SOLUTION BRIEF

Security Operations: Schnellere Incident Response mit FortiSOAR

Zusammenfassung

Die Angriffsflächen von Netzwerken werden durch neue Bedrohungen und digitale Innovationen weiter vergrößert. Um damit Schritt zu halten, ergänzen viele Unternehmen vorhandene Security-Lösungen um Einzelprodukte. Dadurch erhöht sich jedoch die Sicherheitskomplexität, was zahlreiche Probleme verschlimmert: Zu viele Geräte verschiedener Anbieter müssen verwaltet werden, zum Untersuchen der unzähligen Alerts fehlt die Zeit und manuelle Prozesse verlangsamen die Reaktionszeiten. Zudem mangelt es an qualifizierten Fachkräften, um die täglich steigende Arbeitslast zu bewältigen.

Das Ergänzen der Security-Architektur um SOAR-Funktionen (Security Orchestration, Automation and Response) kann diesen Druck verringern. Mit FortiSOAR können Security-Teams ein benutzerdefiniertes automatisiertes Framework erstellen, das alle Security-Tools des Unternehmens vereint, ein Ignorieren von Sicherheitswarnungen verhindert und gleichzeitig das ständige Springen von einem Kontext zum anderen reduziert. Security-Teams können dank dieser Funktionalität nicht nur Sicherheitsprozesse anpassen, sondern auch optimieren.

Disaggregierte Security führt zum Ignorieren von Alerts und erhöhtem Risiko

Die tägliche Flut an Sicherheitswarnungen führt oft dazu, dass Security-Analysten „die Waffen strecken“. Schuld an diesem Problem sind zunehmend komplexere, fragmentierte Sicherheitsinfrastrukturen, weil zu viele Einzelprodukte verschiedener Anbieter implementiert wurden: Um mit neuen Bedrohungen und Risiken Schritt zu halten, setzen Unternehmen im Durchschnitt mittlerweile 47 verschiedene Security-Lösungen und -Technologien ein.[1]

Während die schiere Menge der Alerts einen großen Teil des Problems ausmacht, verlangt das Verfolgen, Untersuchen und Beheben von Warnungen aus unterschiedlichsten Quellen von den Mitarbeitern eines Security Operations Centers (SOC) einen hohen manuellen Aufwand. Doch diese ineffizienten Workflows verlangsamen den Incident-Response-Prozess: Durchschnittlich dauert es 279 Tage, bis eine einzige Sicherheitslücke erkannt und geschlossen wird.[2]

Gleichzeitig sind die Security Operations in den meisten Unternehmen personell unterbesetzt. Fast zwei Drittel (65 %) der Unternehmen verfügen derzeit nicht über die notwendigen Fachkräfte, um einen effektiven Security-Betrieb aufrechtzuerhalten.[3] Diese sich überschneidenden Faktoren erhöhen die Wahrscheinlichkeit, dass ein Verstoß unentdeckt bleibt.

Im Vorjahr verursachten Sicherheitsverletzungen, die unter 200 Tagen bestanden, 1,22 Mio. $ weniger Kosten als Verstöße mit einem Lebenszyklus von über 200 Tagen (3,34 Mio. $ gegenüber 4,56 Mio. $) – ein Unterschied von 37 %.[4]

Der SOAR-Markt wird voraussichtlich von 2019 bis 2024 auf fast 1,8 Mrd. $ bei einer jährlichen Wachstumsrate von 15,6 % anwachsen.[5]

Eine SOAR-Lösung unterstützt das Security-Team bei der Integration von Security-Tools. Separate Komponenten können so in einer defensiven Koordination miteinander kommunizieren und zusammenarbeiten. Das verbessert nicht nur die Netzwerk-Transparenz, sondern führt auch zu wenigeren, strategischeren Cyber-Security-Alerts.[6] Langwierige Routine-Arbeiten, die keine menschliche Kontrolle erfordern, lassen sich zudem automatisieren. Auch liefert eine gute SOAR-Lösung umfassende Informationen und Kontext zu Bedrohungen – eine große Unterstützung für Analysten, wenn Fälle schnell anhand von Kriterien wie Schweregrad des Risikos, Sensibilität und Kritikalität der bedrohten Geschäftsfunktionen gesichtet werden müssen.[7]

