doIT solutions

AUTOMATISIERTER 24/7-SCHUTZ VOR CYBERGEFAHREN

Aufbau und Betrieb eines effizienten Security Operations Centers

Whitepaper - Stand: Okt. 2020

dolT solutions

AUTOMATISIERTER 24/7-SCHUTZ VOR CYBERGEFAHREN

Aufbau und Betrieb eines effizienten Security Operations Centers

Das SOC ist ein zentraler Bestandteil bei der Absicherung mittelständischer und großer Unternehmen vor Cyberattacken. Die Experten im Security Operations Center überwachen die IT-Infrastruktur rund um die Uhr, erkennen Bedrohungen, analysieren Gefahren und bekämpfen sie mit effizienten, gut aufeinander abgestimmten und zunehmend automatisierten Maßnahmen.

Die Cyberbedrohungslage für Unternehmen hat sich in den vergangenen Jahren deutlich verschärft. Die IT-Systeme sind immer enger mit der Geschäftstätigkeit der meisten Firmen verknüpft. Gleichzeitig hat nicht nur die Zahl ungerichteter Angriffe massiv zugenommen, auch sogenannte Targeted Attacks gegen einzelne Betriebe treten zunehmend und mit besonders schweren Auswirkungen auf. Auf der anderen Seite gibt es kaum noch Securityanalysten, die zudem als teuer gelten.

Neue Herausforderungen für Unternehmen

Betroffen von diesen Entwicklungen sind heutzutage nicht mehr nur exponierte Einzelfirmen, sondern Betriebe quer durch alle Branchen. Niemand kann sich mehr dahinter verstecken, dass sein Unternehmen zu unbedeutend oder unauffällig sei. Moderne Cyberkriminelle greifen auf breiter Front an. Dazu verwenden sie – ebenso wie ihre Gegenspieler – aktuelle Techniken wie Automatisierung und sogar künstliche Intelligenz, um ihre Attacken laufend zu verbessern und effektiver zu gestalten.

Auf der anderen Seite bereitet es zunehmend Probleme, gut ausgebildetes und erfahrenes IT-Sicherheitspersonal zu finden, das in der Lage ist, Cyber-bedrohungen schnell und effizient zu erkennen und zu bekämpfen. Gerade der Mittelstand tut sich hier schwer. Aber auch Betriebe mit tausend oder mehr Mitarbeitern haben Schwierigkeiten mit der Aufgabe, alle Angriffe auf ihre Systeme zu identifizieren und abzuwehren.

Einem besonders hohen Gefahrenpotenzial sind Firmen aus dem Bereich „Kritische Infrastrukturen“ ausgesetzt. Dazu gehören etwa der Finanzsektor, das Transportwesen und die Energiewirtschaft. Sie befinden sich besonders häufig „Im Visier der Cybergangster“. So lautet auch der Titel einer vom Marktforschungsunternehmen PricewaterhouseCoopers (PwC) veröffentlichten Studie zur Lage der IT-Sicherheit in Deutschland.

Nach Angaben von PwC macht sich die verschärfte Situation vor allem durch moderne Angriffsarten wie Ransomware oder CEO-Fraud bemerkbar. Zusätzlich wird die Lage durch neue gesetzliche Vorgaben erschwert, die in den vergangenen Jahren erlassen wurden. Bedenklich sei zudem, dass rund 37 Prozent der von PricewaterhouseCoopers befragten Unternehmen, welche die Bedrohungslage für erhöht oder stark erhöht halten, ihre Prozesse zur Identifikation von Cyberangriffen als „höchstens durchschnittlich“ bezeichnen. Elf Prozent gaben sogar an, dass die Maßnahmen zur Erfassung von Cyberattacken „unzureichend implementiert“ seien. Wenn es um Sicherheitsanalysen der eigenen IT-Landschaft geht, stufen 14 Prozent der befragten IT-Entscheider ihre Aktivitäten als „unterdurchschnittlich“ ein. Nahezu jede fünfte von PwC befragte Firma gab darüber hinaus an, in den vergangenen zwölf Monaten von mindestens einem erfolgreichen Cyberangriff betroffen gewesen zu sein.

> „Es gibt noch viele mittelständische Unternehmen, die ihre IT für ausreichend halten“...

