CrowdStrike Falcon Platform and Gigamon ThreatINSIGHT

Seamless Net-to-End Visibility and Detection to Stop Attackers in Their Tracks

Without in-depth visibility into device activity and network traffic to identify adversary behaviors, security teams are at a loss to defend against cyberattacks. Aggregation of logs and alerts from frontline security tools don’t provide SOC and IR teams the context necessary to effectively detect and respond to attackers who have already bypassed those same tools. Security teams seeking to address this SOC visibility gap and increase effectiveness have turned to network detection and response (NDR) and endpoint detection and response (EDR) solutions to establish the foundational visibility necessary to combat adversaries; however, not all NDR and EDR integrations provide the same level of integration, visibility, and detection.

Gigamon has partnered with CrowdStrike to provide users with a fully unified detection and response solution for active threats. As cyberattacks escalate in speed and sophistication, defenders need tools that help them stay ahead. The seamless cloud-to-cloud integration between Gigamon ThreatINSIGHT and the Falcon platform ensures the right data is available at the right time to the right people from within the ThreatINSIGHT web portal.

- Falcon X threat intelligence is applied against real-time network traffic for immediate detections
- Falcon Insight detections appear alongside ThreatINSIGHT machine learning and threat intelligence detections for fast adversary identification
- Falcon Insight endpoint telemetry appears alongside the ThreatINSIGHT solution’s L2 – L7 network telemetry to speed triage, hunting, and investigations
THE CHALLENGE
Gaps in SOC visibility allow adversaries to persist, escalate privileges, move laterally, and exfiltrate data or cause damage, whether it be ransomware or a data breach.

THE SOLUTION
To optimize effectiveness, ThreatINSIGHT NDR integrates with the Falcon platform, delivering seamless net-to-end visibility, combined threat intelligence, behavioral threat detection, and the tools and telemetry to stop attackers in their tracks.

JOINT SOLUTION BENEFITS
+ Close the SOC visibility gap with in-depth host and L2–L7 network telemetry in a single console
+ IoT, BYOD, and unmanaged host visibility for devices where Falcon is not present
+ Indicate if host has Falcon agent present
+ Correlated Gigamon and CrowdStrike ML and threat intel for quicker detections
+ Efficient, effective access to data and tools for hunting/investigation within a single platform
+ Contain compromised endpoints in real time from within ThreatINSIGHT
+ Distraction-free, cloud-to-cloud integration, with zero maintenance
The power of the CrowdStrike EDR/Gigamon NDR integration is twofold: It provides SOC and IR teams unparalleled, in-depth visibility and is a customer-inspired, feature-rich integration to combat adversaries.”

– MICHAEL DICKMAN, GIGAMON CHIEF PRODUCT OFFICER
<table>
<thead>
<tr>
<th>SCENARIOS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical Capabilities</strong></td>
</tr>
<tr>
<td>Avoid multi-vendor headaches</td>
</tr>
<tr>
<td>Close SOC visibility gaps</td>
</tr>
<tr>
<td>Achieve IoT, BYOD, and unmanaged device visibility</td>
</tr>
<tr>
<td>Faster threat intelligence detections</td>
</tr>
<tr>
<td>Behavioral detection corroboration</td>
</tr>
<tr>
<td>Hunting and incident investigations</td>
</tr>
<tr>
<td>Host management</td>
</tr>
<tr>
<td>Host isolation</td>
</tr>
</tbody>
</table>
Conclusion

Focused on enabling and empowering joint customers to detect and respond with certainty, the ThreatINSIGHT, Falcon Insight, and Falcon X products combine to provide a fully unified NDR and EDR integration to close the SOC visibility gap and dismantle adversaries.

For more information on Gigamon ThreatINSIGHT and CrowdStrike, please visit:

GIGAMON.COM/THREATINSIGHT  |  CROWDSTRIKE.COM

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 enjoy industry-leading customer satisfaction with more than 3,000 organizations around the world.

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