Title: Cybersecurity Home Lab with Microsoft Sentinel
Duration: Self-paced project (Completed Jan 2026)
Description: Built a fully functional cybersecurity home lab from scratch using Microsoft Sentinel to detect, analyze, and respond to simulated cyber attacks in a controlled environment.

Objectives Achieved

- ✅ Set up a complete cybersecurity monitoring environment from zero
- ✅ Configured Microsoft Sentinel for real-time threat detection
- ✅ Implemented attack simulation and detection mechanisms
- ✅ Created custom analytics rules and workbooks
- ✅ Established incident response workflows
- ✅ Developed practical threat hunting skills

Technical Stack

- SIEM Platform: Microsoft Sentinel
- Data Sources: Windows Event Logs, Sysmon, Security Logs
- Virtualization: Hyper-V / VMware Workstation
- Operating Systems: Windows Server 2022, Windows 10/11
- Network Components: Virtual Switches, Firewall Rules
- Tools Used: Azure Portal, Log Analytics Workspace, KQL (Kusto Query Language)

Key Implementation Steps

1. Environment Setup

- Configured virtual network with isolated segments
- Deployed Windows Server 2022 as domain controller
- Set up Windows 10/11 client machines
- Established proper DNS and Active Directory services

2. Microsoft Sentinel Configuration

- Created Log Analytics Workspace in Azure
- Onboarded Microsoft Sentinel solution
- Connected Windows Security Events via MMA/AMA agents
- Configured data collection rules for relevant security events

3. Security Monitoring Implementation

- Deployed Sysmon for enhanced visibility
- Configured Windows Event Forwarding
- Set up custom data connectors
- Implemented watchlists for IPs and indicators

4. Threat Detection Development

- Created analytics rules for common attack patterns:
    - Brute force attacks (RDP, SMB)
    - Suspicious process creation
    - Lateral movement detection
    - Data exfiltration attempts
    - Privilege escalation indicators

5. Incident Response Setup

- Configured automation rules for alert triage
- Set up playbooks for automated response
- Created incident classification taxonomy
- Established investigation workflows

Skills Demonstrated

- SIEM Implementation: Microsoft Sentinel deployment and configuration
- Threat Detection: Analytics rule creation using KQL
- Log Management: Centralized logging architecture
- Incident Response: Security operations workflow design
- Network Security: Segmentation and monitoring

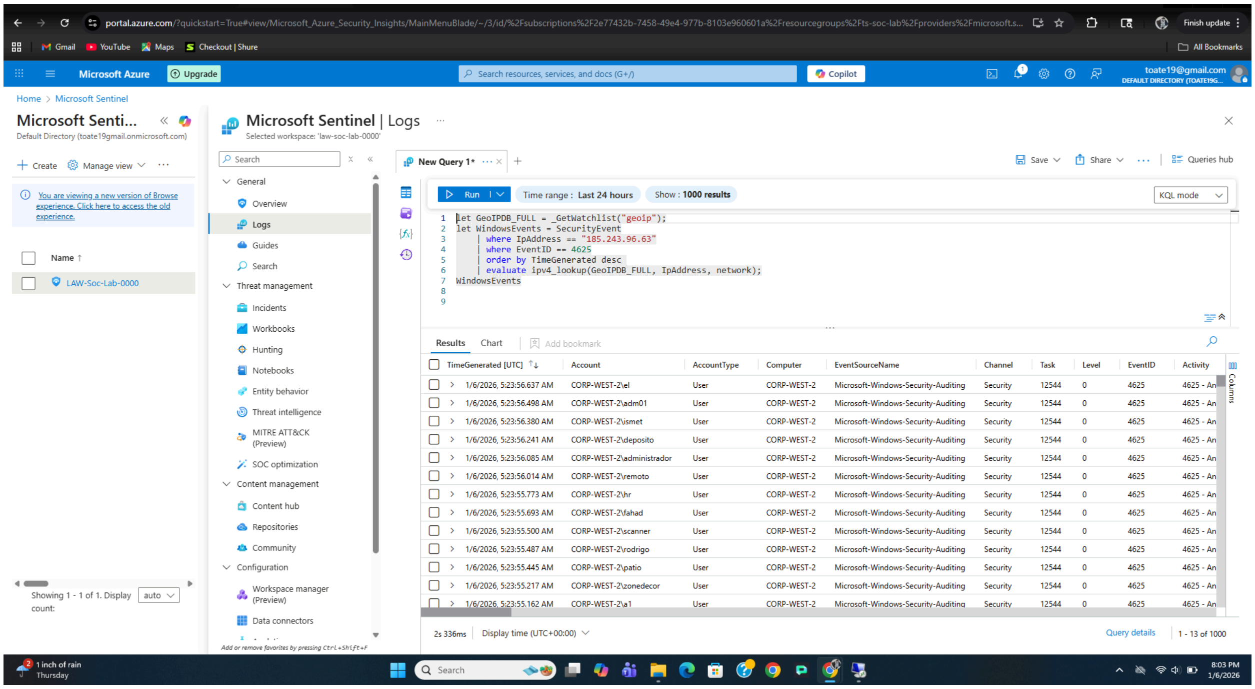
- Cloud Security: Azure security services integration

