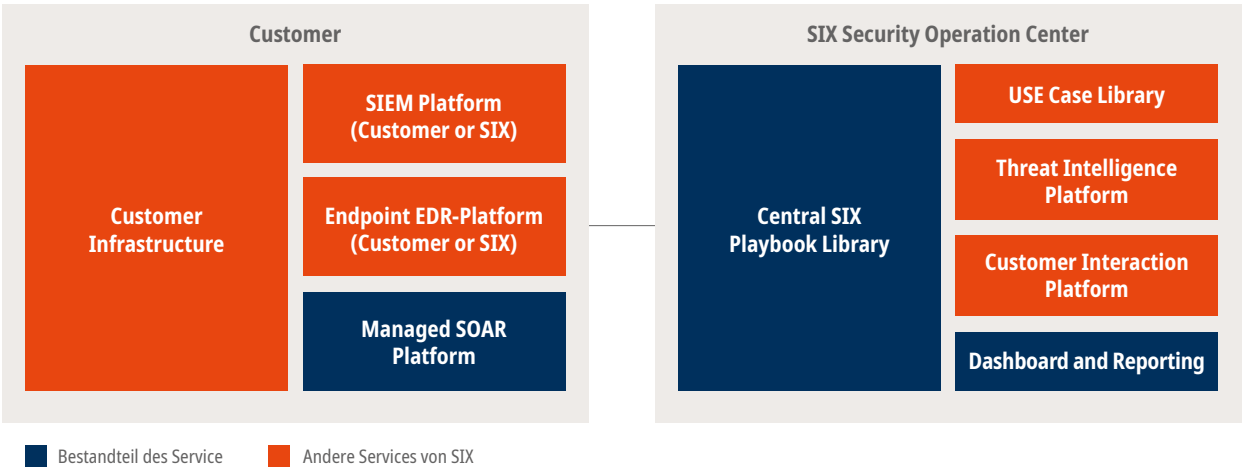
Managed SOAR

Security Orchestration, Automation und Response

Managed SOAR trägt zur Entlastung Ihrer Sicherheitsexperten und zur Verkürzung der Reaktionszeit bei Sicherheitsvorfällen bei. Zusätzlich kann Managed SOAR die Automatisierung Ihrer Workflows optimieren.



So profitiert Ihr Unternehmen

- Finance-driven Playbooks von SIX: Profitieren Sie von dem geistigen Eigentum von SIX und davon, wie SIX ihre eigene systemkritische Infrastruktur schützt.
- Preisgünstigere und besser qualifizierte Ressourcen: Steigern Sie die Kosteneffizienz Ihrer Sicherheitskräfte.
- Vereinfachte Governance, Risk und Compliance: Nutzen Sie die umfangreiche Erfahrung von SIX in Regulierung und Compliance in der Finanzindustrie.

So profitiert Ihr SOC

- Erhöhte Konsistenz des Cyber Security Prozesses zur Incident Response: Automatisieren Sie Ihren Workflow.
- Verkürzte Zeit für Triage, Analyse und Reaktion: Gewinnen Sie mehr Zeit für komplexere Security Projekte.
- Entlasten Sie Ihre SOC-Analysten von langweiligen und repetitiven Aufgaben.

Über den Service

Plattform-Management und -Betrieb

SIX unterstützt Sie bei der Konfiguration, Anpassung und beim Management der benötigten Komponenten, so dass Sie effektiver auf Vorfälle reagieren können. Das bedeutet, dass SIX die SOAR-Plattform bei Ihnen vor Ort betreibt und managed.

SIX konfiguriert und managed die SOAR-Plattform. Sie wird in mindestens zwei Instanzen (Testinstanz und produktive Instanz) eingeführt. Der Service umfasst Upgrades und Patches. SIX integriert Ihre SIEM-Lösung, um dadurch sicherzustellen, dass Sie über generierte Vorfälle oder wesentliche Ereignisse auf Ihrer SOAR-Plattform in Echtzeit informiert sind.

