Technical Review

Gigamon ThreatINSIGHT Guided-SaaS Network Detection and Response

Date: March 2021 **Author:** Tony Palmer, Senior Validation Analyst

Abstract

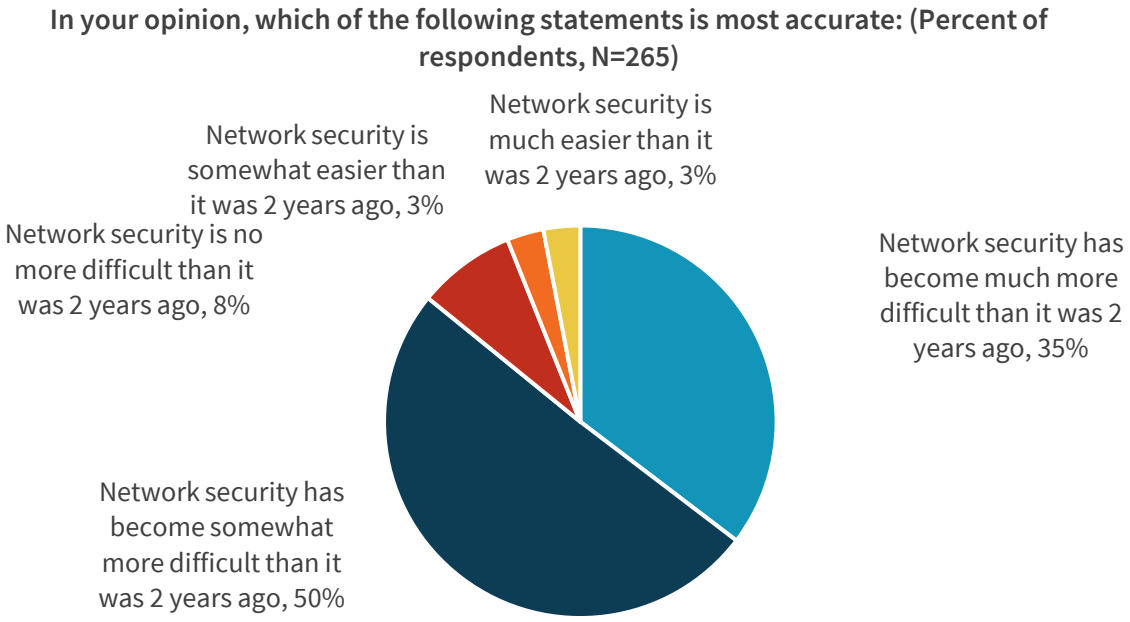
In this Technical Review, ESG examines the Gigamon ThreatINSIGHT Guided-SaaS network detection and response (NDR) solution with a goal of validating the efficiency and effectiveness of its threat detection and incident response capabilities.

The Challenges

As organizations change workforce models and transition to the cloud, their unobserved attack surfaces grow. Limited visibility enables successful attackers to move throughout a network. These conditions heighten risk, even as data protection regulations continue to expand. Information security and incident response teams struggle when they can't see what's happening on the network, can't detect threats with high confidence, and can't respond to attacks quickly and effectively due to a lack of visibility and, more importantly, context.

According to ESG research, 85% of survey respondents reported that network security is somewhat or much more difficult than two years ago (see Figure 1).[1] The most-cited reason for this was an increase in the threat landscape, with nearly half (45%) of respondents identifying this as the cause.

Figure 1. Network Security Is Getting Harder



Source: Enterprise Strategy Group

Respondents in the same survey identified other reasons for the heightened level of complexity, including the increase in mobile and IoT devices accessing the network, pervasive usage of cloud applications, and the swell of distributed users with

[1] Source: ESG Research Report, *The State of Network Security: A Market Poised for Transition*, March 2020. All ESG research references and charts in this technical review have been taken from this report, unless otherwise noted.

access to the network. For all of these reasons, organizations find it difficult to maintain tight security controls across increasingly dispersed resources. While not reaching the level of criticality seen in other cybersecurity segments, the skills shortage in network security still is present and was cited relative to both staffing (23%) and the knowledge level (20%) of respondent organizations.

While there isn't much that organizations can do directly to impact the threat landscape, they can control some aspects of their network complexity—for example, when security controls are built into network designs from the start. However, despite the criticality of cybersecurity, many organizations are not consistently building in controls during the network engineering and design process. Nearly half (48%) of respondents report not always having security controls and monitoring capabilities as part of the network engineering and design process.

