F-SECURE RAPID DETECTION & RESPONSE

Lösungsübersicht

F-Secure

INHALT

Zuletzt aktualisiert: 26. November 2019

1. ZUSAMMENFASSUNG

Zielgerichtete Cyberangriffe zu analysieren und zeitnah darauf zu reagieren, kann schwierig werden – und extrem teuer, selbst wenn die Angreifer zunächst erfolglos bleiben. Allein die Sanierung nach einem Angriff kann über zwei Monate dauern und bis zu zwei Millionen Dollar kosten.[1] Dateilose Angriffe unterlaufen die meisten Antivirenprogramme, zielgerichtete Angriffe bleiben oft über Monate oder sogar Jahre hinweg unentdeckt.[1] Mit F-Secure Rapid Detection & Response schaffen Sie transparente kontextuelle Sicherheit, automatisieren die Bedrohungserkennung und stoppen Angriffe, bevor es zu Datenverlusten kommt und Ihre sensiblen, vertraulichen oder anderweitig geschützten Daten in die Hände von Unbefugten (z. B. Cyberkriminellen) gelangen.

F-Secure Rapid Detection & Response (RDR) ist eine führende kontextbasierte EDR-Lösung (Endpoint Detection and Response), die Unternehmen sofortigen Einblick in IT-Umgebung und Sicherheitsstatus verschafft. Damit schützen Sie Ihr Geschäft und Ihre sensiblen Daten, weil Sie Angriffe schnell erkennen und unter fachkundiger Anleitung ebenso schnell darauf reagieren können. Durch tief verankerten bidirektionalen Erkenntnisaustausch und ihren hohen Automatisierungsgrad schützt die Lösung vor komplexen Bedrohungen, noch bevor es zu Datenverlusten kommt. F-Secure RDR erkennt Vorfälle mithilfe von schlanken Clients, die auf den überwachten Hosts laufen. Die Clients erfassen Daten über Ereignisse wie Dateizugriffe, gestartete Prozesse, neue Netzwerkverbindungen oder Einträge in Registries und Systemprotokollen. Diese Ereignisse analysiert die Lösung dann genauer. Neben der Echtzeiterkennung identifiziert F-Secure RDR Vorfälle auch aufgrund historischer Daten.

Letztlich ist die beste Technologie aber nur ein Teil der Lösung, denn Technologie ist immer nur so gut wie die Menschen dahinter. Unsere Threat Hunter und Forscher zählen zu den führenden Experten der Branche, und sie wollen nur eines: die absolut besten Lösungen auf dem Security-Markt schaffen. Bei F-Secure kombinieren wir Technologie und unvergleichliches Spitzenwissen, sodass wir eine RDR-Lösung der Weltklasse liefern.

Bei F-Secure Rapid Detection & Response leisten wir exklusive Unterstützung: Zur weiteren Bedrohungsanalyse durch erfahrene Experten kann eine Erkennung direkt an F-Secure eskaliert werden.

Die Lösung ist auch als Managed Service unserer Partner verfügbar. Aus der Kombination von Technologie, Bedrohungsanalyse und Partnerdiensten ergibt sich ein umfassender RDR-Komplettservice. Das entlastet die Ressourcen aufseiten des Anwenderunternehmens von Überwachungsaufgaben und Incident Management. Der Kunde wir erst dann alarmiert, wenn tatsächlich eine echte Bedrohung vorliegt.

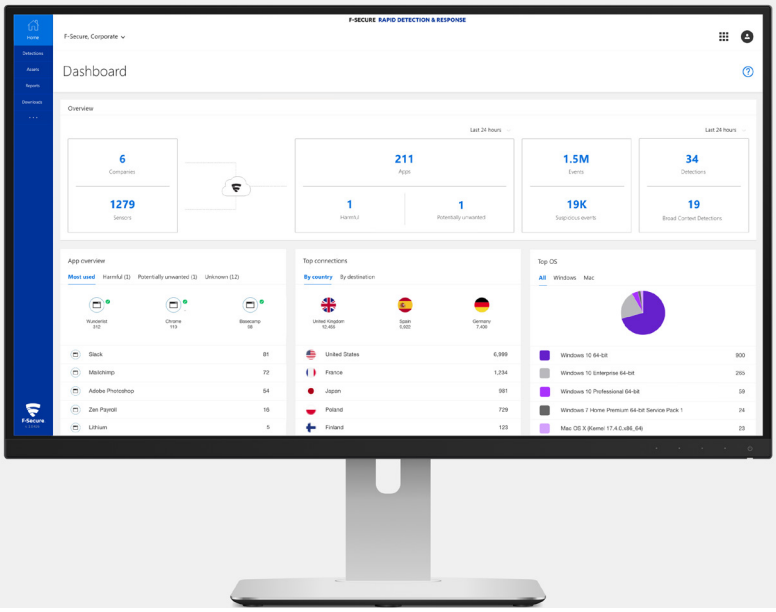
PRÄVENTION MACHT ANGREIFERN DAS LEBEN SCHWER