Security Orchestration

Orchestrieren Sie Ihren ganzen Workflow und integrieren Sie Ihre Tools.

Der Service beinhaltet die Orchestrierung Ihrer verschiedenen Tools wie SIEM, Ticketingsystem, E-Mail, Threat Intelligence Platform, möglicher CIP (Customer Identity Provider) oder CMDB. Das schafft für Sie die Möglichkeit, Sicherheitsvorfälle zu untersuchen und auf sie zu reagieren. Ausserdem umfasst der Service Schulung und ein vordefiniertes Basis- oder Standard-Set von Playbooks. Die Playbooks werden immer in enger Zusammenarbeit entwickelt.

Der Service kann folgende Bestandteile umfassen:

1. Sie nutzen die Funktionalitäten der SOAR-Plattform, wie Integration von Standard-Playbooks und Automatisierung.
2. Sie nutzen die Automatisierungen und die Playbooks von SIX, wie abstrakte, plattformunabhängige Befehle, für individuelle Untersuchungsschritte.
3. Sie erstellen Ihre eigenen Playbooks und stellen die Kompatibilität sicher. SIX steht für Unterstützung gerne zur Verfügung.

Security Automation

Machen Sie die bisherige menschliche Interaktion zu einem Workflow.

SIX unterstützt Sie bei der Automatisierung von mehreren manuellen Tätigkeiten, um das SIEM einzusetzen, und integriert Ihre SIEM-Lösung durch Workflows, damit Sie unter Einsatz der SOAR-Plattform zusammen funktionieren. SIX unterstützt Unternehmen bei der Konfiguration, Personalisierung, Integration und Bereitstellung der SOAR-Playbooks, um die Reaktionszeit zu reduzieren.

Der Service kann folgende Bestandteile umfassen:

1. Unterstützung beim Herausfinden, welche Aufgaben automatisiert werden können, und bei ihrer Anpassung
2. Qualitätsanalyse der Workflows.

Security Investigation and Response

Die Lösung wird an Ihre Vorgaben, Tools und Prozesse angepasst. Unsere Experten werden Sie gerne beraten, unterstützen und betreuen.

Funktionalitäten:	
Verwaltung der Plattform vor Ort	Enthalten
Verfügbarkeit gemäss einem SLA	99.9%
Integration der Standard-Playbooks (Content Pack)	Enthalten
Integration der allgemeinen Playbooks von SIX	Optional
Entwicklung und Integration der kundenspezifischen Playbooks	Optional
Integration in Ihres SIEM	Enthalten
Integration in Ihres Ticketingsystem	Enthalten
Lese-/Schreibzugriff auf die Testumgebung	Optional
Lese-/Schreibzugriff auf die produktive Umgebung	Nicht möglich

SIX – Ihre starke Partnerin aus der Finanzindustrie

Ihre Vorteile

- SIX ist die einzige Dienstleisterin in der Schweiz, die eine Cyber Threat Intelligence (CTI) mit Fokus Finanzthemen anbietet.
- SIX entwickelt Use Cases für den Finanzsektor und aktualisiert diese fortlaufend.
- SIX ist selbst systemkritisch und hat als Betreiberin von systemkritischen Infrastrukturen eine Insider-Sicht auf relevante und sektorspezifische Bedrohungen.

Das könnte Sie auch noch interessieren:

- SOC as a Service
- Incident Response Support
- Digital Risk Monitoring
- Vulnerability Management

SIX Group Services AG
Pfingstweidstrasse 110
Postfach
8005 Zürich

T + 41 58 399 3993
cybersecurity@six-group.com
www.six-group.com/cybersecurity

Ihr Ansprechpartner
Dieter Bartl
Senior Cyber Security Sales Manager
T +41 58 399 3575
dieter.bartl@six-group.com