DATAGROUP

CYBER SECURITY

SERVICES

Grußwort

Sehr geehrte Damen und Herren,

in einer Zeit, in der die digitale Welt immer komplexer und die Bedrohungen durch Cyberkriminalität immer raffinierter werden, ist es unser oberstes Ziel, Ihnen den bestmöglichen Schutz und die nötige Sicherheit zu bieten.

Unsere langjährige Erfahrung und unser tiefgehendes Fachwissen im Bereich Cyber Security ermöglichen es uns, maßgeschneiderte Lösungen zu entwickeln, die Ihre individuellen Bedürfnisse erfüllen. Wir sind stolz darauf, Ihnen nicht nur modernste Technologien, sondern auch ein engagiertes Team von Experten zur Seite stellen zu können.

Gemeinsam mit Ihnen möchten wir die Herausforderungen der digitalen Sicherheit meistern und eine sichere Zukunft gestalten. Lassen Sie uns zusammenarbeiten, um Ihre Daten und Systeme vor den Gefahren der Cyberwelt zu schützen.

Mit freundlichen Grüßen,

Die Geschäftsführung der DATAGROUP im Bereich Cyber Security

Dino Huber, Joachim Rath und Marc Sundermann

Fragen rund um unsere Cyber Security-Services beantworten wir Ihnen auch gerne persönlich.

Kontaktieren Sie uns: cybersecurity@datagroup.de

Inhalt:

datagroup.de/leistungen/it-outsourcing/security-services/

Ihr Partner für IT-Sicherheit

Cyber-Security-Leistungsversprechen

Steigende Bedrohung durch Cyberkriminalität: In den letzten Jahren hat die Gefahr durch hochqualifizierte Cyberkriminelle stark zugenommen. Viele Unternehmen verfügen nicht über die nötige Erfahrung, um sich gegen diese ausgeklügelten Angriffe zu schützen. Mit unserer umfangreichen Erfahrung im Bereich Cyber- und IT-Sicherheit bieten wir Ihnen zuverlässige Lösungen, um Ihr Unternehmen zu schützen.

1. Ein starkes Team für Ihren Erfolg
Unser Team von rund 250 engagierten Mitarbeiterinnen und Mitarbeitern ist jederzeit für unsere Kunden erreichbar. Wir verfügen über eine breite Palette an Qualifikationen und Fachkenntnissen, die von technischer Unterstützung über Kundenservice bis hin zur spezialisierten Fachberatung reichen. Unsere Dienstleistungen erbringen wir zuverlässig aus Deutschland.

2. Strenge Prüfung unserer Tools
Unsere eingesetzten Tools unterliegen strengen Testverfahren. Wir arbeiten ausschließlich mit führenden Anbietern zusammen, um sicherzustellen, dass unsere Kunden den bestmöglichen Managed Service erhalten. Unsere Dienstleistungen erfüllen dabei stets höchste Qualitätsstandards und sind auf dem neuesten Stand der Technik.

3. Proaktive Sicherheitsstrategien
Als Full-Service-Anbieter reduzieren wir das Risiko für unsere Kunden durch umfassende Sicherheitsmaßnahmen. Mit unseren proaktiven Strategien erkennen und neutralisieren wir Bedrohungen frühzeitig. Sollte es zu einem Angriff kommen, reagiert unser engagiertes Team sofort, um die Auswirkungen zu minimieren und Ihre Geschäftsprozesse aufrechtzuerhalten.

4. Kundenzufriedenheit und Partnerschaft auf Augenhöhe
Unser hoher Qualitätsanspruch wird durch regelmäßige Kundenzufriedenheitsumfragen überprüft. Durch den kontinuierlichen Austausch mit unseren Kunden und unsere engagierten Service Manager stellen wir sicher, dass die Partnerschaft auf Augenhöhe bleibt und unsere Kunden stets optimal betreut werden.

Aktuelle Cybersicherheitslage

BSI Lagebericht 2023 - Zusammenfassung:

Die aktuelle Bedrohungslage im Bereich der Cyber Security ist angespannt bis kritisch. Eine der größten Gefahren stellt Ransomware dar, die zunehmend von einer gut organisierten Schattenwirtschaft mit spezialisierter Arbeitsteilung eingesetzt wird. Diese Angreifer zielen dabei oft auf kleinere Unternehmen und Behörden ab, da diese ein günstiges Kosten-Nutzen-Verhältnis bieten.

Neben Ransomware sind auch DDoS-Angriffe durch Hacktivisten und Advanced Persistent Threats (APT) mit dem Ziel der Informationsbeschaffung und Cyberspionage weit verbreitet. Täglich werden etwa 70 neue Schwachstellen entdeckt, von denen rund 15% als kritisch eingestuft werden.

In diesem herausfordernden Umfeld ist es unerlässlich, umfassende Sicherheitsmaßnahmen zu ergreifen und kontinuierlich zu verbessern, um den vielfältigen Bedrohungen wirksam begegnen zu können.

über 200 Milliarden Euro Schaden entstanden 2023 durch Cyberkriminalität

66% aller Spam Mails sind Cyberangriffe: 34 % Erpressungsmails & 32% Betrugsmails

DATAGROUP wurde 2024 mit dem Leader-Status in der ISG-Provider Lens Studie „Cybersecurity – Solutions and Services“ im Bereich Managed Security Services (SOC) für den Mittelstand ausgezeichnet.

