MATERNA
Information & Communications

Whitepaper

Security Operations Center

Alarmstufe Rot im Rechenzentrum und wie Organisationen wirkungsvoll Cyberangriffe abwehren

Schäden durch Cyber-Kriminalität erreichten im Jahr 2020 mit 223 Milliarden Euro einen neuen Höchststand, so die Zahlen des Digitalverbands Bitkom. Neun von zehn Unternehmen wurden demnach Opfer von Diebstahl, Spionage oder Sabotage. Ein Security Operations Center (SOC) hilft dabei, die IT zu schützen. Materna betreibt selbst ein eigenes SOC und bietet darüber eine Reihe von Security-Dienstleistungen für Unternehmen und Behörden.

In diesem Whitepaper lesen Sie:

- warum immer mehr Unternehmen auf externe Security-Dienstleistungen setzen.
- wie ein Security Operations Center dabei hilft, Daten und Infrastruktur abzusichern.
- wie Security-Expert:innen von Materna auf Cyber-Bedrohungen reagieren.
- mit welchen Prozessen und Technologien Materna Cyber-Angriffe abwehrt.

Inhalt

Cyber-Alarm im Rechenzentrum

Anfang März 2021 hatte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Alarmstufe Rot ausgerufen: Allein in Deutschland waren zu diesem Zeitpunkt Zehntausende von Exchang-Mailservern anfällig für einen Angriff durch Schad-Software. In der Folge begann ein Wettrennen: Einerseits versuchten Hacker, sich schnell noch Zugang zu fremden Servern zu verschaffen, solange dies noch technologisch möglich war. Andererseits waren die IT-Expert:innen bei den Anwenderunternehmen bestrebt, ihre Server schnellstmöglich durch Einspielen eines Updates zu sichern.

Wer in so einer Situation kein eigenes IT-Security-Team beschäftigt oder rasch auf externe Expert:innen zurückgreifen kann, begibt sich in eine gefährliche Situation. Denn häufig spielen Hacker die Schad-Software zunächst unbemerkt auf die fremden Rechner, um dann Tage, Wochen oder Monate später zuzuschlagen.

Security-Expert:innen dringend gesucht

Ist Ihre Organisation gegen Angriffe von Hackern geschützt? Oder zählen Sie zu den 14 Prozent der Unternehmen, die keine besonderen Vorkehrungen zur IT-Sicherheit getroffen haben? Eine Cyber-Security-Studie von YesWeHack ergab nämlich, dass tatsächlich jedes siebte befragte Unternehmen in Deutschland seine IT nicht ausreichend schützt. Darüber hinaus zeigt eine Studie der Security-Expert:innen von Kaspersky aus dem Jahr 2020, dass nur rund die Hälfte der weltweit befragten Unternehmen eine eigene Cyber-Security-Abteilung hat, während nur etwa 20 Prozent ein internes Security Operations Center (SOC) betreiben.

Vielleicht liegt dies auch daran, dass einfach nicht genug Fachleute für das komplexe Thema IT-Sicherheit verfügbar sind? Der globale Verband für Informationssicherheit (ISC)² schätzt, dass allein in den USA fast eine halbe Million zusätzlicher Cyber-Security-Expert:innen benötigt werden (Stand 2019).

- **Fachkräftemangel betrifft auch das Thema IT-Security und gefährdet die IT-Sicherheit.**

Wer sich kein eigenes Security-Team aufbauen kann, beispielsweise aus Kostengründen, greift auf externe Dienstleister zurück, die ein eigenes SOC betreiben. Dort arbeiten hochspezialisierte Expert:innen, die rund um die Uhr die IT-Sicherheit der betreuten IT-Systeme der Kunden inklusive der Netzwerke überwachen.