FortiSOAR integriert Security und automatisierte Bedrohungsabwehr

FortiSOAR bietet die Möglichkeit, Alerts aus unterschiedlichen Security-Produkten zu aggregieren und mit Zusatzinformationen anzureichern. Security-Teams erhalten damit eine einfachere Orchestrierung und Verwaltung, da klar definierte Playbooks verwendet werden können. Auch entfallen durch automatisierte Reaktionen zeitaufwändige manuelle Workflows.

Als Teil der integrierten Fortinet Security Fabric-Architektur vereint FortiSOAR unterschiedliche Security-Tools zu „einem einzigen System“. Dadurch kann FortiSOAR viele Alert-Prozesse mit geringem Schweregrad automatisieren, damit sich SOC-Analysten auf kritischere Aufgaben konzentrieren können. Die folgenden vier Anwendungsfälle verdeutlichen den unmittelbaren Wert von FortiSOAR für SOC-Teams, die derzeit an der Belastungsgrenze arbeiten:

Anwendungsfall 1: Einheitliche SOC-Workbench

FortiSOAR vereinfacht die SOC-Komplexität durch die Integration bislang isolierter Security-Einzellösungen in ein zentrales Orchestrierungssystem, das in praktisch in jeder Umgebung bereitgestellt werden kann. FortiSOAR bietet über 280 sofort einsatzbereite Connectors, um nahtlos vorhandene Sicherheitslösungen anderer Anbieter einzubinden, Alert-Informationen zu erfassen und zugleich eine unternehmensweite Transparenz und Kontrolle bereitzustellen. Diese Integration eliminiert die Fragmentierung des Ecosystems, vereinfacht Security-Operations-Prozesse und verlängert die Nutzungsdauer vorhandener Tools, um die Kapitalrendite (ROI) bisheriger Anschaffungen zu maximieren.

Anwendungsfall 2: Automatisierte Alert-Sichtung

FortiSOAR fasst Sicherheitswarnungen zentral zusammen und reichert sie mit zusätzlichem Kontext an, um die Klärung zu verkürzen. Dadurch verringert sich die Anzahl „falsch-positiver" Alerts. Auch bietet FortiSOAR erweiterte Funktionen für das Case-Management, um Untersuchungen zu definieren, zu leiten und schneller abzuschließen. FortiSOAR optimiert einfache SOC-Aufgaben wie das Erfassen von Alerts, ihre Priorisierung anhand des Schweregrads und die Aufgabenverteilung. Komplexere E2E-Aufgaben (Exchange-to-Exchange) wie Sichtung, Anreicherung, Untersuchung und Fehlerbehebung lassen sich zudem automatisieren. Diese intelligenten Integrations- und Automatisierungsfunktionen entlasten Security-Teams und verringern so ein Ignorieren von Sicherheitswarnungen. SOC-Analysten können sich dadurch verstärkt auf die Bedrohungssuche konzentrieren und aktive Sicherheitsverletzungen in kürzeren Zeitfenstern eliminieren.

Anwendungsfall 3: Schnellere Incident Response

Manuelle Workflows verlangsamen die Alert-Untersuchung und die Zeit bis zur Lösung eines Sicherheitsproblems. Auch sind sie anfällig für Fehler von Mitarbeitern. FortiSOAR erweitert die Automatisierungsfunktionen von FortiAnalyzer und FortiSIEM (Security Incident and Event Management) um eine robuste Orchestrierung und Automatisierung aller SOC-Prozesse. Security-Teams können ihre Effizienz steigern, indem sie jede Aufgabe, Änderung oder Aktualisierung abgestimmt auf die Unternehmensanforderungen automatisieren. Statt nur eine einzelne Entität zu automatisieren, kann FortiSOAR auf das gesamte SOC erweitert werden und so die Gesamtsicherheit verbessern.

