ConSecur

[security and consulting]

ConSecur GmbH

Jederzeit den Überblick mit dem Sicherheitsdienst für Ihre IT

ConSecur ist seit 20 Jahren IT-Sicherheitsexperte für den Mittelstand. Ziel unserer Arbeit ist es, nur berechtigten Personen den Zugriff auf Informationen zu gewähren und Informationen vor Übergriffen Unbefugter zu schützen. Wir fühlen uns der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität der Information verpflichtet. Wir entwickeln IT-Sicherheitslösungen, die wir mit unseren Spezialisten umsetzen und vor Ort dauerhaft betreiben. Seit 1999 betreuen wir dabei einen stetig wachsenden Kundenstamm, der Unternehmen aus Branchen wie Telekommunikation, Automobil, Finanzen, Chemie sowie öffentliche Einrichtungen umfasst.
Basis für unsere Lösungen bilden dabei ein Information Security Management (ISM), ein Security Information and Eventmanagement (SIEM) sowie ein Identity and Ac cess Management (IAM). Gleichermaßen bedienen sich unsere Kunden der ConSecur Managed Security Services, die Informationen im Unternehmen optimal schützen auf Wunsch 24/7.

Unsere vernetzte Welt hat in den vergangenen Jahren in einem beeindruckenden Tempo an Mobilität und Flexibilität gewonnen. Wir rufen Informationen dort ab, wo wir uns gerade befinden, und teilen sie mit Kunden, Partnern und Kollegen. Allerdings erfordert diese Freiheit gleichermaßen unsere erhöhte Wachsamkeit. Denn überall dort, wo etwas rausgeht, kann eben auch immer jemand hereinkommen.

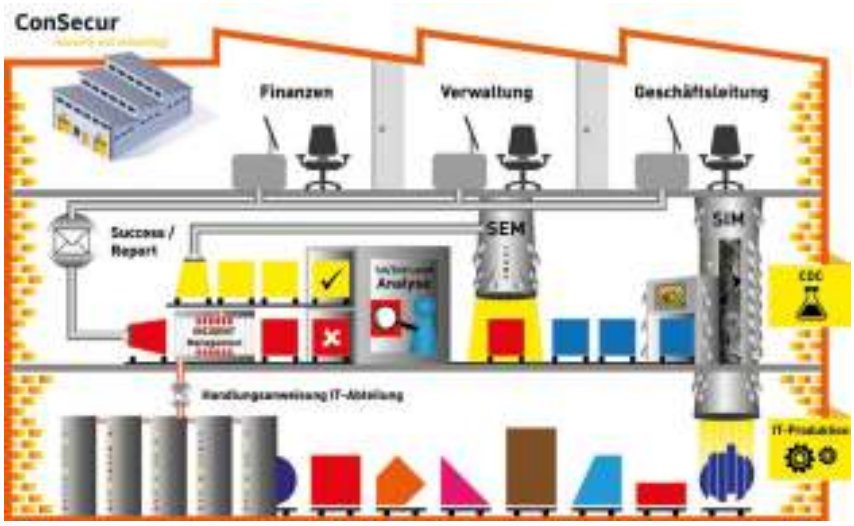
Damit genau das nicht passiert, gibt es das Cyber Defense Center der ConSecur GmbH. Hier überwachen unsere Security-Analysten rund um die Uhr die Sicherheit von IT-Infrastrukturen. Sie behalten Ihre Systeme permanent im Auge und analysieren sämtliche sicherheitsrelevanten Vorgänge. Im Zusammenspiel mit der bestehenden Sicherheitsarchitektur bietet das Cyber Defense Center einen Hochleistungsschutz für Ihre IT. Darüber hinaus erkennen unsere Analysten Schwachstellen und identifizieren Sicherheitsvorfälle aller Art.

Permanente Sicherheit für Ihre Information mit Managed SIEM

Damit haben Sie die Gewissheit, dass ausschließlich berechtigte Personen Zugang zu Ihrem Netzwerk und damit auf Informationen, Daten und Dokumente haben. Das gilt sowohl für Angreifer, die von außen auf Ihr Netzwerk zugreifen wollen, als auch für Innentäter aus den eigenen Reihen. Das Cyber Defense Center erkennt diese Angriffe rechtzeitig und leitet gezielte Abwehrmaßnahmen ein. Deshalb ist Ihre IT bei der ConSecur GmbH in den besten Händen.

Welche Vorteile bietet Managed SIEM?

Die Implementierung eines SIEM ist eine Sache, die Aufrechterhaltung aller sicherheitsrelevanten Maßnahmen eine andere. Hochwertige Sicherheitslösungen können Ihre Schutzwirkung nur entfalten und er-



halten, wenn sie kontinuierlich überwacht, geprüft, dokumentiert und analysiert werden. All dies benötigt eine enorme Menge an Wissen und beansprucht Ressourcen und Zeit. ConSecur unterstützt Ihre hauseigene IT nach Bedarf und organisiert mit Ihnen zusammen ein optimiertes Sicherheitsmanagement. Unternehmen und Organisationen profitieren von einem solchen Managed SIEM in mehrfacher Hinsicht: Zunächst schont das Managed SIEM die eigenen personellen Ressourcen und Systeme. Mitarbeiter, die ansonsten mit der Überwachung des SIEM beschäftigt wären, können sich ihren eigentlichen Aufgaben widmen. Die Kosten für ein Managed SIEM sind deutlich transparenter als bei einer hauseigenen Überwachung des SIEM, zudem wird die interne IT-Infrastruktur ebenfalls entlastet. Die Geschäftsführung hat damit die Gewissheit, dass Ihr Unternehmen durch Fachkräfte und IT-Experten im Einklang mit der hauseigenen IT gesichert wird und im Bedrohungsfall alle notwendigen Maßnahmen professionell durchgeführt werden.