What is needed is a solution that can provide the visibility, threat detection, and context to improve an organization's security posture and enable comprehensive response, including triage, investigations, threat hunting, and integrations for mitigation actions to reduce exposure times to incidents.

The Solution: Gigamon ThreatINSIGHT

Traditional on-premises NDR solutions typically require a hefty deployment effort and ongoing management, upgrades, and storage. Historically, on-premises NDRs are detection-focused and rely on unsupervised anomaly-based machine learning (ML) techniques. They train on your networks, users, peer groups, and device activity using a time-consuming process to establish a baseline and then alert on anomalies. This approach unearths large numbers of benign anomalies due to the lack of additional context. Significant time and resources are required to manually triage these alerts and filter out the actual threats because many on-premises solutions lack robust investigative and threat-hunting capabilities. Further, on-premises NDRs typically do not provide visibility of encrypted or work-from-home traffic.

A Guided-SaaS, cloud-native NDR solution, Gigamon ThreatINSIGHT provides both threat detection and incident response capabilities. It blends unsupervised and supervised ML, behavioral analysis, and crowdsourced, curated threat intelligence-based detection techniques to identify known, emerging, and unknown threats as well as pre- and post-exploit adversary behavior. ThreatINSIGHT is designed to provide accurate detections quickly with the context needed to identify real threats and speed incident response.

Unlike traditional NDRs, ThreatINSIGHT is a Guided-SaaS solution, which includes access to Gigamon technical success managers (TSMs)—who are generally experienced SOC and IR specialists, to accelerate the customer's product proficiency and provide advisory guidance on active threats and incidents. Guided-SaaS also refers to the inbuilt workflows designed to help security analysts effectively and efficiently do their jobs.

Guided-SaaS includes the Gigamon Applied Threat Research (ATR) team of security experts and specialized data scientists who create efficient, actively managed, high-fidelity detection techniques that span the breadth of the MITRE ATT&CK framework.

Physical and virtual sensors are deployed to provide comprehensive visibility across environments spanning on-premises to multi-cloud. After a sensor is installed, it prompts for a registration code that can be generated from within a user's ThreatINSIGHT portal. After the code is received, the sensor completes setup, connects to the customer's ThreatINSIGHT deployment, and begins delivering network activity, visibility, and detection data. The ThreatINSIGHT team monitors the sensor installation process to assure all steps are completed properly.

Information security and incident response teams can see all traffic on every device and every network where traffic from sensors is being monitored, including non-VPN users who work from home with the ThreatINSIGHT solution's integration with Zscaler. Rapid response encompasses triage, investigation, threat hunting, and guided next steps based on situational context.

The benefits of using ThreatINSIGHT include:

