axians

FORTINET

FortiSOAR - Security Automation

Techupdate 26.08.2025

VINCI ENERGIES

axians

FortiSOAR Agenda

- Was ist FortiSOAR?
- Warum SOAR? Die Herausforderungen der Cybersecurity
- An welcher Stelle im Netz zu positionieren
- Architektur & Hauptkomponenten
- Use Case: Ein Beispiel aus der Praxis
- Vorteile: Was SOAR so wertvoll macht
- Fragen & Antworten

FORTINET®

Was ist FortiSOAR?

- FortiSOAR steht für **Security Orchestration, Automation and Response**.
- Es ist eine Plattform, die es Sicherheitsteams ermöglicht, Routineaufgaben zu **automatisieren**, Sicherheitsprozesse zu **orchestrieren** und auf Vorfälle **schneller zu reagieren**.
- **Ziel:** Die Effizienz des Security Operations Center (SOC) zu steigern, menschliche Fehler zu reduzieren und die Reaktionszeit auf Cyberbedrohungen zu verkürzen.
- FortiSOAR ist Teil des Fortinet Security Fabric, kann aber auch als eigenständige Lösung betrieben werden.

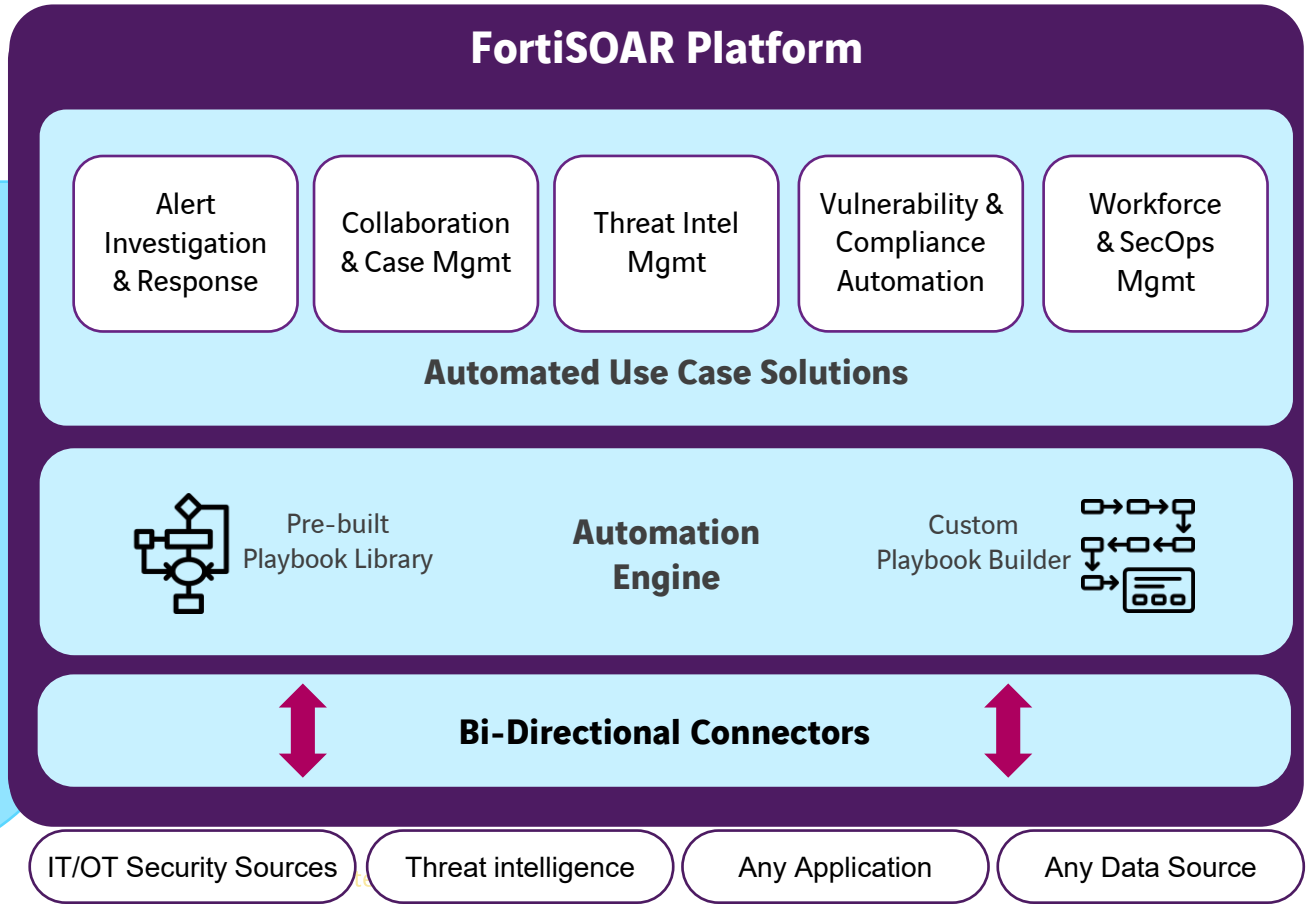
axians

Was ist FortiSOAR?

Connect anything, automate everything

Automation for the modern Enterprise & MSSP SOC

- 600+ system connectors
- 800+ pre-built playbooks
- Simple playbook creation
- Flexibility & customization for any SOC/NOC/IT use case
- Proven performance & scale
- Powered by GenAI and ML
- Leading TCO value



Warum SOAR? Die Herausforderungen im SOC

