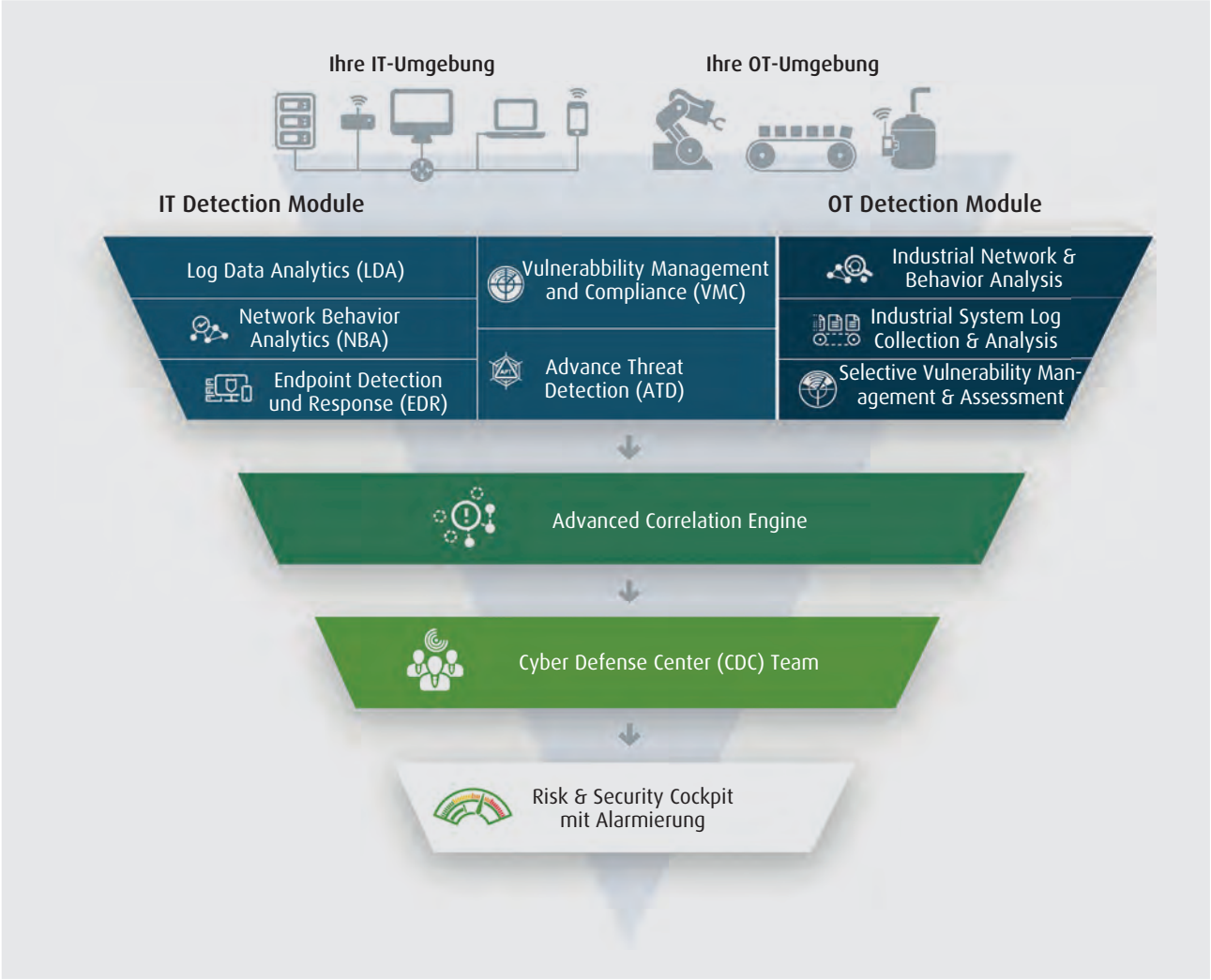
Mehr Cyberresilienz

Mit einem Security Operations Center Cyberkriminellen Paroli bieten

Es gibt immer mehr Cyberangriffe auf kritische Infrastrukturen und die Attacken werden komplexer. Angesichts der wachsenden Bedrohung sind Betreiber gut beraten mit einer Sicherheitsüberwachung rund um die Uhr durch bestens ausgebildete Experten, die sich ganz auf das Thema Cyberabwehr konzentrieren – und das möglichst kosteneffizient. Was fast zu schön klingt, um wahr zu sein, lässt sich mit einem externen Security Operations Center realisieren.