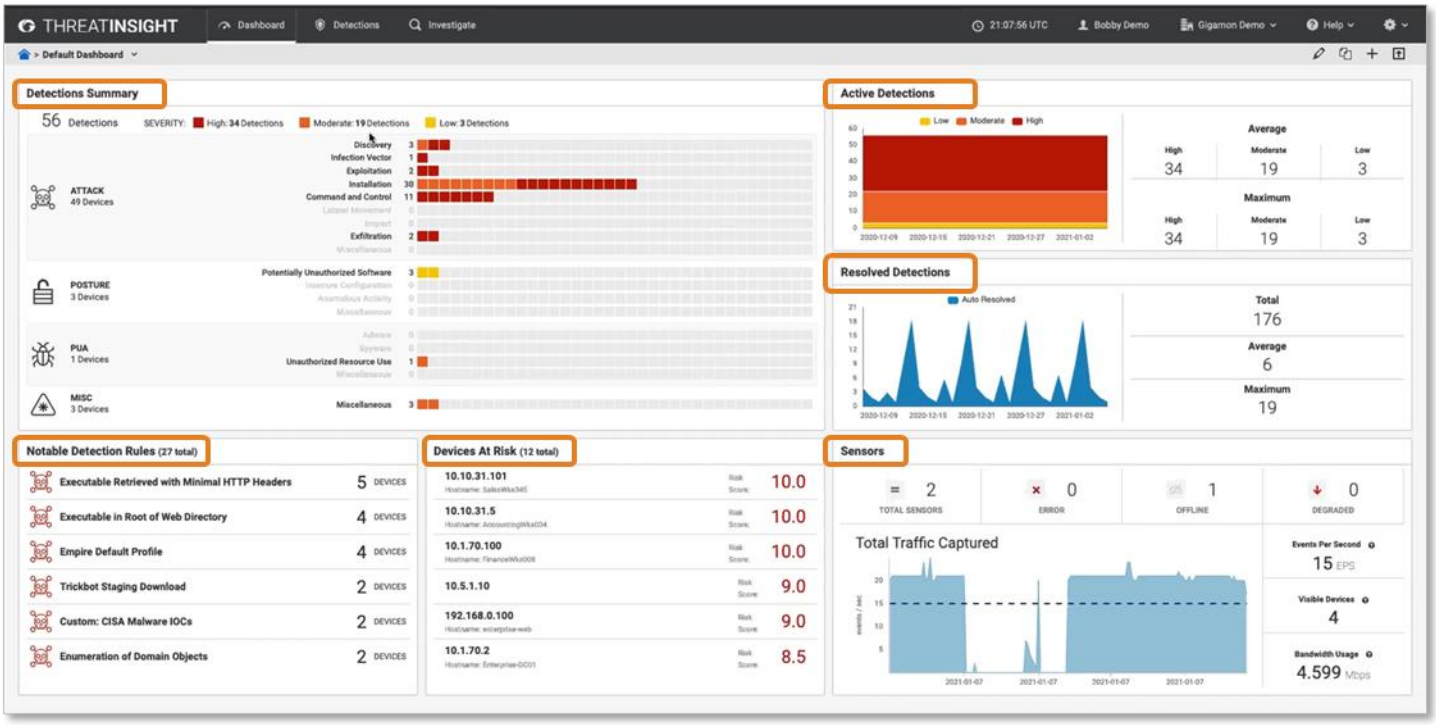
- **High-fidelity detection**—designed to minimize false positives while reducing investigation time and alert fatigue to allow analysts to focus on real threats.
- **Applied threat researchers and data scientists—**pairs threat researchers and data scientists who identify network activities across the MITRE ATT&CK framework to deliver diverse detection use cases using machine learning, deep learning, and proprietary threat intelligence.
- **Expert guided support from Technical Success Managers** —provides expert assistance to ensure fast time to value along with advisory threat/incident support and best practices.
- The ability to decrypt and inspect TLS traffic—customers who also have the Gigamon Visibility and Analytics Fabric gain visibility into encrypted traffic, including TLS 1.3, allowing visibility and analysis into all data flows.
- **Access to critical metadata—**provides enriched historical data and scalability, without the need to correlate data, while minimizing storage.
- **Omnisearch—**simplifies searches and speeds queries of large data sets.
- **Integrations with leading security solutions—**enables one-click response actions.

ESG Tested

ESG performed remote evaluation of Gigamon ThreatINSIGHT, focusing on the efficiency and effectiveness of incident detection and response.

ESG began by logging into the ThreatINSIGHT dashboard, shown in Figure 2, which provided a quick, comprehensive view of key metrics, including summaries of categorized detections, active and resolved detections, exceptions to detection rules, top at-risk devices, and sensor activity. The devices at risk were listed in order of severity. We also noted that detections are annotated immediately to the MITRE ATT&CK-observed activities in the *Detections Summary*.

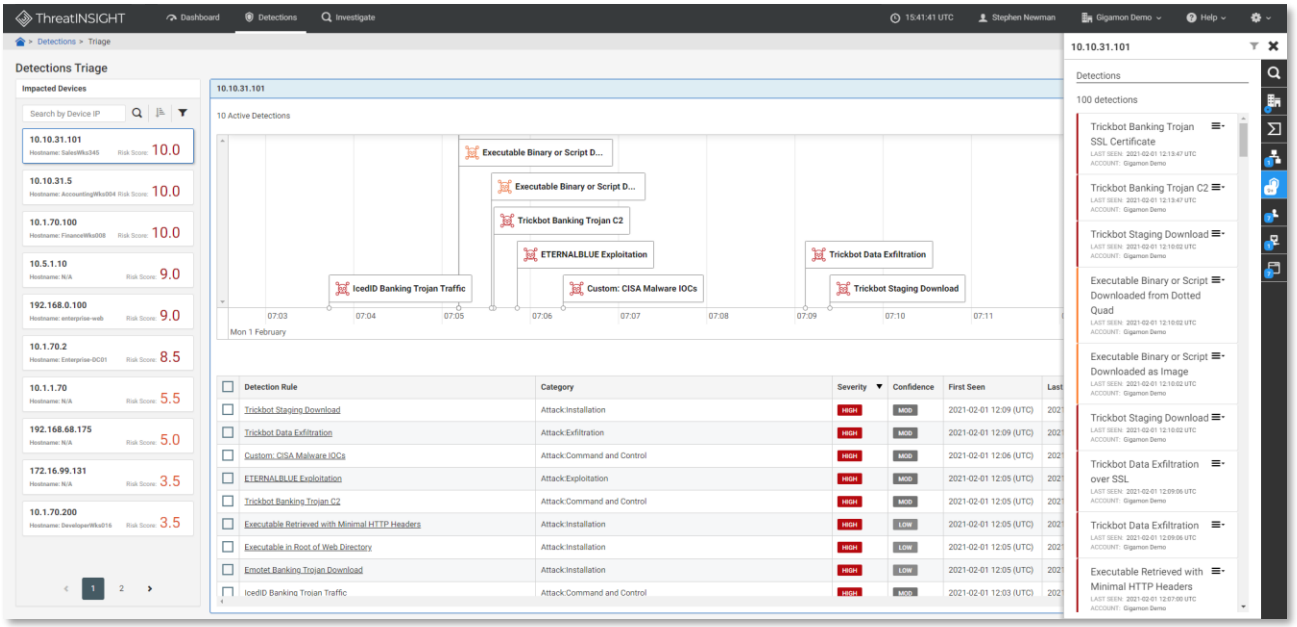
Figure 2. Gigamon ThreatINSIGHT User Portal Dashboard



