infopulse
Part of Tietoevry Group

eBook

SOC-Einführung: Drei Szenarien für eine bessere Sicherheitslage

infopulse
Part of Tietoevry Group

Inhaltsverzeichnis

Im vergangenen Jahr haben Unternehmen auf der ganzen Welt bei der Digitalisierung einen großen Sprung nach vorn gemacht. Die massive Umstellung auf Remote-Arbeit und die rasche Einführung neuer Technologien führten zu einer größeren Belastung der Sicherheitsteams.

59% der Befragten gaben an, dass ihr Unternehmen in den letzten 12 Monaten mit einem wesentlichen oder bedeutenden Vorfall im Bereich der Cybersicherheit konfrontiert war.

EY Global Information Security Survey 2020

Viele Führungskräfte sahen sich nicht ausreichend auf die Kehrseite der Digitalisierung vorbereitet - ein erweitertes Portfolio an digitalen Assets und Endpunkten, die einen robusten Schutz und eine 24/7-Überwachung erfordern.

Die in der Cloud entstandene und cloudbasierte IT-Infrastruktur muss verstärkt werden. Bei älteren und lokalen Systemen sind ebenfalls regelmäßige Sicherheitspatches und Wartungsarbeiten erforderlich. Neu eingerichtete und erweiterte Datenspeicher müssen entsprechend den Industriestandards gesichert werden. Gleichzeitig sind die Sicherheitsteams (und oft auch einzelne IT-Mitarbeiter) bereits mit der Unterstützung von Remote-Mitarbeitern überfordert.

Um die immer größer werdende Lücke zwischen den IT-Sicherheitsfunktionen und den aktuellen betrieblichen Anforderungen zu schließen, erwägen immer mehr Führungskräfte die Einführung eines Security Operations Center (SOC). In diesem eBook bieten wir einen detaillierten Einblick in die Einführung, Einrichtung und Verwaltung von SOCs.

infopulse
Part of Tietoevry Group

Was ist SOC?

SOC-DIENSTLEISTER FÜHREN AUCH REGELMÄSSIGE BEWERTUNGEN DER ALLGEMEINEN SICHERHEITSLAGE DES UNTERNEHMENS DURCH

Das Security Operations Center (SOC) ist eine spezielle Geschäftseinheit, die nach festgelegten Verfahren arbeitet und Technologien einsetzt, um Vorfälle im Bereich der Cybersicherheit kontinuierlich zu überwachen, zu analysieren, darauf zu reagieren und zu verhindern.

In ihrer Funktion als Knotenpunkt übernehmen die SOC-Teams die volle Kontrolle über die im Voraus festgelegten sicheren Betriebsverfahren (SOPs), um so viel wie möglich von der technischen Umgebung und der Infrastruktur des Unternehmens zu erhalten und die Einhaltung der gesetzlichen Normen zu gewährleisten. SOC-Teams sind für die Überwachung der Infrastruktur des Unternehmens (vor Ort und in der Cloud), der Netzwerke, der angeschlossenen Geräte und des Datenaustauschs zwischen ihnen verantwortlich.

SOC-Dienstleister übernehmen nicht nur die Rolle des “Wächters”, sondern führen auch regelmäßige Bewertungen der allgemeinen Sicherheitslage des Unternehmens durch und schlagen weitere Verbesserungen als Reaktion auf neue Bedrohungen vor.

infopulse
Part of Tietoevry Group

Zu den Aufgaben des SOC eines Unternehmens gehören:

- Proaktive Sicherheitsüberwachung
- Ausarbeitung und Durchführung eines Notfallmanagementplans
- Reaktion auf Bedrohungen und Abhilfemaßnahmen
- Log-Management
- Priorisierung, Verwaltung und Reaktion auf Alarme
- Analyse der Grundursache
- Bewertung und Management von Schwachstellen
- Härtung der Infrastruktur und des Netzes

Im Wesentlichen legen SOC-Teams das Protokoll für die präventive Sicherheitswartung fest und handeln entsprechend. Proaktive Erkennungs- und Reaktionsmechanismen für Cybersicherheitsvorfälle sollten bereits vor der Einrichtung der Cybersicherheitsabteilung des SOC vorhanden sein.

infopulse
Part of Tietoevry Group

Wie funktioniert das SOC?

infopulse
Part of Tietoevry Group

Das SOC steht an der vordersten Front der Unternehmenssicherheit und überprüft die Unternehmensanforderungen rund um die Uhr auf Bedrohungen, Schwachstellen, Verstöße und Nichteinhaltung von Vorschriften. Das SOC übt in erster Linie Aufsichts- und Ermittlungsfunktionen aus. Die Einheit fungiert als sekundäre Struktur für die grundlegenden IT-Sicherheits- und Cybersicherheitsteams und -prozesse.

IT-SICHERHEIT

Menschen, Prozesse und Technologie, die darauf abzielen, die IT-Assets des Unternehmens vor internen Vorfällen wie versehentlichen Datenverletzungen, Insider-Angriffen, Fehlkonfigurationen und Nichteinhaltung von Vorschriften zu schützen.

CYBERSICHERHEIT

Menschen, Prozesse und Technologie zum Schutz von Organisationen vor gezielten Angriffen (Hacking) und externen Sicherheitsbedrohungen (Malware, DDoS-Angriffe usw.).

Das SOC fungiert als Kontrollinstanz, die sicherstellt, dass alle IT-Sicherheits- und Cybersicherheitsrichtlinien vorhanden sind, ordnungsgemäß umgesetzt und regelmäßig als Reaktion auf neue Bedrohungen aktualisiert werden. Neben der Kontrolle erfüllt ein gut eingerichtetes SOC auch die folgenden vier grundlegenden Funktionen:

1

ÜBERWACHUNG

SOC-Teams analysieren die gesamte IT-Umgebung und sorgen für einen hohen Endpunktschutz vor internen und externen Bedrohungen. Mit einer Reihe von Tools zur Erkennung von Assets, zum planmäßigen Scannen der Infrastruktur und zur Echtzeitüberwachung sorgen SOC-Teams dafür, dass potenzielle Bedrohungen und andere verdächtige Aktivitäten frühzeitig erkannt werden.

2

JAGD AUF UND PRÄVENTION VON BEDROHUNGEN

Mit einem passenden Toolkit und einer Rund-um-die-Uhr-Verfügbarkeit kann ein SOC-Team aufkommende Bedrohungen proaktiv erkennen und gezielte Folgemaßnahmen planen - Sicherheits-Patches, Richtlinienanpassungen, individuelle Risikobehandlungspläne oder die Implementierung neuer Sicherheitssysteme.

3

UNTERSUCHUNG UND AUFDECKUNG VON BEDROHUNGEN

Alle von den SOC-Teams gesammelten Bedrohungsdaten werden weiter analysiert und in neue Sicherheitsinformationen für das Unternehmen umgesetzt. Anhand der gesammelten Informationen über die Art, den Ursprung und die potenziellen Auswirkungen der Bedrohung können die SOC-Analysten neue Empfehlungen für die Systemhärtung, die Behebung von Schwachstellen und die Aktualisierung des Sicherheitsprogramms entwickeln.

4

REAKTION

Ausgestattet mit ausreichenden Daten und einem leistungsstarken Toolkit kann ein SOC-Team schnell auf die ausgeklügeltsten Angriffe reagieren, Bedrohungen isolieren und die Auswirkungen auf den Geschäftsbetrieb und sensible Daten abmildern.

62%

Der Sicherheitsvorfälle sind auf Fahrlässigkeit zurückzuführen[1]

$11.45 Millionen

Durchschnittliche Kosten der Bedrohungen durch Insider[2]

$368 Millionen

Durchschnittliche Gesamtkosten durch eine Datenschutzverletzung[3]

280 Tage

Durchschnittliche Zeit zur Erkennung und Eindämmung einer Sicherheitsverletzung[4]

[1] Observe IT: 2020 Cost of Insider Threats Global Report
[2] Ibid.
[3] IBM: Cost of a Data Breach Report 2020
[4] Ibid.

infopulse
Part of Tietoevry Group

Arten von SOC-Operationen nach Reifegraden

Vorhandene Fähigkeiten	Stufe 1	Stufe 2	Stufe 3	Stufe 4	Stufe 5
	Grundlegende Sicherheitsüberwachung und Reaktion Ad-hoc-Protokolldatenerfassung und -verwaltung Reaktion auf Endpunkt-Erkennung auf Einstiegsstufe	Zentralisierung von Sicherheitsereignissen Reaktive Workflows für Bedrohungsdaten Grundlegende Sicherheitsanalytik Automatisierte Priorisierung von Warnmeldungen Manuelle Schwachstellenbewertungen	Dokumentierter Überwachungsprozess Analytik-basierte Bedrohungsanalyse Management von Zwischenfällen und Reaktionspläne Proaktive Bedrohungserkennung Proaktive Bedrohungsidentifizierung Automatisierte Arbeitsabläufe für die Untersuchung von Bedrohungen	Konsolidierte Protokolldaten und Zentralisierung von Sicherheitsereignissen Server-, Endpunkt- und Netzwerk-Forensik Ausgereifte Verfahren zur Erkennung von und Reaktion auf Bedrohungen ML/DL-basierte Tools zur Reaktion auf Bedrohungen KPI/SLA-basierte Leistung	Rund-um-die Uhr Sicherheitsüberwachung, Präventions- und Detektionssysteme Proaktive Fähigkeiten zur Erkennung und Behebung von Schwachstellen Ausgereifte SIEM-Architektur, SIEM-Protokollquellen, SIEM-Korrelationsregeln Funktionsübergreifende Integration Bedrohungsinformationen in Echtzeit Automatisierung von Arbeitsabläufen und Reaktionen Proaktive und iterative Fähigkeiten zur Bedrohungssuche Starke SOC-Programmsteuerung

infopulse
Part of Tietoevry Group

VOR DER IMPLEMENTIERUNG VON SOC, SOLLTEN SIE MIT EINEM AUDIT DER BESTEHENDEN SICHERHEITSPROZESSE BEGINNEN

Die Ergebnisse und Erfolgsquoten der SOC-Einführung korrelieren stark mit dem allgemeinen Reifegrad des Unternehmens in Bezug auf Sicherheit und ITIL-Service-Management. **In Anbetracht der Komplexität der SOC-Implementierung empfehlen wir unseren Kunden immer, mit einer Vorprüfung der bestehenden Sicherheitsprozesse, der technischen Möglichkeiten und des Sicherheitsbedarfs zu beginnen.**

