📁 Portfolio Page 1 – Shadow Hunter Tabletop

Theme: Credentialed Simulation of PHI Exfiltration and SOC Response
Author: Kim Lien Chu – Healthcare Cybersecurity Analyst
Issued by: Microsoft Security Marketing Program
Date: August 27, 2025
Credential Earned: Microsoft Security Agent – Intermediate Level
Format: 5-Hour In-Person Immersion

🧭 Program Overview

The Shadow Hunter immersion simulated real-world threat scenarios using Microsoft Defender for Cloud and Sentinel. Participants navigated alerts, applied remediation, and mapped threats to MITRE ATT&CK tactics.

Skills Gained:

- Cloud Security Applications
- Cybersecurity Compliance
- Microsoft Security Essentials
- Multi-Cloud Defense
- Security Analytics
- Threat Detection

Performance Highlights:

- 100% module completion
- 1350 points earned
- Top 50 rank out of all participants

Credential earned through hands-on immersion

Figure 1 – Shadow Hunter badge earned through immersion

🧪 Tabletop Scenario #1

Title: PHI Exfiltration via SQL Shell & Misconfigured Storage

Scenario Summary:

A hybrid healthcare cloud environment triggers a high-severity alert:

- **SQL Server (corp-sql-02-arc1)** spawns a Windows command shell
- **Executable** pneumaEX-windows.exe downloaded
- Storage account shadostoruri1cfb9c flagged for public access
- Container registry shregistry1 shows 507 vulnerabilities
- VM bulk-0001 flagged for Defense Evasion (MITRE ATT&CK)

MITRE Mapping: Defense Evasion

SQL Server exploited via command shell—external access detected. Alert triggered by suspicious use of xp_cmdshell.

Public access misconfiguration flagged as critical—potential PHI exposure. Registry vulnerabilities suggest lateral movement risk. Alert mapped to Defense Evasion tactic—hybrid VM compromised.

