SOC

SECURITY OPERATION CENTER

www.she.net

IHR SECURITY CENTER
FÜR MEHR SICHERHEIT

S|H|E

CONTENT

she.net

Ertem Albayrak
Teamlead Cyber Security
security@she.net

„Immer eine IT voraus“ ist unser Slogan – nicht nur, wenn es um Digitalisierung und klassische IT Security geht, sondern auch dann, wenn es um die Next-Generation IT-Security geht.

Mit unserem **Security Operation Center** wollen wir unsere Kunden gegen Gefahren aus dem Netz schützen. Wir beobachten, dass die Gefahren durch **Cyber Crime** sprunghaft zunehmen und rechnen damit, dass sie noch weiter zunehmen werden. Um dieser Entwicklung direkt eine starke Antwort entgegenzusetzen, wurde das Security Operation Center der SHE ins Leben gerufen.

Unsere Ambition ist, unsere Kunden bestmöglich schützen zu können. Damit das funktioniert, ist es natürlich zwingend notwendig, das **Schutzlevel in Ihrer Infrastruktur** auf ein Level zu bringen, dass Sie **vor allen Gefahren schützt**.

Wie Sie ja auch selber wissen, ist es heute extrem schwer, ein bezahlbares Team auf die Beine zu stellen, das Sie zuverlässig gegen diese Gefahren von außen schützen kann.

Wir nehmen Ihnen diese Last ab. Und das Gute dabei ist: Sie können sich auf unsere Expertise verlassen

Kontakt

Ihre Sicherheit ist unsere Mission

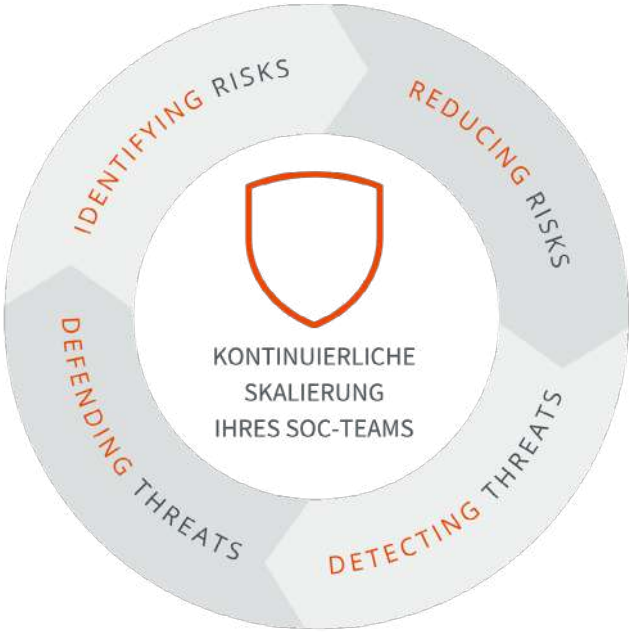
Die Entwicklung bleibt bei uns nicht stehen

„Immer eine IT voraus“ heißt auch bei uns im Umkehrschluss, den Angreifern immer einen Schritt voraus zu sein.

Wir versprechen unseren Kunden nicht nur das Beste, sondern wir liefern auch:

- bei höchster Sicherheit
- bei der Qualität
- bei unserer Dienstleistung.

Mit einem persönlichen Plan, der genau auf Sie und Ihre Bedürfnisse abgestimmt und und individuell ist, passen wir unsere Leistung Ihrem **SOC-Dienstleistungsplan** an.



Was hat sich eigentlich von früher zu heute geändert?

Früher waren es Burgen und Festungen, die vor Eindringlingen geschützt werden mussten.

Heute sind es Unternehmen, die es zu schützen gilt doch die Gefahren lauern heute im Inneren.

Lassen Sie uns Ihre Festung gemeinsam schützen – von innen und von außen.