Auf der Grundlage der obigen Ausführungen variieren die Unternehmen zwischen Stufe 1 und Stufe 5 in Bezug auf die Sicherheitsreife - und die Bereitschaft für verschiedene Arten von SOC-Einführungsszenarien.

infopulse
Part of Tietoevry Group

Stufe 1

Die Unternehmen verfügen bereits über die folgenden Sicherheitskontrollen:

- Grundlegende Sicherheitsüberwachung und -reaktion, abgestimmt auf die Compliance-Anforderungen
- Ad-hoc-Protokolldatenerfassung und -verwaltung
- Reaktion auf Endpunkt-Erkennung auf Einstiegsstufe
- Keine formellen Reaktions- und Managementpläne für Zwischenfälle

Diese Unternehmen haben die Mindestsicherheitsanforderungen erfüllt. Sie sind jedoch nicht in der Lage, wirksam auf gezielte Angriffe zu reagieren und bleiben anfällig für Verletzungen durch Insider. In den meisten Fällen ist der niedrige Reifegrad darauf zurückzuführen, dass es an Sicherheitsspezialisten und Fachwissen fehlt, um eine effektive Erkennung, Priorisierung und Verwaltung von Bedrohungen zu ermöglichen.

EMPFOHLENES SOC-EINFÜHRUNGSSZENARIO:

- Sicherheitsbewertung
- Identifizierung von Assets, Einschätzung des Risikoniveaus, Definition von Anwendungsfällen und Reaktionsszenarien
- Gemeinsam genutztes oder fest zugeordnetes SOC-as-a-Service.
- Dokumentation und Systematisierung der internen Prozesse

infopulse
Part of Tietoevry Group

Stufe 2

In diesem Stadium verlassen sich die Unternehmen auf manuelle und proaktive Bedrohungsabwehr, doch es fehlt an Standardisierung. Dies führt häufig zu einer sporadischen Sicherheitsberichterstattung und einer langwierigen Reaktion auf Sicherheitsvorfälle.

Auf Stufe 2 verfügen Unternehmen bereits über:

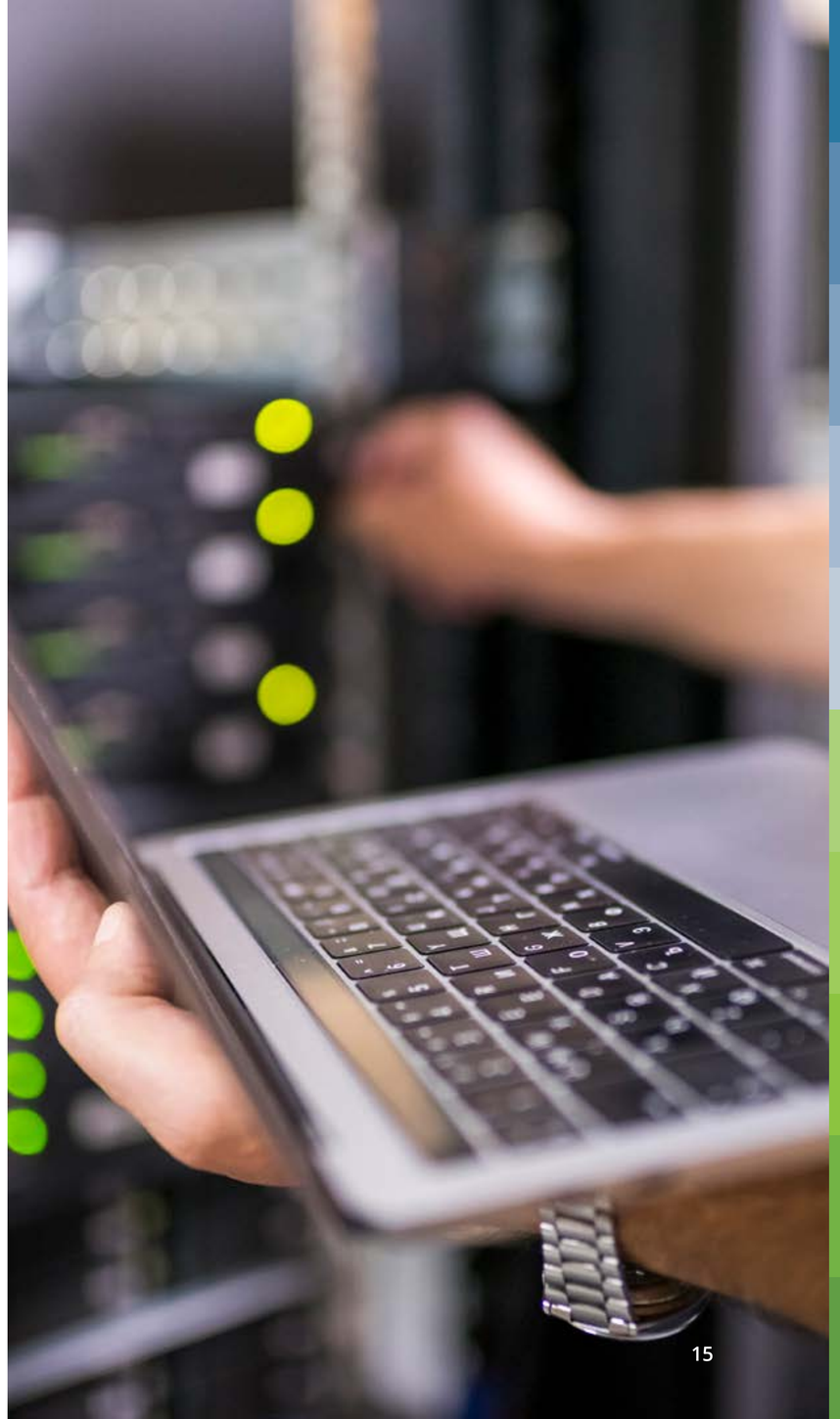
- Etablierte Fähigkeiten zur Zentralisierung von Sicherheitsereignissen
- Reaktive Workflows für Bedrohungsdaten
- Analysefähigkeiten auf Einstiegsniveau
- Automatisierte Priorisierung von Warnmeldungen
- Manuelle Schwachstellenbewertung.

All dies führt zu einem höheren Maß an Sicherheit. Das Unternehmen ist in der Lage, größere Bedrohungen zu erkennen und nicht nur die ersten Anzeichen einer Verletzung oder Gefährdung zu identifizieren.

Sicherheitsteams haben immer noch blinde Flecken, vor allem, wenn es um ausgeklügelte Angriffe geht. Die Sichtbarkeit interner und externer Bedrohungen ist mäßig.

EMPFOHLENES SOC-EINFÜHRUNGSSZENARIO:

- IT-Sicherheitsbewertung, einschließlich des bestehenden Infrastruktur-Ereignis-Managements
- Beratung zu Cybersicherheit
- Kosteneffizienter Ansatz für die Datenerfassung und -verarbeitung
- Risikobewertung
- Überwachung geschäftskritischer Assets
- Dokumentation von grundlegenden Prozessen, Verfahren und Zuständigkeiten
- Gemeinsam genutztes oder fest zugeordnetes SOC-as-a-Service



infopulse
Part of Tietoevry Group

Stufe 3

Unternehmen der Stufe 3 verlassen sich auf dokumentierte, konsistente Best Practices für die Sicherheit und nutzen Sicherheitstools, um sich wiederholende Aufgaben zu rationalisieren.

Das Leistungsspektrum umfasst:

- Formalisierter Überwachungsprozess
- Analytik-basierte Bedrohungsanalyse
- Etablierte Notfallmanagement- und Reaktionspläne
- Eine breitere Palette an Funktionen zur Erkennung von Bedrohungen
- Proaktive Bedrohungsidentifizierung
- Automatisierte Arbeitsabläufe für die Untersuchung von Bedrohungen

SOC-Lösungen und -Teams können an diesem Punkt effektiv eingesetzt werden, um weitere betriebliche Verbesserungen in Bezug auf Transparenz, Absicherung und proaktive Überwachung zu erzielen. Unternehmen der Stufe 3 sind gut in der Lage, Vorfälle frühzeitig zu erkennen, benötigen aber unter Umständen eine längere Reaktionszeit, da es ihnen an funktionsübergreifenden Koordinierungsmöglichkeiten mangelt.

EMPFOHLENES SOC-EINFÜHRUNGSSZENARIO:

- Sicherheitsbewertung
- Definition und Messung von KPIs für einen formalisierten Überwachungsprozess
- Nutzung kommerzieller Bedrohungsmeldungen
- Kosteneffizienter Ansatz für die Datenerfassung und -verarbeitung
- SOC-as-a-Service oder SOC-Delegierung

infopulse
Part of Tietoevry Group

Stufe 4

Unternehmen der Stufe 4 können dank eines gut dokumentierten Reaktionsprozesses, der durch automatisierte Tools für die Erkennung, Untersuchung und Analyse von Bedrohungen unterstützt wird, entschieden auf eine Vielzahl von Sicherheitsvorfällen reagieren.

