IT-Sicherheit auf höchstem Niveau

Security Operations Center

iteracon.de

We manage IT.

Die Zeit der singulären und starren Sicherheitssysteme ist endgültig vorbei.

„Kriminelle sind sehr gut organisiert und entwickeln ständig neue Cyberangriffe. Studien zeigen, dass diese Angriffe Unternehmen immer schwerwiegendere Schäden zufügen. Die Sicherheit in der IT muss daher oberste Priorität haben. Genau hier setzt unser Security Operations Center an.“

- David Schwalen, Director Managed Service & Strategy, iteracon GmbH

Herausforderungen

In einer Zeit der professionell organisierten Cyber-Kriminalität, gilt es die Daten Ihres Unternehmens bestmöglich zu schützen und gleichzeitig hochverfügbar zu machen.

Optimale Lösung

Ein zentralisiertes Sicherheitsmanagement, das Ihre IT-Systeme rund um die Uhr überwacht und Experten die auf jede Bedrohungen individuell reagieren.

Ergebnis

Die Experten des iteracon SOC übernehmen alle sicherheitsrelevanten Angelegenheiten Ihrer Organisation. Mögliche Angriffe werden hierbei in Echtzeit abgewehrt, um den Geschäftsbetrieb nicht zu gefährden.

Gold
Microsoft Partner
Microsoft

ITERACON

ITERACON

Die Lösung:

ITERACON

Defender for Identity

Microsoft Defender for Identity nutzt Informationen ihrer Active-Directory Instanzen, um komplexe Bedrohungen, gefährdete Identitäten und schädliche Insideraktionen gegen Ihre Organisation aufzudecken.

Gold
Microsoft Partner
Microsoft

We manage IT.

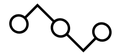
Defender for Identity

ITERACON

Profiling von Benutzeraktivitäten

Der Defender for Identity überwacht netzübergreifend Benutzeraktivitäten, um Anomalien zu erkennen. Dadurch können in Echtzeit komplexe Bedrohungen erkannt werden.

Kill Chain



Identifikation von Bedrohungen über die gesamte 5-phasige Kill Chain, indem die klassischen Angriffs-vektoren registriert und angezeigt werden.

Schutz von Hybridumgebungen

AD FS spielt bei der Authentifizierung in Hybridumgebungen eine wichtige Rolle. Der Defender for Identity schützt diese Verbunddienste, indem Authentifizierungsereignisse auf mögliche Angriffe untersucht werden.

Zero-Trust-Prinzip

Mit Hilfe des Zero Trust Ansatzes sichern wir Ihre Systeme über die genannten Schutzmechanismen hinaus. Jede Anforderung muss hierbei vollständig authentifiziert, autorisiert und verschlüsselt sein.

Gold
Microsoft Partner
Microsoft

We manage IT.

ITERACON

Defender for Endpoint

Der Defender for Endpoint ist eine in diverse Lösungen integrierbare Sicherheitsplattform, die Bedrohungen auf Ihren Endgeräten frühzeitig erkennt und abwehrt.

Gold
Microsoft Partner
Microsoft

We manage IT.

Defender for Endpoint

ITERACON

Endpunkterkennung

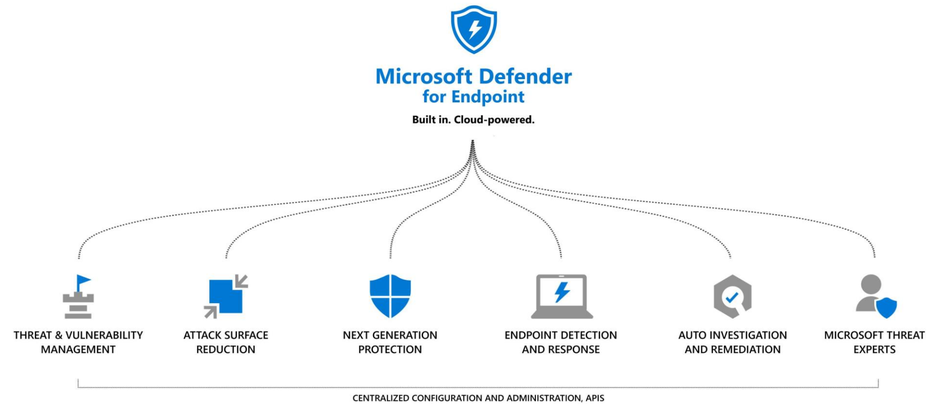
In Ihre Betriebssysteme eingebettete Sensoren sammeln Verhaltenssignale, um Anomalien aufzudecken und Bedrohungen frühzeitig zu erkennen und abzuwehren.

