DATENBLATT

FireEye Threat Intelligence API

Branchenführende FireEye-Bedrohungsdaten direkt in Ihrer Sicherheitsinfrastruktur

FEATURES

Die Threat Intelligence API ermöglicht Unternehmen, die Bedrohungsdaten von FireEye in ihre Umgebung zu integrieren und an ihre Anforderungen anzupassen. Sie bietet folgende Vorteile:

- **Unterstützung für Structured Threat Information Expression (STIX) 2.1:** Verwendung eines JSON-Datenformats, das die bidirektionale Nutzung von Bedrohungsdaten vereinfacht (Beisteuern zum und Einspeisen aus dem Datenpool) und die Beziehungen zwischen Datenobjekten aufrechterhält
- **Schnelle Bereitstellung von Indikatoren:** Extraktion von Indikatoren aus Berichten und Bereitstellung nahezu in Echtzeit, um Unternehmen eine zeitnahe Reaktion zu ermöglichen
- **Zuverlässigkeitsbewertung:** Zuverlässigkeitsbewertung von Indikatoren mithilfe einer vordefinierten Skala (0–100)
- **Digital Threat Monitoring:** Abrufen und (benutzerdefiniertes) Filtern großer Datenmengen, die über den FireEye-Service Digital Threat Monitoring bereitgestellt werden
- **Erweiterte Metadaten:** Metadatenfelder für den Ausschluss bestimmter Indikatoren und die Integration externer Referenzquellen in Berichten
- **Flexible Berichterstellung:** Bedrohungsprofile in maschinell (STIX 2.1) und für Menschen lesbaren (PDF, HTML) Formaten
- **Intelligente Suche:** Auf Suchmustern bzw. Beziehungen basierende Suchvorgänge, die das schnelle Auffinden relevanter Informationen ermöglichen

Mit der API für FireEye Threat Intelligence können Sicherheitsteams in Unternehmen bei alltäglichen Entscheidungen schnell und unkompliziert hochwertige Bedrohungsanalysen heranziehen.

FireEye-Kunden können die branchenführenden Bedrohungsdaten von FireEye direkt in ihren vorhandenen Sicherheits- und Compliance-Management-Technologien nutzen, um Bedrohungen wirksam zu erkennen, zu untersuchen und abzuwehren. Die API verknüpft die Sicherheitstechnologien des Kundenunternehmens mit der Threat Intelligence Cloud von FireEye, einem Cybersicherheits-Repository, das über den weltweit größten Bestand an Bedrohungsdaten (und einen Erfahrungsschatz aus über zehn Jahren) verfügt.

Einfach, flexibel und integrationsfreundlich

Die FireEye Threat Intelligence API ermöglicht eine Machine-to-Machine-Integration der ergiebigsten Kontextdaten, die derzeit auf dem Markt verfügbar sind. So erhalten Unternehmen automatisch Zugang zu Gefahrenindikatoren (wie IP-Adressen, Domain-Namen und häufig von Angreifern verwendeten URLs) und detaillierte Informationen zu den Hackern, was die Wirksamkeit der vorhandenen Sicherheitssysteme weiter stärkt. Die API unterstützt die Programmiersprachen Python, Java, PHP, C++ und C#. Weitere Informationen finden Sie in der **Online-Dokumentation für die FireEye Threat Intelligence API**.

Tabelle 1: Features der FireEye Threat Intelligence API v3.	
Indikatoren	Indikatoren mit bzw. ohne Kontext (Indikatoren aus Berichten UND Indikatoren ohne Berichte)
Berichte	Unterstützte Formate: • HTML • PDF • STIX 2.1 JSON
Angreifer- und Malware-Daten	Gefahrenindikatoren und Berichte mit Angaben zu Angreifergruppen, Malware-Familien und Beziehungskontext
Suche	Auf Beziehungen bzw. Mustern basierende Suchvorgänge
Wechsel zwischen verschiedenen Suchen	Beziehungsbasierte Suchvorgänge

Anwendungsbereiche

Der unmittelbare Zugang zu FireEye Threat Intelligence hilft Unternehmen, fundierte Entscheidungen zu treffen, ihre Prozesse anzupassen und gezielt Prioritäten zu setzen, um von einer reaktiv ausgerichteten Sicherheitsstrategie zu einem proaktiven Ansatz überzugehen. Die API unterstützt zahlreiche Aspekte eines typischen Sicherheitsprogramms:

- **Sicherheitsprozesse:** Sie können Ereignisse in Ihrer SIEM- oder Analyseplattform mit entsprechenden Gefahrenindikatoren abgleichen. Auf diese Weise können Sie die wichtigsten Ereignisse automatisch identifizieren, um die Warnungsflut zu bewältigen.
- **Incident Response:** Da die Bedrohungsdaten von FireEye direkt in Ihre IR-, Analyse- und Forensik-Tools eingespeist werden, können Sie sich ein genaues Bild über jede Situation verschaffen.
- **Schwachstellen- und Patchmanagement** Sie erhalten hochaktuelle Informationen über die neuesten Schwachstellen und Exploits – oft noch bevor sie in die National Vulnerability Database aufgenommen werden oder eine CVE-Nummer erhalten.
- **Netzwerkaktivitäten:** Sie erhalten sorgfältig validierte Gefahrenindikatoren und können daher sicher sein, dass Sie auf echte Bedrohungen reagieren.

Wenn Sie wissen möchten, wie FireEye Threat Intelligence Ihr Unternehmen dabei unterstützen kann, Cyberbedrohungen immer einen Schritt voraus zu sein, besuchen Sie: **www.fireeye.de/solutions/cyber-threat-intelligence.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE