SOLUTION BRIEF

Fortinet and Arcanna.ai Security Solution

SOC Analyst Decision Emulation Enables High Accuracy and Consistent, Continuous Triage of Security Alerts

Executive Summary

Arcanna.ai is a decision intelligence platform that uses multiple types of AI and user feedback. It can be integrated with Fortinet FortiSOAR and FortiSIEM to assist in decision-making, learn from daily incident resolutions, incorporate knowledge to scale your team's capacity, and lead to a true autonomous decision-making system all without changing the SOC analysts' incident management screen.

The Challenge

Over the past decade, the core challenges facing security operations centers (SOCs) have remained broadly consistent yet have intensified significantly.

- **Shortage of skilled analysts:** The industry needs more highly skilled analysts. These professionals, with their capacity to address diverse technical and non-technical issues, are frequently pulled into various contexts to support business needs. This constant context switch places additional strain on their productivity and focus.
- **Expanding attack surface:** The organization's attack surface grows with each new technology adoption. Lowered barriers to entry for attackers compound this, increasing the volume and sophistication of attacks that analysts must address.
- **Fragmented tooling and information:** Analysts face a complex ecosystem of security tools and information sources when triaging potential threats. Much critical knowledge needs to be more consistent across internal and external databases, leading to inefficiencies and possible gaps in situational awareness.
- **Automation gaps:** SOAR platforms like FortiSOAR have advanced automation for gathering the necessary context. However, critical decisions, whether to escalate, investigate, or dismiss alerts, often require human intervention. This hybrid approach, while essential, can lead to inconsistency, slower response times, and reduced overall productivity. As a result, SOCs are increasingly vulnerable to errors, which can escalate rapidly, increasing the likelihood of significant security incidents or breaches.

Joint Solution

Integrating Arcanna.ai AI-driven decision-making platform with Fortinet FortiSOAR and FortiSIEM enhances cybersecurity teams' efficiency, accuracy, and consistency by automating incident management and streamlining threat response processes. Arcanna.ai machine learning (ML) models augment FortiSOAR robust security orchestration and automation capabilities, allowing security teams to:

Solution Components

- Fortinet FortiSOAR
- Fortinet FortiSIEM
- Arcanna.ai Platform

Solution Benefits

- Improve operational efficiency and response time by emulating human decisions in the SOC
- Enhance automated decision-making by building customized deep-learning models tailored to each organization's unique environment
- Embed feedback capabilities directly into existing FortiSOAR and FortiSIEM workflows for a seamless experience

FORTINET FABRIC-READY

- **Reduce alert fatigue** by automatically filtering and prioritizing security alerts
- **Automate complex decision-making**, enabling faster and more accurate incident responses
- **Scale cybersecurity operations** effectively by emulating the decisions of your best analysts to improve response times and simplify complex threat management processes

This integration empowers organizations with a comprehensive, automated approach to managing evolving cyberthreats, enhancing their security posture and operational efficiency.

Solution Components

Arcanna.ai offers AI-driven solutions for cybersecurity incident management, integrating advanced ML and automation to enhance threat detection and response. Key components include real-time threat analysis, incident prioritization, and decision support systems that reduce alert fatigue and streamline operations. By augmenting human expertise, Arcanna.ai enables organizations to effectively manage complex cyberthreats, improve operational efficiency, and ensure faster, more informed decision-making in cybersecurity.

Fortinet FortiSIEM provides the centralized IT/OT event collection, advanced detection analytics, incident management, and other NOC/SOC functions that today's security teams need. Built on UEBA analytics, a unique CMDB, and GenAI assistance, the intuitive analyst experience supports all aspects of threat investigation, incident response, and compliance validation for organizations of any size.

Fortinet FortiSOAR provides a holistic security orchestration, automation, and response workbench designed for SOC teams to efficiently respond to the ever-increasing influx of alerts, manage repetitive manual processes, and bolster the resource shortage. With broad integrations, rich use-case functions, hundreds of prebuilt workflows, and simple playbook creation, this patented and customizable security operations platform provides automated playbooks, incident triaging, and real-time remediation for enterprises to identify, defend, and counterattack.

