RAPID DETECTION & RESPONSE

Lösungsüberblick

F-Secure

CONTENTS

1. EXECUTIVE SUMMARY

Mitunter ist es schwierig, gezielte Angriffe auf die Cybersicherheit zu analysieren und darauf zu reagieren. Noch bevor sich daraus tatsächliche Datensicherheitsverstöße ergeben, können sie für Unternehmen zu einem extrem kostspieligen Problem werden. Allein die Wiederherstellungsphase nach einem Angriff kann über einen Monat dauern und Kosten von fast einer Million US-Dollar verursachen(1. Dateilose Angriffe werden von herkömmlichem Virenschutz oft nicht erkannt, und gezielte Angriffe bleiben häufig über Monate oder gar Jahre hinweg unentdeckt(2. Die Lösung F-Secure Rapid Detection & Response liefert Ihnen einen kontextbezogenen Überblick über Ihre Sicherheit. Sie automatisiert zudem die Bedrohungserkennung und stoppt Angriffe, bevor Datensicherheitsverstöße auftreten.

F-Secure Rapid Detection & Response (RDR) ist eine führende EDR-Lösung (Endpoint Detection & Response) auf Kontextebene, mit der sich Unternehmen umgehend einen transparenten Überblick über ihre IT-Umgebung und ihren Sicherheitsstatus verschaffen. Sie bietet die Möglichkeit, Angriffe schnell zu erkennen und mithilfe fachkundiger Handlungsempfehlungen darauf zu reagieren, sodass das Business und sensible Daten geschützt sind. Die Lösung von F-Secure schützt mit ihrer tiefgehenden bidirektionalen Analyse und ihrem hohen Automatisierungsgrad vor komplexen Bedrohungen, noch bevor Sicherheitsverstöße auftreten. Sie erkennt Vorfälle mittels schlanker Clients, die auf den überwachten Hosts im gesamten Unternehmensnetzwerk installiert werden. Diese Clients erfassen Daten zu Verhaltensereignissen, darunter Dateizugriffe, gestartete Prozesse, aufgebaute Netzwerkverbindungen oder Einträge in die Registry oder Systemprotokolle. Diese Ereignisse werden dann von der Lösung weiter analysiert. Die Lösung erkennt Vorfälle nicht nur in Echtzeit, sondern auch anhand von vorhandenen aufgezeichneten Daten.

VERWALTETER EDR-SERVICE

Die Lösung steht als von einem unserer Partner verwalteter EDR-Service zur Verfügung, der Technologie, Bedrohungsinformationen und Partnerservices verbindet. So erhalten Kunden einen Komplettservice für die Erkennung von Sicherheitsverstößen und die Reaktion darauf.

Durch Managed EDR Services entlasten Unternehmen ihre eigenen Ressourcen von hochentwickelter Bedrohungsüberwachung und Vorfallsmanagement. Sie senden dem Unternehmen nur dann Warnmeldungen, wenn echte Bedrohungen erkannt wurden.

Der Service wird von F-Secure unterstützt. Das bedeutet, dass ein erkannter Vorfall zur weiteren Bedrohungsanalyse durch erfahrene Cybersicherheitsexperten an F-Secure weitergeleitet werden kann.

Im Endeffekt ist der Einsatz modernster Technologie nur ein Teil der Lösung, denn Technologie ist nur so gut wie die Menschen, die dahinterstehen. Unsere Threat Hunter und Forscher zählen zu den führenden Experten der Branche und arbeiten mit großem Einsatz daran, die besten Lösungen auf dem Markt für Cybersicherheit bereitzustellen. Bei F-Secure vereinen wir diese Technologie und diesen unübertroffenen Sachverstand miteinander, um eine erstklassige EDR-Lösung bereitzustellen.

Die Lösung F-Secure Rapid Detection & Response wurde entwickelt, um mit jeder beliebigen Endgeräteschutz-Lösung zusammenzuarbeiten und funktioniert mit der Endgeräteschutz-Lösung F-Secure Protection Service für Business (PSB) als Einzel-Client- und Cloud-basierte Management-Infrastruktur. Da es sich bei F-Secure Rapid Detection & Response um eine Lösung zur Erkennung von komplexen Angriffen für den Einsatz nach einem Vorfall handelt, ist weiterhin eine leistungsstarke Lösung für den Endgeräteschutz erforderlich, die Commodity-Bedrohungen wie Ransomware abwehrt.

