Cyber Operations Log Analysis for Threat Actors

Student Credits: Ethan Healey, Emily Pascetta, Logan McKinley, Will Gawron, Aaron Limbat, and Christopher Thorn
Advisor: Professor Lisa Henry | Project Owners: Tom Nodd, David Yasenchock, Joseph Gray, and Joshua Annis

Introduction

The University System of New Hampshire experiences constant student and staff activity, generating vast amounts of log data every second. With various login methods, this influx can lead to numerous false alarms. The Cyber Security team is responsible for reviewing these logs, which are aggregated in Splunk, and correlating data to help analysts focus on true positive incidents. This is achieved by developing new detection rules and refining or filtering out inefficient ones. The project aims to reduce false positives by 15% per use case, significantly decreasing the volume of false positive alerts.

Requirements

Functional Requirements:

- Search & querying logs In Splunk
- Dashboards & visualization to support alerts
- Alerts to warn of suspicious activity
- Alerts must be associated with at least three techniques from the MITRE D3FEND framework

Non-Functional Requirements:

- Queries must perform at fast & efficient speeds
- Availability - alerts need to be running at all times
- Alerts must be sent only to appropriate users
- Dashboards must be easy to navigate with only necessary information
- Alerts must be scalable and able to accommodate for increasing user traffic

Project Design

Our project uses Splunk, a cloud-based logging tool, to collect, filter, and analyze data from various sources (Figure 01). It triggers alerts based on set conditions, helping analysts focus on relevant threats.

Use Cases Developed:

- Account Takeover detection is part of the 'Connection Attempt Analysis' use case and leverages multiple factors—like those shown in Figure 1
- User Activity Analysis crafts network baselines in order to detect anomalies in traffic for general population accounts.
- Domain Account Monitoring uses domain monitoring services to detect misconfigurations and malicious activity.

Project Design - Figure 01

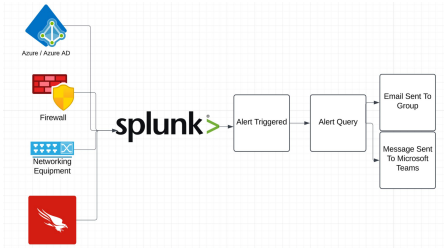
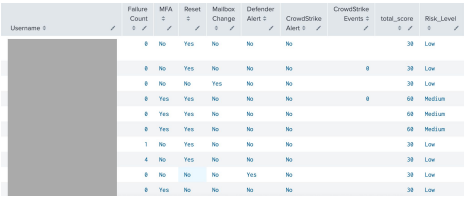


Figure 01 shows icons representing different tools that send logs to Splunk, along with a high-level overview of the behind-the-scenes logic and process flow

- Splunk extracts relevant fields and information, making them available for querying.
- Alerts can be created based on predefined criteria when conditions are met.
- Notifications are typically sent to analysts via Microsoft Teams channels.
- Email notifications can also be used when necessary.

Results - Figure 02



Username	Failure Count	MFA	Reset	Mailbox Change	Defender Alert	CrowdStrike Alert	CrowdStrike Events	total_score	Risk_Level
[redacted]	0	No	Yes	No	No	No		30	Low
	0	No	Yes	No	No	No	0	30	Low
	0	No	No	Yes	No	No		30	Low
	0	Yes	Yes	No	No	No	0	60	Medium
	0	Yes	Yes	No	No	No		60	Medium
	0	Yes	Yes	No	No	No		60	Medium
	1	No	Yes	No	No	No		30	Low
	4	No	Yes	No	No	No		30	Low
	0	No	No	No	Yes	No		30	Low
	0	Yes	No	No	No	No		30	Low

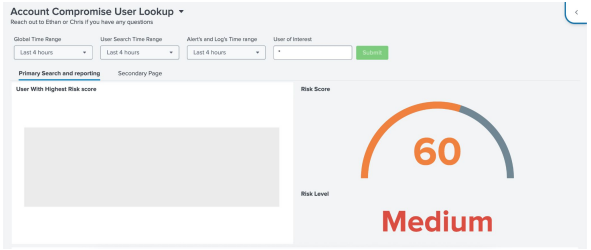
The team developed alerts to enhance security monitoring by correlating and alerting on real-time data. Using SPL queries, alerts transform raw data into visual tables that can use key metrics like risk score to alert on. Figure 02 illustrates how one of our alerts displays information for analysts to investigate:

- **Purpose:** Detects potential account compromise by analyzing security events within a short time frame. Sends an alert to a Microsoft Teams channel or email group if an alert is triggered.
- **Trigger Mechanism:** If certain high-risk events occur within **4 hours**, they add **30 points** to the total score
- **Alert Threshold:** A risk score of **90** or higher triggers an alert
- **Findings:** This alert detected one account takeover during its three-month implementation, matching UNH's statistics. It effectively minimized false positives, triggering only on true threats.

Key Risk Factors:

- Password Change
- MFA Device Registration
- Microsoft Defender Alerts
- Email Mailbox Rule Changes

Splunk Dashboards - Figure 03



Purpose of Dashboards: Enhance security monitoring by visualizing real-time and historical log data

Data Processing: Utilizes SPL or splunks custom query language to aggregate and transform raw log data into charts, tables, and graphs

Structure: Dashboards consist of multiple panels, allowing analysts to monitor various data sets in one place

Benefits:

- Provides actionable insight for threat detection
- Streamlines investigations by centralizing key information
- Ensures all relevant data is readily available

Figure 03 provides an example of a dashboard we created that visualizes the compromised account alert. The dashboard contains additional information not shown here due to NDA constraints, but it allows user specific lookup so a more in depth dive on one entity can be done.

Implementation & Testing

Alerts were developed using **MITRE D3FEND** use cases and built with **SPL Queries** to detect specific activity patterns. Testing involved simulating threats with **test UNH accounts** to validate alert functionality. To reduce analyst workload, alerts were sent to a separate **Microsoft Teams** channel for verification.

- **Framework**: Based on **MITRE D3FEND** security use cases
- **Query Design:** SPL queries detect and return events matching threat patterns
- **Testing**: Simulated alerts using **test USNH accounts** to ensure accuracy
- **Notification System:** Alerts routed to **Microsoft Teams** for verification
- **Current Status:** Several alerts implemented with ongoing refinements

Conclusions

In summary, our project has enhanced the USNH threat detection system by minimizing false positives by 15% per use case, exceeding our targeted threshold as outlined in our MOV or Measurable Organizational Value. By improving detection accuracy for key attack scenarios, and thus minimizing the amount of alerts, we reduced alert fatigue for both analysts and the system.

The alerts and dashboards created during the course of the project will be used by the analysts and future student workers to further the effectiveness and efficiency of Splunk and Enterprise Security.

Tools Used

- **Splunk**
  - Used to filter logs from multiple sources and build dashboards
- **SPL (Splunk's internal query language)**
  - Used to generate searches and alerts
- **Office 365, Azure, CrowdStrike, Palo Alto, Active Directory, Microsoft Entra/Defender**
  - Aided in data correlation, verification, and fact-checking