Managed Detection and Response

für Microsoft Sentinel

Schützen Sie Ihr Unternehmen vor den neuesten Bedrohungen **so schnell, wie sie entstehen**

claranet cyber security®

Claranet Managed Detection and Response für Sentinel

Nutzen Sie das volle Potenzial von Microsoft Sentinel, um Bedrohungen innerhalb Ihrer Unternehmensgrenzen schnell zu erkennen und zu bekämpfen. Verkürzen Sie die Zeit für Einrichtung und Konfiguration, greifen Sie auf die neuesten Bedrohungsdaten zu und erstellen Sie eine zentrale Ansicht für Ihre Bedrohungserkennung und -reaktion. Unser Team aus CREST- und Microsoft-zertifizierten Threat Huntern und Cybersicherheitsanalysten verwaltet alles für Sie.

Ihr Security Information and Event Management (SIEM) kann nur so viel leisten wie die Menschen, Prozesse und Technologie, die für ein effizientes Funktionieren erforderlich sind. Unsere MDR-Lösung (Managed Detection and Response) für Microsoft Sentinel berücksichtigt alle diese Faktoren, um sicherzustellen, dass Ihr Unternehmen vor den neuesten Bedrohungen geschützt ist, **genauso schnell, wie sie entstehen.**

Schutz Ihres Unternehmens mit Cloud-Geschwindigkeit

Bauen Sie Ihre Erkennungsmöglichkeiten umfassend aus. Dank aktueller Bedrohungsdaten, benutzerdefinierter Analysen und Überwachung funktionieren die Eindämmung und das Bedrohungsmanagement rund um die Uhr. All diese Aufgaben werden von einem interdisziplinären Security Operations Center (SOC) verwaltet.

Optimierung von Kosten und Ressourcen

Steigern Sie Ihre Kosteneffizienz durch Auslagerung an unser Team aus dedizierten SOC-Spezialisten. Kommen Sie Alarmermüdung zuvor, vereinfachen Sie die Einrichtung, reduzieren Sie Störddaten sowie Speicherkosten und optimieren Sie die Kosten pro Alarm.

Sachkundige Investition in Sicherheit

Nutzen Sie Erkenntnisse aus detaillierten, von Experten durchgeführten Untersuchungen und der automatisierten Verfolgung des Benutzer- und Anwendungsverhaltens. Erkennen Sie, wo zusätzliche Abwehrmechanismen am meisten benötigt werden, um Ihre Cybersicherheitslage kontinuierlich zu verbessern.

Ein Service für echte Sicherheits-Herausforderungen

Eine wachsende Infrastruktur, veraltete und nicht verwaltete Systeme, Schatten-IT und Datenspeicher bilden eine Angriffsfläche, deren Größe und Komplexität Angreifern in die Hände spielt.

Die Angriffserkennung erfordert den Einsatz von Mitarbeitern, doch unternehmensinterne Kapazitäten sind teuer und erfordern Zeit und Arbeit, um effektiv zu werden.

Cloud Computing hat die Spielregeln des Cybersecurity-Lebenszyklus verändert. Die für die Erkennung verantwortlichen Teams müssen heute neben der Cloud-Steuerungsebene auch das Netzwerk und seine Endpunkte im Blick haben.

Angriffserkennung lässt sich nicht mit einem einzigen Tool bewältigen, sondern erfordert eine Plattform von Technologien, die ineinandergreifen und effektiv verwaltet werden müssen.

22 Durchschnittliche Anzahl der Sicherheitsverletzungen, von denen ein Unternehmen 2022 betroffen war [Accenture]

claranet cyber security®

Die Schlüssel-elemente

Unsere MDR-Lösung besteht aus 4 Schlüsselkomponenten, die Mitarbeitende, Prozesse und Technologie einbeziehen

Threat Intelligence (TI)

Unsere MDR-Lösung nutzt weltweit führende Bedrohungsdaten (Threat Intelligence), sodass neue Bedrohungen umgehend erkannt und abgewehrt werden können, bevor sie in Ihrem Unternehmen Schaden anrichten.