1. Im Cybersecurity Trend Report 2016 des Ponemon Institute geben 252 Befragte an, dass es bei ihnen im Durchschnitt 45 Tage dauert, um einen Cyberangriff zu beheben. Dies führt allein während der Wiederherstellungsphase nach einem Angriff zu Ausgaben von etwa 973.000 US-Dollar.
2. Gartner spricht 2017 von 99 Tagen in Amerika; in seinem Cybersecurity Trend Report 2016 meldete das Ponemon Institute 98 Tage für Finanzdienstleister und 197 Tage für Einzelhändler.

2. HAUPTVORTEILE

Mit F-Secure Rapid Detection & Response sind Sie für die Erkennung komplexer Bedrohungen und gezielter Angriffe ausgerüstet, bevor Datensicherheitsverstöße auftreten. Dank der Spitzentechnologie von F-Secure sind Sie immer in der Lage, Vorfälle schnell zu analysieren und auf sie zu reagieren.

Einige der Hauptvorteile der Lösung für Transparenz, Vorfallserkennung und -reaktionen sind im Folgenden aufgeführt:

TRANSPARENZ	ERKENNUNG	REAKTION
Direkter kontextbezogener Überblick über die IT-Umgebung und den Sicherheitsstatus	Schutz Ihres Unternehmens und seiner sensiblen Daten durch schnelles Erkennen von Datensicherheitsverstößen	Prompte Reaktion auf Angriffe mithilfe von Automatisierung und Handlungsempfehlungen

1. **Direkter kontextbezogener Überblick über Ihre IT-Umgebung und Ihren Sicherheitsstatus**
   - Verbessern Sie den Überblick über den Status und die Sicherheit der IT-Umgebung durch Anwendungs- und Endgeräteinventarisierung
   - Unterscheiden Sie problemlos zwischen missbräuchlicher und bestimmungsgemäßer Nutzung, indem Sie über Malware hinaus verhaltensbezogene Ereignisse erfassen und korrelieren
   - Reagieren Sie dank Warnmeldungen mit umfangreichem Kontext und Host-Kritikalität schneller auf die erkannten gezielten Angriffe

2. **Schutz Ihres Unternehmens und seiner sensiblen Daten durch schnelles Erkennen von Sicherheitsvorfällen**
   - Erkennen und stoppen Sie gezielte Angriffe schnell, um negative Auswirkungen auf Geschäftsabläufe und den Ruf des Unternehmens zu verhindern
   - Richten Sie in nur wenigen Tagen Funktionen für die hochentwickelte Bedrohungserkennung und -reaktion ein und seien Sie vorbereitet, bevor Sicherheitsverstöße auftreten
   - Halten Sie Vorschriften wie PCI, HIPAA und die Datenschutz-Grundverordnung ein, die eine Meldung von Datensicherheitsverstößen innerhalb von 72 Stunden verlangt

3. **Prompte Reaktion auf Angriffe mithilfe von Automatisierung und Handlungsempfehlungen**
   - Verbessern Sie die Fokussierung Ihres Teams mit integrierter Automatisierung und Informationen, die eine schnelle Reaktion auf echte komplexe Bedrohungen und gezielte Angriffe ermöglichen
   - Nutzen Sie die Handlungsempfehlungen aus den Warnmeldungen, die Sie erhalten, mit der Möglichkeit, rund um die Uhr automatische Reaktionsmaßnahmen auszuführen (Automatisierungsfunktionen werden als Update bereitgestellt)
   - Schließen Sie Kompetenz- und Personallücken in Ihren Teams durch das Outsourcing der Überwachung komplexer Bedrohungen an einen von F-Secure zertifizierten Managed-Service-Anbieter, der Unterstützung von F-Secure-Experten erhält

3. LÖSUNGSÜBERBLICK

F-Secure Rapid Detection & Response (RDR) besteht aus einer Kombination aus einfach zu installierenden Clients auf Hosts, einem Cloud-basierten Management-Portal und optionalen Managed Services von zertifizierten Partnern. Die Lösung bietet Funktionen für die Erkennung komplexer Bedrohungen und gezielter Angriffe sowie Broad Context Detections zur Klärung des Gesamtrisikos und zur Reaktion auf Bedrohungen. Der Vor-Ort-Teil der Bereitstellung umfasst einen Endpunkt-Überwachungs- und Reaktions-Client, der auf den Endpunkten eines Unternehmens installiert wird.