Ihr individuelles SOC

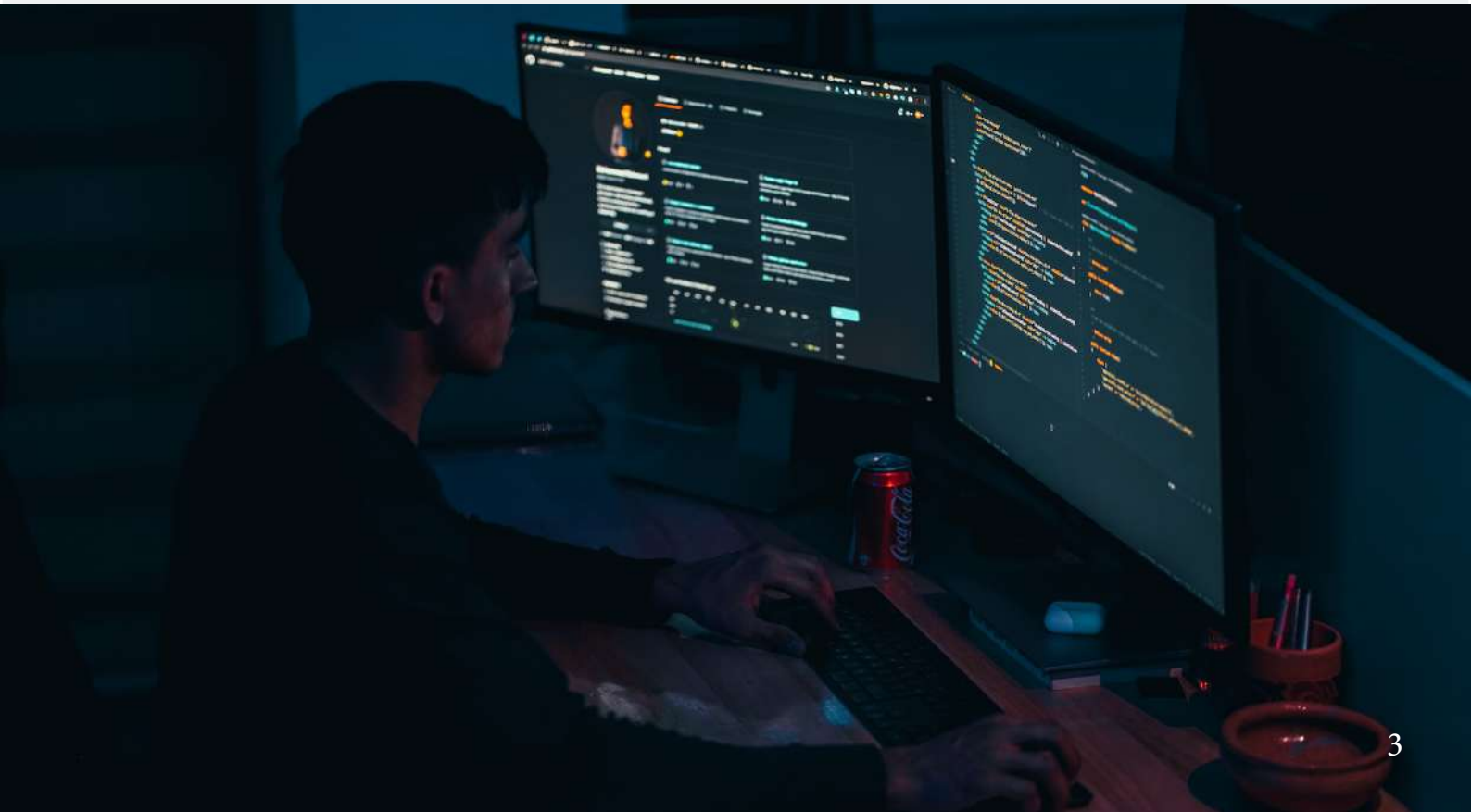
Security Operation Center

Jahrelang haben wir Sie mit unserer traditionellen IT Security und unseren Managed Security Services unterstützt. Jetzt setzen wir mit unserem **Security Operation Center** noch einen oben drauf: denn außergewöhnliche Umstände in der Cyber Security erfordern auch außerordentliche Maßnahmen. Ein eingespieltes **Team von Experten** steht Ihnen in unserem SOC zur Verfügung. Und das – unkompliziert – alles aus einer Hand !

SHE SOC Unterstützung

- Cyber Security Team SHE
- Spezielle Fachteams:
  - Microsoft
  - Linux
  - Virtualisierung / Backup

- Tier 1-4 Analysten
- Malware Analyst
- Forensik Spezialist
- Threat Hunter
- Vulnerability Assessment Expert



