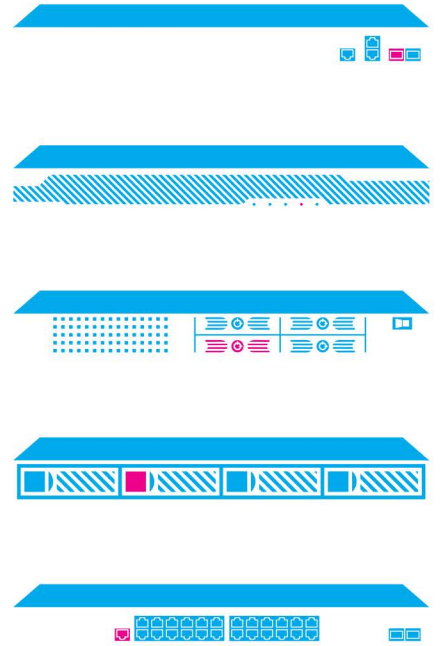


Securing critical data assets is **critical** to business objectives.



Correlated events trigger Incident Response, but uncorrelated **events** create noise.

Security Staffing

Process Building

System Tuning



Costly

Difficult

Tedious

Staged Security | Intel Automation
Information Risk Practice by



Readiness Workshop

Company Preparation

We help enterprises identify the foundations of SIEM readiness and develop cost effective SIEM capabilities. We help define the scope of security solutions to be managed or co-managed, which may include SIEM, Firewall, IDS, & VPN.

STAGE 1

\$35,000

Timeframe:

4 weeks

Deliverables:

- Asset criticality documentation
- Security monitoring strategy
- Business case development
- Event handling processes

SIEM Deployment

Turnkey Construction

We architect and deploy instances of **AlienVault** SIEM to suit business objectives, network topologies, and the critical data & systems assets of enterprises. We train staff on basic and advanced SIEM operational functionality.

STAGE 2

Starting at \$45,000

Timeframe:

6 weeks

Deliverables:

- AV console & monitoring systems
- Asset inventory & network map
- Work detail (defined by SOW)
- IR guide & escalation details

AlienVault MSSP

SOC Monitoring

Managed AlienVault SIEM

- Platform health & uptime
- Updates & upgrades

Managed Security Operations

- Incident detection & triage
- Escalation to customer

Vulnerability & Threat Reporting

- Malicious probe identification
- Compromised system flagging
- Correlated event reporting

STAGE 3

node-based pricing

