SOLUTION BRIEF

Massive Zeitersparnis bei der Erkennung, Eindämmung, Untersuchung und Beseitigung von Bedrohungen mit Fortinet Security Operations

Zusammenfassung

Bedrohungsakteure, die erfolgreich in Unternehmensnetzwerke eingedrungen sind, können dort oft ungehindert und in aller Ruhe ihre Ziele verfolgen: Laut einer Studie braucht ein durchschnittliches Security-Team 16 bis 204 Tage für die Aufdeckung eines Sicherheitsvorfalls[1] – und das angesichts einer Bedrohungslage, die 75 % der Sicherheitsexperten verglichen mit den letzten fünf Jahren als extrem kritisch bewerten.[2]

Die Fortinet Security-Operations-Lösung nutzt KI und fortschrittliche Analysen, um die Aktivitäten von Benutzern, Geräten, Netzwerken, E-Mails, Anwendungen, Dateien und Protokollen zu überwachen sowie anomale oder bösartige Aktionen zu erkennen, die Mitarbeiter leicht übersehen können. Durch die native Integration einzelner Sicherheitskomponenten über die Fortinet Security Fabric bietet diese SecOps-Lösung einen einzigartigen Austausch von Bedrohungsinformationen, der eine automatisierte Eindämmung, Prognosen für proaktive Maßnahmen sowie eine Risikominimierung ermöglicht. Security-Teams gewinnen so mehr Zeit für die umfassende Untersuchung und koordinierte, automatisierte Behebung von Sicherheitsvorfällen. Davon profitiert nicht nur die SecOps-Produktivität, sondern auch die konsequente Durchsetzung der Sicherheitsrichtlinien.

Zur schnelleren Bedrohungserkennung investiert die Hälfte der Unternehmen in künstliche Intelligenz (KI) und maschinelles Lernen (ML), während 44 % mit SIEM- und SOAR-Lösungen die Reaktionszeit verkürzen.[4]

Im Durchschnitt verkürzt die Fortinet Security-Operations-Lösung die Erkennung und Eindämmung von Angriffen von 180 Stunden auf unter 1 Stunde (oft sogar nur Minuten) mit einer anschließenden Untersuchung und Behebung in 10 bis 15 Minuten.[3]

Mehr Komplexität (und Kosten) durch neue Bedrohungen und erweiterte Angriffsflächen

Die hochdynamische Bedrohungslage, eine ständig wachsende Angriffsfläche und der anhaltende Fachkräftemangel verlangt Security-Teams tagtäglich einiges ab. Selbst personell gut besetzte Teams mit erfahrenen Sicherheitsexperten haben mittlerweile Schwierigkeiten, Unternehmensnetzwerke wirksam zu schützen. Laut dem FortiGuard Incident Response Team, das häufig zur Untersuchung von Cyberangriffen herangezogen wird, bleiben Bedrohungsakteure in Unternehmensnetzwerken durchschnittlich 36 Tage lang unentdeckt.[5] Diese Zahl liegt zwar deutlich unter den 204 Tagen, die ein IBM-Bericht nennt,[6] lässt aber keinen Zweifel daran, dass Bedrohungsakteure oft viel zu viel Zeit zum Erreichen ihrer Ziele haben.

Dazu kommt, dass die Eindämmung von Sicherheitsvorfällen immer kostspieliger wird. Bei einer aktuellen Umfrage berichteten 84 % der Unternehmen von mindestens einem Sicherheitsvorfall in den letzten 12 Monaten mit erheblichen Kosten: 48 % der Befragten zahlten über 1 Million US-Dollar oder mehr für die Beilegung von Cybervorfällen.[7]

Schnellere Bedrohungserkennung und Reaktion mit der Fortinet Security-Operations-Lösung

Die befragten Unternehmen investieren vorrangig in fortschrittliche Technologien wie künstliche Intelligenz (KI) und maschinelles Lernen (ML) zur schnelleren Eindringlingserkennung sowie in zentralisierte Technologien wie SIEM und SOAR, die die Reaktion auf Sicherheitsvorfälle verkürzen. Bevorzugt werden integrierte Sicherheitsprodukte, um Komplexität abzubauen.[8]

Die Fortinet Security-Operations-Lösung ist für diese Sicherheitsziele wie geschaffen und bietet Unternehmen entscheidende Vorteile wie:

- frühzeitige Erkennung und Verhinderung von Cyberangriffen mit dem breitesten Spektrum verhaltensbasierter Sensoren, die sich in bestimmten Bereichen oder bereichsübergreifend einsetzen lassen
- zentrale Security-Automatisierung zur Zusammenfassung, Anreicherung und Analyse von Sicherheitsinformationen (von verhaltensbasierten und anderen Sensoren) sowie Visualisierung, Orchestrierung und Automatisierung der Untersuchung und Behebung von Sicherheitsvorfällen

