SOLUTION BRIEF

Fortinet and DFLabs Security Solution

Integrated and Automated Security Solution To Improve Security Operations Processes and Aid Security Analysts To Proactively Address Emerging Threats

Executive Summary

DFLabs and Fortinet have partnered to deliver an integrated security solution that provides advanced detection and automated response capabilities, and enables customers to better triage events and prioritize and respond to threats that are more critical to their organization. These capabilities enable customers to improve their security operations processes and aid security analysts in proactively addressing emerging threats in the rapidly evolving cybersecurity landscape.

Nowadays, cyber threats are becoming more difficult to trace, which leaves analysts with the difficult task of investigating and containing each threat as it arrives in real time. Security operations require the merging of intelligence, both from in-house staff and technological solutions. Cyberattacks are becoming more unpredictable than ever, and that exact unpredictability led to the following challenges that prompted the birth of a whole new cybersecurity technology:

- An increasing number of alerts
- False positives and false negatives
- Overwhelming workload for SecOps and SOCs
- Sophisticated attacks with no recognizable patterns

Sophisticated attack techniques must be met with sophisticated solutions. In order for organizations to beat their attackers at their own game, they must be able to bring the fight to them at all layers of an attack surface. With traditional manual intervention no longer being an effective means of response, security teams must look beyond their internal boundaries for assistance.

Joint Solution Benefits

- Automate mundane tasks in your security operations processes
- Reduce false positives and focus on real threats
- Respond to attacks in less time
- Centralize threat intelligence
- Easily orchestrate your security tools leveraging the Open Integration Framework
- Leverage the industry-leading FortiGate next-generation firewall and Fortinet Security Fabric for unparalleled network security protection

FORTINET Fabric-Ready

The integration between DFLabs IncMan SOAR and the Fortinet security suite provides advanced detection mechanisms needed at each layer and rapid response capabilities through automated actions to orchestrate complete and automatic containment on behalf of the security staff. The assistance provided by this integration will level the playing field for security professionals and give them the tools necessary to combat their adversaries.

Joint Solution

DFLabs and Fortinet have partnered to deliver an industry-leading security solution to address the above challenges. The integration of DFLabs IncMan SOAR and Fortinet products delivers validated threat intelligence to enable customers to triage events and prioritize and respond to threats that are more critical to their organization.

Joint Solution Components

The DFLabs IncMan SOAR (security orchestration, automation, and response) platform helps enterprises and managed security service providers (MSSPs) to improve their security operations processes. IncMan's Triage capability enables reduction of the number of false positives and handles suspicious events that require deeper analysis. With DFLabs IncMan SOAR and Fortinet solutions, an analyst can orchestrate and efficiently implement a more effective security solution that can keep up with the pace of emerging threats. Thanks to application programming interface (API) integration, you can easily leverage Fortinet solutions in your processes to enrich, validate, and block threats.

FortiAnalyzer

FortiAnalyzer provides deep insights into advanced threats through single-pane orchestration, automation, and response for an organization's entire attack surface, to reduce risks and improve their overall security. Integrated with the Fortinet Security Fabric, FortiAnalyzer simplifies the complexity of analyzing and monitoring new and emerging technologies that have expanded the attack surface, and delivers end-to-end visibility, helping identify and eliminate threats.

FortiGate NGFW

FortiGate next-generation firewalls (NGFWs) enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. FortiGate NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

FortiMail

FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyber threats to help secure the dynamic enterprise attack surface, prevent the loss of sensitive data, and help maintain compliance with regulations. High-performance physical and virtual appliances deploy on-site or in the public cloud to serve any size organization—from small businesses to carriers, service providers, and large enterprises.

FortiSIEM

FortiSIEM enables unified data collection and analytics from diverse information sources including logs, performance metrics, Simple Network Management Protocol (SNMP) traps, security alerts, and configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos—from security operations centers (SOCs) and network operations centers (NOCs)—and brings that data together for a more holistic view of the security and availability of the business. Every piece of information is converted into an event that is first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules, dashboards, and ad hoc queries.

