

SYDNEY – June 11, 2021 – Gigamon, the leader in cloud visibility and analytics, today announced ThreatINSIGHT Guided-SaaS NDR (network detection and response), which was purpose built to improve SOC (Security Operations Center) effectiveness and reduce analyst burnout.

ThreatINSIGHT Guided-SaaS NDR, which redefines how SaaS-based security solutions are delivered, arrives at a critical juncture in threat defence as exponential growth in infrastructure complexity, and ever-increasing cyber threat activity, is negatively impacting InfoSec team's ability to efficiently do their jobs, ultimately contributing to high burnout rates.

ThreatINSIGHT alleviates the three most common problems that continue to plague SOC analysts and incident responders.

They are often working in the dark without foundational visibility to observe adversary movement, leading 69% of IT and security practitioners to cite network visibility as the top reason for SOC ineffectiveness.

They continually face the distraction of burdensome tool maintenance, prompting 43% of SOC analysts to indicate that maintaining, tuning and providing updates to their security tools is their core responsibility.

Finally, they are often operating alone, without expert support, which is a factor CISOs must consider when addressing why 70% of their SOC analysts report burnout due to high-pressure environments.

Gigamon ThreatINSIGHT removes these burdens that otherwise prohibit teams from focusing on effectively identifying adversary activity across the MITRE ATT&CK framework. In addition, during high-pressure, active incidents, customers benefit from access to expert-level guidance from the experienced security analysts and incident responders on the Gigamon Technical Success Managers (TSM) team.

"Security analysts are consistently overwhelmed, stressed, and understaffed, leaving the majority pretty much unable to anticipate, recover from, or adapt to new attacks (without reaching burnout, which is common)," wrote analyst Allie Mellen from Forrester in a recent series of blog posts.

"Security tools must support security teams in doing their jobs better, from the people side, the process side, and the technology side."^[1]

With Gigamon ThreatINSIGHT Guided-SaaS NDR, teams are more effective with less stress as a result of:

Visibility. ThreatINSIGHT ensures SOC analysts are never in the dark by delivering guided visibility to adversary network activity, not observable by EDRs and SIEMs. Network traffic provides the essential foundation for incident response including visibility to lateral movement, command and control, and other steps along the MITRE ATT&CK framework.

ThreatINSIGHT can observe and identify adversary activity on any device or network, across any type of traffic, including encrypted traffic, thereby eliminating the SOC visibility gap.

Focus. ThreatINSIGHT minimises distractions by guiding security professionals to high-confidence detections crafted by the Gigamon Applied Threat Research (ATR) team. By continuously delivering QA'd and tuned advanced machine learning, behavioural analytics, and proprietary threat intelligence for true positive adversary detection, clients are not distracted with laborious false-positive tuning.

Expertise. ThreatINSIGHT guides SOC analysts via product and people. The solution guides investigative workflows built by our expert responders, on top of a powerful and flexible Insight Query Language. TSMs, included as part of the service, are security analysts and incident responders themselves who provide best practices and threat knowledge to directly assist clients when they need it most. "As hybrid cloud and hybrid workforces become the new normal and as threat actors continually increase their sophistication, the job of security analysts and incident responders becomes even more complex," said Michael Dickman, Chief Product Officer at Gigamon.

"The rise in recent ransomware attacks is a strong reminder that security teams need defence-in-depth with visibility, focus, and expertise. Now, with the world's first Guided-SaaS NDR, customers no longer have to fight this battle alone, or without full visibility of their adversary. InfoSec teams now have the tools and expertise to respond with speed and confidence."

For more information on the efficiency and effectiveness of ThreatINSIGHT, read the ESG Technical Review to learn how ESG independently validated the efficacy of Gigamon ThreatINSIGHT.

About Gigamon

Gigamon helps the world's leading organizations run fast, stay secure and innovate. We provide the industry's first Guided-SaaS NDR (network detection and response) solution which closes the Security Operations Center (SOC) visibility gap, removes unnecessary distractions and provides expert advisory guidance when it matters most. With visibility into network traffic across their entire hybrid cloud infrastructure, organisations eliminate security blind spots while benefiting from Gigamon security expert guidance, helping improve SOC effectiveness and reducing burnout of their security teams.

Gigamon has been awarded over 90 technology patents and enjoys world-class customer satisfaction with more than 4,000 organisations, including over 80 percent of the Fortune 100 and hundreds of government and educational organisations worldwide. Headquartered in Silicon Valley, Gigamon

operates globally. For the full story on how Gigamon can help you to run fast, stay secure and innovate, please visit www.gigamon.com and follow us on Twitter. and LinkedIn.

Media Inquiries:

Gigamon

Email: public.relations@gigamon.com

Contacts

David Frost

(02) 7903 9567

[mailto: david.frost@prdeadlines.com](mailto:david.frost@prdeadlines.com)