Juli 2024, Pliezhausen

SOC

Unser Security Operations Center lässt Sie nicht im Regen stehen

SOC as a Service (SOCaaS)

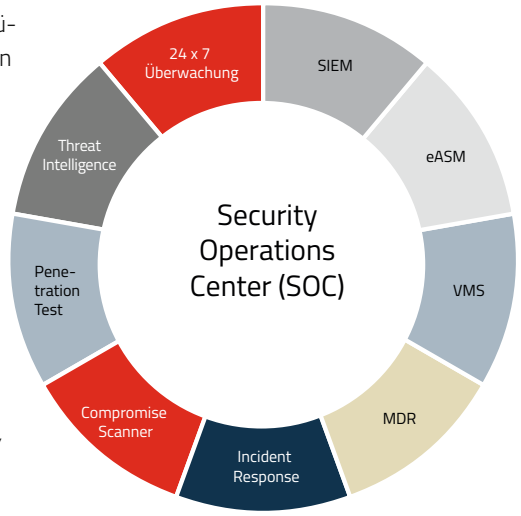
Ein Security Operations Center (SOC) fungiert als zentrale Anlaufstelle für Cybersecurity in Unternehmen und Organisationen und hat die Aufgabe, deren IT-Sicherheit zu gewährleisten. Das Hauptziel eines SOC besteht darin, die IT-Infrastruktur der Organisation vor Cyberangriffen zu schützen. Diese Arbeit lässt sich grob in drei Bereiche unterteilen:

Monitoring und Bedrohungsanalyse
Unser SOC überwacht eine Vielzahl von Sicherheitswarnungen, einschließlich Meldungen von Sicherheitstools über potenzielle Bedrohungen sowie Informationen von Mitarbeitern, Partnern und externen Quellen. Viele moderne SOCs nutzen ein SIEM-System (Security Information and Event Management) zur zentralen Sammlung und Verwaltung dieser Alerts.

Analyse und Verifizierung
Die gemeldeten Bedrohungen oder Vorfälle werden von den SOC-Spezialisten untersucht, um sicherzustellen, dass es sich nicht um Fehlalarme handelt, also gemeldete Bedrohungen, die tatsächlich harmlos sind.

Abwehrmechanismus
Wenn ein Sicherheitsvorfall validiert wird und eine Reaktion erforderlich ist, übergibt das SOC den Fall an die entsprechenden Personen oder Teams, um Gegenmaßnahmen zu ergreifen.

Der Betrieb eines SOC erfordert eine ausgeklügelte Kombination aus Fachwissen, Prozessen und Technologie.



Die Grafik zeigt das SOC im Zentrum, umgeben von Schlüsselkomponenten wie SIEM, eASM, 24x7-Überwachung und Kompromiss-Scannern, die eine ganzheitliche Cyberabwehr bilden.

SOC
Unsere Security Analysten - Ihre Schirmhalter

Aufgaben eines Security Operations Centers

- Planung von Vorsorgemaßnahmen
- Erkennung und Management von Schwachstellen (Vulnerability Management)
- Vordefinierte Handlungsanweisungen zur schnellen und
- effizienten Reaktion auf typische Sicherheitsvorfälle (Playbooks)
- Forensische Analyse von Vorfällen

DATAGROUP SOC Hauptmerkmale

- 24/7 Überwachung
- Expertise und Erfahrung (Qualifikationen, Zertifizierungen und relevantes Know-How)
- schnelle Reaktionszeit (Anwendung von SOAR)
- IT-Sicherheit aus einer Hand

In unserem Security Operations Center (SOC) arbeiten hochqualifizierte Security Analysten, die in drei Tiers unterteilt sind, um unterschiedlichste Bedrohungen effizient zu identifizieren und zu bekämpfen.

TIER 1 – Erste Anlaufstelle:
Unsere TIER 1 Analysten überwachen kontinuierlich Sicherheitsalarme und sind der erste Kontaktpunkt. Sie analysieren grundlegende Vorfälle und leiten diese bei Bedarf an höhere Tiers weiter. Ihre Aufgabe ist es, Bedrohungen frühzeitig zu erkennen und erste Maßnahmen einzuleiten.

TIER 2 – Tiefgehende Analyse:
TIER 2 Analysten verfügen über fortgeschrittene Fachkenntnisse und untersuchen Vorfälle im Detail. Sie führen digitale Forensik durch und analysieren die Angriffswege, um die Methoden der Angreifer zu verstehen und maßgeschneiderte Lösungen zu entwickeln.

TIER 3 – Strategische Sicherheit:
TIER 3 Experten bearbeiten hochkomplexe Bedrohungen und entwickeln langfristige Sicherheitsstrategien. Sie optimieren kontinuierlich die Sicherheitsinfrastruktur und sorgen dafür, dass das Unternehmen auch gegen gezielte Angriffe geschützt ist.

SIEM
Security Information & Event Management

Managed SIEM - das zentrale Alarmierungssystem

Ein SIEM (Security Information and Event Management) ist ein Security-Management-System, das volle Sichtbarkeit und Transparenz zu mitprotokollierten Aktivitäten innerhalb des Netzwerks bietet – dies versetzt uns und den Kunden in die Lage, basierend auf vordefinierten Use Cases in Echtzeit auf Bedrohungen zu reagieren.

