Expertise on Your Side

The People Behind ThreatINSIGHT Guided-SaaS NDR

Gigamon ThreatINSIGHT™ is a network detection and response (NDR) solution built by responders for responders, but also staffed by responders for responders to ensure expertise is available to customers in every aspect of the offering: technology, management, and guidance.

Being prepared, ever vigilant, and ready to respond efficiently and effectively when cyber incidents strike is critical for your organization's SOC/IR defenses. Guided-SaaS NDR redefines SaaS offerings to ensure security teams have access to expert advisory guidance during critical incidents, are not distracted by security tool maintenance or detection tuning, and are extracting the highest value from their NDR solution through visibility, health checks, and ongoing team enablement.

ThreatINSIGHT Guided-SaaS is powered by both Gigamon Applied Threat Research (ATR) and the Technical Success Management (TSM) team, composed of expert SOC, incident response (IR) and threat professionals who are field tested practitioners in responding to cyber-attacks. Their first-hand experience establishes credibility with clients and a partnership to dismantle cyber-adversaries. By removing distractions, ensuring optimal visibility and technology performance, and providing expert threat knowledge and investigation best practices, ThreatINSIGHT customers improve their SOC/IR team's effectiveness while easing high-pressure situations that lead to burnout.

WORLD-CLASS EXPERTISE

Applied Threat Research
Knowledgeable incident responders, threat researchers and data scientists that deliver:

- Threat research to accelerate detections
- Detection engineering and QA to achieve high-fidelity findings
- Security R&D to continue to innovate

Technical Success Management Team
Experienced security analysts and incident responders that:

- Ensure fast time to proficiency and value
- Provide advice when it matters most
- Partner to secure the customer's success

Guided-Saas Benefits

Technology built by responders, for responders providing:

- Network visibility, closing the SOC visibility gap across the ATT&CK framework
- Advanced, hi-fi adversary detection, using a blend of ML, behavioral, & threat intel techniques
- Threat context, accessible & searchable
- Threat specific guided next steps
- Rapid, informed response, workflows and retained network metadata

Redefined SaaS management staffed by experts to remove distractions and ensure:

- Your team's ongoing product proficiency
- Deployment, configuration, and visibility optimization, even as networks change
- You stay current with SaaS maintained updates and system availability
- Minimal tool maintenance and zero detection tuning for your team

Expert advisory guidance when it matters most; during high-pressure active threats and incidents, Gigamon TSMs can provide:

- Threat /adversary knowledge supported by Gigamon ATR
- Incident management guidance
- Triage and threat hunting best practices

Applied Threat Research

MISSION Dismantle an adversary's ability to impact customers.

METHOD Gigamon ATR pairs security experts who track adversary activity and behaviors with specialized data scientists to create efficient, actively managed high-fidelity detection techniques that span the breadth of the MITRE ATT&CK framework.

Threat Research to Accelerate Detection

+ Research threat actors, their tools, and their infrastructure to produce proprietary ATR threat intelligence
+ Curate public and private intel feeds to augment ATR's threat intelligence
+ Provide ThreatINSIGHT with knowledge of threat actors' intent, TTPs, and tools

Detection Engineering to Achieve High-Fidelity

+ Research, build, and maintain high quality Machine Learning and Behavioral Analysis engines
+ Apply all techniques to global crowdsourced data sets, enabling identification of emerging threats
+ Rigorous QA to all detection techniques and intelligence to ensure high-true positive rates without customer's needing to perform detection tuning

Security R&D to Innovate

+ Continuous research, prototyping, and validation of future detection and investigation capabilities

EXPERTISE

ATR pairs threat and R&D experts to deliver accurate network detections of adversary behavior and knowledge of the adversary's intent and tactics to help your SOC/IR team triage, investigate and respond with certainty.

