Windows Security Event Log Analysis

Tool Used: Microsoft Excel

Dataset: Simulated Windows event logs (~9 million entries)

Project Type: Security triage using PivotTables and charts

Project Overview:
This project simulates the kind of log triage a junior SOC analyst might perform when investigating unusual system activity. While larger environments often use SIEM tools, Excel is still a great way to learn how to work with raw event logs. It helps build foundational skills like spotting patterns, identifying suspicious trends, and understanding how different event types relate to each other. This hands-on method keeps you close to the data, reinforces how to think like an analyst, and allows you to clearly document and present findings in a way that is easy to share with technical teams or stakeholders.

Key Findings:

- March showed an unusually high spike in log volume, with over 6 million events recorded that month
- Most of these events were associated with Event ID 4624, which indicates successful logon attempts
- A deeper look revealed that the system MSEDGEWIN10 generated repeated events at the exact same timestamp
- The repetition and volume suggested automation, possibly from a scheduled task, script, or misconfiguration
- Additional PowerShell-related events were observed around the same time, supporting the idea of scripted activity

Figure1: Pivot chart showing a dramatic spike in log volume during March

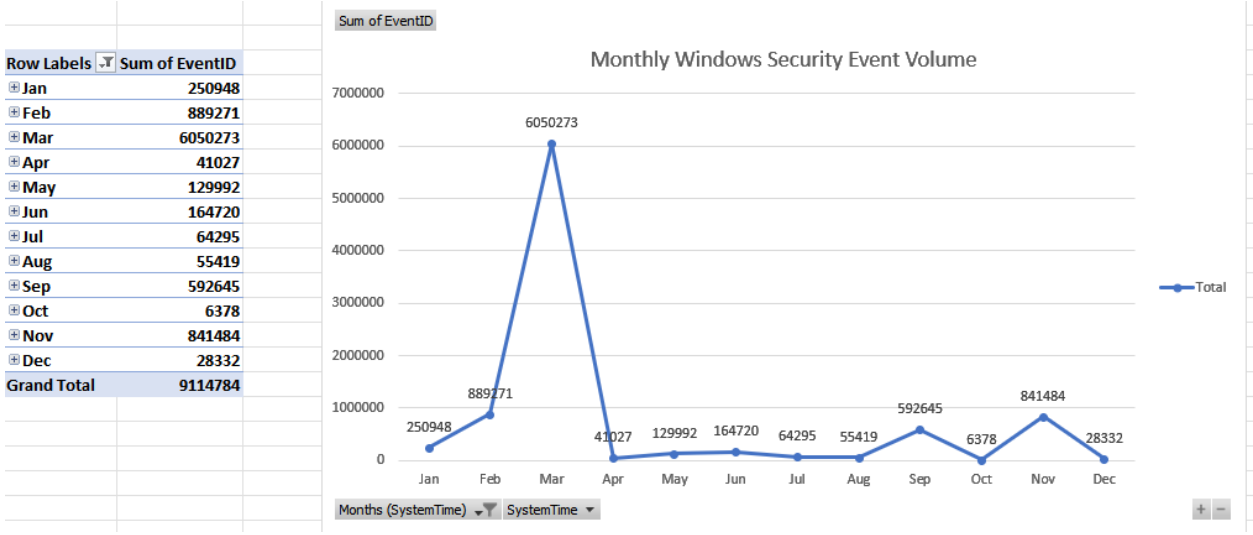

Figure 2: Detailed breakdown of a repetitive Event ID activity from MSEDGEWIN10

Details for Count of EventID

Channel	Computer	EventID	SubjectUserName	SystemTime
Microsoft-Windows-PowerShell/Operational	MSEDGEWIN10	40961		3/12/2019 14:23
Microsoft-Windows-PowerShell/Operational	MSEDGEWIN10	53504		3/12/2019 14:23
Microsoft-Windows-PowerShell/Operational	MSEDGEWIN10	40962		3/12/2019 14:23
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27
Application	MSEDGEWIN10	33205		3/6/2019 9:27

Conclusion:

This investigation demonstrates how basic log data, when properly visualized and analyzed, can reveal potentially abnormal system activity. By identifying a sharp increase in logon events tied to a single endpoint, I was able to detect patterns that may indicate misconfiguration or scripted behavior.

Presenting the data visually made the anomaly easy to spot and explain, while the documentation supports how findings can be communicated to technical teams or non-technical stakeholders. This process highlights the importance of both technical analysis and clear reporting in effective cybersecurity practices.