Sicherheitsbewertung für Ihre Geräte

Mit Hilfe der Microsoft-Sicherheitsbewertung für Endgeräte, können Sie den Sicherheitsstatus Ihres Netzwerks dynamisch bewerten, unsichere Systeme identifizieren und anschließend empfohlene Aktionen ausführen.

Automatisierte Cloud-Sicherheit

Defender for Endpoint funktioniert Agent-los in der Cloud. Ohne Verzögerungen oder Kompatibilitäts-problemen bei Updates ist es immer auf dem neuesten Stand und bedarf keiner zusätzlichen Bereitstellung oder Infrastruktur.



Gold
Microsoft Partner
Microsoft

We manage IT.

ITERACON

Azure Sentinel

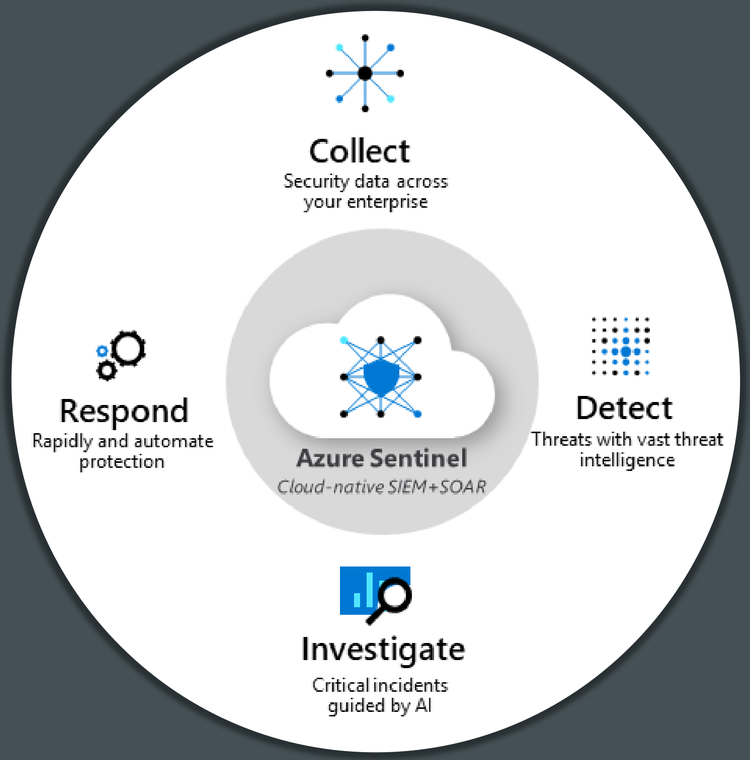
Als cloud-basierte SIEM-Lösung stellt Azure Sentinel das Herzstück des ITERACON SOC dar. Für die Sicherheitsanalysen und Gefahrenabwehr kommen hier künstliche Intelligenz und Machine Learning zum Einsatz.

Gold
Microsoft Partner
Microsoft

We manage IT.

Azure Sentinel

Microsoft Azure Sentinel liefert Sicherheitsanalysen für Ihr gesamtes Unternehmen und bietet die Möglichkeit, potenzielle Bedrohungen frühzeitig zu erkennen und abzuwehren.



Log Management

Daten über alle Benutzer, Geräte, Anwendungen und Infrastrukturen werden in der Cloud gesammelt. Über Schnittstellen können hier Daten von Microsoft Lösungen und anderen Anbietern gesammelt werden.

Threat Detection

Entdecken von Anomalien mit Hilfe von Erkennungsregeln und externer Threat Intelligence, unterstützt durch von Microsoft Engineers entwickelte Machine Learning Systeme.

