IS4IT KRITIS

Security Operations

IS4IT Modern SOC

LEISTEN SIE SICH SICHERHEIT STATT KRITISCHER AUSFÄLLE

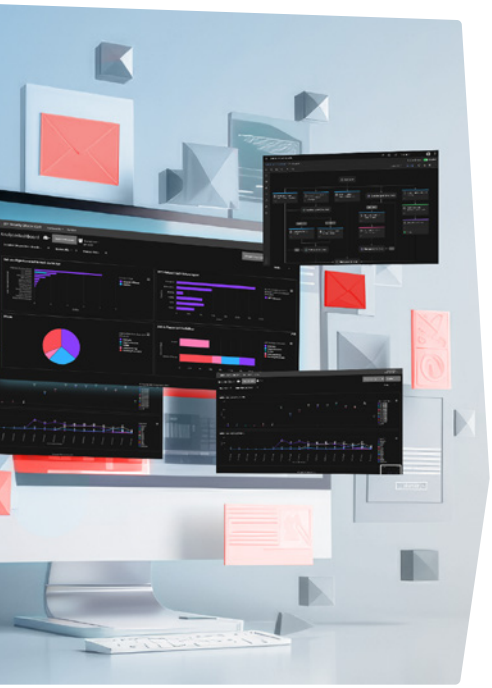
SIND IHRE GESCHÄFTSKRITISCHEN SYSTEME RUND UM DIE UHR GESCHÜTZT?

Angriffe rechtzeitig erkennen und abwehren

Angriffe aus dem Internet, aber auch aus dem internen Netz, steigen seit Jahren kontinuierlich an und sorgen für beträchtliche Schäden. Eine Vielzahl an Lösungen am Markt trägt dazu bei, die Sicherheit zu gewährleisten. Die Komplexität der verschiedenen Systeme ist jedoch groß, die Kosten für Lizenzen und Personal sind sehr hoch und die Verfügbarkeit eigener qualifizierter Mitarbeiter ist unzureichend. Oft fehlen darüber hinaus die notwendige kontinuierliche Systemüberwachung sowie fundierte Analysen.

Mit der Sicherheitslösung **Microsoft Defender XDR**, die viele KMUs häufig bereits mit ihren Microsoft-Paketen lizenziert haben, lässt sich die Systemüberwachung in einem cloudbasierten Security Operations Center zwar sehr effektiv umsetzen, aber ...

... qualifizierte Mitarbeiter, die 24x7 für die Analysen zur Verfügung stehen, sind nicht nur Mangelware, sondern können durch ein einzelnes Unternehmen auch nicht ausgelastet werden. Outsourcing ist eine Option – wenn die Voraussetzungen hierfür stimmen.



Anforderungen an ein risikofreies Outsourcing

- Leistungsfähiger Anbieter im Bereich Managed Security Services
- Umfassendes Sicherheitsportfolio
- Zertifizierte Serviceorganisation
- SOC-Services eines deutschen Managed Services Provider
- Hohe Kompetenzen in der Microsoft-Plattform
- Langjähriger Microsoft-Partner

Damit *alle* Unternehmen SOC umsetzen können: IS4IT Modern SOC

Technologisch basiert der Service auf **Microsoft Defender XDR** und steht für Überwachung rund um die Uhr. Dabei sorgen unsere Analysten für die Sicherheit Ihrer Server und Workstations zu monatlich kalkulierbaren Kosten, die auch für kleine und mittlere Unternehmen finanzierbar sind.

Als Spezialist im Bereich Managed Security Services für sichere Infrastrukturen bis hin zu KRITIS-Umgebungen decken wir gemeinsam mit Microsoft und dem **IS4IT Modern SOC** sämtliche Anforderungen an ein zuverlässiges Outsourcing Ihres Security Operations Center ab.

Einfach. Sicher. IS4IT Kritis.

ALLES ANDERE ALS BASIC: SO FUNKTIONIERT DER MANAGED SECURITY SERVICE

Das Hauptziel des Security Operations Center besteht darin, eine möglichst umfassende Überwachung und Analyse der Informationssicherheit zu realisieren, um potenzielle Sicherheitsvorfälle frühzeitig zu erkennen und zu bewältigen.

Das **IS4IT Modern SOC** identifiziert etwaige Bedrohungen sämtlicher Endgeräte und schlägt Gegenmaßnahmen zur Verhinderung oder Eindämmung von Cyberangriffen vor. Alle Meldungen der Sensoren werden im Sicherheits-Cockpit zusammengefasst. Dies erlaubt es unseren Security-Experten, sowohl ein Monitoring als auch eine Analyse durchzuführen, damit verborgene Bedrohungen erkannt und abgewehrt werden. Zur Optimierung und Automatisierung der Incident-Response-Prozesse kommt intern ein Security Orchestration, Automation and Response (SOAR) zum Einsatz, das standardisierte Prozesse in der Bearbeitung der Incidents mithilfe von Playbooks gewährleistet.

