MANAGED SERVICES
protectONE vSOC SERVICES

Teilnehmer der Allianz für Cyber-Sicherheit

protectONE™ ....protect your Business

protectONE - 24/7 SOC Service | made in Germany

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 vSOC Services bietet **protectONE** vielfältige Leistungen, die die Cyber-Sicherheit in Ihrem Unternehmen auf das nächste Level heben.

Sie suchen nach einem dauerhaften 24/7 Threat Detection and Response Service?

IT-Sicherheit auf höchstem Niveau

Angeboten werden die Leistungen aus dem **protectONE** Security Operations Center (vSOC). Vor allem kleine und mittlere Unternehmen sind auf Unterstützung angewiesen, um eine zeitgemäße IT-Sicherheit gewährleisten zu können. Mit vSOC as a Service ist **protectONE** in der Lage, gerade bei diesen Unternehmen proaktiv Bedrohungen zu stoppen.

Optional wird das vSOC durch führende intelligente Sicherheitsanalysen und Threat Intelligence Lösung **Sentinel** von Microsoft erweitert. Das vSOC ist kompatibel mit bereits vorhandenen Cybersecurity-Tools. Ggf. vorhandene Telemetriedaten können automatisch konsolidiert, korreliert und priorisiert werden.

Vorteile von protectONE vSOC as a Service

- 24/7-Angriffsüberwachung und –Abwehr in Echtzeit
- Analyse der Informationen unter Berücksichtigung der aktuellen Bedrohungslage
- Bereitstellung von neuen Bedrohungsalarmen, Leistungs- & Sicherheitsberichten
- Koordination und Management der Reaktionen auf Cyberbedrohungen und - vorfälle
- Deutschsprachiges SOC Team an deutschen Standorten
- Flexibilisierung Ihrer IT-Kosten: OpEx statt CapEx

protectONE vSOC ist ein Fully-Managed-Service. Unsere Experten erkennen für Sie Cyberangriffe auf Computer, Server, Netzwerke, Cloud Workloads und E-Mail und ergreifen Reaktionsmaßnahmen.

vSOC AS A SERVICE

Die **vSOC** Lösung basierend auf **Sentinel** von Microsoft 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 vor allem Cloud Dienste. Das Ergebnis sind intelligente Alarmierungen an die **protectONE** Security Analysten. Durch Threat Intelligence und Informationen über Bedrohungen, wie etwa Schadprogramme oder Tätergruppen, können unsere Analysten zudem individuelle Ereignisse mit globalen Bedrohungen verknüpfen.

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

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

SOC AS A SERVICE MIT INCIDENT RESPONSE

Als Erweiterung zu vSOC as a Service bietet **protectONE** 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 Ihre Mitarbeiter gerade verfügbar sind. Durch die im Runbook festgelegten Handlungen lassen sich Angriffe abwehren oder Schäden vermeiden bzw. minimieren.

Erweiterte Service-Leistungen:

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

SCHWACHSTELLENMANAGEMENT

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 noch schneller zu identifizieren.

Folgende Leistungen sind enthalten:

* Erkennen von IT-Schwachstellen mit anschließender Dokumentation
* Schwachstellen-Scan der Zielsysteme
* Informationsbasierte, konkrete Empfehlungen bzgl. notwendiger Maßnahmen
* Alarmierung bei Erkennung neuer Systeme mit entsprechenden Schwachstellen
* Optional: Einbindung in das SIEM-System

Security-Maßnahmen und Security-Kompetenz sinnvoll miteinander verknüpft

Das **protectONE** 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.