UNSERE LEISTUNGEN

- Betrieb der SIEM-Umgebung
- Erstellen, Pflege und Schärfung neuer Use Cases
- Unterstützung in der Anbindung an Kundensysteme
- Einbindung des MITRE ATT&CK Frameworks möglich
- Aktive Ticketsteuerung, Nachhalten der Incidents 24/7 in Business Critical

IHRE VORTEILE

- Ganzheitliche Betrachtung der IT-Sicherheit und der angebundenen Systeme
- Planbare Kosten
- Einfache Skalierbarkeit durch Anpassung an die IT-Umgebung
- Erfahrungen aus allen Branchen fließen in Bewertungen und Services ein
- Automatisierte Erkennung bei definierten Vorfällen
- Grundlage für die Erkennung und Nachbearbeitung von nicht definierten Vorfällen

SOAR

Security Orchestration Automation & Responses

DATAGROUP SOAR-Services

SOAR optimiert Sicherheitsoperationen durch die Integration und Automatisierung von Tools und Prozessen. Es ermöglicht eine schnellere Identifikation, Analyse und Reaktion auf Vorfälle, indem es manuelle Aufgaben automatisiert und die Zusammenarbeit im SOC verbessert.

Wir empfehlen unsere SOAR-Technoloige für Unternehmen, die ihre Sicherheitsoperationen durch Automatisierung und Orchestrierung verbessern möchten, um schneller auf Vorfälle zu reagieren und Reaktionszeiten zu verkürzen.

Hauptfunktionen

- Sicherheitsautomatisierung: Automatisierung wiederkehrender Aufgaben und Reaktionen.
- Orchestrierung: Integration und Koordination von Sicherheits-Tools.
- Incident Response: Schnelle Reaktion auf Vorfälle mit Playbooks.
- Monitoring und Reporting: Echtzeit-Überwachung und Berichterstattung.

Vorteile

- Effizienzsteigerung: Weniger manuelle Eingriffe und schnellere Incident Response.
- Konsistente Reaktionen: Standardisierte Vorfallreaktionen.
- Verbesserte Zusammenarbeit: Nahtlose Integration im SOC.
- Kostenersparnis: Reduzierung manueller Aufgaben und Entlastung des Sicherheitsteams.

VMS

Schwachstellenmanagement

DATAGROUP Schwachstellenmanagement

Was ist Schwachstellenmanagement?
Der Prozess zur Identifizierung, Bewertung, Priorisierung und Behebung von Sicherheitslücken in IT-Systemen, um potenzielle Angriffspunkte zu minimieren und die Systemsicherheit zu gewährleisten.

Warum ist Schwachstellenmanagement wichtig?
- Schnellere Sichtbarkeit der Sicherheitslücken
- Priorisierte Abarbeitung von kritischen Sicherheitslücken

DATAGROUP´s Schwachstellenmanagement
- regelmäßige Schwachstellenscans.
- Automatisierte Erkennung und Bewertung.
- Priorisierung und schnelle Behebung kritischer Schwachstellen.
- Kontinuierliche Überwachung und Nachverfolgung.

VORGEHEN
- Erkennung: Automatisierte Scans identifizieren Schwachstellen.
- Bewertung: Analyse der Risiken und Auswirkungen.
- Priorisierung: Lücken werden nach Dringlichkeit priorisiert.
- Behebung: Patches und andere Maßnahmen werden umgehend umgesetzt.

SECURITY ADVISORY PROZESS
- Sicherheitshinweise werden im Security Operations Center gesichtet und nach dem Common Vulnerability Scoring System (CVSS) und dem Vulnerability Priority Rating (VPR) bewertet.
- Ableitung gezielter Maßnahmen bei kritischen Vorfällen.

HAUPTFUNKTIONEN
- Regelmäßige Scans.
- Risikobewertung und Priorisierung.
- Berichterstattung und Handlungsempfehlungen.
- Kontinuierliche Überwachung und Nachverfolgung.

VORTEILE
- Reduziertes Sicherheitsrisiko durch frühzeitige Erkennung.
- Zugang zu Expertenwissen.
- Unterstützung bei der Einhaltung von Sicherheitsstandards.

eASM
external Attack Surface Management

Ein external Attack Surface Management (eASM) beschreibt den fortlaufenden Prozess zur Identifikation, Überwachung, Bewertung, Priorisierung und Beseitigung von Bedrohungen auf die externe Angriffsfläche eines Unternehmens.

Die externe Angriffsfläche umfasst sämtliche internetverbundenen Assets eines Unternehmens, wie z.B. Domänennamen, SSL-Zertifikate, Betriebssysteme, Server, IoT-Geräte und Netzwerkdienste. Diese Assets sind über lokale Infrastrukturen, Cloud-Umgebungen und Drittanbieter verteilt und stellen potenzielle Einfallstore für Cyberangriffe dar.

HAUPTFUNKTIONEN

- Erkennung und Inventarisierung aller öffentlich zugänglichen IT-Assets
- Bewertung der Sicherheitslage externer Systeme und Anwendungen
- Risikobasierte Priorisierung von Schwachstellen und Bedrohungen
- Regelmäßige Berichterstattung über Sicherheitslücken und Empfehlungen zur Absicherung

IHRE VORTEILE

- Reduzierte Angriffsfläche: Minimierung der Risiken durch proaktive Identifikation und Behebung von Schwachstellen
- Ständige Überwachung: Kontinuierliche Anpassung an neue Bedrohungen und Änderungen in der IT-Infrastruktur
- Compliance-Unterstützung: Sicherstellung der Einhaltung von Sicherheitsanforderungen und Standards

Sicherheitslösungen

EDR, NDR und MDR

Erkennungs- und Reaktionsansätze im Vergleich,um den individuellen Anforderungen unserer Kunden gerecht zu werden

EDR-Lösungen (Endpoint Detection and Response) ergänzen klassische Virenscanner, indem sie verdächtige Aktivitäten über alle Endpunkte des digitalen Perimeters hinweg erkennen und untersuchen. Dabei werden Endpunktereignisse kontinuierlich auf ihr Verhalten und Anomalien überwacht.

