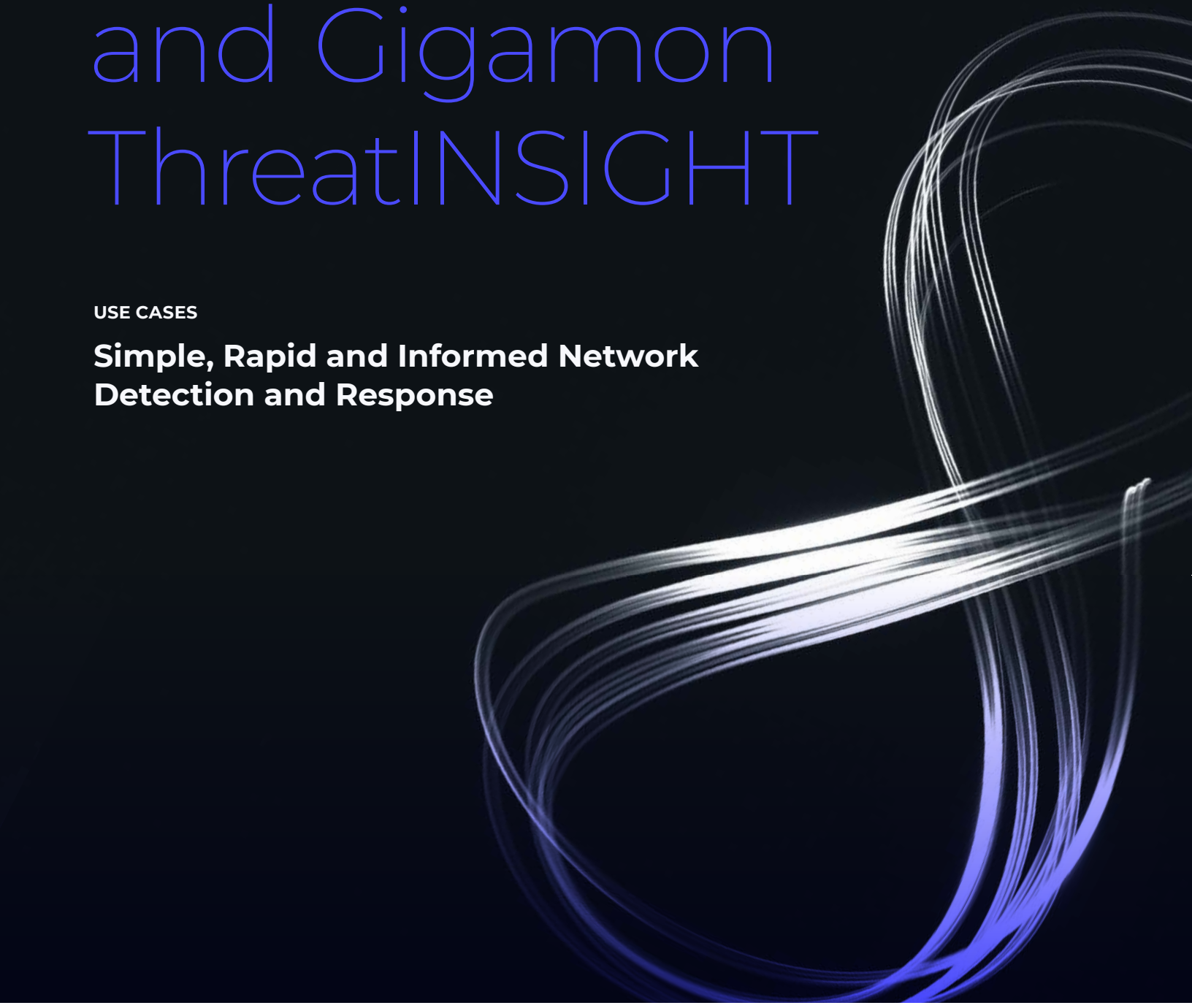
Cisco SecureX and Gigamon ThreatINSIGHT



USE CASES

Simple, Rapid and Informed Network Detection and Response

Gigamon®

For security analysts and incident responders who want to identify active threats and resolve them without incident will want to look at Cisco SecureX and Gigamon ThreatINSIGHT™. This innovative combination simplifies security and delivers unequaled visibility, high-fidelity behavioral-based detection and rapid, informed, wide-ranging response options. The fully integrated solutions enable enhanced detections, dynamic threat hunting, full threat investigations and one-click mitigations.

