DIAGNOSTIK AUF HÖCHSTEM NIVEAU

Ob Cyber-Defence- und Datenanalyse-Plattformen oder SIEM-Infrastrukturen – so holen Sie das Beste aus Ihren Investitionen heraus

Security Monitoring und Analytics ist inzwischen zur Pflicht für Unternehmen geworden. Ein gut funktionierendes SIEM (Security Information & Event Management) bringt wertvolle Einblicke und zweifelsohne mehr Sicherheit für die IT eines Unternehmens. Vorausgesetzt, das Tool wird für seinen Einsatzzweck optimal implementiert, konfiguriert und betrieben und in Cyber-Defence-Prozesse und weitere Technologien integriert.

SIEM-Lösungen – und Analyse-Plattformen insgesamt – sind flexibel anpassbar und erweiterbar, und bieten schier unendlich viele Möglichkeiten. Dies erfordert allerdings einen recht hohen Entwicklungs-, Integrations- und Betriebsaufwand – wofür umfassendes Expert:innenwissen nötig ist. Weil wie so oft auch in diesem Bereich Fachkräfte fehlen, kommen die Lösungen häufig nicht dazu, ihre Stärke optimal auszuspielen.

FACHWISSEN FÜR MEHR SICHERHEIT

Genau hier setzt unser SIEM Center of Excellence an. Aus jahrelangen Erfahrungen bei Aufbau, Konfiguration und Betrieb von Cyber Defence Centern wissen wir sehr genau, wie ein effizientes SIEM aussieht. Das SIEM Center of Excellence bündelt unser umfassendes Spezialist:innenwissen rund um die Themen Use-Case-Entwicklung, Dashboarding & Reporting, Analytics, Machine Learning, Automatisierung, Test, Rollout, Orchestration, Qualitätssicherung, Standardisierung und Best Practices rund um SIEM-Plattformen wie Splunk, Azure Sentinel, Exabeam Advanced Analytics und IBM QRadar. Wir beraten Sie einerseits bei der Auswahl der passenden Technologien und unterstützen Sie andererseits bei Aufbau, Konfiguration, Implementierung und Betrieb Ihrer Analyseplattform. So erhalten Sie auch ohne eigenes Fachwissen eine SIEM-Lösung, die höchsten Ansprüchen gerecht wird.

UNSERE SIEM-SERVICES

- SIEM STRATEGIE- UND TOOL-BERATUNG

  Haben Sie noch kein Analyse-Tool im Einsatz, erarbeiten wir gemeinsam mit Ihnen eine SIEM-Strategie und beraten Sie bei der Auswahl einer individuell passenden Technologie. Auf Basis Ihrer Ziele erarbeiten wir ein SIEM-Konzept und zeigen anhand einer Roadmap auf, wie die Umsetzung erfolgen kann – die Services unseres SIEM Center of Excellence unterstützen Sie gern dabei.

- AUTOMATION DER INFRASTRUKTUR

  Dieser Service umfasst den automatischen Rollout der Analyse-Plattform Ihrer Wahl. Ob Umgebungen mit wenigen Maschinen oder weltweit verteilte Umgebungen mit verschiedenen Standort-Ausprägungen, Größen, Komplexitäten und Verknüpfung mit dem Rest der IT-Landschaft des Kunden – wir haben schon alles gesehen und umgesetzt. Analog hierzu unterstützen wir auch bei Aktualisierung (Update/Upgrade), (SIEM-) Migration und Betrieb – und zwar mit automatisierten Lösungen. Das reduziert nicht nur Ihre Betriebsaufwände, sondern sorgt auch für stabile und leistungsfähige SIEM-Infrastrukturen.