NDR (Network Detection and Response) ist auf die Erkennung und Reaktion von Bedrohungen im Netzwerkverkehr fokussiert. NDR-Lösungen überwachen das Netzwerk kontinuierlich, um Veränderungen und auffällige Aktivitäten zu identifizieren und darauf zu reagieren.

MDR (Managed Endpoint Detection and Response) ist ein vollständig verwalteter Service zur Überwachung, Erkennung und Reaktion auf Bedrohungen auf Endgeräten. Managed EDR bietet umfassenden Schutz durch kontinuierliche Analyse und Echtzeit-Reaktion auf sicherheitsrelevante Ereignisse auf allen Endpoints.

IHRE VORTEILE MIT DATAGROUP

- **Ganzheitlicher Schutz:** Kombinierte Lösungen bieten umfassenden Schutz für Endpunkte, Netzwerke und das gesamte Unternehmen.
- **Zentralisierte Verwaltung**: Eine einheitliche Plattform ermöglicht eine zentrale Verwaltung und Überwachung aller Sicherheitsaspekte.
- **Schnellere Reaktionszeiten:** Koordinierte Erkennung und Reaktion auf Bedrohungen ermöglichen eine schnellere und effektivere Schadensbegrenzung.
- **Kosteneffizienz:** Eine einheitliche Lösung kann kostengünstiger sein als der Einsatz mehrerer separater Systeme.
- **Skalierbarkeit:** Integrierte Lösungen lassen sich leichter an die wachsenden Anforderungen eines Unternehmens anpassen.
- **Erhöhte Automatisierung:** Automatisierte Prozesse reduzieren den manuellen Aufwand und minimieren menschliche Fehler.
- **Konsistente Sicherheitsrichtlinien:** Einheitliche Richtlinien und Standards können einfacher durchgesetzt und überwacht werden.

Sicherheits-lösung XDR

Extended Detection and Response - XDR

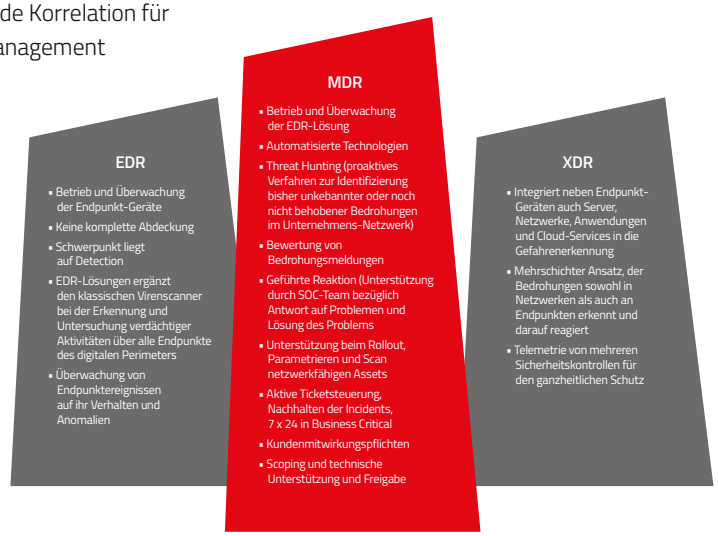
XDR vereinheitlicht Sicherheitsoperationen über alle Ebenen hinweg, einschließlich Benutzer, Endpunkte, E-Mail, Anwendungen, Netzwerke, Cloud-Workloads und Daten.
Durch den Einsatz von Künstlicher Intelligenz (KI) und Automatisierung bietet XDR eine umfassende und effiziente Methode, um sich gegen komplexe Cyberangriffe zu schützen und darauf zu reagieren. Es sammelt und korreliert Daten aus verschiedenen Quellen, um Bedrohungsmuster automatisch zu erkennen und priorisiert die erkannten Bedrohungen nach ihrem Schweregrad.