- **Informationsflut:** SOC-Analysten werden täglich mit Tausenden von Alarmen aus verschiedenen Sicherheitstools (SIEM, EDR, Firewalls) überflutet.
- **Manuelle Arbeit:** Die meisten Triage- und Reaktionsaufgaben sind repetitiv und zeitintensiv.
- **Personalmangel:** Es gibt nicht genug qualifizierte Sicherheitsexperten, um die steigende Anzahl an Bedrohungen zu bewältigen.
- **Schlechte Kommunikation:** Die Zusammenarbeit zwischen den Teams ist oft ineffizient, was zu längeren Reaktionszeiten führt.

An welcher Stelle im Netz zu positionieren

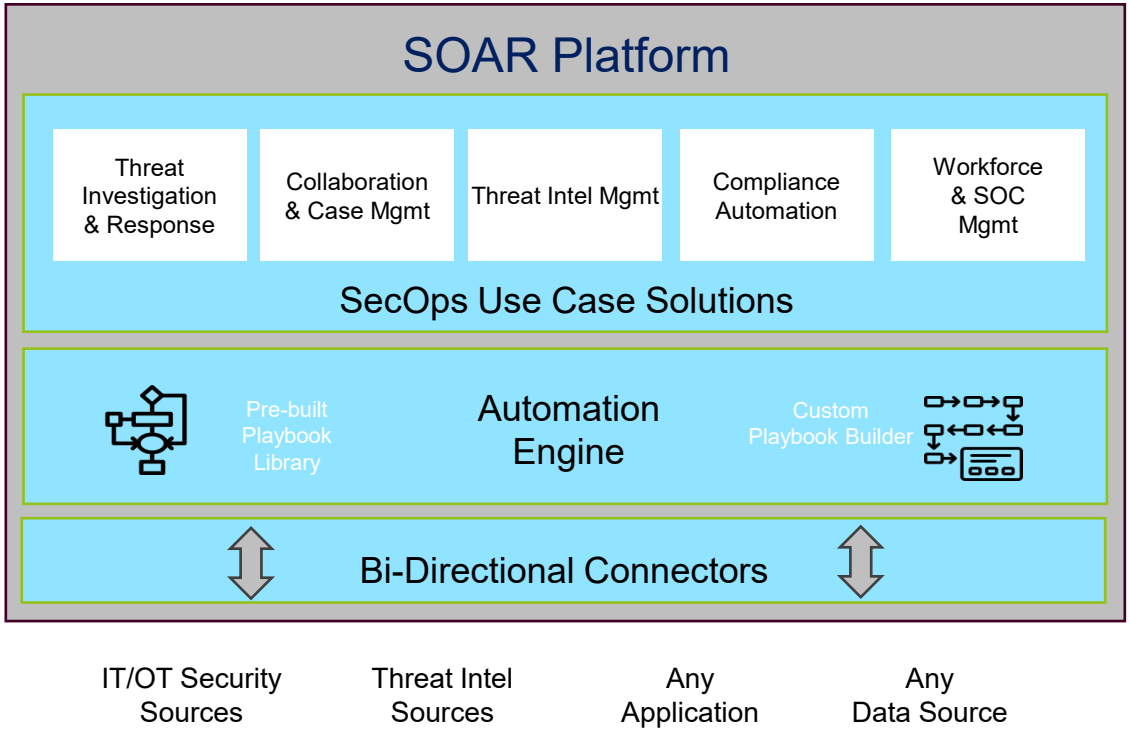
- Das SOAR-System agiert als eine Art **Steuerzentrale** für das gesamte Sicherheits-Ökosystem.
- **Zugriff auf Datenquellen:** Das SOAR muss in der Lage sein, Alarmmeldungen von verschiedenen Systemen zu empfangen. Dazu gehören SIEM, Firewalls, EDR-Lösungen, Vulnerability-Scanner und Threat-Intelligence-Feeds.
- **Kommunikation mit Reaktions-Tools:** Um automatisierte Aktionen auszuführen, muss das SOAR-System in der Lage sein, mit den operativen Sicherheitstools zu kommunizieren
- **Skalierbarkeit und Verfügbarkeit:** Für größere Umgebungen wird das SOAR-System oft in einer hochverfügbaren Konfiguration bereitgestellt. Es sollte so positioniert sein, dass es mit den jeweiligen Agenten oder APIs aller zu steuernden Systeme im Netzwerk kommunizieren kann.