Solution Integration

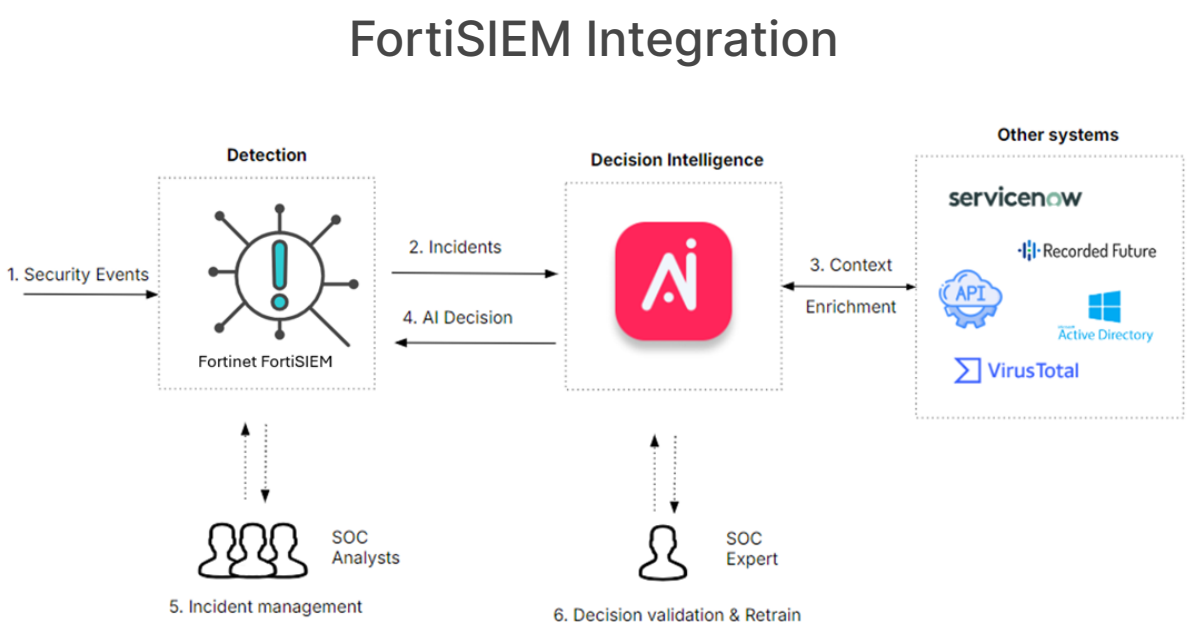

Figure 1: Arcanna.ai and FortiSIEM integration architecture

Architecture and Data Flow

Arcanna.ai integrates directly with FortiSIEM by ingesting incident data generated by the SIEM's monitoring of diverse security events and data sources across the environment. The architecture is designed to leverage FortiSIEM robust data collection and correlation capabilities, feeding this enriched data into Arcanna.ai's decision intelligence platform.

Data ingestion: FortiSIEM gathers and correlates security events from multiple sources, creating incidents and alerts based on predefined rules.

Decision intelligence integration: Arcanna.ai ingests these incidents via a direct API connection, applying AI models to analyze each alert's context, relevance, and priority to make a decision.

Feedback loop: Once incidents are resolved, security analysts can collect and provide feedback to Arcanna.ai. This feedback is then used to retrain and refine the AI models, improving decision-making accuracy over time. This process helps reduce false positives and enhances the system's ability to handle future incidents more effectively.

Output: Arcanna.ai will deliver decisions on all alerts, similar to an L1-L2 security analyst (whether an alert requires further action or can be safely ignored), updating FortiSIEM with these conclusions in real time. This integration reduces manual intervention and accelerates response times.

FortiSOAR Integration

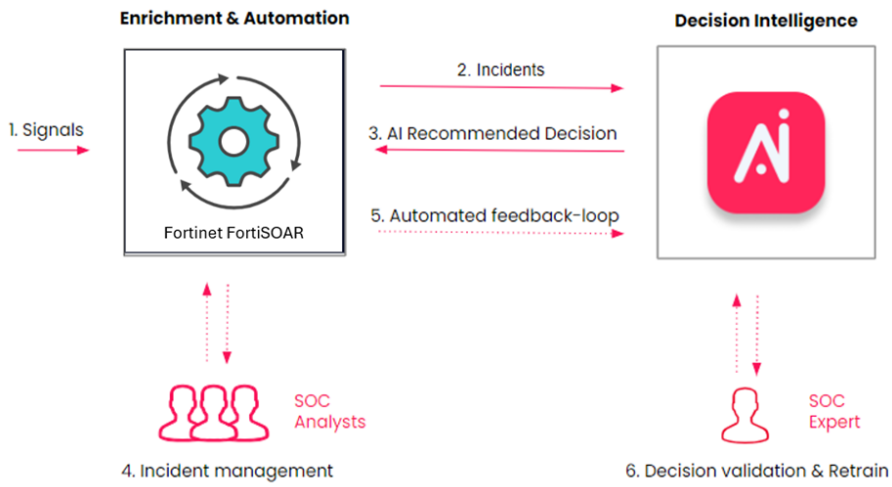

Figure 2: Arcanna.ai and FortiSOAR integration architecture

Architecture and Data Flow

The integration between Arcanna.ai and FortiSOAR enhances automation and decision-making capabilities in orchestrated security operations.

Incident enrichment: FortiSOAR creates and enriches security incidents through automated playbooks, adding valuable context and data before sending it to Arcanna.ai.

AI decision integration: At any point within the SOAR playbook, Arcanna.ai's AI models can augment decision-making by providing recommendations on incidents, such as classifying severity, suggesting remediation actions, or advising on escalation.

Feedback mechanism: FortiSOAR automatically sends the outcome back to Arcanna.ai when the incident is closed, reinforcing the decision models with new data. This ensures that Arcanna.ai continually improves its accuracy and relevance for future incidents.

Playbook optimization: With Arcanna.ai embedded in FortiSOAR automation workflows, its recommendations can trigger actions such as containment, remediation, or escalation, helping to resolve incidents swiftly. These AI-augmented decisions support analysts in responding more efficiently and accurately within the existing playbooks, streamlining workflows while maintaining human oversight.

Joint Use Cases

Use case #1: Intelligent incident decision-making

Arcanna.ai enables the training of bespoke neural networks to make decisions at scale on security incidents by the decision process of the security analysts, whether it is initial triage, an intermediate decision deciding whether to respond, or the final decision for that incident. Integrated with FortiSIEM or FortiSOAR, it quickly identifies critical incidents, reducing the workload on human analysts and ensuring faster incident resolution.

Use case #2: Continuous feedback and learning

Arcanna.ai retrains models based on feedback from resolved incidents, improving its decision-making capabilities. With FortiSOAR, this feedback loop is automated, allowing Arcanna.ai to adapt and stay effective against evolving threats without requiring manual updates.

About Arcanna.ai

Arcanna.ai stands for Automated Root Cause Analysis Neural Network Assisted, reflecting the platform's focus on leveraging AI, specifically neural networks, to automate and improve the identification of the root causes of cybersecurity incidents. This highlights Arcanna.ai's emphasis on combining machine learning with advanced analytics to help security teams efficiently manage and respond to complex cyberthreats.

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

December 5, 2024 10:16 PM / MKTG-336-0-0-EN