SHD.
WIR BEWEGEN IT.

SHD SOC SERVICES

Digitale Welt absichern und Cyberangriffe abwehren

SHD SOC Services

Digitale Welt absichern und Cyberangriffe erfolgreich abwehren

Microsoft Defender

Sicherheitsvorfälle nehmen zu und verursachen Störungen in den Abläufen in Behörden und Unternehmen. Wie können Sie sich schützen?

Mit einem Frühwarnsystem können Sie verhindern, dass Geschäftsprozesse stillstehen. Die Cyberexperten in unserem Security Operations Center (SOC) schützen mit ihren Superkräften Ihre IT-Infrastruktur und Ihre Daten.

Rund um die Uhr überwacht das SOC-Hauptquartier Ihre IT und ergreift sofortige Gegenmaßnahmen, um Ihr Unternehmen zu schützen.

Ablauf eines Angriffs: Die CYBER KILL CHAIN im Detail

Dieses Konzept gliedert Cyberangriffe in insgesamt sieben Ebenen, die ein Täter für die Umsetzung seines Vorhabens sukzessiv erreichen muss. Umgekehrt ist es auf der Verteidigungsebene möglich, den gesamten Angriff des Cyberkriminellen durch Unterbrechung auf einer Stufe zu blockieren.

APT – advanced persistent threat

komplexer, zielgerichteter und effektiver Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten

mittlere Verweildauer der Angreifer

~66 TAGE

BSI 2022: > 200 Tage!

Was ist ein SOC?

Das Security Operations Center (SOC) ist der Hauptsitz der Helden der Cybersicherheit. Sie haben die Verantwortung für den Schutz der IT-Infrastruktur eines Unternehmens. Das SOC-Team ist eine Sicherheitsleitstelle und darauf spezialisiert, Bedrohungen zu verhindern, zu erkennen und darauf zu reagieren. Mithilfe von Dashboards überwacht das Team rund um die Uhr Endpoints, Identitäten, Server, M365 Services, Datenbanken, Netzwerkanwendungen und andere Systeme, um potenzielle Cyberangriffe in Echtzeit zu entdecken.

Doch das ist nicht alles. Die SOC-Experten bleiben stets auf dem neuesten Stand und nutzen die aktuellsten Informationen, um über Bedrohungsszenarien informiert zu sein. Sie identifizieren und beheben Schwachstellen in Systemen und Prozessen, noch bevor sie von Angreifern ausgenutzt werden können.

DIESE LEISTUNGEN KÖNNEN SIE VON UNS ERWARTEN:

24 × 7 Services

Überwachung aller IT-Systeme auf proaktiver Basis und auslösen von Alarmen bei potenziellen Bedrohungen und Angriffen.

Schwachstellen & Sicherheitslücken

Aufspüren und beseitigen von Schwachstellen und Sicherheitslücken.

Abwehrmaßnahmen

Durchführung von Abwehrmaßnahmen zur Schadensbegrenzung bei Cyberattacken.

Reportings & Analysen

Laufende Erstellung von Analysen zur jeweiligen Bedrohungslage und die Erstellung von regelmäßigen ganzheitlichen IT-Sicherheitsreportings.

