Guided-SaaS NDR

Expertise on Your Side

Leaders of security teams face a two-front battle. On one front, they must acquire visibility into cyber-adversary activity on their network. On the other front, they are challenged to improve SOC effectiveness while reducing analyst burnout. Gigamon ThreatINSIGHT™ Guided-SaaS NDR closes the SOC visibility gap and provides high-fidelity adversary detection to enable rapid, informed response. Redefining how SaaS-based security is delivered, ThreatINSIGHT Guided-SaaS NDR ensures security teams:

ARE NOT ALONE
Guided-SaaS provides access to advisory guidance from ThreatINSIGHT security analysts and incident response experts during high-risk incidents, reducing burnout

ARE NOT DISTRACTED
Guided-SaaS means minimal maintenance and zero detection tuning required, improving SOC/IR efficiency and effectiveness

ARE NOT IN THE DARK
Guided-SaaS closes the SOC visibility gap necessary to effectively identify cyber-adversaries across any network, device and traffic

As a company's first responders to cyber adversaries, security operations and Incident Response (IR) teams are well versed in tackling challenges. However, in a two-front battle, mature security teams seek vendors that understand the SOC/IR workload and design solutions that focus not only on analyst effectiveness, but also burnout. Specifically, an ideal network detection and response (NDR) solution should alleviate:

VISIBILITY GAPS LEAVE SOC IN THE DARK

Analysts are missing visibility they need to be effective:

+ SIEMs & EDRs have visibility gaps (devices, networks, and traffic)
+ Workforces are changing to work from home (WFH)
+ Encrypted traffic is rapidly growing, making inspection difficult

UNNECESSARY TOOL DISTRACTIONS

Analysts are overwhelmed because:

+ They face constant false-positive alerts
+ Time-consuming detection tuning falls on the security team rather than the vendor
+ Solutions require hidden care and feeding costs (maintenance, updates, visibility optimizations)

FIGHTING INCIDENTS ALONE

Analysts are facing high-pressure incidents on their own:

+ Alerts lack context or guidance for what to do next
+ Vendors charge for product expertise enablement
+ Vendors charge for threat knowledge or incident investigation guidance

Of SOC analysts cite lack of visibility into network traffic as the top reason for SOC ineffectiveness[1]

Visibility is a foundational need

Of SOC analysts report rank "Minimization of false positives" as the most important SOC activity (detection tuning)[2]

Reducing FPs should be the vendor's responsibility

Of SOC analysts indicate maintaining, tuning, and providing updates to their security tools is a core responsibility[2]

SecOps should have a single focus . . . Threat Management

Of SOC analysts report burnout quickly because of the high-pressure environment[2]

SecOps teams benefit from Trusted Advisors

The ThreatINSIGHT Difference

Gigamon ThreatINSIGHT Guided-SaaS NDR is a unique, modern SaaS offering that includes a purpose-built platform for adversary detection and response, together with human talent for security expertise when it counts most. The Gigamon Technical Success Management (TSM) team is staffed with field tested security analysts and incident responders who work alongside Gigamon Applied Threat Research (ATR) to ensure ThreatINSIGHT customers are best positioned to dismantle adversaries.

CLOSING THE SOC VISIBILITY GAP

While SIEMs and EDRs have increased a SOC/IR team's effectiveness in identifying active infections, visibility gaps to devices, networks and traffic remain. The result is analysts are left in the dark when trying to identify all adversary activity described across the MITRE ATT&CK framework. ThreatINSIGHT Guided-SaaS NDR solution:

+ **Provides visibility and recording of near packet-level metadata**

  Any device, any network, and any traffic, including N | S | E | W and encrypted

+ **Delivers high-fidelity adversary detections**

  Blending machine learning, behavioral analysis, and crowdsourced threat intelligence

+ **Fast omnisearch powered triage and investigation capabilities**

  7-, 30-, or unlimited day access to enriched network metadata

+ **Embeds recommendations for analysts and responders**

  Guided threat specific next steps for incident management

ELIMINATING DISTRACTIONS

Purchasing a security solution should enable security professionals to focus on protecting their organization. However, all too often, security vendors deliver solutions that create distractions rather than positive results. Many NDR solutions have hidden costs and time tied to providing care and feeding, solution proficiency, addressing false positives, and performing detection tuning—all negating their intended value. ThreatINSIGHT Guided-SaaS NDR includes expertise from product and threat experts to remove distractions and ensure:

+ **Fast time to value**

  Gigamon Technical Success Managers (TSMs) provide deployment, configuration, and health check assistance along with ongoing product enablement to ensure continuous customer proficiency

+ **Minimal maintenance**

  Gigamon TSMs and SaaS Ops teams provide sensor and traffic diagnostics, fully managed ThreatINSIGHT portal, and automatic software updates

+ **Zero detection tuning with true-positive detections**

  ATR performs ongoing detection tuning and QA of all machine learning, behavioral analysis, and threat intelligence detection engines

> You can't do big things if you're distracted by a thousand small things. — ANONYMOUS

Cyberattack incidents are high-pressure situations for SOC/IR analysts who are in a race against time to protect their enterprise. With little knowledge of the adversary's intent, tactics, techniques, or procedures and working without external guidance, the security team must often go it alone. External threat knowledge is often scarce, and security tools traditionally only offer generic recommendations. Most tools don't provide the necessary context and search capabilities required to gain insight into what systems the attacker has compromised, the data they have accessed, or the identities and credentials they have obtained. These limitations make it difficult for the SOC/IR team to develop a comprehensive response plan.

ThreatINSIGHT Guided-SaaS NDR is backed by Gigamon ATR threat researchers and Gigamon TSMs, who are experienced security analysts and incident responders, both focused on ensuring customers are best positioned to dismantle adversaries

+ **ATR performs reverse engineering, tracking, and detailing of adversary behavior**

  Building first-hand knowledge on adversaries to empower both ThreatINSIGHT and the TSMs

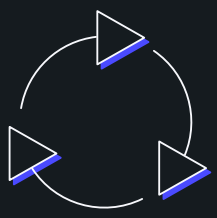
+ **TSMs work directly with customers to provide expert advisory guidance upon request**

  Sharing threat information and incident response best practices and guidance during high-pressure events

ThreatINSIGHT Guided-SaaS NDR

PURPOSE BUILT NDR TECHNOLOGY

Unparalled visibility
+
High-fidelity adversary detection
+
Rapid, informed response



DISTRACTION FREE SaaS MANAGEMENT

Minimal maintenance
+
Zero detection tuning
+
Automatic software updates

ADVISORY GUIDANCE WHEN IT MATTERS MOST

Threat/adversary knowledge
+
Incident management guidance
+
Triage and hunting best practices

ThreatINSIGHT Guided-SaaS NDR

ThreatINSIGHT provides NDR as it should be. A solution built for responders, by responders that:

+ Augments your SIEM and EDRs with network detection and response to complete the SOC visibility triad, identifying threat actor behaviors not observable by other technologies across the ATT&CK framework so your team is not in the dark
+ Delivers NDR technology that requires no detection tuning and SaaS delivery that requires minimal solution management and maintenance so your team is not distracted
+ Eases high-pressure scenarios for security analysts with Guided-SaaS expertise on your side so your team is not alone

Learn more at gigamon.com/threatinsight.

REQUEST A DEMO AT GIGAMON.COM/DEMO.

[1] Ponemon: Improving the Effectiveness of the SOC, 2020
[2] Ponemon: The Economics of Security Operations Centers, 2020

Gigamon®

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

5.21_01