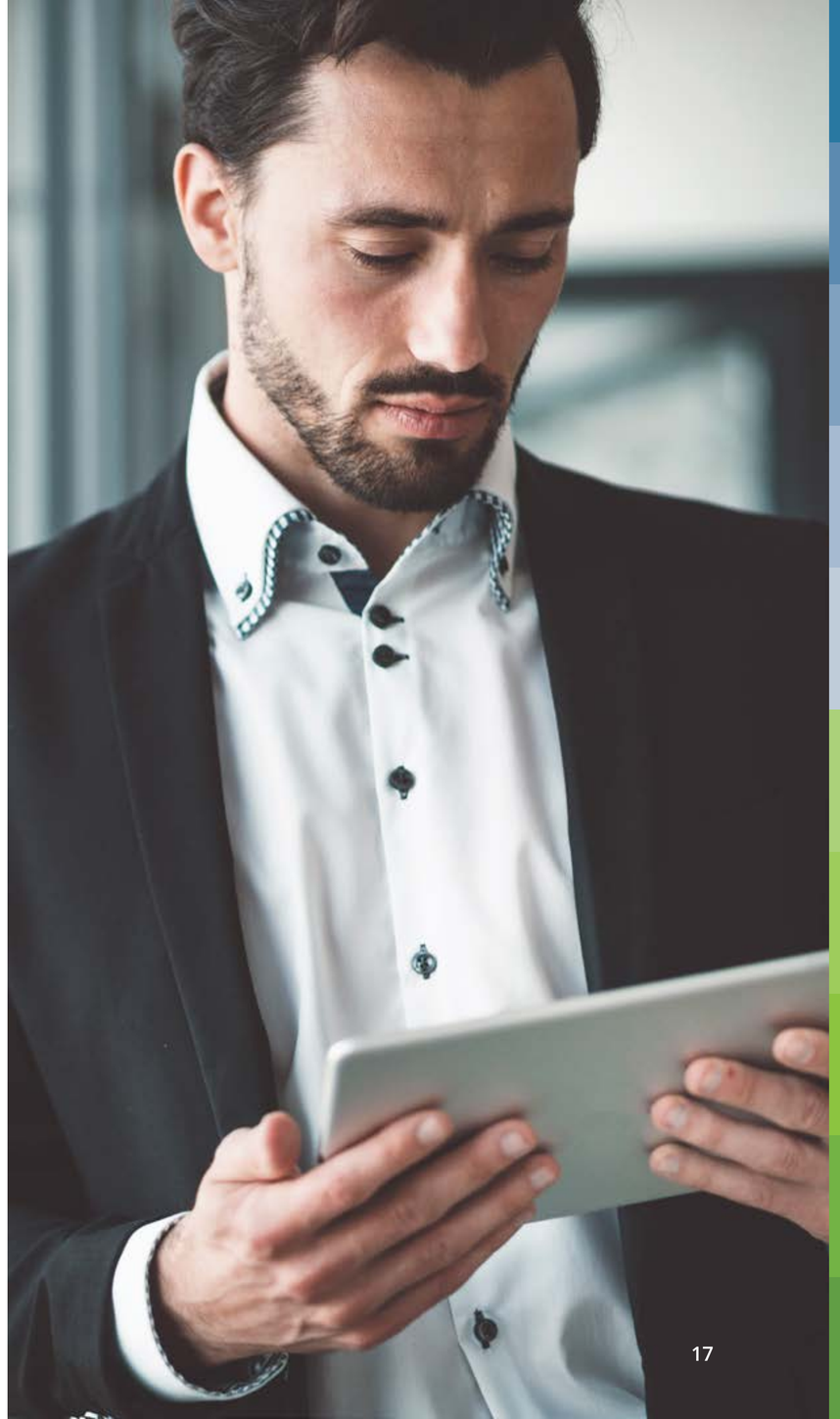
Die folgenden Sicherheitsaspekte sind vorhanden:

- Konsolidierte Protokolldaten und Zentralisierung von Sicherheitsereignissen
- Server-, Endpunkt- und Netzwerk-Forensik
- Ausgereifte Verfahren zur Erkennung von und Reaktion auf Bedrohungen
- Lösungen für Machine Learning zur Erkennung von Anomalien
- KPI/SLA-basierte Leistungsfunktionen

Unternehmen der Stufe 4 sind in der Lage, aufkommende Bedrohungen bereits im Anfangsstadium zu erkennen und effektiv untereinander zusammenzuarbeiten, um unternehmensweite Sicherheitsverbesserungen zu erzielen. Solche Unternehmen haben wahrscheinlich auch 24/7-SOC-Teams vor Ort oder verlassen sich auf einen Anbieter von SOC-as-a-Service.

EMPFOHLENES SOC-EINFÜHRUNGSSZENARIO:

- Sicherheitsbewertung
- Automatisierung der Reaktion auf Bedrohungen
- Kosteneffizienter Ansatz für die Datenerfassung und -verarbeitung
- Nutzung von Überwachungsdaten für fundierte Entscheidungen
- SOC-as-a-Service oder SOC-Delegierung



infopulse
Part of Tietoevry Group

Stufe 5

Sicherheit ist eine unternehmensweite Aufgabe, die von allen Beteiligten aktiv unterstützt wird. Unternehmen der Stufe 5 nehmen eine proaktive Haltung in Bezug auf Bedrohungsmanagement und Sicherheit ein. Sie verfügen über:

- Eine unternehmensweite Agenda zur Gewährleistung einer bestimmten Sicherheitsstufe und zur kontinuierlichen Verbesserung
- 24/7-Sicherheitsüberwachung, Präventions- und Detektionssysteme
- Proaktive Fähigkeiten zur Erkennung und Behebung von Schwachstellen
- Eine ausgereifte SIEM-Architektur und unterstützende SOC-Technologien, um die Effizienz ihrer Mitarbeiter zu maximieren.

Unternehmen der Stufe 5 sind in der Regel in regulierten Branchen tätig, z. B. im Finanz-, Telekommunikations- und Gesundheitswesen, und ihr Streben nach exzellenter Sicherheit wird auch durch gesetzliche Vorschriften und Compliance-Anforderungen bestimmt. Sie sind auch ein bevorzugtes Ziel für Cyberkriminelle, verfügen aber über die nötige Widerstandsfähigkeit, um gezielten Angriffen zu widerstehen und neuen Bedrohungen einen Schritt voraus zu sein.

EMPFOHLENES SOC-EINFÜHRUNGSSZENARIO:

- Beratung zu Cybersicherheit
- CIRT (Cyber Incidents Response Team)-Kooperation mit Behörden und anderen Unternehmen
- Proaktive Erkennung von Zero-Day-Bedrohungen
- SOC-Delegierung oder SOC-Wartung

infopulse
Part of Tietoevry Group

Drei Wege zur Einführung von SOC in Ihrem Unternehmen

Traditionell war die SOC-Implementierung eine Option, die transnationalen Unternehmen vorbehalten war, die über beträchtliche Budgets für die Einrichtung interner Abläufe verfügten. In den letzten Jahren haben sich jedoch alternative SOC-Einführungsszenarien herausgebildet, die ein besseres Preis-Leistungs-Verhältnis und geringere betriebliche Herausforderungen bei der Implementierung bieten.

In diesem Kapitel erörtern wir **drei Wege zur Einführung von SOC:**

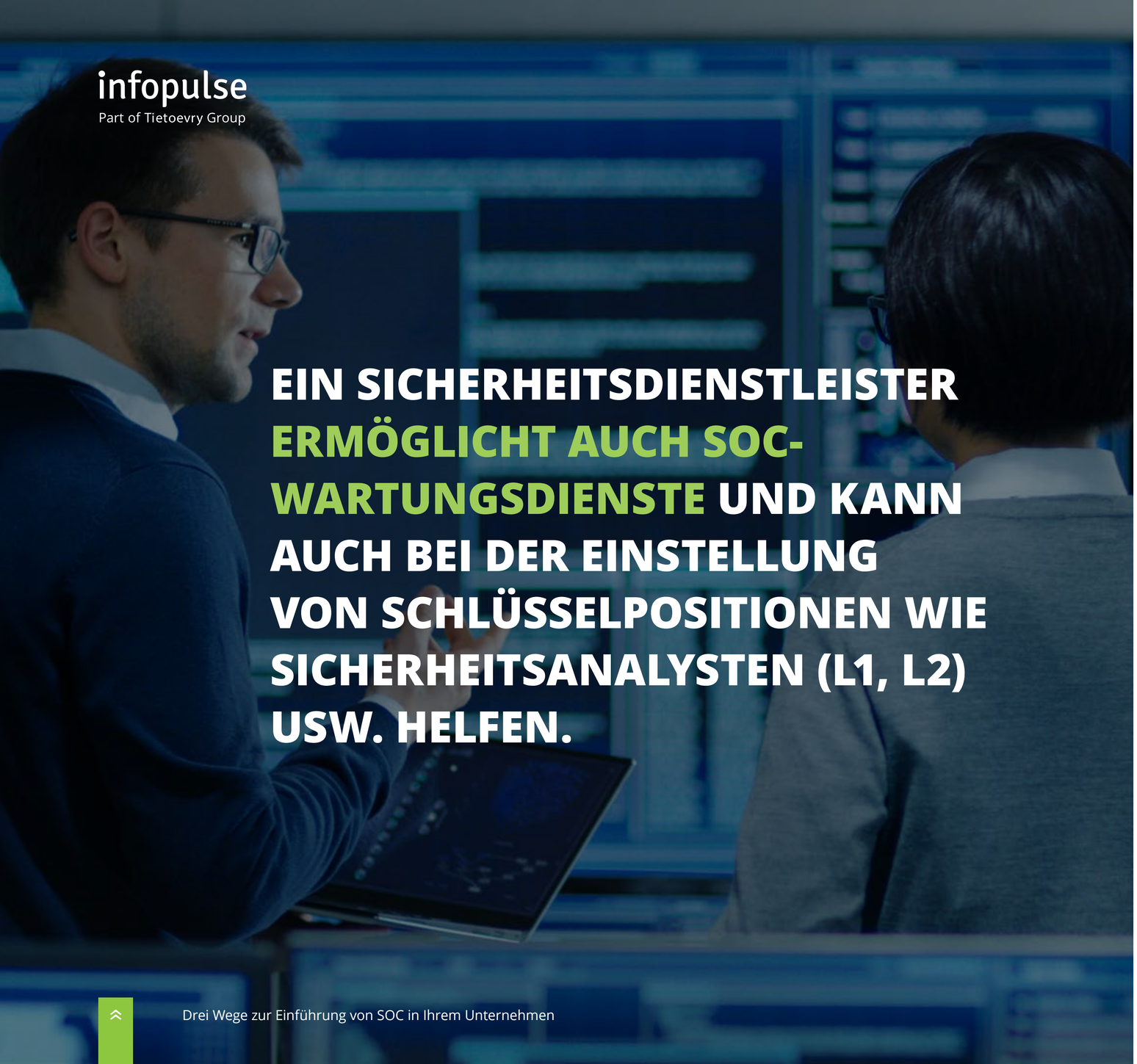
- Interne SOC-Einrichtung und -Wartung
- Outsourcing der SOC-Wartung
- Managed SOC

SOC-BETRIEB - EINRICHTUNG UND WARTUNG

Wie der Name schon sagt, geht dieses SOC-Einführungsmodell von einer proaktiven Beratung zur SOC-Einführung aus. Ein erfahrener Sicherheitsdienstleister führt eine Bewertung Ihrer aktuellen Prozesse, Infrastruktur und Compliance-Anforderungen durch, um notwendige Sicherheitsverbesserungen, betriebliche Änderungen und Sicherheitsinvestitionen vorschlagen zu können.