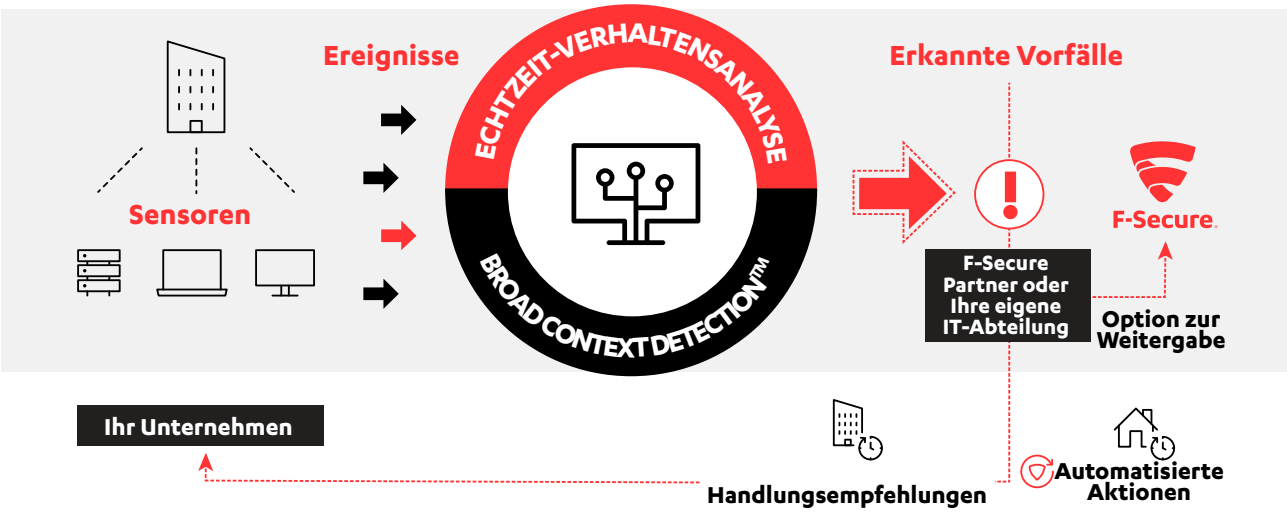


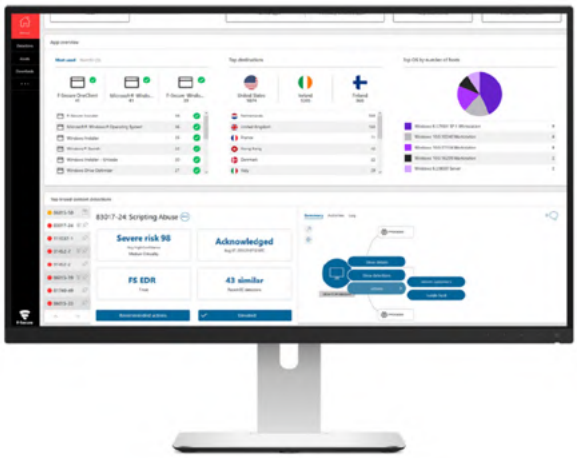
Abbildung 1: Überblick über die Lösung F-Secure Rapid Detection & Response

Die Abbildung oben gibt einen Überblick über die Funktionsweise der Lösung F-Secure Rapid Detection & Response:

1. **Schlanke Clients** überwachen verschiedene Endgeräteaktivitäten, die von Angreifern ausgeführt werden, und streamen Verhaltensereignisse in Echtzeit in unsere Cloud.
2. **Die Echtzeitanalyse von Verhaltensdaten** kennzeichnet und überwacht sowohl die Prozesse als auch andere Verhaltensweisen, die die Ereignisse auslösen.
3. **Broad Context Detection™-Mechanismen** reduzieren die Daten weiter und stellen den Zusammenhang zwischen miteinander verbundenen Ereignissen her, sodass echte Angriffe schnell erkannt werden können. Sie priorisieren sie im Hinblick auf Risikoniveau, Host-Kritikalität und die vorherrschende Bedrohungslandschaft.
4. **Nach der bestätigten Erkennung einer Sicherheitsverletzung führt die Lösung** die IT- und Sicherheitsteams durch die erforderlichen Schritte, um die Bedrohung einzudämmen und Schäden zu beheben.