Wenn sie es wirklich darauf anlegen, schaffen es erfahrene Angreifer vermutlich immer, dass sie in Ihr Netzwerk eindringen. Aber das ist noch lange kein Grund, ihnen auch noch den roten Teppich auszurollen. Indem Sie sich bereits bei der Prävention von unbefugten Zugriffen stark machen, erschweren Sie den Angreifern den Einbruch in Ihr Netzwerk spürbar. Indem Sie Ihre Gegner zwingen, größeren Aufwand zu betreiben, steigen deren Gesamtkosten, was zur Abschreckung beitragen kann.

Wenn Sie F-Secure Rapid Detection & Response zur Erkennung komplexer Angriffe nach einer Kompromittierung verwenden, benötigen Sie nach wie vor eine starke Lösung zum Endgeräteschutz, die Standardbedrohungen wie Ransomware blockiert.

F-Secure Rapid Detection & Response ist so konzipiert, dass die Lösung mit jedem beliebigen Endgeräteschutz kompatibel ist. Zusammen mit unserer Endgerätesicherheitslösung F-Secure Protection Service for Business (PSB) ergibt sie eine cloudbasierte Single-Client-Management-Infrastruktur.

1 Laut der Ponemon 2018 Cost of Data Breach Study dauert es bis zur Erkennung von Sicherheitsvorfällen je nach Branche zwischen 150 und 287 Tage; die Vorfallreaktion kostet durchschnittlich 1,76 Millionen Dollar und dauert 69 Tage.



2. HAUPTVORTEILE

Mit der Lösung F-Secure Rapid Detection & Response sind Sie bestens darauf eingerichtet, komplexe Bedrohungen und zielgerichtete, dateilose Angriffe zu erkennen, bevor es zu Sicherheitsvorfällen kommt. Und Sie können mit hochmoderner Technologie von F-Secure Angriffsversuche jederzeit schnell analysieren und darauf reagieren.

Dies sind die Hauptvorteile der Lösung in Bezug auf Einblick, Erkennung und Reaktion:

IT-Umgebung und Sicherheitsstatus: unmittelbarer kontextueller Einblick

- Einblick in IT-Status und Sicherheit durch die Erfassung von Anwendungen und Endgeräten.
- Frühzeitige Erkennung von Missbrauchsmustern – und nicht nur von Malware – durch die Sammlung und Korrelation von Verhaltensweisen.
- Schnellere Reaktion auf identifizierte zielgerichtete Angriffe – dank Alarmen mit Kontext-Einordnung und Einbezug der Host-Kritikalität.

Schnelle Erkennung von Sicherheitsvorfällen: Schutz des Unternehmens und seiner Daten

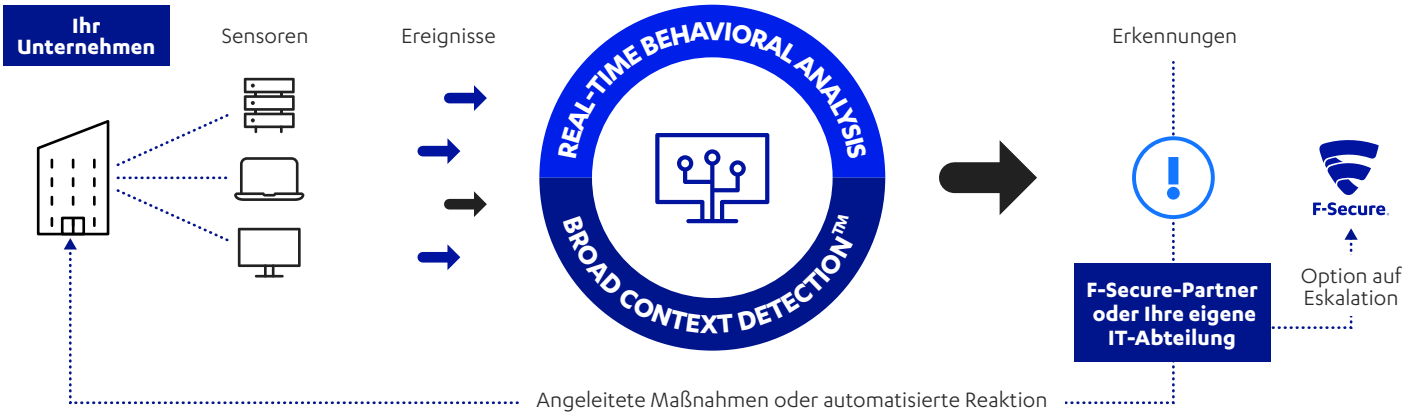
- Schnelle Erkennung und Abwehr zielgerichteter Angriffe – weniger Ausfallzeiten und Image-Schaden.
- Setup fortschrittlicher Bedrohungserkennung und -reaktion binnen weniger Tage.
- Erfüllung regulatorischer Standards wie PCI, HIPAA und EU-DSGVO, die die Meldung von Datenschutzverstößen binnen 72 Stunden vorschreiben.

