EXCLUSIVE NETWORKS

SALES SHEET

Managed Security Services Distributor Security Operations Centre

MSSD SOC: MONITORING & ALERTING + PREVENTION & COUNTERMEASURES

Monitoring& Alerting + Prevention & Countermeasures Service for Cybersecurity Solutions

As cyber skills become increasingly rare, and customer demand for managed security services grows by 15% a year, partners no longer have to contemplate committing capital or incurring risk in order to take advantage. With ***MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures***, end customers receive a complete managed service experience that increases their security and compliance posture, and maximises incident response capability.

INTRODUCING MSSD SOC: MONITORING & ALERTING + PREVENTION & COUNTERMEASURES

MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures is a complete reactive and proactive managed security service for next-gen security infrastructure. Use it to benefit end customers with:

- Improved security posture and faster incident response
- Reduced IT security operations costs and skills overheads
- Predictable opex
- Enhanced security and compliance 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

Driven by our global 24/7 SOC, ***MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures*** is a premium offering that builds on the foundation of the MSSD SOC: Monitoring & Alerting service to maximise strategic value both for partners and their end customers.

E GOT THIS!
MSSD
BY EXCLUSIVE NETWORKS

100% CHANNEL READY

MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures 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
- Palo Alto Networks (NGFW, TRAPS, CORTEX-XDR, Redlock)
- Fortinet (NGFW)

TOP 3 CUSTOMER CHALLENGES

Cyber threats are becoming more complex and regulators are introducing tougher compliance for data protection.

- ***MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures*** supports good data governance, enhancing security and compliance posture without committing more internal skills or infrastructure.

Cloud strategies and digital transformation initiatives are getting delayed or compromised because of cybersecurity concerns.

- ***MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures*** prevents cybersecurity from being an inhibitor to strategic IT progression, removing management burden to focus on other priorities.

Organisations are actively seeking complete IT 'as-a-service' packages that reduce capex liability and allow transition to a leaner opex-based consumption models.

- ***MSSD SOC: Monitoring & Alerting + Prevention & Countermeasures*** meets the demand for comprehensive 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 + Prevention & Countermeasures combines a comprehensive SOC-based monitoring and alerting service with managed capabilities for dynamic network environments, including proactive software upgrades and policy management – all driven by our webscale security automation and orchestration platform. It incorporates:

- Monitoring & Alerting
    - Threat Event Enrichment, Analysis and Correlation
    - Incident Monitoring, Alerting and RCA
    - Remote Breach Support
    - Security Dashboard
    - Compliance Reporting
    - AI-based threat hunting (optional)
    - Post-breach investigation (optional)
- Prevention & Countermeasures
    - Availability Monitoring and Backup
    - Operational and Capacity Management
    - Updates and Upgrades
    - Policy Compliance and Best Practice Validation
    - Device and Policy Configuration Change Management
    - Automated Rules of Engagement
    - Policy Topology Reporting
    - Behaviour Baselining (optional)
- Service management reporting
- Security improvement advisories

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)