Source: Enterprise Strategy Group

We selected the top device at risk, 10.10.31.101 (host name SalesWks345). It's important to note that ThreatINSIGHT tracks systems by MAC address to allow them to follow devices when their IP address changes, storing historical context on the entity. Figure 3 provides detection details, including 10 active detections on a timeline and a risk score of 10—risk scores are on a scale of one to 10—which was calculated based on the number of detections, severity of the threat, and confidence of the Gigamon threat research. The panel at the right displayed additional contextual information, including the activity observed on the device, the malware that executed it, the type of host (domain controller, web server, or desktop), the detection rules that were triggered, the severity of the threat, and the confidence level of the detection.

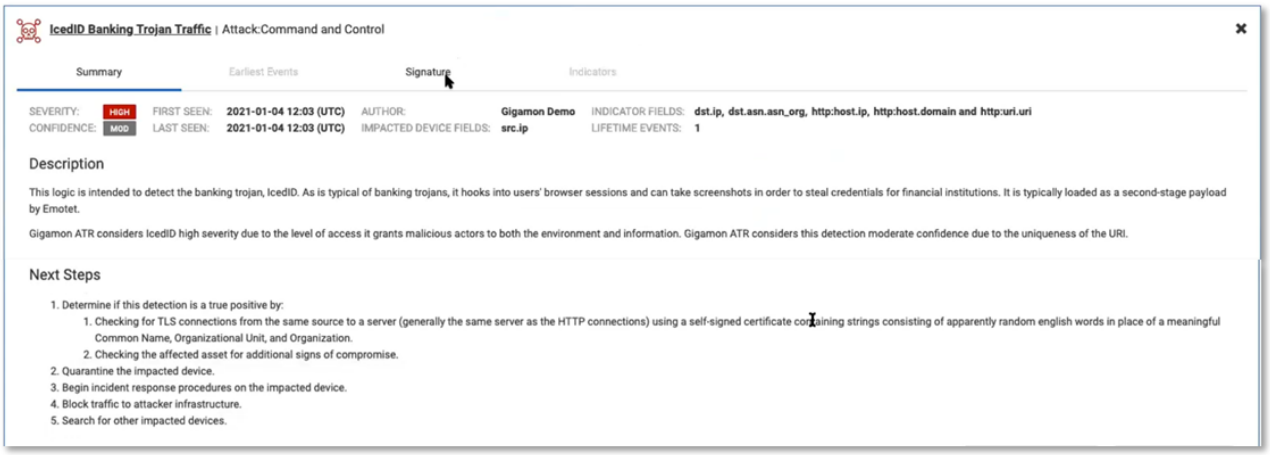
Figure 3. Gigamon ThreatINSIGHT Detections Triage



Source: Enterprise Strategy Group

Then, we selected the first-seen event, *IcedID Banking Trojan Traffic* (see Figure 4). The plain English explanations in the *Description* and *Next Steps* sections made it easy to understand the logic of the supplied research and recommended next steps. In this case, *Next Steps* included directions to determine if the detection was a true positive, quarantine the device, begin incident response procedures, block traffic to the attacker infrastructure, and search for other impacted devices. Overlapping detections, such as a trojan download, an executable binary script download, and others in the timeline in Figure 3 indicated additional potential activity and context. This is also helpful in understanding the evolution of an incident and quickly pivot to better determine its scope and identify other potentially impacted systems.