Automatisierung und Anleitung durch Experten: schnelle Reaktion auf Angriffe

- Konzentriertere Security Teams dank Automatisierung und Erkenntnissen zur Bedrohungslage – das erleichtert die schnelle Reaktion auf echte komplexe Bedrohungen und zielgerichtete Angriffe.
- Anleitungen zum Vorgehen bei Warnmeldungen, mit der Option, Reaktionsmaßnahmen rund um die Uhr zu automatisieren (diese Automatisierungsfunktionen sind als Update vorgesehen).
- Ausgleich von fehlenden Skills oder Ressourcen im eigenen Team durch die Übertragung der erweiterten Bedrohungsüberwachung an einen von F-Secure zertifizierten Managed Service Provider, der direkt von F-Secure-Experten unterstützt wird.

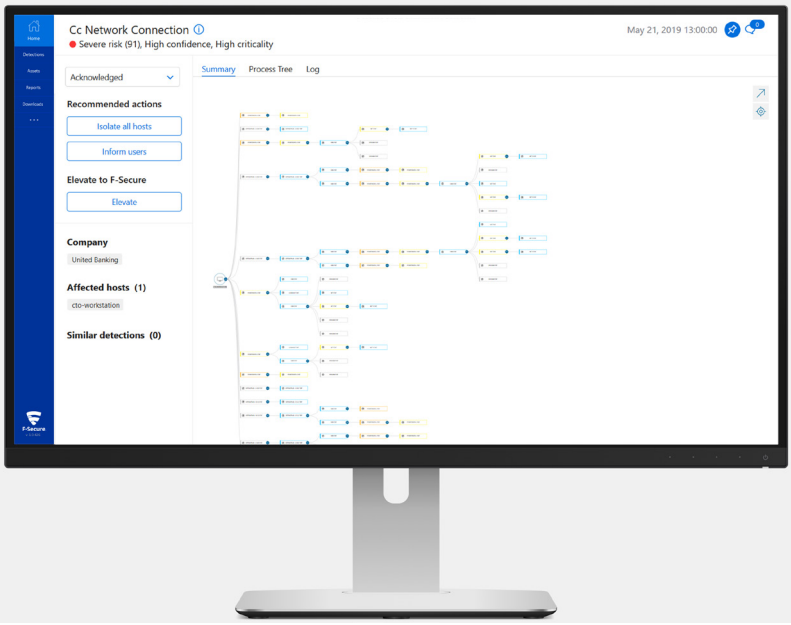
3. LÖSUNGSÜBERSICHT

F-Secure Rapid Detection & Response (RDR) besteht aus Clients, die einfach auf den einzelnen Hosts gestartet werden, einem cloudbasierten Management-Portal sowie wahlweise den Managed Services unserer zertifizierten Partner. Die Lösung dient der Erkennung komplexer Bedrohungen und zielgerichteter Angriffe sowie der Anomalieerkennung im weiteren Ereigniszusammenhang zur Klärung von Gesamtrisiko und Reaktion. Die Bereitstellung vor Ort umfasst die Endgeräteüberwachung sowie einen Response Client, der auf den Endgeräten des Unternehmens installiert wird.



Das obenstehende Schema zeigt die Funktionsweise von F-Secure Rapid Detection & Response:

1. **Ressourcenschonende Clients** überwachen die einzelnen Endgeräte auf Angreiferaktivitäten und streamen Verhaltensereignisse in Echtzeit an unsere Cloud.
2. **Echtzeitanalysen der Verhaltensdaten** markieren und überwachen sowohl die Prozesse als auch weitere Aktivitäten, die Auslöser von Ereignissen waren.
3. **Broad Context Detection™** grenzt die Daten weiter ein, bringt verwandte Ereignisse miteinander in Zusammenhang und identifiziert dadurch schnell echte Angriffe. Diese werden nach Risikoniveau, Kritikalität des Hosts und der vorherrschenden Bedrohungslandschaft priorisiert.
4. **Automation und angeleitete Reaktionen** sind die Hilfestellungen, mit denen IT- und Sicherheitsteams die Bedrohung nach einer bestätigten Erkennung handlungssicher eindämmen und beheben können.