Solche “Build”-Szenarien setzen Unterstützung bei den folgenden Punkten voraus:

- Formalisierung der Liste der wichtigsten SOC-Servicefunktionen, die die täglichen Prozesse und Verfahren für die Mitarbeiter leiten werden.
- Bestimmung aller erforderlichen Prozesse und Dienste, die zur Unterstützung der Sicherheitsabläufe im Unternehmen erforderlich sind (je nach Unternehmensgröße, Branche und Kundenstamm unterschiedlich).
- Festlegung der optimalen SIEM-Architektur, Identifizierung des erforderlichen Toolkits und Erstellung einer nach Prioritäten geordneten Liste von Investitionen in Sicherheitstechnologien.
- Entwicklung eines SOC-Besetzungsplans, Formalisierung der erforderlichen Rollen und der mit jeder Rolle verbundenen Verantwortlichkeiten. Schaffung einer abgestuften SOC-Struktur und Zuweisung von Verantwortlichen für die Verwaltung verschiedener Ereignisarten.
- Erstellung einer Reihe interner Vorschriften, z. B. Playbooks, Richtlinien, Verfahren, Eskalations- und Managementpläne, um den SOC-Betrieb zu standardisieren und die Reaktion und Abdeckung zu gewährleisten.
- Vorschlagen von Workflow-Automatisierungsszenarien und Investitionen in erstklassige prädiktive Sicherheitsanalyselösungen oder Algorithmen zur Erkennung von Anomalien.
- Begleitung des Übernahmeprozesses und Erleichterung der Anpassung des neu eingerichteten SOC-Teams an die unternehmensweiten ITIL-Service-Management-Standards.



infopulse
Part of Tietoevry Group

EIN SICHERHEITSDIENSTLEISTER ERMÖGLICHT AUCH SOC-WARTUNGSDIENSTE UND KANN AUCH BEI DER EINSTELLUNG VON SCHLÜSSELPOSITIONEN WIE SICHERHEITSANALYSTEN (L1, L2) USW. HELFEN.

GESCHÄFTSSZENARIO

Ein transnationales Telekommunikationsunternehmen verfügt bereits über ein etabliertes Network Operations Center (NOC), das für die Überwachung von und die Reaktion auf Bedrohungen, zuständig ist, welche von Netzwerkgeräten ausgehen. Für die Sicherheit der internen Geschäftsanwender ist die IT-Abteilung zuständig. Beide Abteilungen sind jedoch personell unterbesetzt, haben nur einen begrenzten Einblick in die Abläufe der jeweils anderen Abteilung und erbringen keine ausreichenden Leistungen, wenn es darum geht, externe oder interne Bedrohungen zu analysieren und einen 24/7-Bedrohungsschutz zu gewährleisten.

WIE SOC HELFEN KANN

In einem solchen Fall könnte die Einrichtung eines SOC-Teams dazu **beitragen, die bestehenden Sicherheitsanstrengungen zu konsolidieren, einen besseren Einblick** in die gesamte Infrastruktur **zu erhalten und die Fähigkeiten zur Untersuchung**, Eindämmung und Abwehr **von Bedrohungen zu verbessern**. Wenn die SOC-Kernfunktionen von einem externen Dienstleister ausgeführt werden, können sich die internen Teams besser auf die Gewährleistung der grundlegenden Benutzersicherheit, die rechtzeitige Umsetzung neuer Sicherheitsrichtlinien und hohe Standards bei der Bereitstellung von IT-Diensten für die Benutzer des Unternehmens konzentrieren.

Vorteile

- Fachkundige SOC-Anleitung, die das Risiko von unzureichenden Sicherheitsentscheidungen minimiert
- Akute Beratung zu bestehenden Verfahren und notwendigen Verbesserungen
- Möglichkeit, Ihre Sicherheitsteams mit vom Anbieter bereitgestellten Sicherheitsexperten zu verstärken
- Nachhaltiger, risikoarmer und schneller Aufbau von SOC-Betrieben
- Hohe betriebliche Leistung, gestützt durch etablierte Messgrößen und SLAs
- Die Beibehaltung eines separaten SOC im Unternehmen gewährleistet auch eine höhere Datensicherheit und die Einhaltung von Vorschriften.

Herausforderungen

- **Hohe Reife erforderlich:** Unternehmen mit einem geringen Reifegrad der Cybersicherheit (unter Stufe 4), unzureichendem Sicherheitspersonal und geringer Betriebserfahrung werden Schwierigkeiten haben, eine neue SOC-Einheit nach deren Einrichtung zu betreiben. Unternehmen, die nicht zwischen reaktiven und proaktiven Sicherheitsansätzen unterscheiden können, werden wahrscheinlich nicht von dieser Option profitieren.
- **Starker ITIL-Sicherheitsmanagementprozess:** Unternehmen, die bereits über ein starkes IT-Servicenetz und eine Reihe von Sicherheitsexperten verfügen (oder in der Lage sind, solche einzustellen), sind bessere Kandidaten für eine Ad-hoc-SOC-Implementierung. Durch die Kombination des externen Know-hows bei der Verwaltung von SOC mit ihrem internem Sicherheitswissen kann Ihr Unternehmen schnell auf die nächste Stufe der Sicherheitsoperationen wechseln.
- **Kosten der SOC-Einrichtung.** Die Aufrechterhaltung eines internen SOC-Teams, das rund um die Uhr zur Verfügung steht, ist eine budgetintensive Initiative. Abgesehen von den Grundgehältern sollten Sie auch die Kosten für die Personalbeschaffung, Bonuszahlungen für Urlaubszeiten, Mitarbeiterbindung und Schulung berücksichtigen. Unternehmen mit einem durchschnittlichen Cybersicherheitsbudget von 31 Millionen Dollar geben ein Drittel davon für SOC aus. Daraus folgt, dass interne SOC-Einheiten für alle, aber nicht für landesweite oder globale Organisationen kostenintensiv sein können.

[5] Security Boulevard: Businesses Now Spend a Third of Their Cybersecurity Budget on SOC

infopulse
Part of Tietoevry Group

EINER DER GRÖßTEN
TELEKOMM-BETREIBER
IN DER UKRAINE

FALLBEISPIEL

So legte Infopulse den Grundstein für die SOC-Implementierung

infopulse
Part of Tietoevry Group

Ein landesweiter Telekommunikationsdienstleister plante den Aufbau eines SOC mit einem SIEM-System als Kernstück. Der Kunde beschloss, Azure Sentinel zu testen und seine Fähigkeiten kennenzulernen. Eine wesentliche Anforderung war die effiziente Kontrolle der Ausgaben.

Infopulse führte eine Bewertung der bestehenden IT-Infrastruktur und -Lizenzen durch und glich die Verbindungen aus, wobei der Schwerpunkt sowohl auf den Kosten als auch auf den SOC-Fähigkeiten lag, indem nicht abrechenbare (Microsoft) und abrechenbare (Drittanbieter) Systeme und Lösungen definiert wurden. Die Implementierung umfasste fünf Testfälle:

EINER DER GRÖßTEN TELEKOMM-BETREIBER IN DER UKRAINE

1. **Erkennung von nicht autorisierten Dateikopien aus SharePoint.**
2. **Erkennung von untypischen Benutzerautorisierungen in Cloud-Diensten.** (für Azure AD-Benutzer).
3. **Erkennung von untypischen Benutzerberechtigungen durch Verwendung gesperrter Benutzerkonten** (für Azure AD-Benutzer).
4. **Konfiguration und Prüfung der Erkennung von Phishing-E-Mails** (z. B. Weiterleitung verdächtiger E-Mails durch die Benutzer zur anschließenden Selbstanalyse).
5. **Konfigurieren und Testen eines Falles, der Daten von einer externen Quelle** (z. B. Check Point FW) **verwendet.**

ERGEBNIS

Ein Pilotprojekt demonstrierte die Vorteile von Azure Sentinel als Cloud-native SaaS-Lösung und integriertes SIEM/SOAR mit Automatisierung:

- Getestete und bewiesene Azure Sentinel-Funktionen im Hinblick auf die nahtlose Integration in das Microsoft-Cloud-Ökosystem.
- Optimierung der Kosten der Lösung durch Analyse und Bewertung der Realisierbarkeit von Verbindungen mit den Systemen Dritter.
- Erstellung eines Berichts mit Empfehlungen zu weiteren Umsetzungsschritte

Der Kunde plant nun, Azure Sentinel als Teil seines Security Operations Center zu nutzen.

Kontaktieren Sie unsere Experten, um zu erfahren, wie wir Ihre Sicherheitsausgaben optimieren können

infopulse
Part of Tietoevry Group

OUTSOURCING VON SOC-DIENSTEN

Im Vereinigten Königreich mangelt es in über 48% der Unternehmen an grundlegenden Kenntnissen im Bereich der Cybersicherheit. Das Cybersicherheitspersonal verfügt nicht über ausreichende Fähigkeiten, um die im Rahmen des Cyber Essentials-Programms vorgesehenen Aufgaben zu erfüllen, und wird nicht von einem externen Cybersicherheitspartner unterstützt.