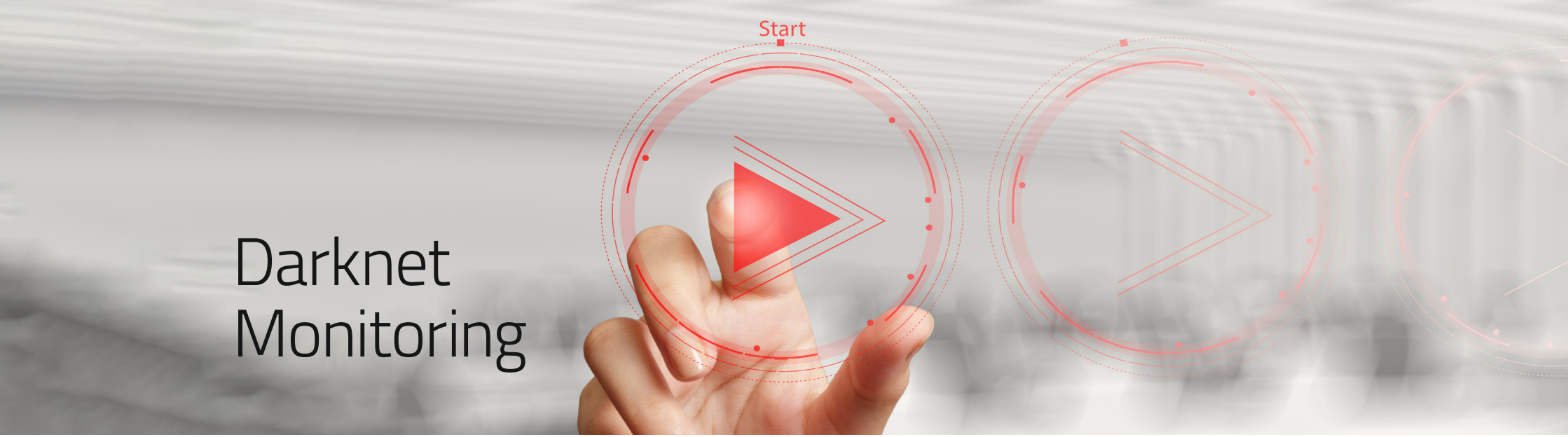
HIGHLIGHTS

- Einheitliche Sichtbarkeit
- Proaktives Threat Hunting
- Integrierte Threat Intelligence
- Automatische Bedrohungserkennung und -Reaktion
- Automatisierte Untersuchung von Vorfällen und Forensik
- Umfassende Integration von Drittanbietern

HAUPTMERKMALE

- Umfassende Informationen über Bedrohungen
- Fortgeschrittene Datenanalyse und maschinelles Lernen
- Benutzerdefinierte Dashboards, Complince und Berichterstattung
- Benutzerdefinierte Playbooks und Automatisierung
- Domain-übergreifende Korrelation für effektives Threat Management





Darknet Monitoring

Managed Darknet Monitoring ist das Schlüsselwort unserer Zusammenarbeit mit Secutec.

Die Darknet Monitoring Plattform gibt Unternehmen jederzeit einen kompletten Überblick der externen Cyber-Risiken.

Die Managed Darknet Monitoring-Plattform (**secureSIGHT**) liefert Ihrem Unternehmen Informationen zu Sicherheitslücken, gestohlenen Daten, Passwörtern, Keyloggern und Keywords, bevor Hacker dies gegen das Unternehmen einsetzen und somit Zugang zu relevanten Systemen erhalten können.

24/7 wird auf der Threat Intelligence Plattform das Darknet auf beispielsweise Chats, Foren, Marktplätzen oder Darknet-Webseiten überwacht und alarmiert aktiv bei auftretenden Cyber-Risiken.

Das Tool **secureDNS** innerhalb der Managed Darknet Monitoring Plattform verfügt über folgende Services:

- Verteilung über 16 weltweite Rechenzentren
- Blockieren bedrohlicher, neuer Domains innerhalb der ersten 24 Stunden
- Aktives Warnen bei Bedrohungen aus dem Darknet
- 24/7 Überwachung des DNS- und IP-Datenverkehrs

Informationen über unseren Partner Secutec

- Secutec wurde 2005 mit der Vision gegründet, weltweites Wissen über Bedrohungen in einer Technologie zu bündeln
- Das Unternehmen hat Erfahrung aus über 500 Attacken und 300 Verhandlungen mit professionellen Hacker-Organisationen
- Secutec ist führender europäischer Cybercrime Negotiator

CTEM
Continous Threat Exposure Management

Wir ermöglichen Ihnen Hybrid-Cloud-Sicherheitslösungen.

Eine schnelle Schwachstellenidentifizierung und Risikobehebung wird durch eine entwickelte Angriffsmodellierung mithilfe des Digital Twin-Konzepts ermöglicht.

Das **Attack Path Management** zeigt die Schwachstellen aus der Angreifer-Perspektive sowie die möglichen Eintrittstore auf und bietet Komplettlösungen zur Risikominimierung.
Attack Simulation führt eine vollständig sichere Simulation basierend auf tatsächlichen Benutzeraktionen in Echtzeit durch. Dies beinhaltet maßgeschneiderte Angriffsszenarien von einem beliebigen Ausgangspunkt (BreachPoint) zu einem beliebigen Zielobjekt (Critical Asset).
Innerhalb des **Attack-based Vulnerability Managements** werden durch einen Schwachstellenscan die gefundenen Schwachstellen priorisiert und verwaltet.

Security Posture Visibility unterstützt Ihr Unternehmen beim Risikomanagement, Ressourcenmanagement und Erfüllung der Anforderungen (Compliance Support).
Das **Cloud Security Posture Management** gewährleistet einen sicheren Umgang von externen Tools wie AWS, Office 365 und vielen weiteren Plattformen.

IHRE VORTEILE

- **NO BLIND SPOTS:** Erhalten Sie einen individuellen, umfassenden Überblick aller kritischen Eintrittswege für Hacker über Ihr gesamtes Hybridnetzwerk.
- **NO GUESSWORK:** Verwenden Sie Analysen und Modelle, um die Schwachstellen zu identifizieren. Definieren Sie im Anschluss die Stelle zur Unterbrechung der Eintrittswege.
- **NO STOPPING:** Führen Sie eine automatisierte, kontinuierliche Risikoreduzierung durch (sicher, skalierbar und unabhängig von der dynamischen Umgebung).

Penetration Testing

Penetration Testing als gezielter Versuch, die Schwachstellen in IT-Systemen aufzudecken und auszunutzen

Unser Penetration Testing Service bietet eine umfassende Sicherheitsprüfung, um die Widerstandsfähigkeit Ihrer IT-Infrastruktur gegenüber potenziellen Angriffen zu gewährleisten. Durch gezielte Simulation von Angriffsszenarien identifizieren wir Schwachstellen und ermöglichen es Ihnen, proaktiv Sicherheitsmaßnahmen zu ergreifen.

