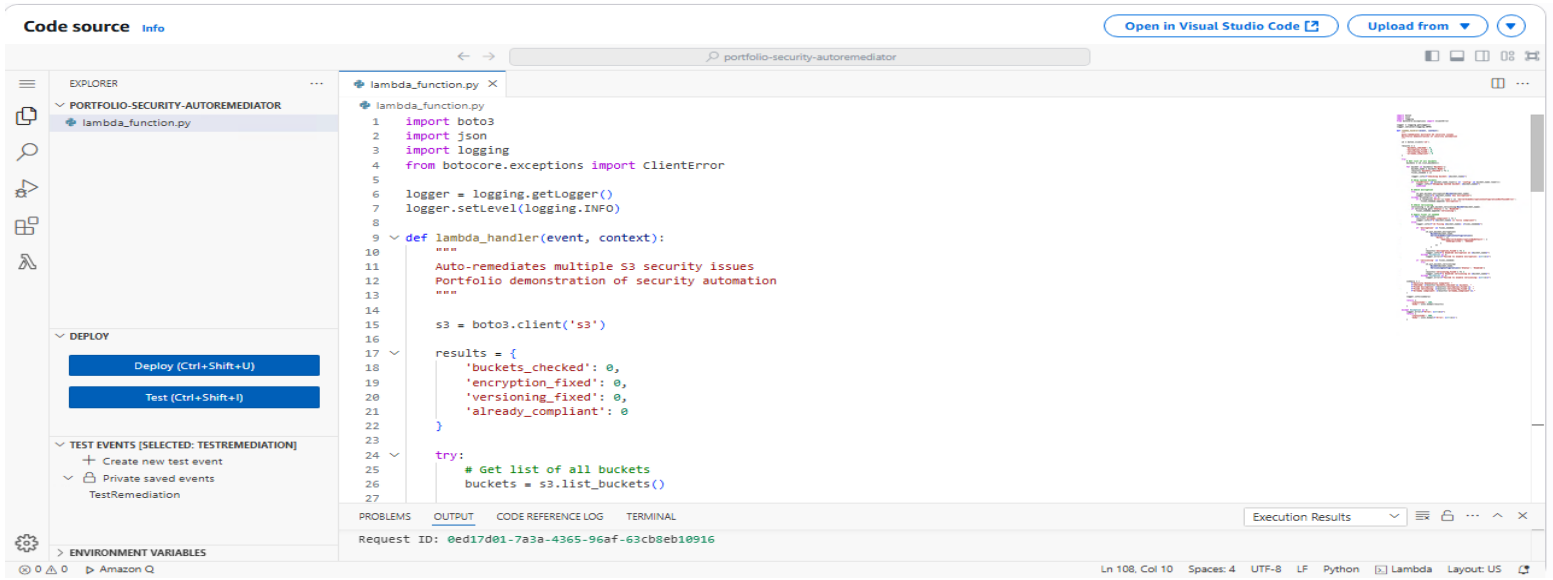
We found user test-developer actions via CloudTrail – We will now remove compromised key!



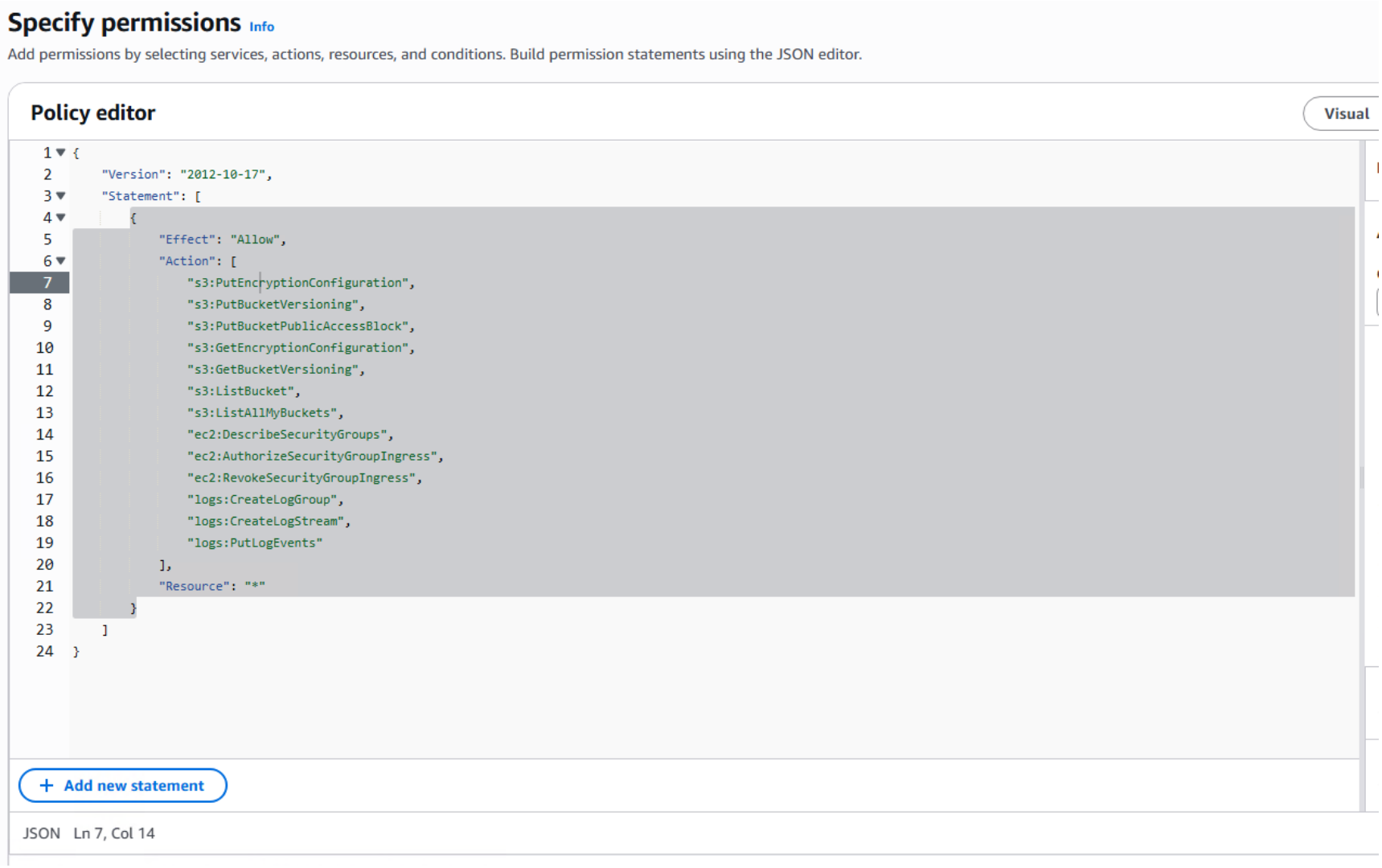
Lambda Security Automation



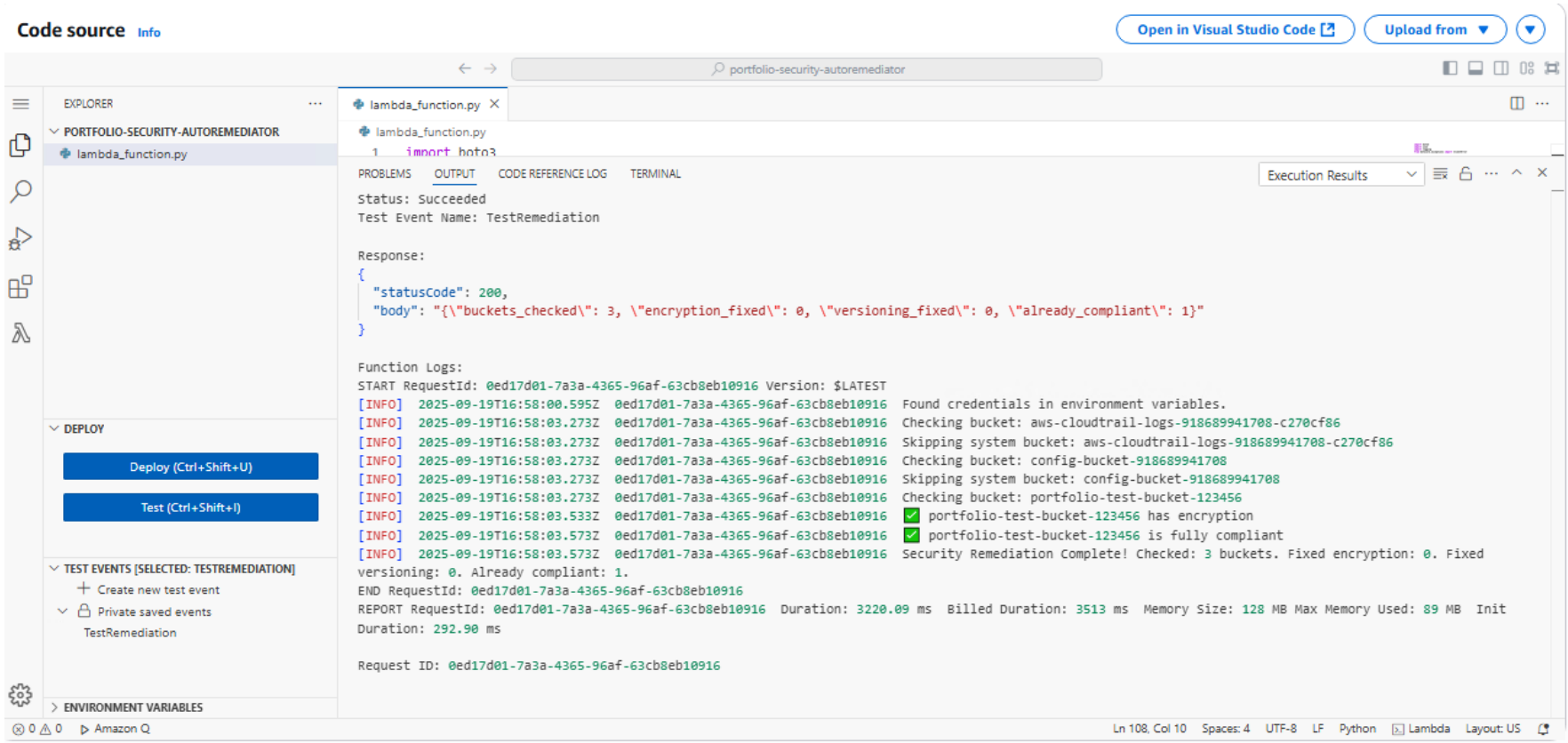
Add Auto-Remediation Code



Create policy via policy editor

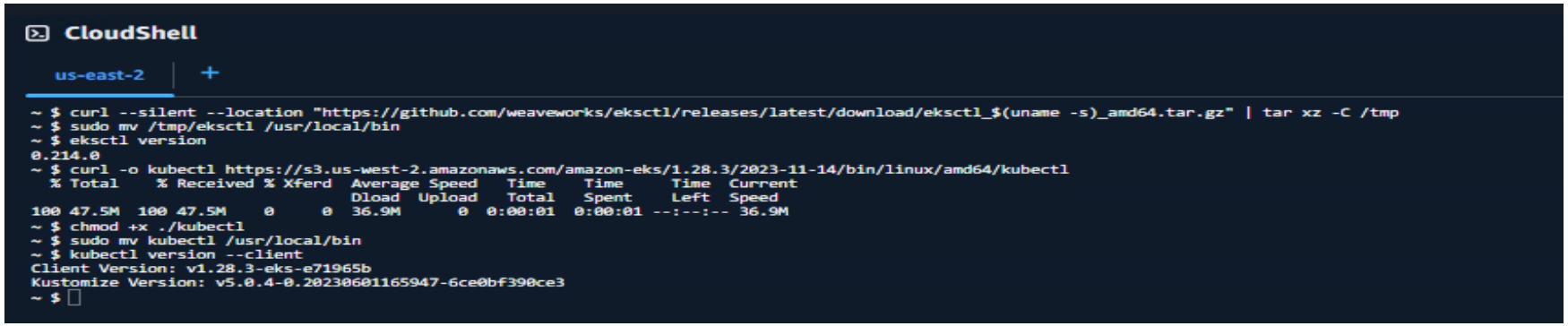


Run test

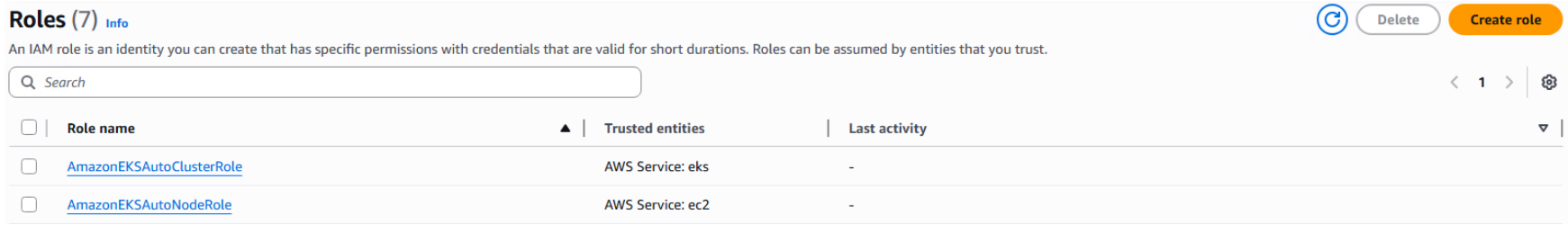

Code source Info
Open in Visual Studio Code
Upload from
portfolio-security-autoremediator
EXPLORER
PORTFOLIO-SECURITY-AUTOREMEDIATOR
lambda_function.py
lambda_function.py
import boto3
DEPLOY
Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)
TEST EVENTS [SELECTED: TESTREMEDIATION]
Create new test event
Private saved events
TestRemediation
ENVIRONMENT VARIABLES
PROBLEMS
OUTPUT
CODE REFERENCE LOG
TERMINAL
Execution Results
Status: Succeeded
Test Event Name: TestRemediation
Response:
{
"statusCode": 200,
"body": "{\"buckets_checked\": 3, \"encryption_fixed\": 0, \"versioning_fixed\": 0, \"already_compliant\": 1}"
}
Function Logs:
START RequestId: 0ed17d01-7a3a-4365-96af-63cb8eb10916 Version: $LATEST
[INFO] 2025-09-19T16:58:00.595Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Found credentials in environment variables.
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Checking bucket: aws-cloudtrail-logs-918689941708-c270cf86
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Skipping system bucket: aws-cloudtrail-logs-918689941708-c270cf86
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Checking bucket: config-bucket-918689941708
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Skipping system bucket: config-bucket-918689941708
[INFO] 2025-09-19T16:58:03.273Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Checking bucket: portfolio-test-bucket-123456
[INFO] 2025-09-19T16:58:03.533Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 ✅ portfolio-test-bucket-123456 has encryption
[INFO] 2025-09-19T16:58:03.573Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 ✅ portfolio-test-bucket-123456 is fully compliant
[INFO] 2025-09-19T16:58:03.573Z 0ed17d01-7a3a-4365-96af-63cb8eb10916 Security Remediation Complete! Checked: 3 buckets. Fixed encryption: 0. Fixed versioning: 0. Already compliant: 1.
END RequestId: 0ed17d01-7a3a-4365-96af-63cb8eb10916
REPORT RequestId: 0ed17d01-7a3a-4365-96af-63cb8eb10916 Duration: 3220.09 ms Billed Duration: 3513 ms Memory Size: 128 MB Max Memory Used: 89 MB Init Duration: 292.90 ms
Request ID: 0ed17d01-7a3a-4365-96af-63cb8eb10916
Ln 108, Col 10
Spaces: 4
UTF-8
LF
Python
Lambda
Layout: US

EKS Security Portfolio Project - AWS Console & CloudShell

Install EKS Management Tools in CloudShell



Create Cluster and new NodeRole and ClusterRole!



Configure cluster

Configuration options - *new* Info

Choose how you would like to configure the cluster.

- (●) **Quick configuration (with EKS Auto Mode) - *new***
  Quickly create a cluster with production-grade default settings. The configuration uses EKS Auto Mode to automate infrastructure tasks like creating nodes and provisioning storage.
- ( ) **Custom configuration**
  To change default settings prior to creation, choose this option. This configuration gives the option to use EKS Auto Mode and customize the cluster's configuration.

Cluster configuration

Name
Use the auto-generated name or enter a unique name for this cluster. This property cannot be changed after the cluster is created.

security-demo-cluster

The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.

Kubernetes version | Info
Select Kubernetes version for this cluster.

1.33

Cluster IAM role | Info
Select the Cluster IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This cannot be changed after the cluster is created. To create a new custom role, follow the instructions in the Amazon EKS User Guide.

AmazonEKSAutoClusterRole — Create recommended role

Node IAM role | Info
Nodes need an EC2 Instance IAM Role to launch and register with a cluster. To create a new custom role, follow the instructions in the Amazon EKS User Guide.

AmazonEKSAutoNodeRole — Create recommended role

VPC | Info
Select a VPC to use for your EKS cluster resources.

vpc-02d0a11cd2dabebf6 | portfolio-vpc-vpc — Create VPC

Subnets Info
Choose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the VPC console.

