SIEM and SOAR Implementation for Unified Security Operations

Deployment of an integrated SIEM and SOAR platform that centralizes security event data, correlates threats across sources, and automates response playbooks to reduce analyst workload and improve mean time to respond.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

Federal SOC or cybersecurity team needing centralized threat detection, log correlation, and automated incident response across hybrid infrastructure

Challenge

- Security events scattered across siloed tools with no centralized correlation
- Alert fatigue from high volumes of untuned alerts overwhelming SOC analysts
- Manual incident response processes leading to slow containment times

Approach

- Design centralized log ingestion architecture with parsing for all critical data sources
- Tune detection rules and alert thresholds to reduce false positives and prioritize high-fidelity alerts
- Implement SOAR playbooks for automated triage, enrichment, and containment of common incident types
- Build SOC dashboards and executive reporting for threat landscape visibility

Typical Outcomes

- Centralized visibility across all security event sources with correlated alerting
- Reduced mean time to detect and respond through automated playbooks
- Freed analyst capacity for threat hunting and proactive defense activities

Procurement Paths

- DoD ESI for Elastic and Palo Alto Networks security platforms
- NASA SEWP V and SEWP VI for SIEM/SOAR infrastructure
- GSA MAS for SOC engineering and integration services

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- Elastic Security
- Palo Alto Networks (Cortex XSOAR)
- CrowdStrike
- Splunk

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.