FIREEYE™

## Lösungsübersicht

# Einsatzbereiche für Bedrohungsdaten

## Incident-Response-Experten

### Herausforderungen für Incident-Response-Teams

Incident-Response-Experten sind bei Cyberangriffen als Erste im Einsatz. Sie analysieren mutmaßliche Sicherheitsverletzungen, identifizieren komplexe Angriffe, führen Reverse-Engineering-Maßnahmenund foren-sische Untersuchungen durch und beheben gegebenenfalls den entstandenen Schaden. Die Teams bestehen in der Regel aus erfahrenen Sicherheits-analysten, die unter Umständen als Level-2- und/oder Level-3-Analysten zu einem SOC (Security Operations Center) gehören.

Zu den aktuellen Herausforderungen für Incident-Response-Experten gehören:

- Sie müssen schnell einschätzen, welche Vorfälle tatsächlich eine Bedrohung darstellen, und die Bearbeitung von Sicherheitsverletzungen dem Risiko entsprechend priorisieren.
- Sicherheitsverletzungen müssen bestimmten Hackern und Kampagnen zugeordnet werden.
- Sie betreiben aufwendige Suchen in Bedrohungs- und Wissensdatenbanken, um Details zu komplexen Angriffen und den TTP der Hacker zu finden.
- Ihnen obliegt es, Führungskräften die Auswirkungen von Sicherheitsproblemen auf das Unternehmen begreiflich zu machen, damit diese die Bedrohung nachvollziehen und entsprechende Maßnahmen veranlassen können.

Einer Umfrage zufolge kosten Fehlalarme Unternehmen im Durchschnitt 1,27 Millionen US-Dollar pro Jahr.


**So profitieren Incident-Response-Experten von Cyberbedrohungsdaten**
Mithilfe von Bedrohungsdaten können Incident-Response-Experten schwerwiegende Bedrohungen besser erkennen, schnell Fragen zu den Angriffsdetails (wer, was, warum, wann und wie) beantworten, Abwehrmaßnahmen und die Schadensbehebung beschleunigen sowie Beweise für bereits stattgefundene, aber bis dato unerkannte Angriffe auf das Unternehmensnetzwerk finden.

**Tabelle 1:** Einsatzbereiche – Incident-Response-Teams

| Einsatzbereich | Ziel | Erforderliche Bedrohungsdaten |
|---|---|---|
| **Validierung und Priorisierung von Sicherheitsvorfällen** | • Ermitteln der relevanten Bedrohungen für das Unternehmen und Priorisieren der Sicherheitsvorfälle, die die größte Gefahr für den Geschäftsbetrieb darstellen | • Gefahrenindikatoren in den Kontextinformationen der Bedrohungsdaten |
| **Analyse von Sicherheitsvorfällen** | • Beantworten der Fragen zu den Angriffsdetails (wer, was, warum, wann und wie)<br>• Ermitteln, ob der Angriff noch läuft, und Identifizieren der Folgen des Angriffs | • Gefahrenindikatoren mit Kontextinformationen zu Kampagnen, Hackern und Zielen<br>• Bedrohungsdatenbank mit detaillierten Informationen zu bisherigen Angriffen und Techniken |
| **Eindämmung von Angriffen und Schadensbehebung** | • Blockieren der Kommunikationskanäle der Angreifer<br>• Entfernen von Malware und Rückgängigmachen der Änderungen<br>• Patchen der Sicherheitslücken | • Bedrohungsdatenbank mit detaillierten Informationen zu bisherigen Angriffen und Techniken |
| **Spurensuche** | • Aufdecken bisher unerkannter Angriffe, die in Verbindung mit aktuellen Sicherheitsvorfällen oder Bedrohungen der Branche, Region, Anwendungen usw. stehen | • Gefahrenindikatoren mit Kontextinformationen zu Kampagnen, Hackern und Zielen<br>• Bedrohungsdatenbank mit detaillierten Informationen zu bisherigen Angriffen und Techniken |

### Validierung und Priorisierung von Sicherheitsvorfällen: Einschätzung der potenziellen wirtschaftlichen Folgen

Wenn ein Level-1-SOC-Analyst Sicherheitsvorfälle an den Incident-Response-Experten weiterleitet, muss dieser die Bedrohungen priorisieren und entscheiden, in welchen Fällen detaillierte Untersuchungen durchgeführt werden sollen. Mithilfe der Cyberbedrohungsdaten kann er besser einschätzen, welche Angriffe gezielt auf das Unternehmen gerichtet sind und welche den größten Schaden anrichten könnten.