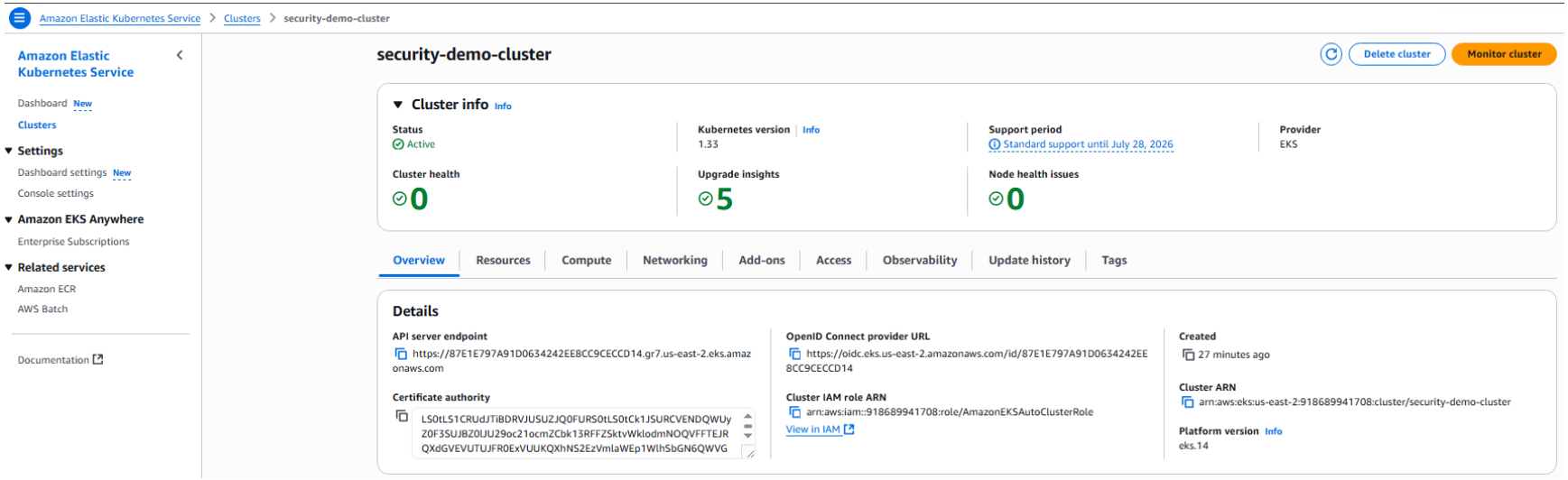
Select subnets — Clear selected subnets

- subnet-024a9aa1503bec0e2 | portfolio-vpc-subnet-private2-us-east-2b
  us-east-2b 10.0.144.0/20 Type: Private
- subnet-0b8072fbd60258d52 | portfolio-vpc-subnet-private1-us-east-2a
  us-east-2a 10.0.128.0/20 Type: Private

▶ **View quick configuration defaults**

Cancel Create

Cluster Created!



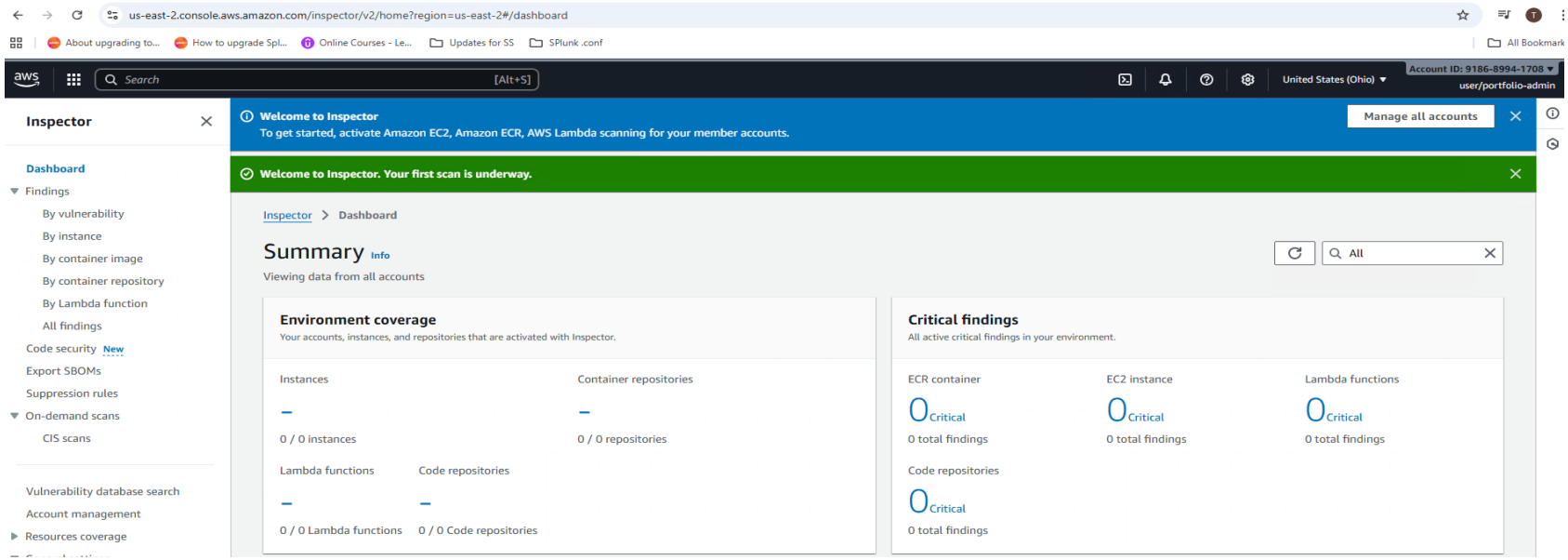
Connect kubectl to your new cluster

```
~ $ aws eks update-kubeconfig --region us-east-2 --name security-demo-cluster
Added new context arn:aws:eks:us-east-2:918689941708:cluster/security-demo-cluster to /home/cloudshell-user/.kube/config
~ $
```

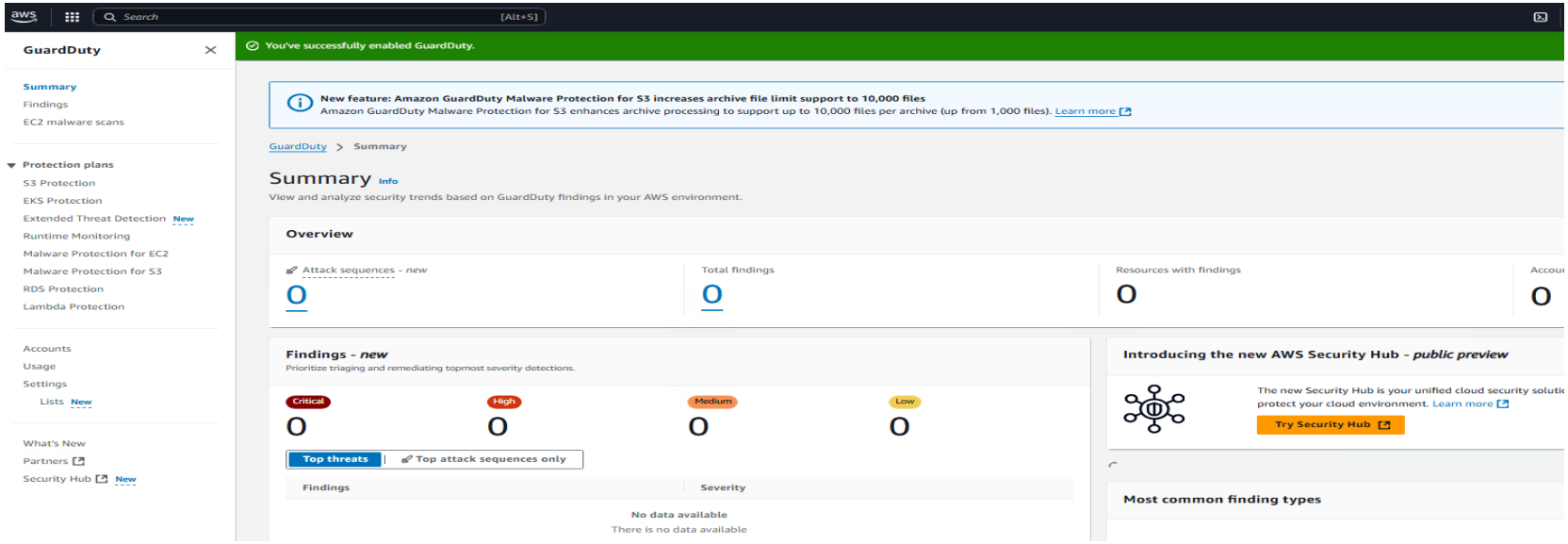
verify access

```
~ $ kubectl get nodes
E0919 18:17:53.197581     251 memcache.go:287] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:17:53.213734     251 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:17:53.219792     251 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:17:53.222433     251 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
NAME                STATUS   ROLES    AGE   VERSION
i-07a4e58d2bb0c3c48   Ready    <none>   14m   v1.33.1-eks-f5be8fb
~ $ kubectl get pods --all-namespaces
E0919 18:18:10.233291     260 memcache.go:287] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:18:10.246051     260 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:18:10.248585     260 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
E0919 18:18:10.254128     260 memcache.go:121] couldn't get resource list for metrics.k8s.io/v1beta1: the server is currently unable to handle the request
NAMESPACE     NAME                              READY   STATUS             RESTARTS   AGE
kube-system   metrics-server-7d7546bdc4-rfvdq   0/1     ImagePullBackOff   0          14m
kube-system   metrics-server-7d7546bdc4-xxh2n   0/1     ImagePullBackOff   0          14m
~ $
```

Activate Amazon Inspector



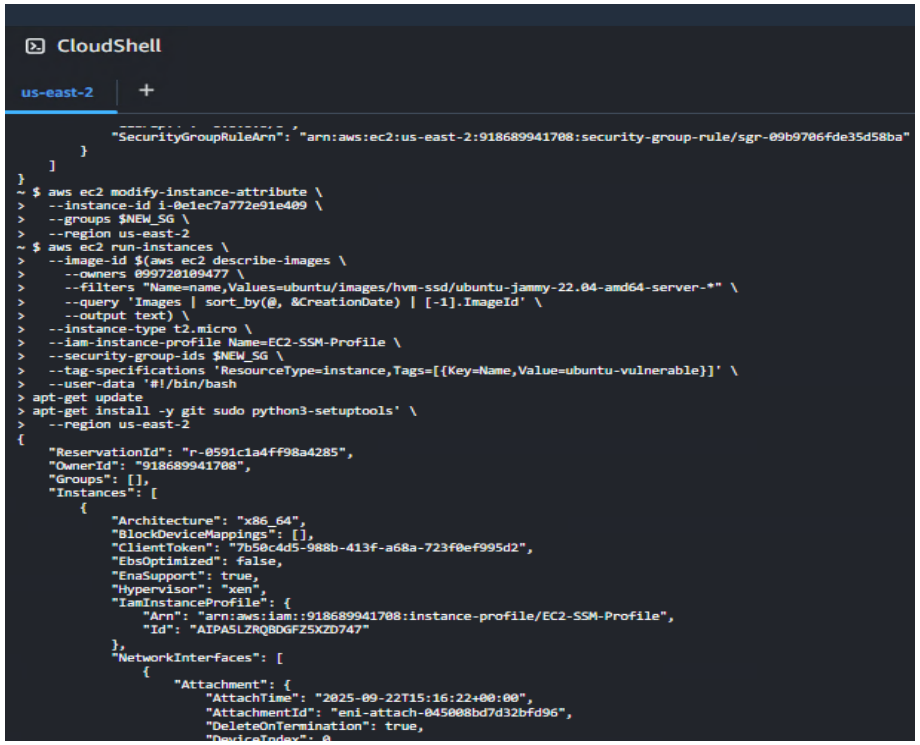
Activate Amazon GuardDuty



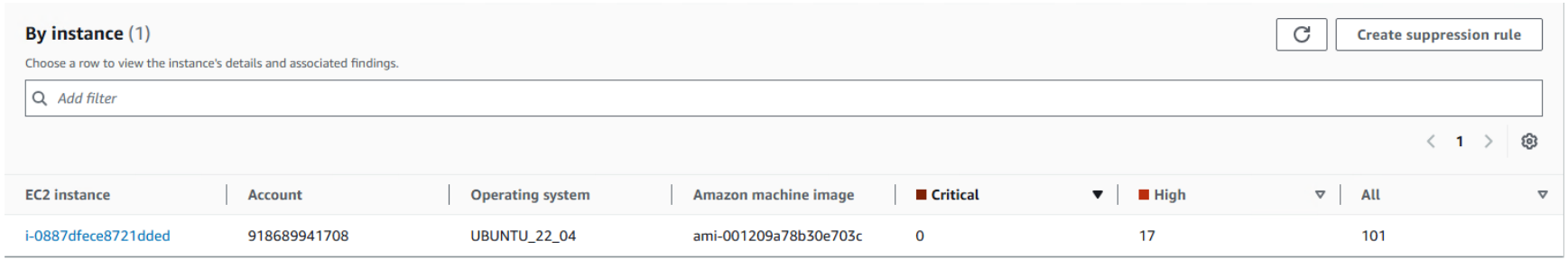
Verify GuardDuty Active – Via CloudShell CLI

```
~ $ clear
~ $ kubectl logs -n amazon-guardduty aws-guardduty-agent-45nv7 --tail=20
2025-09-22T13:20:51.191788Z  INFO amzn_guardduty_agent: GuardDuty agent starting with 8 worker thread(s) and 100 max blocking threads.
2025-09-22T13:20:51.216047Z  INFO amzn_guardduty_agent: Agent fingerprint: 64b651fb444b18ae8e6813e8895ac771d9a7a55c3c58448e9b1c002d19ebb4c9
2025-09-22T13:20:51.216275Z  INFO amzn_guardduty_agent: Agent config for Component(s): AgentConfig { component_channel_size: 100, ingestion_endpoin
rocket_(EKS_Auto,_Standard)_2025.9.11_(aws-k8s-1.33-standard)", os_version: OSUnknown, kernel_version: LinuxKernel6_12, region: None, stage: None,
ity: 16384, pid_namespace_cache_capacity: 1024, pre_suppressor_cache_capacity: 32768, post_suppressor_cache_capacity: 32768, docker_socket_file_pat
iod: 600s, scan_for_task_metadata_period: 600s, eks_cluster_name_env_var: "CLUSTER_NAME", max_file_size_to_hash: 536870912, proc_folder_path: "/hos
calculation_timeout: 5s, file_open_timeout: 1.5s, mnt_ns_pids_map_capacity: 1024, pid_set_cap: 32 }

2025-09-22T13:20:51.231903Z  INFO amzn_guardduty_agent::dependency_checks: Dependency checks complete.
2025-09-22T13:20:51.235825Z  INFO amzn_guardduty_agent::dependency_checks: Health check: EXECUTABLE (connectivity OK)
2025-09-22T13:20:51.240555Z  INFO amzn_guardduty_agent_data_model::schema: Event schema rabin fingerprint = "b6ce8be84715ced5"
2025-09-22T13:20:51.240715Z  INFO amzn_guardduty_agent_data_model::schema: Container schema rabin fingerprint = "5a675cafcf525a5d"
2025-09-22T13:20:51.240796Z  INFO amzn_guardduty_agent_data_model::schema: Pod schema rabin fingerprint = "8504ac7492b3cb8b"
2025-09-22T13:20:51.240877Z  INFO amzn_guardduty_agent_data_model::schema: Task schema rabin fingerprint = "195a73fa36862425"
2025-09-22T13:20:51.244256Z  INFO amzn_guardduty_agent: GuardDuty agent started ...
2025-09-22T13:20:51.244265Z  INFO amzn_guardduty_agent: Type Ctrl+C to terminate
2025-09-22T13:20:51.940027Z  INFO amzn_guardduty_agent_core::decorator: Decorator started ...
```

Generate Package Vulnerabilities



Check Amazon Inspector for Vulnerabilities



By instance (1)

Choose a row to view the instance's details and associated findings.

