Managed Detection and Response (MDR)

Überwachung, Alert Triage und operative Unterstützung, die Ihre Ressourcen schont.

Anwendungsfälle

- Aktive Abwehr von Ransomware und Trojanern
- Bewertung und Eskalation der Sicherheitsvorfälle
- Unterstützung bei Sicherheitswarnungen
- Verwaltung von Zugriffen auf USB-Schnittstellen
- Isolierung der Endgeräte
- Forensische Untersuchungen auf Abruf
- Sicherheitsexperten, die Ihr Team ergänzen

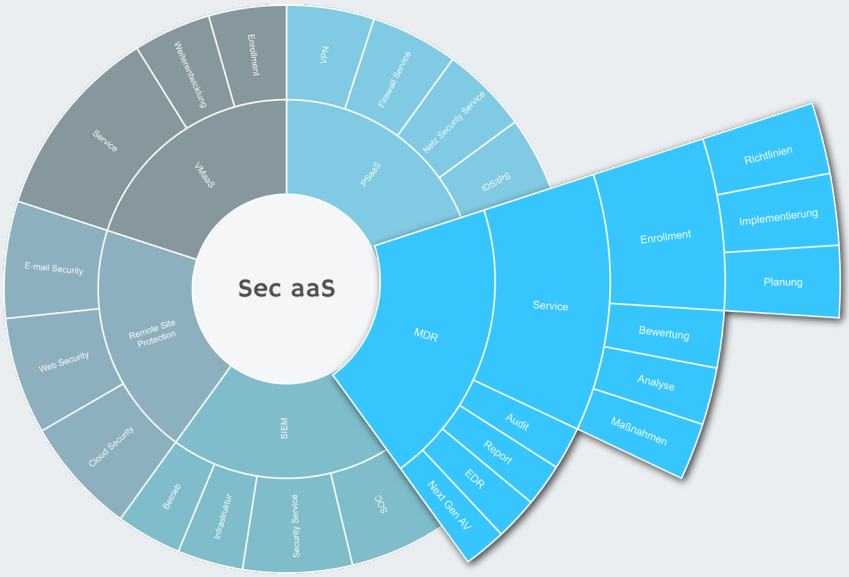
Vorteile

- Keine eigene Infrastruktur erforderlich
- Effiziente und proaktive Sicherheitsabläufe
- Entlastung des IT-Personals
- Schnellere Ursachenforschung
- Warnungen und Priorisierung potenzieller Angriffe
- Kontinuierliche Transparenz
- Einfache Skalierbarkeit
- Reduzieren der Komplexität
- Identifizieren von Sicherheitstrends zur Steuerung von Richtlinien
- Proaktive IT-Hygiene
- Automatisieren der Audit-Berichte
- Ad-hoc Berichte
- Vollständige Ursachendokumentation für weiterführende forensische Untersuchungen

Die Vielzahl unterschiedlichster Endgeräte zu überwachen ist eine Herausforderung für die Krankenhaus-IT. Alarme zu validieren kostet Zeit, insbesondere wenn die Historie der Ereignisse nicht bekannt ist. Durch die eingeschränkte Analyse und Nachverfolgung der Angriffe steigt das Risiko von Ransomware oder Trojanern angegriffen zu werden. Doch weitere IT-Sicherheitsexperten sind rar und teuer. Ein Dilemma, das häufig zu Lasten anderer IT-Sicherheitsaufgaben geht.

Mit Managed Detection and Response (MDR) von omniIT erhält Ihr Krankenhaus den dringend benötigten Einblick in Angriffe, ohne eigene Sicherheitsexperten einzustellen. Wir überwachen Ihre Endgeräte, reichern die Daten mit fortschrittlichen algorithmischen Tools auf Basis von Machine Learning an und benachrichtigen Sie über Bedrohungen, Ursachen und umsetzbare Abwehrmaßnahmen. Gemeinsam mit Ihrem Team validieren und priorisieren unsere Experten Alarme, decken Bedrohungen auf und beschleunigen die Untersuchungen.