Je digitaler die Energiewirtschaft auf allen Ebenen der Wertschöpfungskette wird, desto größer werden die Angriffsflächen in den Kommunikationsnetzen der Informationstechnologie (IT) und in der Operativen Technologie (OT). Ins Visier nehmen Cyberkriminelle längst nicht mehr nur Großkonzerne, sondern zunehmend kleine und mittelgroße Betreiber von kritischen Infrastrukturen (Kritis). Die internen IT-Abteilungen sind mit ihren bisherigen Aufgaben oft schon völlig ausgelastet und können zusätzliche Herausforderungen kaum noch bewältigen. Das wiederum erleichtert den Kriminellen ihre Arbeit. Hinzu kommt: Das neue IT-Sicherheitsgesetz 2.0 erweiterte den Kreis der Kritis-Unternehmen



Quelle: Radar Cyber Security

Bild 1. Informationen aus unterschiedlichen Sicherheitsmodulen werden automatisiert aufbereitet, von Experten bewertet und in einem Risk&Security-Cockpit visualisiert.

und verschärfte ihre Verpflichtungen. So müssen sie seit Mai 2023 Systeme zur Angriffserkennung, die dem aktuellen Stand der Technik entsprechen, einsetzen und das ordnungsgemäß nachweisen. Vor diesem Hintergrund gewinnt die Unterstützung durch ein externes Security Operations Center (SOC) an Bedeutung.

IT-Kenntnisse reichen nicht

Vorstellen kann man sich ein SOC wie eine Leitzentrale, in der Fachleute mit Spezialkenntnissen, technischen Security-Tools und bewährten Prozessen daran arbeiten, die Cyberabwehr zu stärken. Diese Kombination ermöglicht einen 360-Grad-Blick, um alle sicherheitsrelevanten Systeme eines Unternehmens zu integrieren, zu analysieren und zu überwachen.

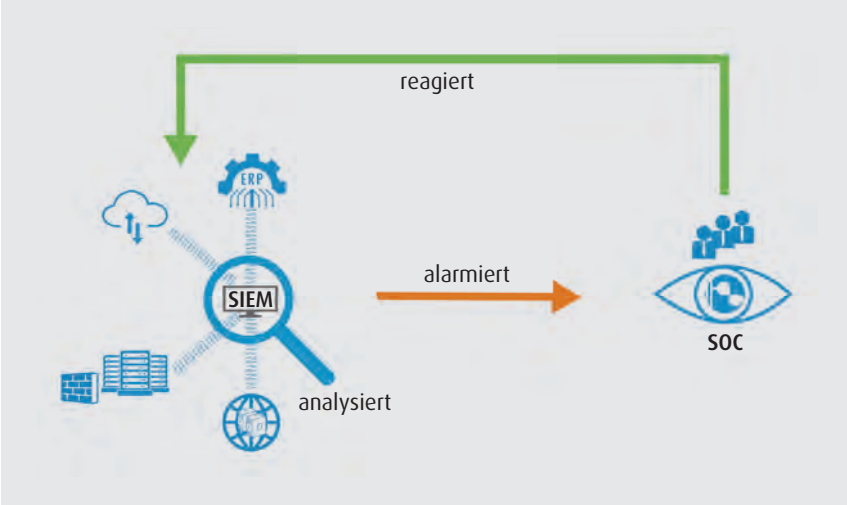
Bei der Auswahl eines externen SOC-Dienstleisters kommt es entscheidend darauf an, dass dessen Team die richtigen Fähigkeiten mitbringt, damit er die individuelle Situation des künftigen Auftraggebers verstehen kann. Für den Kritis-Sektor reicht IT-Security-Fachwissen allein nicht aus. Denn ein erfolgreicher Angriff auf die OT, auf industrielle Kontrollsysteme (ICS) oder die Hardware von Scada-Systemen könnte sich erheblich auf die Versorgung und Sicherheit der Bevölkerung auswirken. Wer in diesem Kontext Cyberkriminellen Paroli bieten will, braucht ein tiefes Verständnis der OT-Infrastrukturen und ihrer Automatisierungs-, Prozess- und Netzleittechnik. Denn: IT ist nicht gleich OT. Das beginnt damit, dass sich Softwarelösungen, die zum Schutz typischer IT-Produkte wie Serversysteme oder Router entwickelt wurden, nicht einfach 1:1 auf die OT übertragen lassen. Die Programme sprechen nicht dieselbe Sprache und können beispielsweise Industrieprotokolle von Anlagensteuerungen nicht verstehen.

Wie groß die Unterschiede zwischen IT und OT sind, zeigt sich an etwas so Selbstverständlichem wie Updates, die regelmäßig auf IT-Equipment aufgespielt werden. Bei der OT hingegen ist die Sorge der Betreiber nicht unberechtigt, dass das Patchen älterer Bestandsanlagen problematisch sein kann. Anlagenverfügbarkeit hat in der Welt der OT höchste Priorität. Die Folgen eines ungeplanten Maschinenstillstands sind auch wesentlich gravierender als der kurzfristige Ausfall eines Büro-PC.

Alarmierungen dezidiert bewerten

Ein modular aufgebautes SOC, das auf einer technischen Plattform-Lösung beispielsweise des europäischen Anbieters Radar Cyber Security basiert, kann vielfältige Managed Services abdecken (**Bild 1**). Um herauszufinden, was ein Unternehmen benötigt, starten Security-Experten mit einer Bestandsaufnahme der vorhandenen Infrastruktur und der aktuellen Sicherheitsmaßnahmen. Denn grundlegende Dinge aus der IT, wie sichere Passwörter, sauber segmentierte Netze oder ein etabliertes Patch-Management, sind in der OT noch selten. Doch solche Basismaßnahmen sind unerlässlich, damit die Sicherheitsfachleute im SOC überhaupt ein modernes Security Information and Event Management (SIEM) etablieren können. Ein SIEM ist für die Security-Analysten ein wichtiges Handwerkszeug. Es sammelt Meldungen, Logfiles und eine Vielzahl anderer Daten aus allen relevanten Bereichen der IT/OT-Infrastruktur, aggregiert diese und weist auf Auffälligkeiten hin (**Bild 2**).

In der Praxis ist die Anzahl der Alarmierungen enorm hoch. Um sinnvoll darauf zu reagieren, braucht es erfahrene Fachleute. Sie müssen die bereitgestellten Daten qualifiziert sichten und mit Blick auf die betriebliche Infrastruktur, zum Beispiel die verwendeten Softwareversionen, bewerten. Um diesen Prozess gleichermaßen schlank wie schlagkräftig zu gestalten, definiert das SOC-Team gemeinsam mit dem Unternehmen für dessen kritische Geschäftsprozesse potenzielle Gefährdungssituationen, die Use-Cases. Auch hierfür braucht es zwingend interdisziplinäre Fachkenntnisse.



Quelle: telent GmbH

Bild 2. Ein SIEM erfasst in Echtzeit unzählige Daten aus der IT/OT-Infrastruktur und ist ein wichtiges Handwerkszeug für das Security-Team im SOC.

Vielfalt an Sicherheitsmodulen

Mit einem SIEM erfüllen Kritis-Betreiber auch ihre gesetzliche Pflicht, Sicherheitsvorfälle zu protokollieren und zu detektieren, um darauf reagieren zu können. Definierte Use-Cases erhöhen die Produktivität des zuständigen Security-Moduls »Log Data Analytics« (LDA) erheblich, da sämtliche Korrelationsregeln, Compliance-Standards und bekannte Gefährdungslagen jederzeit verfügbar sind und sofort nach der Implementierung für alle Anwendungen bereitstehen. LDA visualisiert die Daten transparent, sodass das SOC-Team sie interpretieren kann.

Ein weiteres wichtiges Sicherheitsmodul ist »Vulnerability Management & Compliance« (VMC). Die Software scannt automatisiert in regelmäßigen Abständen die komplette IT/OT-Infrastruktur in so hoher Güte, dass Produktionsanlagen nicht gestört werden. Darüber identifizieren die Experten, ob die Systeme des Unternehmens bekannte Sicherheitslücken enthalten, die Cyberkriminelle als Einfallstor nutzen.

Daneben erkennt das Modul »Network Behaviour Analytics« (NBA), ob gefährliche Malware, Anomalien und andere Bedrohungen im Netzwerk unterwegs sind, indem es signatur- und verhaltensbasierte Methoden einsetzt.

Daten von Computern, Smartphones und Tablets beziehungsweise Netzleit-, Fernwirk- und Steuerungstechnik – also, den Endpunkten in der IT oder OT – erfasst die integrierte Sicherheitslösung »Endpoint Detection & Response« (EDR) und kombiniert sie mit regelbasierten Reaktions- und Analysefunktionen.

Die Qualität eines SOC entscheidet sich allerdings nicht an den technischen Tools, sondern an der Fachkompetenz der Security-Analysten. Der Mehrwert entsteht durch ihr Spezialwissen, mit dem sie die Cyberabwehr so positionieren, dass sie IT und OT gleichermaßen schützt.

Selbstverständlich können auch interne IT-Abteilungen ein SOC aufbauen. Da es vielen von ihnen aber an Zeit und Personal mangelt, werden sie dauerhaft nicht auf externe Hilfe verzichten können. Ein SOC als Dienstleistung füllt nicht nur diese Lücken, sondern kann vor allem für mittelständische Kritis-Betreiber der günstigere Weg sein, sich diese Kapazitäten einzukaufen. Denn die Unternehmen müssen nicht selbst in Security-Software, Sicherheitsexperten, Schulungen und vieles mehr investieren, die beim Aufbau eines eigenen SOC anfallen.

Daniel Weber,
Senior Manager Security Solutions,
telent GmbH, Backnang

>> info.germany@telent.de

>> www.telent.de