... sagt Peter Bartels. Er ist Vorstandsmitglied und Leiter für den Bereich Familienunternehmen und Mittelstand bei PwC. Viele Firmen unterlägen dem „Irrglauben, dass ihr Bekanntheitsgrad nicht so hoch ist und sie damit weniger im Visier von Cyberkriminellen“ stünden. Aber gerade sie seien „oft hochattraktiv, wenn es zum Beispiel um den Diebstahl geistigen Eigentums“ gehe.

SCHWIERIGE SITUATION

Aus eigener Kraft können viele Betriebe die Aufgabe nicht mehr schultern, selbst umfassend für eine Absicherung vor aktuellen und künftigen Cyberbedrohungen zu sorgen. Herkömmliche Sicherheitsmaßnahmen wie die Installation von Antivirensoftware, Firewalls und aktueller Patches reichen nicht mehr aus, um alle Arten von Angriffen zu stoppen. Derzeit registrierte Attacken auf Unternehmen erfolgen oft zielgerichtet, mehrstufig und über einen längeren Zeitraum. Mit singulären Lösungen, die unabhängig voneinander arbeiten, lassen sich solche Anschläge nicht mehr erkennen und stoppen. Dann entsteht erheblicher Schaden.

Heutzutage ist es deshalb notwendig, kontinuierlich und tagesaktuell über die Bedrohungslage informiert zu sein, die neuesten Gefahren und geeignete Gegenmaßnahmen zu kennen und sie auch bewerten zu können. Viele Angriffe erfolgen zudem zu Zeiten, an denen in mittelständischen Unternehmen nur noch wenige oder gar keine Mitarbeiter mehr arbeiten. Die aktuellen Bedrohungen erfordern jedoch eine 24/7-Bereitschaft an allen 365 Tagen im Jahr. Diese Aufgabe lässt sich nur mit einem dedizierten, effizienten und hochgradig automatisierten Security Operations Center (SOC) bewältigen.

In den vergangenen Jahren hat das SOC-Konzept deutlich an Fahrt gewonnen und immer mehr Firmen- und IT-Leiter überzeugt. Das liegt unter anderem auch daran, dass sich viele Herausforderungen in einem SOC an einen kompetenten Dienstleister übertragen und von ihm in enger Zusammenarbeit mit den internen Experten erledigen lassen. Gemeinsam entsteht so eine effiziente Absicherung der IT-Infrastruktur eines Unternehmens. Die externen Dienstleister können bei der Auswahl und Priorisierung der Überwachungsfälle helfen, aber auch bei der technisch optimalen Umsetzung dieser sogenannten Use Cases sowie bei der Automatisierungskonfiguration. Dieser moderne Ansatz unterscheidet sich deutlich von der klassischen und mittlerweile veralteten Variante, bei der sich die Mitarbeiter im SOC vor allem um grundlegende Aufgaben wie das Sammeln und Analysieren von Log-Dateien, um das Erkennen von Eindringlingen und um das Einleiten von geeigneten Gegenmaßnahmen kümmern sollen.

In diesem Whitepaper erfahren Sie, was ein SOC ausmacht, wie es funktioniert und welche Vorteile seine Einführung für Sie hat. Darüber hinaus erläutert es, welche Mitarbeiter Sie für ein SOC benötigen und wie Sie ein Dienstleister dabei unterstützen kann, wenn zum Beispiel die Personaldecke dünn ist. Außerdem erfahren Sie, wie die typische Rollenverteilung beim SOC-Betrieb aussieht und wie Sie es in Ihrem Unternehmen einführen können. Nicht zuletzt geht das Whitepaper auch auf die Frage ein, wie es nach der Etablierung eines SOCs weitergehen soll.

BEGRIFFSDEFINITION:

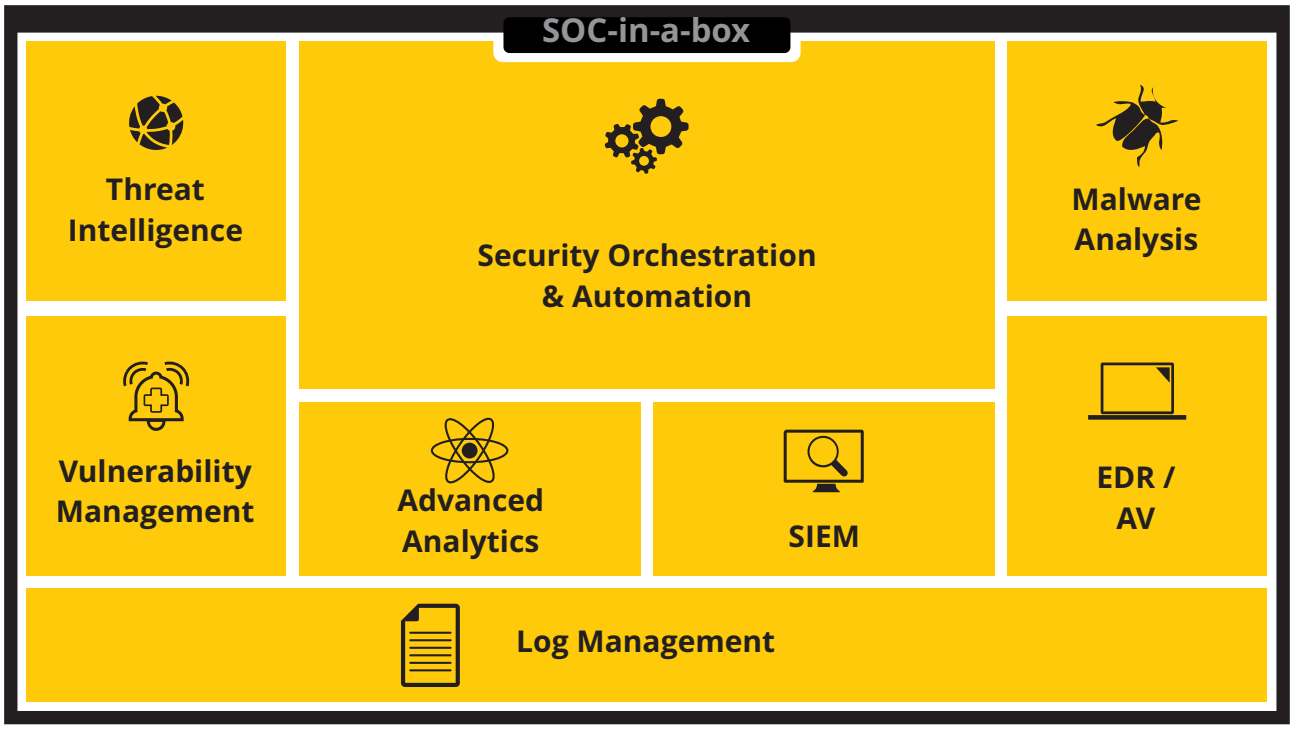
Was ist ein Security Operations Center?

Unter einem Security Operations Center (SOC) verstehen wir ein mit Sicherheitsexperten besetztes Einsatzzentrum, das die aktuelle Sicherheitslage in einer IT-Umgebung kontinuierlich und rund um die Uhr überwacht. Die Mitarbeiter bleiben mithilfe von Threat-Intelligence-Diensten auf dem Laufenden, nutzen aktuelles Know-how zur Malware-Analyse und zum Vulnerability Management, überwachen und werten Logs aus, bekämpfen Angriffe und nutzen modernste Techniken wie Security Orchestration & Automation sowie SIEM-Lösungen zur Bekämpfung neuer Bedrohungen und Aufklärung aller sicherheitsrelevanten Vorfälle. Viele SOCs werden in Zusammenarbeit mit einem kompetenten Dienstleister betrieben.