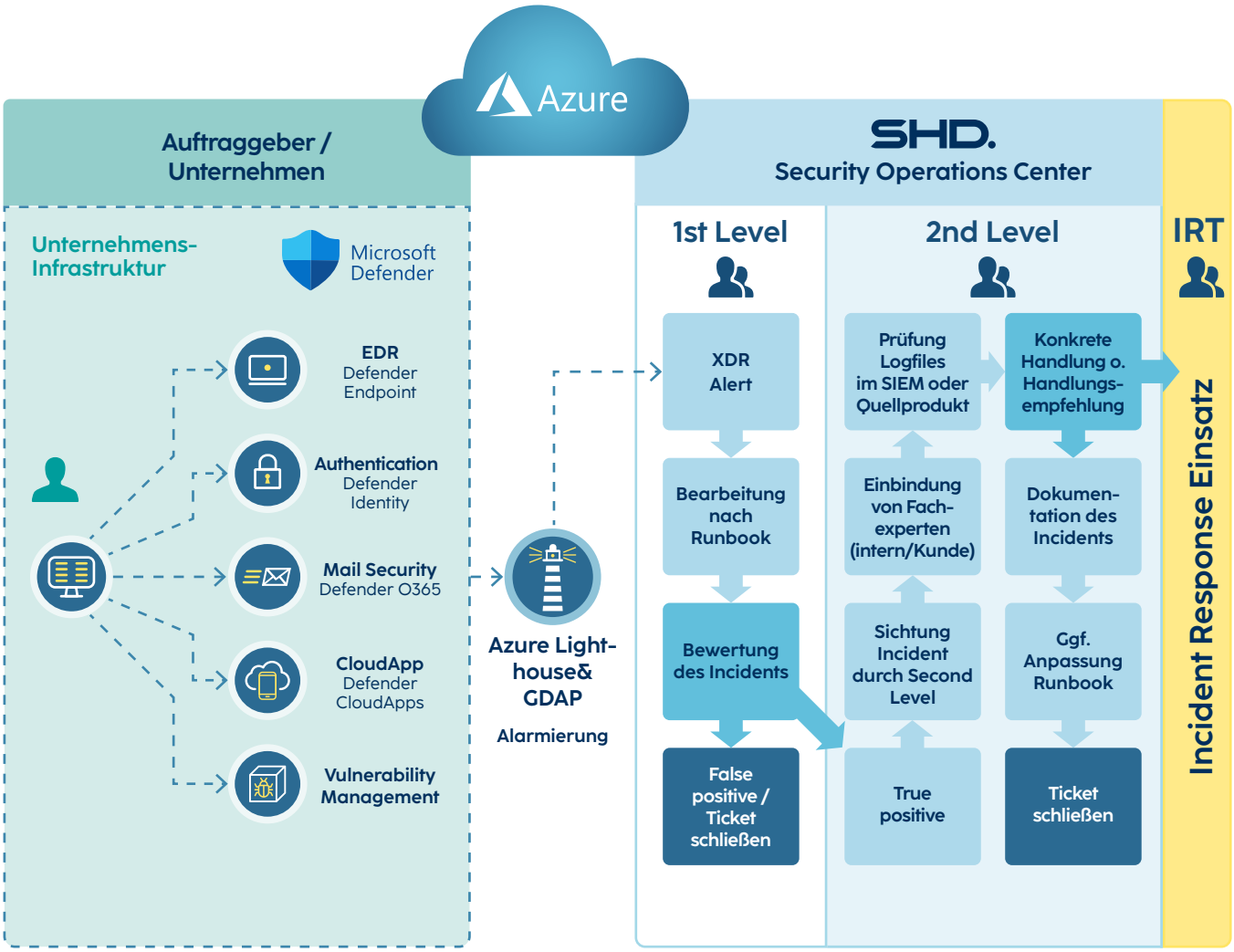
Security Assessments

Durchführung von Security Assessments, um den Reifegrad Ihrer Informationssicherheit stetig zu verbessern.

Workshops

Awareness-Steigerung
Aufzeigen der Potenziale
Erhöhung der Adoption

Die Organisation des Security Operations Center



DANIEL AMLUNG
Senior System Engineer / Cybersecurity Architect

*Mit unseren **SHD-SOC-Services** unterstützen wir die gesamte Unternehmens-IT-Infrastruktur in der Abwehr aktueller Cyberbedrohungen. Wir setzen modernste Technologien und das langjährige Know-how unserer Cybersecurity Spezialist:innen ein, um Sie vor den Gefahren der digitalen Welt zu schützen.*

Von der Erkennung bis zur Abwehr – wir sind für Sie da, um Bedrohungen frühzeitig zu erkennen und effektiv zu bekämpfen. Mit unserem Service haben Sie die Gewissheit, dass Ihre Sicherheit immer an erster Stelle steht!

Nutzen für Unternehmen

PREVENTION

- Planung von Vorsorgemaßnahmen
- Vordefinierte Handlungsanweisungen auf Sicherheitsvorfälle (Runbooks)
- Erkennung und Eliminierung von Schwachstellen
- Erfahrungsaustausch und Nutzung von Security Best Practices

DETECTION

- Professionelle Unterstützung im Angriffsfall durch Cyber-Security-Experten
- Registrierung und zentrale Protokollierung sicherheitsrelevanter Vorgänge
- Minimierung bzw. kein Reputationsverlust durch rechtzeitige Schadenserkennung
- Forensische Analyse von Vorfällen, um den Angriff zu verstehen und geeignete Schutzmaßnahmen abzuleiten

COMPLIANCE

- Einhaltung gesetzlicher Vorgaben, zum Beispiel NIS-2 und IT-SiG 2.0
- Erhöhung der Betriebssicherheit durch Risikominimierung von Geschäftsausfällen

Entscheiden Sie sich für eine wirtschaftlich effiziente Lösung

- Investitions- und Personalkosten für Etablierung und Betrieb eines eigenen SIEM / SOC einsparen, denn Managed Services sind oft günstiger als Eigenerbringung
- Mögliche Einsparungen bei Cyber-Versicherungsprämien durch Reifegradermittlung der Unternehmens-IT
- Hohe Skalierbarkeit durch vorhandene und automatisierbare Security-Plattformen

Die Leistungspakete im Überblick

Die Komponenten setzen sich aus Services, Lizenzen, Tickets und Onboarding zusammen.

