

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 shows the Microsoft Sentinel Logs page. On the left, there's a navigation sidebar with options like Create, Manage view, General, Logs, Guides, Search, Threat management, Incidents, Workbooks, Hunting, Entity behavior, MITRE ATT&CK (Preview), SOC optimization, Content management, Content hub, Repositories, Community, Configuration, Workspace manager (Preview), and Data connectors. A message indicates you're viewing a new version of the Browse experience. Below the sidebar, there's a tree view showing a workspace named 'LAW-Soc-Lab-0000'.

In the main area, there's a search bar at the top with the placeholder 'Search resources, services, and docs (G+)', a Copilot button, and a 'Run' button. To the right of the search bar, it says 'Time range: Last 24 hours' and 'Show: 1000 results'. Below this, there's a 'KQL mode' dropdown and a 'Save' button.

The central part of the screen displays a table of log results. The columns are: TimeGenerated (UTC), Account, AccountType, Computer, EventSourceName, Channel, Task, Level, EventID, and Activity. There are 1000 results listed, each with a checkbox and a small icon. At the bottom of the results table, it says '2s 336ms | Display time (UTC+00:00)' and 'Query details | 1 - 13 of 1000'.

At the very bottom of the page, there's a taskbar with various icons and a system status bar showing '1 inch of rain Thursday' and the date '1/6/2026'.

```

let GeoIPDB_FULL = GetIngestList("geolite");
let WindowsEvents = SecurityEvent
| where IpAddress == "185.243.96.63"
| where EventID == 4625
| project TimeGenerated desc
| evaluate ipv4_lookup(GeoIPDB_FULL,IpAddress, network);
WindowsEvents
    
```

Screenshot of a Microsoft Defender interface showing a Windows VM Attack Map.

The left sidebar navigation includes:

- 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

The main content area displays a world map titled "Windows VM Attack Map". The map shows several green dots indicating attack locations. A legend below the map provides the following data:

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

Map controls include zoom (+/-), location search (magnifying glass), and a refresh button. Navigation buttons for "Open in Azure", "Edit", "Save", "Save As", and "Auto refresh" are also present.

The taskbar at the bottom shows various pinned icons and the system tray indicates "1 inch of rain Thursday". The system clock shows "8:02 PM 1/6/2026".