

Optimiertes Schutzniveau durch 3 Verteidigungslinien

Erste Verteidigungslinie



- Netzwerksicherheit
- Firewall, Virenschutz, Proxy, Mail Security, Schwachstellenscanner

Zweite Verteidigungslinie



- SIEM: Auswertung von gesammelten Sicherheitsvorfällen aus 1LOD
- Frühzeitige Erkennung von Angriffsmustern und auffälligem Verhalten im Netzwerk
- 24/7-Überwachung im SOC
- Vorfallsbeseitigung



Achtung, Sicherheitsproblematik!

Sicherheitsvorfälle werden selten gesammelt oder ausgewertet. Dadurch bleibt der Schutz lückenhaft. Eindringlinge bleiben meist unmerklich, da auffälliges Verhalten im Netzwerk nicht ausreichend kontrolliert wird!

Dritte Verteidigungslinie



- IT-Sicherheitsmaßnahmen durch Prozesse (z. B. ISMS/ISO 27001)
- Unternehmensrichtlinien (Sicherheitspolicies)
- Mitarbeiter-Awareness (Schulungen)

Zertifizierte Informationssicherheit nach DIN ISO 27001:2017

- Spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems
- Berücksichtigt Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken
- Bestätigt die Implementierung von geeigneten Sicherheitsmechanismen

Warum GIP?

- Zertifizierte Cyber Analysten/-Analystinnen mit höchster Expertise
- Einsatz marktführender Technologien
- Reduzierter personeller und finanzieller Aufwand für das Cyber Security Monitoring
- Keine langfristigen Risiken durch Investitionen in teure Hard- und Software
- Keine Weiterbildung Ihrer eigenen IT-Sicherheitspezialisten
- Ablösung von Insellösungen und Einzelsystemen



G.I.P. S.à r.l.
Eine Beteiligung der KÖTTER Unternehmensgruppe
22, rue Gabriel Lippmann ■ L-5365 Munsbach
E-Mail: sales@g-i-p.tech ■ Tel.: +352 2060 8844 22
Web: www.g-i-p.tech

Cyber Defense as a Service
IT-Security Services
IT-Compliance



Unser Leistungspaket gegen digitale Bedrohungen

Cyber Defense as a Service (CDaaS)



- Vulnerability & Hardening Detection
- Intrusion Detection
- Threat Intelligence
- 24/7-SOC-Monitoring
- Active Incident Response
- Managed SIEM & Log Management
- Investigation / Fraud-detection
- MITRE ATT&CK

Cloud Security Consulting & Operations



- Security Consulting
- Cloud Operations
- IaaS Operations
- Application Operations

Professional Services Consulting & Operations



- Maßgeschneiderte Überwachungsleistungen (herstellerunabhängig)
- IT-Compliance
- IT-Security Consulting
- IT-Crisismanagement

IT-Security Consulting



- Identifikation und Bewertung von Sicherheitsrisiken
- Entwicklung von Risikominderungsstrategien
- Gestaltung sicherer IT-Infrastrukturen
- Implementierung von Sicherheitsrichtlinien und -protokollen
- Analyse aktueller Bedrohungen und Schwachstellen
- Entwicklung von Abwehrstrategien und Notfallplänen
- Durchführung von Schulungen für Mitarbeiter
- Förderung einer Sicherheitskultur im Unternehmen

IT-Compliance



- Überblick über relevante Gesetze, Vorschriften und Standards (z. B. DSGVO, HIPAA, NIST, PCI/DSS, TSC, ISO 27001)
- Entwicklung und Implementierung von Compliance-Richtlinien
- Aufbau eines Compliance-Management-Systems
- Vorbereitung und Durchführung von Compliance-Audits
- Kontinuierliche Überwachung der Einhaltung von Vorschriften und Richtlinien
- Identifikation und Bewertung von Compliance-Risiken
- Implementierung von Maßnahmen zur Risikominderung und -kontrolle
- Schulung der Mitarbeiter zu Compliance-Themen und Best Practices

Security Operations Center



Detektion

- Erkennen von Angriffsversuchen
- 24/7-Überwachung
- Alarmierung bei Sicherheitsvorfällen
- Ständige Schwachstellen-Überwachung

Schutz

- Aktive Abwehr von Angriffen
- Automated Response
- Unterstützung bei der Beseitigung von Sicherheitsvorfällen (auch vor Ort)

Prävention

- Threat Intelligence
- Dark-Web-Überwachung
- Bedrohungsanalyse
- Security-Awareness-Maßnahmen