DATA SHEET

SECURITY INCIDENT DETECTION & RESPONSE

SIEM Based Security Monitoring

AT A GLANCE

Increasing threat volume, sophistication and the proliferation of our customers' networks is driving a requirement for advanced real-time alerting, event correlation, analysis and auditing. Organizations need to reconcile the fact that not all threat risks can be prevented or mitigated, data breaches will occur. Your fate will be determined by the accuracy and speed of response.

Our real-time monitoring services address these issues and are 24x7, scalable, compliant and cost effective. With over 20,000 devices under management, our cloud-based service is secured across our redundant global Security Operations Centres (SOCs) and offers a resilient and dependable service.

HOW IT WORKS

Our global SOCs are located in London, New York, Pune and Dubai and are all backed by certified expert staff. We provide around-the clock-support, staffed with security experts who have in-depth knowledge and experience working with complex network environments for highly distributed environments. Our 24x7 monitoring service enables our Clients to focus on delivering their core services whilst we secure their networks and systems.

WHAT DO WE MANAGE?

SERVERS & SYSTEM OS, APPLICATIONS & DATABASES	CORE NETWORK EQUIPMENT	NETWORK SECURITY EQUIPMENT
Security Managed Servers (Windows, Linux, Unix, ESX)	Network Routers / Switches	Managed Firewalls
Applications	Network Wireless LAN	Managed Network IDS or IPS
Databases	Network Load-Balancers / Accelerators	Managed Network VPS Routers
Email Servers		Managed Network AntiSpam / Proxys
		Managed UTMs

CUSTOMER DASHBOARD

Our customers benefit from direct access to our award winning SOC platform, which is powered by LogRhythm. This provides real time security event monitoring, anomaly detection and policy violation. This allows us to correlate event traffic and contextualize logs with threat, policy and vulnerability metrics.

BENEFITS

- Certified & experienced Engineers
- Fault & Change Management
- 24x7 SIEM Incident Detection
- 90 Day Log Retention
- 24x7 Incident Response
- SLA Backed Services
- Reporting (Weekly & Monthly)
- Secure Web Portal (SIEM, Service Management, SLA)
- Firewall Optimization & Rule Reviews

24 X 7 INCIDENT MONITORING

Not all threats can be prevented or mitigated and in the event of a security breach your fate will be determined by your speed to respond.

24x7 Security Monitoring is supported by mature processes, trusted staff and award winning technology.

SECURITY INCIDENT DETECTION & RESPONSE
SIEM Based Security Monitoring

SI CYBER

SERVICE FEATURES

SOURCE HARDWARE	TARGET HARDWARE	INCIDENT MONITORING	FIREWALL MANAGEMENT
Threat Management	24x7 Proactive Security Incident Monitoring	✓	✓
	Detection & Notification	✓	✓
	SIEM & Correlation	✓	✓
	Security Policy Consultation	✓	✓
	Incident Management	✓	✓
Configuration Management	Configuration / Rule reviews	✓	✓
	Firewall Optimisation	✓	✓
Fault Management	Availability Monitoring	✓	✓
	Fault Detection	✓	✓
	Vendor Management		✓
Change Management	Maintain Documentation		✓
	Policy & Signature Configuration Changes		✓
	OS Updates, Patches & Signatures		✓
	Operating System Upgrades		✓
Reporting	Executive Reports, Incident Reports, Compliance and Monthly Reports	✓	✓
Secured Web Portal	LogRhythm SIEM UI, SLA and Service Management	✓	✓

SLA METRICS

SECURITY ALERT NOTIFICATION		
PRIORITY	SEVERITY LEVEL	MEAN RESPONSE TIME
P1	Critical	15 Minutes
P2	Major	45 Minutes
P3	Minor, Informational	120 Minutes

RESOLUTION / ESCALATION		
PRIORITY	SEVERITY LEVEL	MEAN RESPONSE TIME (HRS)
P1	Critical	4
P2	Major	8
P3	Minor, Informational	24

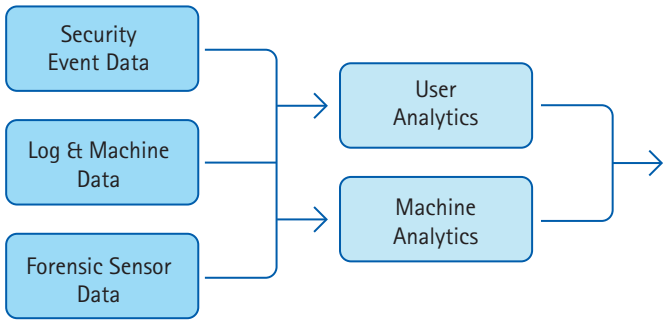
CHANGE MANAGEMENT		TARGET LEAD TIME	
		EVALUATION (HRS)	EXECUTION (HRS)
P1	Emergency	4	4
P2	Planned - Major	120	120
P3	Planned - Minor	72	72
P3	Routine	72	72

INCIDENT DETECTION & RESOLUTION

Within Security Incident Monitoring & Management, success is measured in the speed to detect (MTTD), respond (MTTR) and the quality of the resolution. In simple terms a rapid MTTD + MTTR = Less Time = Less Damage

INCIDENT DETECTION + INCIDENT RESPONSE

TIME TO DETECT



TIME TO RESPOND

QUALIFY	INVESTIGATE	MITIGATE
Assess threat & determine if it possesses a risk & if investigation is required.	Analyse threat and associate risk. Determine if an incident has occurred & prioritise.	Apply triage to isolate incident, contain & recover.

15 Minutes to Notify (P1)

4 Hours to Mitigate

Contact Us: Sales@siconsult.com

www.siconsult.com