So funktioniert ein modernes und effizientes SOC

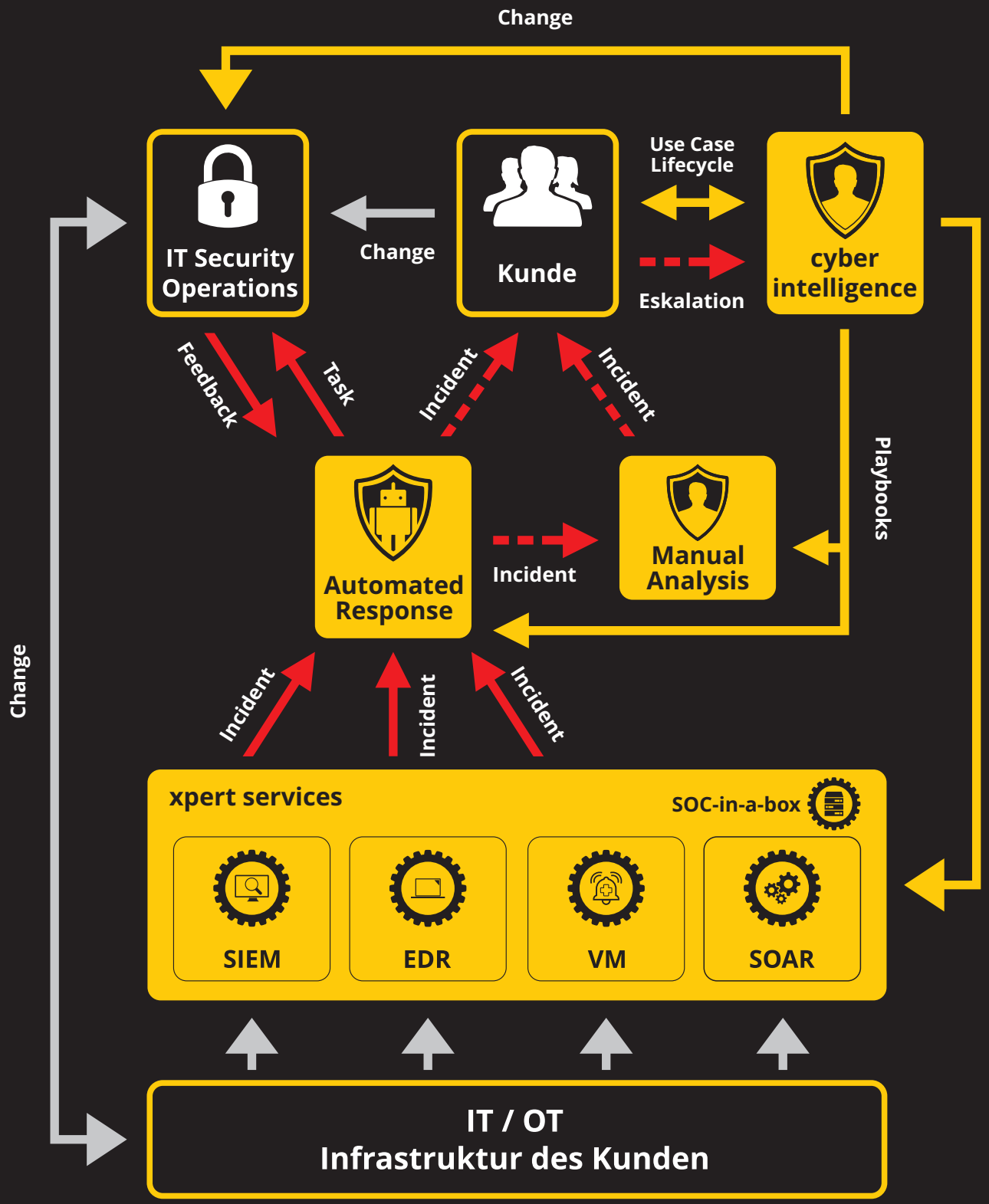
Anders als klassische IT- und Support-Abteilungen kümmert sich ein Security Operations Center ausschließlich um den Bereich der IT-Sicherheit in einer Firma. Die Mitarbeiter können umgehend auf sicherheitsrelevante Vorfälle reagieren. Das hat den großen Vorteil, dass die Absicherung der IT-Umgebung nicht mehr nur eine mehr oder weniger verhasste Zusatzaufgabe für meist bereits überlastete Abteilungen ist.

Zu den Aufgaben, die ein SOC übernimmt, zählt ein umfassendes Log-Management. Damit lassen sich gerade ablaufende Angriffe frühzeitig erkennen. Außerdem erweisen sich die gesammelten Daten als nützlich, um später auf historische Informationen zugreifen zu können oder um Schwachstellen zu identifizieren und zu schließen. Sensoren im Netzwerk und in der gesamten IT-Infrastruktur sammeln kontinuierlich Daten, die in einer zentralen SIEM-Lösung (Security Information and Event Management) erfasst werden. Das SIEM bildet sozusagen das Rückgrat jedes Security Operations Centers, da es die gesammelten Fakten mit Angriffsmustern vergleicht, um gegebenenfalls einen Alert auszulösen, auf den dann entweder automatisiert oder individuell reagiert wird.