KEY FEATURES

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 ThreatINSIGHT'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 BENEFITS

Identify hidden and emerging threats rapidly within your network with advanced machine learning and behavioral analysis techniques

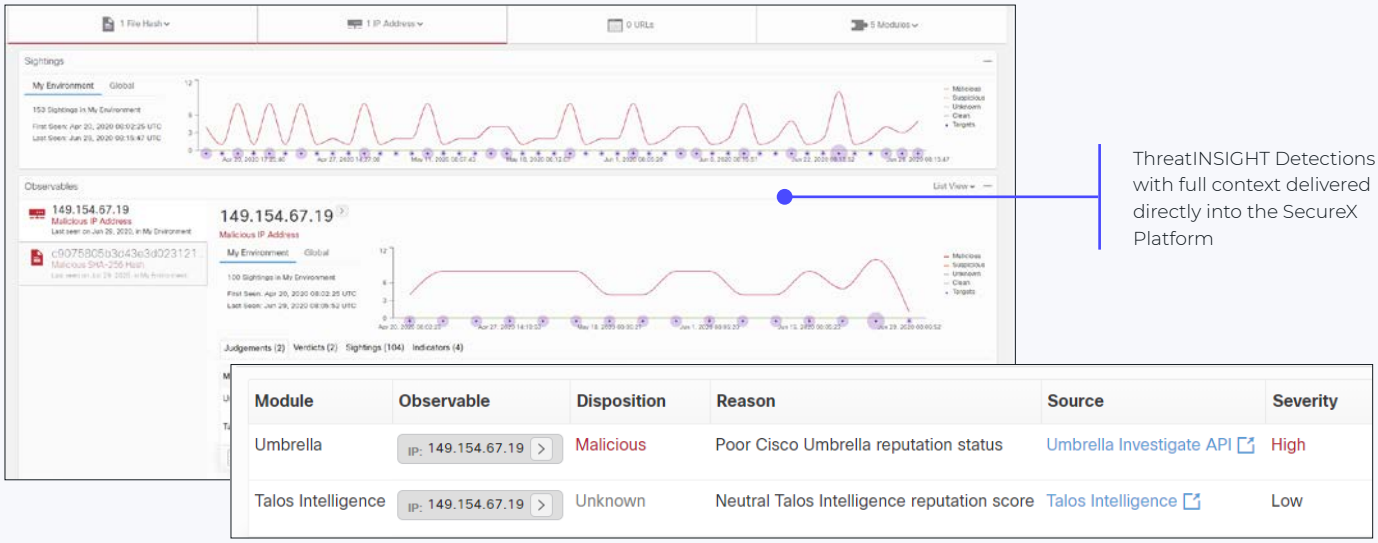
Discover targeted threats by providing threat hunters with comprehensive visibility, near packet-level detail and contextually rich workflows

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)

USE CASE

Enhanced Detections



Gigamon ThreatINSIGHT provides high-fidelity behavioral-based detections to uncover tactics and malicious activity across the entire MITRE ATT&CK framework, delivering findings directly to the Cisco SecureX platform. ThreatINSIGHT's unequaled network visibility enables rapid identification of hidden and emerging threats for security analyst and incident responders.

GIGAMON THREATINSIGHT NETWORK VISIBILITY

Providing analysis of North, South, East and West traffic for on-premise and cloud infrastructures to identify threat activity related to any device type without need for endpoint clients. It records in the Gigamon INSIGHT cloud data warehouse up to 30 days of enriched network metadata that is more comprehensive than FLOW data, providing near packet level context while keeping storage needs to a minimum.

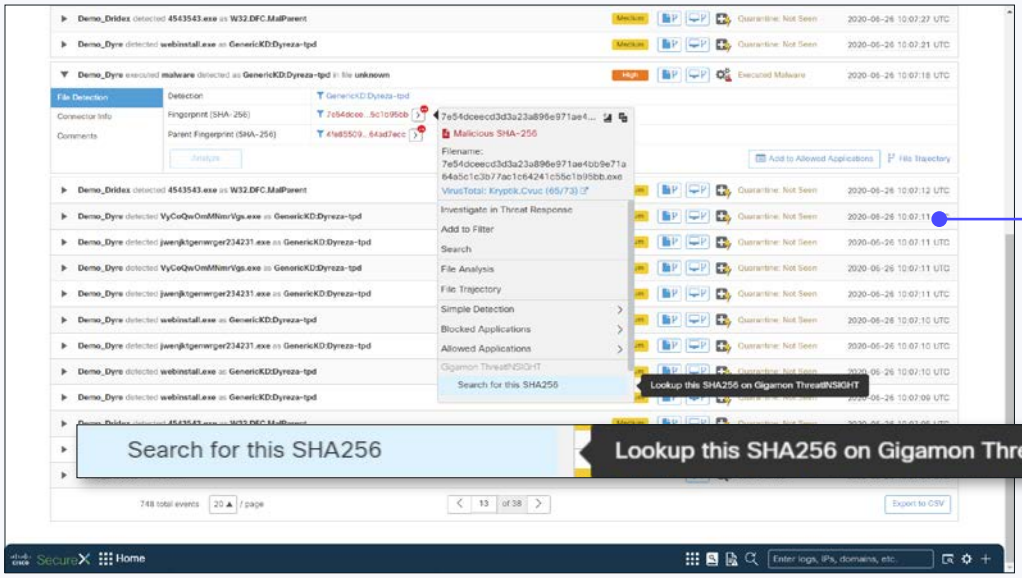
THREATINSIGHT DETECTION TECHNIQUES

Powered by Gigamon Applied Threat Research (ATR), composed of veteran security researchers and data scientists, invent and deliver accelerated, high-fidelity detection capabilities.

