SOLUTION BRIEF

Fortinet and IntSights Security Solution

Integrated Security for Intelligence-driven Security Operations

Executive Summary

The IntSights and Fortinet security solution enables customers to triage, prioritize, and respond to critical threats that pose the greatest risk to the enterprise. The solution gives security operations center (SOC) teams the information and tools they need to act quickly and protect the business from rapidly moving cyber threats.

Challenges

A fundamental challenge facing every SOC team is how to respond effectively to massive numbers of security events and alerts. Many organizations report receiving over 1 million alerts per day. Security teams of all sizes ignore real threats while spending precious time on false positives. To keep up, security leaders are turning to integrated threat intelligence and security information and event management (SIEM) solutions. Data aggregation, correlation, and analysis enable security teams to reduce the amount of time required to identify and respond to threats targeting the organization.

Joint Solution

IntSights and Fortinet have partnered to deliver an industry-leading security solution to address the above challenges. The integration of the IntSights External Threat Protection Suite and FortiSIEM and FortiManager, key components of the Fortinet Security Fabric, enables mutual customers to triage, prioritize, and respond to critical threats that pose the greatest risk to the enterprise. The combination of externally sourced indicators of compromise (IOCs) with internally detected events gives SOC teams the information and tools they need to act quickly and protect the business.

Joint Solution Benefits

- Identify and focus on high-priority tailored alerts
- Triage threats based on rich contextual threat intelligence
- Respond faster and more effectively to targeted threats
- Automatically ingest enriched IOCs from IntSights into Fortinet devices
- Trigger remediation across the existing security infrastructure
- Gain unparalleled network security protection with the Fortinet Security Fabric

FORTINET Fabric-Ready

Joint Solution Components

The IntSights Threat Intelligence Platform

The IntSights TIP centralizes and operationalizes threat intelligence. IOCs from numerous public and private threat feeds and sources are aggregated and visible via a single dashboard for analysis and collaboration. Relevant IOCs are enriched with tailored intelligence based on your digital assets and ranked based on severity, enabling you to investigate, prioritize, and accelerate remediation efforts. Threat intelligence is automatically pushed to/pulled from existing systems, like FortiSIEM and FortiManager, in your security stack for continuous monitoring and proactive threat blocking.

Fortinet FortiManager

FortiManager provides representational state transfer application programming interfaces (REST APIs), scripts, connectors, and automation stitches.

Fortinet 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 takes the analytics traditionally monitored in separate silos—security operations center (SOC) and network operations center (NOC)—and brings that data together for a comprehensive view of the security and availability of the business.

Joint Solution Integration

IntSights and Fortinet mutual customers can configure on-premises devices to pull (via FortiSIEM) or push (via FortiManager) IOCs from IntSights once the devices have been integrated into the ETP Suite using the virtual appliance. Once set up, the devices will appear in the On-Premises tab in the IntSights Automation > Integrations dashboard. Once devices are syncing with the IntSights virtual appliance, they are ready to receive or pull IOCs from the IntSights TIP. Customers can create a bundle of IOCs from specific feeds and choose to monitor and/or block specific types of IOCS (IP addresses, URLs, and/or domains). IOCs based on customer-defined rules are then automatically sent to Fortinet device(s).

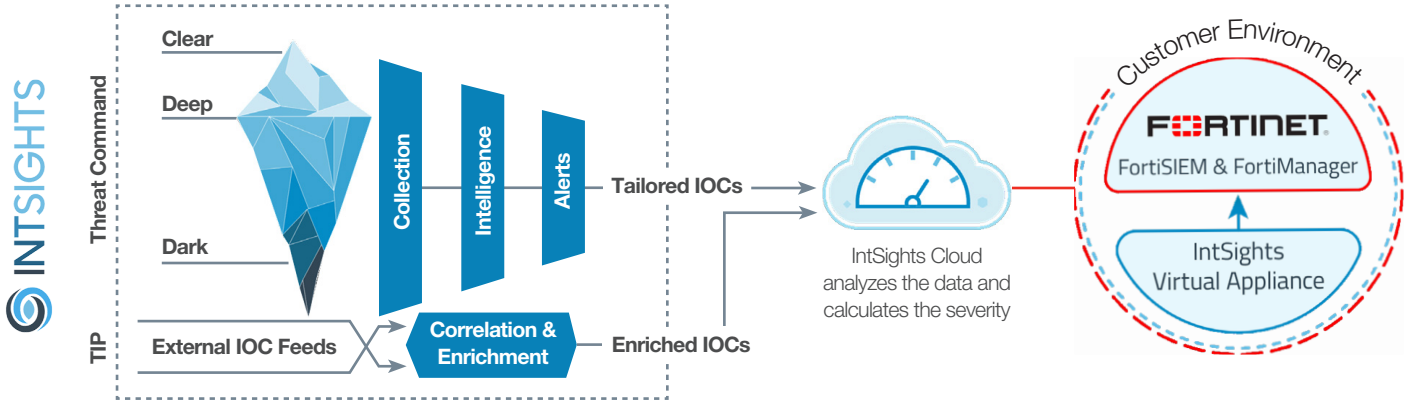

Figure 1: Ingesting enriched IOCs from IntSights into Fortinet solutions.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

September28,202011:54AM
787696-0-0-EN
C:\Users\cyan\Documents\AEM\09-28-2020\sb-fortinet-and-intsights-security-solutions\sb-fortinet-and-intsights-security-solutions\sb-fortinet-and-intsights-security-solutions