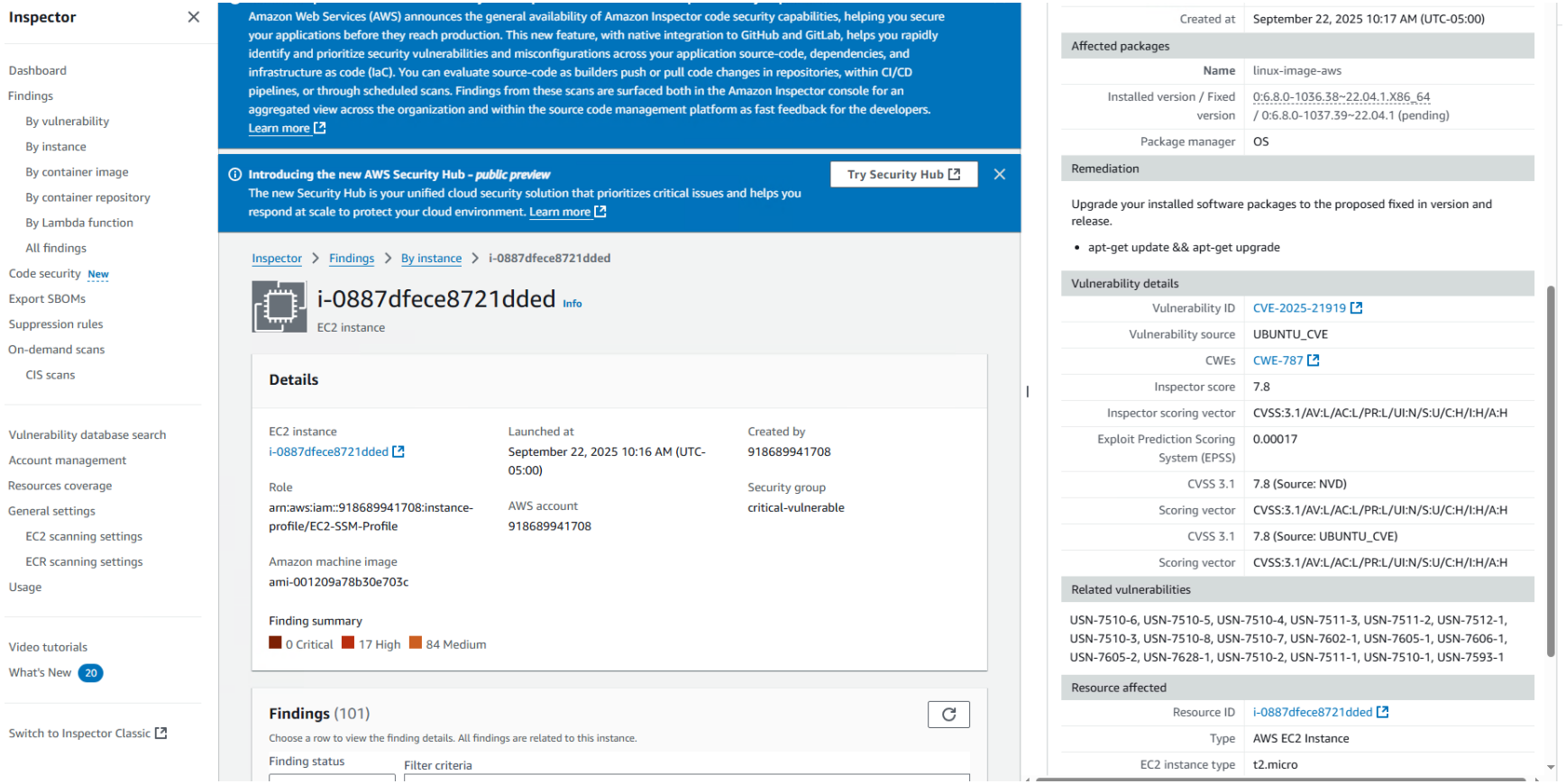
Create suppression rule

Add filter

1

EC2 instance	Account	Operating system	Amazon machine image	Critical	High	All
i-0887dfece8721dded	918689941708	UBUNTU_22_04	ami-001209a78b30e703c	0	17	101

Check Remediation fix



Inspector

Dashboard
Findings
By vulnerability
By instance
By container image
By container repository
By Lambda function
All findings
Code security New
Export SBOMs
Suppression rules
On-demand scans
CIS scans
Vulnerability database search
Account management
Resources coverage
General settings
EC2 scanning settings
ECR scanning settings
Usage
Video tutorials
What's New 20
Switch to Inspector Classic

Amazon Web Services (AWS) announces the general availability of Amazon Inspector code security capabilities, helping you secure your applications before they reach production. This new feature, with native integration to GitHub and GitLab, helps you rapidly identify and prioritize security vulnerabilities and misconfigurations across your application source-code, dependencies, and infrastructure as code (IaC). You can evaluate source-code as builders push or pull code changes in repositories, within CI/CD pipelines, or through scheduled scans. Findings from these scans are surfaced both in the Amazon Inspector console for an aggregated view across the organization and within the source code management platform as fast feedback for the developers. Learn more

Introducing the new AWS Security Hub - *public preview*
The new Security Hub is your unified cloud security solution that prioritizes critical issues and helps you respond at scale to protect your cloud environment. Learn more
Try Security Hub

Inspector > Findings > By instance > i-0887dfece8721dded

i-0887dfece8721dded Info
EC2 instance

Details

EC2 instance: i-0887dfece8721dded
Launched at: September 22, 2025 10:16 AM (UTC-05:00)
Created by: 918689941708
Role: arn:aws:iam::918689941708:instance-profile/EC2-SSM-Profile
AWS account: 918689941708
Security group: critical-vulnerable
Amazon machine image: ami-001209a78b30e703c
Finding summary: 0 Critical 17 High 84 Medium

Findings (101)

Choose a row to view the finding details. All findings are related to this instance.

Finding status
Filter criteria

Created at	September 22, 2025 10:17 AM (UTC-05:00)
Affected packages	
Name	linux-image-aws
Installed version / Fixed version	0:6.8.0-1036.38~22.04.1.X86_64 / 0:6.8.0-1037.39~22.04.1 (pending)
Package manager	OS
Remediation	

Upgrade your installed software packages to the proposed fixed in version and release.

- apt-get update && apt-get upgrade

Vulnerability details	
Vulnerability ID	CVE-2025-21919
Vulnerability source	UBUNTU_CVE
CWEs	CWE-787
Inspector score	7.8
Inspector scoring vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Exploit Prediction Scoring System (EPSS)	0.00017
CVSS 3.1	7.8 (Source: NVD)
Scoring vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS 3.1	7.8 (Source: UBUNTU_CVE)
Scoring vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Related vulnerabilities	

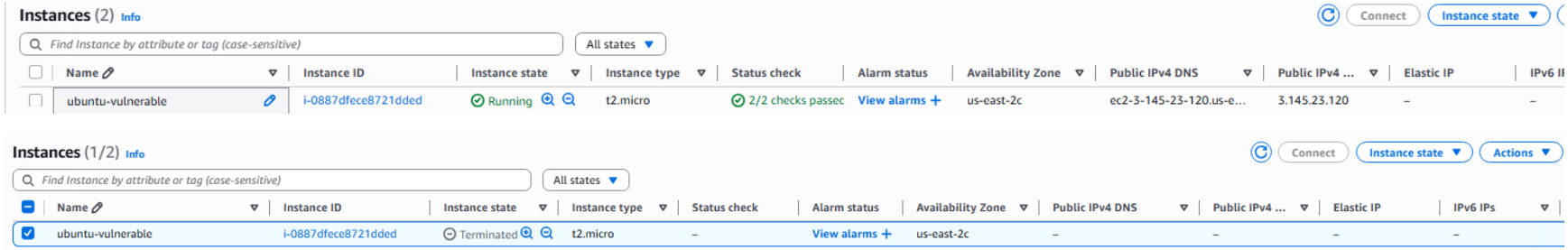
USN-7510-6, USN-7510-5, USN-7510-4, USN-7511-3, USN-7511-2, USN-7512-1, USN-7510-3, USN-7510-8, USN-7510-7, USN-7602-1, USN-7605-1, USN-7606-1, USN-7605-2, USN-7628-1, USN-7510-2, USN-7511-1, USN-7510-1, USN-7593-1

Resource affected	
Resource ID	i-0887dfece8721dded
Type	AWS EC2 Instance
EC2 instance type	t2.micro

Verify there is a Remediation patch available if not document. (Vulnerable, NO patch!)

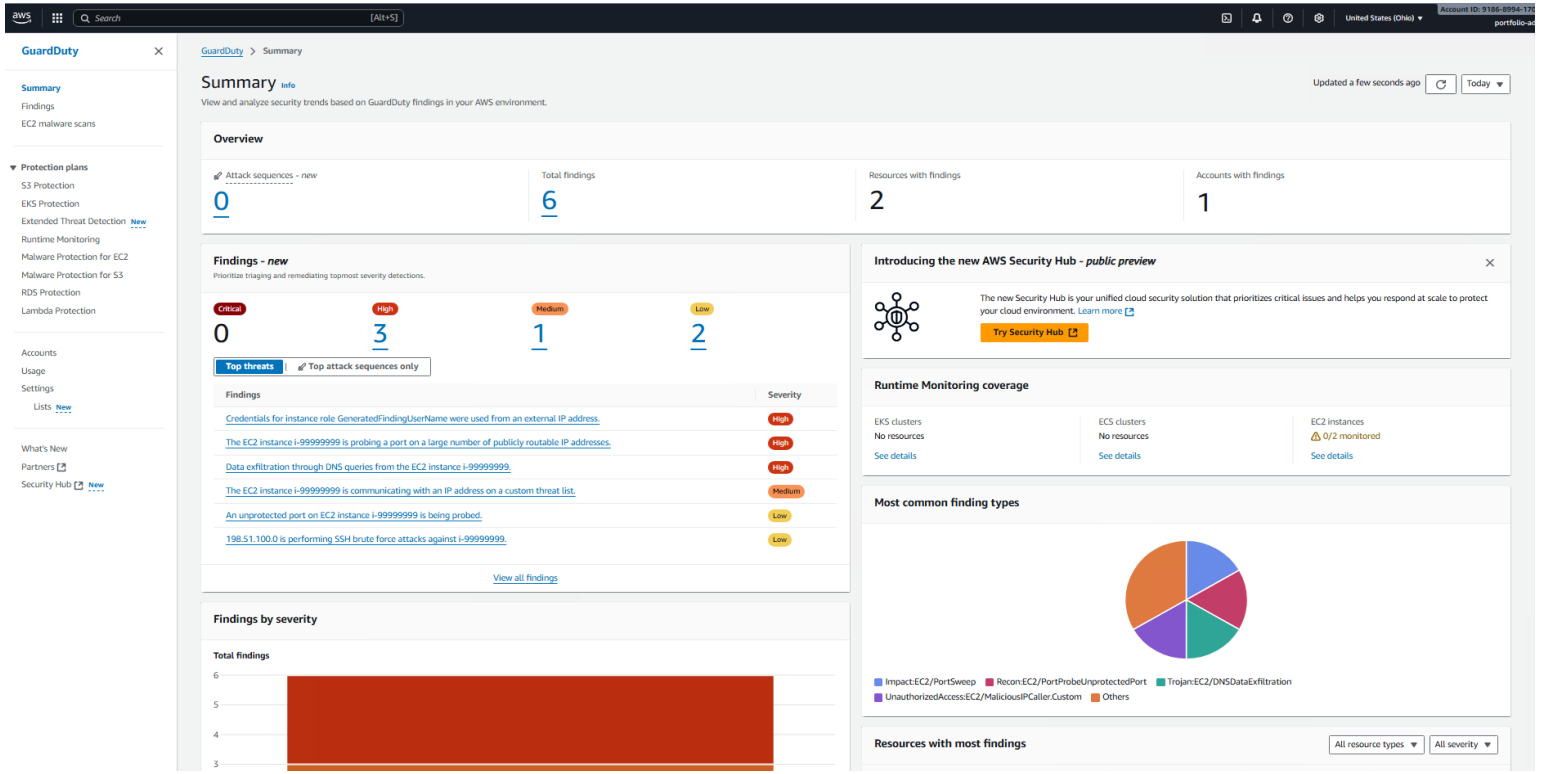
linux-aws-6.8	25.04 plucky	Not in release
	24.04 LTS noble	Not in release
	22.04 LTS jammy	Vulnerable, work in progress
	20.04 LTS focal	Not in release
	18.04 LTS bionic	Not in release
	16.04 LTS xenial	Not in release
	14.04 LTS trusty	Not in release
linux-hwe-6.8	25.04 plucky	Not in release
	24.04 LTS noble	Not in release
	22.04 LTS jammy	Vulnerable, work in progress
	20.04 LTS focal	Not in release
	18.04 LTS bionic	Not in release
	16.04 LTS xenial	Not in release
	14.04 LTS trusty	Not in release

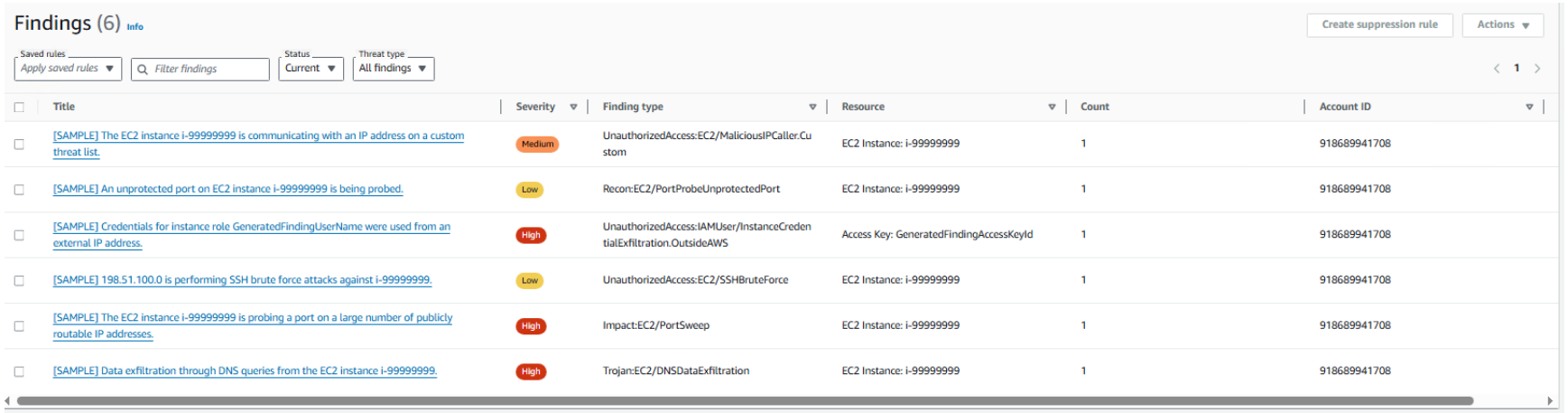
No patch so lets remove Instance



Generate Sample finings for GuardDuty

```
~ $ DETECTOR_ID=$(aws guardduty list-detectors --query 'DetectorIds[0]' --output text --region us-east-
~ $
~ $ echo "Detector ID: $DETECTOR_ID"
Detector ID: 7eccb8b03cff3a081bf7dc7204c9a55c
~ $ celar
-bash: celar: command not found
~ $ clear
~ $ aws guardduty create-sample-findings \
>   --detector-id 7eccb8b03cff3a081bf7dc7204c9a55c \
>   --finding-types \
>     "Recon:EC2/PortProbeUnprotectedPort" \
>     "UnauthorizedAccess:EC2/SSHBruteForce" \
>     "UnauthorizedAccess:EC2/MaliciousIPCaller.Custom" \
>     "CryptoCurrency:EC2/BitcoinTool.B!DNS" \
-bash: !DNS: event not found
>     "Trojan:EC2/DNSDataExfiltration" \
>     "Impact:EC2/PortSweep" \
>     "UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS" \
>   --region us-east-2
~ $
```





Findings (6) Info

Create suppression rule | Actions

Saved rules: Apply saved rules | Filter findings | Status: Current | Threat type: All findings

1

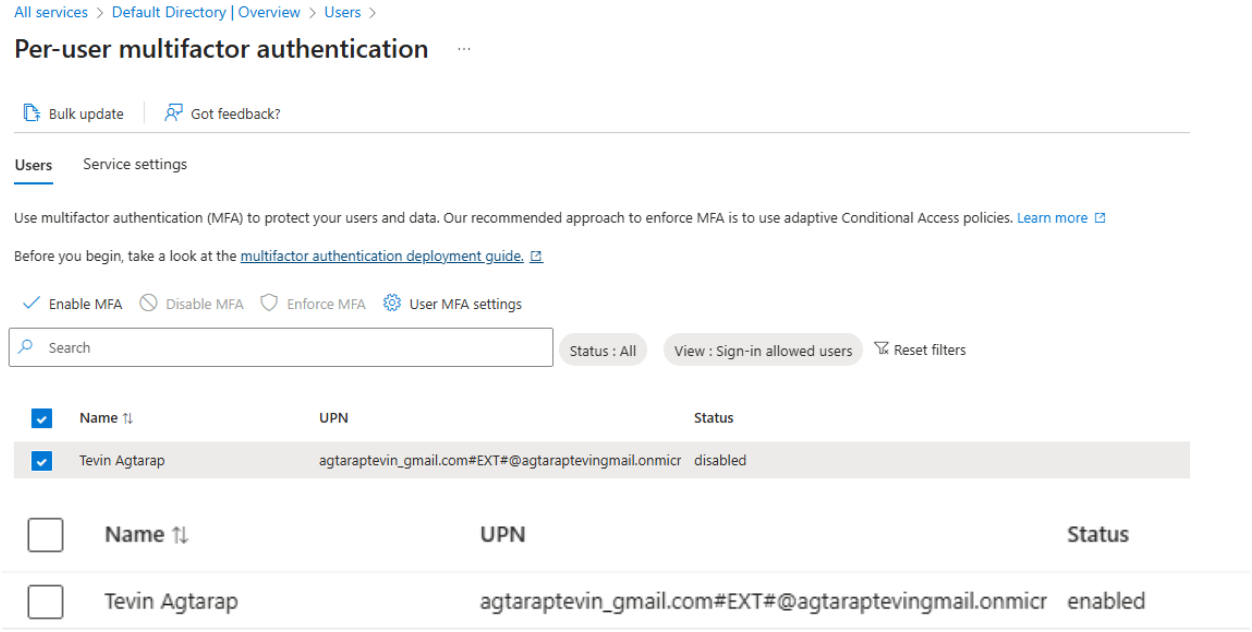
Title	Severity	Finding type	Resource	Count	Account ID
[SAMPLE] The EC2 instance i-99999999 is communicating with an IP address on a custom threat list.	Medium	UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2 Instance: i-99999999	1	918689941708
[SAMPLE] An unprotected port on EC2 instance i-99999999 is being probed.	Low	Recon:EC2/PortProbeUnprotectedPort	EC2 Instance: i-99999999	1	918689941708
[SAMPLE] Credentials for instance role GeneratedFindingUserName were used from an external IP address.	High	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Access Key: GeneratedFindingAccessKeyId	1	918689941708
[SAMPLE] 198.51.100.0 is performing SSH brute force attacks against i-99999999.	Low	UnauthorizedAccess:EC2/SSHBruteForce	EC2 Instance: i-99999999	1	918689941708
[SAMPLE] The EC2 instance i-99999999 is probing a port on a large number of publicly routable IP addresses.	High	Impact:EC2/PortSweep	EC2 Instance: i-99999999	1	918689941708
[SAMPLE] Data exfiltration through DNS queries from the EC2 instance i-99999999.	High	Trojan:EC2/DNSDataExfiltration	EC2 Instance: i-99999999	1	918689941708