Bei den SOC-Mitarbeitern handelt es sich um Sicherheitsexperten, die sich laufend über neue Gefahren und über bekannt gewordene Sicherheitslücken informieren. Auf dieser Basis entwickeln sie passende Überwachungsfälle, die in Verbindung mit Automatisierung effiziente Gegenmaßnahmen einleiten können. Ein SOC arbeitet also nicht nur reaktiv, sondern auch proaktiv. Dafür kommen nicht nur interne Sensoren zum Einsatz, sondern auch externe Quellen über die Integration eines oder mehrerer Threat-Intelligence-Dienste. Ein SOC betrachtet das Thema IT-Sicherheit immer als Gesamtsystem, dessen Schutz nicht nur mit einzelnen Lösungen gelingt. Dank moderner Automatisierungstechniken werden zudem Ressourcen freigesetzt, um sich etwa intensiv mit besonders schweren Vorfällen beschäftigen zu können.

doIT solutions



Wie bereits ausgeführt, darf ein SOC nicht als zusätzlich zu erledigende Aufgabe für die interne IT-Abteilung verstanden werden. Ein ernsthaftes Problem stellt zusätzlich noch der erhebliche Fachkräftemangel bei IT-Security-Spezialisten dar. Für ein SOC-Team benötigt eine Firma jedoch ein mehrstufig aufgebautes Team aus gut ausgebildeten und erfahrenen Analysten.

Die personelle Rollenverteilung

- Den klassischen **Tier-1-Security-Analysten** gibt es in dieser Form nicht mehr. Um seine Aufgaben kümmern sich heute oft Plattformen zur Security Orchestration & Automation. Sie sorgen dafür, dass die SOC-Mitarbeiter nicht durch die zahlreich auftretenden Alerts überlastet werden. Richtig eingesetzt, erkennen die Software-Roboter kritische Alerts deutlich schneller und effektiver, als es menschliche Security-Analysten je vermocht haben.

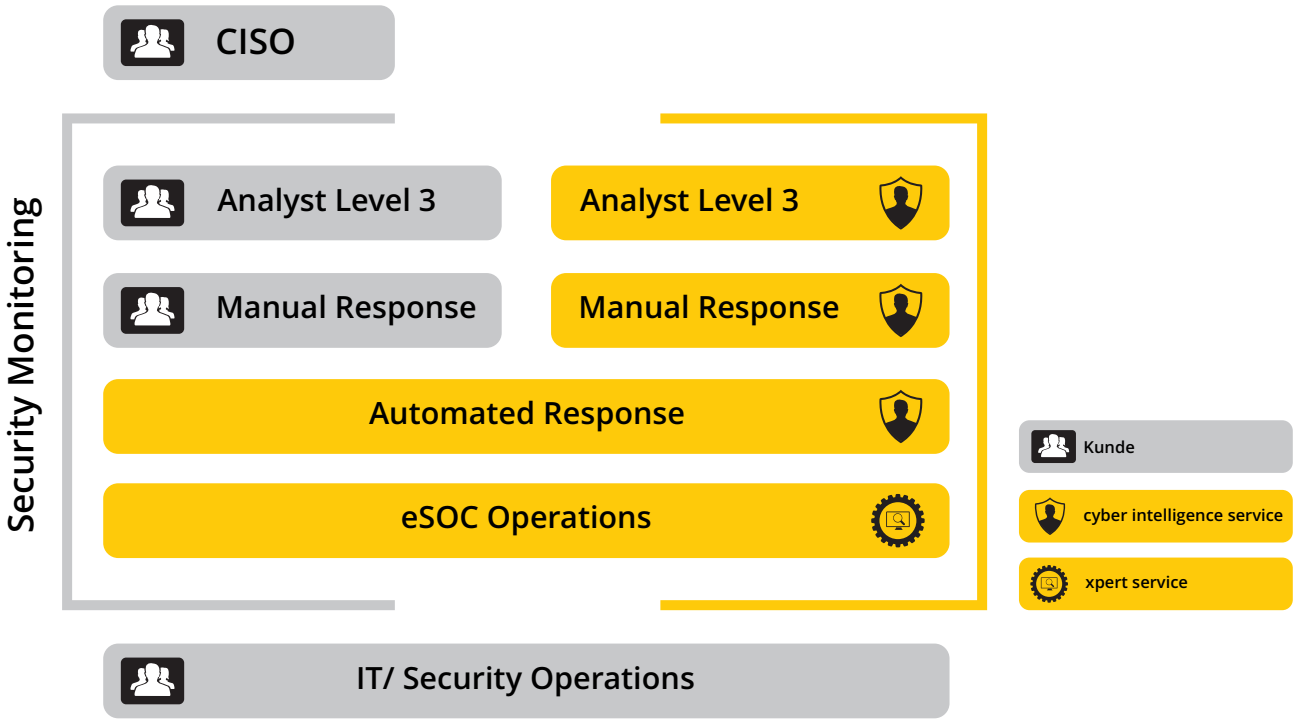
- Zu den Aufgaben eines **Tier-2-Security-Analysten** gehört heutzutage nicht mehr die direkte Abwehr von Cyberangriffen. Stattdessen versucht er beispielsweise, durch manuelle Maßnahmen herauszufinden, welche Incidents als False Positives aussortiert werden können. Alle anderen Sicherheitsvorfälle landen dann in Tier 3.