So arbeitet ein SOC

Ein SOC dient ganz unterschiedlichen Zielen. Ein zentraler Aspekt ist das schnelle Erkennen von Cyber-Angriffen – idealerweise noch bevor es den Angreifern gelingt, brisante Daten zu entwenden. Darüber hinaus analysieren die Security-Expert:innen die Auswirkungen einer Attacke, um beispielsweise eine Priorisierung des Vorfalls vorzunehmen. Im Anschluss leiten die Mitarbeiter:innen Sofortmaßnahmen für die Eindämmung ein und können Prozesse starten, um Systeme wiederherzustellen.

Weiterhin überwachen die SOC-Mitarbeiter:innen zuvor definierte IT-Policies und Kennzahlen. So können sie schneller auch auf interne Angriffe reagieren. Sind bei einem Unternehmen neue Standorte zu integrieren, bewerten die Expert:innen gemeinsam mit dem Kunden die bestehenden Maßnahmen neu. Eine ebenfalls wichtige Aufgabe ist die Erkennung und Priorisierung von Schwachstellen. Dadurch können eine angepasste Strategie für das Patchmanagement entwickelt, aber auch die Anzahl der Angriffsvektoren gezielt verringert werden.

Schließlich übernehmen die Mitarbeiter:innen auch das Monitoring von Netzwerkaktivitäten, da sie Attacken sehr schnell durch veränderten Netzwerk-Traffic erkennen können. Auch fehlerhafte Konfigurationen von Netzwerkgeräten lassen sich so identifizieren, sodass diese nicht mehr als Angriffspunkt genutzt werden können. Darüber hinaus kann das SOC den laufenden IT-Betrieb mit einem Monitoring unterstützen, falls auf Kundenseite ein Kapazitätsengpass auftritt.

- **Das Security Operations Center bildet eine wichtige Verteidigungslinie gegen Cyber-Angriffe.**

Dies sind nur einige Beispiele für die vielfältigen Aufgaben, die Mitarbeiter:innen eines SOCs übernehmen.

SIEM gilt als wichtiger Baustein

Damit ein SOC bei seiner Kernaufgabe wirkungsvoll arbeitet, sind spezialisierte Software-Tools notwendig, wie eine Lösung für Security Incident und Event Management (SIEM). Das SIEM ist ein wichtiger Baustein innerhalb des SOCs. Diese Anwendung verdichtet an zentraler Stelle die Logdaten von Security Devices und anderen Quellen, um sie zentral für Security-Expert:innen verfügbar zu machen, aber auch, um eine automatisierte Analyse nach Angriffsmustern zu unterstützen. Ohne den genauen Angriff zu kennen, lassen sich mit dieser Software Regeln definieren, die auf bestimmte Angriffsmuster reagieren und es so ermöglichen, neue unbekannte Angriffstechniken zu erkennen – die sogenannten Zero Days.

Auch ein SIEM lässt sich komplett als externer Service von einem Dienstleister beziehen. Hierbei sollte eine Organisation ähnlich wie bei den anderen SOC-Prozessen vorgehen: Nach einer Bestandsaufnahme der vorhandenen Kapazitäten und des eigenen Risikos sollte bestimmt werden, welche Prozesse von einem Dienstleister benötigt werden.

Worauf es ankommt

Um einen Angriff auf die IT erfolgreich abzuwehren, werden eine Vielzahl von Kompetenzen und Werkzeugen benötigt. Eine innovative Software allein reicht jedoch nicht, denn es müssen die drei Komponenten Menschen, Prozesse und Technologien erfolgreich zusammenarbeiten, damit ein SOC wirkungsvoll arbeiten kann.

