MSSD SOC: MONITORING & ALERTING

More businesses are responding to the deepening cybersecurity skills shortage by entrusting expert engineers to monitor their security infrastructure and begin gaining freedom from resource-intensive cybersecurity management. **MSSD SOC: Monitoring & Alerting** is the perfect foundation for enabling customer ROI from cybersecurity deployments at a predictable recurring cost, with no need for expensive infrastructure, resources or skills.

INTRODUCING MSSD SOC: MONITORING & ALERTING

**MSSD SOC: Monitoring & Alerting** protects organisations and their next-gen security investments through 24/7 firewall monitoring, alerting and reporting. Use it to benefit end customers with:

- Reduced IT security operations costs and skills overheads
- Enhanced security with expert validation of the cyber infrastructure function
- Extended value and greater ROI of deployed cyber solutions
- Greater freedom to focus finite resources i.e. on strategic IT initiatives
- Predictable opex
- Faster incident response via efficient processes and workflow automation

Driven by our global 24/7 SOC, **MSSD SOC: Monitoring & Alerting** is the perfect foundation for enabling customer ROI from cybersecurity deployments at a predictable recurring cost, with no need for expensive infrastructure, resources or skills.

100% CHANNEL READY

**MSSD SOC: Monitoring & Alerting** is a 100% channel product, exclusively for partners to sell to end customers.

- You choose the contract terms (1 / 2 / 3 years)
- Comprehensive SOC portal for live status and reporting tickets
- Email/phone/portal enquiries answered by accredited and experienced engineers
TOP 3 CUSTOMER CHALLENGES

Overstretched IT departments have limited qualified resources to make necessary changes to increasingly sophisticated cyber infrastructure.

- **MSSD SOC: Monitoring & Alerting** fills the skills gap by providing expert oversight of core security infrastructure. Spend less on overtime and training budgets with 24/7 monitoring and alerting.

The variety, volume, intensity and frequency of threats is growing fast.

- **MSSD SOC: Monitoring & Alerting** allows organisations some much-needed breathing space to pursue priorities without worrying about the increasing complexity of cybersecurity challenges.

Organisations are actively seeking IT ‘as-a-service’ approaches that reduce capex liability and allow transition to a leaner opex-based consumption models.

- **MSSD SOC: Monitoring & Alerting** meets the demand for managed security services that is rising x2 faster than for traditional resale business, helping address the needs of finance and IT decision makers.

WHAT’S INCLUDED

**MSSD SOC: Monitoring & Alerting** is a comprehensive SOC-based monitoring and alerting service driven by our webscale security automation and orchestration platform. It incorporates:

- Threat Event Enrichment, Analysis and Correlation
- Incident Monitoring, Alerting and RCA
- Remote Breach Support
- Security Dashboard
- Compliance Reporting
- AI-based threat hunting (*)
- Post-breach investigation (*)
- Service management reporting
- Security improvement advisories

(*) Requires XDR

The standard service operates to a 4-hour response time and 8-hour resolve time, and currently supports the following vendor solutions:

- Palo Alto Networks (NGFW, TRAPS, CORTEX-XDR, Redlock)
- Fortinet (NGFW)