3.1 Management-Portal

Mit F-Secure Rapid Detection & Response fällt das Setup ebenso leicht wie das Endgeräte-Monitoring auf fortschrittliche Bedrohungen und der Umgang damit: Alles geschieht über eine einzige, intuitive, webbasierte Konsole. Sie verschafft Ihnen sofortigen kontextbezogenen Überblick in der IT-Umgebung und zum Sicherheitsstatus Ihres gesamten Netzwerks – egal, ob Ihre Mitarbeiter im Büro oder unterwegs tätig sind. Das Portal ist dazu gedacht, das Security Management in anspruchsvollen Umgebungen mit mehreren Standorten zu vereinfachen und zu beschleunigen.

Im Folgenden finden Sie einige Beispiele dafür, wie die Lösung den Zeit- und Ressourcenaufwand erheblich reduziert:

- F-Secure Rapid Detection & Response ist so konzipiert, dass die Lösung mit sämtlichen Formen von Endgeräteschutz kompatibel ist. Mit Endgeräte Security von F-Secure funktioniert das mit demselben Client und konsolidiertem Management.
- Zusammen mit F-Secure Protection Service for Business (PSB) kann die Lösung sowohl Malware als auch komplexe Bedrohungen erkennen und handhaben.
- Erkannte Bedrohungen werden interaktiv visualisiert, sodass der Kontext zielgerichteter Angriffe auf einer Zeitleiste mit allen betroffenen Hosts, Ereignissen und empfohlenen Maßnahmen sichtbar wird.
- Dadurch, dass das Management komplexer Bedrohungen in einem einzigen Sicherheitsportal konsolidiert ist, wird die Verwaltung schlanker und spart deutlich an Zeit.
- Weil die Management-Konsole ein von F-Secure verwalteter Cloud-Service ist, gibt es keine Server, Hardware oder Software zu installieren oder zu warten – alles, was Sie brauchen, ist ein Browser und eine Internet-Verbindung.

Das Management-Portal unterstützt die aktuellen Versionen von Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome und Safari.

Das Management-Portal ist (Stand Februar 2019) für folgende Sprachen verfügbar: Bulgarisch, Chinesisch, Chinesisch (Hongkong), Chinesisch (Taiwan), Dänisch, Deutsch, Englisch, Estnisch, Finnisch, Französisch, Französisch (Kanada), Griechisch, Italienisch, Japanisch, Koreanisch, Litauisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Portugiesisch (Brasilien), Rumänisch, Russisch, Schwedisch, Slowenisch, Spanisch (Mexiko), Tschechisch, Türkisch, Ungarisch und Vietnamesisch.

Die Partner-Managed-Version des Management-Portals umfasst spezielle Funktionen für Diensteanbieter, z. B. Endkunden-Reporting, ein Dashboard mit einer praktischen Übersicht über alle verwalteten Unternehmen sowie Zugriff auf deren Mandanten-Dashboards.

3.2 Endgeräte-Clients

Die Clients auf den Endgeräten sind ressourcenschonende, diskrete Monitoring Tools zur Erkennung von Anomalien, einschließlich neuer und zuvor nicht identifizierter Ereignisse bzw. Ereignisfolgen, die höchstwahrscheinlich auf böswillige Aktivitäten zurückzuführen sind. Sie laufen auf allen relevanten Windows- und MacOS-Computern des Unternehmens, und erfassen das Ereignisverhalten der Endgeräte. Die Clients sind so konzipiert, dass sie mit sämtlichen Endgeräteschutzlösungen kompatibel sind und zusammen mit den Endgeräte-Sicherheitslösungen von F-Secure eine cloudbasierte Single-Client-Management-Infrastruktur ergeben.

Die folgende Tabelle zeigt die unterstützten Betriebssysteme und die jeweiligen Funktionen.

	WINDOWS WORKSTATIONS	WINDOWS SERVER	MAC OS
BETRIEBSSYSTEM	7 / 8 / 10	2019 / 2016 / 2012 / 2011 / 2008 R2	10.12 oder neuer
SINGLE-CLIENT MIT F-SECURE-ENDGERÄTESCHUTZ	Ja	Ja	Ja
CLIENT MIT ENDGERÄTE-SCHUTZ VON DRITTANBIETERN	Ja	Ja	Ja
VERHALTENSEREIGNISSE	Ja	Ja	Ja
ANWENDUNGSÜBERSICHT	Ja	Ja	Nein*
REMOTE-HOST-ISOLATION**	Ja	Ja	Ja

*** In Arbeit; die Funktion ist derzeit noch nicht verfügbar. ** In Verbindung mit F-Secure Business Suite, manueller Eingriff erforderlich.**

Außer mit F-Secure Protection Service for Business (Computer/Server Protection) und F-Secure Business Suite (Client/Server Security) ist die Lösung auf Kompatibilität mit den folgenden Endgeräteschutzprodukten getestet (Stand August 2018): Bitdefender Endpoint Security Tools, ESET Endpoint Security, Kaspersky Endpoint Security, McAfee Endpoint Security, Microsoft Windows Defender, Panda Adaptive Defense 360, Trend Micro Business Security, Sophos Endpoint Security and Control, Symantec Endpoint Protection and Webroot SecureAnywhere.