Menschen machen den Unterschied

- **Auch wenn zahlreiche Abläufe in Rechenzentren automatisiert sind, benötigt ein SOC gut ausgebildete Expert:innen.**

Trotz der fortschreitenden Automatisierung von IT-Abläufen sind es letztlich die Menschen, die über den Erfolg eines Security Operations Centers entscheiden. Bei der Planung eines SOCs sollte daher frühzeitig die Expertise aller Fachbereiche eingeholt werden, um mögliche Schadensszenarien sowie ihre Auswirkung auf die Organisation bestimmen zu können. Da sich Angriffsarten und Technologien stetig weiterentwickeln, müssen sich auch die Security-Spezialist:innen kontinuierlich fortbilden. Weiterhin sollte das Team eines SOC ausreichend groß dimensioniert sein, um 24 Stunden am Tag sowie 365 Tage im Jahr handlungsfähig zu sein. Dies macht es erforderlich, entsprechende Kapazitäten vorzuhalten, um auch Urlaube oder Krankheitsfälle auffangen zu können.

Die Qualifikation der Security-Expert:innen eines SOCs teilt sich in drei Ebenen auf. Von First Level-Analyst:innen, die einfache Alarme bearbeiten, bis hin zu den Third Level-Expert:innen, die z. B. bei der Forensik unterstützen. Ebenso arbeitet ein Team kontinuierlich daran, das Threat Hunting zu verbessern, um Angriffe frühzeitig zu erkennen und proaktiv Schwachstellen aufzudecken. Zu den weiteren laufenden Optimierungen zählen beispielsweise das Anbinden neuer Logquellen sowie die Definition neuer Funktionen für Machine Learning-Anwendungen, um damit zum Beispiel den Automatisierungsgrad der Gefahrenerkennung zu erhöhen.

Prozesse sichern den Erfolg

Richtlinien sowie definierte Abläufe bilden die Basis für eine erfolgreiche Sicherheitsarchitektur. Die Prozesse, nach denen Mitarbeiter:innen im SOC arbeiten, sollten die relevanten Anforderungen rund um das Thema IT-Security sowie eventueller Branchenstandards unterstützen. Beispiele hierfür sind der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die ISO 27001, die KRITIS-Definitionen (Kritische Infrastrukturen), die Anforderungen der US-Behörde NIST sowie branchenspezifische Vorgaben wie PCI (Payment Card Industry Data Security Standard) oder HIPAA (Health Insurance Portability and Accountability Act) und viele weitere Standards und Normen.

Die Kontrolle, ob eine IT-Organisation die genannten Vorhaben einhält, kann optional auch über die Security-Expert:innen eines SOCs erfolgen, die dafür dann in übergeordnete Prozesse integriert sind, wie die Einhaltung von Compliance-Vorgaben.

Auch IT-Service-Management-Systeme, -Maßnahmen und -Methoden müssen technisch eingebunden werden. Individuelle Richtlinien können bei Bedarf ebenfalls IT-technisch überwacht werden. Verantwortlichkeiten und Prozesse für die Incident Response müssen klar beschrieben sein. Eine automatische Incident Response, das heißt Reaktion auf Angriffe oder IT-Ausfälle, muss sich nahtlos und fehlerfrei in die Technik einfügen. Alle Prozesse und Informationsflüsse müssen daher so gestaltet sein, dass sie reibungslos ineinandergreifen. Im Falle eines Angriffes muss das Team in der Lage sein, schnell und koordiniert zu handeln, um Schaden abzuwehren, Datenverlust zu verhindern oder mindestens zu minimieren.

Technologie liefert die Fähigkeiten

Eine Anwendung für SIEM liefert Security-Expert:innen die benötigten Funktionen, um auf Bedrohungen zu reagieren und diese zu bekämpfen. Ein etablierter Software-Hersteller in diesem Segment ist Elastic. Materna ist akkreditierter Professional Partner von Elastic und nutzt die Lösung Elastic Cloud Enterprise (ECE) on Premise in ihrem eigenen SOC.