Gold Microsoft Partner

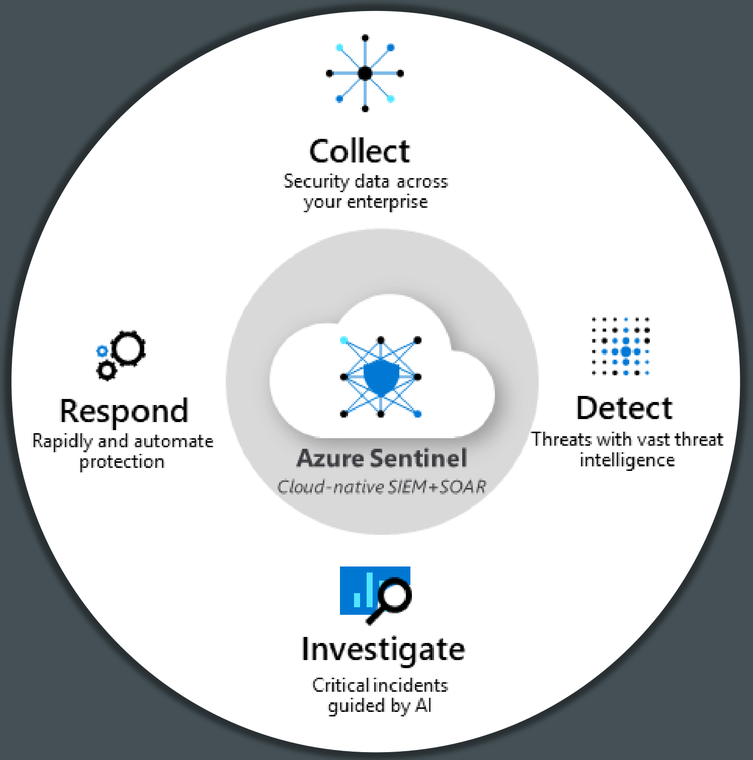
Microsoft

We manage IT.

Azure Sentinel

ITERACON

Microsoft Azure Sentinel liefert Sicherheitsanalysen für Ihr gesamtes Unternehmen und bietet die Möglichkeit, potenzielle Bedrohungen frühzeitig zu erkennen und abzuwehren.



Threat Response

Automatische Reaktion auf Sicherheitsereignisse durch Warnung, Ticketerstellung, Einstufung der Bedrohungslage sowie Abwehrmaßnahmen anhand von Sentinel Playbooks basierend auf Azure Logic Apps.

Network Security

Die zentralen Stellen Ihres Netzwerks, an denen der Datenverkehr konvergiert, werden in Sentinel integriert. Dies sorgt für einen transparenten Datenfluss, wodurch Auffälligkeiten in Echtzeit erkannt werden können.

Gold Microsoft Partner
Microsoft

We manage IT.

ITERACON

Compliance Management

Mit Hilfe des Security & Compliance-Center wird Regelkonformität innerhalb Ihres Unternehmens sichergestellt. Die anhand der ITERACON Best Practices entwickelten Richtlinien schützen sie aktiv vor Datenverlusten und Imageschäden.

Gold
Microsoft Partner
Microsoft

We manage IT.

Compliance Management

ITERACON

Microsoft Defender for Cloud Apps

Defender for Cloud Apps ist ein Cloud Access Security Broker (CASB), der auf mehreren Clouds betrieben wird. Er bietet umfassende Transparenz und Kontrolle über den Datenverkehr und ermöglicht so das Erkennen und Bekämpfen von Cyberbedrohungen.

Datenklassifizierung

Mit Hilfe von Metadateneigenschaften strukturieren wir Ihre Daten entlang der drei Stufen public, internal und confidential. So können sensible Daten und Geschäftsgeheimnisse besonders geschützt werden.

Data Loss Prevention

Mit Hilfe von Data Loss Prevention Richtlinien können vertrauliche Informationen vor Verlust oder unbefugtem Zugriff geschützt werden.

Gold
Microsoft Partner
Microsoft

We manage IT.