LEISTUNGSPAKETE
SECURITY OPERATIONS CENTER

SOC Services powered by SHD START

- 24 × 7 Support inkl. SHD Admin-Hotline
- Automatisierte Alarmierung
- unverzügliche Bearbeitung relevanter Alarme
- fester SHD-Ansprechpartner
- Monitoring und Reporting
- auf Basis des eigenen M365 Defenders

Microsoft Lizenzen und Ticket-Bearbeitung werden separat angeboten

inklusive Themenfelder

Endpoint Detection and Response (EDR)

optionales Themenfeld

Vulnerability Management

SOC Services powered by SHD ADVANCED

- 24 × 7 Support inkl. SHD Admin-Hotline
- umfangreichere Angriffserkennung durch Nutzung erweiterter Sensorik
- Automatisierte Alarmierung
- unverzügliche Bearbeitung relevanter Alarme
- fester SHD-Ansprechpartner
- Monitoring und Reporting
- auf Basis des eigenen M365 Defenders

Microsoft Lizenzen und Ticket-Bearbeitung werden separat angeboten

inklusive Themenfelder

Endpoint Detection and Response (EDR)

Mail Security

Authentication

Cloud App Security

optionales Themenfeld

Vulnerability Management

Endpoint Detection and Response (EDR) erkennt, überwacht und reagiert auf verdächtige Aktivitäten und Angriffe auf Endgeräten wie Laptops, Mobiltelefonen und Servern. Es ermöglicht eine effektive Bedrohungserkennung und schnelle Reaktion zur Eindämmung von Sicherheitsvorfällen.

Mail Security schützt Benutzer vor Bedrohungen wie Malware, Phishing und Spam. Es umfasst Maßnahmen wie Antivirus-Scans, Content-Filterung, URL-Rewriting, Safe-Links und Fraud-Protection.

Authentication überwacht Anmeldevorgänge von Cloud- und onPrem-Entitäten, um verdächtige Benutzeraktivitäten zu erkennen. Mit Künstlicher Intelligenz werden APT-Aktivitäten entlang der Kill Chain analysiert und auf einer Zeitleiste dargestellt, um eine schnelle Erstbewertung zu ermöglichen.

M365 Cloud App Security (CAS) ist der Vermittler zwischen Unternehmen und Cloud-Anwendungen. Es bietet Sicherheitskontrollen und -richtlinien, um den Zugriff auf und die Nutzung von Cloud-Anwendungen zu überwachen, steuern und schützen. CAS ermöglicht umfassende Kontrolle über die Sicherheit und Compliance in der Cloud, einschließlich Bedrohungserkennung, Datenklassifizierung und Schutz sensibler Informationen.

Vulnerability Management identifiziert, bewertet und behebt Sicherheitslücken. Es umfasst regelmäßige Schwachstellen-Scans, Priorisierung nach Risiko und Sicherheitsmaßnahmen oder Update-Empfehlungen, um Ausnutzung durch Angreifer zu verhindern.

SOC – Demo Workshop

In einem Demo-Workshop lernen Sie die Technologie und unseren SOC-Service kennen. Unsere Cybersecurity-Spezialist:innen zeigen live, wie sie Angriffe erkennen und abwehren. Im Workshop identifizieren wir gemeinsam mit Ihnen die für Sie passende SOC-Lösung.

SOC – Proof of Concept

SOC 30 Tage in der eigenen IT-Umgebung testen

1 KICK OFF PoC

- Vorstellung Kundeninfrastruktur
- Festlegung der Erfolgskriterien und Use Cases
- Besprechung Ablauf der Runbooks
- Abstimmung der Ansprechpartner
- Definition Ticket und Informationsübergabe

2 BASISINSTALLATION

- Konfiguration Microsoft Tenant
- Grundinstallation
- ggf. VPN-Anbindung
- Erstellung der Benutzerkonten

3 WORKSHOP(S)

- Anbindung der zu überwachenden Systeme
- Test der Logübertragung
- Feintuning
- Bereinigung und Optimierung der Regeln

4 SOC SERVICES

- Bearbeitung der Incidents innerhalb der Geschäftszeiten
- 4 × wöchentliche Abstimmung (jeweils 1h)
- Laufende SOC-Servcieleistungen mit Abrechnung nach Aufwand

5 PoC ABSCHLUSS

- PoC Abschlussgespräch
- Statusabgleich
- Abgleich der Erfolgskriterien
- Definition weiterer Schritte

SHD ist Ihr Partner in allen Fragen der Cybersecurity, damit Sie sich sicher in der digitalen Welt bewegen können. Als führender IT-Dienstleister in Ihrer Region können Sie sich in den Bereichen IT-Infrastruktur, IT-Security, Digitalisierung, IT-Servicemanagement sowie Cloud und Managed Services auf uns verlassen.

Fordern Sie uns, wir überzeugen Sie!

SHD.
WIR BEWEGEN IT.

Zertifiziert nach
ISO 9001 und ISO 27001

- 1990 in Dresden gegründet
- Stammhaus in Dresden, Geschäftsstellen in Berlin, Leipzig, Hamburg, Nürnberg und in der Lausitz
- Spezielle Lösungen für KRITIS-Anforderungen
- Wir bewegen die IT im Industrie-, Krankenhaus- u. Energiesektor sowie in öffentlichen Einrichtungen

GESCHÄFTLICHE SCHWERPUNKTE

- Digitale Transformation
- IT-Infrastruktur Services
- IT-Sicherheit
- Professioneller IT-Service
- Managed und Cloud Services

KONTAKT: SHD System-Haus-Dresden GmbH · info@shd-online.de · www.shd-online.de