Rund-um-die-Uhr-Analyse

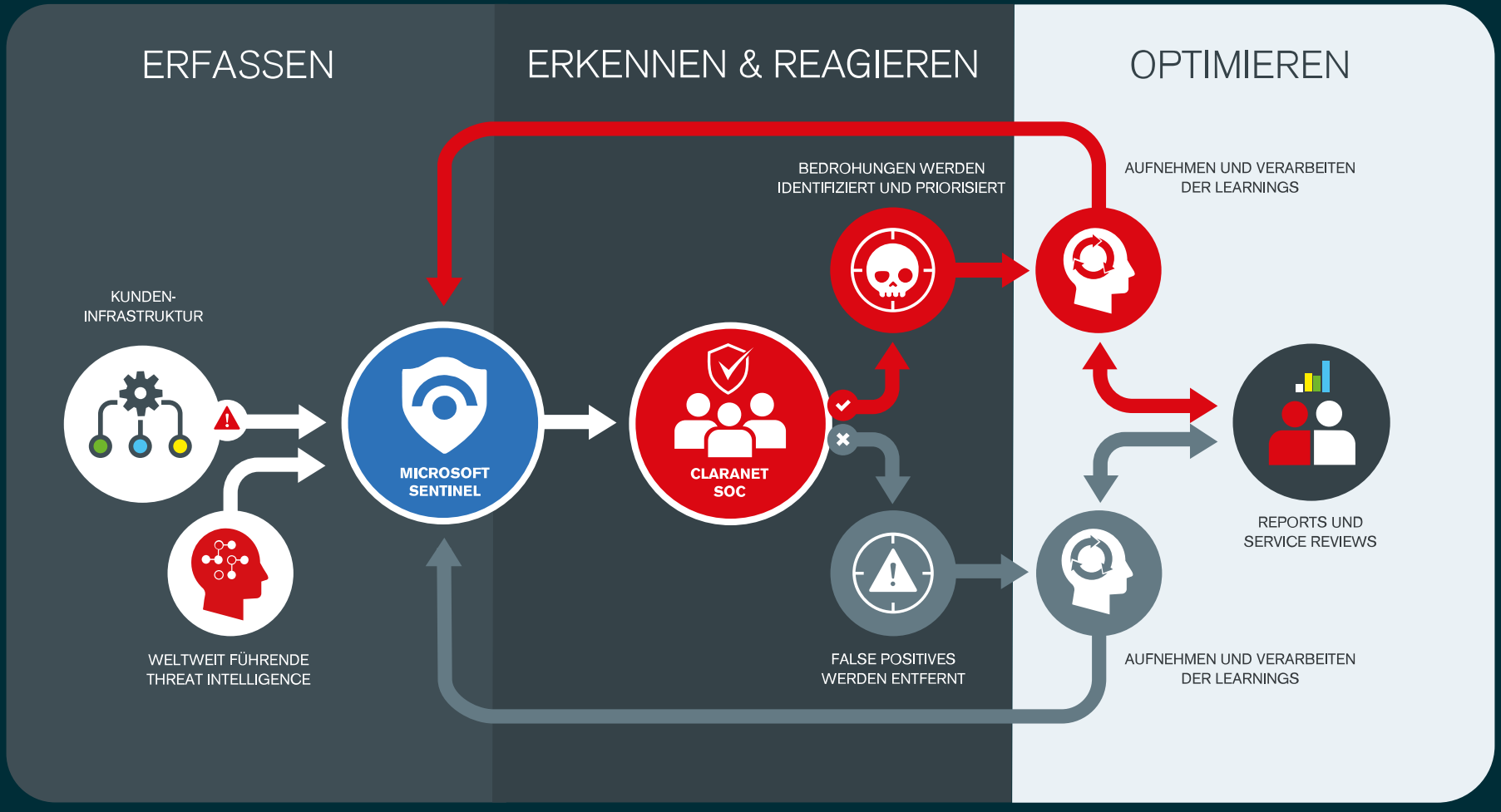
Unser globales SOC ist rund um die Uhr verfügbar und befasst sich mit der Überwachung und Analyse, um Bedrohungen zu erkennen und unschädlich zu machen sowie Ihnen und Ihrem Team umsetzbare Erkenntnisse zu liefern.

Kontinuierliche Optimierung

Software kann „out of the box“ nie sofort ihre volle Wirkung entfalten. Unser Team optimiert Ihr SIEM und entwickelt benutzerdefinierte Regel-sätze, die Fehlalarme verringern und die Erkennung an den relevanten Stellen priorisieren.

Proaktives Aufspüren

Wir ergänzen die Möglichkeiten der KI-gestützten Analyse durch aktives Aufspüren von Bedrohungen (Threat Hunting). So kommen wir komplexen Bedrohungen, die sonst unbemerkt bleiben, zuvor.


