Beratungsgesellschaft für
Informationstechnologie mbH

BFI SOC 365

SERVICE

BESCHREIBUNG

INHALT

BFI SOC365

SOC as a Service ist die Lösung für alle Unternehmen, die ihre IT-Sicherheit auf das nächste Level bringen wollen. Sie erhalten mit unserem managed SOC einen professionellen und kontinuierlichen Schutz vor Cyberangriffen, ohne hohe Investitionen in Hardware, Software oder Personal. Sie profitieren von einem Team aus erfahrenen Sicherheitsexperten, die rund um die Uhr Ihre Systeme überwachen, analysieren und reagieren. Sie erhalten regelmäßige Berichte und Empfehlungen zur Verbesserung Ihrer Sicherheitslage. Somit können Sie sich auf Ihr Kerngeschäft konzentrieren, während wir uns um Ihre IT-Sicherheit kümmern.

ANSPRECHPARTNER

DER BFI

Wir wissen das diese Themen sehr komplex sind und beraten sie auch gerne persönlich, um das für Sie und ihr Unternehmen beste Produkt zu finden.

ANDREAS GOMOLLUCH

MANAGING DIRECTOR

Zum Kontakt

MAIK KIESEWETTER

MICROSOFT SOLUTION ARCHITEKT

Zum Kontakt

HENNING HIRTE

VP SALES

Zum Kontakt

CYBERSECURITY SERVICE: BFI SOC 365

BESCHREIBUNG

MICROSOFT 365 + SOC – PERFECT MATCH

BFI SOC365

WAS IST DER UNTERSCHIED VON UNSEREM ZU ANDEREN?

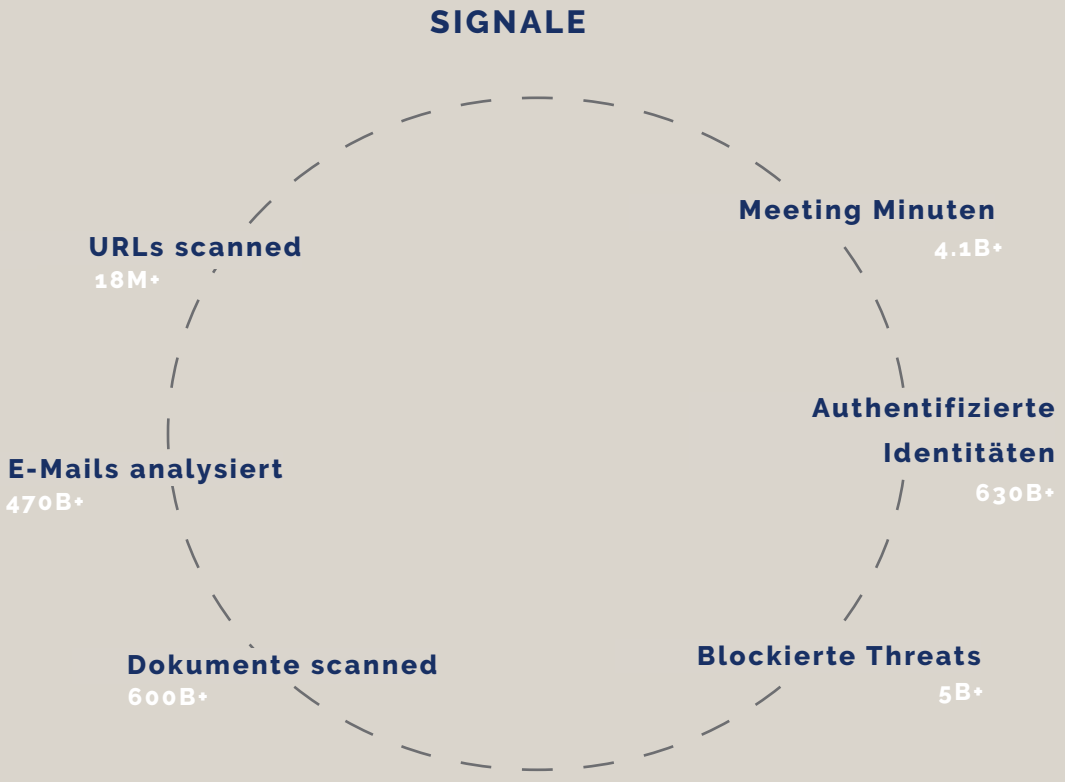
bfi kooperiert mit einem höchst zertifiziertem Partner, welcher seit 2004 einer von 60 MISA (Microsoft Intelligent Security Association) Partner der Microsoft.
Von den ca 15.000 Microsoft Security Partnern sind weltweit nur 60 als MISA Partner benannt.

