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 a threat detection methodology that prioritizes detecting artifacts and indicators that cannot easily be hidden, such as advanced threat actors' tools, tactics and procedures. This methodology must emphasize high detection rates while generating low noise and fewer false positive alerts. The Gigamon ThreatINSIGHT Applied Threat Research (ATR) team has developed a unique and highly effective approach toward balancing this difficult endeavor.

Our Approach

Gigamon ATR 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 third-party sources and 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, Gigamon ThreatINSIGHT leverages the strengths of machine learning (ML), coupled with the experience of Gigamon 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 working to dismantle the ability of an adversary to impact Gigamon customers.
Gigamon ATR Detection Methodology

### Analytic-Based Detection

<table>
<thead>
<tr>
<th>Event Detected</th>
<th>General Threat Indicators</th>
<th>Behavioral Based Detections</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td>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)</td>
<td></td>
</tr>
</tbody>
</table>

#### Ease of Acquisition or Development:

- **Trivial** (e.g. hash values)
- **Easy** (e.g. IP addresses)
- **Simple** (e.g. domain names)
- **Annoying** (e.g. network artifacts)
- **Challenging** (e.g. tools)
- **Tough** (e.g. TTPs)

#### Easily Evaded vs Difficult to Evade

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

---

**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 FOR FASTER RESPONSE**

Our transparent detection logic provides full details and recommended next steps so you can effectively triage, investigate, and respond to alerts.

**WE ACTIVELY MANAGE AND CURATE DETECTIONS AND OBSERVATIONS TO STREAMLINE INVESTIGATIONS**

ATR analyzes threat activities observed globally and within our customer base to ensure our detections and observations are high-fidelity while reducing needless false positives.
Detection Development

Gigamon ATR extensively researches and emulates threat behaviors to understand threat-behavior artifacts. ATR creates new detections 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 device vulnerabilities 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

+ **BEHAVIORAL 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. This ranges from threat—or campaign—specific intelligence to abstract, tactics-based detections.

Each set of detection logic overlaps with other behaviors, enhancing confidence in the detection if multiple detection rules catch a behavior. Gigamon ATR continually assesses rule effectiveness, and dynamic updates to the rules avoids stale detection methodologies.

Attribution

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.

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 offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide.

To learn more, please visit [gigamon.com](http://gigamon.com).

---

**Take ThreatINSIGHT for a test drive, visit [gigamon.com/demo](http://gigamon.com/demo).**