- **Elasticsearch, Logstash und Kibana sind wertvolle Werkzeuge im Kampf gegen Cyber-Angriffe.**

Zentrale Komponenten von ECE sind die Open-Source-Lösungen Elasticsearch, Logstash und Kibana, die auch als ELK-Stack bezeichnet werden. Elasticsearch ist eine Suchmaschine und Analytics Engine, die die Analyse großer Datenmengen in nahezu Echtzeit ermöglicht. Logstash ist eine serverseitige Datenverarbeitungs-Pipeline, die Daten aus unterschiedlichen Quellen erfasst und transformiert und diese an angebundene Analyse-Tools sendet, wie Elasticsearch. Die Funktionen zur Datenaufbereitung sind eine der Stärken von Logstash, da Unternehmen hiermit Daten beispielsweise filtern, normalisieren, anreichern oder pseudonymisieren können. Daten können aus praktisch allen Quellen stammen, wie Logs von Webservern oder Datenbanken, Windows Event-Daten, Netzwerkprotokollen oder IoT-Daten (Internet of Things) von Maschinen und anderen Objekten mit Sensoren, die über eine Internetanbindung verfügen.

Die dritte Komponente Kibana visualisiert Daten mithilfe von Diagrammen und Tabellen. Anwender:innen können damit aussagefähige Dashboards für eine visuelle Analyse definieren inklusive Landkarten, Heatmaps und zahlreichen weiteren Visualisierungen.

Ergänzt wird der ELK-Stack von sogenannten Beats. Diese Agenten sind Software-Tools, die Netzwerkdaten von Windows- oder Linux-Systemen sammeln, analysieren und versenden. Damit lassen sich beispielsweise Metriken zur Auslastung von Systemen und Netzwerken innerhalb der gesamten IT-Infrastruktur erstellen, überwachen und auswerten.

So ist das Materna SOC aufgebaut

Materna definiert die Aufgaben ihres eigenen SOCs sehr breit und kann somit viele unterschiedliche Tätigkeiten aus einer Hand erbringen. Dazu zählt das klassische Log-Management für Operations und Engineering, bei dem Spezialist:innen die aufgetretenen Events analysieren und basierend hierauf Lösungsvorschläge einleiten. Als zentrales Werkzeug nutzen die SOC-Expert:innen die SIEM-Lösung von Elastic und können den Kunden darüber eine ganzheitliche Sicht auf die IT-Security-Maßnahmen geben.

Das SOC bei Materna ist dreistufig aufgebaut und verfügt über Expert:innen für Level 1, Level 2 und Level 3. Während Level 1 meist wiederkehrende IT-Vorfälle aus dem operativen Tagesgeschäft behandelt, greift der Level 3-Support bei einer kritischen und komplexen Gefahrenlage wie einer Ransomware-Attacke ein. Ebenfalls vorhanden sind Expert:innen für Incident Response und digitale Forensik, die eine Spurensicherung im digitalen Raum übernehmen, um beispielsweise Angreifer zu identifizieren oder möglichen Datenverlusten auf die Spur zu kommen. Schließlich übernimmt das SOC bei Materna das Vulnerability Scanning als Service. Hierbei kommen spezielle Software-Werkzeuge zum Einsatz, die systematisch die gesamte IT-Infrastruktur nach potenziellen Sicherheitslücken untersuchen.

Skalierbar durch Cloud-Ressourcen

Mit der optimierten Lastverteilung durch ECE als Cloud-Anwendung wächst das Materna SOC automatisch mit den Anforderungen der Kunden. Mit ECE wird es möglich, praktisch beliebige Cluster aus ELK-Komponenten zu konfigurieren und zu verteilen. So kann Materna passend für jeden Bedarf die benötigte Architektur bereitstellen. Mit Hilfe der ECE-Lösung lassen sich zudem alle Kundensysteme an einem zentralen Ort administrieren. Ein Update des ELK-Stacks oder einzelner Komponenten ist bei dieser Lösung ohne Ausfallzeit durchführbar.