Unser Angebot

- Analyse Ihrer Sicherheitsanforderungen
- Implementierung
- Anbindung der Microsoft Defender Suite
- 24x7 Sicherheitsanalyse und Untersuchung ab Incident Severity „medium“
- Bedrohungsaufklärung und Eskalation bei kritischen Vorfällen
- Ereignisdokumentation und Berichterstattung per Ticket
- Erstreaktion auf Incidents gemäß Playbook
- Deaktivierung von Defender-Regeln im gesamten Leistungszeitraum
- Monatliches Trend-Reporting und quartalsweise Service Meetings
- Individuelle Anpassungen nach Absprache möglich

Microsoft Defender XDR in aller Kürze

- Endpunktsicherheit auf Windows-, macOS-, Linux-, Android-, iOS- und IoT-Geräten
- KI-gestützte Automatisierung bei Nutzung von Microsoft Copilot
- Erstellung einer Configuration Management Database (CMDB) für Microsoft Configuration Manager
- Verwaltung durch Microsoft Intune möglich
- Automatische Angriffsunterbrechung
- Integrierte Täuschungsfunktion für authentisch wirkende Decoy-Konten, Hosts und Köder
- CTI – Cyber Thread Intelligence
- Priorisierte Empfehlungen zum Sicherheitsstatus mithilfe von Defender Vulnerability Management
- Netzwerkerkennung und -reaktion

Nutzen

- Sicherheitsrisiken minimieren durch End-to-End-Sicherheit für Multiplattform- und IoT-Geräte mit umfassender Antiviren-, Erkennungs- und Reaktionslösung (Extended Detection & Reaction)
- Ausgefeilte Angriffe mit KI ausmanövrieren und Cyberangriffe wie Ransomware verhindern
- Prävention mit globaler Bedrohungserkennung erhöhen
- Schutz durch Experten und Entlastung Ihrer Mitarbeiter
- Punktgenaue Gewährleistung Ihrer Service Level Agreements
- Kalkulierbare Kosten durch vereinheitlichte Leistung

DAS RICHTIGE MASS AN SICHERHEIT FÜR IHREN BEDARF

Das **IS4IT Modern SOC** richtet sich an alle Unternehmen, die den Fokus auf den wirtschaftlichen Schutz ihrer IT-Systeme legen und (noch) keine erhöhte Überwachung wünschen. Bei veränderter Bedrohungslage oder wachsenden Sicherheitsanforderungen stehen erweiterte Servicepakete zur Verfügung.

	IS4IT Modern SOC	IS4IT Advanced SOC	IS4IT Infinite SOC
	Wenn Ausfälle ***kritisch*** sind	Wenn Ihre IT funktionieren ***muss***	Wenn erhöhte Überwachung ***unverzichtbar*** ist
Reaktionszeit	**30 Minuten**	**30 Minuten**	**30 Minuten**
Überwachung Server, Workstations, Smart Devices	✓	✓	✓
Überwachung Infrastruktur (Firewall, Storage ...)	✗	✓	✓
Überwachung Applikationen	✗	✓	✓
Fester, technischer Ansprechpartner	✗	✓	✓
On-Premise-Installation, Daten bei Ihnen	✗	✗	✓
Technologien	**EDR**	**Cloud-SIEM**	**On-Prem-Siem**
Kosten	€	€€	€€€

UNSERE SECURITY-PARTNER

Wir setzen auf weltweit erfolgreiche und erprobte Sicherheitstechnologien zur Umsetzung von kosteneffizienten, modernen und ausgereiften Security-Lösungen.

WARUM WIR?

Unsere Mitarbeiter bringen langjährige Erfahrungen aus unterschiedlichsten Security- und Monitoring-Projekten ein. Der Geschäftsbereich Managed Security Services ist seit Jahren erfolgreich am Markt etabliert. Sämtliche Managed-Security-Prozesse der IS4IT-Gruppe sind KRITIS-konform und nach verschiedenen Normen zertifiziert. Auch die Zusammenarbeit mit Organisationen, für die aus Vertraulichkeitsgründen eine Geheimschutzbetreuung unverzichtbar ist, ist sichergestellt.

IS4IT Kritis ist als Mitglied im BSKI, der TeleTrusT „Security made in Germany“ sowie der Allianz für Cyber-Sicherheit aktiv. IS4IT ist nach ISO/IEC 27001und ISO 9001 zertifiziert.

Namhafte Kunden aller Branchen vertrauen auf unsere Expertise.

Wir leben, was wir empfehlen ... tagtäglich!

Daher ist die IS4IT-Gruppe Ihr idealer Partner. Wir sollten uns kennenlernen.

IS4IT KRITIS GmbH
Kraichgaublick 13
74847 Obrigheim
Deutschland
telefon +49 6262 9262594
info@is4it-kritis.de

IS4IT GmbH
Grünwalder Weg 28b
82041 Oberhaching
Deutschland
telefon +49 89 6389848-0
info@is4it.de

IS4IT Schweiz AG
Allmendstrasse 1
6300 Zug
Schweiz
telefon +41 41 7200090
info@is4it.ch

IS4IT Cyber Security Austria GmbH
Franz-Josefs-Kai 49/19
1010 Wien
Österreich
telefon +43 676 889854401
info@is4it.at

Zertifikate/Siegel der IS4IT KRITIS GmbH