Azure Security Portfolio

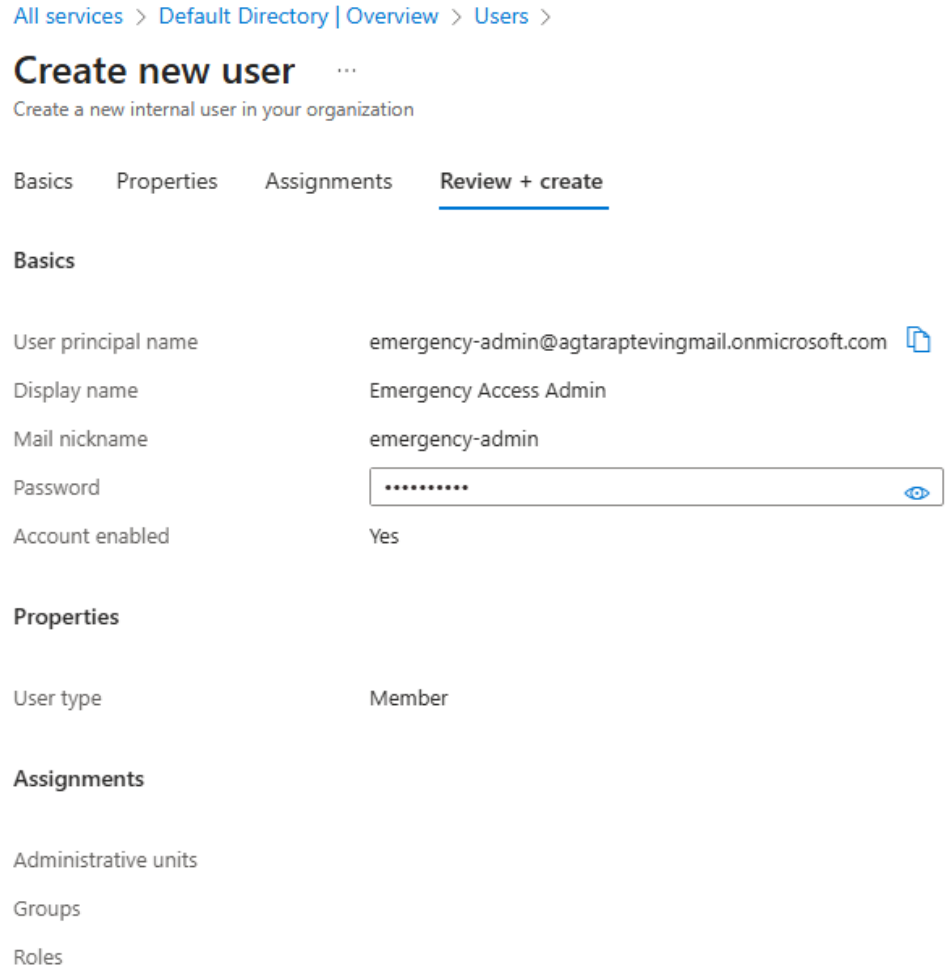
End-to-end Azure cloud build demonstrating secure tenant hardening (MFA, break-glass admin, RBAC), SIEM on boarding with Microsoft Sentinel (Log Analytics + Azure Activity), and full Microsoft Defender plan enablement. I intentionally deployed a vulnerable storage resource to validate detection and guided remediation via Defender for Cloud and network segmentation.

Detection coverage is mapped to MITRE ATT&CK, with KQL hunting for rapid/suspicious resource creation, alert to incident workflows, and documented investigations. I operationalized threat intelligence by creating test IoCs, modeling spear-phishing and simulated APT activity, and confirming enterprise-wide visibility through Threat Analytics and analyst reports—showcasing a complete loop from prevention and detection to response and intel.

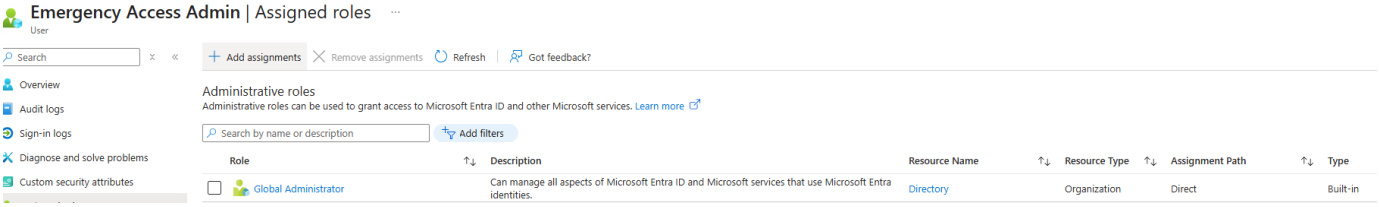
Create and enable MFA on Azure account



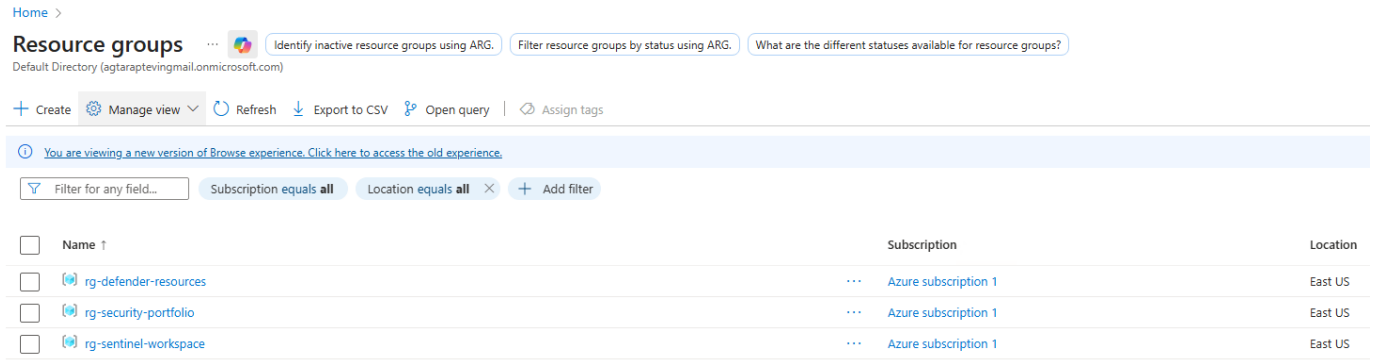
Create emergency Admin account – just in case!



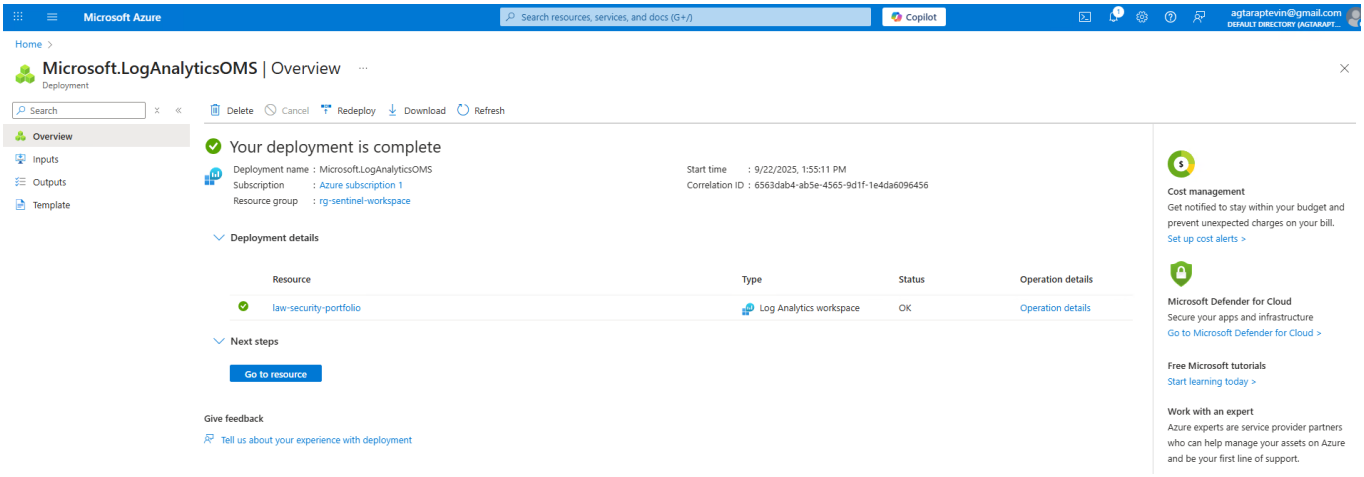
Add Assigned role – Global Admin



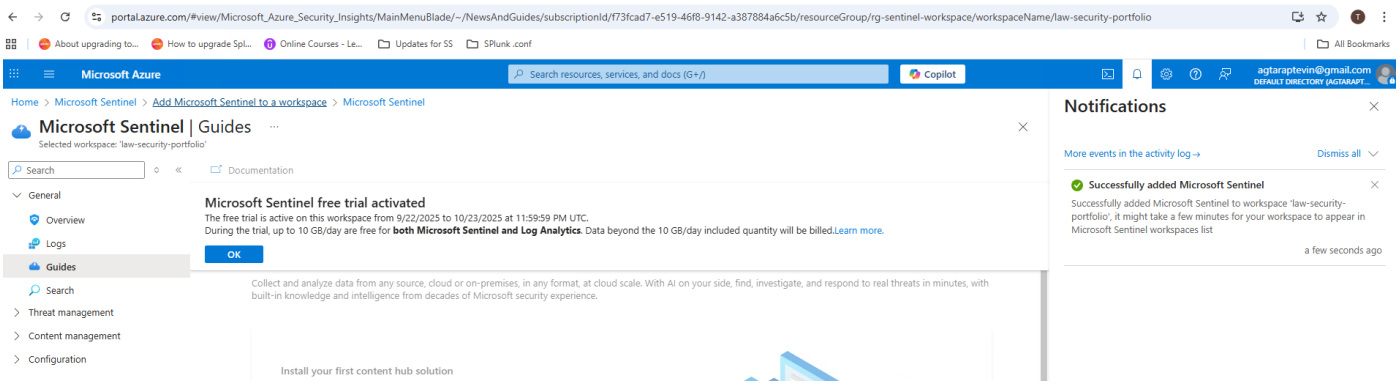
Create Resource groups for the use in Microsoft Sentinel & Defender



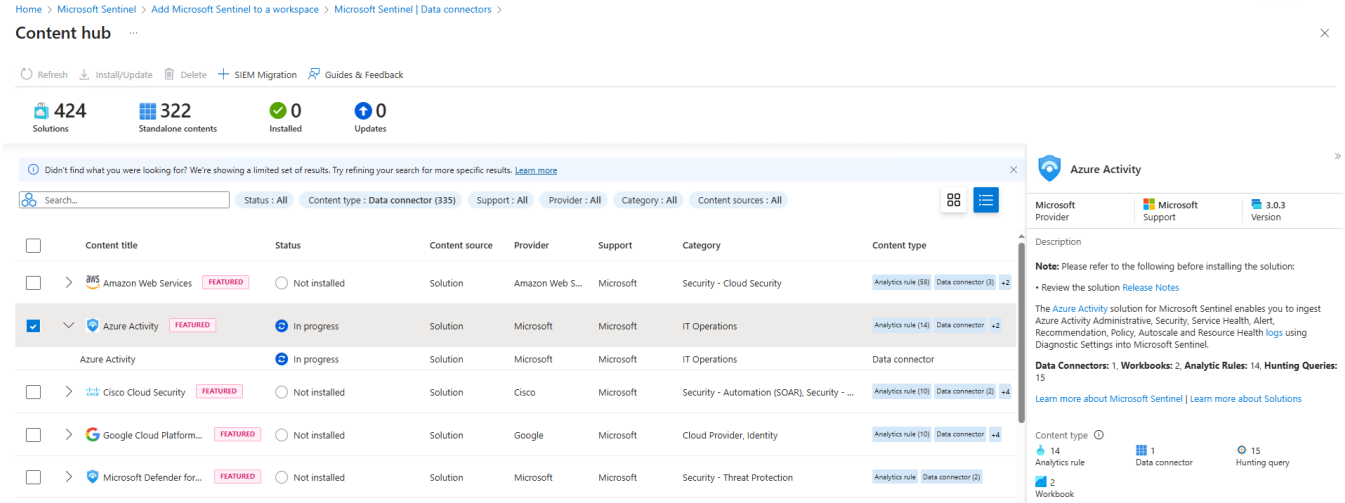
Create Log Analytics Workspace (Required for Sentinel)