Figure 4. Gigamon ThreatINSIGHT Detection Details

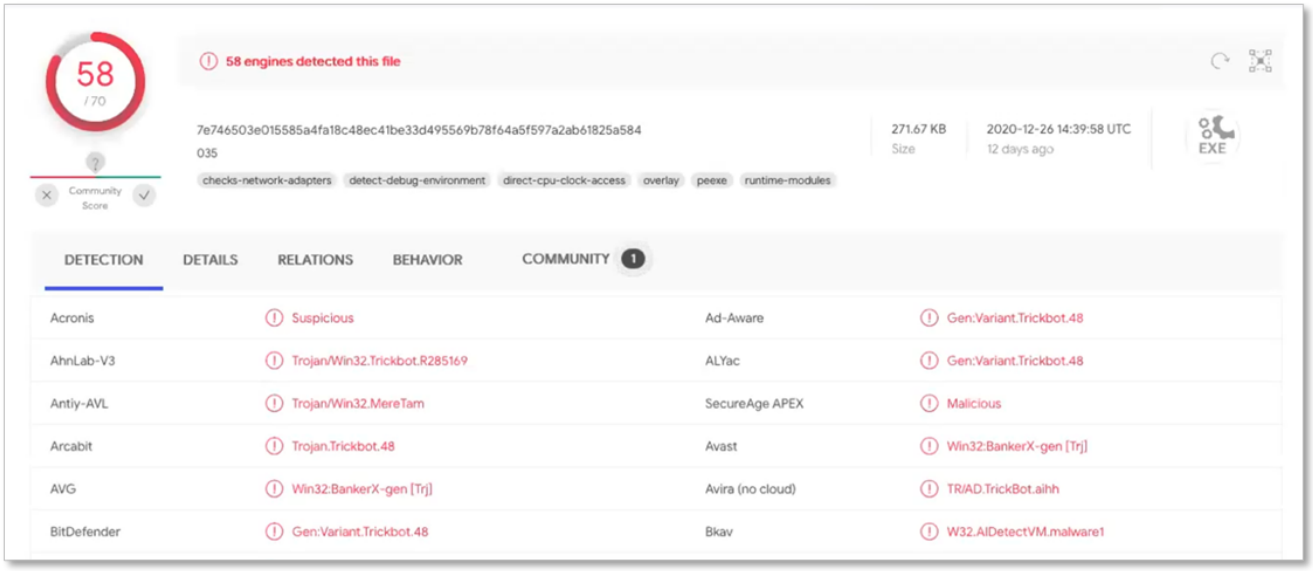


Source: Enterprise Strategy Group

Next, we clicked on *Signature*, which displayed the query language under the hood that showed us what ThreatINSIGHT was looking for and why. We easily applied a custom filter and rules to not show these alerts when they occur in the DMZ network. Another rule we applied was one to prevent devices in one network from talking to another network. Then we looked at the indicators for 10.10.31.101 to capture details useful for reports.

We then searched for information on the destination IP address in the IcedID detection. We saw limited information such as historical threats observed on this device's IP, WHOIS lookups on the destination activity, passive-DNS data, and related information from numerous antivirus scanners and URL/domain blacklisting services all with one click.

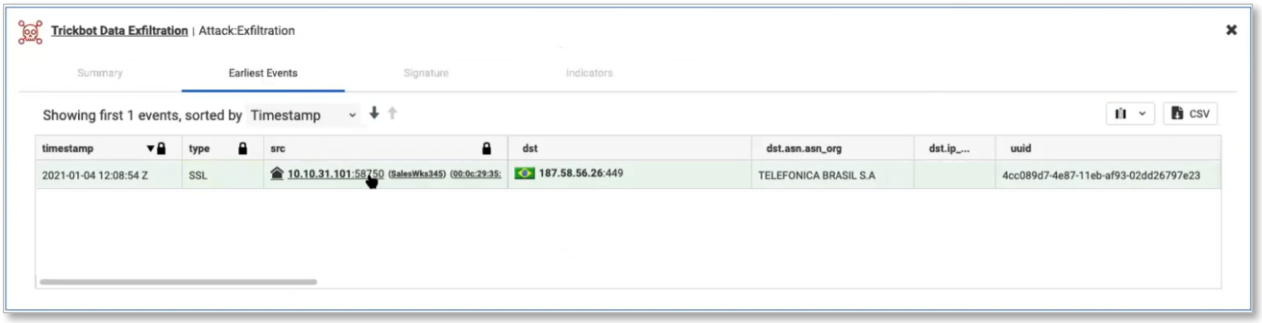
Figure 5. Researching the Destination



Source: Enterprise Strategy Group

After identifying the external IP address, we wanted to know the source and what needed to be addressed. When we clicked on the source IP address, we viewed the DNS information and confirmed that this was a sales workstation (see Figure 6). With one click, we pivoted to detections aggregated over time and saw that this workstation had triggered 91 detections overall.