SOC Betrieb

Incident Response

Managed Firewall Betrieb

Traditionelle IT Security

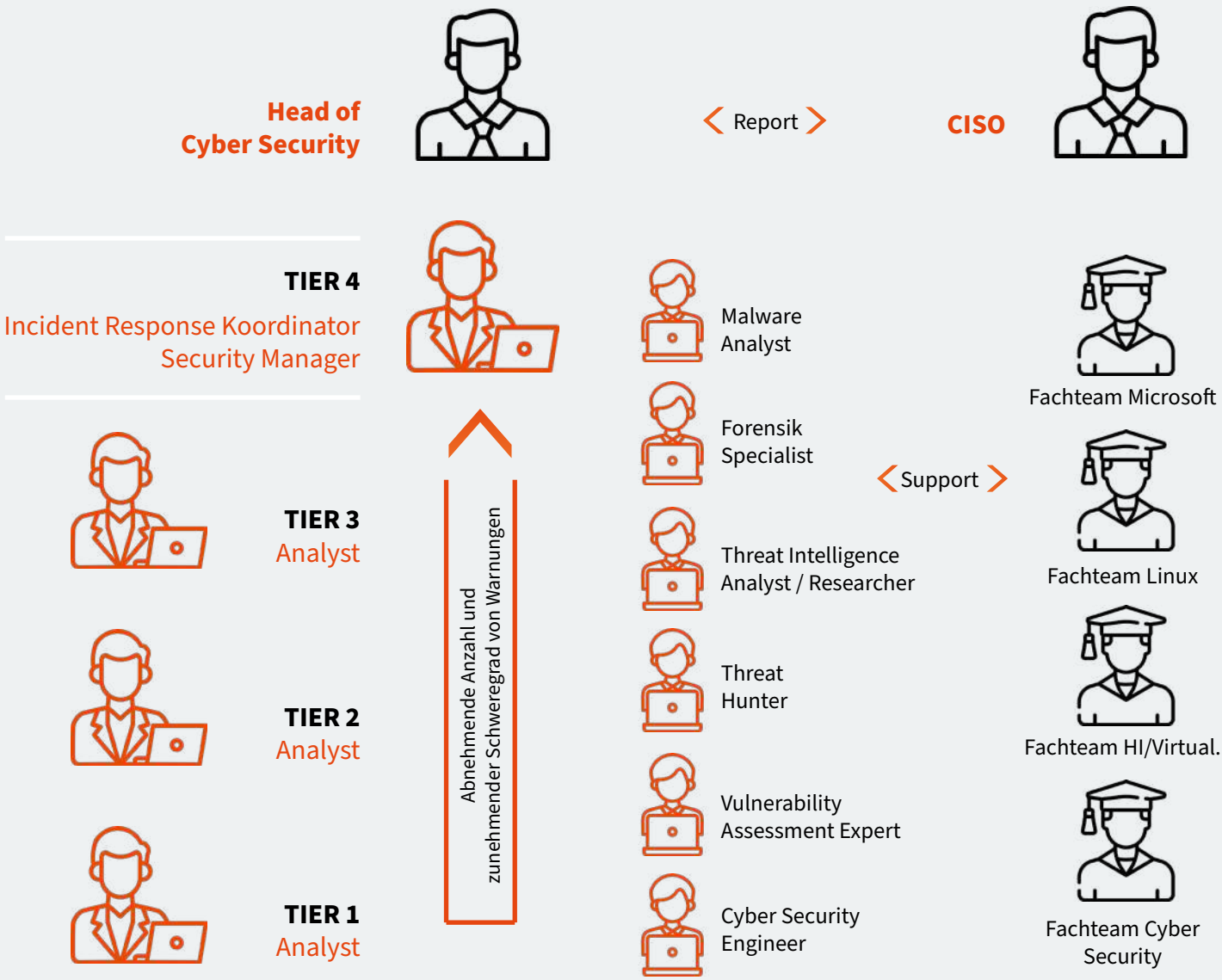
- **Firewall (VPN, IPS/IDS)**
- **Cloud Security**
- **Web Security**
- **Mail Security**
- **Server Security**
- **Web Application Firewall**
- **Endpoint Security**
- **Authentification**

SHE SOC Struktur

Struktur für ein perfekter SOC

Für ein gutes SOC benötigt man auch die dementsprechende Struktur. Mit unserem **qualifizierten Personal** können wir Ihre Struktur absichern. Bei SHE haben Sie jedoch einen **weiteren Vorteil**: Unser SOC nutzt auch seine Ressourcen in den Fachabteilungen, falls in den Bereichen Linux, Microsoft oder Virtualisierung Expertise verlangt wird. So können Sie **jederzeit auf unsere Spezialisten zurückgreifen**. Überzeugen Sie sich selbst von unseren vielversprechenden Möglichkeiten!

So sieht es bei SHE aus:



Planung Rollout SOC

Rollout-Planungsphase für Tools

Tenant einrichten	Architektur	Initiale Policies	Rollout Testgruppe	Alarme bearbeiten	Policies optimieren	Rollout	Betrieb
Tenant beauftragen nach Auftrags- eingang vom Kunden	Definition der Policy Stuktur abstimmen	Erstellen der Policies und Sensor Groups	Rollout der Sensors auf definierten Testsystemen	Prüfen und Bearbeiten der auftretenden Alarme	Konfiguration optimieren	Rollout der Sensoren auf alle Kundensysteme	Übergang von Projekt in Betrieb

