KURZBESCHREIBUNG DER LÖSUNG

ThreatSync

Hacker sind raffiniert. Sie sehen Ihre Sicherheitsmechanismen als Puzzle und Ihre Daten als Ansporn dafür an, dieses Puzzle zu lösen. Jeden Tag schaffen Cyberkriminelle neue Möglichkeiten, eine Abwehr zu umgehen und sich in Ihrem Netzwerk zu verstecken. ThreatSync ist eine Threat Detection and Response-Plattform, die erweiterte Sicherheitssysteme integriert, um Infektionen und Infiltrationen im Verborgenen auszumachen.

Mit Blick auf Ihr erweitertes Netzwerk aus der Cloud-Perspektive erfasst und analysiert ThreatSync Telemetriedaten von Ihren Firebox-Appliances, Endpoints und Benutzern, um proaktiv Sicherheitsbedrohungen zu erkennen und entsprechend zu reagieren. ThreatSync korreliert Sicherheitsereignisse zu einem Bedrohungsindex, der Ihnen ermöglicht, unverzüglich Maßnahmen gegen neue oder verborgene Bedrohungen zu ergreifen.

Erkennung und Abwehr mithilfe von Korrelation beschleunigen

Unternehmen in der heutigen Zeit haben es mit entschlossenen Bedrohungsakteuren zu tun, die mit ausgeklügelten Angriffen ihre Daten ins Visier nehmen.

Egal, wie ausgeklügelt diese Angriffe sind, ist das Grundprinzip immer gleich:

1. Eindringen in das Netzwerk

Hollywood-Filme könnten den Eindruck vermitteln, dass Netzwerke von einem Team von Hackern bedroht werden, die bei dem Versuch, Firewalls zu durchbrechen, wild auf ihren Tastaturen herumtippen. Die Wahrheit ist, dass die meisten Sicherheitsverletzungen entweder auf einen Anwenderfehler, z. B. das Hereinfallen auf Phishing-E-Mails, oder ein unzureichend konfiguriertes Netzwerk zurückzuführen sind. Es ist einfach leichter, einen abgelenkten Mitarbeiter dazu zu bringen, auf einen Link zu klicken oder eine Datei herunterzuladen und ihn so dazu zu bringen, die Payload geradewegs durch die virtuelle Eingangstür hereinzulassen.

2. Erreichen des Ziel-Endpoints

Nachdem die bösartige Payload an den Anwender, Computer oder das Gerät übertragen wurde, manipuliert sie die Ressource und verschafft sich Zugang zur Umgebung. Dabei erfolgt der Zugriff gewöhnlich durch die Ausnutzung einer bekannten Schwachstelle, für die zuvor ein Patch zur Verfügung gestellt wurde. Nachdem sie Fuß gefasst haben, gelangen Angreifer mithilfe der Rechteausweitung von Workstations zu Servern, bewegen sich ungehindert in der gesamten Umgebung und manipulieren individuell anvisierte Rechner.

3. Erreichen der Zielsetzung

Das Ziel eines Angreifers zu ermitteln kann schwierig sein. Je nach ihren Beweggründen können Hacker versuchen, Ihre Daten zu exfiltrieren oder Ihren IT-Ressourcen Schaden zuzufügen. Oder sie warten einfach und beobachten. Sobald ein Angreifer es in Ihr Netzwerk geschafft hat, wird er zu einem normalen Anwender mit Berechtigungen und fester Präsenz. So erhält er Zugang zu vertraulichen Ressourcen und die Möglichkeit, sich noch lukrativere Ziele auszusuchen.

Jede dieser Phasen hinterlässt Spuren, bei denen die Alarmglocken schrillen sollten. Diese Hinweise verlieren sich jedoch leicht in den Protokollen unzusammenhängender Sicherheitslösungen. Sobald sie sich in das Netzwerk ihres Opfers eingeschleust haben, können Bedrohungsakteure ihre Angriffe mit größtmöglichem Schaden durchführen, ganz gleich, ob sie sich nur Minuten oder gar Monate im Netzwerk aufhalten. XDR-Lösungen führen isolierte Sicherheitsinformationen zusammen und ermöglichen so die Korrelation über mehrere Sicherheitsebenen hinweg.