- ergänzende SOC-Services zur Bewertung und Verbesserung der Einsatzbereitschaft interner Teams und Technologien mit optionaler Ad-hoc- oder ständiger Verstärkung interner Teams und Unterstützung bei Krisenvorfällen
- integrierte GenAI-Unterstützung (generative künstliche Intelligenz) zur Information von Analysten, um die Untersuchung von Bedrohungen, Reaktionsstrategien und anderen wichtigen Aktivitäten zu verkürzen

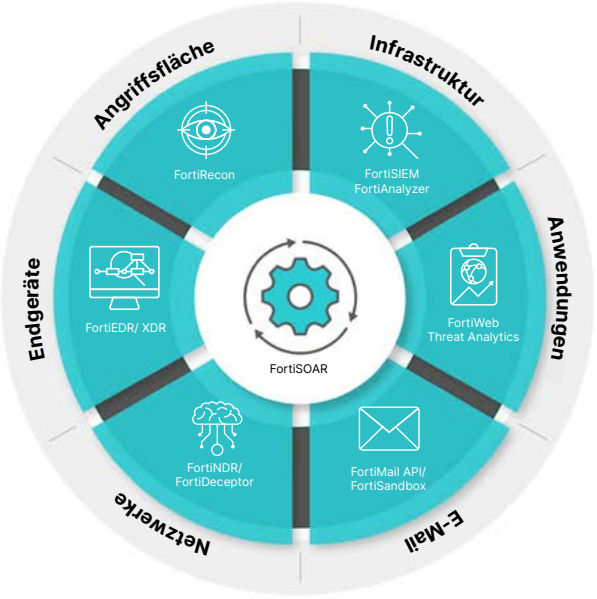

Abbildung 1: Fortinet Security-Operations-Lösung

Automatisierung durch Integration mit der Fortinet Security-Operations-Lösung

Als integriertes Angebot bietet die Fortinet Security-Operations-Lösung eine Leistung, die über den Schutz durch einzelne Sicherheitsprodukte hinausgeht: Alle Security-Komponenten tauschen – zusätzlich zur eigenen Bedrohungserkennung – auch automatisch Bedrohungsinformationen aus und ergreifen Abwehrmaßnahmen. Auf Bedrohungen wird also nicht nur wirksam reagiert, sondern das Unternehmen erhält eine proaktive Cyberverteidigung. Die folgenden Beispiele zeigen, wie die Fortinet Security-Operations-Lösung mit anderen Fortinet-Produkten integriert werden kann und so die unternehmensweite Sicherheit verbessert.

- **FortiEDR:** Nach der verhaltensbasierten Erkennung verdächtiger oder bösartiger Laufzeitaktivitäten auf einem Endgerät und dem Blockieren von riskanten Vorgängen (wie dem Verschlüsseln von Dateien oder dem Herstellen einer Netzwerkverbindung) können Bedrohungsinformationen über die native Fabric-Integration zwischen FortiEDR und FortiGate NGFWs bidirektional als Peer-to-Peer-Verbindung ausgetauscht werden.
- **FortiNDR:** Wurden anhand des Verhaltens eines Geräts verdächtige oder bösartige Netzwerkaktivitäten erkannt, kann FortiNDR die Geräteinformationen von FortiEDR weiterverarbeiten und – dank seiner nativen Integration in die Security Fabric – das verdächtige Gerät sogar in Quarantäne setzen.
- **FortiRecon:** Nach der Bewertung von extern sichtbaren Assets kann FortiRecon von den FortiGate NGFWs über weitere Assets informiert werden und diese bei der Inventarisierung sowie der Überprüfung von Schwachstellen (Scanning) einbeziehen. Auch dieses Zusammenspiel funktioniert über die native Security-Fabric-Integration.
- **FortiDeceptor:** FortiDeceptor ist ebenfalls nativ in die Security Fabric integriert. Wurde ein Bedrohungsakteur im Netzwerk gefunden, kann FortiDeceptor die FortiGate NGFWs anweisen, den Zugriff auf andere Geräte zu blockieren, und gleichzeitig die Geräteantworten senden, die der Angreifer erwartet. So erfährt der Bedrohungsakteur nicht, dass die Fortinet-Lösung ihn bereits erkannt hat, während das Security-Team den unwissenden Angreifer weiter einzingeln kann.
- **FortiSandbox:** FortiSandbox erstellt eine verhaltensbasierte Risikobewertung und kann diese mit vielen Fortinet-Geräten teilen (wie FortiGate NGFWs oder FortiMail), damit Bedrohungen in Echtzeit vor Erreichen ihres Ziels blockiert werden.

