FIU Knight Foundation School of Computing and Information Sciences

Design & Implementation of a Lightweight Security Operations Center (SOC) Using Splunk Enterprise

Cybersecurity

The Problem

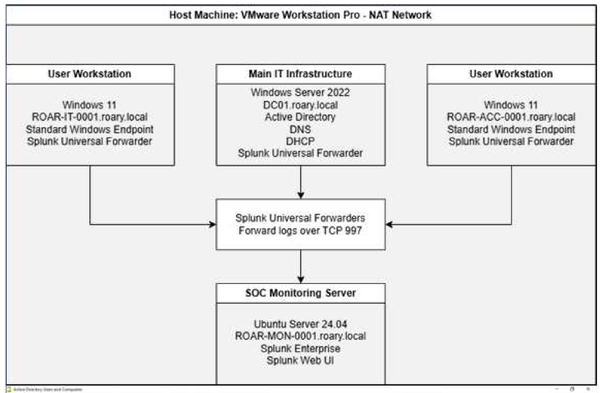
- Small to medium sized organizations lack dedicated SOC due to budgeting constraints and technical limitations. Without centralized event log collection, continuous monitoring, and defined incident response procedures, security incidents may fly under the radar, increasing the risk of data breaches, operational disruption, and financial loss.
- Outsourced SOC services typically cost $120,000–$360,000 annually for small and mid-sized organizations, while building an in-house SOC averages $1–4 million per year.
- Data breaches contained within 200 days averaged $3.74 million, compared with $4.86 million when the breach lifecycle exceeded 200 days.

Our Solution

This project implements a lightweight Security Operations Center (SOC) within a simulated enterprise environment using Windows Server Active Directory, Windows 11 endpoints, Ubuntu Server, and Splunk Enterprise. Splunk Universal Forwarders centralize Windows Event Logs to provide real-time monitoring, custom dashboards, and alerting for authentication activity, account lockouts, and administrative changes. The solution demonstrates how organizations can implement cost-effective security monitoring using widely available technologies without the complexity and expense of traditional enterprise SOC deployments.

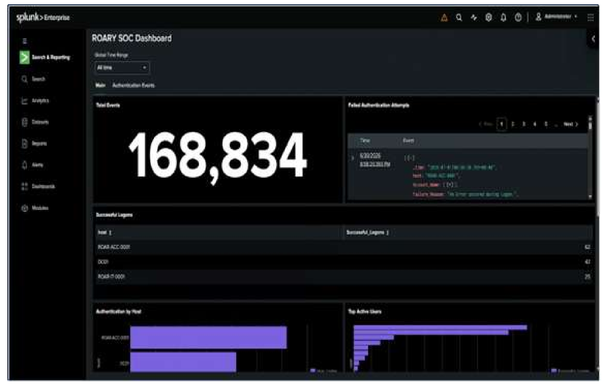
- Centralized security monitoring with minimal operational overhead.
- Cost-effective alternative to traditional enterprise SOC deployments.
- Scalable architecture supporting organizational growth.

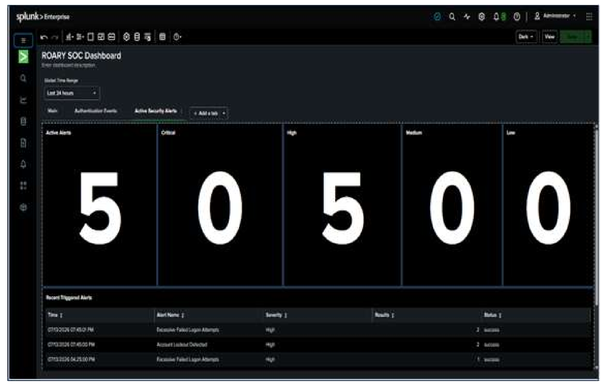
Architecture & How It Works



- Figure #1: Simulated enterprise SOC architecture with centralized log collection using Splunk Enterprise. Windows Event Logs are forwarded for real-time monitoring and analysis.
- Figure #2: Active Directory Organizational Unit (OU) hierarchy for users, groups, servers, and workstations. Supports centralized administration and scalable policy management.
- Figure #3: Risk matrix illustrating the assessment and prioritization of cybersecurity threats based on likelihood and business impact.

Key Features & Results





- Figure #4: Centralized dashboard providing real-time visibility into authentication activity and security events.
- Figure #5: Automated Splunk alerts generated from simulated security events for rapid incident detection.

The implemented lightweight Security Operations Center successfully centralized Windows Event Logs, provided real-time security monitoring, and generated automated alerts for simulated security events. By leveraging widely available technologies such as Splunk Enterprise and Active Directory, the solution demonstrates that organizations can achieve enterprise-level visibility and incident detection without the cost and complexity of traditional SOC deployments. Its modular design also provides extensive configuration flexibility, allowing organizations to expand monitoring capabilities and adapt security controls as operational requirements evolve.

The Team

Rudolph S Durosier — Team Lead

Gabriel Santana — Infrastructure & SOC Engineer

Joshua Aranzazu — Governance, Risk, & Compliance Analyst

Sandro Kelekhidze — Risk Assessment & Policy Analyst

Andre Niovel Lara — SIEM Integration Analyst

Technologies

- Infrastructure:
  - VMware Workstation Pro
  - Windows Server 2022
  - Windows 11 Enterprise
  - Ubuntu Server 24.04
- Security:
  - Splunk Enterprise
  - Splunk Universal Forwarder
  - Search Processing Language (SPL)
- Enterprise Services:
  - Active Directory
  - Group Policy
  - Domain Name Server (DNS)
  - Dynamic Host Configuration Protocol (DHCP)

Acknowledgments

- Prof. Masoud Sadjadi — Knight Foundation School of Computing and Information Sciences

References

- [1] Total Assure. *Outsourced SOC Costs.* https://www.totalassure.com/blog/outsourced-soc-costs
- [2] UpGuard. *The Cost of a Data Breach.* https://www.upguard.com/blog/cost-of-data-breach
- [3] AlertMedia. *What Is a Risk Matrix?* https://www.alertmedia.com/blog/risk-matrix/