- Ein **Tier-3-Analyst** trifft dann unter anderem die Entscheidungen, welche Überwachungsfälle angewandt werden sollen. Außerdem kümmert er sich darum, welche automatischen Maßnahmen das Playbook für die Überwachungsfälle enthalten soll. Darüber hinaus klärt er, was mit einem Incident geschieht, nachdem er die False-Positive-Filter in Tier 1 und 2 durchlaufen hat. Zudem erstellt er Trendanalysen und passt gegebenenfalls die Einstellungen an.

- Der SOC-Leiter wird gelegentlich auch als **Tier-4-Analyst** bezeichnet. Er benötigt nicht nur alle Kenntnisse und Fähigkeiten der Stufen 1 bis 3, sondern Führungsqualitäten sowie ein Talent für Kommunikation selbst in schwierigen Zeiten. Er erstellt auch Krisenreaktionspläne sowie Compliance-Berichte und kümmert sich um die Beauftragung von Audits.

Selbst ein kleines SOC benötigte in der Vergangenheit mindestens acht Mitarbeiter, die in mehreren Schichten auch an Sonn- und Feiertagen arbeiteten. Bezog man noch den zusätzlichen Bedarf wegen Urlauben und Krankheiten mit ein, erhöhte sich diese Zahl weiter. Damit ein Security Operations Center seine Aufgaben vollumfänglich erfüllen konnte, ging man deshalb in der Regel von zehn bis fünfzehn Mitarbeitern aus.

Früher wurde gern die Faustregel genannt, nach der in einem Unternehmen ein bis zwei SOC-Mitarbeiter auf hundert Angestellte kommen sollen. Das hat aber wenig mit der heutigen Realität zu tun. Keine Firma kann sich mehr solche Mengen an Sicherheitspersonal leisten. Die Lösung ist stattdessen eine weitgehende und konsequente Automatisierung der Maßnahmen, um die Effizienz zu erhöhen und Kosten zu sparen. Durch eine moderne Plattform zur Security Orchestration & Automation werden weit weniger Menschen benötigt als früher.



Die SOC-Einführung lässt sich nicht von heute auf morgen erledigen. Unabdingbar ist eine ausführliche Beratung durch einen erfahrenen Partner, bevor Sie die ersten Schritte einleiten oder sich auf eine bestimmte Lösung konzentrieren. Der Dienstleister kann die individuelle Situation in Ihrem Betrieb analysieren und Sie dabei unterstützen, Fehler bei der Implementierung sowie unnötige Kosten zu vermeiden. Wobei anzumerken ist, dass die größten Kosten beim Betrieb eines SOCs in der Regel das Personal verursacht.

Im Folgenden finden Sie ein Beispiel für einen schrittweisen und typischen Ablauf der SOC-Implementierung. Je nach Situation ist aber auch eine andere Vorgehensweise möglich. Auch hier gilt, dass die Mitarbeit eines Dienstleisters beim Erkennen des besten Wegs für Ihren Betrieb helfen kann.

