CANCOM

SECURITY AS A SERVICE

UMFASSENDE IT-SICHERHEIT DANK DEN CYBER DEFENSE SERVICES VON CANCOM

KONTAKT CANCOM

Team Cyber Defense Services
+49 89 54054-0
cyberdefense@cancom.de

CANCOM Cyber Defense Services

Die Anforderungen an Security und Compliance werden immer komplexer und bringen IT-Abteilungen an ihre Grenzen: 24/7-Überwachung der neuesten Bedrohungslagen weltweit, sofortige Reaktionsfähigkeit in Notfallsituationen sowie die neuen EU-Datenschutz- und IT-Sicherheitsregeln verursachen stetig steigende IT-Herausforderungen. Mit den neuen Cyber Defense Services bietet CANCOM vielfältige Leistungen, die die Cyber-Sicherheit in Ihrem Unternehmen auf das nächste Level heben.

IT-Sicherheit auf höchstem Niveau

Angeboten werden die Leistungen aus dem CANCOM Security Operations Center (SOC). Vor allem kleine und mittlere Unternehmen sind bereits mit den Grundvoraussetzungen einer zeitgemäßen IT-Sicherheit überfordert. Mit SOC as a Service ist CANCOM in der Lage, gerade diese Unternehmen zu unterstützen. Optional wird das SOC durch die führende Security-SIEM-Lösung QRadar von IBM und der IBM Security Intelligence erweitert. Um ein noch höheres Maß an Sicherheit sicherzustellen, ist eine Integration von IBM Watson Predictive Analytics und Künstlicher Intelligenz bereits geplant.

Leistungen der CANCOM Cyber Defense Services im Überblick

SOC AS A SERVICE

Die Security-SIEM-Lösung QRadar nimmt zunächst Daten aus unterschiedlichen, definierten Quellen auf. Anschließend werden diese Daten normalisiert, analysiert und korreliert. Zu den Quellen zählen klassische Security Komponenten, Applikationen und heutzutage vor allem Cloud Dienste. Das Ergebnis sind intelligente Alarmierungen an die CANCOM Security Analysten.
Durch Threat Intelligence und Informationen über Bedrohungen, wie etwa Schadprogramme oder Tätergruppen, können unsere Analysten zudem kundenspezifische Ereignisse mit globalen Bedrohungen verknüpfen.

Das SOC as a Service-Modul setzt sich aus drei Kernelementen zusammen:.

- Automatisierte Analyse und Angriffserkennung
- CANCOM Cyber Defense Analysten und Architekten
- Cyber Defense- und Incident Response-Prozesse

SOC AS A SERVICE MIT INCIDENT RESPONSE

Als Erweiterung zu SOC as a Service bietet CANCOM den Incident Response.
Damit können Angriffe auf Basis der gemeinsam definierten Prozeduren (Runbooks) zu jeder Zeit abgewehrt werden – unabhängig von den Betriebszeiten sowie von der Frage, ob die Mitarbeiter des Kunden gerade verfügbar sind. Durch die im Runbook festgelegten Handlungen lassen sich Angriffe abwehren oder Schäden minimieren.

Erweiterte Service-Leistungen:

- Aktivierung des CANCOM Incident Security Response (ISR) im Gefahrenfall
- Durchführung der abgestimmten Prozeduren zur Gefahrenabwehr (Runbook)
- Erweitertes Security Response Reporting

SCHWACHSTELLEN-MANAGEMENT

Das optionale Schwachstellen-Management prüft die Zielsysteme auf bekannte und mögliche Schwachstellen. Mithilfe dieser Informationen lassen sich Bedrohungen gezielt bewerten. Das ermöglicht, den aktuellen Sicherheitsstand der IT-Umgebung zu erkennen und zu dokumentieren. Die gewonnen Informationen können in das SIEM System automatisch integriert werden, um Bedrohungen dadurch noch schneller zu identifizieren.

Folgende Leistungen sind enthalten:

- Erkennen von IT-Schwachstellen mit anschließender Dokumentation
- Schwachstellen-Scan der Zielsysteme
- Empfehlung und Informationen über notwendige Maßnahmen
- Alarmierung bei Erkennung neuer Systeme mit entsprechenden Schwachstellen
- Optional: Einbindung in das SIEM-System

Security-Maßnahmen und Security-Kompetenz sinnvoll miteinander verknüpft

Das CANCOM SOC zeichnet sich durch die zentrale Echtzeitüberwachung Ihrer IT-Ressourcen, die Analyse des Bedrohungsgrads und die Steuerung der Reaktion auf Cyber-Angriffe Ihrer IT-Umgebung aus. Zudem werden aus dem SOC potenzielle Schwachstellen ständig gescannt, wodurch mögliche Angriffsziele identifiziert und Sicherheitslücken noch vor einem Angriff geschlossen werden können. Das Ergebnis: Eine sinnvolle Verzahnung von Abwehr und Vorbeugung Ihrer Cyber-Security.

ZENTRALE VORTEILE VON SOC AS A SERVICE MIT CANCOM

- 24/7-Angriffsüberwachung und -abwehr in Echtzeit
- Analyse der Informationen unter Berücksichtigung der aktuellen Bedrohungslage
- Bereitstellung von neuen Bedrohungsalarmen, Leistungs- und Sicherheitsberichten
- Koordination und Management der Reaktionen auf Cyberbedrohungen und -vorfälle
- SOC Team an deutschen Standorten / SOC Rechenzentren in Hamburg

IBM Platinum Business Partner™