3.1 Management portal

Die Rapid Detection & Response-Lösung vereinfacht die Verwaltung und Überwachung der fortschrittlichen Bedrohungen auf Ihren Endgeräten über eine einzige, intuitive, webbasierte Konsole. Sie erhalten darüber einen direkten kontextbezogenen Überblick über Ihre IT-Umgebung und den Sicherheitsstatus im gesamten Netzwerk – unabhängig davon, ob Mitarbeiter im Büro oder unterwegs sind.



Das Management-Portal wurde entwickelt, um das Sicherheitsmanagement in anspruchsvollen Umgebungen mit mehreren Standorten zu vereinfachen und zu beschleunigen. Unten sind einige Beispiele dafür aufgeführt, wie die Lösung die erforderliche Zeit und die benötigten Ressourcen für die Überwachung und das Management komplexer Bedrohungen deutlich reduziert:

- Die Lösung ist so konzipiert, dass sie mit jeder Endgeräteschutz-Lösung zusammenarbeitet und mit den Endgeräteschutzlösungen von F-Secure in einer Einzel-Client- und Management-Infrastruktur funktioniert.
- In Kombination mit F-Secure Protection Service for Business (PSB) werden sowohl Malware als auch komplexe Bedrohungen erkenn- und beherrschbar.
- Erkannte Vorfälle werden mit einer aussagekräftigen Visualisierung präsentiert. Sie zeigt gezielte Angriffe im Gesamtzusammenhang auf einer Zeitachse mit allen beeinträchtigten Hosts, relevanten Ereignissen und Handlungsempfehlungen.
- Durch die Konsolidierung des komplexen Bedrohungsmanagements von Endgeräten und Systemtools in einem Portal für Endgerätesicherheit wird das Management insgesamt deutlich optimiert, wodurch Sie Zeit einsparen.
- Da es sich um einen von F-Secure verwalteten Cloud-basierten Service handelt, müssen Sie keine Server-Hardware oder -Software installieren. Sie benötigen lediglich einen Browser und eine Internetverbindung.

Das Management-Portal unterstützt die aktuellen Versionen der folgenden Browser: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome und Safari. Es steht in den Sprachen Englisch, Französisch, Deutsch, Japanisch, Polnisch, Spanisch und mexikanisches Spanisch zur Verfügung (Stand Dezember 2018).

Die Partner-Managed-Version des Management-Portals beinhaltet speziell gestaltete Funktionen, die die Service-Anbieter unterstützen, darunter Endkundenberichte, eine Dashboard-Ansicht mit einem praktischen Überblick über alle verwalteten Unternehmen sowie

3.2 Endgeräte-Clients

Endgeräte-Clients sind schlanke, unauffällige Überwachungstools für die Erkennung von Anomalien, die sich auf allen relevanten Windows- und Mac OS-Computern im Unternehmen installieren lassen. Die Clients erfassen Verhaltensereignisdaten von den Endgeräten und sind so konzipiert, dass sie mit jeder Endgeräteschutz-Lösung zusammenarbeiten und nahtlos mit den Endgeräteschutz-Lösungen von F-Secure in einer Einzel-Client- und Cloud-basierten Management-Infrastruktur funktionieren.

In der folgenden Tabelle finden Sie die unterstützten Betriebssysteme und die jeweiligen Funktionen.