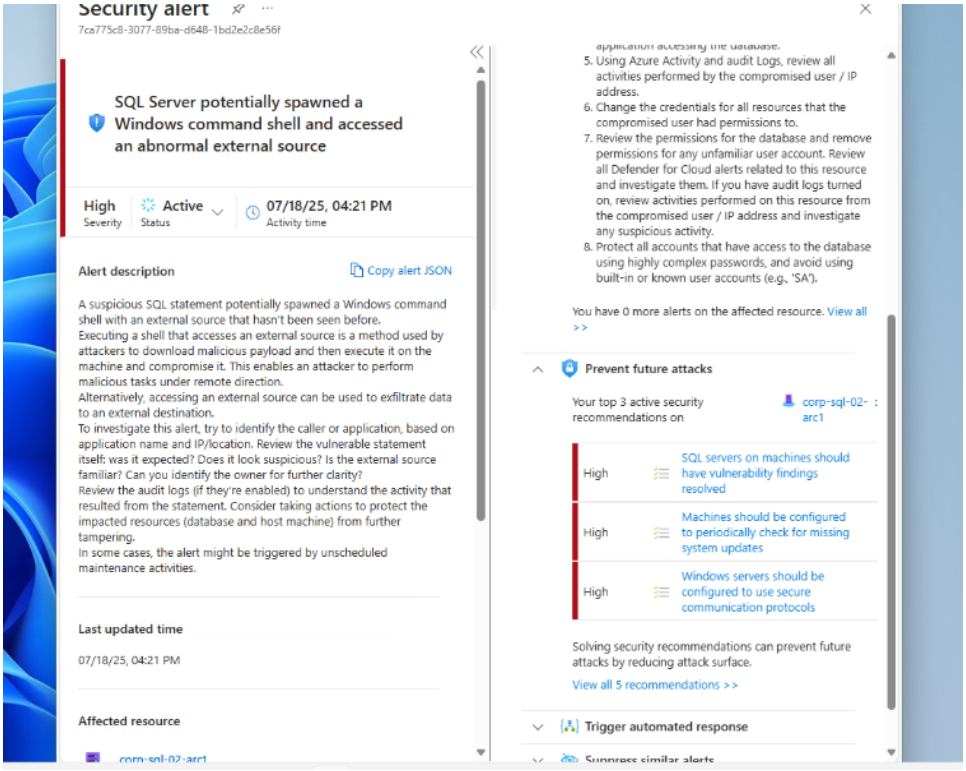

Figure 2 – SQL shell to PHI exfiltration escalation path

📋 SOC Response Checklist

Triage:

- Prioritize alerts by severity
- Map to MITRE ATT&CK tactics
- Confirm PHI exposure risk

Containment:

- Disable public access on storage
- Isolate affected SQL server
- Lock down container registry

Investigation:

- Analyze shell command logs
- Review vulnerability workbook
- Trace external access paths

Remediation:

- Apply Quick Fixes and endpoint protection
- Patch container images
- Harden SQL permissions
- Disable xp_cmdshell

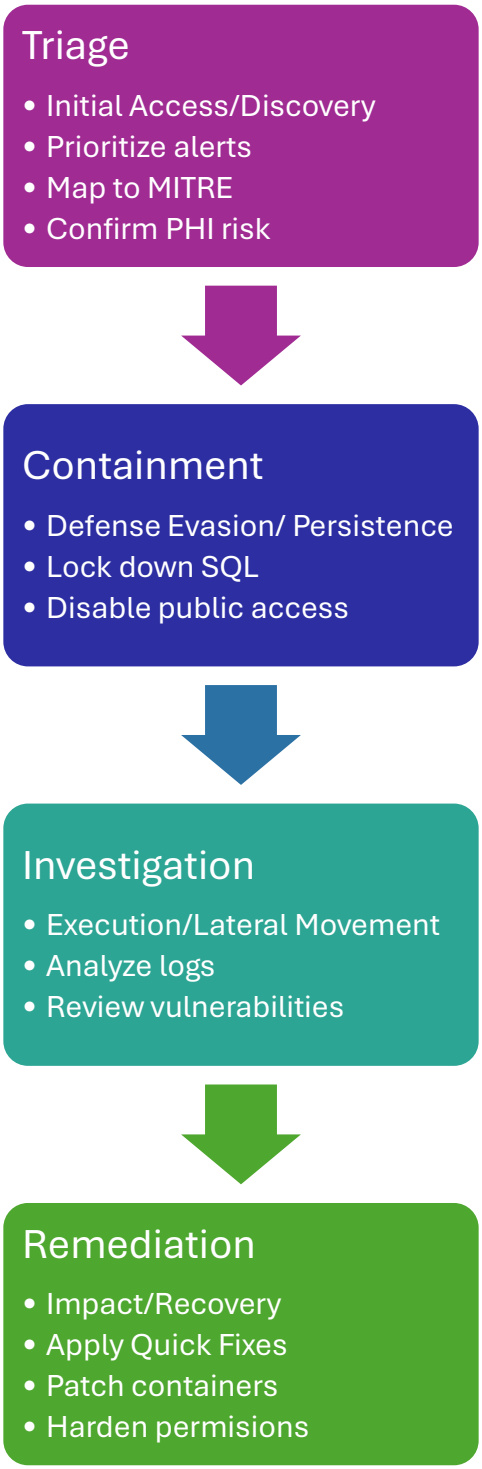

Figure 3 – SOC Response Workflow
Four-phase incident response mapped to MITRE ATT&CK tactics and healthcare governance controls, illustrating triage through remediation of PHI exfiltration alerts.

