Threat Detection Methodologies

It’s a unique challenge to detect active threats in a network. Separating network communications associated with real threats from benign behavior requires threat detection methodologies that prioritize detecting artifacts and indicators that cannot easily be hidden, such as procedures, tactics and techniques. In addition, these methodologies must emphasize high detection rates while generating low noise and fewer false positive alerts. Gigamon has developed a unique and highly effective approach toward balancing this difficult endeavor.

Our Approach

Gigamon ThreatINSIGHT takes a data-centric approach to detecting threats across both inbound and outbound (north/south) and internal (east/west) network communications.

Traffic is collected through physical or virtual sensors that perform deep packet inspection (DPI) and aggregate metadata generated from the inspection. Once relevant information is extracted from network flows, the sensors pass the information into the INSIGHT Cloud Data Warehouse, where the metadata is indexed and enriched with information from sources such as WHOIS and first- and third-party threat intel feeds. Domain names extracted from flows, for example, are compared against enriched data. Those that match known command and control (C2) sites are identified with relevant data stored and indexed.

After the data is correlated and enriched, ThreatINSIGHT leverages the strengths of machine learning (ML), coupled with the experience of Gigamon Applied Threat Research (ATR) to provide transparent, high-quality, actively managed detections based on threat actor tactics and procedures. ATR is a team of specialized data scientists, threat researchers, red team specialists, forensics experts and incident responders acting as customer zero.

WE STUDY ATTACKERS SO YOU GET THE BEST DETECTIONS

ThreatINSIGHT focuses on the detection of threat tactics, techniques and procedures attackers use to move through your network. Why? The tools attackers use may change from attack to attack, but the tactics and techniques they use do not.

WE SHARE THE IMPORTANT DETAILS SO YOU CAN ACT

Our transparent detection logic provides full details and recommended next steps so you can effectively triage and respond to alerts and avoid guessing the why behind the alert.

WE ACTIVELY MANAGE AND CURATE DETECTIONS TO BOOST PERFORMANCE

ATR analyzes threat activities observed globally and within our customer base to maximize quality while minimizing excessive alerting and prevents out of date rules.

Detection Development

Gigamon ATR extensively researches and emulates threat behaviors to understand threat-behavior artifacts. They use the information acquired to develop network-based detection methodologies that prioritize high fidelity and low noise. ATR creates new detection methodologies based on 1) research findings that prioritize multi-vector attacks associated with sophisticated threat actors, 2) trends observed in threats at large and 3) general emphasis on potentially exploitable weak areas of a device on a network.

To provide comprehensive threat coverage, ATR focuses on the following:

+ **DETECTION OPPORTUNITY**
  Research is conducted and information gathered

+ **THREAT EMULATION**
  Threats are emulated and artifacts are gathered

+ **BEHAVIOR ANALYSIS**
  Artifacts are analyzed and detection capabilities are created