	Windows workstations	Windows servers	Mac OS
BETRIEBSSYSTEME	7 / 8 / 10	2016 / 2012 R2 / 2012 / 2008 R2	10.12 oder neuer
EINZEL-CLIENT MIT F-SECURE	JA*	NEIN**	JA*
CLIENT MIT MITBEWERBER-EPP	JA	JA	JA
VERHALTENSEREIGNISSE	JA	JA	JA
EINBLICK IN ANWENDUNGEN	JA	JA	NEIN**
REMOTE-HOST-ISOLIERUNG	JA	JA	NEIN**

*** Eingeschränkte Unterstützung:** Zunächst nur mit Computer Protection des F-Secure Protection Service for Business (PSB). Bitte überprüfen Sie die Client-Kompatibilität mit der vorhandenen Version; es muss z. B. ein Upgrade von Protection Service for Business auf Computer Protection durchgeführt werden.
**** Wird für einen späteren Zeitpunkt erwartet:** Diese Funktion ist noch nicht verfügbar (für späteren Zeitpunkt erwartet).

Zusätzlich zu F-Secure Protection Service for Business (Computer Protection) wurde die Kompatibilität der Lösung mit den folgenden Lösungen für Endgeräteschutz geprüft (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 und Webroot SecureAnywhere.

3.3 Anwendungstransparenz

Durch einen umfassenden Einblick in Ihre IT-Umgebung und Cloud-Services verringert sich Ihr Risiko für Schäden durch komplexe Bedrohungen und den Verlust von Daten. In unserer Lösung sehen Sie eine Liste aller aktiven Anwendungen, die auf Endgeräten im gesamten Netzwerk Ihres Unternehmens ausgeführt werden, und können auf diese Weise problemlos unerwünschte, unbekannte und schädliche Anwendungen identifizieren.

Dank dieser Transparenz lassen sich potenziell unerwünschte Anwendungen (PUA) und unerwünschte Anwendungen (UA) identifizieren. „Potenziell unerwünschte Anwendungen" zeigen ein Verhalten oder Merkmale, die Sie als unerwünscht ansehen. „Unerwünschte Anwendungen" zeigen ein Verhalten oder Merkmale, deren Auswirkungen auf Ihr Gerät oder Ihre Daten schwerwiegender sind.

Anwendungen, die als „potenziell unerwünscht" (PUA) identifiziert werden, können:

- Ihre Privatsphäre oder Produktivität beeinträchtigen – beispielsweise persönliche Informationen offenlegen oder unerlaubte Handlungen ausführen

- Die Ressourcen Ihres Geräts unnötig belasten – zum Beispiel übermäßig viel Festplatten- oder Arbeitsspeicher nutzen
- Die Sicherheit Ihres Geräts oder der darauf gespeicherten Informationen kompromittieren – zum Beispiel, indem es Sie mit unerwarteten Inhalten oder Anwendungen in Berührung bringt

Diese Verhaltensweisen und Merkmale können zu geringfügigen bis schwerwiegenden Auswirkungen auf Ihr Gerät oder Ihre Daten führen. Sie sind jedoch nicht schädlich genug, um eine Klassifizierung der Anwendung als Malware zu rechtfertigen.

3.4 Verhaltensanalyse

Als eine Kernfunktionalität für die Erkennung komplexer Bedrohungen aus der großen Menge von Verhaltensdaten-Ereignissen nutzt F-Secure Verhaltens-, Reputations- und Big Data-Analysen in Echtzeit mit maschinellem Lernen, um mehrere verdächtige Ereignisse zu erfassen, die zusammenhängen können, beispielsweise auf Grundlage von Aktivitäten.

Mithilfe von künstlicher Intelligenz erkennt die Verhaltensanalyse böswillige, versteckte Aktivitäten anhand kleiner einzelner Ereignisse, die der Angreifer im Rahmen seiner Taktiken, Techniken und Verfahren ausführt.

Die künstliche Intelligenz verfügt über Funktionen für maschinelles Lernen, die der kontinuierlichen Erkennungsverbesserung und der Reduzierung von Falschmeldungen dienen. Die Verhaltensanalyse von F-Secure ist ein herausragendes Beispiel für die Kombination aus Data Science und Kompetenz im Bereich Cybersicherheit. F-Secure nennt das Konzept „Man and Machine“, also „Mensch und Maschine“.

