MS04
RightSecurity

End-to-end security services taking care of Confidentiality, Integrity, and Availability across all service towers

sopra steria

Sopra Steria RightSecurity

- End-to-end security for your business

WHY RIGHTSECURITY FROM SOPRA STERIA?

- Reduced attack surface from day one.

- Quality services, tailored to the Customer and the customer's cyber threat landscape.

- Our approach integrate with the customer's security solutions, providing full transparency - leading to a common view of cyber risks and threats.

- A less complex solution that optimizes the customer's security investments with no lock-in

- Rich portfolio of services reducing cyber risk for your business

Security Operations Center)

- Managed Detection and Response
- Vulnerability Management
- Incident Response
- Secure Infrastructure
- Security Awareness
- Secure Collaboration

ISO 27001 Certified — Information Security Management

ISO 27018 Certified — Information Security Management System

ISO 27017 Certified — Information Security Management System

KVALITETSORDNING — ANBEFALT FOR HENDELSESHÅNDTERING — NSM

The SOC provides the Customer with situational awareness in the overall cyber threat landscape, based on the entire range from the external threat landscape to the accumulated intelligence gathered across SOC customers' environments.
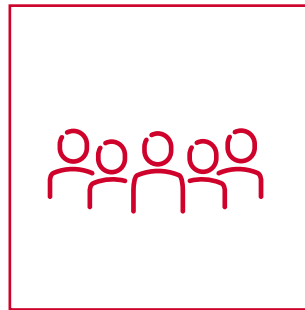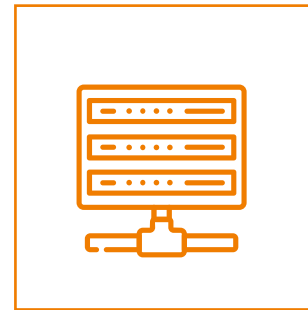
sopra steria

RightSecurity

Managed Security Services

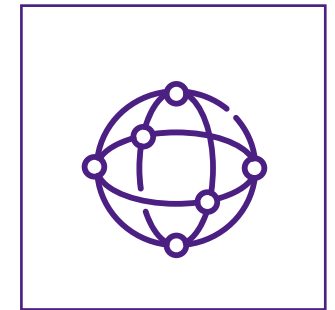| MS0401	MS0402	MS0403	MS0404	MS0405	MS0406
Managed Detection and Response	**Vulnerability Management Services**	**Incident Response Services**	**Secure Infrastructure Services**	**Security Awareness Services**	**Secure Collaboration Services**