Weitere Informationen zu Systemanforderungen und Client-Implementierung finden Sie im Benutzerhandbuch unter https://help.f-secure.com/product.html#business/edr/latest/de/deployment-latest-de.

3.3 Anwendungsübersicht

Ein gründlicher Einblick in IT-Umgebung und Cloud-Dienste reduziert die Gefahr von komplexen Bedrohungen und Datenverlusten. Mit der umfassenden Sicht unserer Lösung auf alle Anwendungen können Sie sämtliche aktiven Applikationen auflisten, die auf Endgeräten im gesamten Netzwerk des Unternehmens ausgeführt werden, sodass Sie unerwünschte, unbekannte und schädliche Apps leicht identifizieren können.

Dank dieser Anwendungstransparenz können Sie potenziell unerwünschte Anwendungen, sogenannte PUAs (Potentially Unwanted Applications) und definitiv unerwünschte Anwendungen (UAs/Unwanted Applications) identifizieren. Mit PUAs sind Verhaltensweisen oder Eigenschaften gemeint, die Sie möglicherweise als unerwünscht oder ungewollt einstufen. UAs sind Verhaltensweisen oder Eigenschaften mit schwerer wiegenden Auswirkungen auf Ihre Dienste oder Daten.

Anwendungen, die als PUA identifiziert werden, können

- den Datenschutz oder die Produktivität beeinträchtigen – zum Beispiel persönliche Informationen preisgeben oder unbefugte Aktionen ausführen;
- die Ressourcen des Geräts übermäßig beanspruchen – z. B. zu viel (Arbeits-)Speicher nutzen;
- die Sicherheit des Geräts oder der darauf gespeicherten Informationen kompromittieren – und Sie z. B. unerwarteten Inhalten oder Anwendungen aussetzen.

Die Folgen für Ihre Geräte und Daten können geringfügig bis schwerwiegend sein. Insgesamt sind PUAs aber nicht so schädlich, dass eine Einstufung als Malware gerechtfertigt wäre.

3.4 Verhaltensanalyse

Die Verhaltensanalyse ist die Funktion, die komplexe Bedrohungen inmitten großer Mengen von Verhaltensereignisdaten identifizieren kann. Sie erkennt verdächtige Ereignisse oder Ereignisabfolgen, die noch nie zuvor beobachtet wurden und vermutlich bösartig sind.

F-Secure kann durch Echtzeit-Verhaltens-, Reputations- und Big-Data-Analysen mit maschinellem Lernen aus mehreren verdächtigen Ereignissen (z. B. Aktivitäten) ein zusammenhängendes Lagebild erstellen. Die Verhaltensanalyse nutzt künstliche Intelligenz, um anhand von kleinen Einzelereignissen versteckte Schadaktivitäten aufzuspüren, die Taktiken, Techniken und Methoden (TTPs/Tactics, Techniques and Procedures) eines Angreifers vermuten lassen. Die Verhaltensanalyse kommt auch bei der automatischen Identifizierung von Host-Profilen zum Zuge, was sich auf die Risikobewertung von Erkennungen in Bezug auf das überwachte Unternehmen, den Host und die gesamte IT-Umgebung auswirkt.

Zu dieser KI gehören auch Funktionen maschinellen Lernens; dadurch verbessert sich die Erkennung stetig und False Positives werden reduziert. Unsere Verhaltensanalyse ist ein Paradebeispiel dafür, wie F-Secure Data Science und Cybersicherheit-Fachkompetenz kombiniert – ein Ansatz, den wir als „Mensch und Maschine" bezeichnen.

3.5 Broad Context Detection™

Broad Context Detection™ ist eine Eigenentwicklung von F-Secure. Die Lösung bewirkt, dass die Anzahl der Erkennungen auf eine kleine Menge bedeutsamer Vorfälle eingegrenzt wird, die darauf hinweisen könnten, dass Systeme oder Daten kompromittiert wurden.