3.5 Broad Context Detection™

Die proprietären Broad Context Detection™-Methoden von F-Secure begrenzen die erkannten Vorfälle auf eine kleine Zahl aussagekräftiger Vorfälle.

Broad Context Detection™ kennzeichnet mögliche Sicherheitsverstöße und sendet den Administratoren Warnmeldungen zu Taktiken, Techniken und Verfahren, die bei gezielten Angriffen eingesetzt werden. Dazu können beispielsweise die folgenden verdächtigen Aktionen gehören:

- Ungewöhnliche Aktivitäten von Standardprogrammen
- Aufrufe laufender Prozesse von atypischen ausführbaren Dateien
- Ausführung unerwarteter Skripte
- Unerwartete Ausführung von Systemtools durch Standardprozesse

Broad Context Detection™ zeigt nur relevante erkannte Vorfälle an und weist ihnen eine Kritikalität zu. Diese basiert auf dem Risikoniveau, Informationen zu betroffenen Hosts und der vorherrschenden Bedrohungslandschaft.

Dank dieser Vorgehensweise erhalten die IT-Teams eine relativ kurze Liste bestätigter Vorfälle, die jeweils mit den verschiedenen Prioritätsstufen gekennzeichnet sind und Handlungsempfehlungen enthalten. Dadurch wissen die Teams nicht nur, worauf sie sich zuerst konzentrieren müssen, sondern können auch schnell und entschieden reagieren.

Weitere Informationen zur Broad Context Detection™ finden Sie im Whitepaper „Detecting Advanced Attacks“ unter www.f-secure.com/RDR.

3.6 Vorfallsmanagement

Die Lösung verfügt über eine integrierte Vorfallsmanagement-Funktion für die Anzeige und das Management von Broad Context Detections. Neu erkannte Vorfälle lösen eine E-Mail-Warnung aus, die einen Direktzugriff zum Management-Portal enthält. Über diesen können Sie sich Details anzeigen lassen und Maßnahmen ergreifen.
Die Broad Context Detections sind in einer benutzerfreundlichen Dashboard-Ansicht aufgelistet, in der Sie die Vorfälle auf Grundlage ihrer Risikobewertung priorisieren können. Diese Bewertung wird automatisch anhand der Kritikalität und Vertraulichkeitsstufen berechnet. Nicht-kritische Broad Context Detections mit niedriger Risikobewertung werden ebenfalls aufgeführt, da aus Angriffen, die sich langsam entwickeln, schwerwiegende Vorfälle mit hoher Risikobewertung werden können.

Im Vorfallsmanagement sind die folgenden Maßnahmen möglich: Broad Context Detections anerkennen oder als „in Bearbeitung" kennzeichnen, überwachen, als abgeschlossen bestätigen, als Falschmeldung oder als unbestätigt schließen.

3.7 Handlungsempfehlungen

Nach der bestätigten Erkennung eines Vorfalls hilft Ihnen die in der Lösung enthaltene Anleitung, dabei, die Bedrohung einzudämmen und Schäden zu beheben. Die Schritte zur Eindämmung und Behebung beinhalten empfohlene Reaktionsmaßnahmen, wie z.B. die Information von Benutzern und die Isolierung von Hosts.

Die Cybersicherheitsexperten von F-Secure haben ihre eigene Erfahrung genutzt, um eine Reihe gängiger Bedrohungen zu analysieren und die Lösung zu trainieren. Deshalb kann die Lösung leicht verständliche Anleitungen für die Reaktion auf eine Vielzahl fortschrittlicher Bedrohungen sowie darauf bezogene Handlungsempfehlungen bieten. Auch weniger versierte IT- und Sicherheitsteammitglieder können auf diese Weise die richtigen Maßnahmen ergreifen, um die Bedrohung einzudämmen und Schäden zu beheben.

3.8 Elevate to F-Secure

Durch „Elevate to F-Secure"-Anfragen über die Lösung erhalten die Bedrohungsanalysten von F-Secure die Berechtigung, auf alle Metadaten zuzugreifen, die von den installierten Clients für einen konkret erkannten Vorfall gesammelt wurden. Die diensthabenden Bedrohungsanalysten von F-Secure nehmen die Anfrage innerhalb von zwei Stunden an und beginnen damit, die Art des potenziellen Vorfalls zu ermitteln. Dafür sammeln sie zusätzliche Informationen und geben weitere sachkundige Handlungsanweisungen, um die Bedrohung zu validieren oder eine detaillierte Bedrohungsanalyse und einen Bericht bereitzustellen.