Die Managed Service Lösung von omniIT basiert auf den marktführenden Plattformen von VMware (Carbon Black), SentinelONE oder TrendMicro. Schützen Sie Ihre Endgeräte wirksam und kostengünstig mit unserer Kombination aus Technologie und Expertise.



Cybersicherheit im globalen Kontext

- omniIT Experten nutzen die ungefilterten Daten des EDR Systems, um Bedrohungen zu verfolgen.
- Globale Bedrohungsdaten ermöglichen uns, Angriffstrends zu erkennen und proaktive Maßnahmen zu treffen.

Features

- Hosting in Europa/Deutschland nach höchsten Sicherheitsstandards
- Erkennung von Angriffen
- Anpassbare Verhaltenserkennung
- Überprüfung von Bedrohungen
- Visualisierung der Angriffskette
- Echtzeit Warnungen
- Ursachenanalyse
- Informationen zu Bedrohungen
- Monatliche Berichte

Unterstützte Plattformen

Windows:	Desktop 7/8/10/(11) Server 2008 - 2019
Mac OS X:	10.6.8+
Linux:	RHEL 7+ Debian 9+ Ubuntu 16+ CentOS 6+ Oracle 6+ SUSE 12+ + weitere*

Erfahren Sie mehr

Kontaktieren Sie uns für eine gratis Demo oder individuelle Beratung durch unsere KHZG-zertifizierten Experten.

Michael Ruhdorfer
Tel.: +49 (89) 998 241 920
Mail: secaas@omniit.de

omniIT GmbH
Georg-Hallmaier-Str. 6
81369 München
Telefon +49 89 998 24192 0
E-Mail: info@omniit.de
Web: www.omniit.de
KHZG Webpage: www.khzg.omniit.de
Geschäftsführer: Patryk Wlodarczyk, Marek Chroust

Ihr Mehrwert

Volle Transparenz
Mit einer vollständigen Abdeckung der IT-Landschaft kann Ihr Team sicher sein, dass nichts unentdeckt bleibt. Die omniIT Experten bearbeiten proaktiv die Alarme und Informieren Sie über potenzielle Bedrohungen.

Roadmap zur Grundursache
Anhand von wiederkehrenden Auffälligkeiten wird eine Korrelation der vom System generierten Alarmen durch unsere Experten sichergestellt. Damit helfen wir Ihnen, Untersuchungen zu rationalisieren und Sicherheitsprobleme dauerhaft zu lösen.

Echtzeit-Unterstützung
Mit der Unterstützung in Echtzeit stellen unsere Experten eine sichere Verbindung zu infizierten Endgeräten her, um die verdächtigen Dateien, Prozesse oder Verbindungen zu analysieren und zu beheben. Auf diese Weise kann ein krankenhausweiter Ausbruch von Schadsoftware vermieden werden.

Reporting
Auf Basis der Berichte können Richtlinien verfeinert werden. Dies hilft Ihrem Team, Trends im Gesamtbild zu erkennen. Sie erhalten einen detaillierten Überblick über alle verdächtigen Aktivitäten in Ihrer Umgebung einschließlich Informationen über die am häufigsten angegriffenen Endgeräte.

cybereason · SentinelOne · vmware Carbon Black · Windows Defender · SOPHOS · TREND MICRO

Features	omniSec X monatlich ab 9,90 € / Gerät	omniSec X Complete monatlich ab 16,90 € / Gerät
24/7/365 Schutz & Überwachung	✓	✓
NGAV Antivirus System der nexten Generation	✓	✓
Aktive Analyse der Vorfälle und Unterstützung	8/5	24/7
Echtzeit Dashboards und Reporting	✓	✓
Faktor-Mensch Risikoanalyse	✓	✓
Erweiterte Policies (MITTRE ATT&CK, PCI, HIPA)	✓	✓
Kontinuerliche Analyse der Schwachstellen	✓	✓
Client Rollout	✓	✓
Management und Update der Sensoren	✓	✓
Support per Mail, Telefon und Portal	✓	✓
SIEM & Korrelation der Sicherheitsvorfälle		✓
Forensische Analyse		✓
Kundenspezifische Anwendungsfälle und Playbooks		✓
Dedizierter Ansprechpartner		✓
Incident Response	auf Anfrage	