- ATR delivers and constantly curates proprietary threat intelligence that serves ThreatINSIGHT
- ATR develops advanced machine learning and behavioral classifiers to analyze the in-depth metadata in the INSIGHT cloud data warehouse extracted from all network activity to identify signals for hunting and investigations
- ThreatINSIGHT covers all stages of the MITRE ATT&CK Framework to provide accelerated advanced threat detection: initial access, execution, persistence, privilege escalation defense evasion, credential access, discovery, lateral movement, collection command and control, exfiltration and impact

USE CASE

Dynamic Threat Hunting



The SecureX/ThreatINSIGHT integration enables security experts to pivot directly into ThreatINSIGHT to use purpose-built threat hunting interfaces and workflows that automatically populate contextual evidence and allow rapid identification of threat actor tactics and behaviors.

THE COMPREHENSIVE SECUREX/THREATINSIGHT INTEGRATION ALLOWS FOR SIMPLE CONSOLE INTERACTION

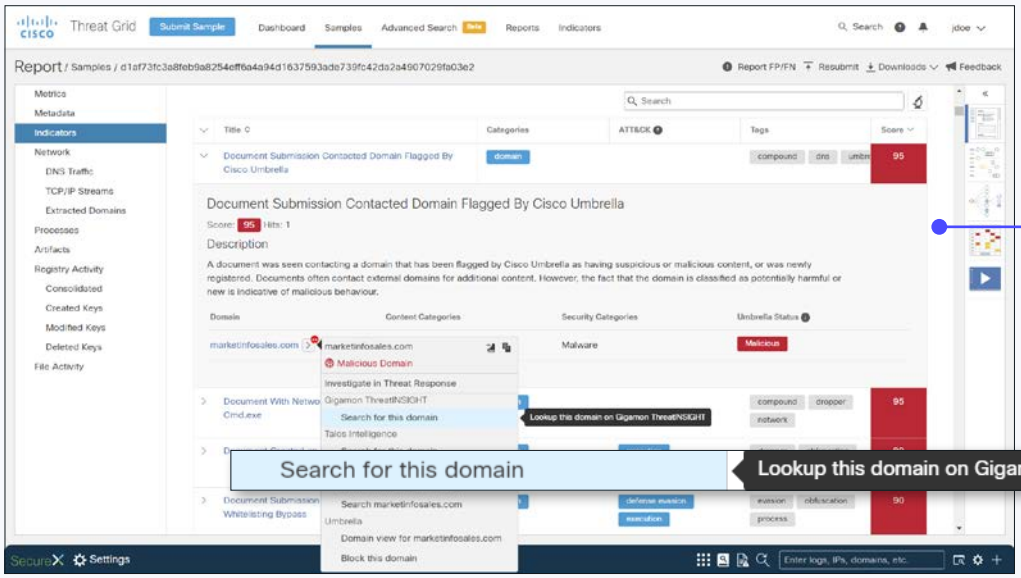
- Within the SecureX platform, Observables from any SecureX integrated solutions or threat hunter-populated Indicators of Compromise can be delivered into ThreatINSIGHT to kick-off threat hunting efforts
- ThreatINSIGHT records of up to 30 days of enriched network metadata (N/S/E/W) enabling threat hunters to identify activity not flagged by traditional detection-based solutions
- ThreatINSIGHT's rich metadata allows threat hunters to discover and understand the malicious behavior of the threat actors inside their network

THREATINSIGHT HUNTING

- Create Boolean searched for specific patterns of behavior
- Breakdown all observed ports and protocols of the threat's communication and see instant replay into behaviors seen PRIOR to the observed detection (leading indicators)
- Uncover initial access, execution, persistence, privilege escalation defense evasion, credential access, discovery, lateral movement, collection command and control, exfiltration and impact

USE CASE

Investigate Root-Cause and Forensic Sequencing



Pivot from SecureX directly into ThreatINSIGHT to investigate the root-cause of any incident and establish the forensic sequencing of events across your entire network for up to the previous 30 days

From any Sighting identified within SecureX, use ThreatINSIGHT to investigate and understand an attack's origin, lateral spread, targets and sequence of events — even if those events were not known at the time of occurrence.

