

Portfolio Page 1 – Shadow Hunter Tabletop

Theme: Credentialled 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

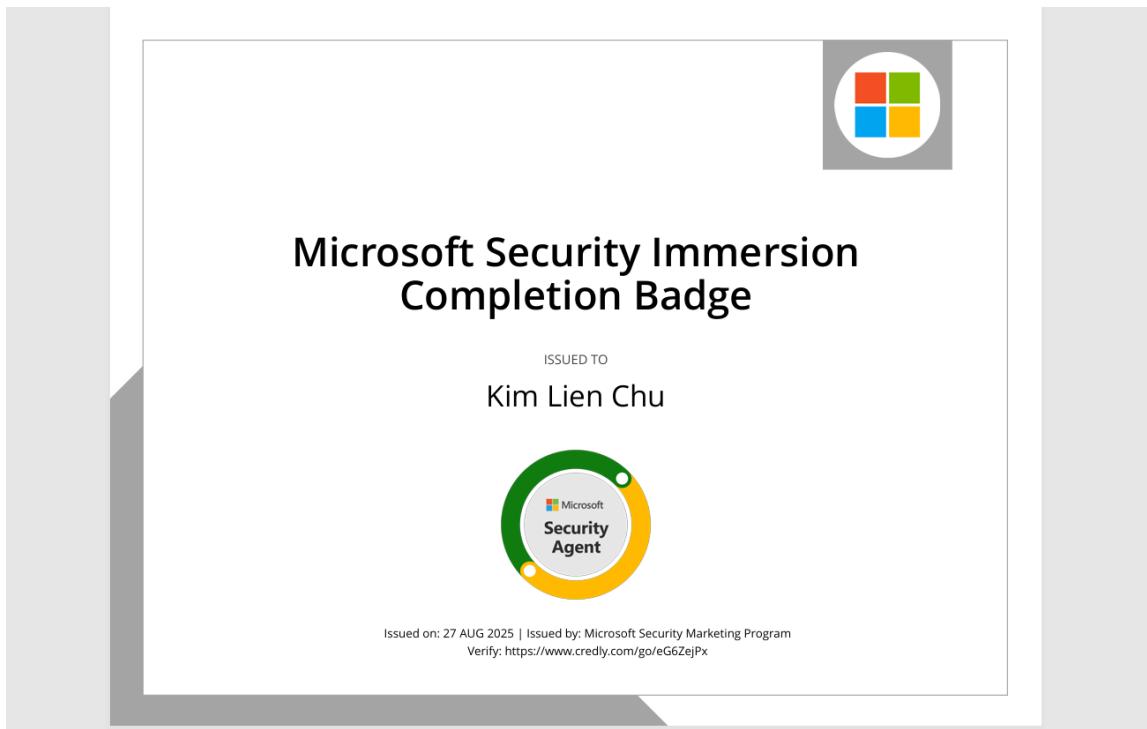


Figure 1 – Shadow Hunter badge earned through immersion

💡 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.

The screenshot shows a Microsoft Defender Cloud Security alert for a SQL Server exploit. The alert details are as follows:

- Alert Type:** Security alert
- Alert ID:** 7ca775c8-3077-89ba-d648-1bd2e2c8e56f
- Severity:** High
- Status:** Active
- Activity time:** 07/18/25, 04:21 PM
- Description:** SQL Server potentially spawned a Windows command shell and accessed an abnormal external source.
- Alert description:** A suspicious SQL statement potentially spawned a Windows command shell with an external source that hasn't been seen before. Executing a shell that accesses an external source is a method used by attackers to download malicious payload and then execute it on the machine and compromise it. This enables an attacker to perform malicious tasks under remote direction. Alternatively, accessing an external source can be used to exfiltrate data to an external destination. To investigate this alert, try to identify the caller or application, based on application name and IP/location. Review the vulnerable statement itself: was it expected? Does it look suspicious? Is the external source familiar? Can you identify the owner for further clarity? Review the audit logs (if they're enabled) to understand the activity that resulted from the statement. Consider taking actions to protect the impacted resources (database and host machine) from further tampering. In some cases, the alert might be triggered by unscheduled maintenance activities.
- Last updated time:** 07/18/25, 04:21 PM
- Affected resource:** corp-sql-02 : arc1

The alert also includes a sidebar with security recommendations:

- Using Azure Activity and audit Logs, review all activities performed by the compromised user / IP address.
- Change the credentials for all resources that the compromised user had permissions to.
- Review the permissions for the database and remove permissions for any unfamiliar user account. Review all Defender for Cloud alerts related to this resource and investigate them. If you have audit logs turned on, review activities performed on this resource from the compromised user / IP address and investigate any suspicious activity.
- Protect all accounts that have access to the database using highly complex passwords, and avoid using built-in or known user accounts (e.g., "SA").

Below the recommendations, there's a section for "Prevent future attacks" with three items:

- SQL servers on machines should have vulnerability findings resolved
- Machines should be configured to periodically check for missing system updates
- Windows servers should be configured to use secure communication protocols

Solving security recommendations can prevent future attacks by reducing attack surface. There are links to "View all 5 recommendations" and "Trigger automated response".

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

The screenshot shows the Microsoft Defender for Cloud Inventory page. The left sidebar has sections like General, Setup, Recommendations, Attack path analysis, Security alerts, and Inventory. Under Inventory, there are links for Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems, Cloud Security, Security posture, Regulatory compliance, Workload protections, Data and AI security, Network security, DevOps security, and Management. The main area shows a summary of resources: Total resources (70), Unhealthy resources (49). Below this, it shows Resource count by environment: Azure (70), AWS (0), GCP (0). A table lists individual resources with their names and resource types. At the bottom, there are navigation buttons for < Previous, Page 1 of 2, Next >.

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)
-