+ **TESTING**
  Detection capabilities are staged and tested

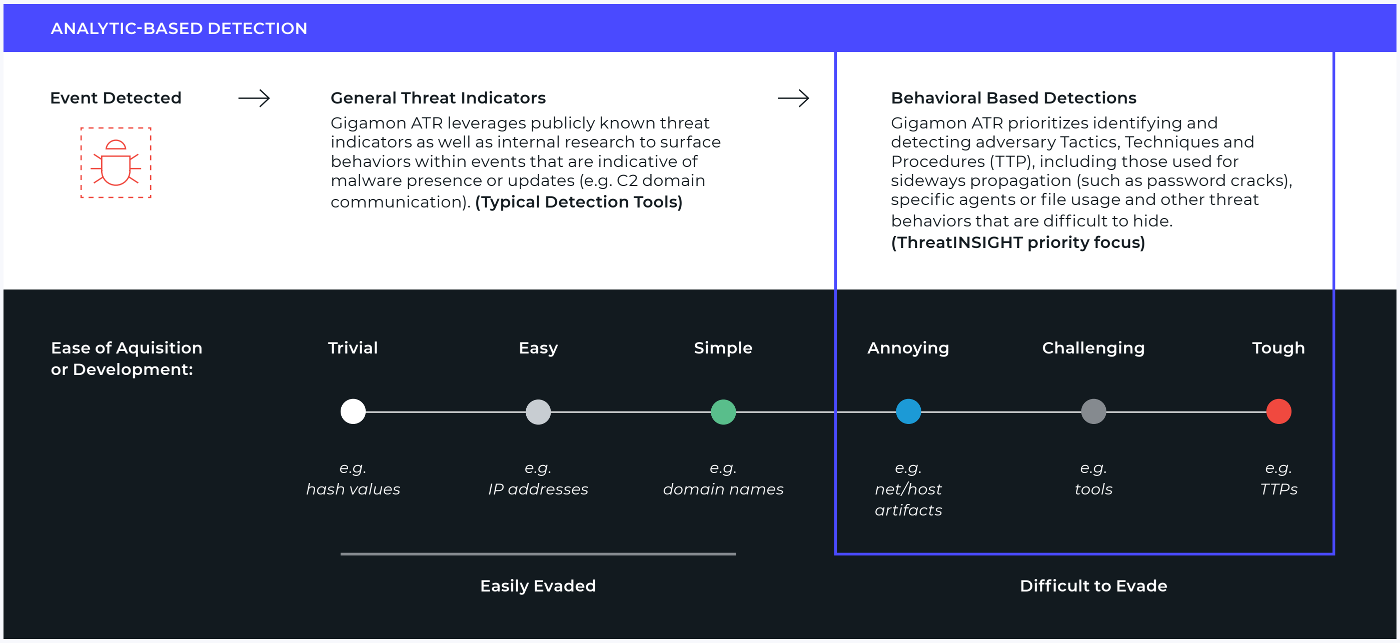
+ **DEPLOYMENT & QUALITY CONTROL**
  Detection capabilities are deployed and are monitored over time to ensure quality

Detection Methodologies

Once an attack is isolated, Gigamon ATR identifies ways to provide the best detection coverage against attacks by focusing on the spectrum of detectable behaviors, ranging from threat- or campaign-specific intelligence to abstract, tactics-based detection. When ATR can map discovered artifacts to specific threat actor groups, they attribute the artifacts to those groups. Many threat artifacts, however, are associated either with multiple threat groups or are artifacts that simply should not be present in a secure network.

Each set of detection logic overlaps with other behaviors, enhancing confidence in the detection if multiple detection rules catch a behavior. Overlapping rules across the spectrum of specificity, that use different detection tactics, results in a higher level of detection quality with lower noise. Gigamon ATR continually assesses rule effectiveness, and dynamic updates to the rules avoids stale detection methodologies.

Gigamon ATR Detection Methodology



ANALYTIC-BASED DETECTION

Event Detected →

General Threat Indicators
Gigamon ATR leverages publicly known threat indicators as well as internal research to surface behaviors within events that are indicative of malware presence or updates (e.g. C2 domain communication). **(Typical Detection Tools)** →

Behavioral Based Detections
Gigamon ATR prioritizes identifying and detecting adversary Tactics, Techniques and Procedures (TTP), including those used for sideways propagation (such as password cracks), specific agents or file usage and other threat behaviors that are difficult to hide.
(ThreatINSIGHT priority focus)

Ease of Aquisition or Development:

Trivial	Easy	Simple	Annoying	Challenging	Tough
e.g. hash values	*e.g. IP addresses*	*e.g. domain names*	*e.g. net/host artifacts*	*e.g. tools*	*e.g. TTPs*

Easily Evaded

Difficult to Evade

Source: *David Bianco, SANS Institute: https://bit.ly/PyramidOfPain*

CONCLUSION

ATR has attained threat expertise through extensive research, experience as adversaries within red teams and work with clients across all verticals as an extension of their security teams. This gives us an in-depth comprehension of threat actor tactics that we pass on to you via effective threat detection within ThreatINSIGHT, resulting in the time savings, efficiency and agility needed to combat today's sophisticated threats.

WHY GIGAMON?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network. The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organizations around the world.

Take ThreatINSIGHT for a test drive, visit gigamon.com/demo.

Gigamon®

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