Learning Outcomes

- Gained hands-on experience with enterprise SIEM solutions
- Developed understanding of attacker TTPs (Tactics, Techniques, Procedures)
- Learned to write effective detection queries using KQL
- Understood the complete SOC workflow from detection to response
- Acquired skills in security architecture design for monitoring

Project Impact

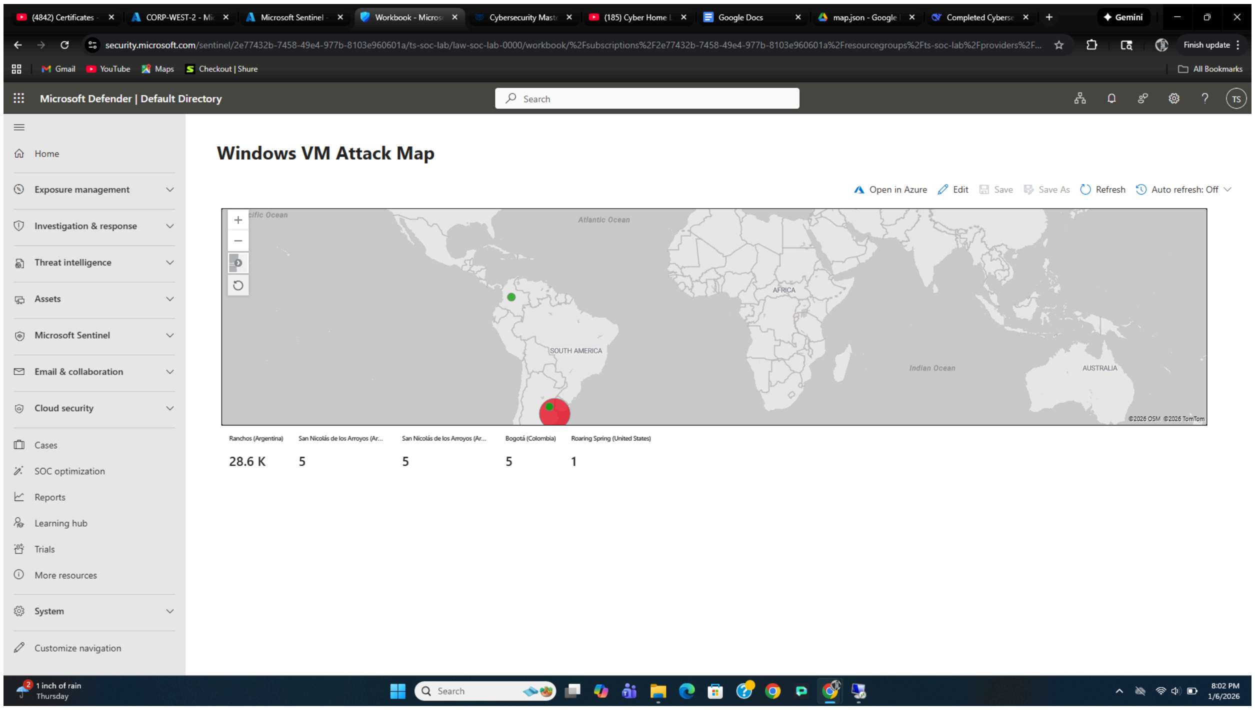
- Created a realistic training environment for continuous skill development
- Developed reusable detection content for common attack vectors
- Built a foundation for advanced threat hunting exercises
- Established methodology for testing security controls



```
let GeoIPDB_FULL = _GetWatchlist("geoip");
let WindowsEvents = SecurityEvent
    | where IpAddress == "185.243.96.63"
    | where EventID == 4625
    | order by TimeGenerated desc
    | evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
WindowsEvents
```

TimeGenerated [UTC]	Account	AccountType	Computer	EventSourceName	Channel	Task	Level	EventID	Activity
1/6/2026, 5:23:56.637 AM	CORP-WEST-2\el	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:56.498 AM	CORP-WEST-2\adm01	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:56.380 AM	CORP-WEST-2\ismet	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:56.241 AM	CORP-WEST-2\deposito	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:56.085 AM	CORP-WEST-2\administrador	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:56.014 AM	CORP-WEST-2\remoto	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.773 AM	CORP-WEST-2\hr	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.693 AM	CORP-WEST-2\fahad	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.500 AM	CORP-WEST-2\scanner	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.487 AM	CORP-WEST-2\rodrigo	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.445 AM	CORP-WEST-2\patio	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.217 AM	CORP-WEST-2\zonedecor	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An
1/6/2026, 5:23:55.162 AM	CORP-WEST-2\a1	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An

2s 336ms | Display time (UTC+00:00) | Query details | 1 - 13 of 1000



Windows VM Attack Map

Ranchos (Argentina)	San Nicolás de los Arroyos (Ar...	San Nicolás de los Arroyos (Ar...	Bogotá (Colombia)	Roaring Spring (United States)
28.6 K	5	5	5	1