SOLUTION BRIEF

Fortinet and ServiceNow® Integrated Security Solution

Integrated NOC-SOC Solution To Automate IT Processes and Security Response

Challenges

Security teams are overwhelmed with millions of alerts from dozens of security products. Manual analysis and containment processes from siloed products take time and leave room for error. Lack of business context makes prioritization difficult. Both security and IT teams are challenged by resource constraints, yet workloads and the rate of cyber threats continue to rise in scope and complexity. As IT increasingly supports complex applications that are spread across systems in multiple locations, from on-premises data centers to the public cloud, the workforce shortage and complexity of these new environments demands a new approach to security.

Integration across security disciplines—not merely products—enables a greater level of visibility, control, and operational management. As the industry faces a cyber talent shortage and the pressure to maintain operational efficiency and security efficacy is critical for digital business, it is critical to bring visibility and control into the security operations center (SOC) with workflow and response automation from the network operations center (NOC).

Fortinet and ServiceNow® have established a technology partnership to address the above needs. The integrated NOC-SOC security solution bridges the gap across operational and security disciplines, delivering broad, integrated, and automahted responses.

Solution Description

Fortinet's integrated NOC-SOC solution combines the latest capabilities of FortiManager, FortiAnalyzer, and FortiSIEM, coalescing the operational context of the NOC, such as appliance status, network performance, and application availability, with the security insights of the SOC, including breach identification, data exfiltration prevention, and compromised hosts discovery. This level of management and automation crosses traditional siloed functions, allowing each team to operate with the benefit of the other's perspective. In this new model, once a threat is identified, the SOC teams have a real-time view of all assets, their current state, and who owns them, allowing them to immediately understand the scope of the threat and automatically orchestrate action to remediate damage. This intersection and overlap in operations and security is paramount for the defensive posture and risk management of today's dynamic business environments.

The solution enables automation of security responses across NOC-SOC organizations, based on predefined triggers (system events, threat alerts, user and device status), ServiceNow® IT Service Management (ITSM) and ServiceNow® Security Operations integration. ServiceNow® Security Operations is also integrated into NOC-SOC-based workflows that span operational silos. Security incidents

Joint Solution Components

- Fortinet FortiGate Next-generation Firewall (NGFW)
- Fortinet FortiManager
- Fortinet FortiAnalyzer
- Fortinet FortiSIEM
- ServiceNow® IT Service Management (ITSM), Security Operation

