DATA SHEET

FIREWALL MANAGEMENT

24x7 Proactive Defense

BENEFITS

- Certified & experienced Engineers
- Fault & Change/Patch 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

Technology Partners:

AT A GLANCE

24x7 monitoring & management of firewalls is a highly skilled operation which is resource intensive and specialist work. Our Managed Firewall service enables our Clients to focus on delivering their core services whilst we secure their networks and systems.

Our Firewall Management service is scalable, cost effective and compliant and is designed for financial, government, healthcare and enterprise customers.

With over 20,000 devices under management, our cloud based service is secured across our redundant global Security Operations Centers (SOCs) and offers a resilient and dependable service.

HOW IT WORKS

Our global SOC network enables us to offer managed firewall services for the leading vendors such as Cisco, Fortinet and Juniper Networks, all backed by certified expert staff. Our SOCs in London, New York, Dubai, Doha and Pune provide around-the clock-support, staffed by security experts who have in-depth knowledge and experience working with complex network environments for highly distributed environments.

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.

FIREWALL MANAGEMENT

Firewall management is part of our DNA. Our certified engineers provide the following services:

- Firewall architecture planning
- Device migration / deployment
- Policy and rule-set management
- Performance / availability management
- Patch management
- Backup and recovery
- Compliance reporting

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.

FIREWALL MANAGEMENT
24x7 Proactive Defense

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 & Resolution		✓
	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

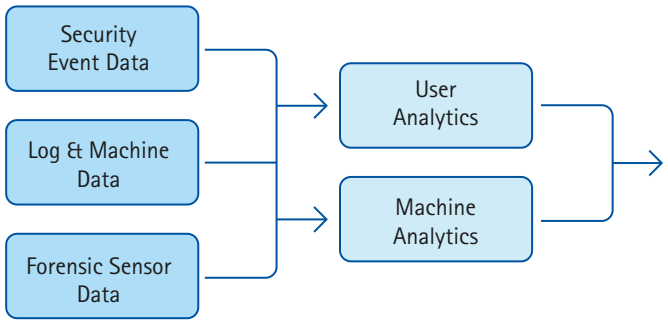
CHANGE MANAGEMENT		TARGET LEAD TIME	
		EVALUATION (HRS)	EXECUTION (HRS)
P1	Emergency	4	4
P2	Planned - Major	120	120
P3	Planned - Minor	72	72
P3	Routine	72	72

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 associated 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