Figure 6. Investigating the Source

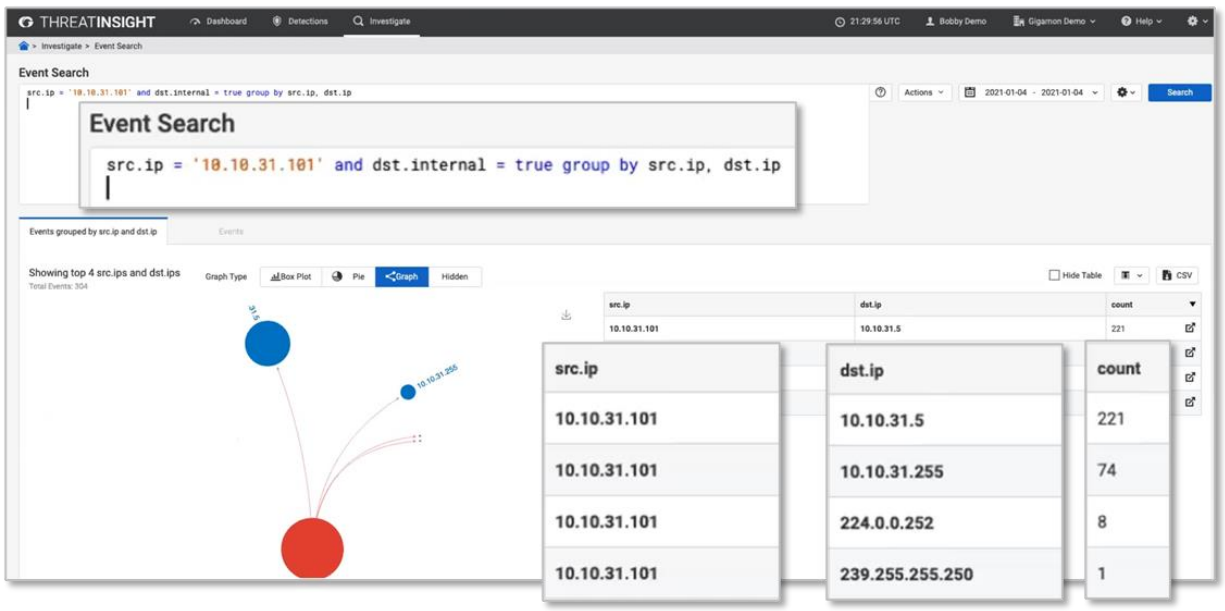


Source: Enterprise Strategy Group

Another click presented accounts being leveraged to access this workstation to help determine who owns the workstation, where it is located, and what unauthorized accounts have accessed it. This level of detailed context is made possible by the type of metadata that ThreatINSIGHT observes from the network traffic. Gigamon refers to this as near-packet-level context, meaning that while they don't write all packets to disk—which would require a tremendous amount of storage and be quite costly to maintain for any length of time—ThreatINSIGHT extracts detailed context from layers one through seven of the stack, makes it available to their customers, and enriches the data with information about the user, their device information, threat intelligence, and passive DNS. All that data is collected, aggregated, and indexed so that users can search, pivot, and respond effectively.

A drill-down into *Event Search* allowed us to initiate an investigation with a targeted search. There are multiple prebuilt queries, but we entered our own using the INSIGHT query language (IQL). The query (see Figure 7) provided information useful to understanding the internal movement of the threat.