Mithilfe der Korrelation können Bedrohungen früher identifiziert werden. Außerdem kann festgestellt werden, welche Endpoints befallen sind, der Infektionsweg kann nachverfolgt und der Ursprung der Bedrohung ermittelt werden. Die Korrelation bietet Administratoren die erforderliche Visualisierung, um unbekannte und schwer fassbare Bedrohungen zu stoppen, bevor sie Schaden anrichten und sich im Unternehmen ausbreiten können.

Reduzierung der Angriffsfläche mit ThreatSync

ThreatSync ist eine cloudbasierte Lösung mit Erkennungs- und Reaktionsfunktionen, die Sie mit Ihrer Firebox verwenden können, um die Auswirkungen von Datensicherheitsverletzungen, Malware-Infektionen und Infiltrationen durch frühzeitige Erkennung und entsprechende automatisierte Abwehrmaßnahmen zu minimieren. ThreatSync korreliert Daten über die gesamte Unified Security Platform, sodass technische Teams über die Transparenz und den Kontext für ein effektives Arbeiten verfügen. Die Korrelations-Engine von ThreatSync erfasst und analysiert Telemetriedaten zur Identifizierung von Anzeichen bekannter Bedrohungen, die sich unerkannt in Ihrem Netzwerk verstecken. Gleichzeitig können Zero-Day-Bedrohungen frühzeitig aufgedeckt werden.

WatchGuard hostet ThreatSync-Server in den folgenden Regionen:

- Vereinigte Staaten (Oregon)
- Europa (Frankfurt)
- Asiatisch-pazifischer Raum

Mithilfe von Korrelation stellt ThreatSync ein detailliertes, kontextuelles und verwertbares Bild Ihrer Bedrohungsoberfläche bereit. Gefährdungsindikatoren von der Firebox, dem Endpoint Security-Portfolio von WatchGuard und von AuthPoint werden zusammengeführt, analysiert, korreliert und einzeln bewertet, um abschließend in Vorfällen zusammengefasst zu werden. Diese Bedrohungsindizes vereinfachen eine Priorisierung und sind auch für normale Anwender leicht verständlich.

ThreatSync korreliert die folgenden Datentypen:

Netzwerk

- Verbindungsereignisse: Blockierungen, Abbrüche oder Verweigerungen
- Reputationsereignisse: Verbindungsversuche zu einem bekannten schädlichen Standort über FQDN, IP, DNS, URL
- Erkennung von Malware bei HTTP-, HTTPS-, FTP-, TCP, UDP-, SMTP- und POP3-Datenverkehr: über Signatur, maschinelles Lernen oder Cloud-Sandboxing

Endpoint

- Bösartige Dateien, Prozesse, Anwendungen und Netzwerkverbindungen

Licht ins Dunkle bringen

Ohne Korrelation kann es übermäßig viel Zeit in Anspruch nehmen, angegriffene Endpoints und Anwender zu identifizieren und zu bestätigen. Technische Teams sind teilweise einfach durch unzusammenhängende Bedrohungsdaten überfordert und übersehen häufig frühzeitige Hinweise auf mögliche Angriffe, die ohne richtigen Kontext nicht als solche zu erkennen sind. ThreatSync rettet Ihre Teamzyklen, beschleunigt die Erkennung von Bedrohungen und erhöht die Genauigkeit durch die automatische Korrelation relevanter Bedrohungsdaten von der gesamten WatchGuard Unified Security Platform.

Weitere Informationen zu den prämierten Netzwerksicherheitslösungen von WatchGuard finden Sie unter www.watchguard.com.

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von 250.000 Kunden. Die Philosophie von WatchGuard ist es, hochprofessionelle Sicherheitslösungen für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter **WatchGuard.de**.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder auf unserer Seite auf LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: **www.secplicity.org**

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de