Plan & Deploy

Learn & Optimize

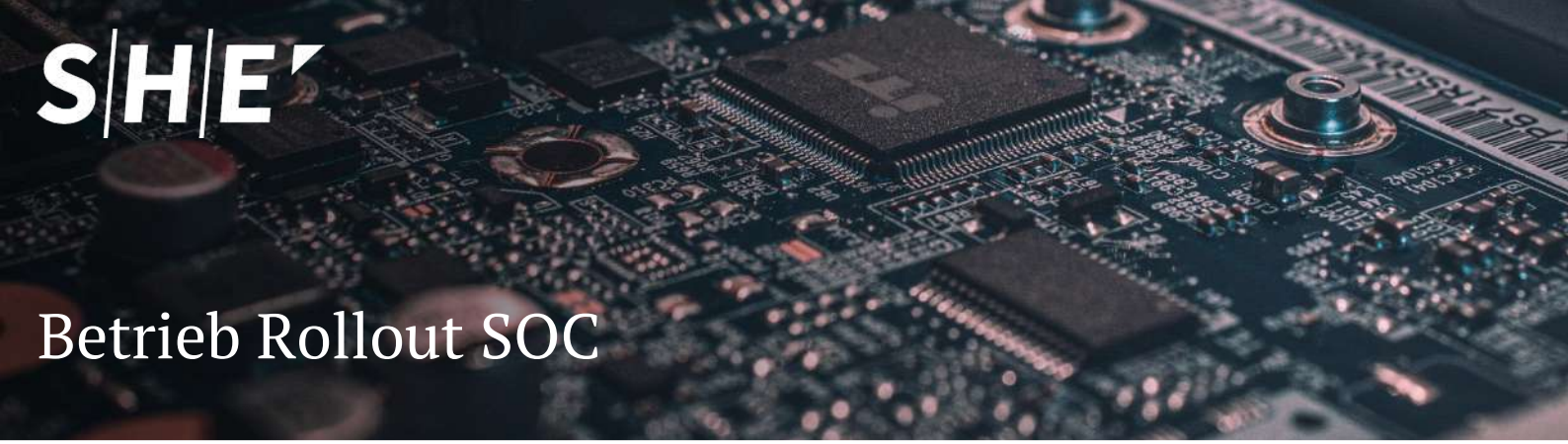
Rollout & Betrieb

Effektive Tools für ein reibungsloses SOC-Management

Für ein gutes SOC werden gute gute Tools benötigt, damit der Betrieb reibungslos laufen kann. Hierbei ist es wichtig, dass diese Tools kontrolliert ineinander zahnen.

Ein spezialisierter Workflow ist hier sehr wichtig, damit später der Betrieb im SOC richtig laufen kann. Umso besser die Planung ist und die komplette Infrastruktur geschützt werden kann, umso besser funktioniert auch die Überwachung.

Und umso detaillierter die Planungsphase ist, umso kleiner ist das Risiko, von unerkannten Gefahren überrollt zu werden.