FortiSOAR-Architektur

- **SOAR Engine:** Der Kern der Plattform, der Playbooks ausführt und die Automatisierung steuert.
- **Connectors:** Vorgefertigte Integrationen zu Hunderten von Sicherheitstools und -diensten (FortiGate, SIEMs, Threat Intelligence Feeds etc.).
- **Playbooks:** Automatisierte Arbeitsabläufe, die aus einer Abfolge von Aktionen bestehen. Sie definieren, wie auf bestimmte Ereignisse reagiert werden soll.
- **Incident Management:** Zentrale Konsole zur Verwaltung aller Vorfälle, Alarme und Fälle.
- **Dashboards & Reporting:** Visualisierung von Metriken, Vorfallstatistiken und der Effizienz des SOCs.

FortiSOAR-Architektur

- Verbindet sich mit praktisch jeder App, jedem System oder jeder Datenquelle.

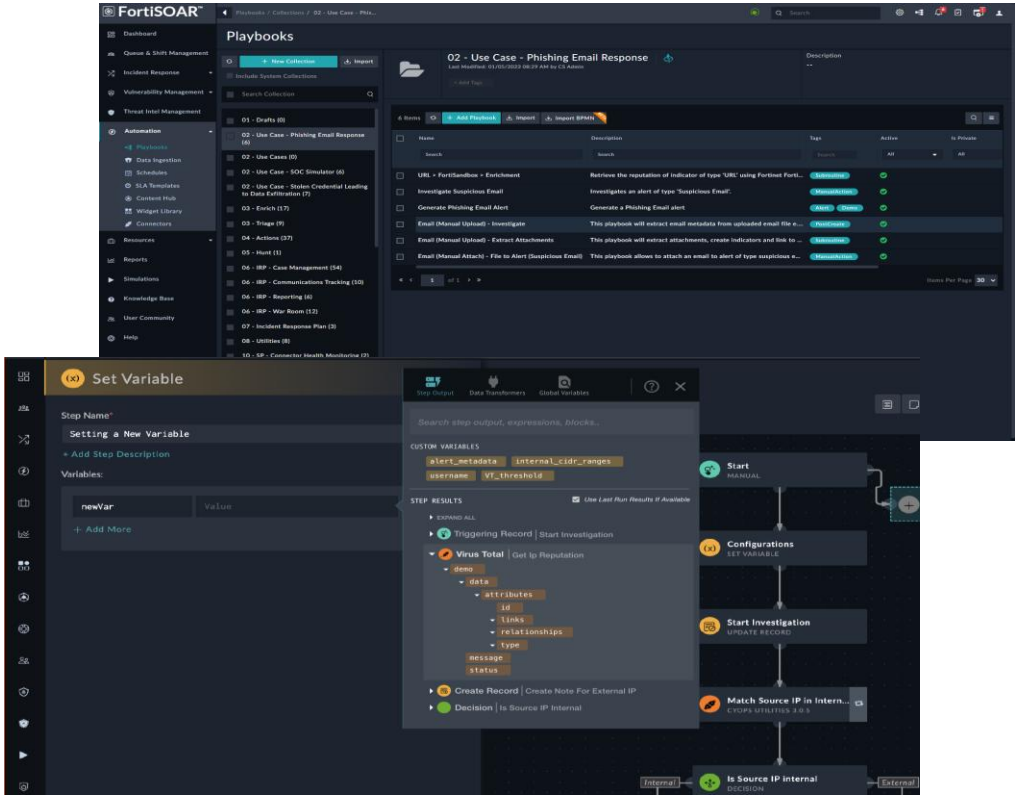


Playbooks: Das Herzstück der Automatisierung

- Playbooks sind visuell gestaltete Workflows, die Sicherheitsanalysten ganz einfach per **Drag-and-Drop** erstellen können.
- Sie definieren die Schritte, die als Reaktion auf einen Vorfall ausgeführt werden sollen.
- **Beispiel-Schritte:**
- Eingang eines Alarms aus dem SIEM.
- Automatisches Abrufen von Informationen über die verdächtige IP-Adresse (Threat Intelligence).
- Überprüfung der IP in internen Systemen.
- Wenn die IP bösartig ist: Automatisches Blockieren in der Firewall.
- Erstellung eines Tickets im Incident-Management-System und Benachrichtigung des Analysten.

Playbooks: Das Herzstück der Automatisierung

- Playbooks und neue Konnektoren sind einfach erstellen.
- Nutzen Sie die No/Low-Code-GUI und Empfehlungen.
- Simulieren und testen Sie vor der Bereitstellung.



axians

Use Case: Phishing-E-Mail-Analyse

