InfoGuard
SWISS CYBER SECURITY

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) SERVICE

Ihre Sicherheit in der Hand von Schweizer Cyber Security Experten.

Der SIEM (Security Information & Event Management) Service bildet den Grundpfeiler der InfoGuard SOC Services. Dank der real-time Analyse von Informationen aus Ihrer Infrastruktur werden Bedrohungen und Schwachstellen in der ICT-Infrastruktur aufgedeckt, so dass diese gezielt und schnell eliminiert werden können. Gleichzeitig erhalten Sie die vollständige Transparenz über die Sicherheit Ihrer ICT-Infrastruktur und können so das Sicherheitsniveau nachhaltig erhöhen.

- Professionelles Security Information & Event Management durch ausgewiesene Cyber Threat Analysten
- Überwacht Ihre Infrastruktur rund um die Uhr und erkennt externe und interne Bedrohungen frühzeitig
- Alarmiert bei Gefahren oder Störungen dank Echtzeit-Analyse
- Entlastet Ihre IT von der Analyse riesiger und komplexer Datenmengen
- Permanente Weiterentwicklung der Angriffsszenarien durch unsere Pentester und Analysten
- Unterstützt Sie bei der Einhaltung von Auflagen und Compliance-Anforderungen
- Wöchentliches Reporting und bedarfsgerechte Serviceerbringung zu fixen Kosten

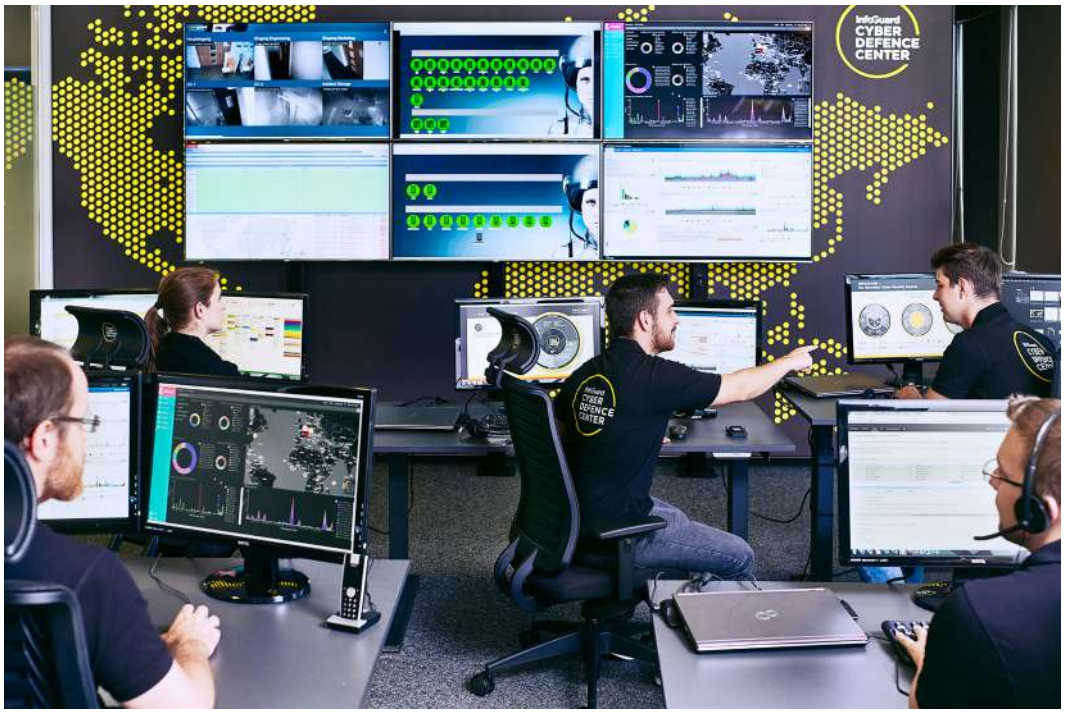
INFOGUARD SIEM SERVICE

Cyber Defence aus der Schweiz

Im Rahmen des SIEM Service übernimmt das InfoGuard Cyber Defence Center für den Kunden die Konsolidierung und Auswertung sicherheitsrelevanter Log-Daten und unterstützt auf Wunsch bei der Behebung von Schwachstellen. Gleichzeitig stehen Ihnen die InfoGuard-Experten rund um die Uhr mit ihrer langjährigen Erfahrung in der Cyber Security zur Verfügung. Dank fundierter Branchenkenntnis, der interdisziplinären Kompetenz zwischen offensiver und defensiver Cyber Security und der grossen Erfahrung im Bereich Penetration Testing und Ethical Hacking können wir einschätzen, welche Sicherheitsbedrohungen auf das jeweilige Unternehmen zutreffen. Der Standort in Zug, Geo-Redundanz, ein mehrstufiges Sicherheitskonzept und die redundante Auslegung von Strom-, Netzwerk- und Systemkomponenten garantieren zudem höchste Vertraulichkeit und Verfügbarkeit. Die Anbindung der Kundeninfrastruktur erfolgt über redundante site-to-site VPN-Verbindungen.