Die mit unserem MISA Partner entwickelte Gesamtlösung gehört zu den wenigen, denen der Status einer von Microsoft verifizierten MXDR-Lösung verliehen wurde.

Seit 2019 ist dieser Service im Betrieb und wird seit dem weiterentwickelt. Beispielhaft zu erwähnen ist hier der CO-Pilot für Security. Seit dem 01.04.2024 im managed SOC Service von uns integriert.

Hauptaugenmerk dieses Dienstes liegt darauf, dass entweder vollautomatisch oder von Analysten bereitgestellte Reaktionsmaßnahmen durchgeführt werden. Derzeit erreichen wir eine Mean Time to Acknowldge (MTTA) von <5 Minuten und eine Mean Time to Close (MTTC) von <18 Minuten.

Die Microsoft Cloud ist die größte Business Cloud weltweit. Somit greifen wir auf die größte Signalvielfalt der Welt zurück, die sonst kein Marktbegleiter bieten kann.



MICROSOFT 365 + SOC – PERFECT MATCH

BFI SOC365

SOC as a Service ist die Lösung für alle Unternehmen, die ihre IT-Sicherheit auf das nächste Level bringen wollen.

WARUM MICROSOFT?

Der Sicherheitsansatz von Microsoft besteht darin, sowohl die Breite als auch die Tiefe des gesamten Bestands zu verstehen und alles, was vor sich geht, End-to-End zu betrachten.

Wir nutzen die schiere Menge an Telemetriedaten und Informationen, auf die Microsoft Zugriff hat. Die Fähigkeit, Bedrohungen schnell zu erkennen, beruht auf dieser Ebene von Intelligenz und Big Data - und die Transparenz und die Signale (24 Billionen täglich), die Microsoft erhält, sind unübertroffen.

Es geht auch über die reine Erkennung von Bedrohungen hinaus. Mit Microsoft werden neue oder aufkommende Bedrohungen, sobald sie aus all ihren Signalen identifiziert sind, in Echtzeit blockiert und geschützt.

Der Einsatz der Technologien in Microsoft 365 Defender bedeutet, dass wir Bedrohungen aufspüren können, wenn sie irgendwo in Ihrer Umgebung auftauchen - und, was noch wichtiger ist, Wir können im Idealfall die Zeit verkürzen, um sie zu bewerten und zu beseitigen.

MICROSOFT – EIN LEADER IN GARTNER MAGIC QUADRANT-BERICHTEN

2024 Gartner® Magic Quadrant™ for Security Information and Event Management

WORAUS BESTEHT UNSER SOC?

BFI SOC365

01

WERKZEUGE

- Ganzheitliche Erfassung und Prüfung aller Endpunkte
- tägliche Erfassung und Auswertung von Metadaten 24x7x365 Tage im Jahr
- Bewertung von Schwachstellen
- Überwachung von Verhaltensanomalien

02

GESCHULTES TEAM:

- erprobtes Team an Analysten
- großes Team an Forensiker
- umfangreiches Team an Sicherheitsexperten
- automatisiertes Vorgehen bei Vorfällen

03

PROZESS:

- Klassifizierung, Priorisierung und Analyse von Vorfällen
- schnelles Handeln bei ungewöhnlichem Verhalten:
  - Isolierung von kompromitierten Endpunkten, proaktiver Informationsfluss an den Kunden
- Ausführliche und regelmäßige Berichterstattung (Reports, Security Reviews, Updates der Umgebung auf aktuelle Sicherheitsstandards)

WIR BIETEN ZWEI UNTERSCHIEDLICHE SERVICESTUFEN FÜR UNSEREN MANAGED BFI SOC365 AN.