IHRE VORTEILE

- Früherkennung von Schwachstellen: Durch die frühzeitige Erkennung können Unternehmen proaktiv Maßnahmen ergreifen, um Ihre Systeme zu schützen
- Simulation realer Angriffsszenarien: Diese Simulationen helfen dabei, die Reaktion und Widerstandsfähigkeit der IT-Infrastruktur unter Bedingungen nachzuvollziehen, die in der Realität auftreten können
- Bewertung der Netzwerksicherheit: Durch interne und externe Penetrationstests können Schwachstellen in Netzwerken, Servern und Endpunkten identifiziert werden
- Webanwendungsprüfungen: Penetration Tests für Webanwendungen decken Sicherheitslücken in Online-Plattformen auf, um Datenverluste, unauthorisierten Zugriff und andere Angriffsszenarien zu verhindern.

DER DATAGROUP PENETRATION-PROZESS:

Incident Response

Incident Response - professionelle Hilfe im Cyber-Notfall

Ein Incident Response Retainer ist ein vertraglich vereinbarter Service, der Unternehmen schnellen Zugang zu einem spezialisierten Incident Response Team bietet. Im Falle eines Cyberangriffs oder eines Sicherheitsvorfalls können Unternehmen sofort auf die Expertise und Ressourcen des IR-Teams zurückgreifen, um den Vorfall effizient zu bewältigen.

HAUPTFUNKTIONEN

- Vorrangiger Zugang zu einem Incident Response Team im Notfall
- Vorab definierte SLAs für Reaktionszeiten und Support
- Unterstützung bei der Wiederherstellung und Behebung nach einem Vorfall

IHRE VORTEILE

- Schnelle Reaktionszeit: Sofortige Unterstützung im Ernstfall, um Schäden zu begrenzen
- Fachkundige Unterstützung: Zugang zu erfahrenen Incident Response-Experten
- Kostenkontrolle: Planbare Kosten für Incident Response Services
- Verbesserte Vorfallsbereitschaft: Vorbereitung und proaktive Maßnahmen zur Risikominderung

DATAGROUP als Mitglied des Deutschen Incident Response Teams (DIRT)

DIRT verfügt über deutschlandweite Incident-Response-Teams, die für den schnellen Einsatz vor Ort bereitstehen. Diese Teams werden von über 50 BSI-Vorfallexperten unterstützt. Zusätzlich gibt es regionale mobile Notfall-Rechenzentren, die bei Bedarf eingesetzt werden können. Ein Netzwerk von Krisenmanagern und IT-Forensikern steht ebenfalls zur Verfügung, um in Krisensituationen zu unterstützen. Insgesamt sind 4.500 IT-Spezialisten in allen Bereichen tätig, um eine schnelle Wiederherstellung der IT-Systeme zu gewährleisten.

OT- / IoT-Sicherheit

Warum OT-Sicherheit so wichtig ist!

Operational Technology (OT) steuert und überwacht physische Prozesse in vielen Industrien. Angriffe auf OT-Systeme können nicht nur finanzielle Verluste, sondern auch physische Gefahren verursachen. Ein erfolgreicher Angriff kann Produktionsausfälle, Umweltschäden und lebensbedrohliche Situationen zur Folge haben.

Einsatzbereiche von OT
OT wird in der industriellen Fertigung, Energieversorgung, Wasser- und Abwassermanagement, im Transportwesen und im Gesundheitswesen eingesetzt. Diese Systeme steuern Roboter, überwachen Energieverteilungsnetze und gewährleisten den Betrieb medizinischer Geräte. Ihre Verbindung zu IT-Netzwerken erhöht die Anfälligkeit für Cyber-Angriffe.

Bedrohungen und Herausforderungen
Die Bedrohungen für OT-Systeme haben zugenommen, besonders durch staatlich unterstützte Hackergruppen. Diese Angriffe zielen oft auf kritische Infrastrukturen ab. Viele OT-Systeme sind veraltet und nicht für die heutige Bedrohungslandschaft ausgelegt, was sie besonders anfällig macht.

Maßnahmen zur Absicherung von OT
Unternehmen müssen eine umfassende Sicherheitsstrategie entwickeln. Dazu gehören regelmäßige Updates und Patches, Netzwerksegmentierung, Überwachung von OT-Netzwerken und Schulungen für Mitarbeiter, um das Bewusstsein für Sicherheitsrisiken zu erhöhen.

Zukunft der OT-Sicherheit
Technologien wie Künstliche Intelligenz (KI) und Machine Learning können helfen, Anomalien frühzeitig zu erkennen. Die Zusammenarbeit zwischen IT- und OT-Sicherheitsteams wird immer wichtiger, um eine ganzheitliche Sicherheitsstrategie zu gewährleisten.

- Beratung und Konzepte zu Absicherung von OT Systemen
- als MSSP (Managed Security Service Provider) betreiben wir Plattformen und Hardware zur Absicherung von OT
- OT Security Operation Center für KRITIS Unternehmen
- Ganzheitlicher OT-IT Cyber Security Ansatz

VIP Guard
Cyber Security Service

Umfassender Schutz für VIPs:

Cybersicherheit in der digitalen Ära

Wichtigkeit der C-Level-Sicherheit
Führungskräfte haben oft wenig Zeit für digitale Sicherheit, was sie zu attraktiven Zielen für Cyberkriminelle macht. Diese Angreifer sind oft wirtschaftlich motiviert und zielen auf das C-Level ab, da diese Positionen umfassende Zugriffsrechte auf IT-Assets haben und wichtige Entscheidungen treffen.