Global gesehen sind die Dinge ebenso komplex. Während 51% der Führungskräfte[7] planen, ihre Teams um weitere Vollzeitkräfte für Cybersicherheit zu erweitern, haben die meisten Schwierigkeiten, geeignete Kandidaten zu finden. Vor allem in den Bereichen Cloud-Sicherheit und Sicherheitsanalyse ist das Angebot am geringsten.

27%

der britischen Unternehmen haben eine Lücke in der Reaktionsfähigkeit auf Zwischenfälle (und lagern diese Aufgabe nicht aus)[8]

30%

der britischen Unternehmen haben Lücken in Bereichen wie Penetrationstests, forensische Analyse und Sicherheitsarchitektur

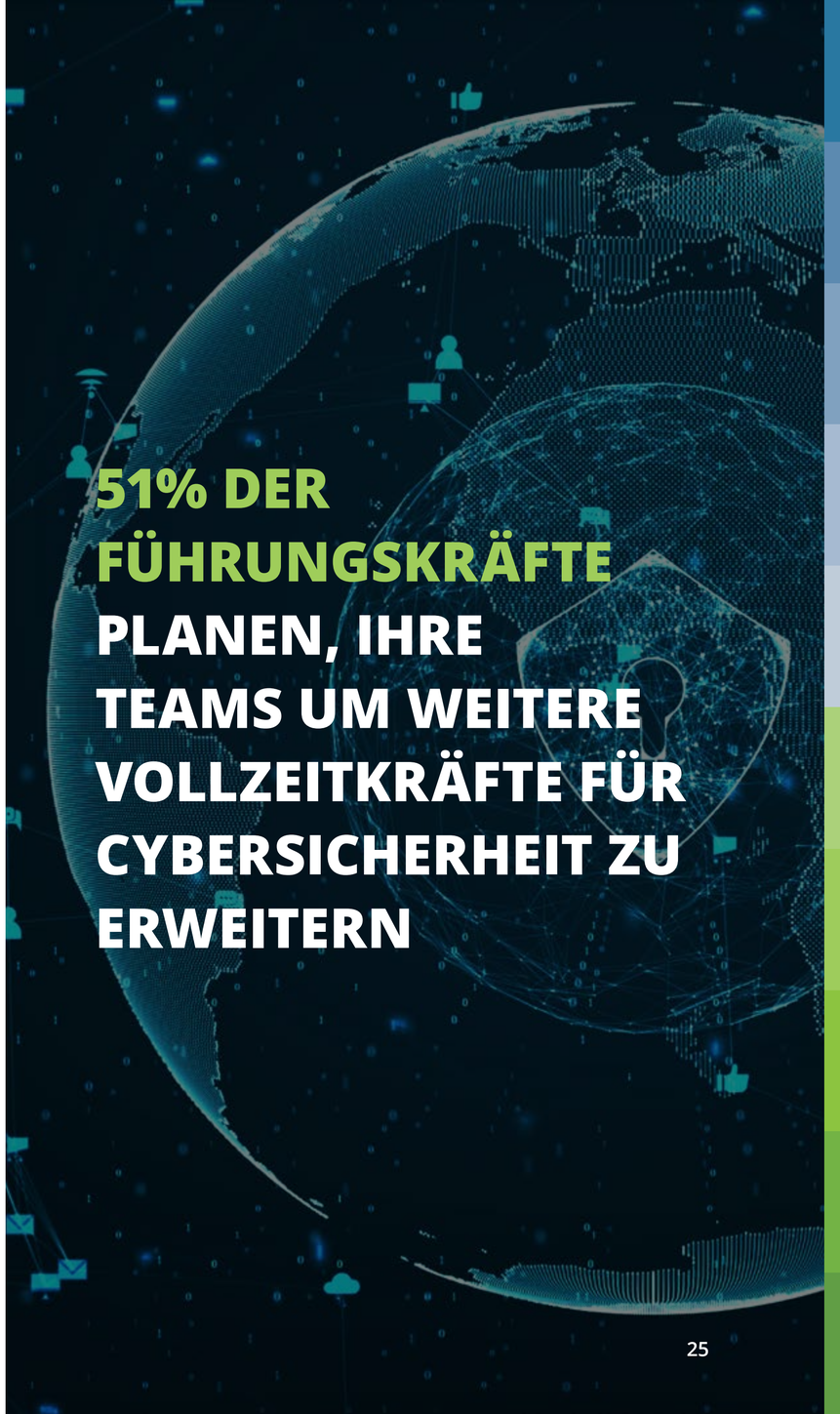
50%

weniger Experten für Cybersicherheit als benötigt, stehen in den USA zur Einstellung zur Verfügung[9]

$3.5 millionen

Jobs im Bereich Cybersicherheit werden bis Ende 2021 voraussichtlich unbesetzt bleiben[10]

[6] Gov.UK: Cyber security skills in the UK labour market 2020
[7] ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2020
[8] Gov.UK: Cyber security skills in the UK labour market 2020
[9] Security Magazine: New research shows US cybersecurity talent shortage
[10] PwC: Global Digital Trust Insights Survey 2021



infopulse
Part of Tietoevry Group

VIELE UNTERNEHMEN ENTSCHEIDEN SICH DAFÜR, SOC-DIENSTE AN EINEN EXTERNEN ANBIETER AUSZULAGERN. DIESER BIETET EINEN BEDARFSGERECHTEN ZUGANG ZU FEHLENDEM FACHWISSEN

Aufgrund des eingeschränkten Zugangs zu Fachkräften entscheiden sich viele Unternehmen dafür, SOC-Dienste an einen externen Anbieter auszulagern. Dieser bietet einen bedarfsgerechten Zugang zu fehlendem Fachwissen und eine kostengünstige Möglichkeit, rund um die Uhr L2/L3-Support zu leisten.

Ein qualifizierter Sicherheitsdienstleister kann bei der Sicherung der Cloud-Infrastruktur, der SIEM/SOAR-Bereitstellung und der Ausführung der festgelegten Anzahl von Anwendungsfällen im Einklang mit den SLAs helfen.

Die Delegierung von SOC-Diensten ist dann sinnvoll, wenn Sie bereits über grundlegende Sicherheitsrichtlinien und -praktiken verfügen, Ihnen aber die Mitarbeiter fehlen, um zeitnahen Support, 24/7-Überwachung und proaktive Bedrohungserkennung zu gewährleisten. Häufig sind Cloud-Migrationen die Voraussetzung für die Einrichtung eines SOC. Mit einer erweiterten Verteidigungsfläche haben interne Teams möglicherweise nicht die Kapazität und das Fachwissen, um die Cloud-Sicherheit neben der lokalen Infrastruktur zu bewältigen.

GESCHÄFTSSZENARIO

Ein Einzelhandelsunternehmen erweiterte seine grenzüberschreitenden Aktivitäten und startete eine neue, in der Cloud gehostete E-Commerce-Website. Das Unternehmen verfügt bereits über genügend L1-Support-Mitarbeiter, um die grundlegenden Ereignisse abzudecken und Kundenanfragen 8x7 zu beantworten. Ein firmeninternes Sicherheitsteam ist für die Wartung des Rechenzentrums vor Ort und die Gewährleistung der IT-Sicherheit der Geschäftsnutzer zuständig.

Allerdings fehlt es dem Unternehmen an Personal und Fachwissen, um rund um die Uhr optimale Cloud-Sicherheit zu gewährleisten. Nach der grenzüberschreitenden Expansion sind ihre Aktivitäten auch anfälliger für externe Bedrohungen (Hacking) geworden, und sie möchten einen proaktiveren Sicherheitsplan aufstellen. Sie verlassen sich auch auf einen maßgeschneiderten Zahlungsprozessor, der zusätzlich gesichert werden muss.

WIE SOC HELFEN KANN

In einem solchen Szenario kann der Dienstanbieter die L2- und L3-Supportdienste an einen externen Anbieter auslagern, **um eine bessere Sicherheitsabdeckung zu erreichen.** Darüber hinaus kann ein SOC-Anbieter dem Einzelhandelsunternehmen dabei helfen, **sein individuelles Zahlungssystem zu sichern,** einen **Schutz** gegen die wichtigsten Angriffsvektoren einzurichten und d**ie gängigen Bedrohungen** mithilfe der installierten SIEM/SOAR-Lösungen **zu überwachen.**

infopulse
Part of Tietoevry Group

Die am häufigsten delegierten SOC-Anwendungsfälle

- L2/L3 24/7-Bereitschaftsdienst
- Automatisierung der Reaktion auf Bedrohungen
- NIDS-Einsatz
- Scannen auf Schwachstellen
- SIEM/SOAR-Einsatz
- Erkennung und Aufklärung von Bedrohungen
- 24/7-Sicherheitsüberwachung
- Überwachung des Netzwerkverkehrs

- Reaktion auf Bedrohungen und Eindämmung
- Erkennung von Anomalien (Benutzerzugriff und -authentifizierung, Exploit, Netzwerk-Baselines)
- Überwachung unbefugter Zugriffe (Benutzer, Geräte, Netzwerke)
- Log-Management

Vorteile

- Umfassende und kostengünstige Sicherheitsabdeckung
- Zugang zu fehlenden Fachkenntnissen und Fähigkeiten
- Geringere Sicherheitsrisiken und Bedrohungslage durch professionelles Management
- SLA-gestützte SOC-Teamleistung
- Fähigkeit zur schrittweisen Umsetzung neuer Sicherheitsaspekte und bewährter Verfahren
- Skalierbarkeit - Erweitern Sie Ihren technischen Fußabdruck, ohne sich um die Wartung zu kümmern.

