CANCOM
SOC Light as a Service

Die Anforderungen an Security und Compliance werden immer komplexer und bringen IT-Abteilungen zunehmend an ihre Grenzen: 24/7-Überwachung der neuesten Bedrohungslagen weltweit, sofortige Reaktionsfähigkeit in Notfallsituationen sowie die EU-Datenschutz- und IT-Sicherheitsregeln verursachen stetig steigende IT-Herausforderungen.

Mit dem Security Operations Center bietet CANCOM vielfältige Leistungen, die die Sicherheit in Ihrem Unternehmen auf das nächste Level heben. Das CANCOM SOC zeichnet sich durch die zentrale Echtzeitüberwachung Ihrer IT-Ressourcen, die Analyse des Bedrohungsgrads und die Steuerung der Reaktion auf Angriffe Ihrer IT-Umgebung aus.

Das SOC Light ist eine preiswerte SOC-Variante der CANCOM. Der Service ist auf maximal 500 EPS (Events per Second) beschränkt und berücksichtigt die neun wichtigsten Use Cases zur Erkennung von Security-Incidents. SOC-Light-Kunden profitieren durch fest festgelegte Use Cases und die Beschränkung auf definierte Systemtypen von einem schnellen Onboarding und einem hochgradig standardisierten Betrieb.

IT-Sicherheit auf höchstem Niveau – mit SOC Light

Ihre Situation?

Sie sind Opfer von Cyberkriminalität geworden oder haben Sorge dies zu werden? Sie sind sich unsicher in Bezug auf vorhandene Schwachstellen bzw. können nicht klar benennen, welches Sicherheitslevel Sie haben? Vorhandene Sicherheitsvorkehrungen (Prävention) sind durchlässig und bieten keinen 100%-igen Schutz? Sie haben keine ausreichenden Maßnahmen im Bereich Detektion und Reaktion (laut BSI vergehen über 200 Tage bis zur Aufdeckung eines Angriffs)?

Gesetzliche Regularien schreiben zunehmend indirekt eine Detektion vor. Schäden durch Cyberangriffe werden immer höher, während die Anzahl an Angriffsmöglichkeiten stetig wächst. Das CANCOM SOC Light ermöglicht Ihnen, auf diese Probleme schnell und nachhaltig reagieren zu können und unterstützt Sie bei der Erkennung von Angriffen auf Ihr Unternehmen.

Unsere Vorteile für Sie:

- Vollautomatisierte Analyse und Angriffserkennung durch IBM QRadar
- 24/7-Angriffsüberwachung und -abwehr in Echtzeit durch qualifizierte Security Analysten
- Analyse der Informationen unter Berücksichtigung der aktuellen Bedrohungslage
- Schnelles Onboarding und voll standardisierte Use Cases und Prozesse
- SOC Team und SOC Rechenzentren an deutschen Standorten
- Schnelle Steigerung sowie Erweiterung des Security Levels durch ergänzende Use Cases (hoher Skalierungsgrad)*

In maximal 4 Wochen zum Go Live!

Durch ein hochgradig standardisiertes Onboarding gehen unsere SOC-Light-Kunden schon innerhalb von vier Wochen Live. Während einer kurzen Übergangsphase werden die Use Cases optimal auf Sie und Ihre Umgebung angepasst, um Ihnen einen optimal abgestimmten Service bieten zu können. Selbstverständlich ist unsere Lösung höchst skalierbar aufgebaut.

Unser CANCOM-Angebot für Sie

Die folgenden Leistungen bieten wir Ihnen im Rahmen des SOC Light as a Service.

ONBOARDING & LIGHT GO LIVE	**Onboarding** • Einrichtung VPN in Zusammenarbeit mit Ihnen • Aufsetzen des Cybercollectors innerhalb des vorher festgelegten IP-Adressbereichs • Anbindung der Logquellen an das SIEM • Aktivierung der Light Use Cases • Import der bereitgestellten Netzwerkhierarchie • Import der bereitgestellten Service Accounts • Testdurchlauf der Use Cases in Absprache mit Ihnen **Light Go Live** • Fine-Tuning der Use Cases bzw. SIEM-Regeln	**UNSERE PREISE:** **1 Monatsrate** **€ 1.900,-** oder **€ 2.800,-**
USE CASES	**Folgende Use Cases sind im SOC-Light-Paket enthalten*:** • Erkennung von schadhaften URLs • Erkennung von erlaubten Firewall-Verbindungen nach einem Portscan • Erkennung von Account Manipulationen • Ausführung von Powershell Scripting • Erkennen von „Scheduled Task“ • Deaktivierung von Security Tools • Erkennung von Antivirus-Alarmen • Erkennung von IDS-Alarmen	
SOC LIGHT	**Leistungen der CANCOM während des Regelbetriebes:** • Plattformbetrieb und Lizenzmanagement • 24x7 Security Monitoring und Analyse durch Security Analysten • Automatisierte Korrelation und Analyse von Daten auf Basis des SIEMs QRadar • Nutzung von Threat Intelligence Feeds • Automatische Einstufung der Gefährdung durch ein abgestimmtes Regelwerk • Alarmierung des Kunden im Gefahrenfall und Handlungsempfehlung • Archivierung der Ereignisse (Events) und der Sicherheitsvorfälle (Incidents) • Laufende Anpassung und Optimierung • Monatliches Reporting	**UNSERE PREISE:** **SOC Light mini** (max. 250 EPS): **€ 1.900,-** **SOC Light maxi** (max. 500 EPS): **€ 2.800,-**

*Weitere Use Cases können auf Wunsch ebenfalls aktiviert sowie für ein erweitertes Schutzlevel entwickelt werden (zusätzlicher Aufwand).

Competence Center Security
Fachvertrieb.Security@cancom.de