ERFASSEN
ERKENNEN & REAGIEREN
OPTIMIEREN
KUNDEN-
INFRASTRUKTUR
MICROSOFT
SENTINEL
CLARANET
SOC
BEDROHUNGEN WERDEN
IDENTIFIZIERT UND PRIORISIERT
AUFNEHMEN UND VERARBEITEN
DER LEARNINGS
REPORTS UND
SERVICE REVIEWS
WELTWEIT FÜHRENDE
THREAT INTELLIGENCE
FALSE POSITIVES
WERDEN ENTFERNT
AUFNEHMEN UND VERARBEITEN
DER LEARNINGS

Tiefgreifende Analyse-Services zur Bedrohungserkennung

Rund-um-die-Uhr-Erkennung und -Triage

Wir sind immer auf der Suche

Das SOC von Claranet verbindet die Automatisierung unseres Erkennungstechnologie-Stacks mit einem proaktiven, von Mitarbeitern durchgeführten Threat Hunting und der Triage von Alarmen. Dieser dreifache Ansatz bietet maximale Transparenz, damit Angreifer nicht unbemerkt ihr Unwesen treiben können. Zudem wird sichergestellt, dass Bedrohungen sorgfältig priorisiert werden, bevor sie an den Kunden weitergeleitet und von ihm zielgerichtet beantwortet werden.

- Kontinuierliche Logsammlung und Ereigniskorrelation
- Erfassung aller Logs aus sämtlichen Datenquellen, sowohl lokal als auch in der Cloud-Infrastruktur
- Malware-Analyse unter Berücksichtigung der aktuellen Belastungen
- Umfassende Triage, einschließlich Entfernen von Fehlalarmen und Priorisieren von Bedrohungen
- Direkte Eskalation von Sicherheitsereignissen mit hoher Priorität

Bedrohungsdaten und Analyse

Wir spüren Angreifer auf, bevor sie angreifen können

Wir erfassen kontinuierlich Bedrohungsdaten, um neue Bedrohungen und Angriffsaktivitäten identifizieren zu können, sobald sie beim Kunden auftauchen. Darüber hinaus verwenden wir Microsoft-Sicherheitstools, automatisierte und manuelle Datenanalysen und unser proaktives Threat Hunting, um Angriffe aufzudecken durch:

- Abhören von Hackerkanälen
- Absuchen des Dark Web nach bösartigen Aktivitäten
- Manuelle Analysen von Threat-Intelligence-Feeds
- Untersuchen Ihres Netzwerks auf komplexe, andauernde Bedrohungen (Advanced Persistent Threats, APT)
- Durchführen unternehmensinterner offensiver und defensiver Untersuchungen

Beschleunigen Sie Ihre Reaktion

MDR zur Eindämmung und Beseitigung

Eine effektive Angriffserkennung hilft dabei, die erste Reaktion auf einen Vorfall zu beschleunigen. Mit unserer MDR-Lösung für Microsoft Sentinel werden Vorfälle über unser Bedrohungs- und Incident-Management-Portal Claranet Online gemeldet, einschließlich Kontext bezüglich geschäftlicher Priorität und potenzieller Auswirkungen. Diese zentrale Verwaltungskonsole bietet Ihrem Team eine kontinuierliche Transparenz und Kontrollmöglichkeit für Ihre Azure-basierten Erkennungstools und eine ganzheitliche, umfassende Sicht auf Ihre Cybersicherheitsprogramme über verschiedene Services und Plattformen hinweg, damit Sie alle Aktivitäten optimieren können.

Dank des vollständigen Supports zur Eindämmung des Vorfalls wird sichergestellt, dass sich die Dauer der Sicherheitsverletzung von Monaten auf nur wenige Stunden verkürzt. Claranet Cyber Security antwortet Ihnen gemäß definierter SLAs mit einer kontextabhängigen Klassifizierung der Auswirkungen eines Vorfalls, sodass Sie sich auf kritische Probleme konzentrieren können.

Tickets umfassen detaillierte Informationen zu:

- Quelle, Ort und Schwere des Vorfalls
- Empfohlene Maßnahmen zur Eindämmung
- Empfohlene Maßnahmen zur zukünftigen Vermeidung

claranet cyber security®

Die Wirkung unseres Ansatzes

Zentrale Korrelationsregeln
Unsere Korrelationsregeln sind so konzipiert, dass Microsoft Sentinel echte bösartige Aktivitäten ohne Verzögerung erkennen kann. Sie werden unter Berücksichtigung der schwersten Bedrohungen kontinuierlich optimiert.