Herausforderungen

- **Die richtige Dimensionierung des Leistungsumfangs.** SOC ist eine komplexe Einheit. Nicht jede Branche oder jedes Unternehmen muss ein Team hochqualifizierter Sicherheitsanalysten unterhalten, die rund um die Uhr erreichbar sind. Bevor Sie sich für einen Dienstanbieter entscheiden, sollten Sie überlegen, ob Ihr Unternehmen wirklich ein SOC benötigt oder ob es nicht auch mit einer weniger anspruchsvollen Cybersicherheitslösung auskommt. Beispielsweise können die meisten Cloud-Operationen mit nativen SaaS-Tools wie Azure Sentinel, Azure Traffic Monitoring und Azure Security Center effektiv abgesichert werden, wenn Sie Microsoft Azure verwenden, oder mit AWS Control Tower, CloudTrail und AWS Security Hub, wenn Sie die Amazon Web Services nutzen.
- **Auswahl des Dienstleisters.** Die verschiedenen Dienstleister übernehmen ein unterschiedliches Maß an Verantwortung, wenn es um die Delegation von SOC-Diensten geht. Achten Sie beim Vergleich der Leistungsangebote auf den Umfang, die Grenzen und die SLAs, die jeder Anbieter vorschlägt. Der beste Weg, das Risiko einer suboptimalen Vereinbarung zu verringern, ist die Suche nach einem ausgereiften Dienstleister, der ein aufgeschlüsseltes, ergebnisorientiertes Dienstleistungsmodell anbietet.

SOC-AS-A-SERVICE

SOC-as-a-Service ist ein neues Paradigma der SOC-Servicedelegation, das einen “ganzheitlichen” Ansatz für die SOC-Einführung bietet - von der grundlegenden Sicherheitseinrichtung bis zur laufenden Wartung und kontinuierlichen Verbesserung.

Bei Infopulse strukturieren wir die Managed SOC-Services in abgestufte Servicepakete, die sich in Bezug auf den Umfang unterscheiden:

- Anzahl der unterstützten Nutzer und Standorte
- Logs im Paket enthalten
- Verfügbarkeit von L1/L2/L3-Unterstützung
- Antwort-Automatisierung
- Entwicklung und Unterstützung von Kunden-SOC-Anwendungsfällen
- Aufschlüsselung und Arten der Berichterstattung

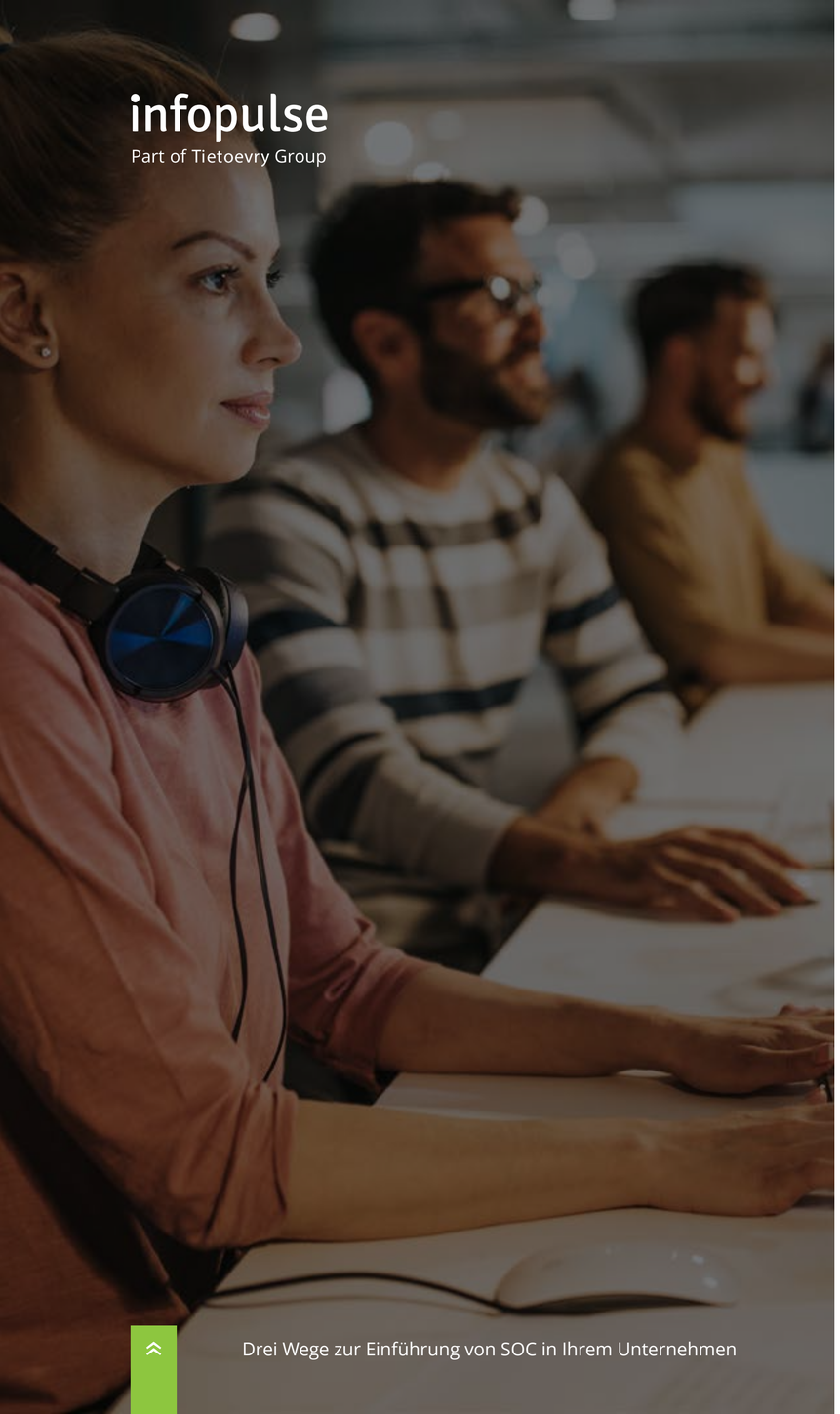
SOC-as-a-Service ist eine hervorragende Lösung sowohl für etablierte als auch für neue Unternehmen, die ihre Sicherheit strukturell und technologisch verbessern wollen. In jedem Fall beginnen wir einen Auftrag mit einer umfassenden IT-Sicherheitsbewertung, die darauf abzielt, das optimale Maß an Sicherheitsabdeckung für Ihr Unternehmen zu bestimmen und die fehlenden Sicherheitsaspekte zu implementieren.

SOC-as-a-Service ist eine hervorragende Lösung sowohl für etablierte als auch für neue Unternehmen, die ihre Sicherheit strukturell und technologisch verbessern wollen

Mit einem SOC-as-a-Service-Modell erhalten Sie ein maßgeschneidertes Servicepaket, eine Sicherheitsarchitektur und eine Toolkit-Konfiguration sowie ein Bereitschaftsteam, das alle Ihre Sicherheitsanforderungen erfüllt und die festgelegten SLAs einhält.

Während der **Einarbeitungsphase (zwischen zwei und zwanzig Wochen)** werden Sie eng mit unseren Beratern zusammenarbeiten:

- Bericht über den aktuellen Stand der Sicherheit, ermittelte Schwachstellen und Unzulänglichkeiten
- Vorschläge für die optimale Sicherheitsarchitektur, Lizenzen und Strategien zur Kostenoptimierung
- Implementierung und Anpassung des erforderlichen Sicherheits-Toolkits und Einrichtung unterstützender Prozesse
- Implementierung von Unterstützung für benutzerdefinierte Anwendungsfälle - Dienstleistungsvereinbarungen, die spezifische Geschäftsanforderungen, Unternehmensausrüstung (z. B. IoT-Systeme) oder intern entwickelte Geschäftssysteme abdecken
- Übernahme aller etablierten SOC-Verantwortlichkeiten, basierend auf der Paketstufe
- Durchführung von Schulungsworkshops für interne Mitarbeiter
- Regelmäßige Berichterstattung über neue Erkenntnisse und Vorschläge für weitere Verbesserungsbereiche



infopulse
Part of Tietoevry Group

Bei Infopulse kombiniert das Managed SOC eine Ad-hoc-Sicherheitsberatung und eine Anleitungen zur Einführung - die von anderen Anbietern als Einzellösung angeboten werden - mit der Delegation von SOC-Diensten, die ein höheres Maß an Vorhersehbarkeit, Effizienz und Fachwissen bieten.

Mit einem Managed SOC müssen Sie nicht nach einzelnen Experten suchen, um Ihre Sicherheitsabläufe zu erweitern, oder mit anderen Arbeitgebern um gefragte Sicherheitskräfte konkurrieren. Außerdem optimieren Sie die SOC-Betriebskosten, indem Sie die Kosten für die Schulung, Fortbildung und Bindung von Mitarbeitern eliminieren.

75%

der SOC-Fachleute berichten über Burnout aufgrund der erhöhten Arbeitsbelastung[11]

60%

finden, dass eine Karriere im Bereich der Cybersicherheit sehr anstrengend ist, was die Vereinbarkeit von Beruf und Privatleben angeht[12]

65%

der Spezialisten für Cybersicherheit sind der Meinung, dass ihr Arbeitgeber nicht genügend Schulungen anbietet[13]

[11] Devo:2020 Devo SOC Performance Report
[12] ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2020
[13] Ibid.

infopulse
Part of Tietoevry Group

Wir sorgen nicht nur für eine ausreichende Personalausstattung, sondern helfen Ihnen auch bei der Auswahl, Konfiguration, Bereitstellung und Anpassung von Sicherheitstools, die Ihren Geschäftsanforderungen entsprechen. Die Sicherheitstechnologie hat in den letzten fünf Jahren erhebliche Fortschritte gemacht, insbesondere in Bezug auf Analysen, Automatisierung und Vorhersagefunktionen. Investitionen in modernste Tools führen jedoch nicht automatisch zu messbaren Verbesserungen der Sicherheitslage eines Unternehmens.

82%

der Führungskräfte im Bereich Cybersicherheit geben mehr als 20 % ihres IT-Budgets für Investitionen in fortschrittliche Technologien aus.