Der „Elevate to F-Secure"-Service konzentriert sich auf die Analyse der technischen Beweise in Bezug auf die betreffenden potenziellen Vorfälle. Dies umfasst die Methoden und Technologien, Netzwerkrouten, Verkehrsursprünge und zeitlichen Abläufe. Das Team von F-Secure gibt praktische Handlungsanweisungen, wie man die vorliegende Situation eindämmen und beheben kann. Diese Anweisungen vermittelt das Team jedoch nur über die Lösung. Zusätzliche Professional Services zur Unterstützung bei der Reaktion auf Vorfälle müssen gesondert vereinbart werden.

Wenn der Kunde aufgrund der Untersuchungen davon ausgeht, dass eine Straftat verübt wurde, empfiehlt F-Secure, die zuständigen Behörden zu kontaktieren.

3.9 Automatisierte Aktionen

Ferngesteuerte Reaktionsmaßnahmen stehen als automatisierte Aktionen zur Verfügung. Die automatischen Reaktionsmaßnahmen können die Auswirkungen von gezielten Cyberangriffen reduzieren, da diese rund um die Uhr eingedämmt werden, sobald ein entsprechendes Risiko-Level erreicht ist. Mithilfe automatisierter Aktionen können Sie zudem Regeln dafür festlegen, wann Sie über die erkannten Vorfälle informiert werden sollen. Die Automatisierung basiert auf vordefinierten Zeitplänen und wurde speziell für Teams entwickelt, die nur während der Geschäftszeiten die Vorfallserkennung überwachen und für die Reaktion auf Vorfälle verfügbar sind.
Automatisierte Aktionen werden voraussichtlich mit dem kommenden Update zur Verfügung gestellt.

4. DATENSICHERHEIT

4.1 Datenschutz und Vertraulichkeit

Da F-Secure seinen Sitz in Finnland hat, halten wir uns an die strengen Datenschutz- und Sicherheitsgesetze Finnlands und der Europäischen Union. Wir erfüllen die Vorgaben des Datenschutz-Frameworks der Europäischen Union und verstehen die Datenschutzanforderungen unserer Kunden. F-Secure arbeitet gemäß der finnischen Umsetzung der EU-Datenschutzrichtlinie, und die Lösung F-Secure Rapid Detection & Response wurde im Einklang mit der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union gestaltet. Weitere Informationen zur Konformität von F-Secure mit der Datenschutz-Grundverordnung finden Sie hier https://www.f-secure.com/GDPR.

4.2 Maßnahmen für Datensicherheit

Als Sicherheitsunternehmen nehmen wir die Sicherheit unserer Rechenzentren sehr ernst und ergreifen deshalb zahlreiche Sicherheitsmaßnahmen, darunter:

- **Sicherheit by Design:** Unsere Systeme sind von Grund auf sicher konzipiert. Datenschutz und Sicherheit berücksichtigen wir bei der Entwicklung unserer Technologien und Systeme ab den frühen Phasen der Konzeption und des Designs bis hin zur Implementierung und zum Betrieb.
- **Strenge Zugriffskontrollen:** Nur eine kleine, überprüfte Gruppe von F-Secure-Mitarbeitern hat Zugriff auf die Kundendaten. Zugriffsrechte und -stufen basieren auf ihrer Arbeitsaufgabe und Position. Hierbei kommt das Least-Privilege-Prinzip zur Anwendung, das mit den festgelegten Zuständigkeiten abgestimmt wird.
- **Hohe Betriebssicherheit:** Betriebliche Sicherheit ist ein alltäglicher Teil unserer Arbeit und umfasst Schwachstellenmanagement, Abwehr von Malware und stabile Vorfallsmanagement-Prozesse für Sicherheitsereignisse, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten beeinträchtigen können.