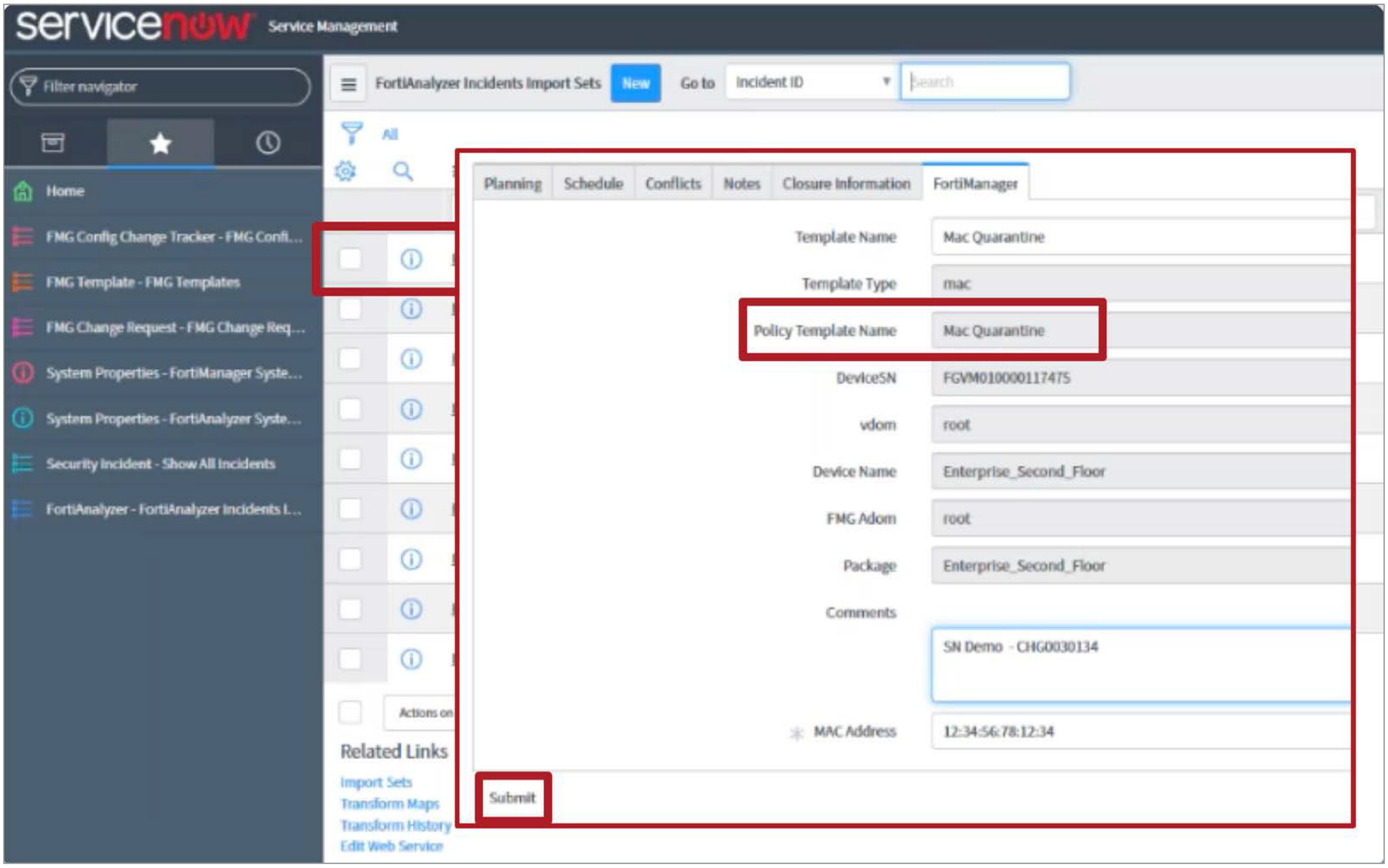
Joint Solution Benefits

- Faster security response through automation of security detection, escalation, security incident response, and remediation
- More efficient and coordinated operations across NOC and SOC teams, through automation of processes and data flows needed for optimal decision-making
- Comprehensive end-to-end security visibility provided via the Fortinet Security Fabric
- Leverage the industry's best validated security protection offered by the Fortinet FortiGate network security platform to protect against sophisticated cyber threats

created in FortiAnalyzer or FortiSIEM, with appropriate evidence and forensics added to the ticket, are automatically passed to ServiceNow® for security incident response. Analysts working from the ServiceNow® platform can determine how to resolve the incident and choose from a catalog of responses. Responses that require changes to device configuration are automatically implemented through FortiManager, thus closing the loop and seamlessly bridging the security and operations teams.

Representative Use Case

The solution delivers automated cybersecurity threat detection, security incident response, escalation, and remediation. Fortinet's award-winning FortiGate enterprise firewall platform provides end-to-end security across the entire network. Security incidents created in FortiAnalyzer or FortiSIEM, based on Fortinet's advanced threat detection capabilities, are automatically propagated to the ServiceNow® platform. SOC security analysts can review the ticket and determine needed actions. Workflow management features enable the incident response supervisor to approve change requests, which could be an optional process check, depending on the security policies and procedures of the organization. The change request is then automatically implemented in the underlying deployment. Example automated actions could be to instruct FortiManager to effect changes in firewall security policies to block traffic on the firewall, or to quarantine an endpoint (as illustrated in the user interface snapshot below), effectively stopping malware, and preventing cybersecurity threats.


servicenow
Service Management
Filter navigator
Home
FMG Config Change Tracker - FMG Confi...
FMG Template - FMG Templates
FMG Change Request - FMG Change Req...
System Properties - FortiManager Syste...
System Properties - FortiAnalyzer Syste...
Security Incident - Show All Incidents
FortiAnalyzer - FortiAnalyzer Incidents I...
FortiAnalyzer Incidents Import Sets
New
Go to
Incident ID
Search
All
Planning
Schedule
Conflicts
Notes
Closure Information
FortiManager
Actions on
Related Links
Import Sets
Transform Maps
Transform History
Edit Web Service
Submit

Template Name	Mac Quarantine
Template Type	mac
Policy Template Name	Mac Quarantine
DeviceSN	FGVM010000117475
vdom	root
Device Name	Enterprise_Second_Floor
FMG Adom	root
Package	Enterprise_Second_Floor
Comments	SN Demo - CHG0030134
* MAC Address	12:34:56:78:12:34

Figure 1: ServiceNow integration.

Summary

As customers introduce cloud, virtualization, endpoint, and other technologies that expand their attack surface, operations and security processes must be more closely integrated to ensure effective security response. Fortinet's integration with ServiceNow® enables joint customers to benefit from automated detection, security incident response, escalation, and remediation of cybersecurity issues. Through automation, the solution significantly compresses the time to identify and contain incidents and vulnerabilities, ultimately reducing an organization's overall risk.

About ServiceNow®

ServiceNow® is changing the way people work. We help the modern enterprise operate at lightspeed and be more scalable than ever before. Customers use our platform to define, structure and automate the flow of work, removing dependencies on email, spreadsheets and other manual processes to transform the delivery of service to the enterprise. With ServiceNow® Security Operations, customers can bring incident data from their security tools into a structured enterprise security response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

Learn more at https://www.servicenow.com.

March 31, 2021 12:02 AM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\March\Branding Refresh\913517 - Update Connecting SBs\sb-FA-fortinet-and-servicenow-3302021\sb-FA-fortinet-and-servicenow-3302021

209472-C-0-EN