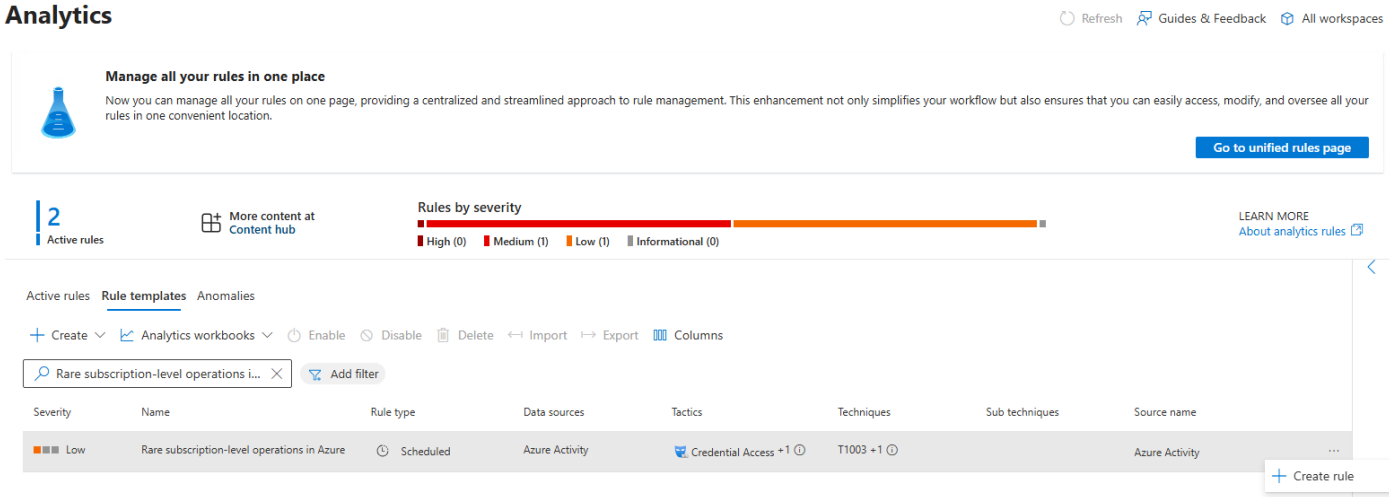
Add Sentinel to Workspace

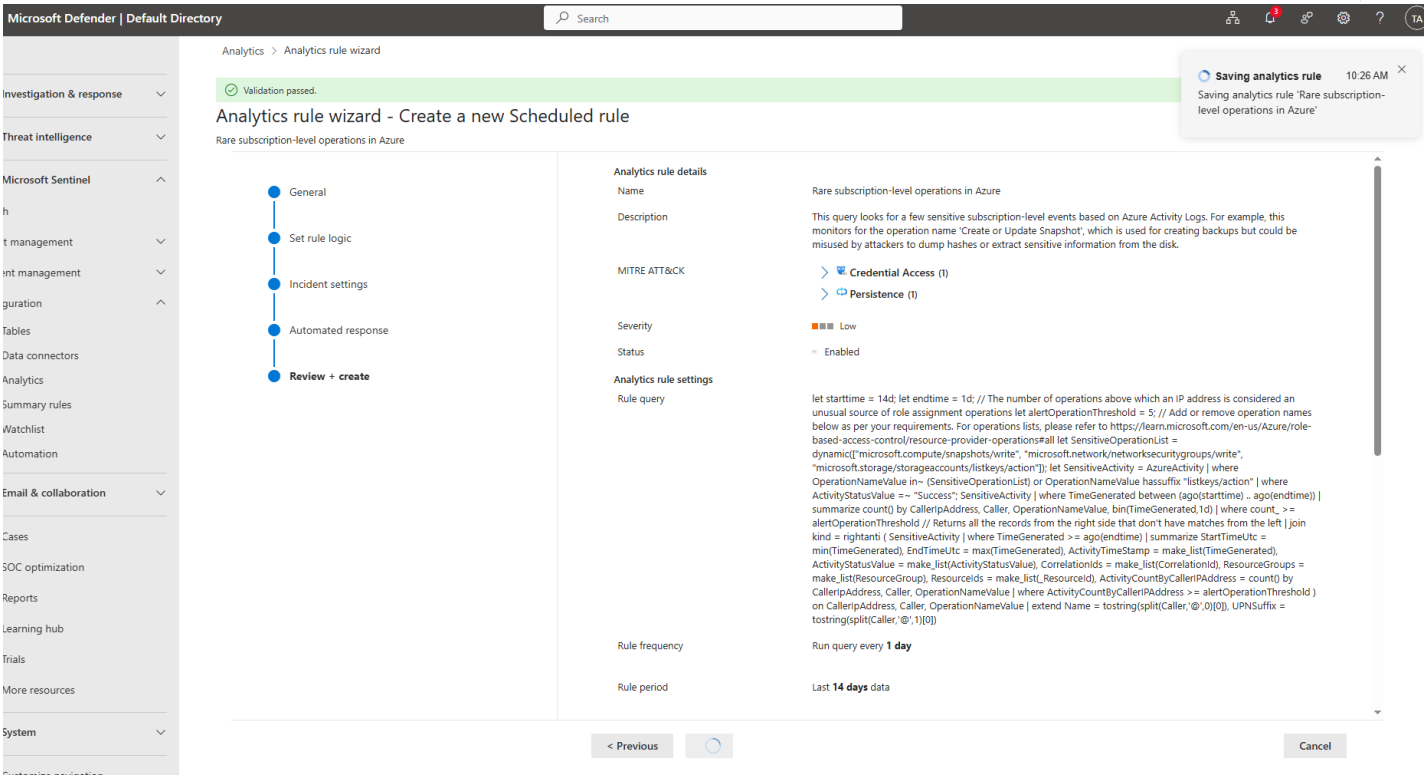


Install Azure Activity

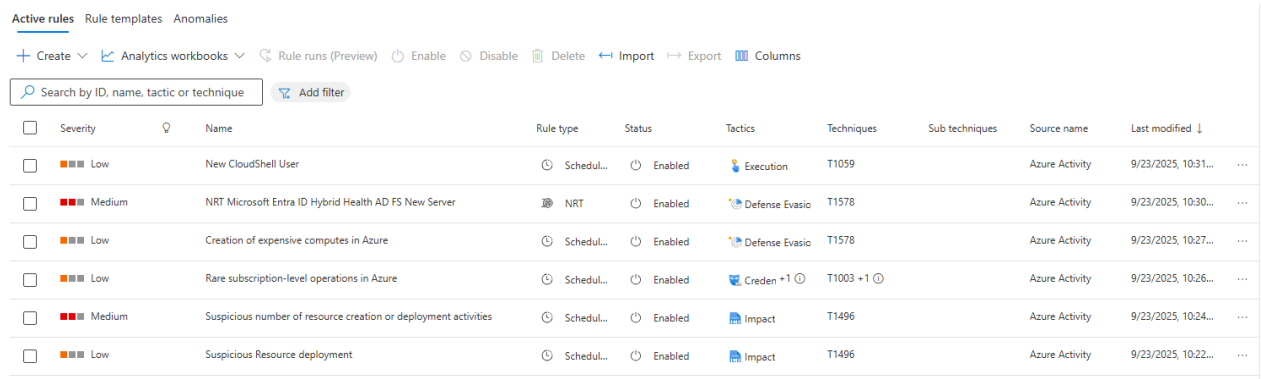


Add Rules through Microsoft Defender Configuration Analytics dashboard





Activate 6 various rules to help cover portions of the MITRE ATT&CK frame work



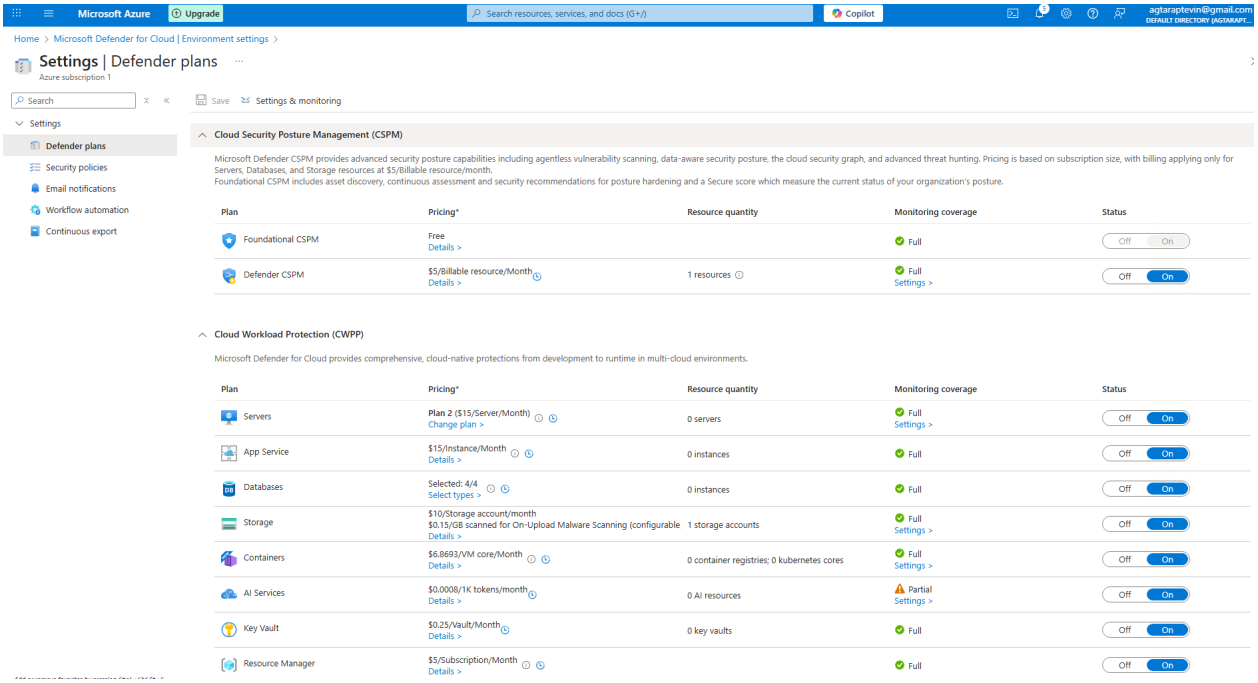
Active rules | Rule templates | Anomalies

Create | Analytics workbooks | Rule runs (Preview) | Enable | Disable | Delete | Import | Export | Columns

Search by ID, name, tactic or technique | Add filter

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Low	New CloudShell User	Schedul...	Enabled	Execution	T1059		Azure Activity	9/23/2025, 10:31...
Medium	NRT Microsoft Entra ID Hybrid Health AD FS New Server	NRT	Enabled	Defense Evasic	T1578		Azure Activity	9/23/2025, 10:30...
Low	Creation of expensive computes in Azure	Schedul...	Enabled	Defense Evasic	T1578		Azure Activity	9/23/2025, 10:27...
Low	Rare subscription-level operations in Azure	Schedul...	Enabled	Creden +1	T1003 +1		Azure Activity	9/23/2025, 10:26...
Medium	Suspicious number of resource creation or deployment activities	Schedul...	Enabled	Impact	T1496		Azure Activity	9/23/2025, 10:24...
Low	Suspicious Resource deployment	Schedul...	Enabled	Impact	T1496		Azure Activity	9/23/2025, 10:22...

Activate all Defender plans



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | agtaraptevin@gmail.com DEFAULT DIRECTORY (AGTARAPT...

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

Azure subscription 1

Search | Save | Settings & monitoring

Settings
- Defender plans
- Security policies
- Email notifications
- Workflow automation
- Continuous export

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at $5/Billable resource/month.
Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

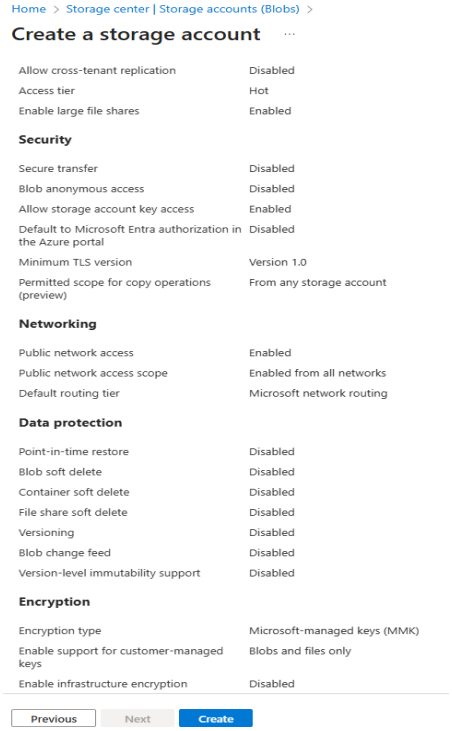
Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		Full	Off On
Defender CSPM	$5/Billable resource/Month Details >	1 resources	Full Settings >	Off On

Cloud Workload Protection (CWPP)

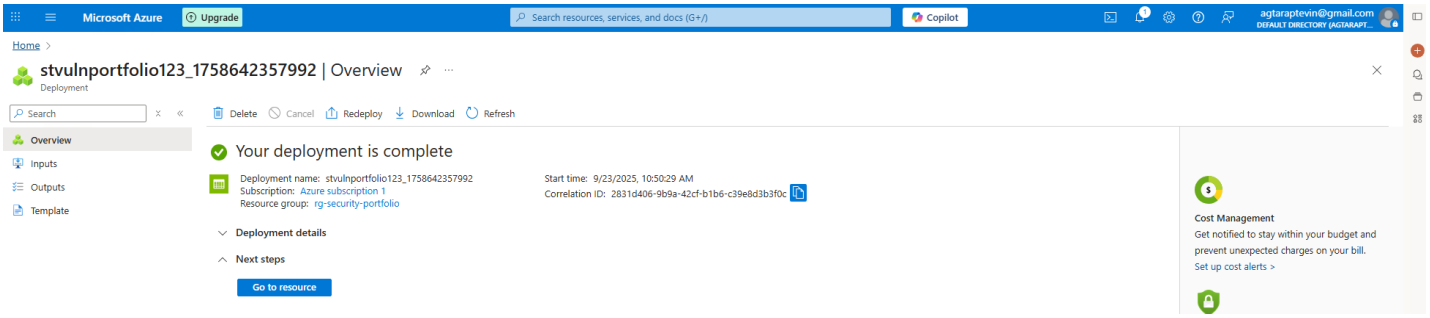
Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 ($15/Server/Month) Change plan >	0 servers	Full Settings >	Off On
App Service	$15/Instance/Month Details >	0 instances	Full	Off On
Databases	Selected: 4/4 Select types >	0 instances	Full	Off On
Storage	$10/Storage account/month $0.15/GB scanned for On-Upload Malware Scanning (configurable Details >	1 storage accounts	Full Settings >	Off On
Containers	$6.8693/VM core/Month Details >	0 container registries; 0 kubernetes cores	Full Settings >	Off On
AI Services	$0.0008/1K tokens/month Details >	0 AI resources	Partial Settings >	Off On
Key Vault	$0.25/Vault/Month Details >	0 key vaults	Full	Off On
Resource Manager	$5/Subscription/Month Details >		Full	Off On

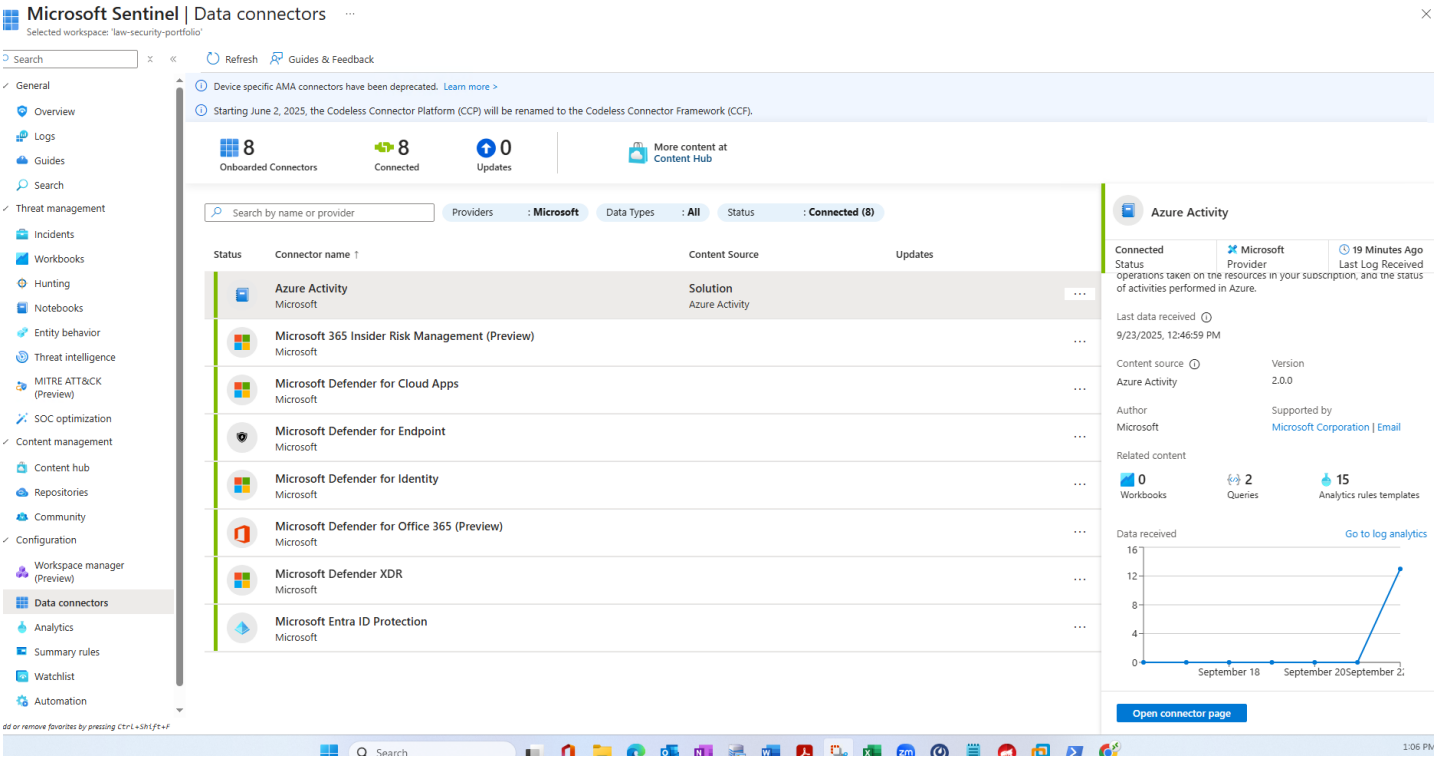
Deploy a Storage account with vulnerabilities so we can use Azure to find and then remediate them!



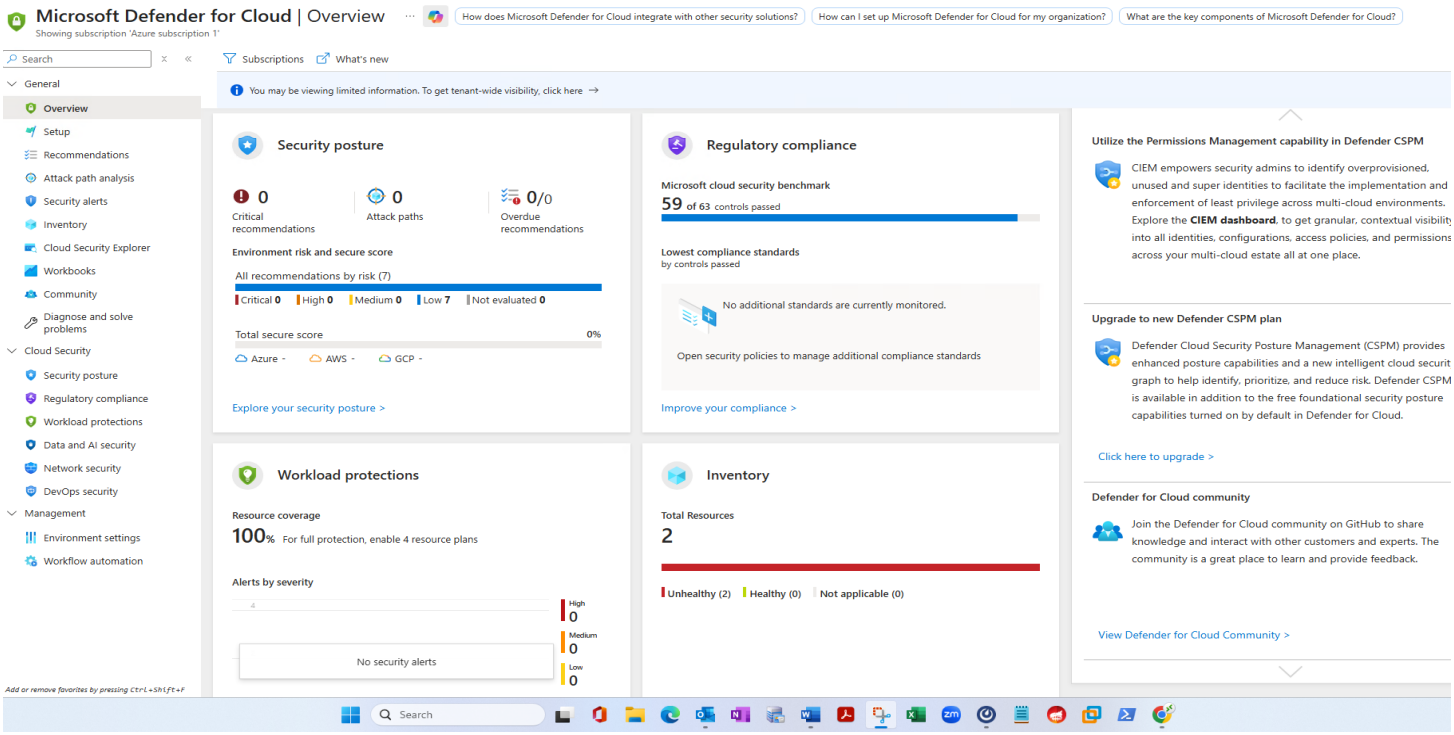
Confirm deployment



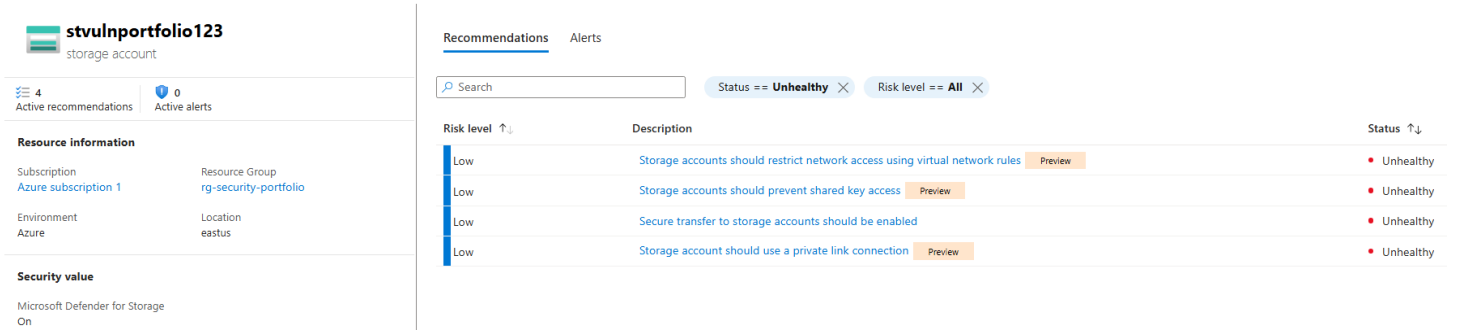
Verify we are now connected with Azure Activity



Use Microsoft Defender for Cloud to check for our Vulnerabilities



Several found let’s Remediate



Storage accounts should restrict network access using virtual network rules ...

