



Threat Intelligence Platform as a Service

Sammeln und vergleichen Sie Ihre Quellen für Threat Intelligence

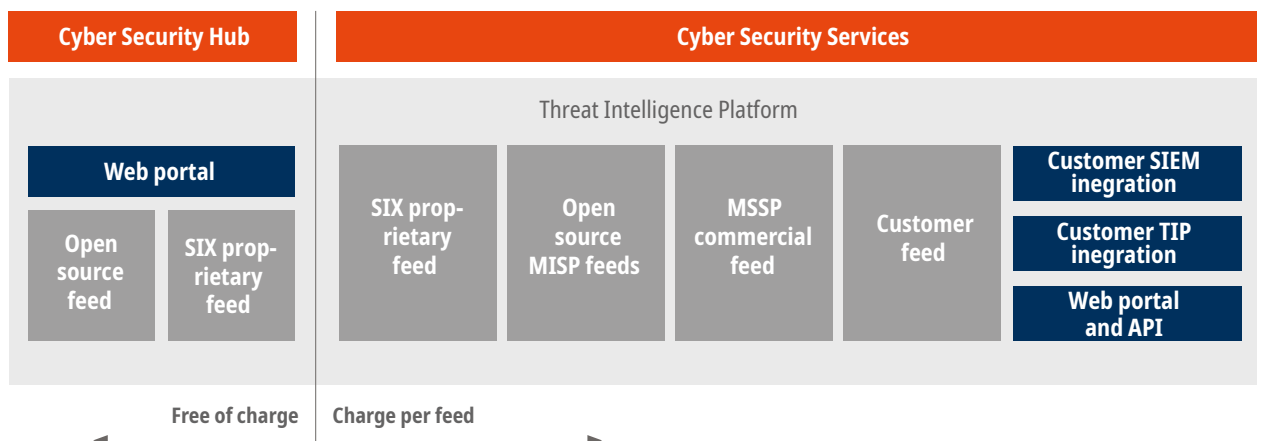
Eine effektive Threat Intelligence verbessert die Qualität Ihrer Analysen. Entscheidend ist dabei sicherzustellen, dass die richtigen Feeds und Informationen an einem Ort gesammelt und in Ihre Umgebung integriert werden.

Eine bloße Sammlung verschiedener Feeds überfordert viele Sicherheitsteams. Eine weitere wichtige Herausforderung besteht darin, herauszufinden, wie effektiv die globalen Feeds für ein Schweizer Finanzinstitut sind und welche sich als absolut notwendig erweisen. Aus diesem Grund betreibt SIX eine Threat Intelligence Plattform, die auf Feeds von relevanter Bedeutung für die Schweizer Finanzbranche ausgerichtet ist.

Darüber hinaus fügt SIX regelmässig eigene Feeds und Bedrohungsinformationen hinzu. Dies stellt sicher, dass

die Threat Intelligence Plattform von SIX nicht nur «eine weitere Quelle von Threat Intelligence», sondern eine kontinuierlich optimierte Plattform für den Schweizer Finanzplatz ist.

Schliesslich können die bestehenden Feeds von Kunden hinzugefügt werden. Das Gesamtergebnis kann entweder über einen Webzugriff oder durch die Integration der Threat Intelligence Plattform mithilfe einer kundenseitigen API verbraucht werden.



Leistungsversprechen und Vorteile des Service

Mit Threat Intelligence Plattform as a Service können Sie Ihre Sicherheitslage durch die Cyber Threat Intelligence (CTI) verbessern, die für den Schweizer Finanzplatz optimiert ist und sich in Ihr eigenes oder Managed SIEM integrieren lässt. Die Hauptvorteile sind:

- schnellere und sachbezogenere Erkennung von Bedrohungen.
- proaktive Prävention von Bedrohungen, die sich auf Ihre Organisation auswirken.
- aggregierte und zentral verwaltete Threat Intelligence Feeds. Sie umfassen die von einem Kunden unmittelbar erhaltenen Feeds, aber auch solche, die zielorientiert sind und von SIX ausgewählt wurden, sowie Feeds, die SIX als Security Service Provider bezieht.
- Erkenntnisse von SIX und unseren Kunden. Sie verbessern die Qualität der Threat Intelligence Informationen für die Schweizer Finanzbranche.
- Indicator of Compromise (IoC) auf der Grundlage einer branchenführenden Threat Intelligence Plattform, die an ein eigenes oder Managed SIEM geliefert werden.
- Integration der Threat Intelligence Plattform in Ihre Systeme. Machen Sie sich keine Sorgen mehr um verschiedene Feeds, die integriert werden müssen.

Der Service

Threat Intelligence Plattform

SIX betreibt eine weltweit führende Threat Intelligence Plattform mit Funktionen, die es ermöglichen, komplexe Aufgaben effizienter zu erledigen.

Webzugriff/Dashboard

Webzugriff auf die Threat Intelligence Plattform jederzeit. Die Kunden können den Kontext in Bezug auf den Indicator of Compromise in den vorhandenen Feeds nachschlagen.

Integration mit SIEM

Direkte Integration der Threat Intelligence Plattform entweder in Ihr vorhandenes SIEM oder in ein hochentwickeltes SOC as a Service Modul von SIX.

Kundenseitige Integration der TIP

Das Feed kann in eine vorhandene Threat Intelligence Plattform des Kunden (z.B. MISP) über eine API integriert werden.

Feeds

Um die Qualität der bereitgestellten Feeds kontinuierlich abzustimmen und zu optimieren, werden vom Threat Intelligence Team von SIX entsprechende Analysen durchgeführt.

- MSSP-Feeds von SIX
- Open-Source-Feeds (MISP)
- Kommerzielles Feed
- Phishing-Feed von SIX
- Feeds des Kunden
- Kommerzielles Feed (wie FS-ISAC, Mandiant, usw.)
- Nicht-kommerzielles Feed
- Vertikale spezifische Feeds
- Eigene Feeds oder Intelligenz des Kunden

Service Level Agreement

- Verfügbarkeit der Plattform: 99,9%

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
- Digital Risk Monitoring
- Incident Response Support
- Vulnerability Management

Keine der hierin enthaltenen Informationen begründet ein Angebot oder eine Empfehlung zum Kauf oder Verkauf eines Finanzinstrumentes. SIX Group AG bzw. ihre direkten und indirekten Tochtergesellschaften (nachfolgend SIX) haften weder dafür, dass die enthaltenen Informationen vollständig, richtig, aktuell und ununterbrochen verfügbar sind, noch für Schäden von Handlungen, die aufgrund von Informationen vorgenommen werden, die in dieser oder einer anderen Publikation von SIX enthalten sind. SIX behält sich ausdrücklich vor, jederzeit die Preise oder die Produktzusammenstellung zu ändern. © SIX Group AG, 2020. Alle Rechte vorbehalten.

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