Erfahrung und Know-how von Cyber Threat Analysten

Unsere Cyber Threat Analysten setzen sich täglich mit der aktuellen Bedrohungslage auseinander und analysieren Informationen aus dem Darknet, von Threat Intelligence Feeds und weiteren Quellen. Sie erkennen und analysieren Bedrohungen, denen Ihr Unternehmen, Ihre Netzwerke und Systeme, sowie Applikationen und Services tagtäglich ausgesetzt sind und schlagen konkrete Massnahmen und Handlungsempfehlungen vor, noch bevor ein Schaden entsteht. Gestützt auf aktuellste Cyber Threat Intelligence sind unsere Analysten stets auf dem neusten Stand und Sie profitieren von den neusten Erkenntnissen in der Detektion von Cyber-Bedrohungen.



Durch standardisierte Incident Management-Prozesse (u.a. Triage, Recherche, Dokumentation) ist sichergestellt, dass die Qualität der Dienstleistungen konstant hoch gehalten wird und alle Schritte nachvollziehbar dokumentiert werden. Genau definierte Eskalationspfade vom Tier 1 Analyst über Tier 2 bis hin zum Tier 3 Teamansatz mit Pentestern stellen sicher, dass zu jedem Zeitpunkt die richtigen Ressourcen, mit dem entsprechenden Know-how involviert werden. Alle Services sind konsequent nach den ITIL-Prozessen gegliedert, umfassen präventive und reaktive sowie operative und strategische Komponenten. Sämtliche Leistungen werden mit einem «Service-Level-Agreement» (SLA) geregelt.

Unser SIEM Service umfasst:

Netzwerk und Asset Klassifikation
Ein wichtiger Bestandteil des SIEM Services ist die Gewichtung der Assets und der Netzwerke in Bezug auf die Bedeutung für Ihr Unternehmen. Diese Gewichtung ist essentiell bei der nachfolgenden Korrelation und Eskalation von Sicherheitsvorfällen.

Logdaten-Analyse in Echtzeit
Die SIEM-Plattform basiert auf der Technologie von IBM QRadar. Sie konsolidiert Ereignisdaten von tausenden Endpunkten und Anwendungen im gesamten Netz und führt Normalisierungs- und Korrelationsaktivitäten auf den Rohdaten aus, um echte Bedrohungen verlässlich zu erkennen und die Anzahl an Falschalarmen (sog. false-positives) zu minimieren. Über das webbasierte cyberguard Portal erhalten Sie Zugang zur SIEM-Plattform und können bei Bedarf selbstständig Logdaten in Echtzeit analysieren und auswerten.

Threat Detection dank InfoGuard Use Case Engineering
Nebst der Erkennung generischer Anomalien und Verhaltensweisen bauen die Detektionsmechanismen des InfoGuard Cyber Defence Center auf selbst erarbeiteten Bedrohungsszenarien, den InfoGuard Use Cases. Diese beinhaltet nebst der genauen Beschreibung der Bedrohung und den Erkennungsmerkmalen auch Reaktionspläne und Vorgehensanweisungen für den Ernstfall. Dies ermöglicht eine zielgerichtete und standardisierte Reaktion auf die Bedrohung einzuleiten. Mit dem SIEM Service profitieren Sie von der stetigen Weiterentwicklung der Use Cases durch unsere Pentester und Analysten.

Threat Intelligence
Die umfassenden Logging-Fähigkeiten der SIEM-Plattform und die integrierte Korrelations-Engine helfen bei der Analyse und Reaktion auf Angriffe, die von anderen Security-Lösungen nicht erfasst oder übersehen werden. Durch die Anreicherung mit minutengenauen Threat Intelligence Daten zu Sicherheitsbedrohungen im Internet können neue Gefahren und bereits infizierte Geräte schneller erkannt und priorisiert werden, was Attacken auf ein Minimum reduziert.

