softline

Softline Security Operations Center

Mit unserem SOC schützen Sie sich gegen interne und externe Gefahren, reduzieren das Risiko in allen sicherheitsrelevanten Bereichen und stellen Compliance mit gesetzlichen Anforderungen sicher.

Die Vorteile eines Security Operations Centers liegen klar auf der Hand: Ein kontinuierliches und ganzheitliches Monitoring Ihrer IT-Sicherheits-Architektur sorgt dafür, Risiken frühzeitig erkennen und abwehren zu können, bevor sie geschäftsschädigend werden. Doch lohnt sich der Aufbau im eigenen Haus? Eine Frage, die wir Ihnen gern beantworten!

Mit unserem SOC as a Service stellen wir Ihnen ein Team von IT-Sicherheitsexperten der Softline und DigiFors GmbH, das Ihre gesamte IT-Infrastruktur rund um die Uhr überwacht, um Cybersecurity-Ereignisse in Echtzeit zu erkennen und so schnell und effektiv wie möglich zu beheben – ohne dass Sie dafür interne Ressourcen selbst aufbauen oder freistellen müssen.

Managed Detection	■ SIEM as a Service ■ Endpoint Detection & Response as a Service ■ Vulnerability Management as a Service ■ Threat Hunting
Managed Intelligence	■ Threat Intelligence ■ Open Source Intelligence (OSINT)
Managed Response	■ Incident Response ■ IT-Forensik
Managed Risk	■ Penetrationstests ■ Auditing

- 24/7 Verfügbarkeit
- Separate Räumlichkeiten mit Zutrittskontrolle
- Ausreichende Anzahl von Büro- und Leitstellen-arbeitsplätzen
- BSI-akkreditierter APT-Response-Dienstleister
- Zertifizierungen nach ISO 27001/ISO 9001
- Dedizierter Internetzugang
- Ausgebildete IT-Forensiker, Informationssicherheits-spezialisten & IT-Sicherheits-experten

Profitieren Sie mit unserem Security Operations Center von umfassender Sicherheitsüberwachung, Gefahrenprävention, Kostenreduzierung und regelmäßigem Reporting.

Managed Detection – SIEM as a Service

Mit dem Security Information and Event Management as a Service bieten wir ein umfassendes, transparentes IT-Security Monitoring für Ihre gesamte IT-Infrastruktur.

Das SIEM erfasst Log- und Ereignisdaten, die von den Anwendungen, Sicherheitsgeräten und Host-Systemen erstellt werden, und speichert diese auf einer zentralen Plattform. Die Software sammelt Daten von Antivirenlösungen, Firewall-Logdateien und anderen Stellen und ordnet sie in Kategorien ein, zum Beispiel Malware-Aktivitäten und fehlgeschlagene oder erfolgreiche Anmeldungen. Wenn sie dabei eine Bedrohung erkennt, löst sie einen Alarm aus und gibt gemäß vordefinierten Regeln eine Bedrohungsstufe an.

Managed Intelligence

Bei Threat Intelligence handelt es sich um evidenzbasierte Informationen über Cyberangriffe. Diese Erkenntnisse helfen Unternehmen dabei, über neue Bedrohungen informiert zu bleiben, damit sie sich schützen können.

Als Open Source Intelligence (kurz OSINT) wird die Recherche mithilfe öffentlich zugänglicher Informationen beschrieben. Dabei werden unterschiedliche Quellen, wie zum Beispiel Google, LinkedIn und Twitter genutzt, um Daten zu einem im Vorfeld deklarierten Ziel zu sammeln. Die daraus gewonnenen Erkenntnisse fließen in Abwehrmaßnahmen und Verteidigungsstrategien ein.

Managed Response

»Eine erfolgreiche und richtige Reaktion auf einen IT-Sicherheitsvorfall kann nur erfolgen, wenn der Zustand des zu untersuchenden Systems weitestgehend dem Zustand zum Verdachtszeitpunkt entspricht.«

Managed Response beinhaltet einerseits präventive Maßnahmen zur Verbesserung der Fähigkeiten in der Firmen-Umgebung, belastbare bzw. forensisch sichere digitale Spuren zu sammeln, anderseits IT-forensische Untersuchungen nach anerkannten Regeln der Technik bei Verdachts- oder Vorfällen durchzuführen.

Managed Risk – Audit

Das Cybersecurity Assessment bewertet den Reifegrad der Cyber Security eines Unternehmens auf Basis der Critical Security Controls des Center of Internet Security (CIS). Sie stellen die renommierteste Norm zur effektiven Cyberabwehr dar und bieten spezifische, umsetzbare Möglichkeiten, um die aktuell am verbreitetsten und gefährlichsten Cyberangriffe zu stoppen.

Die CIS Critical Security Controls versuchen nicht, umfassende Normen wie ISO 27001/27002, BSI IT-Grundschutz oder das NIST Cybersecurity Framework zu ersetzen.

Ein wesentlicher Vorteil besteht darin, dass sie aus den häufigsten Angriffsmustern abgeleitet wurden und die rasche Identifizierung der notwendigen Next Steps ermöglichen.

Transformieren Sie Ihre Cybersicherheitsstrategie grundlegend. Melden Sie sich unter info@softline.de oder +49 341 24051-0.