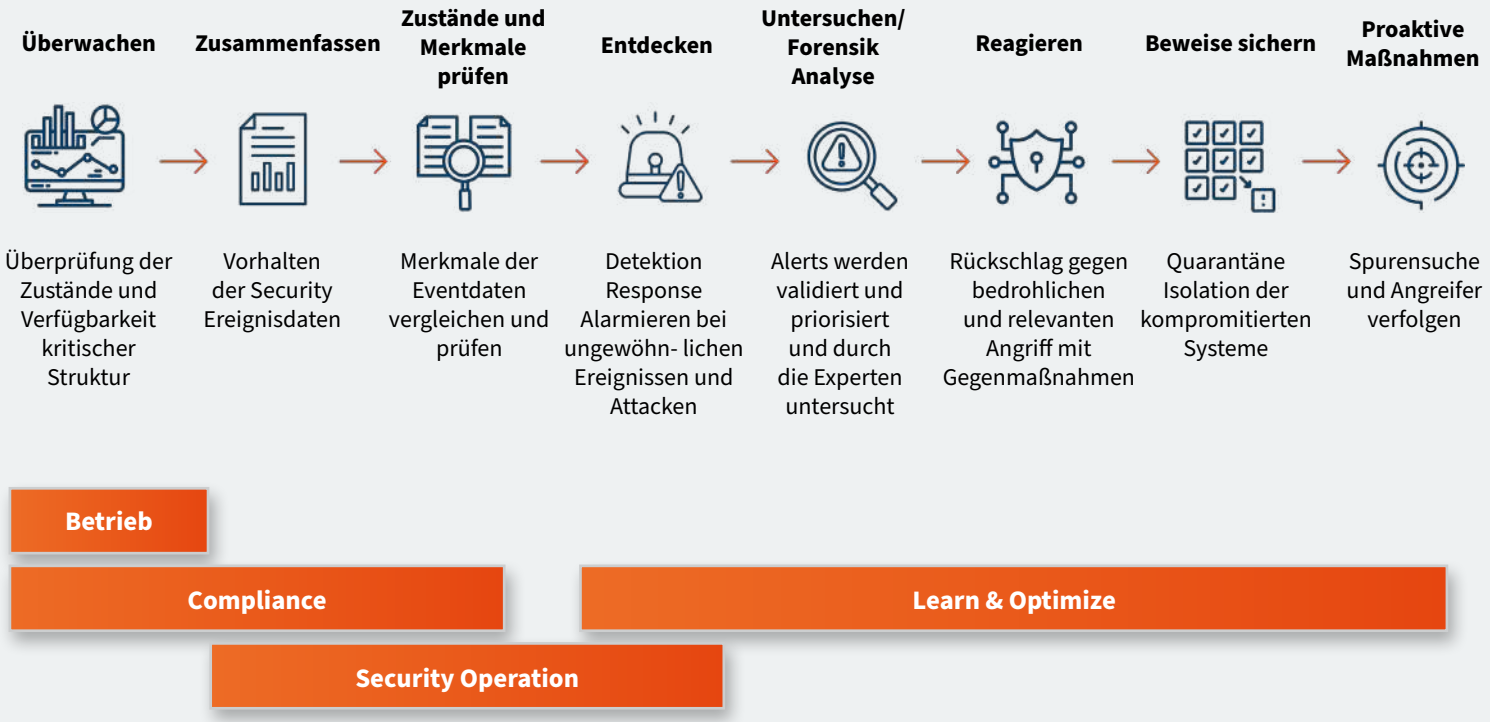


Betrieb Rollout SOC

Struktur für ein perfekter SOC

Nach einen guter Planungsphase kommt der Betrieb – in dem die SOC-Komponenten abgestimmt aufeinander funktionieren. Der Betrieb ist der entscheidende Bestandteil eines SOC. Hier dürfen keine Fehler passieren, deswegen ist es hier wichtig, dass die Verfahren exakt aufeinander abgestimmt wurden. Egal welche Komponenten Sie in Ihrem SOC betreiben – ohne den richtigen Workflow kann das ganze System zusammenbrechen.

SOC Betrieb



Überzeugen Sie sich direkt von unserer Arbeitsweise!

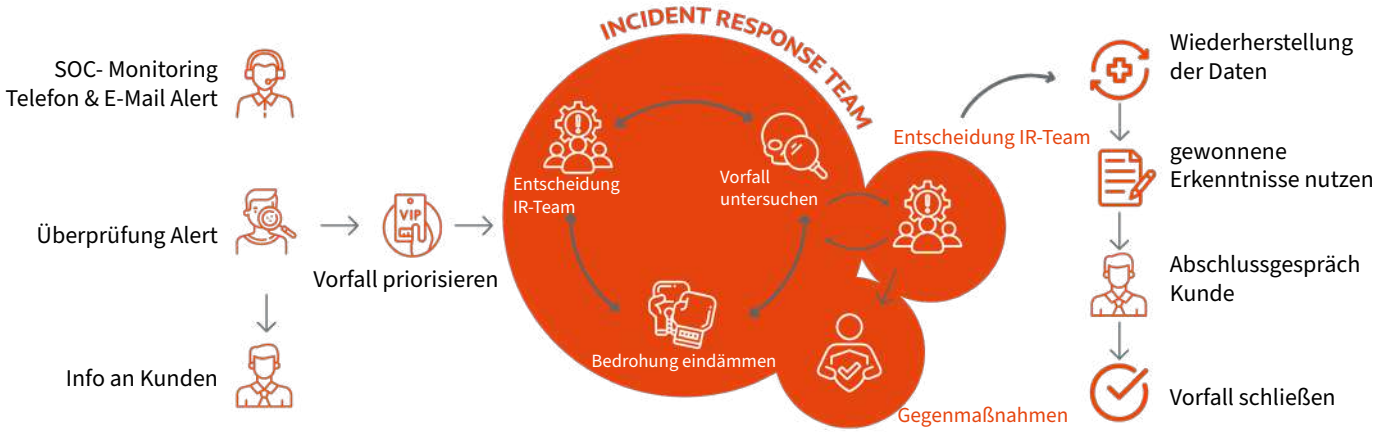
Jetzt Termin vereinbaren und Ihr Unternehmen schützen

Kontakt

SOC Workflow & Incident Response Team (IR)

SOC Workflow

Ein richtiges SOC benötigt den richtigen Ablauf, und damit die Abläufe perfekt funktionieren, müssen auch Maßnahmen ergriffen werden. So weiß jede Schnittstelle, wie sie sich zu verhalten hat. Für ein perfektes Zusammenspiel müssen alle SOC Mitarbeiter Ihre Abläufe zu 100% beherrschen. Falsche Entscheidungen können zu gravierenden Fehlern führen. Unser eingespieltes Team führt Sie sicher ans Ziel.



Incident Response Team

Ein fester Bestandteil des SOC ist unser Incident Response Team. Diese Spezialisten unterstützen das SOC bei aktivem Befall von Malware / Angriffen. Sie kommen zum Einsatz, wenn bei Routineüberprüfungen Ransomware-Angriffe, Datendiebstahl sowie Phishing-Angriffe festgestellt werden.

