Regional Insurance Group SIEM Implementation

SIEM Tool Selection

Reginal Insurance Group should implement Splunk enterprise security as your SIEM solution. It has a proven effectiveness when it comes to logs. Including log aggregation and real time analysis. Splunk includes a strong correlation engine and advanced threat detection tools and capabilities. It is compatible with both firewall and VPN log formats. Splunk is a long trm solution that fits with any size business and is scalable to future growth as a company. Splunk is also a great choice because it is a well documented system which provides support for the security team.

Other tools that were considered include IBM QRadar, Microsoft Sentinel, and DataDog. While these tools are viable options, Splunk offers the best balance of usability, and scalability. Splunk also comes with a MITRE ATT&CK Matrix that allows security analysts to build situational awareness about incidents. Having that built in is a great added bonus and just another reason to go with splunk.

Network Security Objectives

Implementing a Splunk SIEM system will support all of the following network security objectives:

- Centralized Log Management
- Threat Detection and Response
- Secure Remote Access Monitoring: Very important considering a VPN is being implemented for all remote workers which will make up most of the company
- Regulatory Compliance

- Incident Investigation
- Reduced Response Time: Automatic alerts for security incidents, time is so important when it comes to responding to potential security breaches or issues.

Data Sources Integrated

Many data sources will be integrated into the SIEM system in order to best keep track of any security incidents across the network. This includes:

1. Firewall Logs
2. VPN Logs
3. Server Logs
4. Enpoint Security Logs
5. Router logs
6. SWitch Logs
7. Active Directory Logs
8. Web server Logs

This may seem like a lot but splunk will be able to help the security team keep tabs and respond to any security incidents as needed.

Proposed SIEM Rules

The following rules are what make the SIEM system work. These rules will tell Splunk when to generate alerts so that the security team can give the issue immediate attention.

Authentication-Based Rules

- Detect multiple failed login attempts (brute force attacks)
- Identify login attempts outside normal working hours
- Alert on privileged account misuse

Network Activity Rules

- Detect unusual outbound traffic patterns
- Identify communication with known malicious IP addresses
- Detect port scanning behavior

VPN-Specific Rules

- Multiple failed VPN login attempts
- Simultaneous logins from different geographic locations
- Connections from blacklisted or suspicious IP addresses

Firewall-Based Rules

- Repeated denied connections from a single source
- Detection of unusual port or protocol usage
- IDS/IPS alert correlation

Data Exfiltration Rules

- Large or abnormal data transfers
- Unusual file access patterns

Alert Configurations

While the rules tell Splunk when to send alerts, alert cnfigurations tell whoever is responding to the alerts what the severity of the issue is which tells the security professional how much immediate attention should be given to the issue. For example if you were working on a low level alert and a critical alert comes in, attention should be given to the critical alert until the issue is resolved. All alerts should be given attention and all the issues should be fixed in a timely manner but the following configurations show which issues should be addressed first

Critical Level Alerts

- Confirmed intrusion attempts
- Malware detected on critical systems
- Unauthorized privileged access

High Level Alerts

- Brute force login attempts
- Suspicious VPN activity
- Communication with malicious IP addresses

Medium Level Alerts

- Policy violations
- Unusual but non-critical traffic patterns

Low Level Alerts

- Informational events for auditing purposes

Alerts should be delivered in a safe and secure, and reliable manner. For most cases an email notification to the security team, push notifications on a specific system and for the most critical alerts a text message alert. The alerts should be regularly reviewed to limit the number of false positives.

References

O'Donnell, J. (2026, February 1). *Making Siem alerts smarter: Best practices for real-world detection*. Cymulate. https://cymulate.com/blog/smarter-siem-alerts-validation/

SentinelOne. (2026, January 8). *Top 10 SIEM tools for 2026*. https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-tools/

What is splunk? key benefits and features of Splunk. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/what-is-splunk