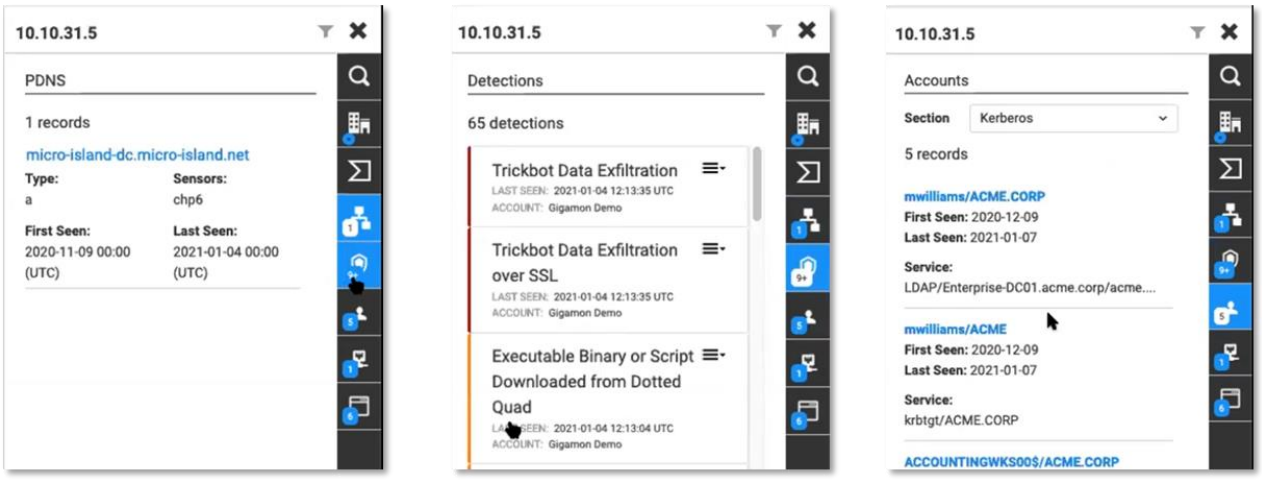
Figure 7. Targeted Event Search



Source: Enterprise Strategy Group

We saw a lot of traffic between the compromised device and an internal device with address 10.10.31.5. We clicked on *Entity Enrichment*, which identified the device as an Active Directory domain controller (DC), pivoted to detections, saw that the DC was compromised with the same malware as the source machine, and identified which user and service accounts were being used to access it (see Figure 8).

