Data sheet

Managed Security Services Security Operation Center as-a-Service

The threat landscape is ever evolving, causing increasing costs and security complexity. **Our SOCaaS leverages your SIEM platform investments to win this battle.**

Security skills

Staffing security operations is a large challenge. Operation of a SIEM platform 24/7 requires deep skills in several areas. Platform management, threat investigation and compliance reporting are areas where many organizations find themselves short of skills.

Existing resources tend to analyze large amounts of alerts but the uncertainty of finding the real attacks remains.

Market leading SIEM platforms have great capabilities for analyzing all events and provide compliance reporting. However very few organizations have the capacity to leverage their investments in security tools and integrate them with the SIEM platform.

Our SOCaaS (Security Operation Center as-a-Service) offers a fully managed service that provides deployment, platform management, detection of cyber threats, compliance reporting, custom use cases, dashboards and incident escalation playbooks.

Demands beyond traditional managed security services provider (MSSP)

Users require instant access to huge quantities and varieties of information, while apps and the data they generate are moving into multiple, mutually supportive cloud environments. These are the new hallmarks for modern business development, allowing you to grow, adapt and stay competitive.

Unfortunately, they are also the latest attack vectors for advanced cyber threats, exposing your business to severe risks which few organizations have the resources to fully combat. As falling short of cybersecurity requirements moves higher up the list of obstacles a successful digital transformation needs to overcome, a clear threat detection strategy – and the ability to implement it – is essential.

The data sources required for regulatory and business compliance reporting are also a moving target. As business applications transform, the sources also shift and the use cases for detecting compliance incidents need to be up to date to enable this. Once compliance reporting is properly implemented it still needs to be constantly adjusted to keep up to date with changes in business processes, new applications and changes in infrastructure.

SOCaaS combines commercial SIEM native capabilities with our advanced analytics and threat intelligence for the detection of cyberattacks. A managed service including SIEM platform management, detection/validation of cyberattacks, custom use cases, dashboards and compliance reporting. Our experienced security analysts provide 24/7 coverage as an integrated part of the SOCaaS, something that you may not be able to deliver with an in-house solution.

Key benefits of our SOCaaS

- Reduce business risks, administrative burden and costs
- Cyber threat detection that evaded SIEM rules
- Comply with regulatory or industry compliance
- Maximize functional use of your SIEM platform
- Scalable and flexible SIEM operations by certified experts

Fresh start or migrate

If you already have a SIEM platform in operation, we can migrate your existing deployment. Otherwise, we will build a new environment, utilizing our best practice installation and configuration guides for SIEM technologies.

SOCaaS Provides

- SOC staffed with certified security experts 24/7
- SIEM platform management including health and availability, software patching and backup
- SIEM platform configuration including fine-tuning of rules
- Creation of custom use cases, dashboard and reports
- 24/7, monitoring of events and alerting of security incidents
- Our Cyber Threat Sensor provides network traffic analysis based on machine learning and threat intelligence
- Compliance monitoring, reporting and notification based on customized playbooks
- Custom playbooks and incident lifecycle support

SOCaaS – how it works

SOCaaS offers a tailored service approach for SIEM and analytics. The service supports leading security products, has proven delivery process and provides access to certified staff. It increases the visibility into your environment, accelerating alert to incident escalation while providing proactive risk modelling and support for mitigation. SOCaaS maximizes value of your investments in security technologies and for achieving your desired security posture. It lets you focus on core business objectives without the overhead of maintaining, monitoring and operating your SIEM deployment with in-house resources.

The configuration of the SIEM customized to every client's specific business requirements. We begin with an assessment identifying key elements such as topology, log sources, data center locations and key logical networking requirements to develop a delivery plan for setting up the service.

Detection, analysis and detailed security incident reporting of cyberattacks is delivered by combining our advanced analytics, machine learning and proprietary threat intelligence with market leading SIEM platform capabilities. Notable events are analyzed by security analysts with well-defined escalation processes to ensure that you receive accurate incident reports in a timely manner allowing for an actionable response.

Regulatory and industry specific compliance reporting leverages the SIEM capabilities. We help configure rules sets for monitoring and detection of compliance and security best practices violations. Adherence to your business policy compliance can be achieved with custom use cases. Event notifications can be selectively configured to be sent when a rule is triggered.

With SOCaaS we establish a consolidation point to augment your existing security organization, so we collaboratively provide real-time visibility of your environment for all forms of security monitoring.

IDC ANALYZE THE FUTURE

Leader in the IDC MarketScape: Worldwide Managed Security Services (MSS) 2020 Vendor Assessment

Leader in the IDC MarketScape: Worldwide Managed Security Services (MSS) 2020 Vendor Assessment

IDC ANALYZE THE FUTURE

Leader in the IDC MarketScape: Asia Pacific Managed Security Services (MSS) 2020 Vendor Assessment

Leader in the IDC MarketScape: Asia Pacific Managed Security Services (MSS) 2020 Vendor Assessment

FROST & SULLIVAN

2020 Asia Pacific Managed Security Services Provider of the Year

2020 Asia Pacific Managed Security Services Provider of the Year

CREST

Certified for Cyber Security Incident Response and Penetration Testing, Audited for SOC Certification

Certified for Cyber Security Incident Response and Penetration Testing, Audited for SOC Certification

Why us?

Detection of advanced threats with close to zero false positives

We deliver validated security incidents reports with actionable recommendations.

Increased visibility of security posture

Monitoring of public, private and hybrid cloud.

Next-generation automation capabilities

Access to comprehensive analytics, service delivery and process development.

Secure cloud adaptation, mobility and SD-WAN

With SASE we can support your digital transformation helping your employees to securely become more mobile.

Get in touch

If you'd like to find out more about our services, speak to your client manager or visit our website