FortiWeb

FortiWeb is a web application firewall (WAF) that protects hosted web applications and APIs from attacks that target known and unknown exploits. Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats.

Joint Solution Integration

An alert is received indicating that a user may have clicked on a malicious link in an email. Once received, IncMan automatically executes the suspicious email activity runbook, which begins to gather email domain information from FortiMail and reputation data from two separate reputation services for evaluation.

The reputation information is then fed into a conditional action that looks to see if the observed domain has a reported reputation score of 50 or greater from either service. If the domain is found to not have a malicious reputation score, the R^3 Rapid Response Runbook will exit without any further action taken. However, if the reputation score is found to be malicious from one or both of the reputation services, the suspicious email activity runbook will proceed to take containment actions and gather more evidence to determine if the incident needs to be escalated to a high-priority incident.

The R^3 Rapid Response Runbook issues a command to the FortiGate NGFW to create a new blocked address group and to create an in-line protection policy in the FortiWeb console. Simultaneously, queries are sent to FortiAnalyzer to gather additional events involving the affected host and for current network traffic originating from the host, and to FortiSIEM to gather any additional hosts who may have communicated with the malicious domain within the last 30 days. Once data is pulled from both FortiAnalyzer and FortiSIEM, the results are evaluated against another conditional action to see if any additional events were observed.

If the FortiAnalyzer has observed that additional suspicious activity has originated from the affected host, the additional event IDs are added to IncMan as incident artifacts and a new incident is created in the FortiAnalyzer for the responsible team to review. If there were no additional events, a ticket is opened in the organization's ticketing system to have the affected host's network traffic reviewed and the host's behavior monitored.

If additional activity from FortiSIEM has been observed for additional hosts and the malicious domain, the additional hosts are added to IncMan as incident artifacts, the incident is upgraded to high priority, and a new ticket is created in the organization's ticketing system for additional follow-up from the responsible team.