Darüber hinaus bietet FortiSOAR die einzigartige Möglichkeit, jede Reaktion zu automatisieren. Bei Erreichen einer gewissen Kritikalität können Security-Teams eine Identität sofort offline nehmen und FortiSOAR Playbooks und Connectors innerhalb des Produkts anwenden.

Anwendungsfall 4: Entlastung begrenzter SOC-Teams

Durch den Wegfall manueller Aufgaben werden überlastete SOC-Teams in Hinblick auf Arbeitszeiten und Arbeitskosten entlastet, wovon auch die Gesamtbetriebskosten (TCO) im Security-Bereich profitieren: FortiSOAR rationalisiert Security-Operations-Prozesse mit automatisierten Workflows auf intelligente Weise. Protokolle und automatisierte Sicherheitsreaktionen lassen sich zudem für spezifische SOC-Anforderungen anpassen.

Für eine einfache Integration werden sofort einsatzbereite Drag-and-Drop-Playbooks unterstützt, die eine sofortige Konfigurierbarkeit und schnelle Rücksetzung auf den Anfangswert ermöglichen. Auch trägt FortiSOAR zu einem einheitlichen Wissensstand und Know-how im SOC-Team bei. Verlässt z. B. ein Mitarbeiter das Unternehmen, bleiben seine Workflow-Insights und Erfahrungen im System dokumentiert.

Management von Risiken, Ressourcen und Ergebnissen

Der Druck auf die Security Operations wird in Zukunft nicht abnehmen – im Gegenteil. Wegen der unablässig wachsenden Angriffsfläche und dem konstanten Mangel an Ressourcen dürfte es weiterhin schwierig bleiben, mit steigenden Risiken Schritt zu halten. Eine effektive SOAR-Lösung mit umfassendem Funktionsumfang kann jedoch SOC-Teams dabei unterstützen, diese Schwierigkeiten anzugehen und gleichzeitig die Sicherheitsprozesse im Unternehmen verbessern, optimieren und stärken.

FortiSOAR bietet eine agile, anpassbare Lösung für die Security Operations, um besser auf eine sich ständig weiterentwickelnde Bedrohungslage zu reagieren. Die Automatisierungs- und Orchestrierungsfunktionen von FortiSOAR helfen Unternehmen dabei, das Security-Ecosystem zu vereinfachen, ein Ignorieren von Alerts zu verhindern, Reaktionszeiten zu verkürzen und personell begrenzte SOC-Teams zu entlasten.

Darüber hinaus bietet FortiSOAR eine einfache Lizenzierung mit einem benutzerbasierten Lizenzmodell zu vorhersehbaren Kosten. Seine skalierbare Architektur zeichnet sich durch eine hohe Verfügbarkeit aus und lässt sich problemlos für Wachstumsphasen und dezentrale Unternehmen skalieren, ohne dabei die erforderlichen Implementierungs- und Management-Ressourcen überzustrapazieren.

[1] „53 % of enterprises have no idea if their security tools are working“. Help Net Security, 31. Juli 2019.

[2] „2019 Cost of a Data Breach Report“. Ponemon Institute und IBM Security, 2019.

[3] „Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019“. (ISC)², 2019.

[4] „2019 Cost of a Data Breach Report“. Ponemon Institute und IBM Security, 2019.

[5] „Security Orchestration Automation & Response (SOAR) World Markets, Outlook to 2024: The High Number of False Security Alerts Presents Lucrative Market Opportunities“. Research and Markets, 15. November 2019.

[6] Muhammad Omar Khan: „Why SOAR is a Good Bet For Fighting Mega Cyber Security Breaches“. Entrepreneur, 23. Mai 2019.

[7] Cian Walker: „SOAR: The Second Arm of Security Operations“. Security Intelligence, 9. April 2019.

FORTINET

www.fortinet.com/de

5. Mai 2020, 14:02 Uhr

587297-0-1-DE