So führen Sie ein SOC in Ihrem Unternehmen ein

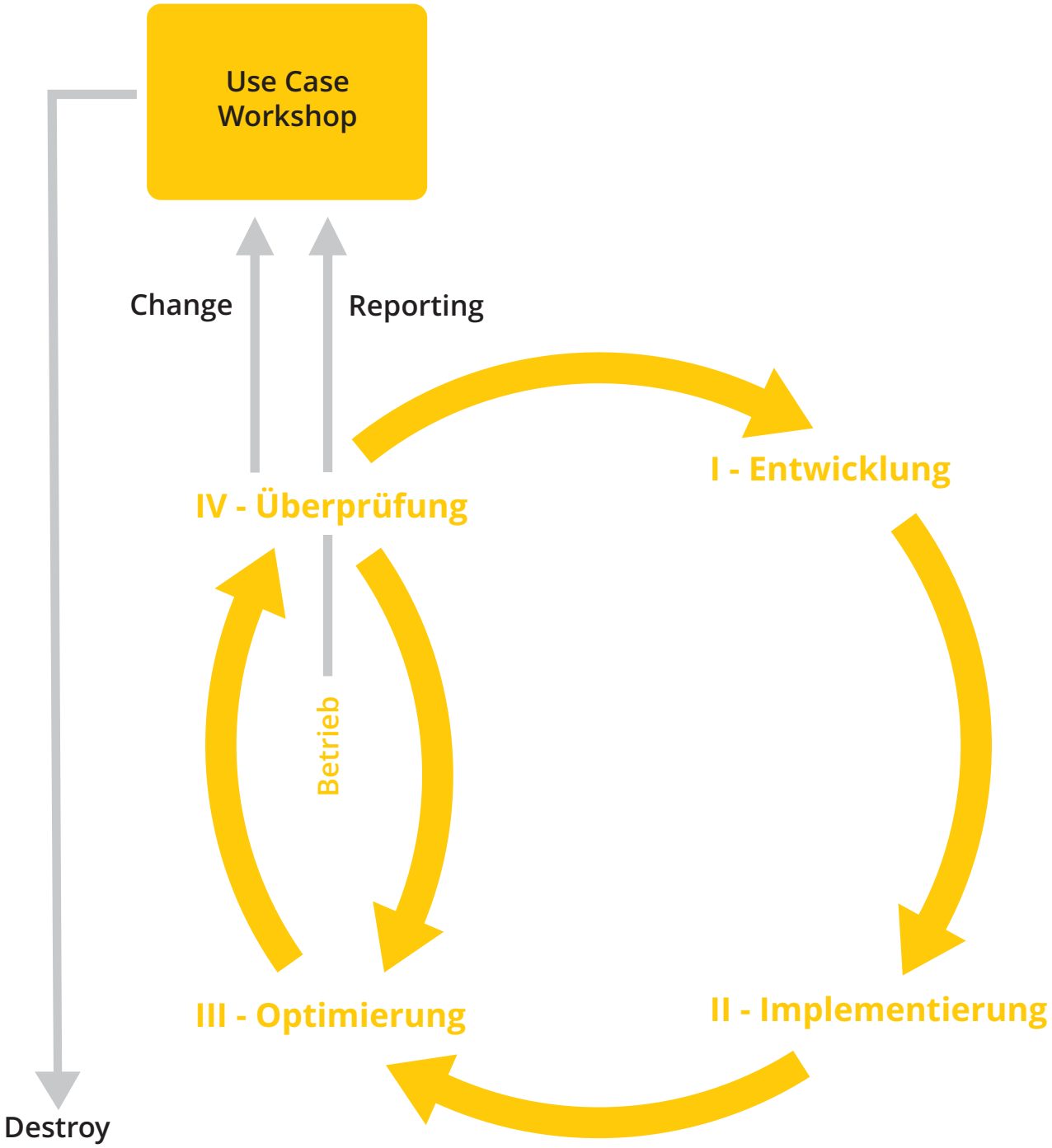
- **Schritt 1:** Eine aktuelle Risikobewertung sowie Anforderungen an Hersteller und Lieferanten müssen erstellt werden. Dazu gehört auch die Definition wichtiger Kennzahlen und Metriken (KPIs). Diese sind für die spätere Optimierung und Anpassung des SOCs an die aktuelle Lage von Bedeutung. Im Idealfall kommt eine betriebswirtschaftliche Betrachtung des SOCs hinzu.

- **Schritt 2:** Organisatorische Maßnahmen wie die Suche nach geeignetem Personal und dem richtigen Betriebsmodell. Dies kann in Eigenverantwortung oder durch Unterstützung eines externen Dienstleisters erfolgen und bestimmt maßgeblich die notwendige Anzahl und Rollen der internen SOC Organisation.

- **Schritt 3:** Passende Use Cases (Anwendungsfälle) müssen definiert und Schutzaktionen geplant werden. Use Cases ergeben nur dann einen Sinn, wenn am Ende eine angemessene Aktion als Ergebnis steht. Der vorgesehene Workflow sollte als Ganzes betrachtet werden. Ein erfahrener externer Berater kann hier helfen. Wichtig ist, dass ein effizientes Security Operations Center Use Cases aus allen Bereichen verarbeiten kann. Dabei darf es keine Rolle spielen, ob es sich um die IT, OT und/oder Cloud handelt, die geschützt werden müssen.

