Security Operation Center

Wir leben Sicherheit.

SkySystems

SOC

MANAGED SOC

Unsere innovative Erkennungs- und Reaktionslösung erkennt Anomalien in Ihrer IT-Umgebung, stoppt Angreifer und informiert Sie in Echtzeit. Ermöglicht und betreut wird dies durch unser Security Operation Center.

24/7 Cyber-Sicherheit - von Experten betreut

Unser Security Operation Center, kurz SOC, ist ein Managed-Service, der eine Bedrohungsüberwachungsplattform nutzt, um verdächtige Aktivitäten in den Angriffsvektoren Endpoint, Netzwerk und Cloud zu erkennen.

Unsere Sicherheitsexperten suchen proaktiv nach Bedrohungen, priorisieren mögliche Gefahrenquellen, erkennen und blockieren Angreifer und informieren Sie in Echtzeit über Ereignisse.

Mit unserem SOC sind Sie Angreifern einen Schritt voraus!

ENDPUNKT-SICHERHEIT

Überwachung von Windows- und macOS-Ereignisprotokollen, Erkennung von Regelverstößen, bösartigen Dateien und Prozessen, Bedrohungen, Einbrüchen, sowie Integration von NGAVs von Drittanbietern und mehr.

NETZWERK-SICHERHEIT

Firewall- und Edge-Geräte-Protokollüberwachung mit Echtzeit-Bedrohungsbewertung, DNS-Informationen und Warnungen bei bösartigen Verbindungen.

CLOUD-SICHERHEIT

Microsoft 365-Überwachung von Sicherheitsereignisprotokollen, Azure AD-Überwachung und Überprüfung verdächtiger Anmeldungen.

- ✔ **permanente 24/7 Überwachung**
- ✔ **über 50 Jahre** IT-Security Erfahrung
- ✔ **Verstoßerkennung** durch die fortschrittlichste Technik, die auf dem Markt zu finden ist
- ✔ proaktives **Threat Hunting** durch unser Sicherheitsteam
- ✔ **keine Hardware erforderlich** durch den Einsatz von Cloud-Technologie
- ✔ **Hand in Hand Zusammenarbeit** mit Ihrem IT-Verantwortlichen

Die folgenden umfangreichen Funktionen ermöglichen es Ihnen, sich auf Ihr Kerngeschäft zu konzentrieren, während unser Expertenteam rund um die Uhr sicherstellt, dass Ihre IT-Infrastruktur bestmöglich gegen Angreifer und Bedrohungen geschützt ist.

SIEMLESS PROTOKOLL-MONITORING

Überwacht, sucht, alarmiert und informiert Sie über die Angriffspfeiler Netzwerk-, Cloud- und Endpointprotokolle, Firewalls und Netzwerkgeräte, Microsoft 365 sowie Azure AD.

VERBINDUNGSÜBERWACHUNG

Echtzeitüberwachung von verdächtigen Aktivitäten und Verbindungen ins (nicht genehmigte) Ausland, nicht autorisierten TCP/UDP-Diensten, Backdoor-Verbindungen zu C2-Servern und lateralen Bewegungen in Ihrem Netzwerk.

THREAT INTELLIGENCE & THREAT HUNTING

Proaktive Arbeitsweise und Zusammenarbeit mit Premium-Intel-Feed-Partnern, die uns Zugriff auf das größte globale Archiv von Bedrohungsindikatoren ermöglicht, wodurch wir Angreifer noch effektiver aufspüren können.

NEXTGEN-MALWARE

Verwenden Sie Ihre eigene Malware-Lösung oder nutzen Sie unsere Command-and-Control-App für Microsoft Defender.

PENETRATION-DETECTION

Das SOC erkennt außerdem Angreifer, die sich herkömmlichen Cybersicherheitsabwehrmaßnahmen wie Firewalls und Antivirenprogrammen entziehen. Es identifiziert Angreifer-TTPs und gleicht sie mit MITRE ATT&CK ab, um eine forensische Timeline der zeitlichen Ereignisse zu erstellen und so den Eindringling zu erkennen, bevor ein Einbruch erfolgen kann.

PSA-TICKETVERWALTUNG

Unsere SOC-Analysten untersuchen jeden Alarm und erstellen ein Ticket für Ihr PSA-System mit den entsprechenden Details.

passende App verfügbar!

Überwachen Sie den Status Ihrer IT-Infrastruktur 24/7 in der verfügbaren App. Aktivieren Sie nur die Benachrichtigungen, die für Sie relevant sind und wählen Sie dazu aus über 35 Anwendungen.

- ✔ Warnungen auch mobil empfangen
- ✔ Status Ihrer IT-Infrastruktur jederzeit einsehen
- ✔ Verknüpfung mit Ihren Sicherheitsanwendungen möglich
- ✔ Und vieles mehr...

PREISE

Leistungen	Basic	Bestseller Business	Premium
24/7 Monitoring	✔	✔	✔
Monatlicher Bericht	✔		
Wöchentlicher Bericht		✔	✔
Call von Security Consultant zur Durchsprache der Ereignisse im vergangenen Zeitraum	jährlich	quartal	monatlich
Individuelle Reaktionen durch SkySystems Service Desk Mo-Fr: 08:00-17:00 Uhr Mo-Fr: 08:00-23:00 Uhr	✔	✔	✔
Benachrichtigung bei kritischen Ereignissen (telefonisch)	Kunde selbst	Mo-Fr 08:00-23:00 Uhr SkySystems	SkySystems
Automatisierte Reaktionen z.B. Runterfahren der Systeme, Sperrung von Konten	✔	✔	✔
Monitoring von M365	optional	✔	✔
Management und Überwachung der regionalen Login Einschränkungen	optional	✔	✔
Preise			
Erstmaliges Setup	299,00€	299,00€	299,00€
Grundgebühr	99,00€	199,00€	299,00€
M365 Tenant Management	49,00€	✔	✔
Management Regio Einstellungen	9,90€ / Änderung	✔	✔
Staffelpreise Server			
1-9 Geräte	9,90€	11,90€	13,90€
10-50 Geräte	7,90€	9,90€	11,90€
51-100 Geräte	5,90€	7,90€	9,90€
ab 101 Geräten	individuell	individuell	individuell
Staffelpreise Clients			
1-19 Geräte	7,90€	9,90€	11,90€
20-50 Geräte	6,90€	8,90€	10,90€
51-100 Geräte	5,90€	7,90€	9,90€
101-250 Geräte	4,90€	6,90€	8,90€
ab 251 Geräten	4,50€	6,50€	7,50€
Beispiele inkl. Tenantmanagement			
Kleinunternehmen 5 Server und 25 Clients	370,00€	481,00€	641,00€
KMU 10 Server und 50 Clients	572,00€	743,00€	963,00€
Größeres KMU 20 Server und 100 Clients	896,00€	1.187,00€	1.527,00€
Großes Unternehmen 40 Server und 250 Clients	1.640,00€	2.320,00€	3.000,00€

Alle Preise netto, zzgl. Mwst.

Herausgeber: SkySystems IT GmbH, Ceger Str. 47, 58642 Iserlohn, Fon: +49 2374 40948-0, Fax: +49 2374 40948-99, info@skysystems.it, www.skysystems.it;
Sitz der Gesellschaft: Iserlohn, Amtsgericht Iserlohn: HRB7768, Geschäftsführer: Roger Geitzenauer; Bilder und Grafiken: Shutterstock; Stand: Mai 2023