Intelligente Workbooks
Unsere benutzerdefinierten Workbooks analysieren Daten dynamisch, sodass sie zur Erstellung detaillierter, visueller Berichte genutzt werden können. Sie zeigen, wie Sie Kennzahlen wie Analyseeffizienz und Cybersecurity Maturity Model Certification (CMMC) messen.

Certifiziertes 24/7/365 SOC
Unser globales SOC besteht aus CREST- und SC-200-zertifizierten Analysten und Threat Huntern mit umfassenden Erfahrungen. Sie arbeiten mit bewährten Methoden, die eine schnelle Erkennung sicherstellen.

Threat Intelligence
Claranet hat Zugriff auf führende Bedrohungsdaten, die von Microsoft Sentinel erfasst werden, um anhand aktueller Verhaltensweisen und Praktiken von Angreifern authentische Indikatoren für eine Kompromittierung (Indicators of Compromise, IoCs) und Alarme identifizieren zu können.

Das Angebot von Claranet

Security Orchestration, Automation and Response (SOAR)
Integrieren Sie Microsoft Sentinel über eine Reihe von Playbooks und Konnektoren für Security Orchestration, Automation and Response (SOAR) in Ihre IR (Incident Response)-Services.

Cloud Practice
Ganz gleich, ob Sie bereits eine Cloud-Strategie haben oder sich erst am Anfang Ihrer Reise befinden – nutzen Sie das Know-how unserer dedizierten Cloud Practice. Dieses Team ist in allen Bereichen der Cloud tätig, von Betrieb und Optimierung bis zu Migration und Governance.

Claranet Online
Unser zentrales Portal bietet Ihnen und Ihrem Team eine kontinuierliche Transparenz und Kontrollmöglichkeit für Ihre Azure-basierten Erkennungstools. Gleichzeitig erhalten Sie eine ganzheitliche Sicht auf Ihre Cybersicherheitsprogramme über verschiedene Services und Plattformen hinweg.

Aufspüren von Bedrohungen
Durch proaktives Aufspüren von Bedrohungen kann das SOC-Team von Claranet komplexe Angriffe und potenzielle Advanced Persistent Threats (APT) über die gesamte Cyber Kill Chain hinweg erkennen und so verhindern, dass Angreifer unbemerkt operieren können.

Erste Schritte

Einrichtung des Service

Zusammen mit Ihnen wählen wir abhängig von Ihren Ressourcen und Kapazitäten den für Ihr Unternehmen und Ihr Team geeigneten Service aus.

Vollständig gemanagtes Setup

Bereitstellung und Einrichtung von optimierter Software, in der Regel innerhalb von Tagen oder Wochen.