Risikofaktoren und Bedrohungen
Das C-Level ist besonders gefährdet durch ihre weitreichenden Zuständigkeiten und den Zugang zu kritischen Ressourcen. Hacker können diese Befugnisse missbrauchen, wie ein Fall zeigt, bei dem Mitarbeiter eines deutschen Autozulieferers 40 Millionen Euro aufgrund einer Phishing-Mail überwiesen. Auch der ständige Wechsel zwischen Aufgaben erhöht die Gefahr, auf schädliche Links zu klicken.

Exponierte Positionen
Führungskräfte sind oft öffentlich sichtbar, sei es auf Messen oder in sozialen Medien. Angreifer nutzen diese Informationen für gezielte Social-Engineering-Angriffe. Daten aus LinkedIn oder Xing werden verwendet, um realistische Phishing-Angriffe zu starten, die auf echte Kunden oder Partner Bezug nehmen.

Notwendige Schutzmaßnahmen
Um das C-Level zu schützen, sind spezielle Sicherheitsmaßnahmen erforderlich. Dazu gehören regelmäßige Schulungen, die Implementierung von Sicherheitslösungen und die Unterstützung durch IT-Administratoren. Diese Maßnahmen helfen, das Bewusstsein für spezifische Risiken zu schärfen und die digitale Identität der Führungskräfte zu schützen.

Zukunft der C-Level-Sicherheit
Geschäftsführer benötigen einen besonderen Schutz, da sie oft von wesentlichen Kontrollen ausgenommen sind. IT-Sicherheitsexperten, sowohl intern als auch extern, spielen eine entscheidende Rolle dabei, diese Schutzmaßnahmen zu implementieren und kontinuierlich zu überwachen. Nur so kann die Sicherheit des C-Level gewährleistet werden.

- Darknet Recherchen
- VIP GUARD Hotline
- Priority Check im Security Operation Center
- VIP GUARD Hardware

ISMS

Informationssicherheit-Management-System

Erfüllen regulatorischer Anforderungen und Erreichen der Informationssicherheitsziele

Ein ISMS dient zur Verwaltung und Erstellung von Richtlinien, Verfahren, Maßnahmen, Kontrollen und Risiken im Kontext der Informationssicherheit, um die Sicherheitsziele des Unternehmens und regulatorische Anforderungen zu erfüllen.
Sicherheitslücken werden dabei identifiziert und behoben, Kosten für Angriffe reduziert und der Geschäftsfortbetrieb sichergestellt.

Unsere Experten unterstützen vollumfänglich bei:

- Informationssicherheitsberatung: Aufbau, Prüfung und Weiterentwicklung eines ISMS
- IS-Risikomanagement: Aufnahme und Bewertung von IS-Risiken
- Richtlinienentwicklung: Bereitstellung und Weiterentwicklung für die notwendigen IS-Richtlinien
- IT-Security: Auswahl von geeigneten und risikobasierten Maßnahmen und IT-Security-Tools für ihr Unternehmen
- Notfallplanung: Erstellung und Überarbeitung von Notfallhandbuch, Wiederherstellung- und Wiederanlaufplänen gegen Ransomware und andere Sicherheitsvorfälle

Unsere Beratungsleistung macht Ihr Unternehmen widerstandsfähig gegenüber Cyberangriffen und regulatorischen Herausforderungen.

Frameworks:

- ISO 27001- Familie
- BSI-IT-Grundschutz (200-0 bis -4)
- ISO 22301

Verordnungen:

- NIS2
- KRITIS
- DORA

Managed Microsoft Security Services

Umfassender Schutz für Endpunkte, Netzwerke, Cloud und IoT

Das „Defender Framework" von Microsoft umfasst Sicherheitslösungen, die Unternehmen vor Cyberbedrohungen schützen. Es bietet Schutz für Endpunkte, Netzwerke, Cloud-Infrastrukturen und Identitäten.

Microsoft Defender for Cloud ist eine Cloud-native Anwendungsschutzplattform (CNAPP), die Schwachstellen in Cloudkonfigurationen erkennt und den Sicherheitsstatus in Multi- und Hybridumgebungen stärkt.

Microsoft Defender for Endpoint schützt Geräte mithilfe fortschrittlicher Technologien wie Antivirus und Anti-Malware und bietet Erkennungs- und Reaktionsfunktionen auf Sicherheitsvorfälle.

Microsoft Defender for Office 365 schützt Anwendungen wie Exchange, SharePoint und Teams vor Bedrohungen wie Phishing und Malware.

Microsoft Defender for Identity erkennt Identitätsdiebstahl und warnt vor Angriffen wie Passwortdiebstahl und Pass-the-Hash-Angriffen.

Microsoft Defender for Cloud Apps sichert SaaS-Anwendungen und schützt vor Datenlecks und Bedrohungen durch unsichere Konfigurationen.

Microsoft Defender for IoT bietet Sicherheitsfunktionen für IoT-Geräte, einschließlich Cyberthreat Detection und Enterprise IoT Protection.

Diese Lösungen bieten umfassenden Schutz und helfen, Sicherheitsvorfälle frühzeitig zu erkennen und zu beheben.

Use Case:
Advanced Persistent Threat (ATP) im Unternehmensnetzwerk

Phase 1: Erkennung des Vorfalls
Ein Alarm zeigt ungewöhnliches Verhalten auf einem Finanzabteilungs-Computer. Ein potenzieller Zero-Day-Exploit wird entdeckt: Verdächtige PowerShell-Befehle versuchen, auf kritische Daten zuzugreifen. Kommunikation mit einer bekannten Command-and-Control (C2)-Infrastruktur. Microsoft Defender erstellt eine Übersicht der Aktivitäten und ein Angriffsdiagramm.