PIVOT FROM SECUREX INTO THREATINSIGHT

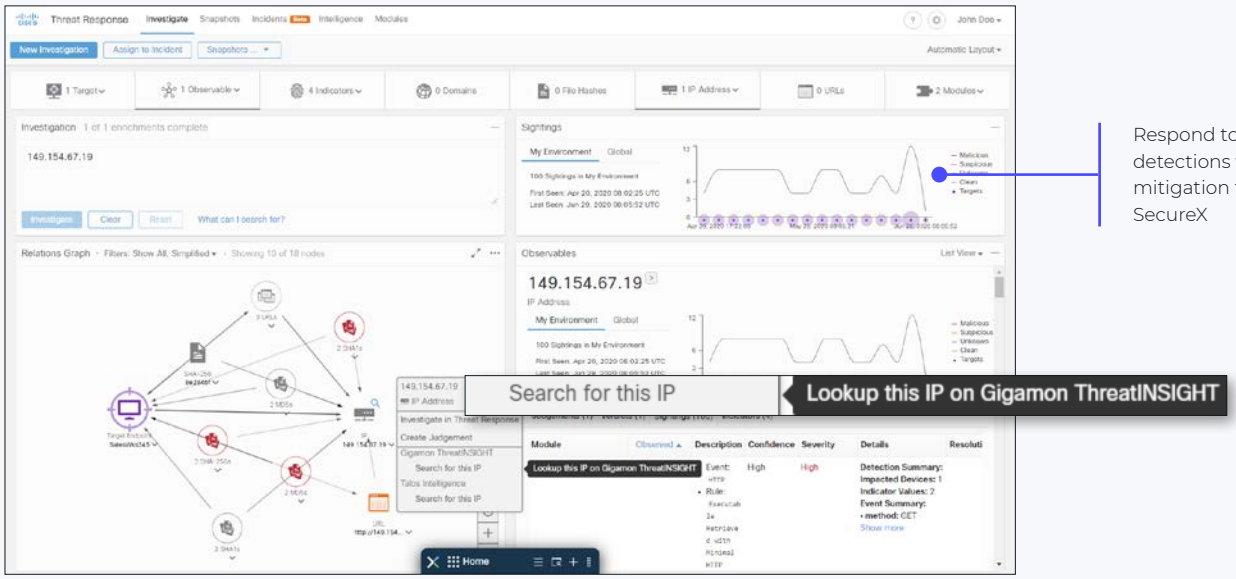
- Within the SecureX platform, Sightings from any SecureX integrated solutions can be delivered into ThreatINSIGHT to kick-off or augment investigation efforts or rapidly validated potential suspicious activity
- ThreatINSIGHT's recording of up to 30 days of enriched network metadata (N/S/E/W) enables investigators to identify related activity to the Sighting
- ThreatINSIGHT's rich metadata enables investigators to build comprehensive cases and understand each incident
- Evidence identified from within ThreatINSIGHT can be added to SecureX threat response cases with one click

THREATINSIGHT INVESTIGATION

- ThreatINSIGHT provides the visibility and activity depth to enable rapid triage and validation of events, so that security experts can identify true positive detections with confidence
- ThreatINSIGHT enables security experts to search current and historical traffic activity to understand the extent of the threat actors reach, damage and ultimate objective across the entire network

USE CASE

Rapid, Informed and Wide-Ranging Response



SecureX enables immediate mitigation of attacks for all threats identified by ThreatINSIGHT or any products integrated with the SecureX platform.

THREATINSIGHT ENABLES RAPID, INFORMED RESPONSES

ThreatINSIGHT augments and guides investigative efforts with data enrichment from threat intelligent sources and knowledge of threat actors' intent to enable thoughtful, informed, and rapid targeted response actions

ONE-CLICK MITIGATION TO THREATINSIGHT DETECTIONS WITHIN SECUREX

- Based on thorough historical investigations of incidents with ThreatINSIGHT, perform thoughtful and rapid targeted response actions to ensure complete mitigation of an actor's malicious activities
- Review ThreatINSIGHT detections and evidence from within the SecureX platform and perform one-click response actions using any SecureX integrated response solutions
- When hunting threats within ThreatINSIGHT, pivot to the SecureX platform to rapidly take mitigation actions using any response solutions integrated with SecureX

Conclusion

The Cisco SecureX Platform and Gigamon ThreatINSIGHT integration simplifies security for security analysts and incident responders. ThreatINSIGHT delivers unequaled visibility, high-fidelity behavioral-based detection and rapid, informed response. For its part, the SecureX Platform aggregates findings, visualizes threat activity and enables effective and comprehensive one-click mitigation actions:

- **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, such as Amp for Endpoints, Umbrella, Cisco Firewalls, Cisco Email Security and Cisco Web Security

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