Broad Context Detection™ schlägt bei Hinweisen auf mögliche Sicherheitsverletzungen Alarm und informiert Administratoren über Taktiken, Techniken und Methoden, die für zielgerichtete Angriffen typisch sind. Dies umfasst z. B. die folgenden potenziell verdächtigen Aktivitäten:

- ungewöhnliche Aktivität von Standardprogrammen;
- Anfragen an laufende Prozesse von nicht standardmäßigen Ausführungsdateien;
- die Ausführung unerwarteter Skripte;
- die unerwartete Ausführung von Systemtools von Standardprozessen aus.

Broad Context Detection™ informiert ausschließlich dann, wenn eine sicherheitsrelevante Erkennung vorliegt. Jedem Vorfall wird ein Risikowert zugewiesen, die u. a. auf Risikoniveau, Informationen zur Kritikalität des betroffenen Hosts und der jeweiligen Bedrohungslandschaft basiert. Ein einzelnes Ereignis muss kein Anzeichen für einen Angriff sein. Aber mehrere Erkennungen innerhalb kurzer Zeit können den Schweregrad dieser Beobachtung hochstufen und eine Broad-Context-Detection™-Warnung auslösen, dass unter Umständen gerade ein Angriff stattfindet.

Im Ergebnis erhalten IT-Teams eine relativ knappe Liste bestätigter Erkennungen, denen jeweils die betreffende Prioritätseinstufung und empfohlene Reaktionsmaßnahmen beigefügt sind. So wissen die Sicherheitsteams genau, was sie zuerst angehen müssen, und sie wissen auch, wie sie dabei am besten vorgehen – und sie können es entsprechend schnell und entschlossen tun.

Weitere Informationen zu Broad Context Detection™ finden Sie in unserem Whitepaper „Mit Broad Context Detection™ komplexe Bedrohungen automatisch erkennen" auf www.f-secure.com/RDR.

AUSGEWÄHLTE AKTIVITÄTEN, BEI DENEN F-SECURE RAPID DETECTION & RESPONSE ANSCHLÄGT

Die folgende Liste ist nicht auf bekannte Angriffe beschränkt, da die Erkennungsdaten kontinuierlich analysiert werden, sodass die Broad Context Detection™ und unsere Threat Hunter laufend neue Arten von Angriffen identifizieren.

Zielgerichteter Angriff auf einen Host.

Seitwärtsbewegungen mit Host-Wechsel.

Spoofing von Informationen im Rahmen eines Angriffs.

Persistenz, z. B. mehrfache Prozessaufrufe auf demselben Host.

Rechteausweitung, z. B. das Erzwingen von Administratorrechten mit Brute-Force-Methoden.

Zugriff auf Berechtigungen, die bei anvisierten Maschinen oder Netzwerken Zugriff und Kontrolle ermöglichen sollen.

Exfiltration, also die Ausschleusung von Informationen aus der Zielmaschine bzw. dem Zielnetzwerk.

Ungewöhnliche Prozessausführungen, zum Beispiel mit verdächtigen Parametern.

Ungewöhnlicher Dateizugriff, z. B. unterschiedliche Dokumenttypen oder Nicht-Root-Zugriff auf Systemdateien.

Client-Manipulationsversuche, z. B. veränderte Einstellungen oder Deaktivierungsversuche.

Injections von Code in Prozesse, z. B. im Kernelmodus oder bei anderen Anwendungen.

Command-and-Control-Verbindungen zu einem Remote-Server.

PowerShell-Skripte von der Position des Angreifers, die als ungewöhnlicher Standort zum Laden eines Skripts erkannt wird.

Durch PowerShell modifizierte PowerShell-Skripte, was typischerweise ein Anzeichen von Persistenz ist.

Ungewöhnliche DLL-Verwendung mit PowerShell durch einen Prozess, der das Modul geladen hat.

Remote-Verbindungen und -Ausführungen, die möglicherweise auf eine Seitwärtsbewegung hindeuten.

3.6 Vorfallmanagement

F-Secure Rapid Detection & Response umfasst ein integriertes Vorfallmanagement, das Broad-Context-Erkennungen anzeigt und handhabbar macht.Neue Erkennungen lösen eine E-Mail-Benachrichtigung aus, die einen Link zum Management-Portal enthält, wo die Sicherheitsbeauftragten sich weitere Details anzeigen lassen und direkt Maßnahmen ergreifen können.

Im benutzerfreundlichen Dashboard sind die Broad-Context-Erkennungen aufgelistet, sodass sich die Einträge leicht auf Grundlage ihrer Risikobewertung priorisieren lassen. Die Risikobewertung wird auf Basis der Kritikalitäts- und Konfidenzniveaus automatisch berechnet. Auch nicht kritische Broad Context Detections mit niedrigen Risikobewertungen werden angezeigt – schließlich können sich Angriffe langsam entwickeln und sich mit der Zeit zu ernsthafteren Vorfällen mit hoher Risikoeinstufung auswachsen.

