SOLUTION BRIEF

Fortinet and ThreatConnect Security Solution

Broad, Integrated, and Automated Solution for Intelligence-driven Security Operations

Executive Summary

Security leaders in organizations have an uphill struggle. The volume and velocity of threats are overwhelming their understaffed security teams, with the number of security events generated by a growing multitude of devices, applications, and users far exceeding what they can track and manage. To keep up, security leaders are turning to SIEM and threat intelligence solutions. Data aggregation, correlation, and analysis enable security teams to reduce the amount of time required to identify and respond to potentially suspicious behavior.

Challenges

As the attack surface expands and the threat landscape accelerates and becomes more complex, lean security teams are no longer able to keep up with the deluge of alerts and other information generated by their security devices. When security teams don't collaborate and tools don't communicate, critical gaps can emerge. Today's adversaries are smart and know how to exploit gaps in security practices.

To address these challenges, security leaders look to security information and event management (SIEM) solutions to correlate data and perform automated analysis. Security leaders are challenged in terms of time and resources, so the SIEM they choose must be easy to implement and highly accurate while offering a low total cost of ownership (TCO) by automating time-consuming, manual workflows. The SIEM must also enable business-driven prioritization, extending monitoring beyond individual devices to the business services they power.

Joint Soluton

Fortinet and ThreatConnect have partnered to deliver an industry-leading security solution to address these challenges. The ThreatConnect Platform delivers validated threat intelligence to FortiSIEM, enabling customers to triage events and prioritize, and respond to threats that are more critical to their organization.

Solution Components

- Fortinet's FortiSIEM
- ThreatConnect's Threat Intelligence Solution

Joint Solution Benefits

- Validated alerting with threat data from ThreatConnect to FortiSIEM
- Triage events with context to quickly spot abnormal trends and patterns and act on them more quickly and efficiently
- Real-time analysis and indicator correlation
- Easy reporting of false positives from FortiSIEM to ThreatConnect

FORTINET Fabric-Ready

Fortinet FortiSIEM

FortiSIEM, the Fortinet Multivendor Security Incident and Event Management solution, brings visibility, correlation, automated response, and remediation in a single, scalable solution. Using a business services view, the complexity of managing network and security operations is reduced, freeing resources and improving breach detection. Worldwide, 80% of breaches go undetected because of skills shortage and event information "noise." FortiSIEM provides cross-correlation and applies machine learning and UEBA to improve response, to stop breaches before they occur.

ThreatConnect Platform

With ThreatConnect's intelligence-driven security operations platform, teams can leverage threat intelligence, automation, and orchestration within a single platform. Automation or orchestration informed by threat intelligence makes your pre-existing technology investments and your entire security team more efficient and more effective. ThreatConnect enables you to gain visibility into threats and understand their relevance to your organization, as well as increase efficiency with automation, task management, and orchestration.

The ThreatConnect and FortiSIEM joint solution enables organizations to aggregate their internal logs and combine them with validated threat intelligence to build processes to identify the most relevant threats, easily spot abnormal trends and patterns, proactively protect their network, and quickly respond to incidents in a measurable way.

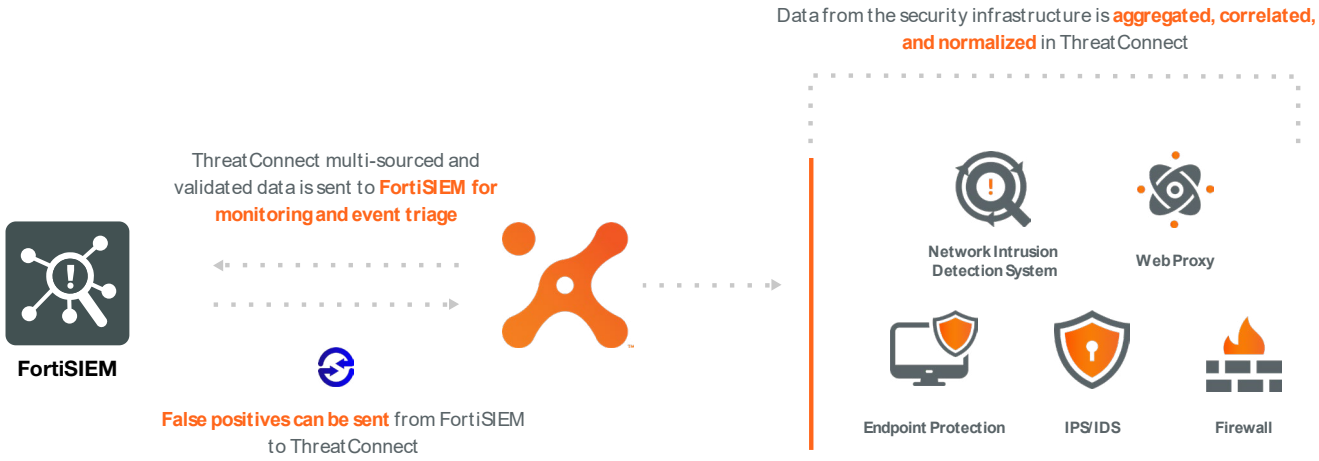

Figure 1: Fortinet and ThreatConnect joint solution.

Use Case 1

Create an intelligence-led IR process

Given the fragmentation and silos prevalent in today's organizations, measuring the ROI in threat data hasn't always been apparent or accessible. Organizations seek to correlate log data across multiple devices to effectively analyze traffic patterns across its network to identify anomalies and security vulnerabilities.

With ThreatConnect, users have the ability to leverage any number of metrics gathered by a global community of intelligence experts, including our own research teams, to gain a broad understanding of the evolving threat landscape and receive experienced guidance on when and how to act based on what's hitting your environment. Through the integration with FortiSIEM, users have unprecedented visibility into where the threat is coming from and can track the entire incident from beginning to end—through reporting, blocking, and mitigation.

Use Case 2

Further analysis of logs, events, and data for better, more informed decision-making

ThreatConnect allows IR teams to look beyond their own network for clues and connections that may suggest relationships between the threat that's attacking the organization and where else it may exist and uncover new intel that may be relevant. Using this acquired knowledge, security teams are transformed from a reactive to proactive defensive force.

With this bidirectional integration, indicators from ThreatConnect are automatically sent to FortiSIEM for alerting, and telemetry and specific events from FortiSIEM can be sent back to ThreatConnect for correlation, analysis, and prioritization. The cycle can then start again as ThreatConnect uses this data to refine and update what is then sent to FortiSIEM for alerting.

When faced with a threat, security professionals can leverage this integration to immediately connect critical dots and make data-driven decisions.

About ThreatConnect

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response, and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit www.ThreatConnect.com.

FORTINET

www.fortinet.com

June 11, 2020 3:53 AM

697774-0-0-EN

D:\Fortinet\Solution Briefs\grey solution briefs\ThreatConnect\sb-fortinet-and-threatconnect-security-solution-V2-6112020-350AM