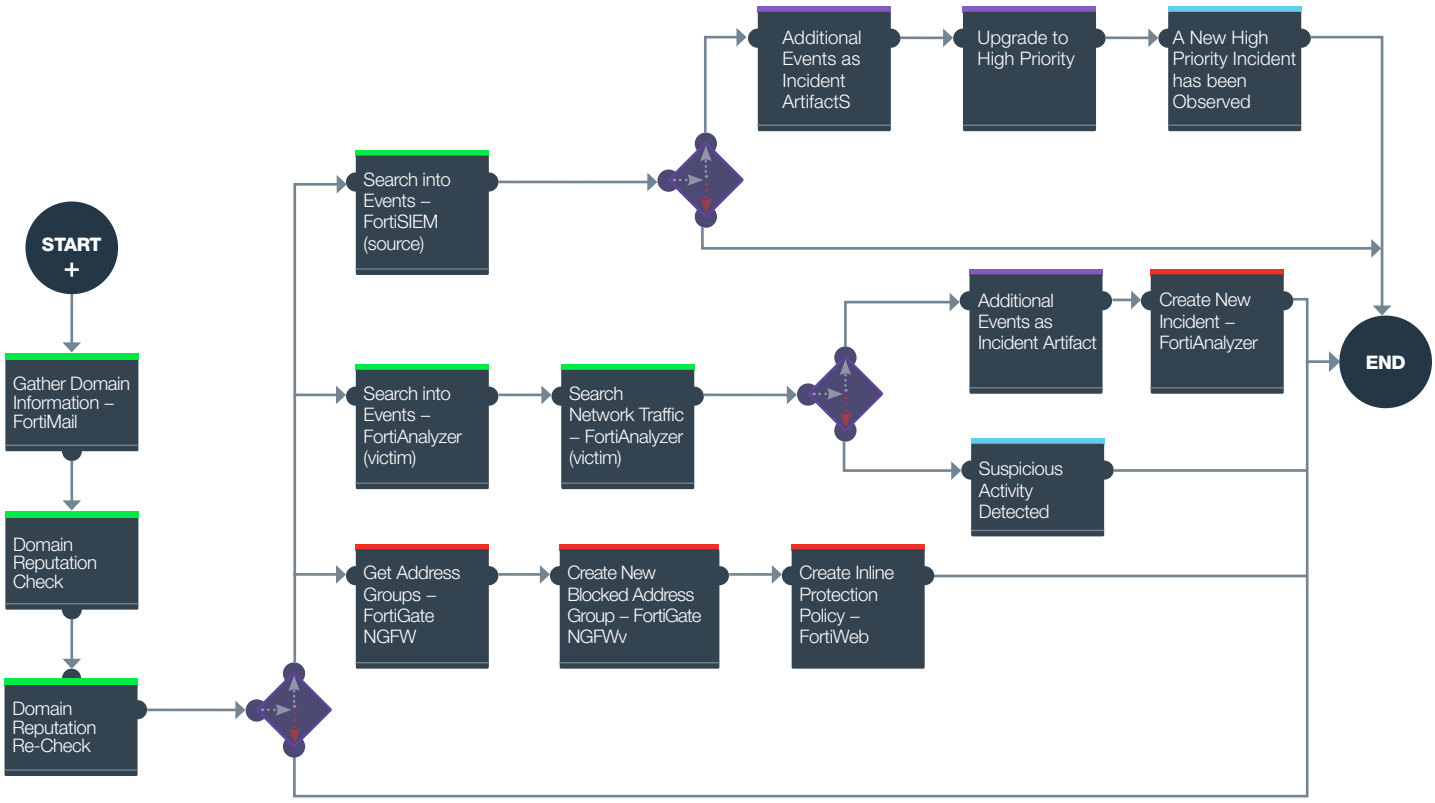

Figure 1: Processing flow in the joint solution.

Joint Use Cases

Below are representative use cases and example actions that can be orchestrated and progressively automated, thanks to IncMan SOAR and the solution integration with Fortinet.

Use case #1 – Enrichment and containment leveraging FortiGate NGFW actions:

Enrichment

- Get Address Groups
- Get Addresses
- Get Firewall Service
- Get Policy
- Get Service Groups

Containment

- Create Address Group
- Create Firewall Service
- Create Policy
- Update Address Group
- Update Policy

Use case #2 – Enrichment leveraging FortiSIEM actions:

Enrichment

- Get Device Information
- Get Devices
- Search Into Events

Use case #3 – Enrichment and notification leveraging FortiAnalyzer actions:

Enrichment

- Get Alert Event Logs
- Get Alert Events
- List Incidents
- Search Into Events
- Search Network Traffic

Notification

- Create Incident
- Update Incident

Use case #4 – Enrichment and containment leveraging FortiWeb actions:

Enrichment

- Get HTTP Service List
- Get In-line Protection Profile
- Get IP List Policy Member
- Get IP List
- Get IP Reputation Exception
- Get Offline Protection Profile
- Get Server Policy
- Get Server Pool
- Get Signature Policy
- Get Trigger Policy
- Get URL Access Policy
- Get URL Access Rule
- Get Virtual Server

Containment

- Create In-line Protection Profile
- Create IP List Policy Member
- Create IP List
- Create IP Reputation Exception
- Create Offline Protection Profile
- Create Server Policy
- Create URL Access Policy
- Create URL Access Rule

Use case #5 – Enrichment and containment leveraging FortiMail actions:

Enrichment

- Get Access Rules
- Get Domain Information
- Get IP Policies
- Get Recipient Policies

Containment

- Create Access Rule
- Create Inbound Recipient Policy
- Create IP Policy
- Create Outbound Recipient Policy

About DFLabs

DF Labs is a pioneer in security orchestration, automation and response (SOAR) technology. The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121. Its flagship product, IncMan SOAR, has been adopted by Fortune 500 and Global 2000 organizations worldwide and awarded three Patents in the USA. DFLabs has operations in EMEA, North America and APAC. IncMan SOAR platform is an award-winning SOAR platform and DFLabs is honored to be acknowledged by a number of leading security award programs.
To learn more, visit https://www.dflabs.com.

September 25, 2020 8:03 AM

D:\Fortinet\Solution Brief\Grey Solution Brief\DF Labs\sb-FA-fortinet-and-dflabs-security-solution-9252020

123456-0-0-EN