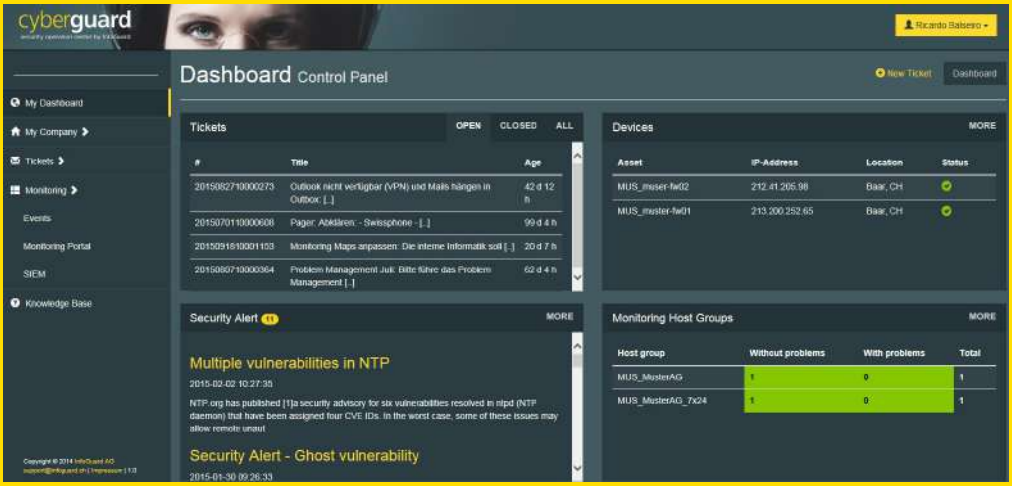
Ausbaumöglichkeiten des SIEM Services

Vulnerability Management
Schwachstellenscans können direkt über die SIEM-Plattform konfiguriert und auf die eigene Systemumgebung ausgeführt werden. Die Kombination mit unserem Vulnerability Management reichert die klassifizierten Assets mit wertvollen Schwachstelleninformationen an, welche für die kontinuierliche Verbesserung des Sicherheitsdispositivs und zur Priorisierung verwendet werden. Die dabei identifizierten Schwachstellen werden analysiert, damit die am stärksten exponierten Systeme prioritär geschützt werden können, bzw. die Regelwerke auf den maximalen Schutz dieser verwundbaren Systeme auszurichten. Zudem bieten der Service Virtual Patch Empfehlungen für die gängigsten IPS Hersteller an. So können extern zugreifbare Infrastrukturen auf Perimeter Ebene geschützt werden, bis die Schwachstelle beseitigt wird.

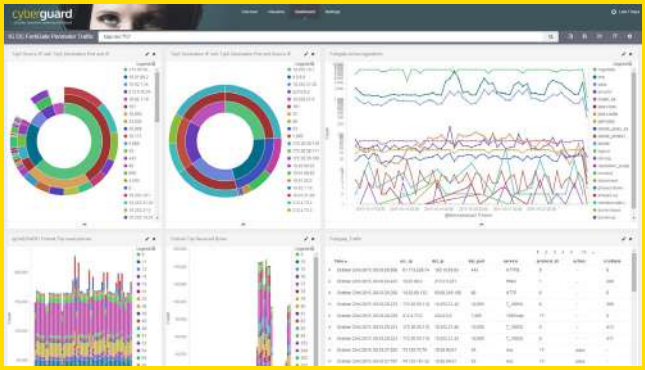
Security Incident Analysis & Response
Mit der Tanium Integration auf den Endpunkten werden bei einem detektierten Angriff im SIEM automatisiert Metadaten von Prozessen zur Analyse gespeichert. Unsere Cyber Threat Analysten können so effizient und schnell mit der Analyse eines Angriffes starten und im Bedarfsfall auch vom Kunden autorisierte Aktionen auf dem Endpunkt ausführen, um den Angriff einzudämmen.

MAXIMALE TRANSPARENZ RUND UM DIE UHR

Das webbasierte cyberguard Portal verschafft Ihnen rund um die Uhr einen schnellen Überblick über den aktuellen Status Ihrer Infrastruktur, alle offenen Tickets und die aktuelle Bedrohungslage. Die History informiert Sie zudem über das Geschehen während eines bestimmten Zeitraums. Gleichzeitig können Sie über das Online-Portal umfassende Reports generieren und Anpassungen am Service oder der Infrastruktur veranlassen.



Nebst den SIEM Dashboards können kundenspezifische Dashboards aus Logdaten nach Bedarf erstellt werden.



Der Security Information & Event Management Service von InfoGuard garantiert Ihnen höchste Service-Qualität zu fixen Kosten.

Cyber Defence Services – 7x24 aus dem ISO 27001 zertifizierten Schweizer SOC

Nebst dem SIEM-Service erbringen wir aus unserem ISO/IEC 27001 zertifizierten InfoGuard Cyber Defence Center in der Schweiz das gesamte Service-Spektrum: Angefangen von Support über ausgelagerte Cloud und Managed Security Services bis hin zum SOC-Service, bei welchem sich unsere Cyber Threat Analysten und Security Experten rund um die Uhr um Ihre Sicherheit kümmern.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
Telefon +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Schweiz
Telefon +41 31 556 19 00

INFOGUARD.CH