Open query | View policy definition | View recommendation for all resources

.ow Risk level	stvulnportfolio... Resource	Unassigned Status

Description

This method is preferred over IP-based filtering, which can leave your storage accounts vulnerable to threats if public IPs gain access.
If IP-based filtering is not disabled, your storage accounts could be exposed to potential threats, compromising the security of your data.

General details

Scope
Azure subscription 1

Ticket ID
-

Last change date
9/23/2025

Freshness
30 Min

Attack Paths
0

Risk

Risk factors
-

Governance

Recommendation owner

Due date
-

Take action | Graph

Take one of the the following actions in order to mitigate the threat:

Remediate

To protect your storage account from potential threats using virtual network rules:
1. In the Azure portal, open your storage account.
2. From the left sidebar, select 'Networking'.
3. From the 'Allow access from' section, select 'Selected networks'.
4. Add a Virtual network under the 'Virtual networks' section. Do not add allowed IP ranges/ or addresses in the firewall. This i
prevent public IPs from accessing your storage account. For details, see: https://aka.ms/storagenetworksecurity.

Recommendation owner and set due date

Assign owner and set due date by which recommendation should be implemented.

Assign owner & set due date

Exempt

Exempt the entire recommendation, or disable specific findings using disable rules.
Exempted resources appear as not applicable and do not affect secure score.

Exempt

Workflow automation

Set a logic app which you would like to trigger with this security recommendation.

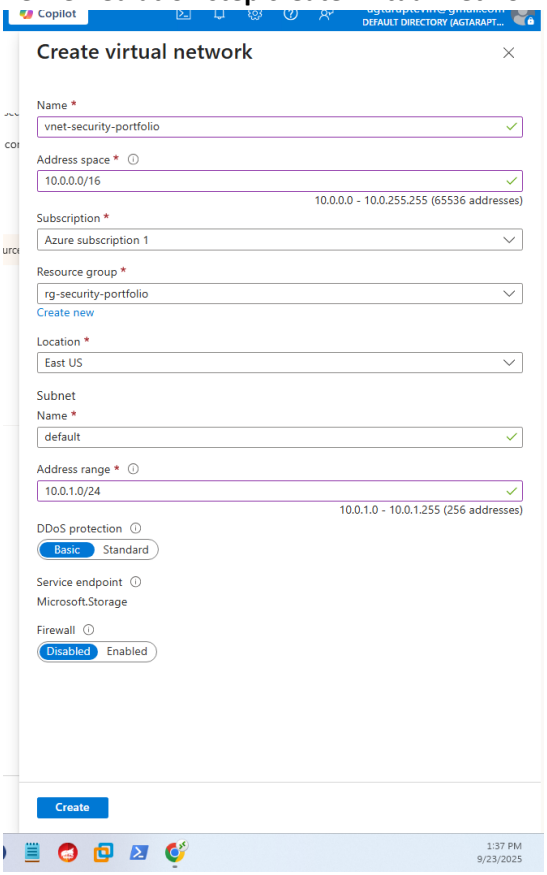
Trigger logic app

Prevention

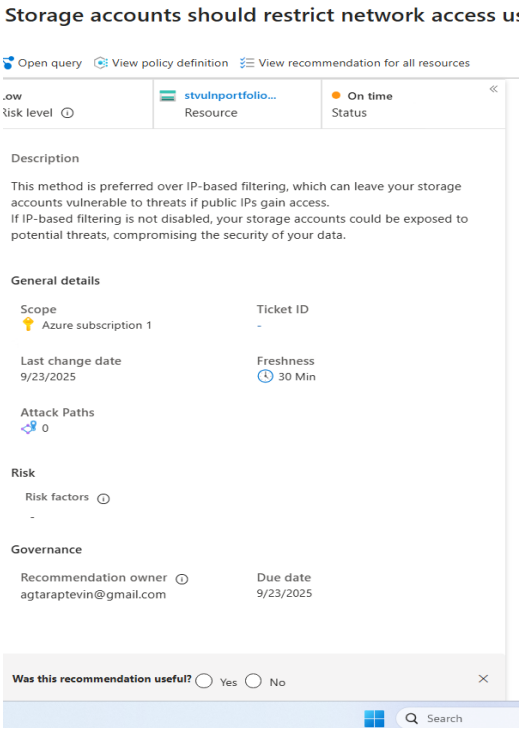
Enforce remediation for future resources or Deny creation of misconfigured resources

Deny

Per remediation step create Virtual Network



Assigned to me and remediated!



Advanced Hunting with KQL in Microsoft Defender

Rapid Resource Creation Pattern (Potential Cloud Abuse)

rg-test-hunt-01	···	Azure subscription 1	East US
rg-test-hunt-02	···	Azure subscription 1	East US
rg-test-hunt-03	···	Azure subscription 1	East US
rg-test-hunt-04	···	Azure subscription 1	East US

Advanced hunting

Selected workspace: law-security-portfolio | Help resources

Detect Encoded PowerShell Commands* | New query

Schema | Functions | Queries

Search

Favorites

Your favorites list is empty. To add an item, click the menu next to it and select "Add to Favorites"

Shared queries

- Microsoft Sentinel

My queries

- Detect Encoded PowerShell Commands

Community queries

- Campaigns
- Discovery
- Impact
- Microsoft Sentinel
- Protection events
- Ransomware

Run query | Set in query | Save | Share link | Create summary rule | Create detection rule

Query

```
// Detect Rapid Cloud Resource Deployment - Potential Account Takeover
let time_window = 24h;
let threshold = 3;
AzureActivity
| where TimeGenerated > ago(time_window)
| where ActivityStatusValue == "Success"
| where OperationNameValue has_any ("write", "create", "Microsoft.Resources")
| summarize
    TotalOperations = count(),
    UniqueResourceTypes = dcount(ResourceProviderValue),
    ResourcesCreated = make_set(Resource),
    FirstAction = min(TimeGenerated),
    LastAction = max(TimeGenerated)
    by Caller, bin(TimeGenerated, 15m)
| extend DurationMinutes = datetime_diff('minute', LastAction, FirstAction)
| where TotalOperations >= threshold
| extend RiskScore = case(
    TotalOperations >= 10, "Critical",
    TotalOperations >= 5, "High",
    TotalOperations >= 3, "Medium",
    "Low"
)
| project TimeGenerated, Caller, TotalOperations, DurationMinutes, RiskScore, ResourcesCreated
| order by TotalOperations desc
```

Results | Query history

Export | Show empty columns | 4 items | Search | 00:01.425 | Low | Chart type | Full screen

Filters: Add filter

TimeGenerated	Caller	TotalOperations	DurationMinutes	RiskScore	ResourcesCreated
Sep 23, 2025 1:30:...	agtaraptevin@gmail.com	5	1	High	[""]
Sep 23, 2025 2:15:...	agtaraptevin@gmail.com	4	1	Medium	[""]
Sep 23, 2025 1:00:...	agtaraptevin@gmail.com	3	10	Medium	[""]
Sep 23, 2025 1:45:...	agtaraptevin@gmail.com	3	10	Medium	[""]

2:38 PM

Investigate Alert! Suspicious Resource deployment!

Microsoft Defender | Default Directory

Search

Home

Exposure management

Investigation & response

Incidents & alerts

Incidents

Alerts

Alerts

Alert service settings

Export | 1 Week | 1 Alert | Search for name or ID | Customize columns

Filter set:

Status: New, In progress | Add filter | Reset all

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Product name	Impacted assets
Suspicious Resource deployment		Low		New	Impact	Scheduled detection	Microsoft Sentinel	2 Accounts

Convert Alert to Incident

Home

Exposure management

Investigation & response

Incidents & alerts

Incidents

Alerts

Hunting

Advanced hunting

Custom detection rules

Incidents

Alert service settings | Email notification

Most recent incidents and alerts

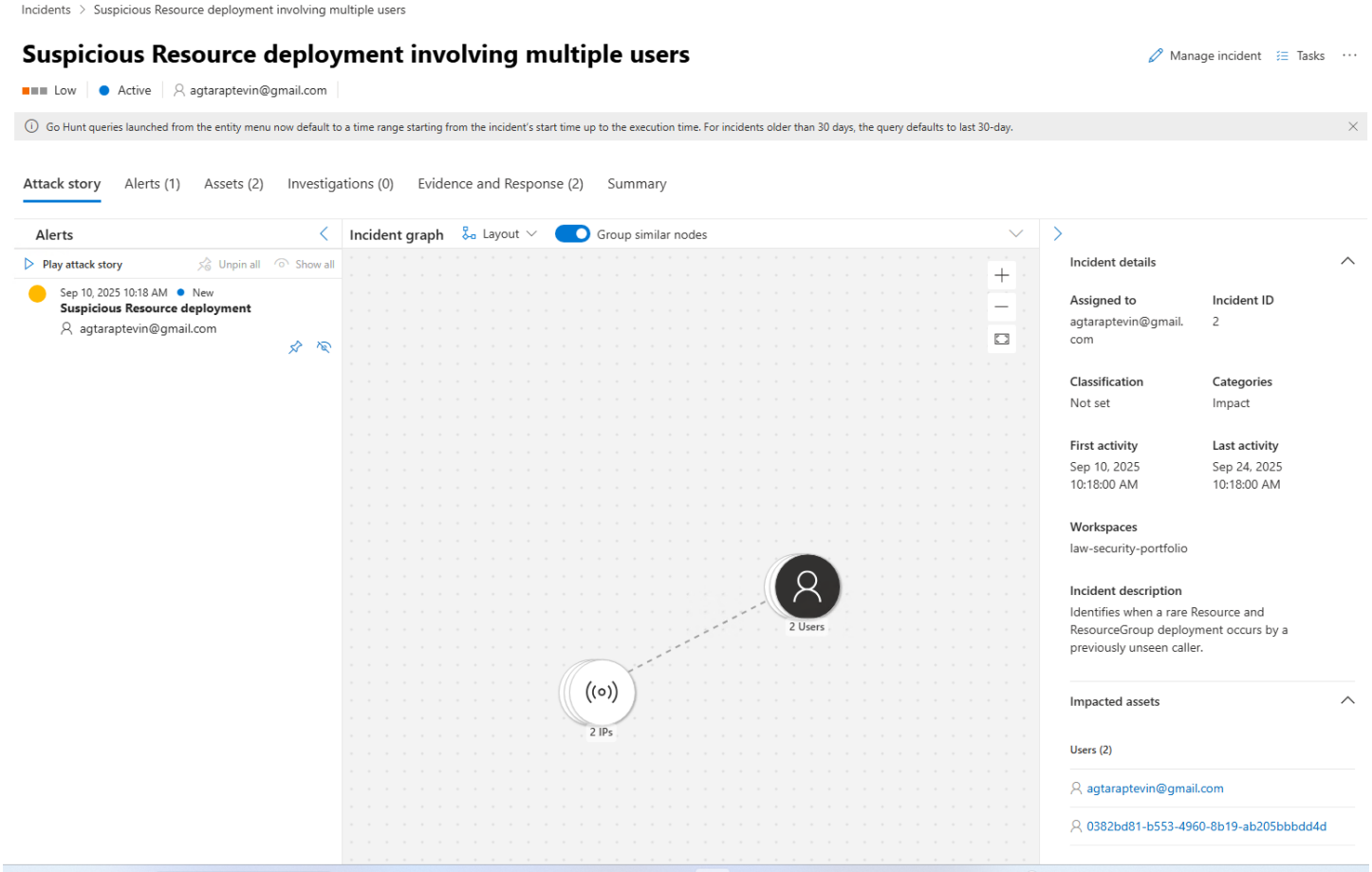
Export | Copy list link | Refresh | 1 Week | 1 Incident | Search for name or ID | Customize columns

Filter set: Save

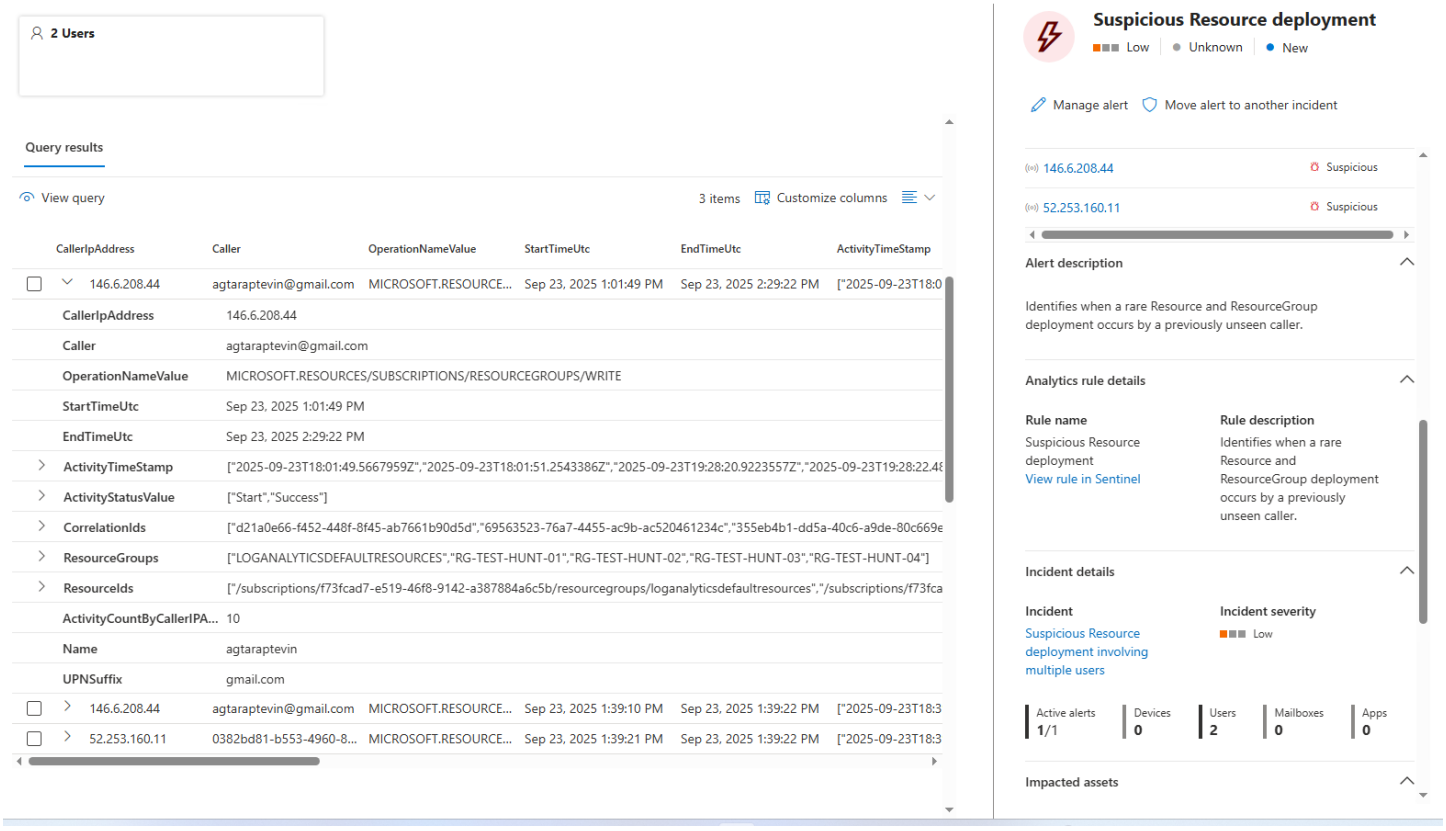
Status: New, In progress | Alert severity: High, Medium, Low | Add filter | Reset all

Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources
Suspicious Resource deployment involving multip...	2		Low		Impact	2 Accounts	1/1	Microsoft Sentinel