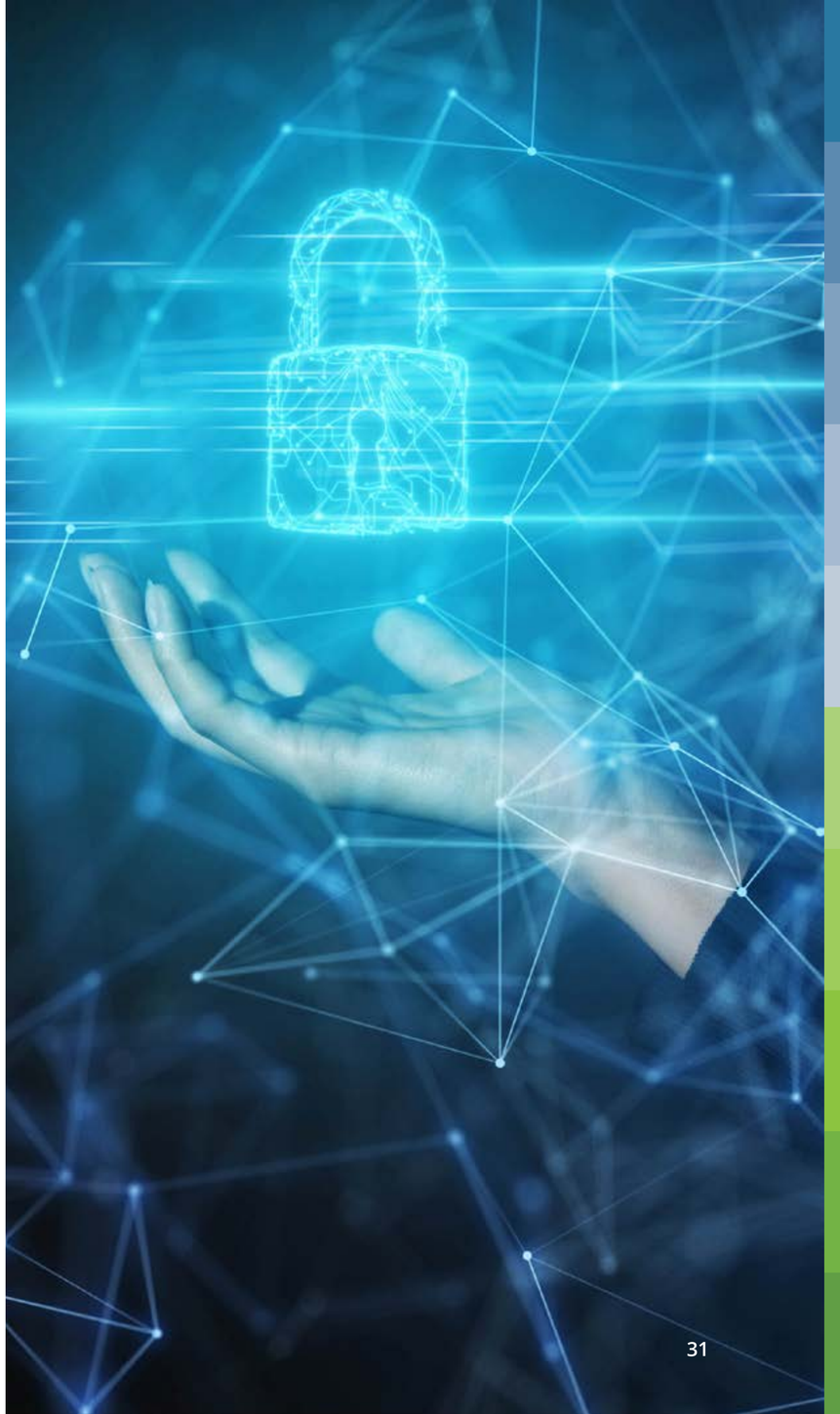
58% vs **24%**

der Unternehmen mit ausgereiften Cybersicherheitsprogrammen haben einen höheren Prozentsatz an eingedämmten Sicherheitsverletzungen, die keine Auswirkungen auf den Betrieb haben.

69%

der Unternehmen haben Schwierigkeiten, Angreifern einen Schritt voraus zu sein, und die Kosten dafür sind nicht tragbar[14]

[14] Accenture: State of Cybersecurity Report 2020



infopulse
Part of Tietoevry Group

Auf der Grundlage der Bewertungsdaten helfen wir Ihrem Unternehmen, neue Technologieinvestitionen mit den aktuellen und zukünftigen Sicherheitsanforderungen in Einklang zu bringen. Auf diese Weise erhalten Sie die beste Abdeckung und die besten Funktionen, die genau auf Ihre Infrastruktur abgestimmt sind, ohne zu viel Geld auszugeben.

Wir helfen bei der Auswahl, Bereitstellung und Konfiguration von:

- SIEM-Tools (einschließlich Abonnement für kommerzielle Bedrohungsdaten)
- SOAR
- Ticketing-Systemen
- Event-Management-Systemen
- Plattform zur Reaktion auf Sicherheitsvorfälle
- Tools zur automatisierten Erkennung von und Reaktion auf Bedrohungen
- fortschrittlicher Sicherheitsanalytik (einschließlich prädiktiver Lösungen)

Nahezu alle Branchen haben im vergangenen Jahr einen deutlichen Sprung nach vorne gemacht, was die Digitalisierung angeht. Auch die Cyber-Bedrohungslandschaft wurde immer gefährlicher und komplexer. Mit SOC-as-a-Service können Sie einen stabilen Sicherheitsbereich entwickeln, der mit den besten kommerziellen Tools ausgestattet ist, und einen engagierten “Wachhund” einsetzen, der diesen Bereich bewacht, ohne eine eigene Sicherheitsabteilung einrichten zu müssen.

infopulse
Part of Tietoevry Group

Vorteile

- Geeignet für Unternehmen auf jeder Stufe der Sicherheitsreife
- Sicherheitsstufen und Schutz, angepasst an Ihre Branche
- Niedrigere TCO von SOC mit vorhersehbaren monatlichen Kosten
- Zugang zu gefragten Fachkräften und Fachwissen im Bereich Cybersicherheit
- Anpassbare Support- und Sicherheitsstufen
- Hohe Serviceniveaus, die an Metriken und SLAs gebunden sind
- Beratung zu Technologieinvestitionen und Unterstützung bei der Erfüllung von Compliance-Anforderungen
- Unterstützung von benutzerdefinierten SOC-Anwendungsfällen für sofort einsatzbereite Sicherheitsszenarien
- Kontinuierliche Sicherheitsverbesserungen und Beratung

Herausforderungen

- **Sichtbarkeit der IT-Infrastruktur erforderlich.** Vor der Einrichtung eines SOC ist es unerlässlich, eine Prüfung der Infrastruktur durchzuführen, um einen umfassenden Überblick über die Komponenten zu erhalten. Sicherheitsexperten betonen, wie wichtig es ist, ihnen ein umfassendes Inventar der Assets und eine Datenklassifizierung zur Verfügung zu stellen, um eine effiziente SOC-Leistung zu ermöglichen.
- **Aufbau einer effektiven Kommunikation.** Wenn das SOC an einen ausgewählten Sicherheitsdienstleister delegiert wurde, sollte ein einziger Ansprechpartner in der Organisation vorhanden sein, um eine effektive Zusammenarbeit zu ermöglichen. Durch die Ernennung eines solchen Mitarbeiters kann das Unternehmen die Zeit und die Ressourcen, die für die Bearbeitung bestimmter Vorgänge erforderlich sind, erheblich reduzieren und damit die Gesamtleistung des SOC-Teams steigern.

AGRARKONZERN

FALLBEISPIEL

Nutzung der Möglichkeiten der Cybersicherheitsautomatisierung für ein großes landwirtschaftliches Unternehmen

infopulse
Part of Tietoevry Group

AGRARKONZERN

Infopulse unterstützte unseren Kunden, einen europäischen Marktführer in der Landwirtschaft, bei der Verbesserung seines Cybersicherheitssystems durch die Neukonfiguration des aktuellen Azure Sentinel Setups mit maximaler Effizienz und der Einführung von Automatisierung. Nach der Bewertung des bestehenden IT-Umfelds entwickelten unsere Experten die High-Level-Architektur der Lösung und die Strategie für die Lösungsimplementierung. Die Fähigkeiten von Azure Sentinel wurden durch vier SIEM/SOAR-Testfälle validiert:

1

Erkennung potenzieller Bedrohungen bei der Verwendung von Microsoft Teams.

Konfiguration einer Reihe von Analyseregeln und Data Parsing über Logic Apps und Office 365 Management Activity API.

2

Identifizierung von Datenlecks in Unternehmen via E-Mails.

Einrichtung einer automatischen Regel zur Erkennung von Benutzern, die mehrere E-Mails an dieselbe externe SMTP-Adresse weiterleiten.

3

Ablehnung potenziell schädlicher Dateien beim Hochladen in den Cloud-Speicher des Unternehmens.

Testen von Warnmeldungen beim Hochladen potenziell schädlicher ausführbarer Dateien in gemeinsame Ordner in SharePoint und OneDrive.

4

Identifizierung potenziell gefährdeter Konten.

Identifizierung von Fällen mit erfolgreichen Anmeldungen von IPs, die versucht haben, gesperrte oder deaktivierte Benutzerkonten auszunutzen.

ERGEBNIS

Die Testszenarien demonstrierten die Vorteile und Fähigkeiten von Azure Sentinel als Cloud-natives (SaaS) Sicherheitsautomatisierungssystem und ermöglichten es unserem Kunden mit:

- Automatisierte Cybersicherheitsregeln für die ausgewählten Testfälle, die es ermöglichen, den menschlichen Faktor zu minimieren.
- Erfolgreiche Integration von Azure Sentinel mit Exchange, SharePoint, Teams und Microsoft Threat Protection.
- Automatisierte Berichterstellung über Azure Sentinel und Power BI.
- Die Roadmap für die weitere Implementierung von Azure Sentinel mit erweiterter Integration in die IT-Infrastruktur des Unternehmens.
- Geschätzte Lizenzkostenreduzierung für Azure Sentinel als einzelnes SIEM- und SOAR-System.

