DATENBLATT

Entwicklung von Funktionen zur Erfassung und Analyse von Bedrohungsdaten

Verbessern Sie Ihre Fähigkeiten im Umgang mit Bedrohungsdaten

HIGHLIGHTS

- Optimieren Sie die Verarbeitung, Analyse und Nutzung von Bedrohungsdaten für Cybersicherheitsprozesse.
- Nutzen Sie unsere mehr als 12-jährige Erfahrung bei der Entwicklung von Funktionen zur Erfassung und Analyse von Bedrohungsdaten für staatliche Stellen und kommerzielle Unternehmen.
- Ermitteln Sie Ihre derzeitigen Fähigkeiten im Umgang mit Bedrohungsdaten und identifizieren Sie Verbesserungspotenzial.
- Ermitteln Sie anhand eines Cyberrisiko-Profils, welche Bedrohungsdaten für Ihr Unternehmen von Wert sind und wo sie eingesetzt werden sollten.
- Planen Sie die strategischen, taktischen und operativen Unternehmensziele unter Einbeziehung von Bedrohungsdaten.
- Stärken Sie die CTI-Kompetenz im Unternehmen mithilfe von Workshops, in denen Ihre Mitarbeiter lernen, CTI-Funktionen effektiv in den Betriebsablauf einzubinden.

Cyberkriminelle haben oft ein besseres Know-how, ein größeres Budget und mehr Ressourcen als Sicherheitsteams in Unternehmen. Das führt dazu, dass Cyberangriffe immer ausgefeilter werden und größeren Schaden anrichten. Aufgrund des anhaltenden Fachkräftemangels fällt es vielen Unternehmen zudem schwer, auch nur einen einzigen qualifizierten neuen Mitarbeiter für die Sicherheitsabteilung zu finden und einzuarbeiten. Nur die wenigsten Unternehmen haben die Mittel, um die ganze Bandbreite des erforderlichen Expertenwissens intern abzudecken.

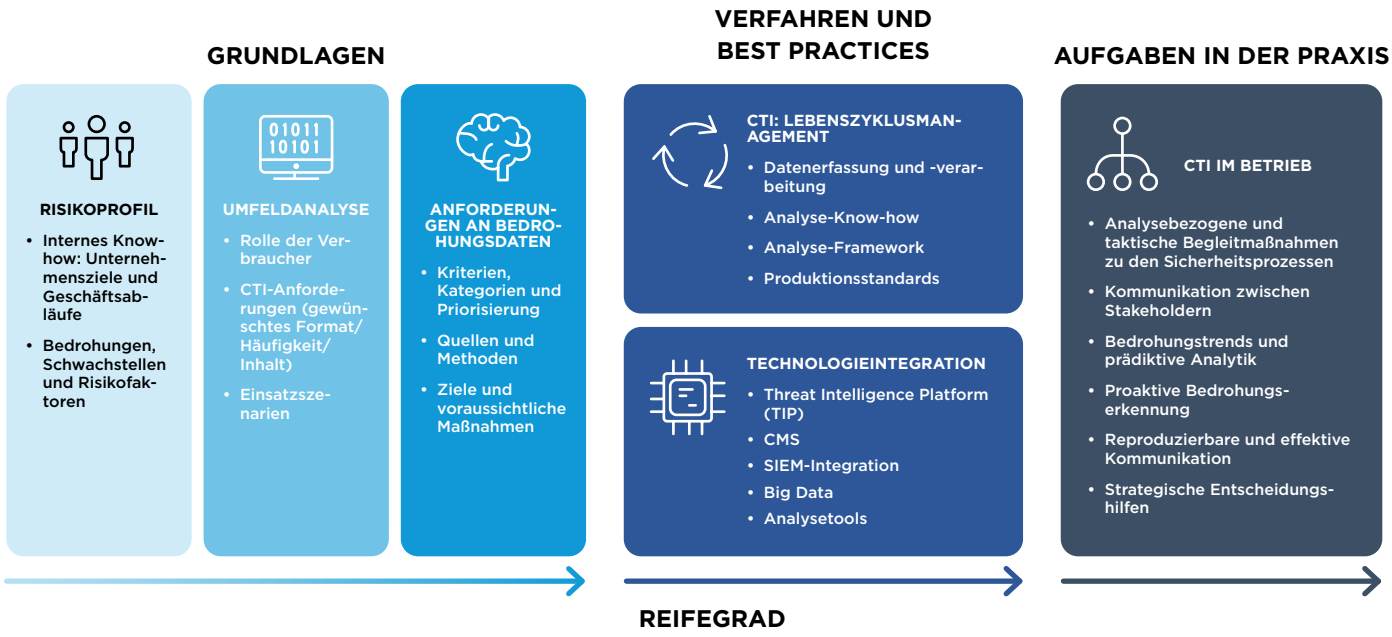
Daher versuchen immer mehr Unternehmen, das Risiko von Cyberbedrohungen mithilfe von CTI-Services (Cyber Threat Intelligence, Cyberbedrohungsdaten) einzudämmen. Doch wo setzt man am besten an? Aus Unwissenheit entscheidet sich so manches Unternehmen einfach für irgendeine Lösung, ohne wirklich zu verstehen, welche Bedrohungsdaten für die Unternehmensstruktur sinnvoll sind und wie sie genutzt werden sollten. Das führt in der Regel zu Ineffizienz und hohen Kosten. Unternehmen müssen wissen, wie sie eine höhere Rendite aus ihren CTI-Investitionen erzielen können.