Sie führen eine Schadensanalyse durch, um den kritischen Zustand der Infrastruktur zu ermitteln. Durch die Schnellanalyse der Systeme wird gezielten und direkten Hinweisen nachgegangen und diese analysiert.

Durch zusätzliche Gegenmaßnahmen wird Ihre Infrastruktur gerettet, die Suche eingegrenzt und die Infrastruktur ggf. gesäubert. So können Sie schnellstmöglich und sicher wieder im Regelbetrieb weitermachen.

Technologien

Mit welchen Technologien arbeiten wir?

EDR Security

EDR **(Endpoint Detection and Response)** ist eine Art von IT-System, die speziell für die Erkennung und Reaktion auf Bedrohungen im Zusammenhang mit Endpunkten entwickelt wurde. Ein Endpunkt ist ein Computer oder ein mobiles Gerät, das mit einem Netzwerk verbunden ist. EDR-Systeme sind darauf ausgelegt, Endpunkte in einem Netzwerk zu überwachen, Bedrohungen zu identifizieren und schnell darauf zu reagieren.

Einige Merkmale von EDR- Systemen:

1. Echtzeit-Überwachung:
EDR-Systeme überwachen Endpunkte in Echtzeit, um Bedrohungen schnell zu identifizieren und darauf zu reagieren.

2. Automatisierte Reaktion:
EDR-Systeme können automatisierte Reaktionen auf Bedrohungen implementieren, um schnell auf Angriffe zu reagieren und Schäden zu minimieren.

3. Verhaltensanalyse:
EDR-Systeme verwenden Verhaltensanalyse-Technologien, um ungewöhnliche Aktivitäten auf Endpunkten zu erkennen und Bedrohun- gen zu identifizieren, die traditionelle Signaturen nicht erkennen können.

4. Forensische Analyse:
EDR-Systeme speichern Daten über Endpunkt- aktivitäten und ermöglichen es, Bedrohungen zu untersuchen und zu analysieren, um An- griffe zu verstehen und zukünftige Sicherheitsmaßnahmen zu verbessern.

5. Integration mit SIEM:
EDR-Systeme können in eine SIEM (Security In- formation and Event Management)-Plattform integriert werden, um umfassendere Sicher- heitsanalysen durchzuführen und Bedrohun- gen im gesamten Netzwerk zu erkennen.

EDR-Systeme sind ein wichtiger Bestandteil der modernen IT-Sicherheit und helfen Unternehmen und Organisationen, Bedrohungen auf Endpunkten schnell zu erkennen und darauf zu reagieren, um Schäden zu minimieren und die Sicherheit des Netzwerks zu gewährleisten.

XDR Security

XDR Security steht für **Extended Detection and Response**. Es handelt sich um eine Weiterentwicklung des SIEM (Security Information and Event Management) - Systems und bezieht sich auf eine integrierte Sicherheitsplattform, die eine erweiterte **Erkennung und Reaktionsfähigkeit auf Bedrohungen** bietet.

Integrierte Sicherheit: XDR-Systeme als All-in-One-Lösung

XDR Security-Systeme sind in der Lage, Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren, indem sie Daten aus verschiedenen Quellen wie Endgeräten, Servern, Netzwerken und Cloud-Diensten sammeln und korrelieren.

Im Gegensatz zu herkömmlichen SIEM-Systemen integrieren XDR-Systeme auch Endpunktsicherheit, Bedrohungsjagd, automatisierte Reaktion und forensische Analyse in einer einzigen Plattform.

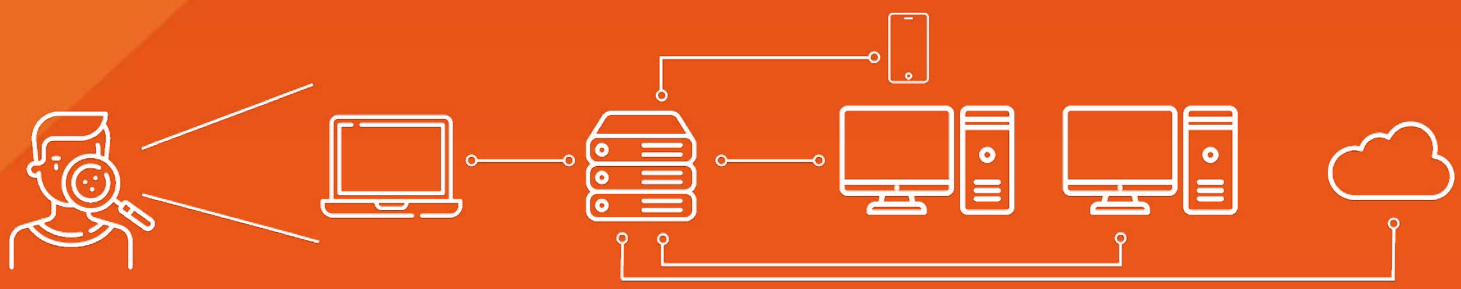
Die Integration von Endpunktsicherheit ermög- licht es XDR-Systemen, tiefere Einblicke in Endpunktaktivitäten zu erhalten und fortschrittlichere Bedrohungen zu erkennen.

