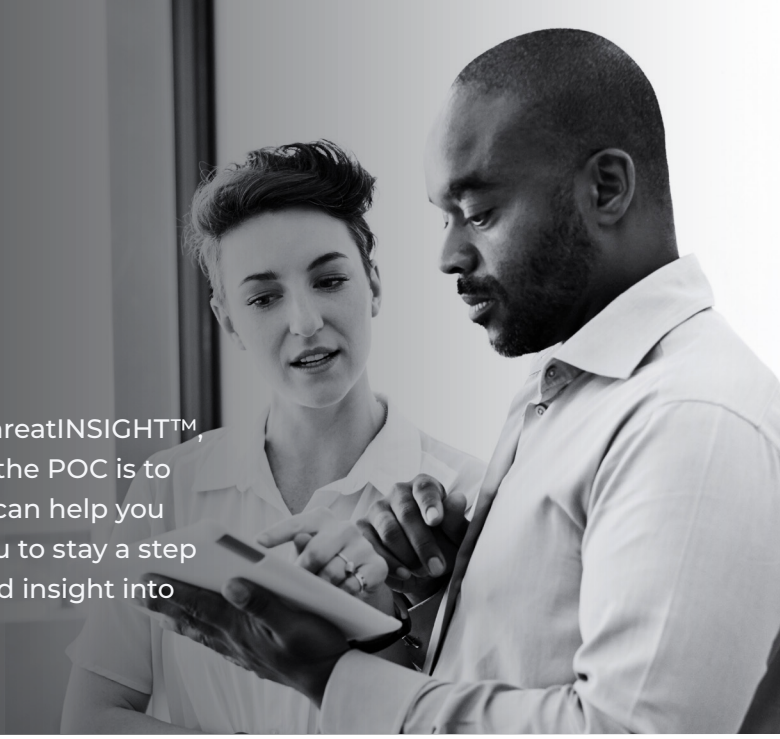
Gigamon® ThreatINSIGHT

Proof of Concept



A proof of concept (POC) is an evaluation of Gigamon ThreatINSIGHT™, a network detection and response solution. The goal of the POC is to help your security team determine how ThreatINSIGHT can help you improve your security posture. ThreatINSIGHT allows you to stay a step ahead by giving your security teams more time, data and insight into attacker behavior with the following capabilities:

HIGH CONFIDENCE DETECTION

The ThreatINSIGHT solution's network visibility combined with its ability to operate quickly at massive scale allows for high-confidence, low false positive detections of malicious activity based on complex behaviors instead of individual indicators. Gigamon Applied Threat Research (ATR) leverages machine learning and behavioral analysis to identify uniquely malicious activity and map it to the MITRE ATT&CK® framework.

CURATED THREAT INTELLIGENCE

Many organizations have feeds of threat intelligence indicators. ThreatINSIGHT can automatically consume these indicators and applie them in real time across your network data. Additionally, Gigamon ATR reviews all threat feeds for accuracy and timeliness to get a confidence in each feed. That confidence is also automatically applied across threat intelligence data.

PASSIVE NETWORK INVENTORY

ThreatINSIGHT has a rich network dataset that allows for the identification of assets and potentially outdated or misconfigured software that may create vulnerabilities that can be exploited by an attacker. Gigamon customers, with support from their Technical Success Manager (TSM), work together to mitigate these issues reducing the risk to the entire organization.

RAPID INVESTIGATION CAPABILITIES

SOC analysts and incident responders need access to data quickly to make decisions on the validity of alerts, the severity of an incident, and the full scope of a breach. ThreatINSIGHT is designed to help analysts quickly answer these questions enabling them to be more expedient and effective at their jobs.

ON-DEMAND TRAINING AND ASSITANCE

Each customer is assigned a Technical Success Manager (TSM) to work with, that is a seasoned incident response analyst and an expert using ThreatINSIGHT for detecting and investigating security incidents. As a customer, you will have regular access to a TSM to help with tool use, training, investigation questions, and assistance with the ThreatINSIGHT solution.

THREAT HUNTING

ThreatINSIGHT gives your team proactive hunting tools like parallel hunting, guided playbooks and observations to find threats that may have evaded your perimeter defenses. The TSMs will help you operationalize and incorporate the Insight solution into your hunting framework as it develops.

POC TIMELINE

A POC of the Gigamon ThreatINSIGHT solution is typically a four-week evaluation engagement beginning on the kick-off meeting. The timeline below highlights the activities performed during each stage and the deliverables provided.

Stage	Activities	Deliverables
Pre-POC	+ Define Use Cases & Success Criteria + POC Scoping + Sensor Installation	+ ThreatINSIGHT Portal Access + Network Sensor(s)
Week 1 (Early in the week) Kick-Off	+ Solution Executive Overview	
	+ Deployment Review + ThreatINSIGHT 101: The Basics + ThreatINSIGHT 101: Detection & Triage	+ Detections Report*
Week 1 (Late in the week) Investigation	+ ThreatINSIGHT 101: Investigation	
Week 2 (Early in the week) Investigation	+ ThreatINSIGHT 101: Dashboards	+ Nework Security Posture Report*
Week 2 (Late in the week) Investigation	+ ThreatINSIGHT 101: Threat Hunting + Technical Success Manager (TSM) Introduction	+ Threat Hunting Methodologies
Week 3 Wrap-Up	+ Executive Review of Deliverables + POC Results Presentation + Next Steps	+ Final Deliverables*

* Initial reports are introduced throughout the POC and final report versions are delivered at the end of the POC.

POC DELIVERABLES

Gigamon will provide deliverable reports related to the network telemetry data collected from the customer environment during the POC. These reports include:

+ **Network Security Posture Report –** highlights security hygiene issues observed on your network.
+ **Detections Report** – provides statistics, metrics, and recommended remediation steps.

REQUIREMENTS

+ Sensors require a passive feed of network traffic from a SPAN (port mirror), network tap, or packet broker.
+ Sensors require uninspected connection over TCP/443 to hardcoded backend IPs (if using in-line decryption or proxy).

For more details reach out to your sales representative or visit gigamon.com/contact-sales.

Gigamon®

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