Die ICD-Services (Intelligence Capability Development) von FireEye sind speziell für die Erfassung und Analyse von Bedrohungsdaten konzipiert und zielen darauf ab, CTI-Services voll auszuschöpfen. In den letzten zehn Jahren haben sich Hunderte von Unternehmen von den ICD-Experten von FireEye zuverlässig beraten lassen und Best Practices für die Nutzung, Analyse und praktische Anwendung von Cyberbedrohungsdaten entwickelt, wodurch ihre Sicherheitsprogramme wirksamer und effizienter geworden sind.

So unterstützen wir unsere Kunden

Wir bieten verschiedene CTI-Services an, die standardisierte Rahmenparameter nutzen, um Ihr Threat-Intelligence-Programm sowie aktuelle Bedrohungsdaten zu **bewerten**, Verbesserungsvorschläge im Hinblick auf die Richtlinien Ihres Unternehmens und gesetzliche Anforderungen **auszuarbeiten** und die unternehmensinternen Fähigkeiten in Bezug auf die Erstellung aussagekräftiger Analysen und die gezielte Anwendung von Bedrohungsdaten zu **verbessern**.

Mit diesen Rahmenbedingungen werden die wichtigsten Aspekte eines wirksamen CTI-Programms definiert.



Unsere ICD-Services decken ein sehr breites Anforderungsspektrum ab, von relativ kurzen Projekten mit einem eng gefassten Aufgabenbereich bis hin zur Implementierung vollständiger Threat-Intelligence-Programme. Das Ziel ist immer, Unternehmen dabei zu unterstützen, externe Bedrohungsdaten so nutzbringend wie möglich einzusetzen und zu diesem Zweck bietet FireEye unter anderem folgende Services:

- **Threat Intelligence Foundations (TIF)**
  Wir schaffen die Voraussetzungen für die effektive Nutzung von Bedrohungsdaten. Neben relevanten Bedrohungen wird auch identifiziert, für welche Personen Bedrohungsdaten von Interesse sein können. Außerdem erarbeiten wir praxisbezogene Verfahren für eine effektive Bereitstellung und Nutzung der Bedrohungsdaten. [Bewerten]
- **Cyber Threat Diagnostic (CTD)**
  Wir überprüfen die aktuelle Infrastruktur Ihres Unternehmens auf Hinweise auf Angriffsversuche und bewerten so die Bedrohungslage Ihres Unternehmens. Die Ergebnisse halten wir in einem Situationsbericht fest. Die Einschätzung der Bedrohungslage ist ein wichtiger Bestandteil der datengestützten Sicherheit, denn sie versetzt Ihr Sicherheitsteam in die Lage, Schutzmaßnahmen an die Motive und Absichten der Angreifer anzupassen und entsprechend zu priorisieren. [Bewerten]
- **Intelligence Capability Assessment (ICA)**
  Wir bewerten die aktuellen Fähigkeiten Ihres Unternehmens im Umgang mit Bedrohungsdaten und die Nutzung dieser Daten im Rahmen Ihres Sicherheitsprogramms. Zudem erhalten Sie eine strategische Roadmap einschließlich einer Analyse der Sicherheitslücken, damit Sie Ihre Ressourcen – Mitarbeiter, Prozesse und Technologie – gezielt zur Verbesserung der Sicherheitsinfrastruktur einsetzen können. [Bewerten]
- **Intelligence Capability Uplift (ICU)**
  Wir erstellen einen Leitfaden für die Implementierung eines erstklassigen Threat-Intelligence-Programms mit skalierbaren, reproduzierbaren Prozessen für die Erfassung, Analyse und Verbreitung relevanter Daten im gesamten Unternehmen. [Ausarbeiten]
- **Intelligence Jumpstart**
  Bietet eine Einführung zum Leistungsumfang der Beratungsdienste von FireEye. In diesem eintägigen Workshop erläutern unsere strategischen und taktischen Analysten anhand von technischen und operativen Anwendungsszenarien, wie Bedrohungsdaten wirksam in Ihrem Unternehmen genutzt werden können. [Ausarbeiten]
- **Analytic Tradecraft Workshop (ATW)**
  In diesem eintägigen Workshop werden die unternehmensinternen Fähigkeiten in der Analyse und Nutzung von Bedrohungsdaten gestärkt. Zu den Themen gehören grundlegende CTI-Konzepte, strukturierte Analyseverfahren, Kommunikation in Bezug auf Bedrohungen sowie Bedrohungs- und Risikomanagement. [Verbessern]
- **Hunt Mission Workshop**
  Ihr Team erlernt systematische Vorgehensweisen, um die Bedrohungssuche innerhalb Ihres Unternehmens zu standardisieren. Dabei werden unter Berücksichtigung der bereits in Ihrem Unternehmen etablierten Methoden reproduzierbare Best Practices für die Bedrohungssuche ermittelt. Der Workshop richtet sich an SOC-, IR- und taktische Datenanalysten, die für die Erkennung und Abwehr von Bedrohungen verantwortlich sind. [Verbessern]

Was spricht für FireEye?

Eine strategische Partnerschaft mit FireEye stellt sicher, dass Ihre Mitarbeiter, Prozesse und Verfahren unabhängig von der Größe Ihrer Infrastruktur den Herausforderungen immer neuer Bedrohungen gewachsen sind.

Unser ICD-Team (Intelligence Capability Development) kann auf mehr als 10 Jahre Erfahrung bei der Entwicklung von Funktionen zur Erfassung und Analyse von Bedrohungsdaten zurückgreifen. Diese macht sich unter anderem bei der Nutzung von FireEye Threat Intelligence und der Entwicklung von Best Practices bezahlt. Im dritten Quartalsbericht für 2018, „The Forrester New Wave™: External Threat Intelligence Services", hat Forrester Research nur einen einzigen Anbieter von Lösungen für Bedrohungsdaten als „Leader" eingestuft – FireEye.

FireEye unterstützt seit über einem Jahrzehnt Unternehmen aus verschiedensten Branchen dabei, CTI-Funktionen wirksam in ihr Sicherheitsprogramm zu integrieren. Im Laufe der Zeit hat sich dadurch ein Service-Angebot entwickelt, das sich an die Anforderungen und Ziele jedes Unternehmens anpassen lässt. Medienkonzerne, Regierungsbehörden und privatwirtschaftliche Unternehmen auf der ganzen Welt vertrauen auf unsere Kompetenz und unsere Lösungen im Bereich Bedrohungsdaten.

ICD-Services können miteinander kombiniert oder einzeln genutzt werden, um die Entwicklung und Pflege eines umfassenden Programms für die Nutzung von Bedrohungsdaten zu unterstützen.

Weitere Informationen erhalten Sie unter **https://www.fireeye.de/solutions/cyber-threat-intelligence/intelligence-capability-development.html** und im **Forrester-Bericht**.

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.