Die Möglichkeit zur Bedrohungsjagd ermöglicht den XDR-Systemen, Bedrohungen proaktiv zu identifizieren und zu eliminieren, bevor sie Schaden verursachen können.

Durch die automatisierte Reaktion können Bedrohungen automatisch blockiert oder isoliert werden und somit Schäden minimiert werden.

XDR-Sicherheitsplattformen bieten Unternehmen eine umfassende und integrierte Lösung zur Erkennung, Reaktion und Vorbeugung von Bedrohungen. Das kann zu einer verbesserten Sicherheit von Unternehmensnetzwerken und – daten beitragen.

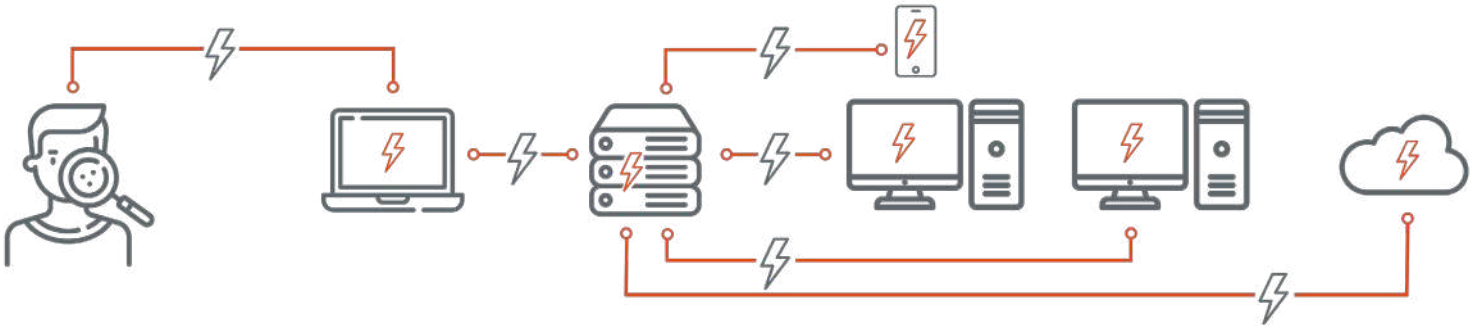
Extended Detection and Response



Vulnerability Management- Systeme

Vulnerability Management-Systeme sind IT-Systeme, die verwendet werden, um Schwachstellen in IT-Systemen, Anwendungen und Netzwerken zu identifizieren, zu bewerten und zu priorisieren. Diese Systeme spielen eine **wichtige Rolle bei der Sicherung** von IT-Infrastrukturen, indem sie Unternehmen und Organisationen in die Lage versetzen, Schwachstellen zu erkennen und **Maßnahmen zu ergreifen**, um diese zu beseitigen oder zu minimieren.

Einige Merkmale von Vulnerability Management-Systemen:



1. Schwachstellenerkennung:
VulnerabilityManagement-SystemescannenIT-Systeme, Anwendungen und Netzwerke, um Schwachstellen zu identifizieren, die von Angreifern ausgenutzt werden können.

2. Schwachstellenbewertung:
Vulnerability Management-Systeme bewerten Schwachstellen und priorisieren diese basierend auf der Schwere und dem potenziellen Risiko, das von einer ausgenutzten Schwach- stelle ausgeht.

3. Berichterstellung und Dashboards:
Vulnerability Management-Systeme generieren Berichte und Dashboards, die den Fortschritt der Schwachstellenbehebung verfolgen und zeigen, welche Schwachstellen noch ausste- hen.

4. Automatisierung:
Vulnerability Management-Systeme können Automatisierungsfunktionen verwenden, um Scans, Bewertungen und Berichterstellung zu automatisieren, was Zeit spart und die Effi- zienz erhöht.

5. Integration mit anderen Systemen:
Vulnerability Management-Systeme können mit anderen IT-Sicherheitssystemen wie SIEM, EDR und Firewall-Systemen integriert werden, um eine umfassendere Sicherheitsanalyse und -reaktion zu ermöglichen.

Insgesamt sind Vulnerability Management-Systeme ein wichtiger Bestandteil der IT-Sicherheitsinfra- struktur und helfen Unternehmen und Organisationen, Schwachstellen zu identifizieren und zu besei- tigen, um ihre IT-Systeme und Netzwerke vor Angriffen zu schützen.