Figure 8. Gigamon ThreatINSIGHT

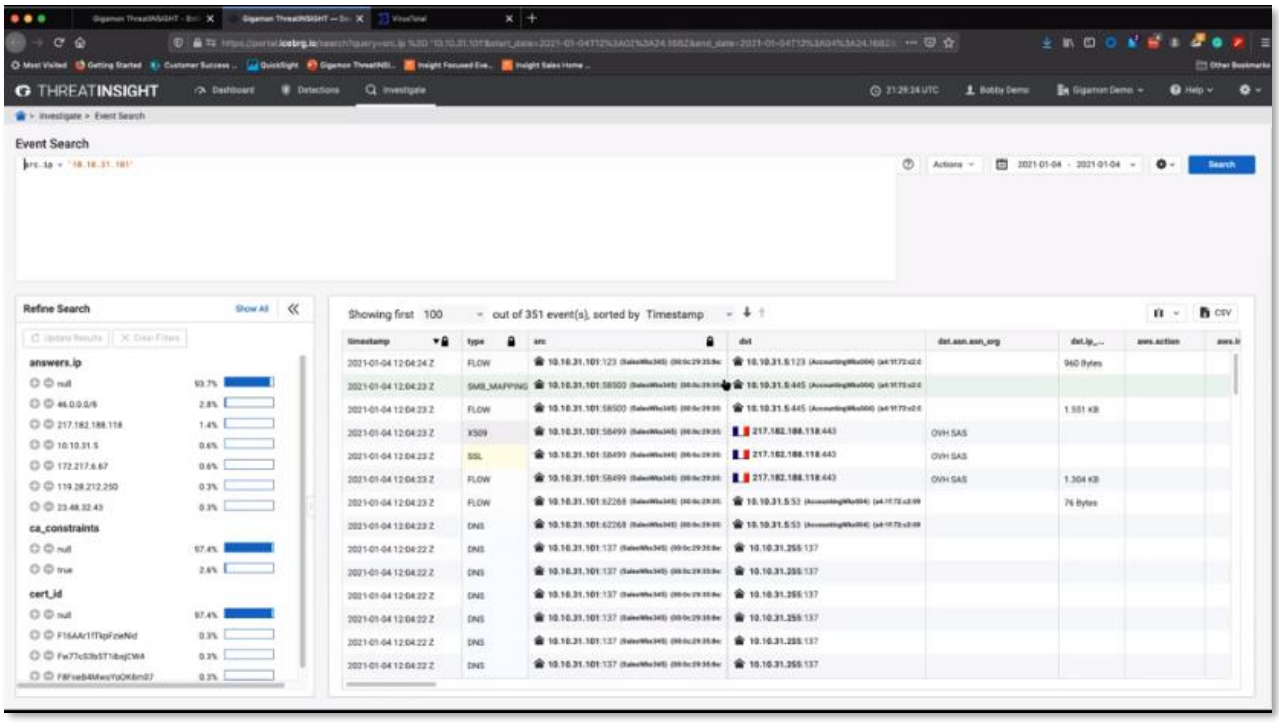


Source: Enterprise Strategy Group

Next, we returned to the targeted search to zero in on root cause. This step opened up a new tab, where we saw activities, such as SMB mapping and file transfers, as shown in Figure 9. Further investigation into an expanded timeframe and additional metadata fields quickly flagged activity that could be considered problematic and allowed us to collect detailed context. These steps, along with some basic correlation, were accomplished within a couple of minutes.

We reviewed the information we could see without decrypting the SSL traffic, noting the target IP address and network activity that was being masked as SSL traffic. Then, we focused on the device itself by targeting a specific timeframe. Here we noted that the raw packet was pulled in and run against sensor analysis before the data was sent to the ThreatINSIGHT backend for correlation. We did not have to wait for or rely on Netflow or do a full-packet capture, although ThreatINSIGHT does support selective packet capture if users want to capture the full-packet.

Figure 9. Events Associated with an Incident



Source: Enterprise Strategy Group

We completed a few more investigative actions based on the recommended next steps, including forensically fingerprinting the file. At the same time, we confirmed that the threat actor tactics and techniques were the same across devices, eliminating duplicate research efforts. We were impressed by ThreatINSIGHT's ability to track down persistent threats, keep analysts on productive paths of inquiry, and document findings that could be copied into a report.

Finally, we observed the integration with security solutions such as Cisco SecureX and Splunk that allow analysts to carry out in-depth incident response actions with one click.

Why This Matters

Network security has become more difficult, and risk mitigation continues to get harder. To compensate for gaps in security solutions like endpoint detection and response (EDR) and security information and event management (SIEM), many organizations implement on-premises NDR. But on-premises NDR involves onerous deployment, training, and management. Visibility is limited. Most focus on detection of on-premises activity and do not include investigation or threat hunting options, the absence of which likely extends mean time to detect (MTTD) and mean time to respond (MTTR).

A Guided-SaaS NDR, Gigamon ThreatINSIGHT simplifies deployment and use. ESG validated that it provides comprehensive visibility, threat detection, situational context, and incident response, including triage, investigation, and threat hunting.

With a few clicks, ESG identified a potentially compromised device, investigated the incident, extracted context, and completed the recommended next steps to resolve and report on the incident. We were impressed with the way the tool focused on "what is most important now" and the experience of fast and efficient investigation and response.

Gigamon ThreatINSIGHT demonstrated three capabilities sought after by cybersecurity teams: efficiency, effectiveness, and expertise.

The Bigger Truth

Network security is getting harder, even as collaboration across IT improves. Nearly nine-out-of-ten organizations report that network security has become more difficult than it was two years ago. While the majority of organizations report that the day-to-day collaboration between networking and IT security groups is good, issues remain due to the fact that these groups are ultimately siloed.

While organizations cannot control the threat landscape, they can reduce network and cybersecurity complexity. ESG testing revealed that Gigamon ThreatINSIGHT enables organizations to quickly deploy and integrate an efficient, effective Guided-SaaS NDR platform for defense-in-depth protection of their critical assets. Organizations not only gain visibility into their networks but also obtain the context that helps analysts detect and neutralize real threats while minimizing false positives—an operational advantage that can help organizations lower risk and keep up with security as they cope with hybrid workforce models, data regulations, and digital transformation. A notable risk-reducing capability is that in the event a sensor or network goes offline, ThreatINSIGHT continues to ingest data, holds it for several days, and time-tags it so customers can follow the incident's timeline to support investigation and response.

The findings presented in this Technical Review are based on remote testing in a controlled environment. Due to many network variables, it is important to conduct your own testing to validate desired outcomes. ESG believes that Gigamon's partnership philosophy and integrations with leading security solutions can provide organizations with desirable advantages.

ESG believes that this solution overcomes the limitations of traditional on-premises NDR approaches and that it can significantly improve the productivity of cybersecurity analysts, strengthening organizations' security postures. With ThreatINSIGHT, Gigamon has expanded not just their offering, but also their role; no longer just a comprehensive network visibility/monitoring plane provider, Gigamon is now a serious cybersecurity player. Organizations would be smart to explore Gigamon ThreatINSIGHT if they are interested in automating the repetitive, tactical activities that consume their security teams today and moving toward a proactive, intelligence-led model of protection.