	THREAT RESEARCHER / INTELLIGENCE	DETECTION ENGINEER	DATA SCIENTISTS
PASSION	Dismantling cyber-adversaries	Solving difficult problems, with agility	Apply ML to real world scenarios
EXPERIENCE	Forensics / reverse engineering Incident response or red team Threat intelligence Intrusion analysis Large dataset analysis	Computer science expert Research mindset Development of native-cloud architectures Data science application Cyber security	Computer/data science expert Interaction with large data stores Utilization of large data processing pipelines Data visualization Cyber security
RESPONSIBILITIES	Drive intelligence collection efforts Identify detection gaps and opportunities Detection sprints to expand detection capabilities Threat actor discovery and emerging threat behavior	Collaboration with internal teams to identify requirements Design, prototype, and deliver new detection systems Detection sprints to expand detection capabilities Maintain, enhance, and QA existing systems	Exploratory data analysis Research, develop, and maintain expert and behavior-based systems Utilize supervised, semi-supervised, unsupervised machine learning and neural network techniques to classify threats and identify patterns

Technical Success Management

MISSION

Be a trusted advisor to and advocate for customers, enabling effective and efficient utilization of ThreatINSIGHT and providing guidance when it matters most.

METHOD

Staffed by analysts and responders, the TSM team understands the challenges facing SOC/IR teams and works tirelessly to ensure every interaction provides value to their customers.

Ensuring Fast Time to Value

+ Deployment & visibility assistance to drive effective detection and response
+ Optimize & expand APIs, workflows, visibility & integrations
+ Ensure customer proficiency & utilization with continuous enablement

Providing Advice When It Matters

+ Share knowledge of specific threat capabilities based on ATR's first-hand incident investigations
+ Provide strategies for comprehensive investigations to enable rapid, informed response

Partnering to Secure Your Success

+ Engage to define & understand customer's strategic security goals & work with customer to achieve
+ Improve security posture by managing progress, accelerating capabilities, and optimizing platform

EXPERTISE

Unlike other security vendor customer success programs, the TSM team is composed of experienced security analysts and incident responders. Their skills include:

TECHNICAL SKILLS / EXPERTISE	EXPERIENCE	ENGAGEMENT
SOC operations	3+ years information security, SOC, IR, or similar cyber experience	**Onboarding and deployment** + Deliver enablement training + Facilitate deployments and system optimization / configurations
In-depth security event analysis skills	5+ years technical delivery and client management experience	**Evaluate and drive success plan** + Deliver periodic detection reviews + Perform visibility/product heath checks + Continued enablement
Experience in incident response, forensics, malware analysis, and remediation	Cyber security relevant certifications	**Advisory guidance** + Upon request, provide threat specific knowledge and incident response best practice guidance
Rich networking knowledge	Experience in collecting, analyzing, and escalating security events	
Enterprise network architectures (data center, server, storage, switching, cloud)	Experience in investigating, developing mitigation plans and responding to computer security incidents	
Security device configuration & administration (e.g., FW, IPS, etc.)		

Case Studies

Guided SaaS in Action

Deployment & Ongoing Maintenance

CHALLENGE
A well-known cyber security vendor sought a single source for network threat visibility that allowed them to identify, triage, and investigate threats in a single console. They wanted a solution that didn't require significant care and feeding or distract their team with noisy false-positive alerts.

SOLUTION
Led by the TSM team, ThreatINSIGHT Guided-SaaS NDR was deployed across the customer's five global datacenters in under 2 hours, providing immediate comprehensive network visibility. The TSM team provides configuration and deployment optimization, periodic system and visibility health checks, and all software updates. By reducing distractions and ensuring ThreatINSIGHT is optimized, customers are able to focus on defending their organization.

Enablement

CHALLENGE
As a large healthcare benefit management firm, acquisitions are common and bring additional security risks. To provide visibility into the security posture of the acquired company, they mandate the deployment of ThreatINSIGHT before networks are connected. New teams at each acquired company must rapidly become enabled on ThreatINSIGHT.

SOLUTION
Led by the TSM team, onboarding and enablement of each new acquired company's security team is delivered. SOC/IR teams are provided with comprehensive product overviews, best practices, and taught how to best use ThreatINSIGHT for triage and investigations. As new staff members arrive, ongoing enablement is delivered by TSMs to ensure ThreatINSIGHT proficiency.

Advisory Guidance

CHALLENGE
Inside a large insurance provider, ThreatINSIGHT identified, with high confidence and severity, an adversary's lateral movement. Not knowing much about the attacker's motivation or tactics, the customer needed guidance.

SOLUTION
Backed by ATR, the TSM team promptly informed the customer of the adversary's intent, tactics, techniques, and procedures. Armed with the specifics on the threat, the TSM provided guidance on best practice investigation and response approaches to mitigate the attack. The customer was able to investigate the full scope of the adversary's activity across their network and mitigate the attack before damage ensued.

Gigamon®

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