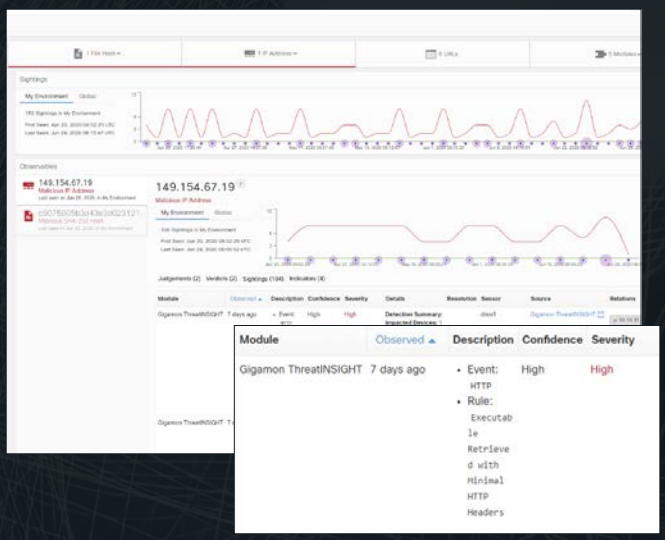
Cisco SecureX and Gigamon ThreatINSIGHT

Partnering to Provide Simple, Rapid and Informed Network Detection and Response

Identifying active threats and resolving them quickly without incident continues to challenge security teams. Cisco SecureX and Gigamon ThreatINSIGHT™ work together accelerate threat detection and response. The SecureX integrated security platform automates and aggregates threat intelligence and data across your security infrastructure into one unified view. ThreatINSIGHT applies machine learning and behavioral-based network threat detection to discover hidden and emerging threats.



KEY JOINT SOLUTION CAPABILITIES

+ **Enhanced detections**
  Augment Cisco/Talos detections with ThreatINSIGHT's high-fidelity network traffic analysis engines to uncover tactics and malicious activity across the entire MITRE ATT&CK framework

+ **Dynamic threat hunting**
  Pivot to ThreatINSIGHT with SecureX platform Observables to use purpose-built threat hunting workflows that automatically populate contextual evidence and enable rapid searches for tactics and behaviors

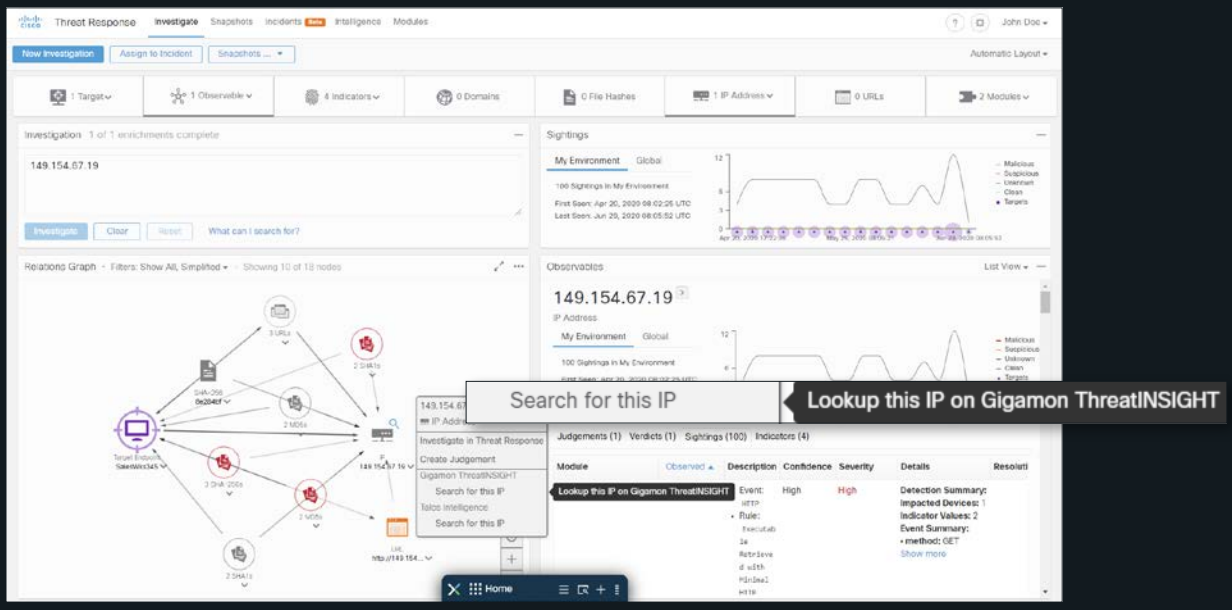
+ **Investigative root-cause and forensic sequencing**
  From any sighting identified within SecureX platform, investigate up to 30 days of related activity from the ThreatINSIGHT solution's network metadata to fully understand the origination of an attack, lateral spread, targets and sequence of events — even if those events weren't known at the time of occurrence