Die Standardmaßnahmen im Vorfallmanagement bestehen darin, Broad Context Detection-Erkennungen zu bestätigen oder sie als „in Bearbeitung", „in Überwachung", „Als bestätigt abgeschlossen", „Als falsch positiv abgeschlossen" oder „Als unbestätigt abgeschlossen" zu kennzeichnen. Durch die Markierung einer Broad-Context-Erkennung als falsch positiv werden zukünftige Ereignisse, die mit dem Eintrag in Erkennungstyp und Prozessparametern übereinstimmen, automatisch als „Auto falsch positiv" geschlossen.

3.7 Angeleitete Reaktion

Nach einer bestätigten Erkennung führt die integrierte Hilfestellung der Lösung durch alle Schritte, mit denen Sie die Bedrohung eindämmen und beheben können. Zu den empfohlenen Maßnahmen gehören Schritte wie die Inkenntnissetzung von Benutzern oder die Isolierung von Hosts.

Die Cybersicherheitsexperten von F-Secure haben auf Basis eigener Erfahrungen eine Reihe gängiger Bedrohungen analysiert und die Lösung entsprechend „trainiert". So kann F-Secure Rapid Detection & Response leicht verständliche Anleitungen und Hilfestellungen für die Reaktion auf ein breites Spektrum komplexer Bedrohungen geben. Diese angeleitete Reaktion macht es auch für weniger erfahrene Mitglieder Ihres IT- und Sicherheitsteams einfach, die richtigen Maßnahmen zur Eindämmung und Behebung einer Bedrohung zu ergreifen.

3.8 Eskalation an F-Secure (Elevate to F-Secure)

F-Secure bietet außerdem einen optionalen Service, für den Fall, dass eine Erkennung weitere Bedrohungsanalysen und Anleitung durch Cybersicherheitsexperten erforderlich macht. Dieser Premium-Service muss für ein Kontingent von Fällen im Voraus bestellt werden.

Mit der Eskalation an F-Secure durch die Lösung erhalten unsere Threat Hunter die Erlaubnis, auf die Gesamtheit der Metadaten zuzugreifen, die von den installierten Clients im Zusammenhang mit der jeweiligen Erkennung gesammelt wurden.

Die diensthabenden Bedrohungsanalysten von F-Secure bearbeiten die Anfrage innerhalb der zweistündigen SLA-Bearbeitungszeitvorgabe. Sie beginnen mit der Identifizierung des potenziellen Vorfalls, dazu sammeln sie zusätzliche Beweise und leisten über unsere Lösung weitere Expertenanleitung, um die Bedrohung zu validieren und bei Bedarf eine konkrete Bedrohungsuntersuchung durchzuführen.

- **Die Bedrohungsvalidierung** liefert zusätzliche Informationen zu einer Broad-Context-Erkennung der vergangenen sieben Tage. Dies umfasst eine Zusammenfassung und Beschreibung der Erkennung durch Experten, außerdem allen anderen relevanten Daten, mithilfe derer Sie bestimmen können, ob Gegenmaßnahmen erforderlich sind.
- **Die Bedrohungsuntersuchung** ist die sehr detaillierte Untersuchung einer Broad-Context-Erkennung, bei der alle aktuellen und historischen Daten berücksichtigt werden. Diese Option umfasst auch eine umsetzbare Anleitung zur Vorfallreaktion von unseren Cybersicherheitsexperten, zusammen mit einem umfassenden Bericht über die Art des erkannten Angriffs.

Der Service „Elevate to F-Secure" konzentriert sich auf die Analyse technischen Beweismaterials im Zusammenhang mit den infrage kommenden potenziellen Vorfällen, z. B. Methoden und Technologien, Netzwerkrouten, Herkunft des Traffics und zeitlicher Verlauf. Anleitungen stellt unser Expertenteam allerdings ausschließlich über F-Secure Rapid Detection & Response zur Verfügung – weitere professionelle Dienstleistungen zur Unterstützung bei der Vorfallreaktion müssen separat vereinbart werden. Kunden, die vermuten, dass ein Verbrechen vorliegt, sollten sich mit den zuständigen Behörden in Verbindung zu setzen und dazu den Bericht der Bedrohungsuntersuchung vorlegen.

3.9 Automatisierte Reaktion

Um die Auswirkungen zielgerichteter Cyberangriffe minimal zu halten, stehen automatisierte Reaktionsmaßnahmen zur Verfügung, die Vorfälle außerhalb der Geschäftszeiten automatisch isolieren, wenn das Risikoniveau hoch genug ist. Dieser Mechanismus ist speziell für Teams entwickelt, die nur während der Geschäftszeiten Erkennungen überwachen und auf Vorfälle reagieren können. An ihrer Stelle ergreift dann nachts oder am Wochenende die Automatik erste Maßnahmen.

