SIEM Detection Rules Lab - Sentinel VM

Cover Page

- Name: Marcus Ashmond
- Date: 1/10/2026
- Project Title: SIEM Detection Rules Lab
- Description: This project demonstrates SIEM detection rules using Windows Security logs from a test VM. Detection rules were written, and simulated alerts were generated based on real event data.

Introduction / Objective

The goal of this lab is to simulate SIEM detection rules in a Windows VM without using live Azure Sentinel. Security event logs were analyzed, and detection rules were created for successful logons, failed logons, new user accounts, and account deletions.

Detection Rule Pages

Rule 1 - Multiple SYSTEM Service Logons

- EventID: 4624 (Successful logon)
- LogonType: 5 (Service logon)
- TargetUserName: SYSTEM
- ProcessName: C:\Windows\System32\services.exe
- Computer: sentinel-winvm
- Condition: Count >= 3 logons within 5 minutes

Event Details Table:

Time | EventID | TargetUserName | LogonType | ProcessName | Computer

1/10/2026 9:27:38 PM | 4624 | SYSTEM | 5 | services.exe | sentinel-winvm

1/10/2026 9:27:40 PM | 4624 | SYSTEM | 5 | services.exe | sentinel-winvm

1/10/2026 9:28:30 PM | 4624 | SYSTEM | 5 | services.exe | sentinel-winvm

Simulated Alert:

ALERT: Multiple SYSTEM service logons detected on sentinel-winvm between 9:27-9:28 PM

Rule 2 - Multiple Failed Logons

- EventID: 4625

- Condition: More than 3 failed logins per user within 1 hour

Simulated Alert Example:

ALERT: User JohnDoe failed login 5 times between 10:00-11:00

Rule 3 - New User Account Created

- EventID: 4720

- Condition: Any new user account creation triggers an alert

Simulated Alert Example:

ALERT: New account 'JohnTest' created at 11:15 AM

Rule 4 - User Account Deleted

- EventID: 4726

- Condition: Any account deletion triggers an alert

Simulated Alert Example:

ALERT: Account 'TempUser02' deleted at 02:40 PM

Conclusion

All rules were simulated using Windows Security logs from the test VM. Alerts were generated in notes and Excel, demonstrating SIEM logic and threat detection workflow.

Optional Screenshots

- Event Viewer showing filtered logs

- Pivot tables for counting failed logins