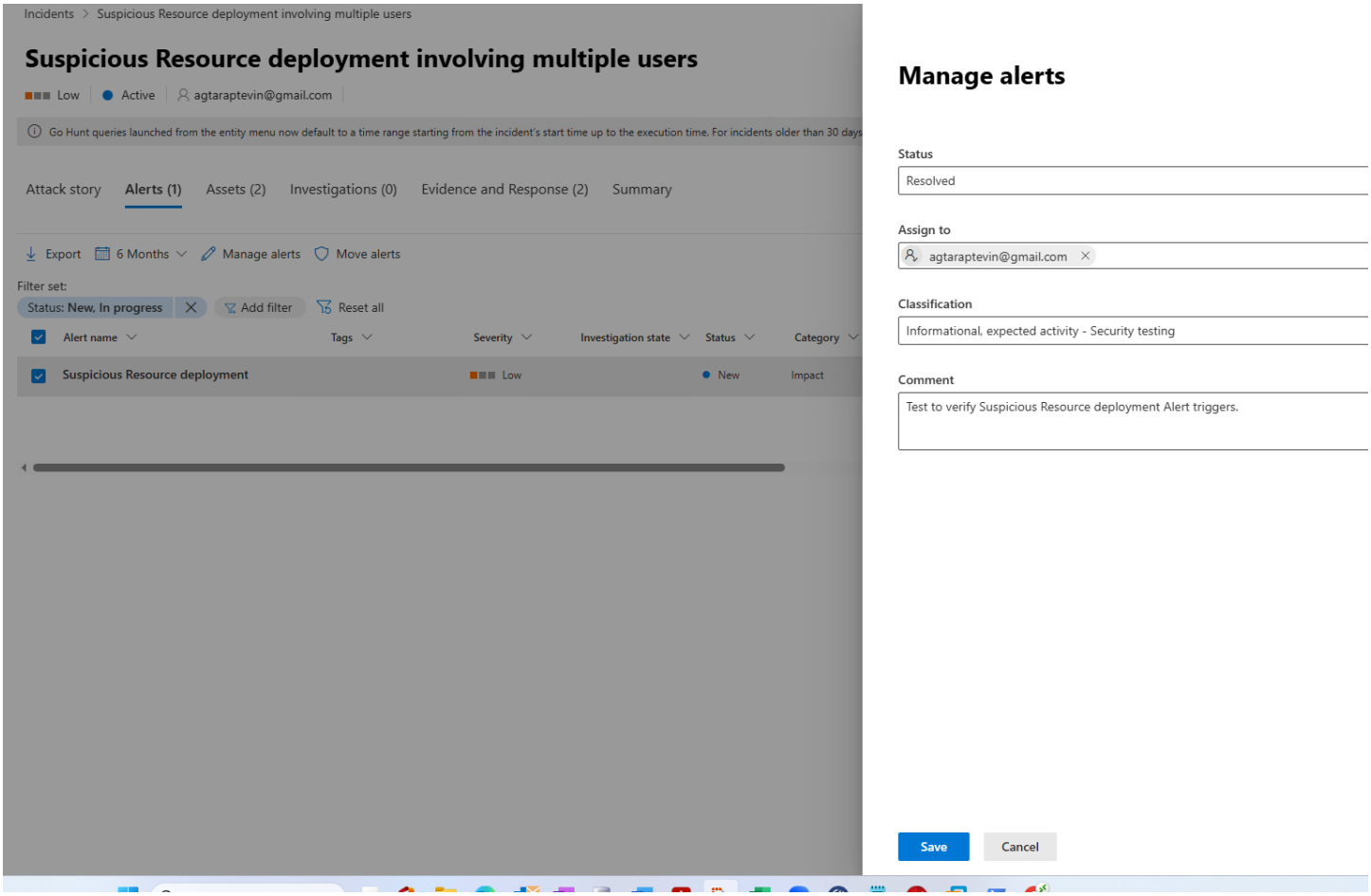
Start Incident/Alert Investigation



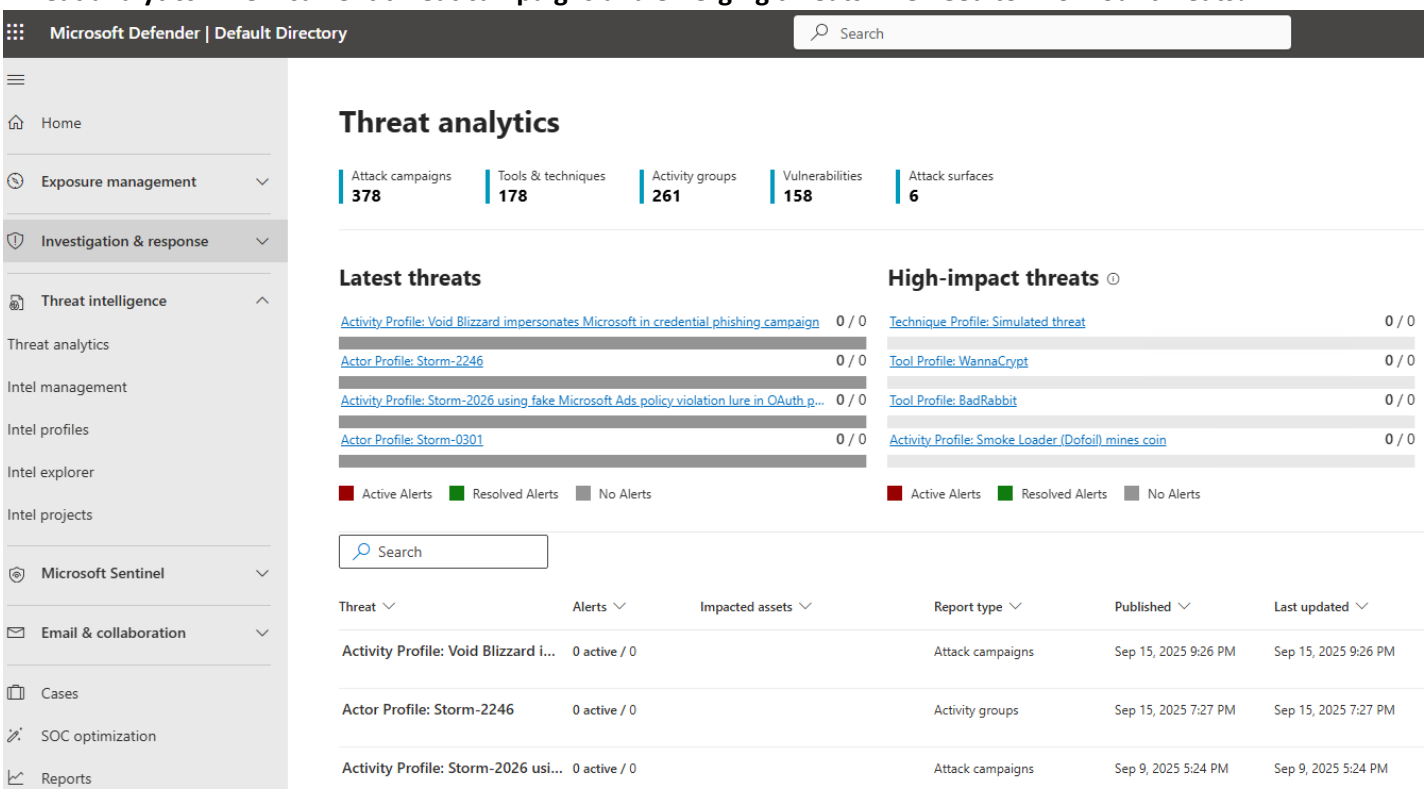
Verify Queries and IPS



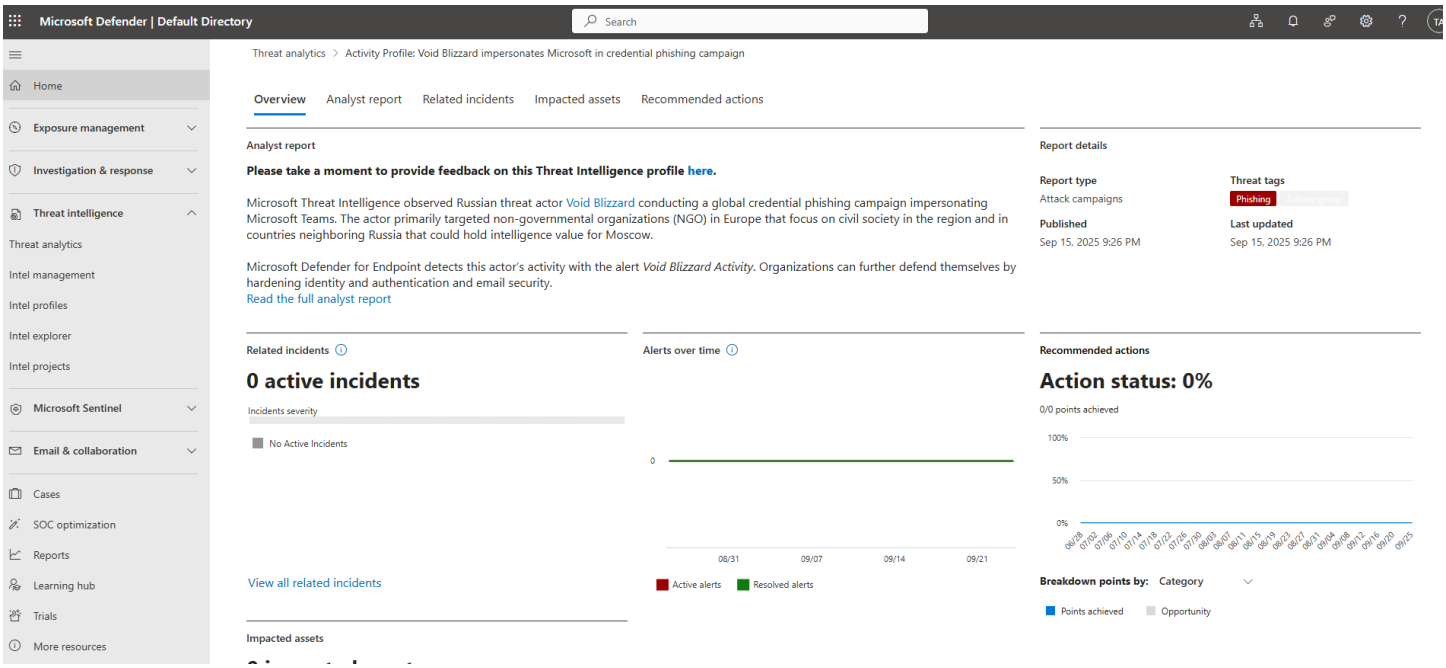
Manage Alert/Incident – Moved to incident to investigate verified test and marked accordingly



Threat analytics - View current threat campaigns and emerging threats. We need to know our threats!



Check enterprise for related incidents and overview including Analyst report.



Executive summary

Please take a moment to provide feedback on this Threat Intelligence profile here.

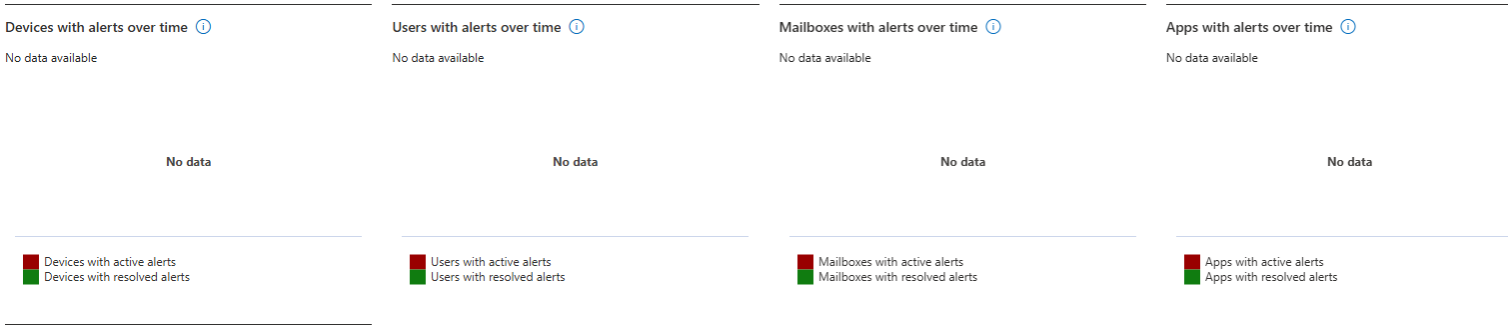
Microsoft Threat Intelligence observed Russian threat actor Void Blizzard conducting a global credential phishing campaign impersonating Microsoft Teams. The actor primarily targeted non-governmental organizations (NGO) in Europe that focus on civil society in the region and in countries neighboring Russia that could hold intelligence value for Moscow.

Microsoft Defender for Endpoint detects this actor's activity with the alert *Void Blizzard Activity*. Organizations can further defend themselves by hardening identity and authentication and email security.

Activity Overview

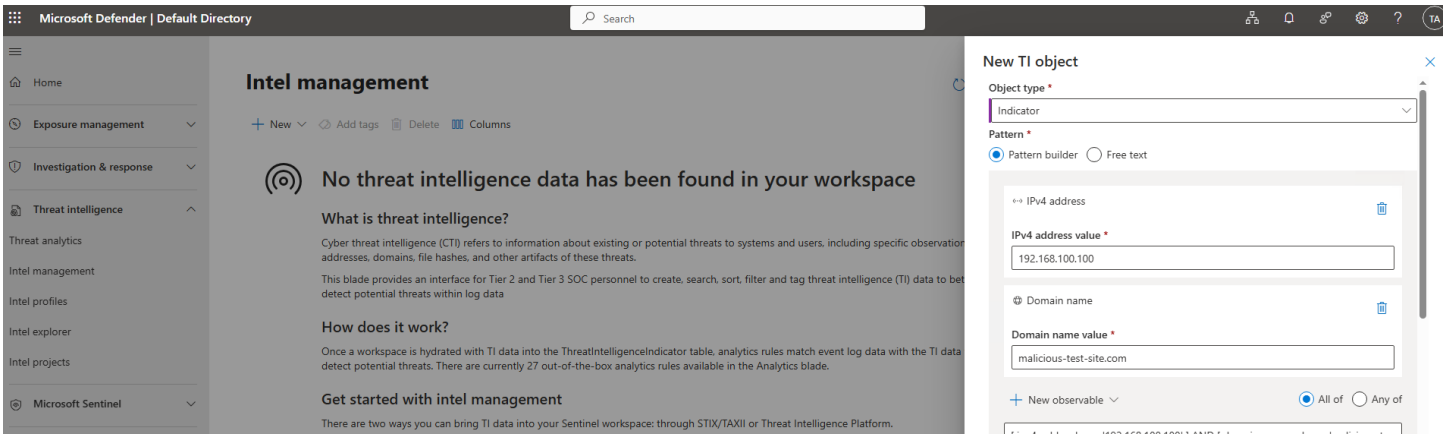
In July 2025, Russian threat actor Void Blizzard conducted a credential phishing campaign posing as Microsoft likely with the end goal to conduct remote email collection. Credential phishing is designed to deceive a target into entering their account details into an actor-controlled application or website for the purpose of directly using and/or reselling stolen information. The campaign targeted nearly a dozen think tanks and NGOs in Europe that focus on security issues and democracy. Microsoft did not observe any successful compromises, which could be due to public exposure of previous Void Blizzard activity as well as other Russian threat actors targeting organizations in similar sectors, increased implementation of automated email protections, and user awareness of this actor's phishing tactics, techniques, and procedures (TTPs). The actor also used domains, such as *office365online[.]co*, that spoof Microsoft services. This domain is not a Void Blizzard-registered domain and is possibly acquired through fraud services, such as offshore domain or phishing kits used in the cybercriminal ecosystem.

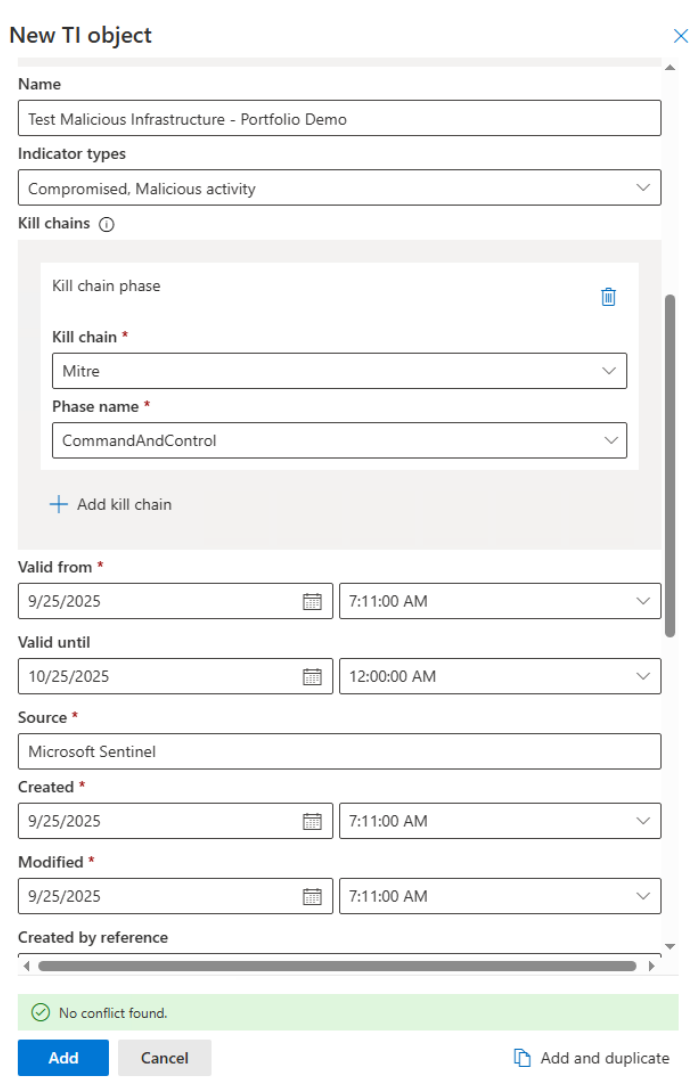
The actor used a well-crafted phishing lure using authentic Microsoft graphics and convincing text informing users that their organization is implementing a Microsoft Teams integration effort. The email body contained a malicious link fronted by Cloudflare, allowing the traffic to obfuscate the actual Evilginx attack server behind it. Microsoft has observed Void Blizzard using Evilginx, which is an open-source phish kit used by other threat groups to facilitate adversary-in-the-middle (AitM) attacks, in previous campaigns.