4. DATENSICHERHEIT

4.1 Datenschutz und Vertraulichkeit

Die auf den Endgeräten erfassten Daten zu Verhaltensereignissen werden innerhalb der Europäischen Union (in Irland) fortlaufend gespeichert, so lange der Kundenauftrag besteht, und binnen zweier Monate nach Beendigung des Auftrags gelöscht.

F-Secure Rapid Detection & Response ist nicht für die Überwachung von Aktivitäten gedacht, die nicht sicherheitsrelevant sind, etwa zur Erstellung von Profilen aus Aktivitäten, Interessen oder Interaktionen von Mitarbeitern. Der Schwerpunkt der Datenerhebung liegt nicht auf einzelnen Mitarbeitern, Dokumenten oder E-Mail-Inhalten. In der ausführlichen Datenschutzerklärung finden Sie genaue Auskünfte hierzu.

Da F-Secure seinen Sitz in Finnland hat, halten wir uns an die strengen Datenschutz- und Sicherheitsvorschriften sowohl Finnlands als auch der Europäischen Union. Wir handeln im Einklang mit den EU-Datenschutzbestimmungen und verstehen die Datenschutzbedürfnisse unserer Kunden. F-Secure arbeitet gemäß der finnischen Umsetzung der EU-Datenschutzrichtlinie, und F-Secure Rapid Detection & Response ist in Übereinstimmung mit der allgemeinen Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) entwickelt. Weitere Informationen zur DSGVO-Konformität von F-Secure finden Sie unter https://www.f-secure.com/GDPR.

4.2 Maßnahmen zur Datensicherheit

Der Schutz unserer Rechenzentren hat für uns als Sicherheitsunternehmen oberste Priorität. Wir setzen zu diesem Zweck Dutzende von Sicherheitsmaßnahmen ein. Dazu gehören zum Beispiel die folgenden:

- Security by Design: Unsere Systeme sind von Anfang an auf Sicherheit ausgelegt. Wir verankern Sicherheit und den Schutz der Privatsphäre bereits in der Entwicklung unserer Technologien und Systeme – von der Konzepterstellung bis zum laufenden Betrieb.
- Strikte Zugriffskontrolle: Nur eine begrenzte Anzahl geprüfter Mitarbeiter von F-Secure hat Zugang zu den Kundendaten. Ihre Zugriffsrechte und -ebenen entsprechen der Funktion und der Rolle, die sie im Unternehmen innehaben, wobei das Prinzip der geringsten Privilegien angewandt und mit den definierten Verantwortlichkeiten abgestimmt wird.
- Starke operative Sicherheit: Operative Sicherheit ist unserer täglich Brot, einschließlich Schwachstellenmanagement, Malware-Abwehr und zuverlässiger Verfahren zum Umgang mit Sicherheitsvorfällen, die sich auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen bzw. Daten auswirken könnten.

4.3 Rechenzentren

Unsere Lösung Rapid Detection & Response nutzt die Rechenzentren von AWS (Amazon Web Services), um höchstmögliche Verfügbarkeit und Ausfallsicherheit sowie bessere Reaktionszeiten und eine bedarfsgerechte Skalierung zu gewährleisten. AWS erklärt, dass jedes seiner Rechenzentren den Richtlinien von Tier 3+ entspricht. Weitere Informationen hierzu finden Sie unter https://aws.amazon.com/compliance/.

Die Verhaltensereignisdaten der Endgeräte werden auf AWS in Europa (Irland) gespeichert. Die Speicherung für ein Jahr ist im Abonnement von F-Secure Rapid Detection & Response enthalten. Es fallen hierfür keine zusätzlichen Kosten an, unabhängig von der Menge der erfassten Daten.

ÜBER F-SECURE

Niemand hat besseren Einblick in echte Cyberangriffe als F-Secure. Wir schließen die Lücke zwischen Erkennung und Reaktion. Wir nutzen dazu unübertroffene Bedrohungsinformationen von Hunderten der besten technischen Berater unserer Branche, von Millionen von Geräten, die unsere preisgekrönte Software nutzen, sowie fortlaufende Innovationen im Bereich maschinelles Lernen. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf unser Engagement bei der Bekämpfung der gefährlichsten Bedrohungen der Welt.

Zusammen mit unserem Netzwerk an Top-Channel-Partnern und über 200 Serviceanbietern ist es unsere Mission, all unseren Kunden maßgeschneiderte unternehmensfähige Cybersicherheit zur Verfügung zu stellen. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure