DATENBLATT

Threat Intelligence als Abonnement

Stärkeren Unternehmensschutz durch aussagekräftige Bedrohungsdaten

HIGHLIGHTS

- Umfassende, praxisrelevante Bedrohungsdaten in unterschiedlichen Sicherheitsbereichen
- Zugriff auf Informationen, die über den typischen Angriffszyklus hinausgehen, wie den Kontext und die Priorität globaler Bedrohungen
- Stärkerer Schutz Ihrer Ressourcen und Zugang zu Expertenwissen für eine fundiertere Risikoeinschätzung
- Tipps zum optimalen Einsatz Ihrer Sicherheitsressourcen für den Schutz gegen Bedrohungen und Angreifer, denen Ihr Unternehmen wahrscheinlich ausgesetzt ist
- Unterstützung beim Erreichen taktischer, operativer und strategischer Unternehmensziele
- Bessere Priorisierung und Reaktion auf Warnmeldungen sowie schnelleres Patching von Sicherheitsschwachstellen

Cyberkriminelle haben oft ein besseres Know-how, ein größeres Budget und mehr Ressourcen als Sicherheitsteams in Unternehmen. Hinzu kommt, dass Cyberangriffe immer ausgefeilter werden und größeren Schaden anrichten. Vielen Unternehmen fällt es schwer, auch nur einen einzigen qualifizierten neuen Mitarbeiter für die Sicherheitsabteilung zu finden und im Unternehmen zu halten. Kaum ein Unternehmen kann es sich leisten, die ganze Bandbreite des erforderlichen Expertenwissens intern abzudecken.

Sicherheitsteams suchen daher nach Möglichkeiten, um ihre Fähigkeiten und Fachkenntnisse auszubauen und Sicherheitsmaßnahmen zu stärken. Dabei ist es besonders wichtig, die Incident-Response-Fähigkeiten des Teams zu verbessern, festzustellen, welchen Risiken das Unternehmen am ehesten ausgesetzt sein könnte und die Sicherheitsstrategie auf die Abwehr dieser Angriffe abzustimmen. Und das alles natürlich im Rahmen des festgelegten Budgets.

Tabelle 1: Vorteile von FireEye Threat Intelligence

Mit relevanten Bedrohungsdaten können Sie ...	Vorteil
Feststellen, welchen Risiken Unternehmen in Ihrem Tätigkeitsbereich, Ihrer Branche oder Ihrer Region am häufigsten ausgesetzt sind	Sie können frühzeitig in die entsprechenden Sicherheitslösungen investieren, um solchen Risiken vorzubeugen.
Entscheiden, welche Warnmeldungen Sie priorisieren und mit entsprechenden Kontextinformationen anreichern sollten	Sie können Bedrohungen schneller erkennen, die Zahl der Fehlalarme reduzieren, um Ihre Analysten zu entlasten, und dafür sorgen, dass Ihren Mitarbeitern stets die passenden Daten zur Verfügung stehen
Ermitteln, welche Sicherheitslücken am ehesten ausgenutzt werden könnten und daher zuerst gepatcht werden sollten	Sie können durch effektiveres Patching das Risiko erfolgreicher Eindringversuche erheblich reduzieren

FireEye Threat Intelligence schafft hier mit einem umfassenden Angebot an kostengünstigen Abonnements und praxistauglichen, effektiven Experteneinblicken auf strategischem, operativem und taktischem Niveau Abhilfe.

Zu den Threat Intelligence-Abonnements, die an die Anforderungen Ihres Unternehmens angepasst werden, zählen:

- **Fusion:** Umfassende Einblicke in aktuelle, historische und mögliche zukünftige Bedrohungen. Im Leistungsumfang miteinbezogen sind die Funktionen der folgenden Abonnements: Operational, Cyber Crime, Cyber Espionage, Cyber Physical (größtenteils) und eine Version der FireEye Digital Threat Monitoring-Services.
- **Operational:** Technische Analyse von Malware und damit verbundenen Taktiken, Techniken und Prozessen (TTPs), die von bekannten Hackern verwendet werden, sowie Zugang zu einer Datenbank mit Malware- und Angreiferprofilen und Gefahrenindikatoren, die nicht manuell verarbeitet werden müssen und die zusätzlichen Kontext zur Bedrohungslage bieten.
- **Cyber Physical:** Praxistaugliche Einblicke in Cyberbedrohungen und -risiken, die auf Industrieanlagen, industrielle Steuersysteme (ICS) und andere Betriebstechnik (OT) abzielen. Zu diesen Einblicken zählen sämtliche von FireEye-Experten gesammelten OT- und ICS-bezogenen Bedrohungsdaten.
- **Cyber Crime:** Detaillierte Überwachung und Analysen finanziell motivierter Hacker: Was sind ihre Angriffsziele, Methoden und Beweggründe?
- **Cyber Espionage:** Kontextinformationen über bekannte APT-Gruppen (Advanced Persistent Threat), die mutmaßlich von spezifischen Regierungen/Staaten unterstützt werden, darunter ihre Angriffsziele sowie ihre Taktiken, Techniken und Prozesse. Diese vermitteln Sicherheitsteams ein besseres Verständnis der Angreifer und ermöglichen eine schnellere, gezielte Reaktion auf Bedrohungen.
- **Strategic:** Branchen- und regionsspezifische Bedrohungsanalysen mit Informationen über die geopolitische Lage und Entwicklungen, die die Bedrohungslandschaft beeinflussen könnten, sowie Prognosen zum kurz- und langfristigen Entwicklungverlauf verschiedener Cyberbedrohungen.
- **Vulnerability:** Risikobewertung von Software-Schwachstellen in proprietären Technologien, um die Wahrscheinlichkeit zu ermitteln, dass diese Schwachstellen von Hackern ausgenutzt werden und um entsprechende Gegenmaßnahmen zu empfehlen.

Wir tragen unsere Ergebnisse und Bedrohungsdaten üblicherweise in Sicherheitsberichten zusammen. Zudem erhalten Sie bei Bedarf Bedrohungsdaten und Gefahrenindikatoren, die Sie direkt in Ihre bestehenden Sicherheitsprodukte wie SIEMs und Vulnerability Manager einspeisen können. Zu dem Leistungsumfang von Threat Intelligence zählen zudem:

- **FireEye Intelligence Portal:** Online-Zugriff auf Ihre Sicherheitsberichte und auf umfassende, für Ihr Abonnement-Modell relevante Informationen aus unserer FireEye Threat Intelligence-Datenbank. Außerdem können Sie Gefahrenindikatoren herunterladen und mit bestimmten Bedrohungsdaten über Angreifer, Malware, Branchen und andere Suchkriterien vergleichen.
- **Kontakt zu Analysten:** Unterstützung durch dedizierte FireEye Threat- und Technical Intelligence-Analysten, die Ihnen ein tieferes Verständnis verschiedener Hacker, Bedrohungen und Risiken, sowie der Vorteile praxistauglicher Bedrohungsdaten für Ihr Unternehmen, vermitteln können.
- **Bereitstellungsoptionen:** Sie bestimmen, über welche Kommunikationskanäle Sie Ihre Bedrohungsdaten erhalten, wie zum Beispiel in Form von E-Mail-Benachrichtigungen oder -Zusammenfassungen.
- **Tägliche Nachrichtenanalyse:** Mit diesem Service erhalten Sie jeden Tag eine E-Mail mit den Top-Stories der Cybersicherheitsbranche, sodass Sie umfassend über die aktuelle Sicherheitslage informiert sind. Jede E-Mail enthält die jeweiligen Medienberichte, eine Einschätzung von FireEye-Experten zu ihrer Glaubwürdigkeit sowie relevante Hintergrundinformationen und Gegenmaßnahmen.
- **Intelligence API:** Einfache Integration unserer Bedrohungsdaten und Gefahrenindikatoren in Ihre Sicherheits- und Netzwerkinfrastruktur, Ihr Vulnerability Management und in Ihre Incident Response-Systeme.
- **Browser-Plug-in:** Mit unserem Plug-in lässt sich FireEye Threat Intelligence in alle von Ihnen genutzte Websites integrieren. Die Anwendung prüft Websites auf technische Bedrohungsindikatoren (wie verdächtige IP-Adressen, Domains und Hashes), nutzt die Intelligence API zur Suche nach Übereinstimmungen der erfassten Daten mit den Datenbeständen von FireEye Threat Intelligence und stellt dann einen Hyperlink zu den relevanten Bedrohungsdaten her.
- **Analysetools:** Mithilfe dieser mit Bedrohungsdaten verbundenen Online-Tools können Sie Kontextinformationen zu Domainnamen, IP-Adressen und Bedrohungen abrufen und verdächtige Dateien zur Analyse hochladen.