- **FortiAnalyzer:** Durch die native Integration mit dem gesamten Fortinet-Portfolio können Unternehmen mit dem FortiAnalyzer bei bestimmten Ereignissen das Auslösen einer Reaktion (Event Trigger) sowie automatisierte Reaktionen festlegen.
- **FortiSIEM:** Nach der Erkennung von Sicherheitsvorfällen durch zahlreiche Analysen (gestützt durch maschinelles Lernen mit einer ML-Workbench) wird die Remediation, die Behebung des Sicherheitsvorfalls, eingeleitet. FortiSIEM kann dafür auf über 300 Technologie-Integrationen zurückgreifen oder Sicherheitsvorfälle nahtlos an FortiSOAR zur robusten Orchestrierung und Automatisierung übergeben.
- **FortiSOAR:** Sobald FortiSOAR Warnungen über verdächtige Aktivitäten erhält, können automatisierte Playbook-Aktionen erfolgen, wie z. B. der Einsatz von Deception-Tools. Damit lassen sich Bedrohungsakteure gezielt täuschen und aufhalten.

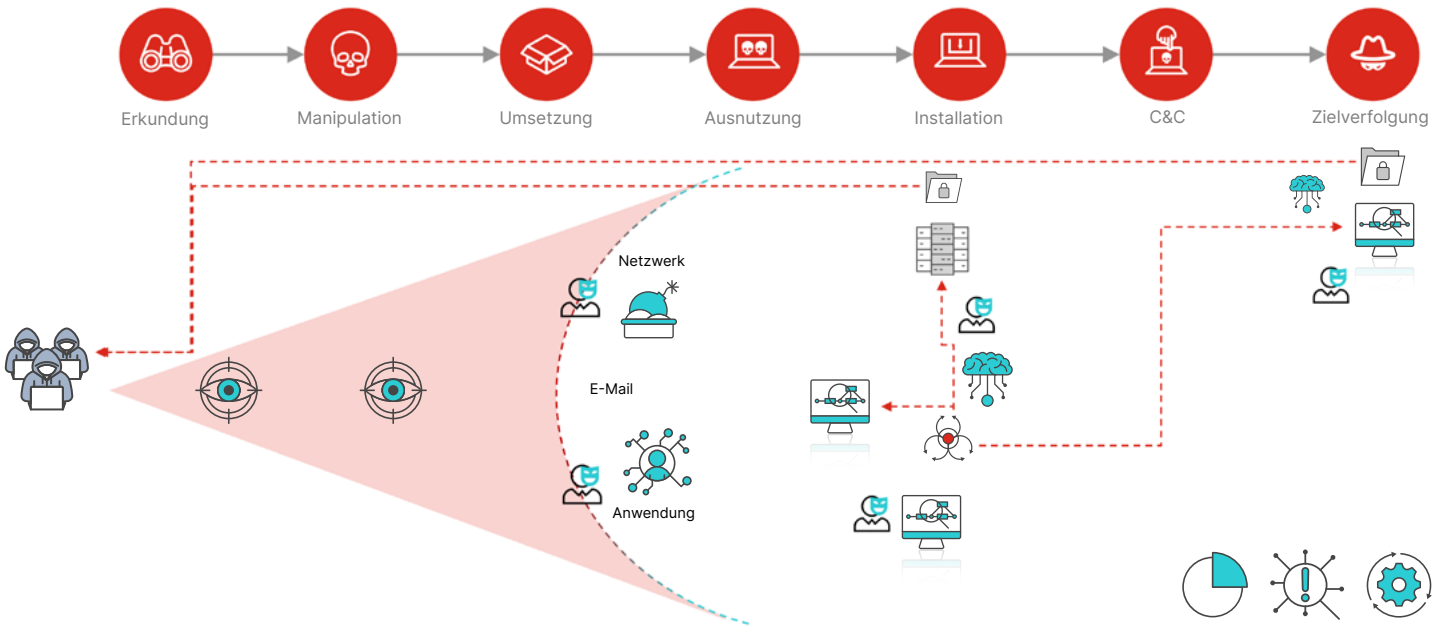

Abbildung 2: Einsatz der Fortinet SecOps-Komponenten in der gesamten Cyber-Kill-Chain

Mit der Fortinet Security-Operations-Lösung profitieren Kunden von einem ROI von bis zu 597 %[9]

Die Investition in Sicherheitsprodukte der Fortinet Security-Operations-Lösung reduziert nachweislich die Verweildauer, das Cyberrisiko und den SecOps-Arbeitsaufwand erheblich. Konkret bedeutet das:

