MANAGED DETECTION AND RESPONSE

NuSpective delivers and manages the Technology and People to perform complete and affordable Cybersecurity Operations and Compliance Monitoring

Features Summary

- Fully Managed SIEM
- Log Analytics & Management
- 24X7 Security Operation
- Customized Detection Rules
- Remediation Guidance
- Compliance Reporting

Log Analytics


24X7 Threat Hunting


Incident Remediation Guidance


Compliance Reporting


SIEM Techbology

Managed SIEM

- Managed HW, SW, and Licenses
- Log Analytics & Management including:
  - Log correlation, tuning, and alerting
  - Comprehensive and extensible analytics
  - Security and anomalous activity monitoring
  - Prioritized security incidents with raw and correlated details
  - Powerful layer-7 rules engine
- Asset Discovery & Inventory:
  - Self Learning, Asset Inventory with Configuration Management Database (CMDB)

Security Operations Center

- Staffed 24x7x365 by trained SOC Security Analysts
- Alert Monitoring & Scoring
- Daily review of ALL severity level incidents
- Daily/ Manual Threat Hunting
- Forensic Investigation
- Remediation guidance & triage support

Interactive Dashboard & Reporting

- Dynamic dashboards, topology maps, and notifications
- Live active threat monitoring from SWAT feedback
- Presents security analyst review & other SOC input

Compliance Reporting & Automation

- Daily Compliance Reviews
- Compliance Out-Of-The-Box:
  - PCI, SOX, FFIEC, COBIT, ISO, HIPPA, ITIL

NuSpective Solutions
nuspective.com
(925) 271-7557