Partner

Starke Partner für Ihre Sicherheit

Beim Thema Sicherheit vertrauen wir auf **langjährige Partner** und **Experten** im Bereich Cyber Security

CrowdStrike ist ein führendes Unternehmen im Bereich der Cybersicherheit, das sich auf den Schutz vor Cyberbedrohungen und die Abwehr von Angriffen spezialisiert hat.

Die Lösungen von CrowdStrike umfassen unter anderem Endpoint-Sicherheit, Threat Intelligence und Incident Response.

Das Unternehmen nutzt fortschrittliche Technologien wie KI und maschinelles Lernen, um Kunden weltweit vor Cyberangriffen zu schützen.

Rapid7 ist ein Software-Unternehmen, das Sicherheitslösungen für Organisationen bereitstellt, um Cyberbedrohungen zu erkennen und darauf zu reagieren. Sie bieten eine Vielzahl von Produkten und Dienstleistungen wie Schwachstellenmanagement, Anwendungssicherheit, Vorfallserkennung und Reaktion sowie Compliance-Management an.

Die Lösungen von Rapid7 sollen Unternehmen dabei helfen, ihre Sicherheitsposition zu verbessern und sich gegen eine Vielzahl von Cyberangriffen zu schützen.

Das Unternehmen wurde im Jahr 2000 gegründet und hat seinen Hauptsitz in Boston, Massachusetts, USA.

Check Point Perimeter von Check Point Software Technologies schützt den Netzwerkperimeter mit verschiedenen Sicherheitsprodukten wie Firewalls, IPS, VPNs und Sicherheitsgateways.

Diese Produkte blockieren unerwünschten Datenverkehr, erkennen Bedrohungen und gewährleisten Datenintegrität.

Unternehmen können damit proaktiv Bedrohungen identifizieren und neutralisieren. Zusätzliche Funktionen wie zentrales Management vereinfachen die Sicherheitsüberwachung.

Darktrace ist ein Unternehmen für künstliche Intelligenz und Cybersecurity, das sich auf die Erkennung von Cyberbedrohungen spezialisiert hat.

Mit selbstlernender KI-Technologie identifiziert Darktrace anomales Verhalten in Netzwerken, Cloud-Umgebungen, Industrieanlagen und IoT-Systemen. Das Unternehmen bietet verschiedene Sicherheitslösungen wie Netzwerksicherheit, Cloud-Sicherheit und Industrie-Sicherheit an.

Sie helfen Unternehmen, sich vor Cyberangriffen wie Ransomware, APTs und Insider-Bedrohungen zu schützen.

Cyber-Sicherheit jetzt

Stets einen Schritt voraus: Kontinuierliche Verbesserung der Cyber-Sicherheit

Insgesamt lässt sich festhalten, dass die Cyber-Sicherheit eine wichtige Rolle für Unternehmen und Organisationen jeder Größe und Art spielt. Die Bedrohungslandschaft entwickelt sich ständig weiter und es ist daher wichtig, dass Sie auf dem neuesten Stand der Technologie und Methoden bleiben, um sich gegen Cyberangriffe zu schützen.

Um eine robuste Cyber-Sicherheitsstrategie zu entwickeln, sollten Sie eine umfassende Risikoanalyse durchführen, um potenzielle Schwachstellen in ihren Systemen und Prozessen zu identifizieren. Ebenso ist es wichtig in der heutigen Zeit ein ausbaubares SOC-Team in der Hinterhand zu haben. Es ist auch wichtig, eine Kultur der Sicherheit zu schaffen, die Mitarbeiter für die Bedeutung der Cyber-Sicherheit sensibilisiert und Schulungen und Trainings bereitstellt.

Technologien wie Firewalls, Antivirus-Software, Verschlüsselung und Zugriffskontrollen sind ebenfalls entscheidend für eine effektive Cyber-Sicherheitsstrategie. Sie sollten jedoch auch auf fortschrittlichere Technologien wie künstliche Intelligenz und maschinelles Lernen achten, die es ermöglichen, Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren.

Durch eine proaktive Herangehensweise an die Cyber-Sicherheit und eine kontinuierliche Überwachung und Verbesserung Ihrer Systeme und Prozesse, können Sie das Risiko von Cyberangriffen reduzieren sowie Ihre Daten und Systeme besser schützen.

Handeln Sie jetzt!

Cyber Resilience, SOC und traditionelle IT Security

Warten Sie nicht auf den Angriff – Schützen Sie Ihr Unternehmen jetzt!

Kontakt

Immer eine IT voraus.

SOC

SECURITY OPERATION CENTER

www.she.net

Donnersbergweg 3
67059 Ludwigshafen

T +49 621 5200-0
security@she.net

SHE