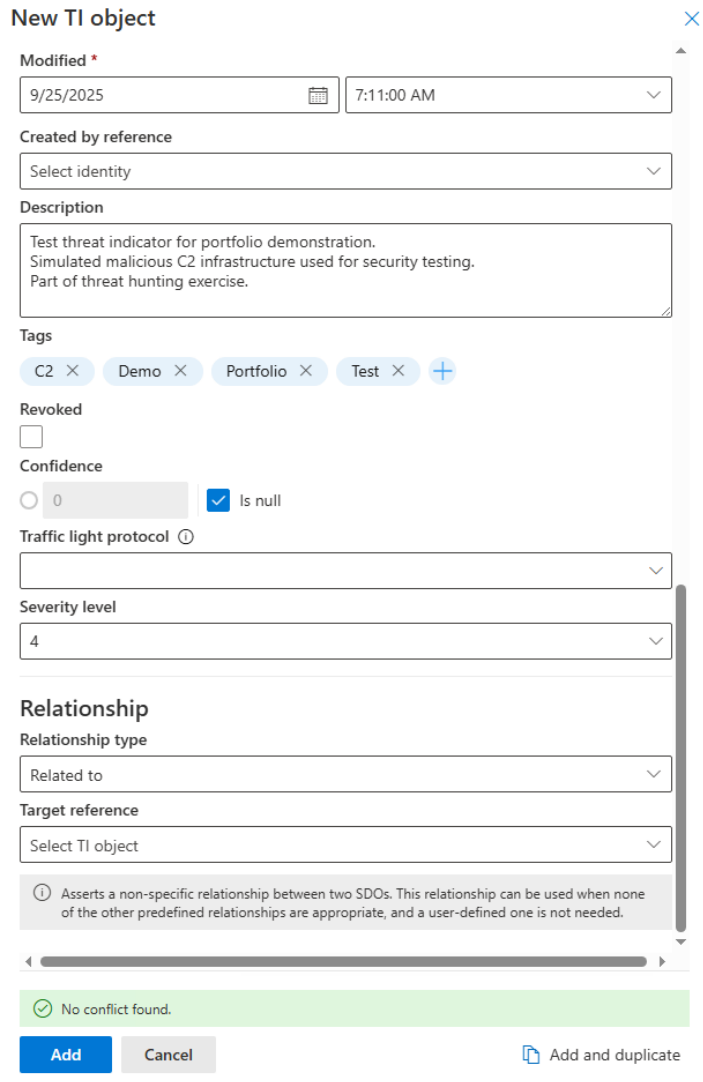


Intel Management (Threat Indicators)

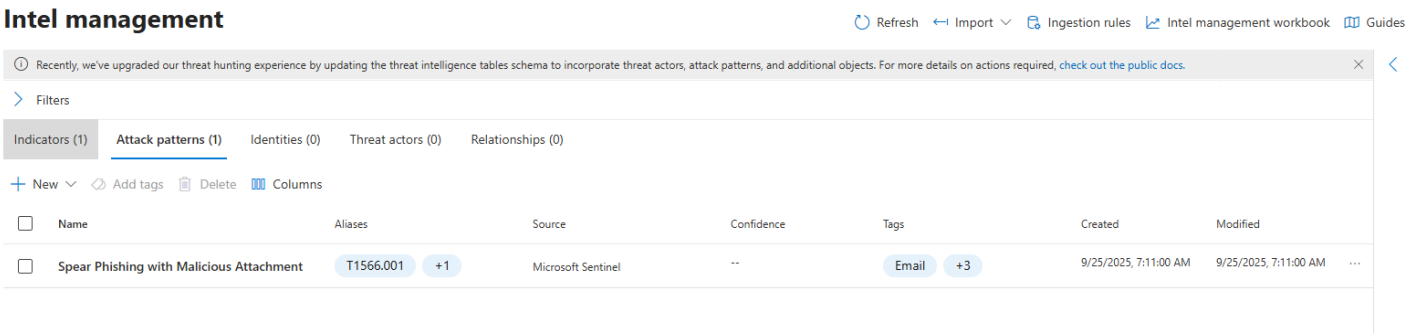
Create Test IoC!



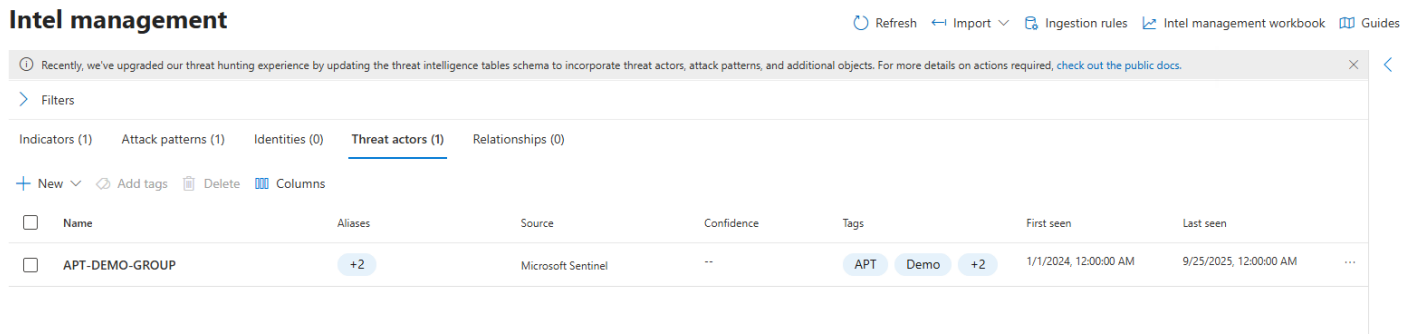




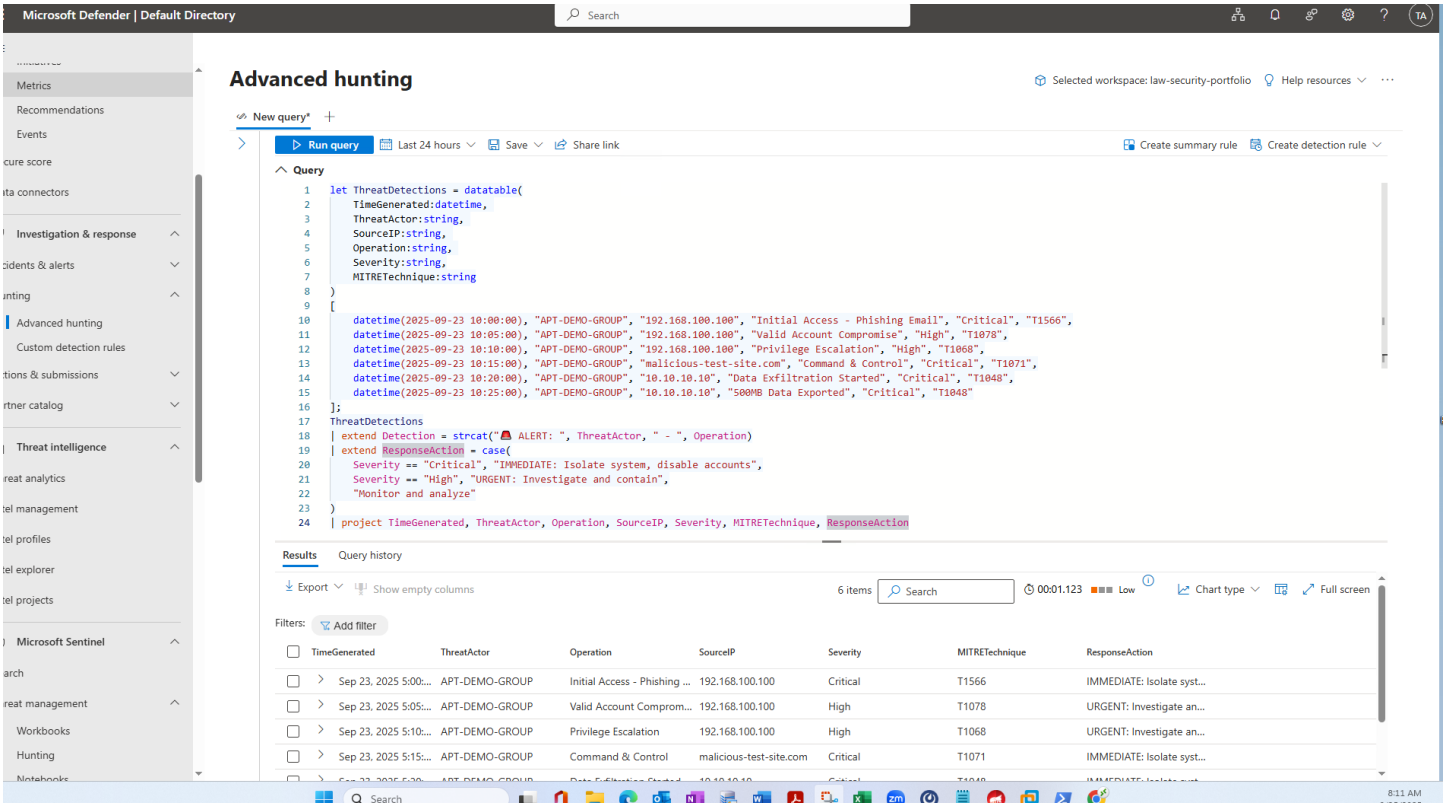
Add attack Pattern – Spear Phisinging



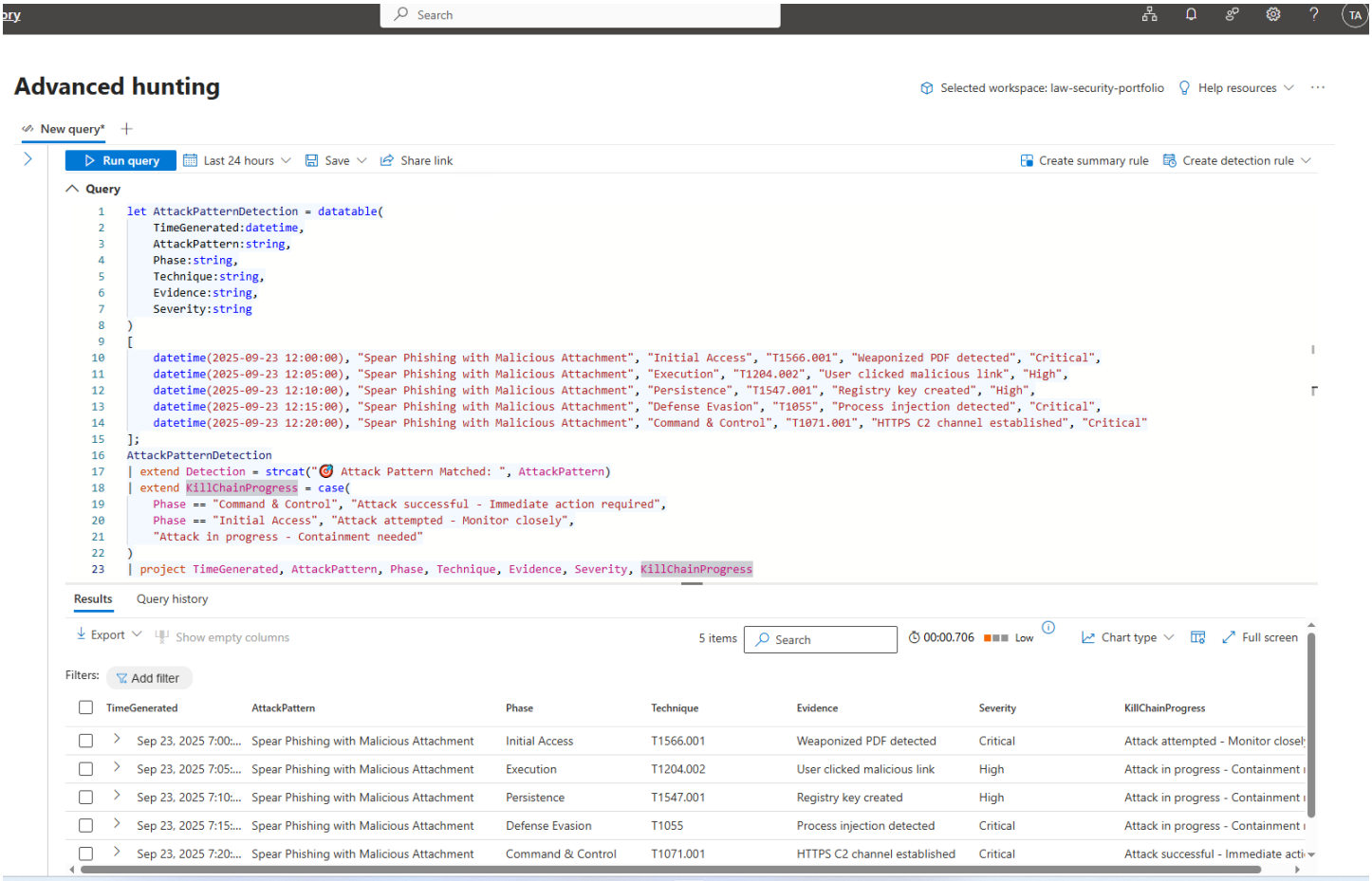
Add Threat actors – APT Group



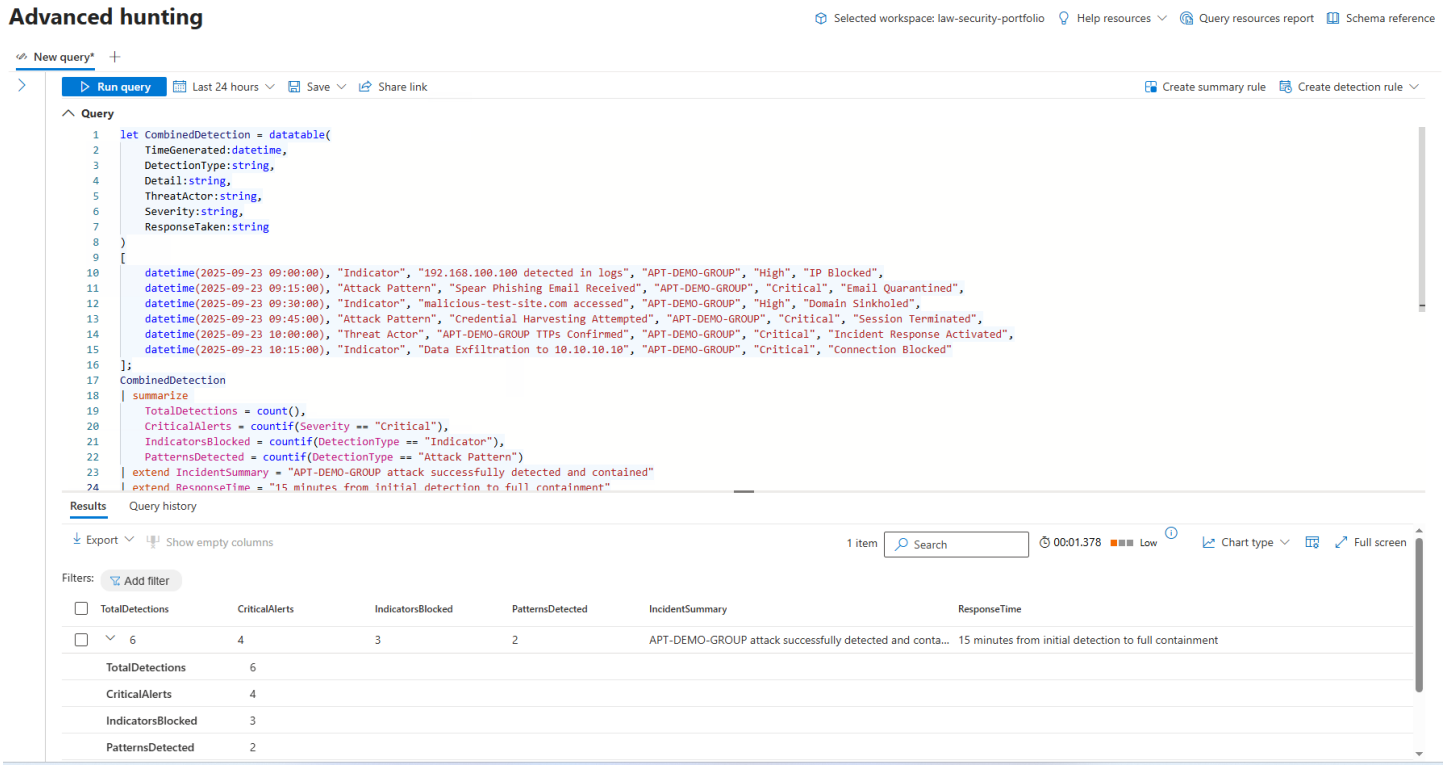
Generate demo logs to show APT Threat Actor - Simulated threat data was used to safely demonstrate detection capabilities without introducing actual malicious indicators into the environment.



Create query to show simulated threat data to match Attack pattern of Spear Phishing



All Threat intelligence/Intel management working together



Created by Tevin Agtarap 2025