ITERACON

Service Delivery Modell

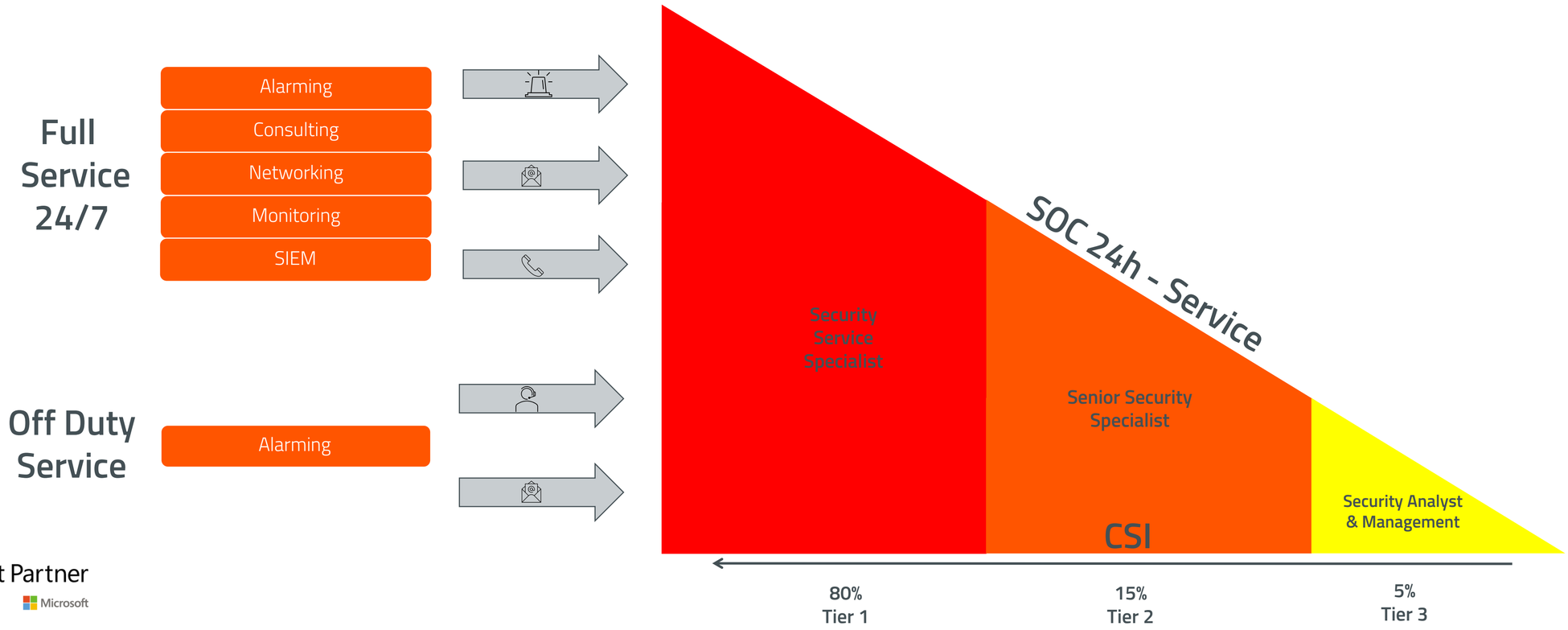
Das Service Delivery Modell visualisiert die Zeitmodelle, High-Level Service Umfänge, Security Skills, Lastenverteilung und CSI Maßnahmen.

Gold
Microsoft Partner
Microsoft

We manage IT.

SOC Service Delivery Modell

Das SOC beinhaltet ein umfassendes Spektrum an Leistungen, Modellen und Security Spezialisten auf allen Ebenen. Intelligente Automatismen sowie die Best Practice Prozesse der ITERACON sorgen dabei für einen hohen Effizienzgrad.



Gold Microsoft Partner

Microsoft

We manage IT.

SOC Service Delivery Modell

ITERACON

Full Service

Unser ganzheitlicher Full-Service-Ansatz für den SOC Betrieb umfasst ein zentralisiertes Sicherheitsmanagement, das die IT-Infrastruktur Ihres Unternehmens rund um die Uhr vollumfänglich absichert.

Off Duty Service

Auch außerhalb Ihrer regulären Betriebszeiten schützt Sie der Off Duty Service vor potenziellen Angriffen, indem definierte Alarmmeldungen in Echtzeit analysiert und bei Bedarf mithilfe von prozessualen Eskalationsketten abgehandelt werden.

Tier Modell

Das Tier Modell beinhaltet qualifizierte Fachkräfte auf allen Ebenen. Sowohl erfahrene Security Analysten als auch unsere Senior Security Consultants sind Teil unseres Know-How Portfolio und schützen die Daten Ihres Unternehmens.

Shift-Left

Durch die definierten CSI-Maßnahmen werden stetige Verbesserungen des Services angestrebt. Die zusätzliche Lernfähigkeit unserer Security-Systeme entlastet darüber hinaus den gesamten Betrieb und resultiert in spürbaren Kostenersparnissen.

Gold
Microsoft Partner
Microsoft

We manage IT.

We manage IT.

ITERACON GmbH
David Schwalen
Talstraße 78, 52531 Übach-Palenberg
Tel.: +49 2451 9434040
david.schwalen@iteracon.de