- **Schritt 4:** Sowohl proaktive als auch reaktive Maßnahmen müssen geplant und erstellt werden. Dazu zählen nicht nur Security-Assessments und Analysen der aktuellen Lage, sondern auch etwa Planungen zum Betrieb und der Wartung der eingesetzten Securitylösungen und -appliances sowie zum Patch-Management.

Die beschriebenen Schritte stellen nur einen Ausschnitt einer typischen Implementierung dar. Im Idealfall sprechen Sie sich mit Ihrem Berater ab, der Sie bei der konkreten Umsetzung unterstützt.



Die Sicherheitslage wandelt sich permanent. Die entwickelten Use Cases dürfen deshalb nicht wie in Stein gemeißelt behandelt werden – zu viel ändert sich im Laufe der Zeit. Neue Gefahren kommen hinzu, andere schwächen sich ab. So stimmt eventuell die Ausrichtung der Use Cases nicht mehr. Oder es wurden seit der Einrichtung des SOCs weitere Abteilungen mit neuen Arbeitsplätzen eingerichtet, die noch nicht ausreichend geschützt sind. Aus diesen Gründen ist eine laufende Anpassung an die aktuelle Situation nötig. Auch die Mitarbeiter müssen kontinuierlich geschult und auf den aktuellen Wissensstand gebracht werden.

Fazit

Vielen Firmen wissen, dass sie beim Thema IT-Security aufrüsten müssen. Ein Security Operations Center, sei es selbst betrieben oder mit der tatkräftigen Unterstützung eines Dienstleisters, gilt als einer der zentralen Bestandteile einer modernen und umfassenden Sicherheitsstrategie. Oft mangelt es jedoch an ausgebildeten und erfahrenen Sicherheitsexperten sowie am internen Know-how. Gute Securityanalysten sind nicht nur begehrt, sondern auch teuer.

Wie es nach der SOC-Implementierung weitergeht

Aber selbst ein individuell auf den eigenen Bedarf zugeschnittenes SOC reicht nicht. Die eingesetzte Technik muss an die jeweilige Organisation angepasst werden. Auch ohne die Fortbildung der Mitarbeiter und die kontinuierliche Überprüfung der Use Cases geht es nicht. Viele Betriebe sind damit überfordert und benötigen dabei Unterstützung.

Das Unternehmen doIT solutions ist ein kompetenter Partner mit umfassender Erfahrung in der Planung, dem Betrieb und der Weiterentwicklung eines SOCs, der die in diesem Whitepaper skizzierten Aufgaben fachkundig für Sie übernehmen kann. Die Spezialisten von doIT solutions haben dazu eigens ein modulares System entwickelt, aus dem die benötigten Elemente ausgewählt werden können. Der cyber intelligence service von doIT solutions unterstützt Unternehmen bei der Priorisierung und Auswahl der richtigen Überwachungsfälle und sorgt für eine technisch optimale Umsetzung. Auf diese Weise und durch umfangreiche Automatisierungsmaßnahmen werden unnötige Personalkosten vermieden. Letztlich wird dadurch der Betrieb eines Security Operations Centers nicht nur technisch umsetzbar, sondern auch bezahlbar.

GLOSSAR DER WICHTIGSTEN FACHBEGRIFFE

- **Endpoint Detection and Response (EDR):**

EDR-Lösungen schützen die Endgeräte in einem Unternehmen vor Malware und anderen Cybergefahren. Anders als bei einem herkömmlichen Antivirenprogramm erfolgen die Steuerung und das Monitoring bei EDR-Lösungen jedoch zentral.

- **Security Orchestration & Automation (SOAR):**

Ein modernes SOAR-System beschleunigt die Reaktion auf erkannte Bedrohungen, da es viele manuell auszuführende oder sich wiederholende Aufgaben automatisiert.

- **Security Information and Event Management (SIEM):**

Eine SIEM-Lösung sammelt Meldungen, Alarme und Log-Dateien aus dem Netzwerk und unterstützt die Analysten bei der Untersuchung von sicherheitsrelevanten Vorfällen. Mit einem SIEM kann man außergewöhnliche Ereignisse und riskante Trends schneller unter die Lupe nehmen.

- **Threat Intelligence:**

Ein Threat-Intelligence-Service versorgt die SOC-Mitarbeiter mit aktuellen Informationen und Daten zu neuen Bedrohungen, Angriffsmustern und gefährlichen Entwicklungen.

- **Vulnerability Management:**

Diese Lösungen spüren bereits bekannte Schwachstellen im Netzwerk auf, sodass sie schneller behoben werden können.