sopra steria
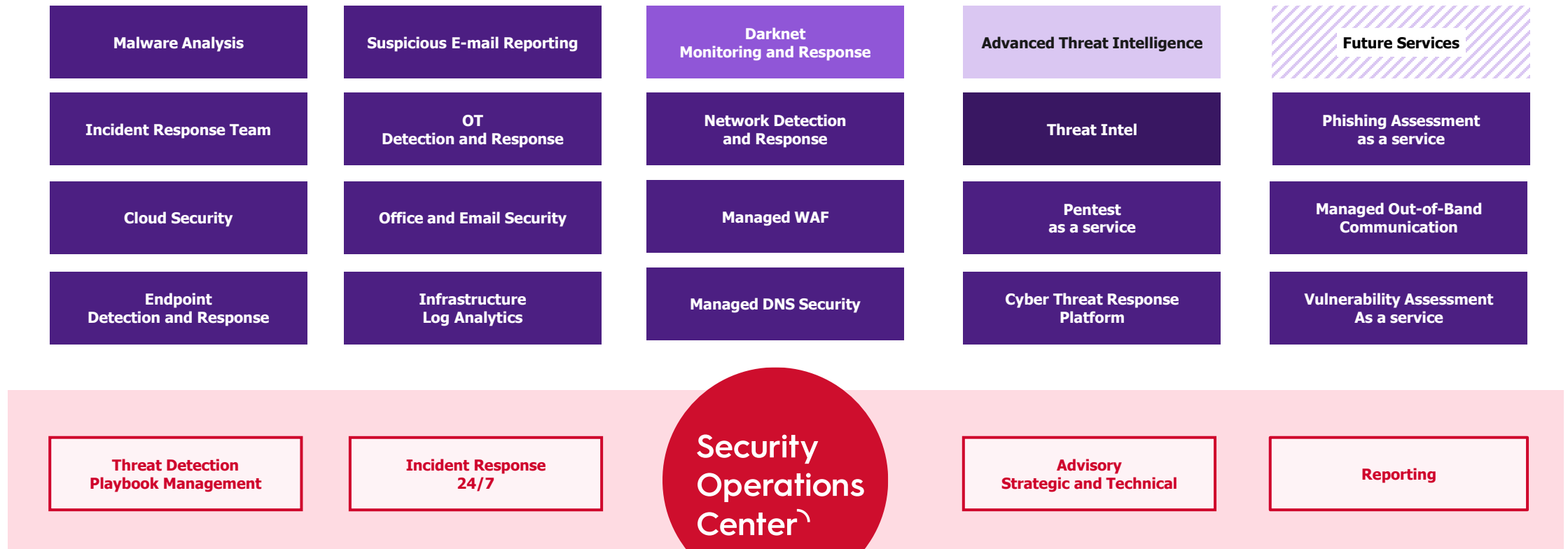
Service overview

SKU	PRODUCT	DESCRIPTION
MS0401 MANAGED DETECTION AND RESPONSE		
MS0401-001	Cyber Threat and Risk detection	Security monitoring and Incident Response
MS0401-002	Infrastructure Log Analytics	Analysis and detection based on collected infrastructure logs
MS0401-003	Endpoint Detection and Response	Monitoring and response to threats targeting clients and servers
MS0401-005	Office and Email Security	Monitoring and response to threats targeting Office 365
MS0401-006	Cloud Security	Monitoring and response to threats targeting identities and cloud services
MS0401-004	Managed DNS Security	Monitoring and blocking of DNS request to malicious domains
MS0401-007	Operational Technology (OT) Detection and Response	Detect and respond to threats targeting operational technology
MS0401-008	Darknet Monitoring and Response	Monitoring and response to threats or company information found for sale on Darknet
MS0401-009	Network Detection and Response	Monitor and response to network-based threats
MS0401-010	Network Detection and Response – National Autonomy	Monitor and response to network-based threats with services supporting national autonomy requirements
MS0401-011	Cyber Threat and Risk Detection – National Autonomy	Security monitoring and Incident Response with services supporting national autonomy requirements
MS0401-012	Infrastructure Log Analytics – National Autonomy	Analysis and detection based on collected infrastructure logs using services supporting national autonomy requirements
MS0402 VULNERABILITY MANAGEMENT SERVICES		
MS0402-001	Vulnerability Assessment as a Service	Vulnerability monitoring, assessment and prioritization
MS0402-002	Pentest as a Service	Continuous security testing of business-critical infrastructure
MS0402-003	Vulnerability Assessment as a Service – National Autonomy	Vulnerability monitoring, assessment and prioritization using services supporting national autonomy requirements
MS0403 INCIDENT RESPONSE SERVICES		
MS0403-001	Incident Response Team (IRT)	Sopra Steria's expert incident response team (IRT) supports managing comprehensive cyber incidents
MS0403-002	Malware Analysis	Analysis of suspected malware in a sandbox

Service overview

SKU	PRODUCT	DESCRIPTION
MS0404 SECURE INFRASTRUCTURE SERVICES		
MS0404-001	Managed Web Application Firewall (WAF)	Protection of internal- and external facing web applications
MS0404-002	Cyber Threat Response Platform	Customer owned, Sopra Steria managed and fully transparent SIEM
MS0405 SECURITY AWARENESS SERVICES		
MS0405-001	Phishing Assessment as a Service	Continuous phishing simulations and security awareness training
MS0405-002	Suspicious Email Reporting	Improve user-experience when facing email-based attacks
MS0406 SECURE COLLABORATION SERVICES		
MS0406-001	Managed Out-of-band Communication	Out-of-band communication based on zero-trust principals that enables autonomous secure collaboration during crisis
MS0408 THREAT INTELLIGENCE SERVICES		
MS0408-001	Customer Threat Monitoring	Specialised support when a security incident has occurred
MS0408-002	Sectoral Threat Assessment	Contextualised threat landscape to support decision making
MS0408-003	Special Event Threat Assessment	Threat assessment of special events that may impact the business
MS0408-004	Threat Actor Profiling	Provides insight into threat actor's TTPs in prioritize efforts and investments to better mitigate risks
MS0408-005	Live Threat Intelligence	Live threat intelligence feed integrated with the customers SIEM platform
MS0409 SECURITY ADVISORY SERVICES		
MS0409-001	Security Manager	Supporting CISO

RightSecurity – Managed Service Portfolio

Malware Analysis	Suspicious E-mail Reporting	Darknet Monitoring and Response	Advanced Threat Intelligence	Future Services
Incident Response Team	OT Detection and Response	Network Detection and Response	Threat Intel	Phishing Assessment as a service
Cloud Security	Office and Email Security	Managed WAF	Pentest as a service	Managed Out-of-Band Communication
Endpoint Detection and Response	Infrastructure Log Analytics	Managed DNS Security	Cyber Threat Response Platform	Vulnerability Assessment As a service

Security Operations Center

Threat Detection Playbook Management	Incident Response 24/7	Advisory Strategic and Technical	Reporting

- Operationalized service
- Under establishment

sopra steria

RightSecurity

MS0401 **Managed Detection and Response**

sopra steria

Standard Product

Cyber Threat and Risk Detection

24/7 Security Operations with local or global security delivery

| Threat Detection Playbook Management | Incident Response 24/7 | Security Operations Center | Advisory Strategic and Technical | Reporting |

24/7 – 365 THREAT DETECTION AND RESPONSE

- Sopra Steria Monitor alerts, prioritizes, classifies and Investigate detected threats.
- Continuous development and maintenance of active threat detection capabilities.
- Support for threat & risk detection in Cloud Infrastructures to minimize data transfer from Cloud Services.

IMPROVED DETECTION AND RAPID RESPONSE TO CYBER THREATS

- Hypothesis-driven Threat Hunting based on known threat actors and techniques on all available data.
- Configurable Security Orchestration, Automation and Response (SOAR).
- Configurable response actions.
- Continuous development of Use Cases based on threat landscape.

WHY CYBER THREAT AND RISK DETECTION FROM SOPRA STERIA?

- We take care of your users and your infrastructure
- Experts with a lot of experience in security analysis and incident management
- Based on technology from market-leading manufacturers

THE FOUNDATION FOR PROACTIVE COOPERATION

We establish a foundation for proactive cooperation, including strategy and operational consulting adapted to the Customer's risk and threat picture. Business-critical systems are protected with standardised and tailor-made mechanisms that reduce risk over time. Mandate and processes for event management

A SERVICE THAT PROVDIES

- Security Monitoring and detection of threats to your business
- Threat Hunting based on changes in the threat landscape
- Development and implementation of Security Automation
- Reporting of Security Incidents and trends

"The SOC becomes an additional security layer in our cyber domain. Simultaneously, we will use the information captured here in our ongoing evaluation of out threat picture."

– Government organisation with critical infrastructure

PRICING MODEL
Fixed price

sopra steria

8