WELCHE SERVICESTUFEN BIETEN WIR AN?

SERVICE BESCHREIBUNG

GENERELL INBEGRIFFEN

- **Service Angebote mit 2 Leveln der Abdeckung**
  - MXDR Advanced
  - MXDR Premium
- **Extended Detection & Response (XDR)** umfasst benutzerdefinierte Regeln zur Erkennung von Bedrohungen sowie die Erstellung und Verwaltung benutzerdefinierter Sicherheits-Playbooks.
- **Hocheffizientes Onboarding**
- **Präventiver Service mit Schwerpunkt auf kontinuierlicher Verbesserung durch kontinuierliche Governance.**
- **Alle Services werden 24x7x365 aus dem Managed Security Operations Center (SOC) geliefert.**
- **Proaktive Cyber-Bedrohungs-Informationen**
- **Wir brauchen durchschnittlich 10 Minuten, um auf eine Bedrohung zu reagieren und sie zu beheben.** Empfehlung der Branche: 60 Minuten.

GEGENÜBERSTELLUNG UNSERER SERVICESTUFEN

DIENST BESCHREIBUNG

	MXDR Advanced	MXDR Premium
Erreichbarkeit über Telefon und E-Mail das gesamte Jahr (24x7x365)	✓	✓
max. 30min Bearbeitungszeit, bei höchster Einstufung des Vorfalls	✓	✓
Proaktive Unterstützung bei erforderlicher Eindämmung und/ oder Behebung erkannter Gefahren	✓	✓
Volle Abdeckung mit sämtlichen Microsoft Sicherheitsdiensten	✓	✓
SIEM Integration von Benutzerdefinierten, nicht Microsoft Produkten und Diensten	✓	✓
Gefahrenkennung und aktive Information für Endpunkte, Identitäten, Server	✓	✓
Gefahrenkennung und aktive Information sowie nicht Azure Dienste, Netzwerkgeräte, Drittanbieter Schnittstellen/Logfiles		✓
Wöchentliche Sicherheitsreports über die eigene, aktuelle Bedrohungslage	✓	✓
Erweiterte Verfolgung von Endpunktbedrohungen mit den aktuellsten Bedrohungsinformationen Weltweit	✓	✓
Playbooks für Sicherheitseinstellungen und Sicherheitsempfehlungen nach neusten Standards und für nicht standardisierte Umgebungen	✓	✓
Erkennungen aktueller TaktikenundTechniken von Angreifern über MITRE Attack		✓
Überwachung Ihrer externen Angriffsfläche		✓

WEITERE LEISTUNGEN

VON BFI & PARTNERN

WELCHE LEISTUNGEN BIETEN WIR DARÜBER HINAUS AN?

- Beratung und Transformation in die Microsoft Cloud (MS 365 / Azure)
- Health Checks und Penetration Tests
- Cybersichere Backup Lösungen für Cloud und hybride Infrastrukturen
- Gemeinsame Unterstützung mit Microsoft beim Assessment und Migration zu Microsoft 365
- Sicherheitsanalyse für relevante Endpunkte/-Geräte/-Anwendungen/-Dienste
- CyberRisikoCheck nach “DIN SPEC 27076”
- Compliance und Governance Beratung und Umsetzung unter Berücksichtigung aller gesetzlichen Verordnungen (geforderte TOMs, NIS-2-Richtlinie und weitere)
- App Risk Management
- KI gestützte mobile Endpoint Protection

bfi Beratungsgesellschaft für Informationstechnologie mbH

Hugh-Greene-Weg 2 | 22529 Hamburg Geschäftsführer: Andreas Gomolluch | Sitz Hamburg | Amtsgericht Hamburg | HRB 66645 @ Ust. Ident Nr. DE 193020604