Zukunftssicher

Bei Materna betreibt ein Team von erfahrenen Security-Expert:innen die SIEM-Lösung von Elastic für Kunden aus allen Branchen. Threat Hunter, Malware-Spezialist:innen und weitere Expert:innen stehen für tiefgehende Analysen bereit. Wachsende Datenmengen fängt die Cloud-Plattform flexibel auf, da die Lösung eine verteilte Architektur nutzt und somit größtmögliche Flexibilität und Skalierbarkeit bietet. Modular lassen sich notwendige Features ergänzen, wie zum Beispiel Funktionen für das Machine Learning. Security-Features wie Authentifizierung, rollenbasierte Zugriffssteuerung, Verschlüsselung und SAML (Security Assertion Markup Language) sind in der Plattform ebenfalls enthalten. Eine integrierte Alarmierung sorgt dafür, dass Ereignisse sofort sichtbar sind und somit schnell von den Security-Expert:innen bearbeitet werden können.

Höchste Priorität hat bei Cyber-Angriffen die eigene Geschwindigkeit. Daher ist es so wichtig, die Situation schnell analysieren zu können, um dann erste Maßnahmen einzuleiten.

Abläufe im SOC bei Materna

Nachfolgend beschreiben wir, wie die Security-Expert:innen von Materna auf die Bedrohungslage durch anfällige Mailserver, wie zu Beginn erwähnt, reagiert haben. Die Analyse der Situation startete bei Materna unmittelbar nachdem bekannt wurde, dass die Server angreifbar sind. Die Expert:innen ermittelten zunächst, welche ihrer Kunden überhaupt einen entsprechenden Mailserver betreiben, und ob es sich bei den eingesetzten Systemen um eine anfällige Version handelt. Dann erfolgte ein erster Check, ob der Server in seinen Logfiles bereits verdächtige Aktivitäten erfasst hat.

In Zusammenarbeit mit den Incident Respondern von Materna waren die Kundensysteme nur wenige Stunden nach Veröffentlichung der Meldung durch den Hersteller des Mailservers erfolgreich gepatcht. Zudem konnten die Forensiker:innen des SOCs nach ausführlichen Untersuchungen ausschließen, dass die Server der betreuten Kunden bereits infiltriert waren. Anschließend mussten die Firewalls mit neuen Regeln aktualisiert werden, damit ähnliche Angriffe in Zukunft erkannt werden. Während dieser Phase informierte das SOC fortlaufend die Verantwortlichen auf Kundenseite mit verständlichen Berichten über alle Schritte und Erkenntnisse.

- **So reagieren die Security-Expert:innen von Materna auf unmittelbare IT-Gefahren.**

Tatsächlich stellten die Expert:innen im SOC schon kurze Zeit nach dem Patchen der ersten Kundenserver fest, dass Angreifer versuchten, einige der Systeme zu infiltrieren. Diese Versuche schlugen jedoch fehl, denn die IT-Security war diesmal schneller!

Der geschilderte Vorfall ist nur ein Beispiel dafür, dass ein SOC unerlässlich geworden ist und dabei hilft, ganz unterschiedliche Ziele zu erreichen – das zuverlässige Erkennen von Cyber-Angriffen ist nur ein Aspekt dabei.

SOC als Service beziehen

Für Organisationen, die kein eigenes SOC aufbauen möchten, bietet Materna die Leistungen eines SOCs als komplett gemanagten Service an, der individuell auf die Anforderungen der Kunden anpassbar ist. Bei dem Angebot „SOC as a Service" hostet Materna die SIEM-Plattform in eigenen Rechenzentren in Deutschland und erbringt die Security-Dienstleistungen komplett aus Deutschland; wahlweise in deutscher oder englischer Sprache. Kunden erhalten so Zugriff auf das Fachwissen der Security-Expert:innen von Materna, die über langjährige Erfahrung verfügen und 24/7 im Einsatz sind.

Glossar

Analytics Engine: ist ein Service bzw. eine Software, um Analyseanwendungen zu entwickeln.