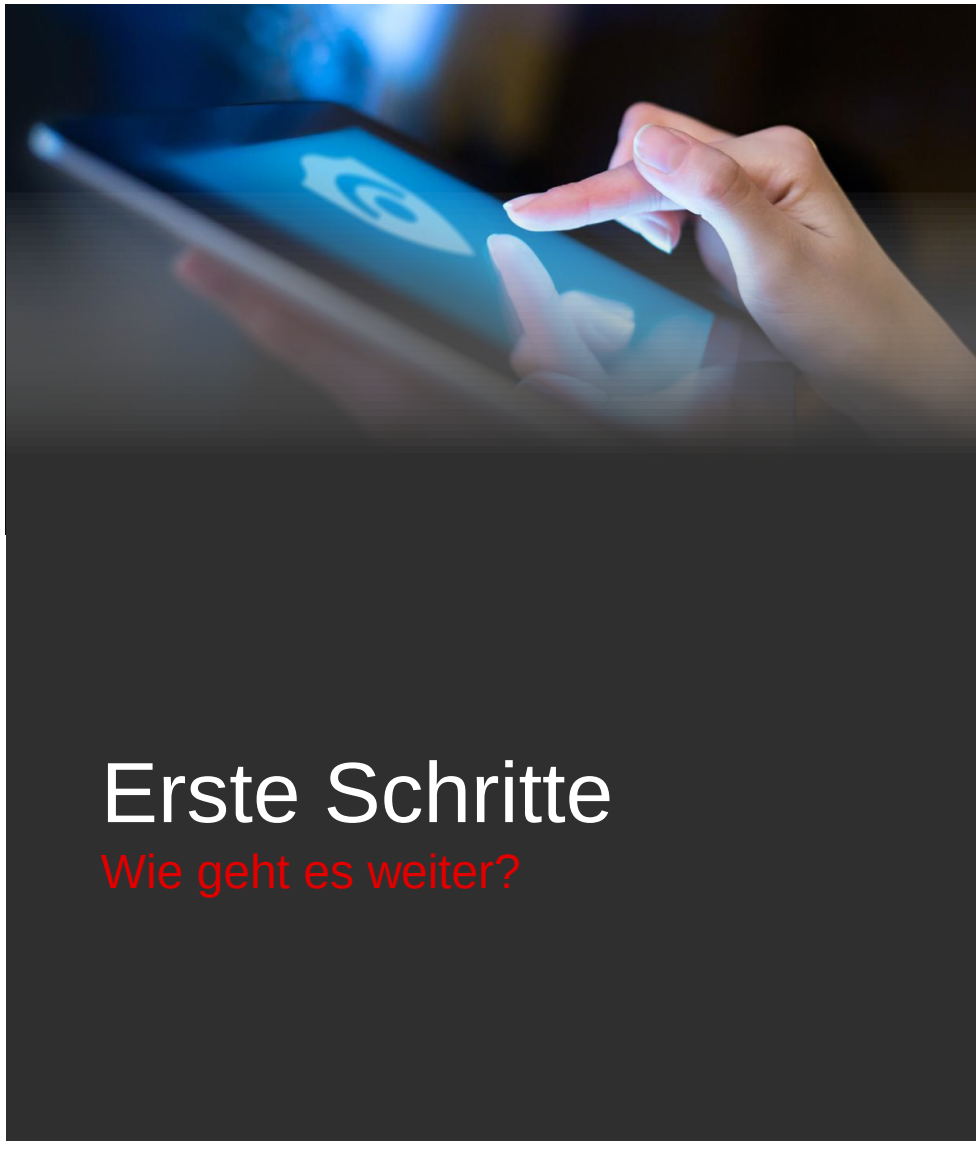
Claranet Online

Vollständige Kontrolle für Sie und Ihr Team innerhalb Ihres Bedrohungsmanagement- und -Meldeportals* ab dem ersten Tag.

Reports und Service Reviews

Monatliche Berichterstattung und vierteljährliche Service Reviews (Videocalls).

**Claranet ist ISO 27001-konform bei Datenspeicherung und Berichtsfunktion*



Claranet Cyber Security

Claranet Cyber Security ist in der Claranet Gruppe die Dienstleistungssparte für Cybersicherheit. Claranet hat einen jährlichen Umsatz von über 600 Mio. Euro, über 10.000 Geschäftskunden und mehr als 3.000 Beschäftigte weltweit.

Das technische Cybersicherheitsteam umfasst 1.500 Fachexperten und 75 Penetrationstester mit mehr als 25 Jahren Erfahrung, einschließlich FTSE 250- und Fortune 500-Unternehmen weltweit.

Claranet Cyber Security wurde von ISG in ihrer Studie Provider Lens™ in den Bereichen „Cybersecurity – Solutions & Services“ und „Public Cloud – Solutions and Services“ als Leader ausgezeichnet.

Claranet ist einer der wenigen MSPs, die den höchsten Akkreditierungsstatus als Partner von Microsoft, AWS und Google erreicht hat. Das Unternehmen wurde im Gartner Magic Quadrant als Leader und als Marktführer im Bereich Cybersicherheit ausgezeichnet.

Unser Serviceportfolio umfasst Managed Detection and Response (MDR), Endpoint Detection and Response (EDR), Penetrationstests, Continuous Security Testing und Cybersecurity-Trainings.

Wir sind einer der weltweit führenden Schulungsanbieter bei Black Hat und haben Schulungspartnerschaften mit Check Point, Nano, Rapid7und QA.

Gold Microsoft Partner | Azure Expert MSP

aws PARTNER Premier Tier Services
- Advanced Tier Training
- Managed Service Provider
- Migration Services Competency

ISO 9001 | ISO 22301 | ISO 27001 | ISO 27017

CYBER ESSENTIALS PLUS | CREST | Qualys

Wir freuen uns auf Ihre Kontaktaufnahme

de-info@claranet.com
+49 (0)69 40 80 18 450
Claranet GmbH – Hanauer Landstraße 196 – 60314 Frankfurt

www.claranet.com/de


claranet
cyber
security®