- Vor der Investition in Sensoren zur Früherkennung und präventiven Bedrohungsabwehr brauchten Fortinet-Kunden nach eigenen Angaben durchschnittlich 21 Tage, um Cyberangriffe zu erkennen, sowie weitere 1½ Tage für deren Eindämmung.[10] Mit Produkten wie FortiEDR, FortiNDR und FortiDeceptor können unsere Kunden jetzt die Aktivitäten von Bedrohungsakteuren innerhalb 1 Stunde (in den meisten Fällen sogar in Minuten) erkennen und eindämmen.[11]
- Vor der Implementierung von Fortinet Security-Operations-Lösungskomponenten berichteten Unternehmen, dass die Untersuchung und Behebung von Alarmen 2 bis 3 Tage dauerte.[12] Seit der Implementierung von Komponenten wie FortiAnalyzer, FortiSIEM oder FortiSOAR werden Untersuchungen in 10 bis 15 Minuten abgeschlossen.[13]
- Kunden berichteten zudem, dass jetzt nur 6 Mitarbeiter (in einem Fall sogar nur 3) die Arbeit eines 12-köpfigen Teams erledigen – eine enorme Verbesserung der operativen Produktivität.[14]

Eine ESG-Studie hat ermittelt, welchen Wert diese Verbesserungen finanziell sowie bei der Risikominderung bringen. Laut der Studie beträgt die Wahrscheinlichkeit eines Sicherheitsvorfalls für ein Unternehmen pro Jahr fast 30 % mit jährlichen Kosten von schätzungsweise 1,4 Millionen US-Dollar.[15] Durch eine schnellere Erkennung, Eindämmung, Untersuchung und Behebung nach der Implementierung von Fortinet Security-Operations-Produkten können Unternehmen dagegen nach den ESG-Berechnungen jährlich 1,39 Millionen US-Dollar beim Kampf gegen Sicherheitsvorfälle einsparen.[16]

Durch die höhere Produktivität nach der Implementierung der Lösung sinken außerdem die Security-Personalkosten um durchschnittlich 1,9 Millionen US-Dollar.[17] Nach ESG-Schätzungen amortisiert sich die Fortinet SecOps-Lösung in weniger als 2 Monaten und hat ein ROI-Potenzial von 597 %.[18]

Abbildung 3: Quantitativer Nutzen der Fortinet Security-Operations-Komponenten

Fazit

Mit der Fortinet Security-Operations-Lösung können Unternehmen leistungsstarke, KI-basierte Erkennungsfunktionen in ihrer gesamten digitalen Architektur einführen sowie in bestehende Sicherheitskontrollen integrieren, um Cyberangriffe in verschiedenen Phasen der Cyber-Kill-Chain sehr viel schneller zu stoppen. Die SecOps-Lösung unterstützt zudem Security-Teams bei der Orchestrierung, Automatisierung und Erweiterung zentraler Untersuchungen von Sicherheitsvorfällen und der Remediation, was eine insgesamt schnellere und koordiniertere Reaktion ermöglicht. Ergänzend zur Fortinet-Lösung wird ein Experten-Service angeboten, der die Einsatzbereitschaft der Security Operations bewertet und dem Unternehmen bei der Reaktion auf Sicherheitsvorfälle zur Seite steht. Die umfassende Sicherheitsfunktionalität und Integrationstiefe der Fortinet Security-Operations-Lösung erleichtert Security-Teams die Einführung zeitsparender Prozesse für eine aktive Cyberverteidigung. Statt zeitraubender Erkennungs- und Reaktionsmethoden steht bei der Fortinet-Lösung das Erkennen und Eindämmen von Sicherheitsvorfällen – und damit die Schadensbegrenzung – an erster Stelle, gefolgt von einer genauen Untersuchung und Behebung.

[1] Cost of a Data Breach Report 2023. IBM, 24. Juli 2023.

[2] How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. ISC2, 31. Oktober 2023.

[3] ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions. Enterprise Strategy Group, 1. August 2023.

[4] 2023 Global Ransomware Report. Fortinet, 20. April 2023.

[5] FortiGuard Labs, abgerufen am 21. November 2023.

[6] Cost of a Data Breach Report 2023. IBM, 24. Juli 2023.

[7] 2023 Global Cybersecurity Skills Gap Report, Fortinet, 21. März 2023.

[8] 2023 Global Ransomware Report. Fortinet, 20. April 2023.

[9] ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions. Enterprise Strategy Group, 1. August 2023.

[10-18] Ebd.

FORTINET

www.fortinet.com/de

16. Februar 2024, 14:59 Uhr
2431037-0-0-DE