4.3 Rechenzentren

Unsere RDR-Lösung (Rapid Detection & Response) nutzt AWS-Rechenzentren (Amazon Web Services), um höchstmögliche Verfügbarkeit und Fehlertoleranz zu gewährleisten. Sie bieten zudem bessere Reaktionszeiten und bedarfsorientierte Skalierbarkeit. AWS gibt an, dass alle seine Rechenzentren den Anforderungen für Tier 3+ entsprechen. Weitere Informationen zu den AWS-Rechenzentren finden Sie unter https://aws.amazon.com/compliance/

Die Lösung ist zunächst auf Basis von AWS in Europa (Irland) verfügbar.

5. GLOSSAR

Liste der Begriffe, die in F-Secure Rapid Detection & Response verwendet werden

Fortschrittliche Bedrohungen	Gezielte Angriffe mit dateilosen Techniken sind ein Beispiel für eine fortschrittliche Bedrohung. Herkömmliche Lösungen für Endgeräteschutz sind nicht so konzipiert, dass sie alle fortschrittlichen Bedrohungen abwehren können.
Anomalie	Ein neues, zuvor nicht identifiziertes Ereignis oder eine Abfolge von Ereignissen, die höchstwahrscheinlich das Ergebnis böswilliger Aktivitäten sind.
Sicherheitsverstoß	Ein Datensicherheitsverstoß ist ein bestätigter Vorfall, bei dem sensible, vertrauliche oder anderweitig geschützte Daten für Unbefugte wie etwa Cyberkriminelle zugänglich werden.
Broad Context Detection™	Die einzigartige und speziell entwickelte F-Secure-Technologie, die mögliche Vorfälle und Anomalien von Kundensystemen mit umfassenderen Kontextinformationen zu allen beeinträchtigten Hosts darstellt.
Client / sensor	Software, die auf überwachten Hosts ausgeführt wird. Der Client, der auch als Sensor bezeichnet wird, überwacht den Gerätestatus und kommuniziert mit dem F-Secure Rapid Detection & Response-Backend.
Elevate to F-Secure	F-Secure bietet eine Support-Funktion an, die Unterstützung bietet, wenn eine weitere Bedrohungsanalyse durch die Bedrohungsanalysten von F-Secure erforderlich ist.
Host/Ressource	Ein Gerät, auf dem ein Client ausgeführt und das vom System überwacht wird.
Vorfall	Ein Ereignis, das darauf hindeutet, dass Systeme oder Daten kompromittiert wurden.
Risiko	Wichtigkeit eines erkannten Vorfalls im Verhältnis zum überwachten Unternehmen und Host.
Verdächtiges Ereignis	Ein neues Ereignis oder eine Abfolge von Ereignissen, die auf einem überwachten Client zuvor noch nie vorgekommen sind. Diese Ereignisse sind höchstwahrscheinlich böswillig und müssen eingehender analysiert werden.

ÜBER F-SECURE

Niemand kennt sich mit Cybersicherheit besser aus als F-Secure. Bereits seit drei Jahrzehnten treibt F-Secure Innovationen in der Cybersicherheit voran und schützt Zehntausende von Unternehmen und Millionen von Menschen vor Angriffen. Mit beispielloser Erfahrung im Endgeräteschutz sowie mit Erkennungs- und Reaktionsvorgängen schirmt F-Secure Unternehmen und Verbraucher gegen alles ab – komplexe Cyberangriffe und Verletzungen der Datensicherheit genauso wie ausgedehnte Ransomware-Infektionen. Die hochentwickelte Technologie von F-Secure verbindet die Leistungsfähigkeit des maschinellen Lernens mit der Kompetenz des Fachpersonals in seinen weltweit anerkannten Sicherheitslaboren zu einem einzigartigen Ansatz mit dem Namen Live Security.

Mit seinen Sicherheitsexperten war F-Secure an mehr europäischen Untersuchungen zu Cyberkriminalität beteiligt als jedes andere Unternehmen am Markt. Unsere Produkte werden weltweit durch über 200 Breitband- und Mobilfunkbetreiber sowie zahlreiche Reseller vertrieben.

F-Secure wurde 1988 gegründet und ist an der Börse NASDAQ OMX Helsinki Ltd. notiert.

Besuchen Sie f-secure.com/RDR

F-Secure