

DATENBLATT

FireEye Managed Defense

Managed Services zur Bedrohungserkennung und -abwehr (MDR), hinter denen die ganze Power von FireEye steht



HIGHLIGHTS

- **Marktführende Bedrohungsdaten:** Sicherheitsanalysten aus verschiedenen FireEye-Teams nutzen kurze Zeit zuvor erfasste und Echtzeit-Daten zu Geräten, Opfern und Angreifern und können daher die Bedrohung in Ihrem System schneller identifizieren.
- **Umfassende Suche:** Bei der proaktiven Suche nach Hinweisen auf bislang unerkannte Angriffe oder andere schädliche Aktivitäten stützen unsere Analysten sich auf die Technologie, die Erfahrungen und die Bedrohungsdaten von FireEye.
- **Untersuchung und Abwehr:** Alle kritischen Bedrohungen werden gründlich analysiert, um ihre Ursache zu finden und effektive Gegenmaßnahmen zu empfehlen.
- **Priorisierung von Warnmeldungen:** Unsere Experten weisen Sie auf die gefährlichsten Bedrohungen hin, damit Sie diese umgehend abwehren können.
- **Managed Defense Consultants:** Die Sicherheitsexperten sind Ihr Ansprechpartner, wenn Sie zusätzliche Unterstützung benötigen, beispielsweise Analysen von Malware-Varianten, umfassende forensische Analysen oder Incident-Response-Einsätze vor Ort.
- **Schutz rund um die Uhr:** SOCs in Irland, Singapur und den USA (Virginia) stehen Ihnen rund um die Uhr zur Verfügung.

Angriffsmethoden werden beständig weiterentwickelt, doch die meisten Unternehmen nutzen immer noch reaktive, technologiebasierte Sicherheitslösungen zum Schutz ihrer wertvollsten Ressourcen. Mit Technologie allein können Sie hartnäckige Hacker nicht aufhalten, aber es ist sehr schwer und meist auch zu teuer, qualifizierte Sicherheitsexperten zu finden, einzustellen, zu schulen und zu binden – insbesondere solche, die sich auf das Aufspüren gut getarnter Angriffe spezialisieren.

Eine bessere Option ist die Zusammenarbeit mit einem vertrauenswürdigen Partner, der Ihr Netzwerk rund um die Uhr überwacht, proaktive Analysen durchführt und dabei die neuesten Bedrohungsdaten und Erfahrungen aus der Praxis nutzt. Genau das bietet FireEye Managed Defense.

Datengestützte Erkennung und Abwehr von Bedrohungen

FireEye Managed Defense ist ein Managed Service zur Bedrohungserkennung und -abwehr (Managed Detection and Response, MDR), der unser branchenweit anerkanntes Cybersicherheits-Know-how, FireEye-Technologien und unsere einzigartigen Kenntnisse zu den Angreifern einsetzt, um die Auswirkungen von Sicherheitsverletzungen zu minimieren.

Managed Defense erhält kontinuierlich die branchenweit umfangreichsten Cyberbedrohungsdaten aus aller Welt. Unsere Experten werten Daten aus unseren Sensoren, der Beobachtung von Cyberkriminellen und ihrer Kampagnen sowie Incident-Response-Einsätzen aus, darunter Untersuchungen der schwerwiegendsten Cyberangriffe weltweit. Diese aktuellen Bedrohungsdaten und Erkenntnisse aus der Praxis informieren die Spurensuche und die Untersuchung der Hackeraktivitäten, sodass unsere Analysten auch die technisch versiertesten Angreifer aufspüren können. Unsere Sicherheitsexperten stellen eine umfassende Einschätzung der Hackeraktivitäten zusammen und geben spezifische Empfehlungen zur Schadensbehebung. Sie stellen die nötigen Kontextinformationen bereit, damit Sie die Bedrohung nachvollziehen, die Risiken einschätzen und angemessene Maßnahmen ergreifen können.

Ablauf

FireEye Managed Defense greift auf unseren hauseigenen Technologiestack zurück, um einen unternehmensweiten Überblick in Echtzeit zu gewinnen – auch über industrielle Steuersysteme und Cloud-Infrastrukturen.

Die Managed-Defense-Analysten von FireEye erkennen und untersuchen Daten aus unseren Sensoren, Incident-Response-Einsätzen und der Beobachtung von Cyberkriminellen auf unbekannte oder bislang unentdeckte Bedrohungen und gehen ihnen aktiv nach.

Wenn sich Indikatoren für Sicherheitsverletzungen nachweisen lassen, informieren wir Sie unverzüglich. Zudem können Sie die neuesten Erkenntnisse in einem sicheren Portal abrufen, während unsere Analysten den Vorfall weiter untersuchen.

Wir stellen Ihnen einen detaillierten Bericht mit einer Zusammenfassung unserer Erkenntnisse, Kontextinformationen und Empfehlungen für die Schadensbehebung bereit, damit Sie effektive Gegenmaßnahmen ergreifen und die Aktivitäten der Hacker unterbinden können.

Methoden und Ziele der Hacker richtig einordnen

Um die immer komplexeren und gezielteren Cyberangriffe vorausszusehen und darauf zu reagieren, sollten Sie auch die Motivationen, Absichten, charakteristischen Merkmale und Methoden der Angreifer kennen. Dabei können Sie auf unsere Praxiserfahrung zurückgreifen.

Die Managed Defense-Analysten nutzen proprietäre Ermittlungsmethoden, um nach Hinweisen auf unbefugte Zugriffe auf Ihre Infrastruktur zu suchen, gegebenenfalls die Vorgehensweise der Angreifer nachzuvollziehen und den Umfang ihrer Fähigkeiten abzuschätzen.

Die erfahrenen Analysten nutzen ihre branchenführenden Einblicke in die Aktionen von über 16.000 Angreifern, darunter mehr als 30 staatlich gesponserte APT-Gruppen in China, Russland und anderen Ländern.

Diese Einblicke in das Verhalten der Angreifer ermöglichen es unseren Experten, die Gefährlichkeit einer Situation rasch einzuschätzen, die Fähigkeiten der Angreifer zu ermitteln, ihren nächsten Schritt vorausszusehen und einen Plan für angemessene Maßnahmen auszuarbeiten.

Abbildung 1: Auf Bedrohungsdaten gestützte Erkennung



Umfassende Suche



Reaktion auf Angriffskampagnen



Erkennung und rasche Abwehr kritischer Bedrohungen

Umfassende Suche

FireEye Managed Defense nutzt für die Spurensuche proaktive Analysen. Unsere Analysten greifen dabei auf ihre Erfahrungen und Kenntnisse zu den Hackern sowie ihren Taktiken, Techniken und Prozessen (TTP) zurück, um schädliche Aktivitäten aufzudecken. Sie suchen systematisch nach neuen TTP, da Hacker immer neue Methoden entwickeln und nutzen, um sich dauerhaft Zugang zu einmal infiltrierten Umgebungen zu sichern und unentdeckt zu bleiben.

Unsere Analysten haben Techniken zur Spurensuche entwickelt und aktualisieren diese fortlaufend mit den Bedrohungsdaten, die wir bei unseren Managed Defense-Kunden, Beratungseinsätzen von FireEye Mandiant und über FireEye ISIGHT Intelligence-Funktionen erfassen.

Reaktion auf Angriffskampagnen

Als Managed Defense-Kunde profitieren Sie von dem Know-how und der Erfahrung, die FireEye beim Schutz von mehr als 6.300 Kunden vor Cyberangriffen gesammelt hat.

Wenn wir Angriffsversuche in Unternehmen erkennen, die Ihrem hinsichtlich Branche, Region oder Technologieprofil ähneln, oder wenn wir Änderungen in den Techniken der Hacker beobachten, beginnen wir umgehend mit der proaktiven Suche nach Hinweisen auf ähnliche Angriffe in Ihrem Netzwerk. Wenn Sie noch nicht angegriffen wurden, wir aber Anzeichen dafür finden, dass Sie zum Ziel einer bestimmten Taktik werden könnten, empfehlen wir Maßnahmen, mit denen Sie diese abwehren können.



Vorteile von Managed Defense

Erfahrung

Die Incident-Response-Teams von Mandiant verbringen über 100.000 Stunden pro Jahr mit der Analyse und Abwehr schwerwiegender Sicherheitsvorfälle. Nutzen Sie ihre Erfahrungen!

Schnellere Erkennung

Bei Managed Defense liegt der Medianwert für die Untersuchung und Abwehr eines Angriffs bei 67 Minuten.

Kosteneffektiv

Der Erwerb und die kontinuierliche Aktualisierung unternehmensinterner Fachkenntnisse kann sehr teuer, zeit- und ressourcenaufwendig sein.

Bedrohungsdaten

Zugriff auf zuverlässige Bedrohungsdaten, die denen staatlicher Sicherheitsbehörden in nichts nachstehen und von mehr als 150 Analysten zusammengetragen werden.

Leistungsstarke Abwehr

Proprietärer Technologie-Stack mit FireEye-Technologien und -Bedrohungsdaten

- 150 Millionen Bedrohungen durch FireEye-Produkte aufgedeckt
- 22 Millionen Managed-Defense-Warmmeldungen analysiert
- 170.000 Untersuchungen durch Analysten
- 91% der Bedrohungen der obersten Prioritätsstufe ohne Rapid Response abgewehrt
- 98% der Rapid-Response-Vorfälle ohne kompletten Incident-Response-Einsatz behoben

Abbildung 2: Schnelle Abwehrmaßnahmen dank umfassender Erfahrung



Ermittlung des Umfangs des Angriffs



Schnelle Reaktion



Empfehlungen zur Schadensbehebung

Erkennung und bevorzugte Abwehr der gefährlichsten Bedrohungen

FireEye Managed Defense-Analysten konzentrieren sich auf die schwerwiegendsten Bedrohungen und ignorieren die zahlreichen irrelevanten Warnmeldungen anderer Produkte. So spart Ihr Team Zeit und kann den Arbeitsaufwand verringern. Ihnen steht das gesamte Know-how unserer Analysten und Incident-Response-Teams zur Verfügung, um schwerwiegende Bedrohungen zu identifizieren. Dazu gehören auch Angriffe, die von herkömmlichen Sicherheitslösungen unter Umständen nicht erkannt wurden.

Ermittlung des Umfangs des Angriffs

Bei der Untersuchung prüfen die Managed Defense-Analysten alle Spuren und Warnmeldungen unter Verwendung sämtlicher FireEye-Bedrohungsdaten. Sie durchsuchen Ihren Netzwerkdatenverkehr oder die Endpunkte, um das Ausmaß der Infiltrierung zu ermitteln, und setzen alle infrage kommenden Vorfälle miteinander in Beziehung, um den zeitlichen Verlauf des Angriffs zu rekonstruieren. Dabei nutzen sie proprietäre Techniken und Bedrohungsdaten, die wir bei über 100.000 Stunden Incident-Response-Einsätzen entwickelt und zusammengetragen haben.

Schnelle Reaktion

Bei schwerwiegenden Angriffen bitten die Managed Defense-Analysten unter Umständen Experten aus unseren Malware-, Bedrohungsdaten- und Incident-Response-Teams um Unterstützung, die detaillierte Analysen eingestufte Vorfälle liefern und Ihr gesamtes Netzwerk durchsuchen, um das volle Ausmaß der Infiltrierung zu ermitteln.

Empfehlungen zur Schadensbehebung

Nach der Untersuchung empfehlen die Managed Defense-Analysten Schritte zur Schadensbehebung, damit Sie möglichst schnell angemessene Maßnahmen ergreifen können.

Wenn die Situation das erfordert, können wir zu einem kompletten Incident-Response-Einsatz zu einem bevorzugten Preis übergehen.

Unterstützung und Bereitstellung von Informationen

Managed Defense-Kunden haben Zugriff auf ein sicheres Portal für die Kommunikation, die Zusammenarbeit und den Zugang zu Berichten und Bedrohungsdaten. Außerdem wird Ihnen ein Managed Defense Consultant (MDC) als Ansprechpartner zugewiesen. MDC sind erfahrene Fachkräfte in den Bereichen Incident-Response-Einsätze und Forensik. Sie können Ihnen strategische Empfehlungen zur Verbesserung des Sicherheitsstatus Ihres Unternehmens geben.

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

© 2019 FireEye, Inc. Alle Rechte vorbehalten.
 FireEye ist eine eingetragene Marke von FireEye, Inc. Alle anderen Marken, Produkte oder Servicenamen sind Marken oder Dienstleistungsmarken der jeweiligen Eigentümer.
 MD-EXT-DS-DE-DE-000115-01

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.