Governance Mapping:

Framework	Control Applied	Scenario Tie-In	MITRE ID
HHS 405(d)	Data Protection & Loss Prevention	Disabled public access on storage	T1080, T1078
NIST CSF	Respond & Recover	Applied Quick Fixes and endpoint protection	T1059.001
HIPAA 164.308(a)(5)(ii)(B)	Security Awareness & Training	Flagged insider risk and retrained affected users	T1566.001

Visual Evidence

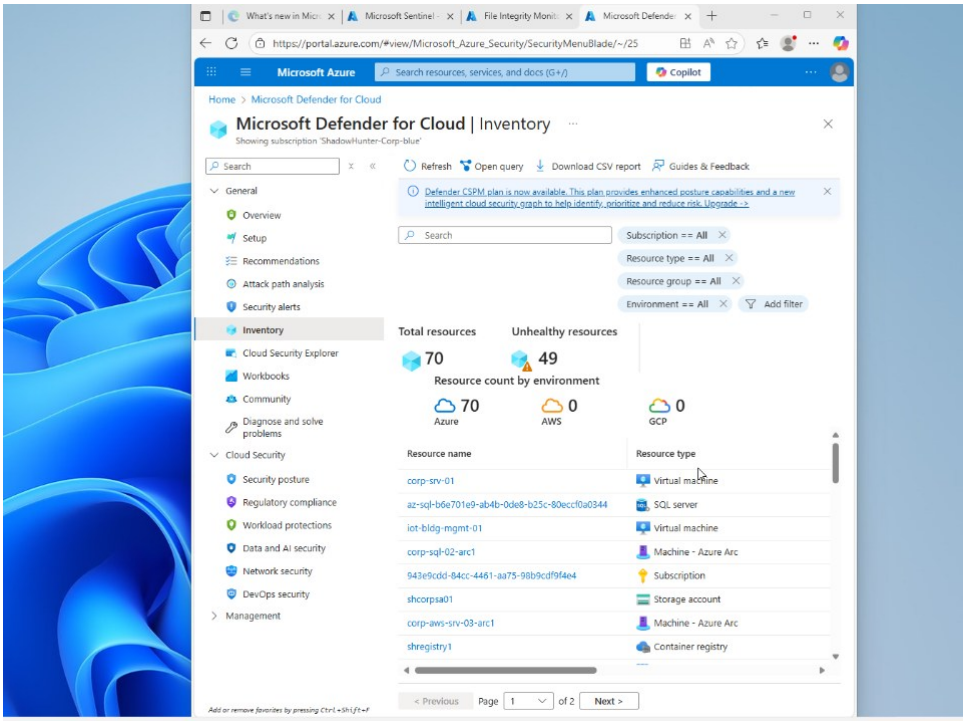

Figure 4 – Initial hybrid cloud posture scan showing 49 unhealthy resources

---

💬 Reflection

This immersion helped me strengthen my ability to triage alerts, interpret MITRE tactics, and align technical response with healthcare governance frameworks. It's a key milestone in my journey toward sector leadership—and now serves as **Portfolio Page 1**, launching my month-long campaign of sector-ready simulations and operational artifacts.

📚 References

1. Microsoft Defender for Cloud Documentation – Alerting, posture management, and remediation workflows
2. MITRE ATT&CK Framework – Execution, Defense Evasion, and Lateral Movement tactics
3. HHS 405(d) Cybersecurity Practices – Volume 1: Data Protection & Loss Prevention
4. NIST Cybersecurity Framework – Respond & Recover functions
5. HIPAA Security Rule – 164.308(a)(5)(ii)(B): Security Awareness & Training
6. Microsoft Sentinel Workbook Templates – Vulnerability and inventory dashboards
7. Microsoft Security Blog – SQL Server xp_cmdshell abuse and mitigation
8. CHIME Central – 405(d) implementation resources for healthcare SOCs
9. CISA Healthcare Sector Risk Profile – Cloud posture, remote access, and insider risk
10. CrowdStrike Threat Intelligence – Hybrid cloud defense trends and adversary tactics (2025)
