







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

The screenshot displays the Microsoft Sentinel interface in a web browser. The left sidebar shows the navigation menu with options like Overview, Logs, Guides, Search, Threat management, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Content hub, Repositories, Community, Configuration, Workspace manager (Preview), and Data connectors. The main pane is titled 'Microsoft Sentinel | Logs' and shows a KQL query being executed. The query is as follows:

```
1 let GeoIPDB_FULL = GetWatchlist('geoip');
2 let WindowsEvents = SecurityEvent
3   | where IpAddress == '185.243.96.63'
4   | where EventID == 4625
5   | order by TimeGenerated desc
6   | evaluate ipv4_lookup(GeoIPDB_FULL, IpAddress, network);
7 WindowsEvents
8
9
```

The results are displayed in a table with columns: TimeGenerated [UTC], Account, AccountType, Computer, EventSourceName, Channel, Task, Level, EventID, and Activity. The table shows 10 results, all from the 'CORP-WEST-2' environment, representing various user accounts and their security events.

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\ismit	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\administrator	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\ahad	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\ia1	User	CORP-WEST-2	Microsoft-Windows-Security-Auditing	Security	12544	0	4625	4625 - An

The bottom of the screen shows the Windows taskbar with the time 8:03 PM on 1/6/2026.

Microsoft Defender | Default Directory

Home

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Email & collaboration

Cloud security

Cases

SOC optimization

Reports

Learning hub

Trials

More resources

System

Customize navigation

Windows VM Attack Map

[Open in Azure](#) [Edit](#) [Save](#) [Save As](#) [Refresh](#) [Auto refresh: Off](#)

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

1 inch of rain
Thursday

Search

8:02 PM
1/6/2026