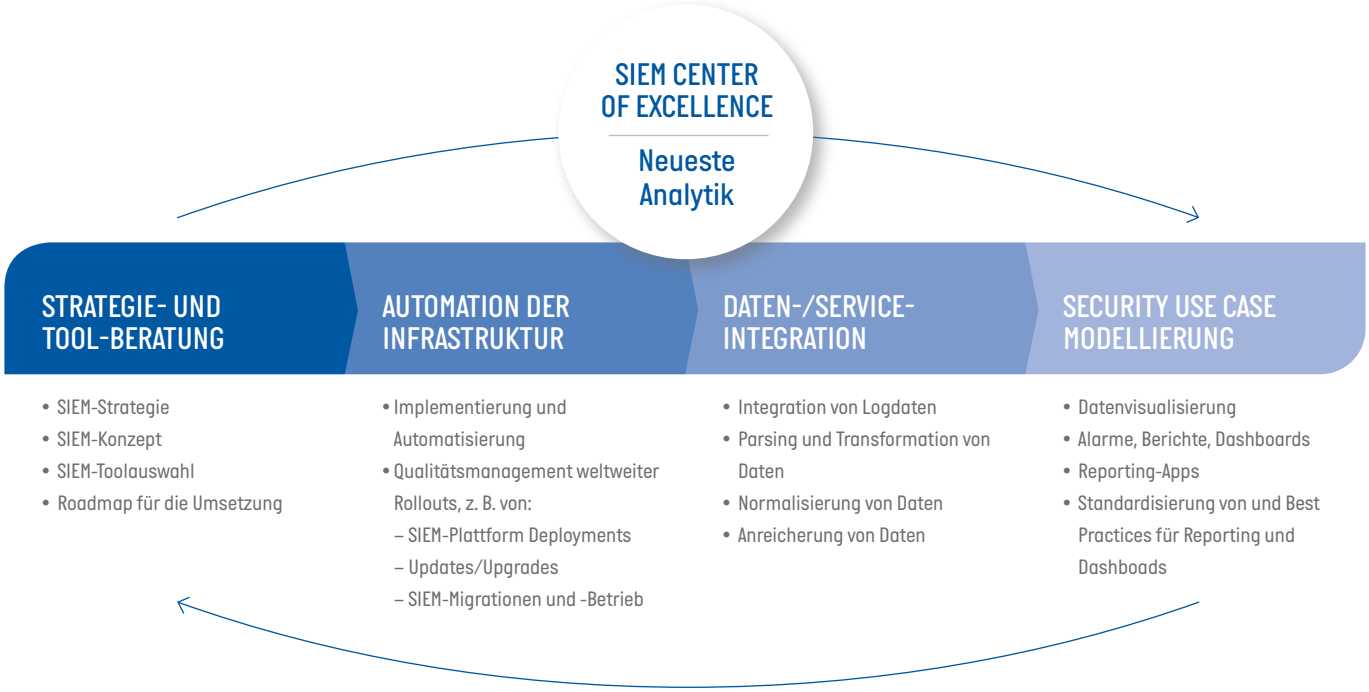
- DATEN-/SERVICE-INTEGRATION

  Dieser Service ist die Basis für den Erfolg bei der Arbeit mit Analyse-Daten. Denn er sorgt dafür, dass die Daten aus Logquellen als normalisierte Informationen beispielsweise im Datenmodell zur Verfügung stehen, um aussagekräftige Daten zu erhalten. Dies geschieht durch Parsing oder Transformation. Typischerweise müssen die Daten zusätzlich noch mit Informationen aus CMDB, Vulnerability-Management oder anderen Systemen angereichert werden, um die benötigte Aussagekraft zu erreichen. Eine komplexe und aufwändige, aber für den Erfolg unabdingliche Aufgabe. Mit Erfahrung, einem prall gefüllten Baukasten an Parsern und bewährten Methoden bringen wir Sie hierbei schneller und besser ans Ziel.

- SECURITY USE CASE MODELLIERUNG

  Damit Sie die erhobenen Daten auch nutzen können, müssen sie zielgruppengerecht aufbereitet und visualisiert werden. Bei der Use Case Modellierung werden Korrelationsregeln für Security Informationen mit Tool-Abfragesprache, Machine Learning und AI modelliert, implementiert und getestet. Außerdem entwerfen wir hier Alarme, Berichte, Dashboards und Visualisierungen und entwickeln bei Bedarf die passenden Apps.

Egal, wie komplex der Zusammenhang oder wie hoch die Erwartungen an die Aufbereitungsform auch sind, wir haben eine passende Lösung: von Standard-SIEM-Regeln aus unserer Regel-Bibliothek bis hin zu maßgeschneiderten SIEM-Regeln für spezifische Machine Learning Use Cases (beispielsweise Active Hunting, UEBA und Fraud-Detection) oder Cross-Analytics mit Daten aus VM-Systemen, CMDBs, Ticket-Systemen.



RELEVANTES AUF EINEN BLICK – EFFIZIENT UND ZUVERLÄSSIG

Die Zeiten, in denen Sie nur ungenügend über den Security-Zustand Ihrer IT informiert waren, sind mit den Services des SIEM Center of Excellence passé. Durch die weitgehende Automatisierung, konsequente Standardisierung, übergreifende Best-Practices, Knowledge Sharing, automatisierte Testprozeduren und ein übergeordnetes Qualitätsmanagement im SIEM Center of Excellence können Sie sich auf Ihre Analytics-Plattform verlassen: Unsere Services sorgen dafür, dass diese effizienter betrieben wird und gleichzeitig die Qualität stimmt. Mit individuellen Dashboards und Reportings – zielgruppengerecht aufbereitet – finden Sie im Dschungel der Logdaten künftig schnell und zuverlässig die für Sie relevanten Informationen. Auf dieser soliden Basis treffen Sie die richtigen Entscheidungen für ein sicheres Business.

UNSER KNOW-HOW RUND UM SIEM-PLATTFORMEN

Sie profitieren von unserem umfangreichen Fachwissen und unserer jahrelangen Erfahrung in Analytics- und SIEM-Projekten. Allein mit Splunk haben wir mehr als 100 Projekte umgesetzt, sind Splunk Elite Partner und haben über 60 Mitarbeiter:innen mit Splunk-Zertifikaten und -Akkreditierungen. Ergänzt werden diese durch umfangreiches Wissen über QRadar, Exabeam und Azure Sentinel.

In unserem Global Solution Center in München betreiben wir ein dediziertes Splunk-Entwicklungs- und Testlabor, wo die Entwicklung von der Quelle bis zur Anwendung – also von der Datenanbindung bis zu Analytics auf Basis des Mitre ATT&CK – zum Daily Business gehört. Unsere Security-Analysten analysieren Sicherheitsvorfälle und Angriffe und entwerfen, entwickeln und integrieren entsprechende Security-Regeln für SIEM Systeme.

Zudem können wir mit unserem Service „SIEM Platform Management“ den Betrieb von Splunk-SIEM-Umgebungen für unsere Kunden übernehmen.

Unternehmensprofil

Computacenter ist der führende, unabhängige Anbieter von IT-Infrastrukturservices und -lösungen für Großunternehmen und große Organisationen des öffentlichen Sektors. Wir unterstützen unsere Kunden bei der Beschaffung, Transformation und Verwaltung ihrer IT-Infrastruktur und bei der Umsetzung ihrer digitalen Transformation.

Computacenter ist eine Aktiengesellschaft, die im Londoner FTSE 250 Index notiert ist und weltweit rund 17.000 Mitarbeiterinnen und Mitarbeiter beschäftigt.

DIGITAL & Trust.
Mastering business security

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

computacenter.de
+49 (0)2273 5970