BSI: Bundesamt für Sicherheit in der Informationstechnik

ECE: Elastic Cloud Enterprise ist ein Software-Werkzeug, um Installationen der Suchmaschine Elasticsearch zu betreiben.

Elasticsearch: eine Suchmaschine des niederländischen Unternehmens Elastic NV.

Exchange: weit verbreiteter Mailserver von Microsoft.

Heatmap: ein Diagramm zur Visualisierung von Daten, um mögliche Probleme schnell visuell identifizieren zu können.

HIPAA: Health Insurance Portability and Accountability Act ist ein US-Gesetz, das die Sicherheit und den Datenschutz im Zusammenhang mit Patientendaten regelt.

Incident Response: Reaktion auf Angriffe oder IT-Ausfälle durch IT-Expert:innen.

IT-Policy: betriebliche Regeln im Umgang und der Nutzung von IT-Systemen.

Kibana: browserbasierte Open-Source-Analyseplattform zur Visualisierung von Daten, die auf der Suchmaschine Elasticsearch aufbaut.

KRITIS: Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall Versorgungsengpässe oder Störungen der öffentlichen Sicherheit zu befürchten sind.

Logdaten: Logdaten sind die Daten, die beim Logging anfallen und in Logfiles gespeichert werden, wie zum Beispiel eine Protokolldatei.

Logstash: Open-Source-Software zur Erfassung, Transformation und Weiterleitung von Daten, die zusammen mit Elasticsearch und Kibana den Elastic-Stack bildet, über den Nutzer:innen große Datenmengen analysieren und visualisieren können.

Machine Learning: maschinelles Lernen ist ein Teilgebiet der Künstlichen Intelligenz und kann durch Software Muster in Datenbeständen erkennen, um so z. B. über Abweichungen des Normalbetriebs frühzeitig zu informieren.

NIST: National Institute of Standards and Technology ist eine US-Behörde, die die Standardisierung vorantreibt, unter anderem im Bereich der IT bzw. IT-Sicherheit.

PCI: Payment Card Industry Data Security Standard, abgekürzt mit PCI bzw. PCI-DSS, ist ein Regelwerk im Zahlungsverkehr rund um die Abwicklung von Kreditkartentransaktionen.

Ransomware: Schadprogramme, die den Computer sperren oder Daten verschlüsseln. Täter erpressen ihre Opfer und verlangen Lösegeld zur Freigabe der Daten.

SAML: Security Assertion Markup Language ist ein offener Datenstandard, mit dem Autorisierungsdaten bzw. Anmeldeinformationen sicher zwischen Anwendungen und IT-Systemen ausgetauscht werden können, damit sich beispielsweise Nutzer:innen bei mehreren Webseiten anmelden können.

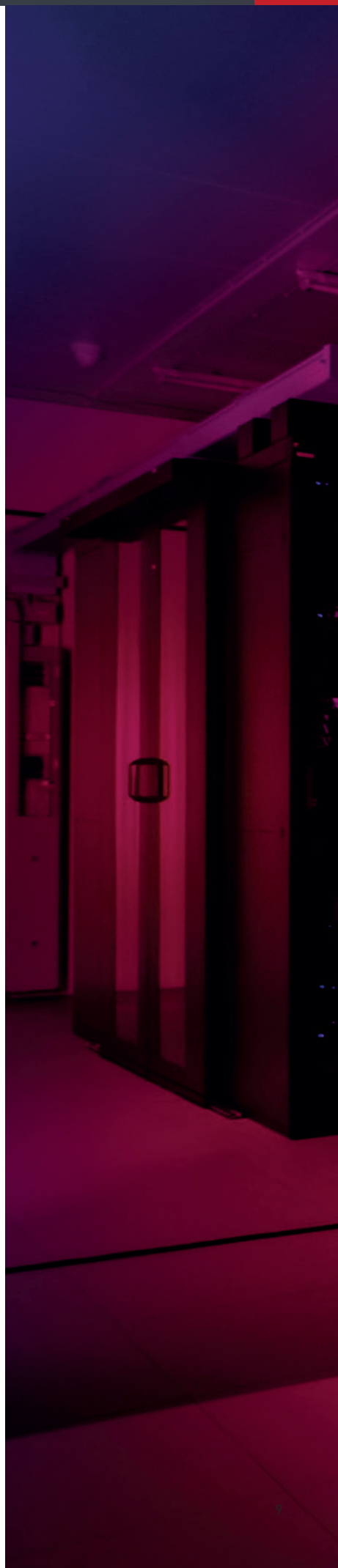
SIEM: Security Incident und Event Management ist eine Software-Anwendung, die einen ganzheitlichen Blick auf die IT-Infrastruktur unter dem Aspekt der IT-Sicherheit gibt. Meldungen und Logfiles verschiedener Systeme werden hier gesammelt und ausgewertet, sodass IT-Expert:innen schnell verdächtige Ereignisse erkennen können.