Selbst die erfahrensten Sicherheitsteams sind nicht allwissend. Auch den Experten fehlen manchmal wichtige Informationen über Angreifer, Bedrohungen, Schwachstellen und die besten Methoden zur Spurensuche und Angriffsabwehr. Eben hier kommt FireEye ins Spiel: Mit unseren Threat Intelligence-Abonnements stehen Ihnen das Know-how, die Erfahrung, die Einblicke und Analysefunktionen des führenden Anbieters von Bedrohungsdaten zur Verfügung und wir können Ihren Teams somit umfassende, über Jahre zusammengestellte Ressourcen zum Schutz Ihres Unternehmens an die Hand geben.

Was spricht für FireEye?
FireEye weiß mehr über Cyberbedrohungen und Hacker als die meisten anderen Unternehmen, und dank unseren außerordentlich umfassenden Bedrohungsdaten aus fortlaufenden Untersuchungen sind unsere Experten immer auf dem neuesten Stand. In Kombination mit Informationen aus Incident-Response-Einsätzen, Kampagnen, der Beobachtung von Cyberkriminellen und Telemetriedaten zu unseren Produkten können wir Kunden einen Sicherheitsservice bieten, der seinesgleichen sucht. Mit FireEye Threat Intelligence profitieren Sie von:

- Der Erfahrung Hunderter Datenwissenschaftler in 23 Ländern weltweit, die über 30 Sprachen beherrschen und im Deep und Dark Web Hacker aufspüren, ihre Taktiken, Beweggründe und Ressourcen ermitteln und diese überwachen.
- Den Erkenntnissen aus über 15.000 Netzwerksensoren, die wir an Kundenstandorten installiert haben und mit denen wir ständig kommunizieren, um immer darüber auf dem Laufenden zu sein, welchen Bedrohungen unsere Kunden in aller Welt ausgesetzt sind.
- Informationen über die TTPs erfolgreicher Hacker aus den Einsätzen der Experten von FireEye Mandiant, dem führenden Unternehmen für Incident Response.
- Der branchenweit umfassendsten Datenbank über Angriffe, Hacker und Bedrohungen, in der wir seit vielen Jahren die Informationen ablegen, die wir bei Einsätzen bei unseren Kunden erfassen.
- Der Expertise des Unternehmens, das als einziger Anbieter als „Leader“ in „The Forrester New Wave™: External Threat Intelligence Services, Q3 2018“ erscheint.

DEDIZIERTER KUNDENSUPPORT

Unsere Intelligence Enablement-Services bieten drei Supportstufen (Levels) zur Nutzung und Unterstützung von Bedrohungsdaten an:

STUFE 1

Baseline: Diese Option schließt eine Übersicht über die zur Nutzung des Bedrohungsdaten-Portals erforderlichen Ressourcen und Prozesse sowie eine Einweisung in die Konfiguration des Intelligence API für Ihr Unternehmen bzw. Ihre Institution ein.

STUFE 2

Koordinierung: Zusätzlich zu den in der Baseline-Version enthaltenen Aktivierungsschritten erhalten Sie mit diesem Supportniveau Unterstützung durch Analysten von FireEye und wir weisen Ihnen einen dedizierten Intelligence Enablement-Manager zu.

STUFE 3

Optimierung: Zum Leistungsumfang gehören die Funktionen der Abonnementsniveaus Baseline und Koordinierung. Zusätzlich wird Ihnen ein dedizierter Intelligence Optimization-Analyst zugewiesen, Sie erhalten speziell auf Ihr Unternehmen abgestimmte Bedrohungsberichte und Sie haben Zugang zu strategischen Workshops und Besprechungen zur aktuellen Bedrohungslage.

Weitere Informationen erhalten Sie unter **https://www.fireeye.de/solutions/cyber-threat-intelligence/threat-intelligence-subscriptions.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.