- **Problem:** Ein Benutzer meldet eine verdächtige E-Mail. Die Analyse ist manuell und zeitaufwändig.
- **SOAR-Lösung:**
- Ein Playbook wird ausgelöst, sobald eine E-Mail als verdächtig markiert wird.
- Es extrahiert automatisch URLs und Dateianhänge.
- Diese werden an einen Sandbox-Service (z.B. FortiSandbox) zur Analyse gesendet.
- FortiSOAR überprüft die Absender-IP in Threat-Intelligence-Feeds.
- Wenn die E-Mail als bösartig eingestuft wird, werden alle anderen E-Mails mit den gleichen Merkmalen automatisch aus den Postfächern gelöscht.
- Ein Bericht wird erstellt und dem Analysten zur Verfügung gestellt.

Die Hauptvorteile einer SOAR-Installation

- **Erhöhte Effizienz:** Reduziert die manuelle Arbeitslast und lässt Analysten sich auf die komplexesten Bedrohungen konzentrieren.
- **Schnellere Reaktion:** Verkürzt die mittlere Zeit bis zur Erkennung und Reaktion (MTTD/MTTR).
- **Geringere Betriebskosten:** Automatisierung senkt den Personalbedarf und die Kosten für die Incident-Reaktion.
- **Konsistente Prozesse:** Standardisiert die Reaktion auf Vorfälle und stellt sicher, dass keine wichtigen Schritte vergessen werden.
- **Bessere Sichtbarkeit:** Bietet übersichtliche Dashboards und Berichte, um die Leistung des SOC zu messen.

Zusammenfassung

- SOAR-Systeme sind die Antwort auf die Herausforderungen der modernen Cybersecurity.
- Sie transformieren manuelle, reaktive Prozesse in automatisierte, proaktive Workflows.
- Durch die Integration von Tools, die Automatisierung von Aufgaben und die Orchestrierung von Prozessen helfen SOAR-Systeme, Sicherheitsteams zu entlasten und die Cybersicherheit zu stärken.

Fragen & Antworten

- Fragen? 🤔