Außerdem lässt sich damit der gesamte Vorgang beschleunigen, da die Bedrohungsdaten Kontextinformationen zu den Gefahrenindikatoren enthalten, zum Beispiel zu potenziellen Hackern, ihren Motiven (finanziellen, wirtschaftlichen und ideologischen), ihren bevorzugten Angriffszielen und den Folgen ihrer bisherigen Angriffe. Anhand dieser gesammelten Informationen sortieren Incident-Response-Experten die Kampagnen aus, die auf andere Unternehmensarten (oder Kunden) abzielen, und können dann die knappen Analyseressourcen für die tatsächlich relevanten Angriffe nutzen, die wichtige Geschäftsprozesse oder wertvolle Daten bedrohen.

### Analyse von Sicherheitsvorfällen: Reverse-Engineering der Angriffe

Incident-Response-Experten müssen nach dem ersten Anzeichen eines Vorfalls zeitnah ermitteln, ob der Angriff noch läuft, welche Änderungen an den Systemen und Anwendungen vorgenommen wurden und ob Schaden angerichtet wurde, also ob Daten gestohlen oder Geschäftsabläufe beeinträchtigt wurden. Mithilfe der Cyberbedrohungsdaten können sie Fragen (wer, was, warum, wann und wie) besser beantworten und sich einen Überblick über den Angriff verschaffen.

Aussagekräftige Daten helfen dem IR-Team, Warnmeldungen und Gefahrenindikatoren den entsprechenden Ereignissen und technischen Spuren zuzuordnen. Beispielsweise können die Experten anhand von Bedrohungsdaten überprüfen, ob mit einem gefundenen Malware-Sample bereits eine bekannte IP-Adresse verbunden ist, die die Malware in der Regel kontaktiert. So lässt sich zum Beispiel schnell feststellen, ob diese bekanntermaßen von einer Hackergruppe als Command-and-Control-Server genutzt wird. Anhand der Logdateien des Netzwerks können die Incident-Response-Experten ermitteln, ob auch andere Unternehmenssysteme mit diesem Server kommuniziert haben, wodurch sich mit hoher Wahrscheinlichkeit sagen lässt, ob diese ebenfalls infiziert sind.

Wenn es in einer Wissensdatenbank ein Repository mit Bedrohungsdaten gibt, können Incident-Response-Experten dort detaillierte Informationen zu den Identitäten und Techniken der Angreifer, ihren Zielen, den TTP und den Folgen für die angegriffen Unternehmen abrufen. So wissen die IR-Teams, wo sie nach Hinweisen auf die Urheber des Angriffs suchen müssen, und können leichter feststellen, welche Aktivitäten durchgeführt wurden, welche Techniken zum Einsatz kamen und ob der Angriff noch läuft.

### Eindämmung von Angriffen und Schadensbehebung: Schließen von Datenlecks und Patchen von Sicherheitslücken

Incident-Response-Experten stellen anderen IT-Teams im Unternehmen die notwendigen Daten bereit und unterstützen sie so dabei, Angriffe einzudämmen und den Schaden zu beheben.

Eine Bedrohungsdatenbank enthält alle wichtigen Informationen zu den Motiven, Techniken und Infrastrukturen der Hacker, denen bereits Angriffe zugeordnet wurden. Mithilfe dieser Angaben können laufende Angriffe blockiert werden, indem beispielsweise die Kommunikation mit einem externen Command-and-Control-Server unterbrochen oder die mit Phishing-Kampagnen gestohlenen Anmeldedaten deaktiviert werden.

Wenn die IT-Teams wissen, wie bestimmte Hacker Systeme angreifen und wie die bevorzugte Malware der Gruppen funktioniert, können sie infizierte Systeme schneller erkennen, die Malware entfernen, Änderungen an der Systemregistrierung und an Dateien rückgängig machen und Sicherheitslücken schließen, damit derartige Angriffe nicht wiederholt werden können.

### Spurensuche: Proaktive Aufdeckung verborgener Angriffe

Die meisten Unternehmen gehen heutzutage davon aus, dass ihre Sicherheitslösungen über kurz oder lang von Hackern überwunden werden und Malware sich unerkannt im Netzwerk festsetzen kann. Mit einer Spurensuche sollen derartige Angriffe proaktiv aufgedeckt werden.

Bei einer reaktiven Suche wird mithilfe von Cyberbedrohungsdaten nach bisher unerkannten Angriffen gesucht, die in Verbindung mit aktuellen Sicherheitsverletzungen stehen könnten. Wird zum Beispiel ein Zusammenhang zwischen einem aktuellen Vorfall und einer Phishing-Kampagne festgestellt, finden sich in den Bedrohungsdaten eventuell Hinweise darauf, dass hinter dieser Kampagne eine bestimmte Hackergruppe steckt, die noch für weitere Kampagnen und Watering-Hole-Angriffe bekannt ist. Da in diesem Fall die Wahrscheinlichkeit sehr hoch ist, dass die Gruppe das Unternehmen über mehrere Vektoren angegriffen hat oder angreifen wird, kann das IR-Team gezielt nach Hinweisen auf andere Phishing-Kampagnen suchen und überprüfen, ob Mitarbeiter die Watering-Hole-Website der Hacker besucht haben.

Proaktive Spurensuchen beruhen auf der Annahme, dass Hackergruppen, die für Angriffe auf ein Unternehmen in einer bestimmten Branche oder auf bestimmte Systeme bekannt sind, auch andere Unternehmen in derselben Branche oder mit denselben Systemen ins Visier nehmen werden. In Bedrohungsdaten (und vor allem den umfassenden Repositorys) finden die Spurensucheteams detaillierte Informationen dazu, welche Hacker es mit höchster Wahrscheinlichkeit auf ihr Unternehmen abgesehen haben. Außerdem finden sie Hinweise darauf, wo sie am besten im Unternehmensnetzwerk nach Beweisen für einen Angriff suchen.

### Vorteile von FireEye Threat Intelligence für IR-Teams

- Umfassende, validierte Bedrohungsdaten aus der Branche und zugehörige Indikatoren
  - Umfassende Kontextinformationen zu Hackern, Kampagnen und TTP
  - Überblick über zahlreiche Hackeraktivitäten von finanziell motivierten Angriffen bis zu Cyberspionage und Hacktivismus
  - Weltweite Quellen und Analysen
  - Datenbank mit Informationen aus acht Jahren
- Zuverlässige API für die Integration in Unternehmenstools und -prozesse
- Kompatibel mit wichtigen Incident-Response-Tools von Partnern
  - Analysen: Splunk, BAE, Palantir und Maltego
  - Endpunktschutz: Tripwire und Ziften
  - TIP: ThreatConnect, Anomali und ThreatQuotient
  - IR: Resilient Systems und viele andere

### Das Ergebnis

Mit den zuverlässigen, praxisrelevanten Bedrohungsdaten und Kontextinformationen von FireEye können Incident-Response-Experten schnell fundierte Entscheidungen treffen, um …

- Ereignisse zu identifizieren, die sofort untersucht werden müssen,
- isolierte Gefahrenindikatoren bestimmten Hackern und Kampagnen zuzuordnen und dadurch die Quelle und die Ziele eines Angriffs schneller zu ermitteln,
- gründliche Untersuchungen durchzuführen und Fragen zu den Angriffsdetails (wer, was, warum, wann und wie) zu beantworten,
- laufende Angriffe schneller zu blockieren und dadurch die Schäden für das Unternehmen zu minimieren,
- eine Wiederholung ähnlicher Vorfälle in Zukunft zu vermeiden und
- Spurensuchen durchzuführen und unerkannte Malware im Unternehmensnetzwerk aufzuspüren.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

**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.