ConSecur – Ihr Partner für Managed SIEM

Ziel unserer Arbeit ist es, Ihnen die größtmögliche IT-Sicherheit zu gewährleisten. Mit einem Managed SIEM übertragen Sie einen zentralen Aspekt Ihrer Informationssicherheit an uns. Wir sind uns der Verantwortung dieser Maßnahmen bewusst. Daher stehen wir mit all unserer Erfahrung und unserem Wissen für die Sicherheit Ihres Unternehmens ein. Unsere Experten analysieren zunächst ausführlich Ihre vorhandenen Maßnahmen zur Informationssicherheit und organisieren mit Ihnen zusammen das Management Ihres SIEM. Da Sie selbst Ihr Unternehmen am besten kennen, analysieren wir mit Ihnen gemeinsam die jeweiligen Maßnahmen und setzen Schwerpunkte in besonders sicherheitsrelevanten Bereichen. Managed SIEM durch ConSecur bedeutet, dass unser gesamtes Team hinter Ihrem Unternehmen steht. Wir entwickeln einen maßgeschneiderten Einsatzplan, stimmen Teams und Einsatzleiter aufeinander ab und halten Ihr SIEM durch kontinuierliche Überwachung und Prüfung auf dem höchsten Sicherheitsstand.

ConSecur betreibt für seine Kunden ein vollständiges Cyber Security Center und verfügt über umfangreiche Erfahrungen im Einsatz moderner SIEM-Tools wie HP ArcSight, Splunk oder IBM QRadar. Im Rahmen des Managed-Service-Modells setzen die Security-Spezialisten aus Meppen mit QRadar von IBM für ihre Kunden ein professionelles Monitoring aller potentiellen Sicherheitsvorfälle auf.

Dazu werden – individuell angepasst an die spezifische Infrastruktur des Kunden – in einem ersten Schritt die Log-Daten und -Events der unterschiedlichen Infrastrukturkomponenten gesammelt, gespeichert, normalisiert und analysiert. Im zweiten Schritt werden diese Informationen korreliert und teilweise um weitere Informationen angereichert. Bei der Korrelation der Daten werden dann auf Grundlage des Regelwerks potentielle Sicherheitsvorfälle identifiziert. Dabei nutzt ConSecur eine hauseigene Datenbank mit mehr als 400 typischen Mustern von Sicherheitsvorfällen, die die Erfahrung aus vielen Jahren in der Praxis bündelt.

Die Sicherheitsvorfälle meldet das SIEM-Tool dann an die Analysten des Cyber Defense Centers, die untersuchen, ob sich hinter der Anomalie ein tatsächlicher Sicherheitsvorfall verbirgt. Ist das der Fall, werden gemeinsam mit den verantwortlichen Fachabteilungen des Kunden entsprechende Gegenmaßnahmen eingeleitet.

Besonders interessant wird dieser Ansatz durch das Managed-Service-Modell auch für Unternehmen des Mittelstands, die oft nicht über ausreichend interne Ressourcen und die notwendige Erfahrung bei der Analyse von Sicherheitsvorfällen verfügen. Zwar setzen viele Unternehmen bereits gute Einzelkomponenten in ihrer IT-Sicherheitsinfrastruktur ein, scheitern aber beim konsequenten Monitoring der Komponenten im Zusammenspiel. Schon in Unternehmen mittlerer Größe entstehenden täglich Unmengen an Log- und Event-Daten. Ohne die entsprechende Unterstützung durch ein SIEM-Tool wie QRadar und das gebündelte Know-how eines speziell dafür ausgebildeten Cyber Defense Centers, können diese wichtigen Daten nicht ausgewertet werden. So bleiben wesentliche Sicherheitsvorfälle oft lange unentdeckt, obwohl im Grunde bereits viel Geld in hochwertige Sicherheitstechnik investiert wurde. Das Managed-Service-Angebot von ConSecur schließt genau diese Lücke.

ConSecur Portfolio Managed SIEM (Cyber Defense Center)

- **Security Monitoring (5/8 oder 24/7)**
- **Log- und Eventanalyse nach risikoorientierten Use-Cases**
- **permanente Weiterentwicklung durch professionelles Use-Case Management**
- **professionelles Incident Management zur Beseitigung von Sicherheitsvorfällen**
- **maximale Investitionssicherheit**
- **Einsatz eines SIEM Systems**

Mehr Informationen zu SIEM als Managed Service von ConSecur finden Sie hier: **www.consecur.de/siem**