SOC ist nicht gleich SOC

Behalten Sie den Überblick und heben Sie Ihr SOC auf das nächste Level!

Die Bedrohung durch Cyberattacken ist vielfältig und Angreifer kombinieren oft verschiedene Angriffsarten, um ans Ziel zu gelangen. Unternehmen mit komplexen und hybriden Infrastrukturen haben oftmals eine mangelhafte Übersicht und Automatisierung - besonders bezogen auf Security Policies und vorhandene Angriffswege und Schwachstellen. Die Analyse eines Netzwerks auf akute Bedrohungen bedingt häufig qualifiziertes Personal mit Erfahrung und Thread Hunting und Mitigation, um Schwachstellen im eigenen Netzwerk aufzudecken, diese zu analysieren und zu bewerten. Diese Fachkräfte sind in der heutigen Marktsituation schwer zu finden und mit hohen Kosten verbunden.

Sie möchten Ressourcen sparen und besonders im Bereich IT- und OT-Security Ihr SOC- und NOC-Team effizient unterstützen? Sie möchten Ihr Risiko minimieren und Ihre Angriffsstellen kontinuierlich managen? Mit dem SOC 2.0 von AirITSystems sorgen Sie nicht mehr nur für die Pflicht, sondern können auch die Kür-Anforderungen nachhaltig meistern.

SOC 2.0 - individuelle Schwachstellen übersichtlich im Blick

Die Vulnerability Control von unserem Technik-Partner Skybox Security kann mit verbundenen Modulen wie der Firewall- und der Networkasurance Angriffsszenarien automatisiert abbilden und dabei den Bedarf an hochqualifiziertem Personal (Red und Blue Teams) verringern. Skybox Security ist in der Lage, relevante Schwachstellen aufzuspüren und den Administratoren gleichzeitig Lösungsansätze zu liefern.

500 der größten Unternehmen der Welt verlassen sich auf Skybox Security, wenn es um Einblicke und Sicherheit geht, die erforderlich sind, um den sich dynamisch verändernden Angriffsflächen voraus zu sein. Die Exposure Management Platform bietet umfassende Transparenz, Analysen und Automatisierung, um Schwachstellen in Ihrem Unternehmen schnell zu erfassen, zu priorisieren und zu beheben. Die anbieterunabhängige Lösung optimiert Sicherheitsrichtlinien, den Betrieb und Änderungsprozesse in allen Unternehmensnetzwerken und Cloud-Umgebungen.

SKYBOX SECURITY

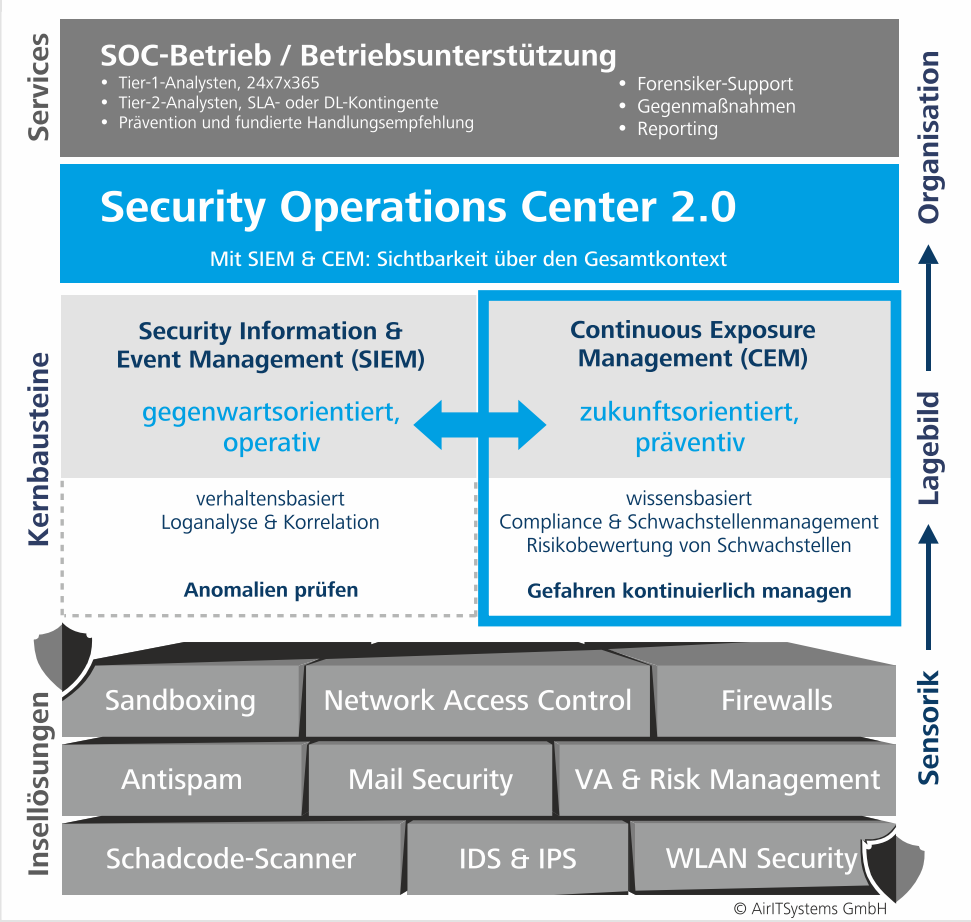
Die Vorteile vom SOC 2.0 im Überblick:

- Kontinuierliches Event-Tracking
- Prävention statt Reaktion - durch konsolidierte Erkennung von Schwachstellen mit Datenanreicherung
- Effizient und zeitsparend durch kontextbezogene Priorisierung
  - Durch inventarisierte Assets und Schwachstellenscans sind veröffentlichte Schwachstellen der im Unternehmen verwendeten Applikationen automatisiert und jederzeit zugeordnet
  - Ermöglicht die einfache Identifizierung der individuell relevanten Schwachstellen
  - Priorisierung vorhandener Schwachstellen samt Lösungsvorschlägen auch ohne tiefere Fachkenntnisse der Cybersecurity möglich
- Automatisierte Dokumentation (bspw. Regelwerksoptimierung)
- Übersicht von Security-Lücken (u. a. mit tagesaktuellem Netzwerkmodell) inkl. Angriffssimulation
- Planbarkeit der Security-Entwicklung
- Durchsetzung und Kontrolle von Richtlinien und Sicherheitskonzepten (Audit und Compliance)
- Zentrale Logspeicherung zur möglichen Aufarbeitung von Security-Incidents

IT Security im Wandel

Reaktiv war gestern - kontinuierlich und präventiv ist heute

Ein SIEM bietet eine kontinuierliche Überwachung von Logs, um auftretende Anomalien schnellstmöglich zu erkennen. Doch auch bereits potenzielle Angriffe sind vorzubeugen. Dafür setzt AirITSystems zusätzlich auf die Prävention durch ein gezieltes Schwachstellenmanagement im SOC.



Ein zukunftssicheres SOC 2.0 verbindet SIEM mit einem Continuous Exposure Management (CEM)
Das SOC 2.0 bietet eine Plattform, die einerseits Security-Event-Analysen durch gezielte Korrelation qualifizierter Analysten durchführt und andererseits Schwachstellen gegenwärtig sowie zukunftsorientiert managt. Es ermöglicht dadurch eine vollständige Übersicht über die IT- und OT- Infrastruktur - inklusive der Analyse möglicher Angriffspfade zu begehrlichen Punkten und Schwachstellen der individuellen Systemlandschaft. Sie erhalten somit eine einzigartige übersichtliche Visualisierung und die Möglichkeit, die Angriffspfade rasch zu neutralisieren bzw. abzusichern.

Warum AirITSystems? Weil Sicherheit nicht optional ist.
IT- und Sicherheitslösungen von erfahrenen KRITIS-Experten
Wir sind ein Gemeinschaftsunternehmen der Flughäfen Hannover und Frankfurt. Unsere Herkunft ist der Flughafen. Damit sind Sicherheit und das Zusammenspiel zahlreicher Komponenten in einem komplexen System unser tägliches Geschäft: eine Vielzahl von Transaktionen, kritische Verfügbarkeit und als klare Anforderung höchste Sicherheit. Diese einzigartige Flughafenerfahrung übertragen wir und unsere zertifizierten Spezialisten mit derselben Sorgfalt auch auf alle anderen Branchen.

NEUGIERIG GEWORDEN? JETZT DEMO VEREINBAREN

AirITSystems GmbH
Benkendorffstr. 6
30855 Langenhagen

Tel.: +49 511 9364 4357
vertriebsinnendienst@airitsystems.de

FÜR WEITERE STANDORTKONTAKTE HIER SCANNEN