Phase 2: Automatisierte erste Reaktion (SOAR)
Die SOAR-Plattform reagiert auf Alarme von Microsoft Defender und führt Playbooks aus: Quarantänemaßnahmen: Isolierung des betroffenen Endpunkts. Forensische Sicherung: Automatisierte Erfassung von Speicherauszügen und Logs sowie Analyse der PowerShell-Befehle.

Phase 3: Eskalation und manuelle Analyse (SOC)
Der Vorfall erfordert eine manuelle Analyse durch das SOC. Ein Analyst erkennt, dass die Angreifer möglicherweise länger im Netzwerk aktiv sind:

- Erweiterte Bedrohungsanalyse: Angreifer zielen auf sensible Finanzdaten und versuchen seitliche Bewegungen.
- Abgleich mit Bedrohungsdatenbanken: Integration mit Threat Intelligence Feeds zeigt einen bekannten, staatlich unterstützten APT.

Phase 4: Koordinierte Reaktion und Eindämmung
Ein umfassender Response-Plan wird erstellt. Microsoft Defender und die SOAR-Plattform arbeiten zusammen:

- User Account Blocking: Deaktivierung betroffener Benutzerkonten.
- Überwachung der Kommunikation: Neue Regeln zur Blockierung von C2-Verbindungen.

Phase 5: Berichterstattung und Nachbereitung
Das SOC wertet Daten aus und implementiert neue Erkennungsregeln. Ein verbessertes Playbook wird entwickelt.

Schlussfolgerung:
Die Integration von Microsoft Defender und SOAR zeigt, wie Automatisierung und menschliche Expertise zu effektivem Security Incident Management führen.

Use Case:
Einführung von Managed Security Services für ein Unternehmen

Einführung: Ein Unternehmen steht vor der Herausforderung, die Sicherheit seiner IT-Infrastruktur signifikant zu erhöhen, um potenzielle Bedrohungen proaktiv zu erkennen und effektiv zu bekämpfen.

Herausforderungen: Die heutige Bedrohungslandschaft entwickelt sich ständig weiter und wird zunehmend komplexer. Traditionelle Sicherheitsansätze sind oft nicht mehr ausreichend, um den ständig wachsenden Bedrohungen standzuhalten. Das Unternehmen muss seine sensiblen Daten und kritischen Systeme vor einer Vielzahl von Bedrohungen schützen, darunter Cyberangriffe, Datendiebstahl und interne Sicherheitsrisiken.

Lösung: Die Einführung von Managed Security Services bietet eine ganzheitliche Lösung, um die Sicherheitslage des Unternehmens zu stärken. Durch die Auslagerung der Sicherheitsverantwortung an erfahrene Sicherheitsexperten kann eine kontinuierliche Überwachung, Analyse und Reaktion auf Sicherheitsvorfälle sichergestellt werden.

Diese Dienste umfassen unter anderem:

Netzwerk- und Endpunktsicherheit: Überwachung des Netzwerkverkehrs und der Endpunkte, um verdächtige Aktivitäten zu identifizieren und zu blockieren.

Identitäts- und Zugriffsmanagement: Implementierung von strengen Zugriffskontrollen und Multi-Faktor-Authentifizierung, um unbefugten Zugriff zu verhindern.

Bedrohungs- und Schwachstellenmanagement: Kontinuierliche Überwachung der Bedrohungslandschaft und Schwachstellenbewertung, um proaktiv Sicherheitslücken zu schließen.

Incident Response: Schnelle Reaktion auf Sicherheitsvorfälle, um den Schaden zu minimieren und die Wiederherstellungszeit zu verkürzen.

Diese Maßnahmen tragen dazu bei, die IT-Sicherheit des Unternehmens signifikant zu verbessern und es gegen die ständig wachsenden Bedrohungen zu wappnen.

One DATAGROUP – in ganz Deutschland

LOKALE STANDORTE UND ZENTRALE LIEFEREINHEITEN FÜR EINE OPTIMALE KOMBINATION AUS WIRTSCHAFTLICHKEIT UND KUNDENNÄHE.

Hochstandardisierte Prozesse und Services, die beständig verbessert werden, sind die eine Seite der Erfolgsmedaille. Nähe zum Kunden die andere! DATAGROUP setzt dafür auf eine optimale Kombination von lokaler und zentraler Produktion. Das bedeutet: Teile der Serviceproduktion – Service Desk, Operations, Application Management Services und SAP Services – sind virtuell in zentralen Liefereinheiten zusammengefasst. Das bringt Skalen- und Qualitätsvorteile durch Spezialisierung und eine bessere Auslastung von Expert*innen und Systemen.

Die Produktion der übrigen CORBOX-Leistungen wie zum Beispiel End User Services erfolgt an lokalen Standorten in allen wichtigen Wirtschaftsregionen Deutschlands. Auch das gesamte Service Management und damit die Verantwortung gegenüber dem Kunden, dass das Leistungsversprechen eingehalten wird, liegt bei den lokalen DATAGROUP-Gesellschaften vor Ort. Sie sind mit ihren Geschäftsführerinnen und Geschäftsführern an der Spitze der zentrale Ansprechpartner auf Augenhöhe für die Kunden.

Das DATAGROUP-Produktionsmodell mit lokalen Standorten und virtuell zentralisierten Leistungseinheiten erlaubt alle CORBOX-Services effizient und in höchster Güte in Deutschland zu produzieren und gleichzeitig die Nähe zum Kunden zu gewährleisten.