SOC: Eine Sicherheitsleitstelle für den IT-Betrieb von Organisationen, um die IT und Daten vor internen und externen Gefahren zu schützen.

Threat Hunter: Ein Sicherheitsexperte, der die gesamte IT inklusive Netzwerke nach potenziellen Bedrohungen durchsucht, wie nach Angreifern, die sich bereits Zugriff verschafft haben, aber sich aktuell noch still verhalten.

Vulnerability Scanning: Systematische Analyse der gesamten IT auf mögliche Schwachstellen, ausgeführt mit spezialisierten IT-Werkzeugen, die unter anderem auf Datenbanken mit bekannten Sicherheitslücken zurückgreifen.

Zero Day: der Begriff steht für Sicherheitslücken, die Hacker neu entdeckt haben. Hersteller haben gerade erst von diesem Fehler erfahren und haben damit „Null Tage“ (Zero Days) Zeit, ihn zu beheben.



Links

Bitkom: Rekordschäden durch organisierte Kriminalität
www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

BSI: Alarmstufe Rot
www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html

YesWeHack: Cybersecurity Studie
www.com-magazin.de/news/sicherheit/siebte-unternehmen-it-sicherheitsmass-nahmen-2668573.html

Kaspersky: viele Unternehmen ohne SOC
www.kaspersky.com/blog/it-security-economics-2020-part-4/

(ISC)2: IT-Security-Expert:innen fehlen
www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145

Elastic: Entwickler einer SIEM-Plattform
www.elastic.co/de/

Das SOC von Materna

- Materna bietet ein Security Operations Center als komplett gemanagten Service an, maßgeschneidert auf die Anforderungen und Bedürfnisse der Kunden.
- Materna hostet die Lösung in eigenen Rechenzentren in Deutschland und erbringt den Service komplett aus Deutschland und in deutscher oder auf Wunsch in englischer Sprache.
- Mit dem Service profitieren Kunden von Security-Expert:innen mit mehrjähriger Erfahrung.
- Security-Analyst:innen, Architekt:innen und Engineers von Materna überwachen 24 Stunden am Tag, sieben Tage die Woche die Sicherheit.

Sie haben Fragen an unseren Experten?

Eugenio Carlon,
Vice President
Cyber Security & Defence

Schreiben Sie einfach an sales@materna.de.

MATERNA
Information & Communications

Kontakt
Materna Information & Communications SE
Voßkuhle 37, 44141 Dortmund
Tel.: +49 231 5599-00
E-Mail: marketing@materna.de
www.materna.de

Über Materna
Materna deckt das gesamte Leistungsspektrum eines Full-Service-IT-Dienstleisters im Premium-Segment ab: von der Beratung über Implementierung bis zum Betrieb. Kunden sind IT-Organisationen sowie Fachabteilungen in Privatwirtschaft und Verwaltung.