+ **Simple, rapid, wide-ranging responses**
  The SecureX platform enables one-click mitigation of attacks for all threats identified by ThreatINSIGHT

KEY JOINT SOLUTION BENEFITS

- **Identify** hidden and emerging threats rapidly within your network with advanced machine learning and behavioral analysis techniques
- **Discover** targeted threats by providing threat hunters with comprehensive visibility, near packet-level detail and contextually rich workflows
- **Optimize** incident response times with comprehensive investigations that enable informed response options
- **Mitigate** threats completely with informed, rapid one-click mitigation actions across your entire Cisco family of security products (for example, Amp for Endpoints, Umbrella, Cisco Firewalls, Cisco Email Security and Cisco Web Security)

Simple, Rapid and Informed Network Detection and Response



SecureX connects the breadth of Cisco's integrated security portfolio and your entire security infrastructure for a consistent experience that unifies visibility, enables automation and strengthens your security across network, endpoints, cloud and applications.

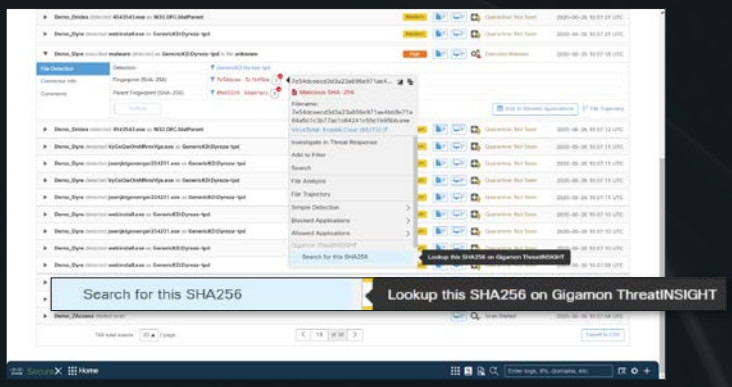
Gigamon ThreatINSIGHT offers security experts unequaled visibility across their entire attack surface, accelerated, high-fidelity threat detection using machine-learning and behavioral-analysis techniques and rapid, informed response through powerful threat hunting and complete investigation and incident management workflows.

Integrated results include simplified security, with interoperability across your existing solutions with the addition of a cloud-native network detection and response solution that delivers faster threat resolution and reduction of risk across your entire attack surface.

The Solution

The combined SecureX/ThreatINSIGHT solution leverages a fully implemented and tested integration to ensure that threat analysts and incident responders spend time resolving threats, not maintaining tools or implementing APIs. The integration provides analysts what they need to be more effective in one unified interface with seamless integration.

cisco Compatible



Pivot from SecureX directly into ThreatINSIGHT with any SecureX Observable or Indicator to hunt for related activity across your entire network for up to the previous 30 days

UNEQUALLED VISIBILITY

ThreatINSIGHT provides comprehensive visibility across your attack surface (N/S/E/W + AWS/Azure/Cloud + Decrypted Traffic*) with indefinite retention of detection-related enriched network metadata (near packet-level context) and up to 30 days retention of all other enriched network metadata to enable threat hunting and complete incident investigation.

The SecureX platform provides visibility to findings and alerts across all your integrated Cisco Security products, including ThreatINSIGHT.

*When coupled with Gigamon SSL Decryption (an optional component of the flagship Gigamon GigaVUE® network packet broker).

HIGH-FIDELITY DETECTION

Augment Cisco/Talos detections with ThreatINSIGHT's leading threat intelligence, machine learning and behavioral analysis technologies applied across your entire network to provide high-fidelity, accelerated threat detection with automatic risk scoring across the entire MITRE ATT&CK framework: Initial access, execution, persistence, privilege escalation defense evasion, credential access, discovery, lateral movement, collection command and control, exfiltration and impact.

RAPID, INFORMED RESPONSE

Built on up to 30 days of enriched network metadata, ThreatINSIGHT provides a fast omnisearch capability to power threat hunting and complete investigation and incident management workflows. Security analysts and incident responders capture robust case evidence enabling informed, complete response decisions.

Fully integrated, security teams can then carry out comprehensive one-click mitigation efforts to effectively respond to threats rapidly.

Conclusion

Cisco SecureX and Gigamon ThreatINSIGHT have partnered to simplify security, bring unequaled visibility, high-fidelity behavioral-based detection and rapid, informed wide-ranging response options to security analysts and incident responders. The fully integrated solutions enable enhanced detections, dynamic threat hunting, full threat investigations and one-click mitigations (for example, Amp for Endpoints, Umbrella, Cisco Firewalls, Cisco Email Security, Cisco Web Security and Threat Grid).

For more information on Gigamon ThreatINSIGHT and Cisco SecureX, please visit:

GIGAMON.COM/THREATINSIGHT | CS.CO/GIGAMON | CISCO.COM/C/EN/US/PRODUCTS/SECURITY/SECUREX

WHY GIGAMON?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network. The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations around the world.

Take ThreatINSIGHT for a test drive, visit gigamon.com/demo.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

08.20_01