Kontaktieren Sie unser Sicherheitsteam, um zu erfahren, wie Azure Sentinel Ihre Sicherheitsprobleme lösen kann

infopulse
Part of Tietoevry Group

Erstellen eines Geschäftsszenarios für die SOC-Einführung: Checkliste

- [ ] **BEWERTUNG DES AKTUELLEN REIFEGRADS DER CYBERSICHERHEIT: VERWENDEN SIE DEN IN DIESEM BUCH ENTHALTENEN LEITFADEN.**
  - [ ] **Stellen Sie sicher, dass Ihr Unternehmen die folgenden Prozesse bereits eingeführt hat:**
    - [ ] Schutz kritischer IT-Infrastrukturen
    - [ ] Grundlegende Ereignisüberwachung und -protokollierung
    - [ ] Reaktionsplan für reaktive Cybersicherheit
    - [ ] Fähigkeiten zur Erkennung, Verhinderung und Überwachung von Bedrohungen
- [ ] **ERSTELLEN SIE EINE LISTE VON ANFORDERUNGEN FÜR SOC-OPERATIONEN:**
  - [ ] **Überwachung von Sicherheitsbedrohungen:**
    - [ ] Verfügen Sie über standardmäßige Sicherheitsabläufe?
    - [ ] Welche Tools (Cloud-basiert und/oder vor Ort) verwenden Sie?
    - [ ] Benötigt Ihr Unternehmen eine 24/7-Sicherheitsüberwachung?
    - [ ] Was sind Ihre derzeitigen blinden Flecken in Bezug auf die Überwachung?
  - [ ] **Management von Sicherheitsvorfällen:**
    - [ ] Welche rechtlichen, Compliance- oder geschäftlichen Anforderungen müssen erfüllt werden?
    - [ ] Gibt es SLA-Ziele für Kunden? Wenn nicht, welche sollten eingestellt werden?
    - [ ] Welche Messgrößen verwenden Sie zur Überwachung der Leistung des Sicherheitsteams?
  - [ ] **SOC-Personal:**
    - [ ] Welche Sicherheitsfunktionen möchten Sie besetzen?
    - [ ] Gibt es für jede Rolle eine klare Beschreibung der Verantwortlichkeiten?
    - [ ] Haben Sie einen Musterbesetzungsplan?
    - [ ] Benötigt Ihr internes Team eine zusätzliche Sicherheitsschulung?
  - [ ] **Prozessentwicklung und -optimierung**
    - [ ] Verfügen Sie über dokumentierte Arbeitsabläufe und SOPs?
    - [ ] Welche Prozesse müssen verbessert/automatisiert werden?
    - [ ] Benötigt Ihr Unternehmen neue Betriebshandbücher?
  - [ ] **Strategie für neue Bedrohungen**
    - [ ] Wie gut kann Ihr Unternehmen auf neue Bedrohungen reagieren?
    - [ ] Wie werden Sie sicherstellen, dass Ihre Cybersicherheitspraktiken auf dem neuesten Stand sind?
    - [ ] Erwägen Sie Investitionen in neue Technologien, um Ihre Ansätze für proaktive Sicherheitsmaßnahmen zu verbessern?

Schlussfolgerungen

Die Cybersicherheitslandschaft hat sich in den letzten Jahren dramatisch verändert. Viele Unternehmen haben jedoch erst vor kurzem erkannt, dass sie proaktive Sicherheit benötigen, die über die grundlegenden Warnsysteme und die schnelle Mobilisierung von Sicherheitsteams im Falle eines Vorfalls hinausgeht. Das SOC ermöglicht eine proaktive Sicherheit, aber ohne geeignete reaktive Maßnahmen (Cybersicherheit) ist es nicht wirksam. Die meisten Unternehmen sind jedoch mit der gleichzeitigen Bewältigung beider Probleme überfordert. Aus diesem Grund sind alternative Szenarien für die Einführung von SOC in den Vordergrund gerückt.

Durch die Entscheidung für ein hybrides SOC-Modell - bei dem ein Teil der Sicherheitsoperationen an einen Managed Service Provider, fortschrittliche SIEM-Lösungen und Endpoint Detection and Response (EDR)-Systeme delegiert wird - können Unternehmen in verschiedenen Reifestadien (und mit unterschiedlichen Sicherheitsbudgets) die Sicherheitsabdeckung erhalten, die sie für einen sicheren und konformen Betrieb benötigen.

Profitieren Sie von einem innovativen Ansatz für die Unternehmenssicherheit, der von Infopulse-Experten mit umfassender Erfahrung in diesem Bereich unterstützt wird.

infopulse
Part of Tietoevry Group

Infopulse Managed Security Operation Center: Enthaltene Dienstleistungen

CLOUD-BASIERTES VERWALTETES SIEM

- Unkomplizierte SIEM-Bereitstellung und -Integration
- Erweiterte integrierte SOAR-Fähigkeiten
- Unbegrenzte Skalierbarkeit
- Über 200 integrierte analytische Regeln
- Kommerzielle Quellen für Bedrohungsinformationen
- Machine-Learning-Modelle und Datenvisualisierung

HETEROGENE LOG-QUELLEN

- Unterstützung von Cloud-basierten, hybriden oder lokalen Log-Quellen
- Native Unterstützung von Microsoft-Logs
- Nicht abrechenbare Azure-Aktivitäten, Office 365- und Microsoft 365-Sicherheitslösungsprotokolle
- Über 100 vordefinierte Datenverbindungen
- Netzwerke, Dienste, Server, Geschäftssysteme, Sammlung, Aggregation und Korrelation von Logs

ANTWORT-AUTOMATISIERUNG

- Automatisierte Reaktion auf häufig auftretende Ereignisse
- Programmierbare Anpassung von Azure Logic Apps
- Integration mit einer großen Anzahl von Geräten, Infrastrukturkomponenten oder Geschäftssystemen

INDIVIDUELLE ANPASSUNG VON DIENSTEN

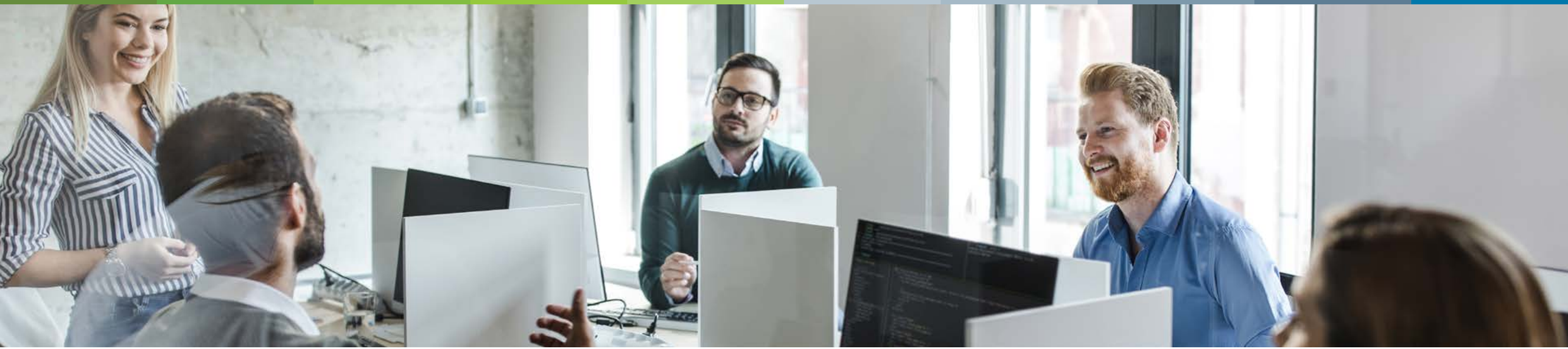
- Modifizierung von Diensten durch die Entwicklung kundenspezifischer Konnektoren und Unterstützung von Protokollen
- Maßgeschneiderte Entwicklung von Anwendungsfällen
- Anpassbare Berichte
- Verschiedene Kommunikationsmittel

ERFAHRENES SOC-L1/L2/L3-TEAM

- Verfügbarkeit bis zu 24/7
- SLA-basierter Dienst
- Erweiterte Kompetenzprofile für Sicherheitsdomänen
- Überwachung von Ereignissen, Untersuchung von Vorfällen, Berichterstattung und Anleitung zur Handhabung

KOSTENVERBESSERUNGEN UND -OPTIMIERUNG

- Bewertung der bestehenden Infrastruktur als Teil des Onboarding-Prozesses
- Optimierung der Kosten, indem nur die erforderlichen Daten erfasst werden
- Bereitstellung von Technologie- und Lösungsvorschlägen zur Optimierung der Dienstleistungsnutzung



ÜBER INFOPULSE

Infopulse, Teil des führenden nordischen, digitalen Dienstleistungs-Unternehmens Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Software-F&E, Anwendungsmanagement, Cloud- und IT-Betrieb sowie Cybersicherheit für KMUs und Fortune-100-Unternehmen auf der ganzen Welt. Das in 1991 gegründete Unternehmen verfügt über ein Team von über 2,300 Fachleuten und ist weltweit in 7 Ländern - in Europa sowie in Nord-, Mittel- und Südamerika - vertreten.

Infopulse genießt das Vertrauen vieler etablierter Marken wie BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Norwegian Oil and Gas Association, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group und vieler anderer.

Für weitere Informationen besuchen Sie bitte

www.infopulse.com/de

KONTAKTIEREN SIE UNS:

PL: +48 (663) 248-737
DE: +49 (69) 505-060-4719
US: +1 (888) 339-75-56
UK: +44 (8455) 280-080
FR: +33 (172) 77-04-80
UA: +38 (044) 585-25-00
BG: +359 (876) 92-30-90
BR: +55 (21) 99298-3389

info@infopulse.com

FOLGEN SIE UNS: