MARSH

Cyber Catalyst by Marsh

Gigamon®

Gigamon ThreatINSIGHT™ — Cyber Catalyst 2020 Designation

Today's information security and incident response teams often struggle with advanced threats because they can't see what is happening on the network, in the cloud, or with remote users. And as rapid cloud migrations and work-from-home practices continue, these visibility challenges increase. Security teams require technologies that detect threats within all communications – inbound, outbound, lateral, cloud and remote user activity – and provide high-fidelity alerts.

Gigamon ThreatINSIGHT is built to address these needs, providing rapid detection of threat activity and tools for effective investigation of suspicious behavior.

The ThreatINSIGHT solution is a cloud-native, high-velocity network detection and response solution built by responders for responders for the rapid identification, investigation, and mitigation of threat activity. It improves Mean time to Detect (MTTD), Mean time to Respond (MTTR), and Dwell time – the time an attacker has access to an organization's environment. And it drives certainty when making security decisions through providing a combination of high-fidelity alerts and quick access to corroborating information. By providing full visibility and contextual information, a security team can accelerate their ability to respond effectively.

ThreatINSIGHT helps organizations:

- Get ahead of investigating suspicious behavior, proactively hunt for potential threats, and direct a fast and effective response, thus lowering risk.
- Prioritize what matters through high-fidelity detections and reduced mean time to detection and response.
- Investigate in real time by quickly triaging alerts and gathering knowledge of the threat actor's activity to direct efficient and effective response efforts.
- Gain broad situational awareness across physical, virtual, and cloud networks along with WFH users through third-party integrations.
- Focus teams on threats, not the management of tools, and act faster with the plug-and-play deployment and zero-maintenance ease of a being supported by a SaaS-solution.
- Improve overall security posture, expand use cases, and align to industry best practices with the support of the Technical Success Management team which consists of seasoned incident response practitioners.

**Product information provided by Gigamon*

For more information on Gigamon ThreatINSIGHT, visit www.gigamon.com/threatinsight.

MARSH & McLENNAN COMPANIES

Why Gigamon ThreatINSIGHT is a 2020 Cyber Catalyst Designated Solution

ADDRESSES A TOP 5 CYBER RISK:

The 2020 program encouraged the submission of solutions that targeted the top five cyber risks identified by participating insurers: ransomware, supply chain/vendor management, cloud migration/management, social engineering, and privacy regulation/data management.

Gigamon ThreatINSIGHT specifically targets privacy regulation/data management, but also has wider utility and applicability in addressing other types of cyber risk.

INSURER RATINGS AND COMMENTARY

Cyber Catalyst participating insurers rated Gigamon ThreatINSIGHT highest on the criteria of efficiency, cyber risk reduction, and differentiation.

In their evaluation, the insurers commented:

- "Powerful tool when configured and operated correctly. It can provide a significant reduction of risk: clear triage and mitigation dashboard and lack of blackbox security product. Companies with more mature cyber operations would benefit."
- "Platform provides granular level insight on inbound, outbound, and lateral movement and connections by threat actors. Good threat intelligence features, including information about discrete network transactions and anomalous behaviors."
- "Many capabilities and a ton of features to help sort and filter information. The techniques used to gain insight into threat information are balanced in terms of detection methods. Pivoting through the system is easy with the overall product flow. A great solution for a more experienced analyst, enabling them to produce useful reporting information."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst designated products and services in accordance with certain "implementation principles" that have been developed by the insurers and product vendors.

The implementation principle for Gigamon ThreatINSIGHT is:

- There is an individual designated within the organization to monitor activity and escalate critical findings to key stakeholders. The product is implemented broadly across critical assets.

Evaluation Process

Applications for evaluation of cybersecurity products and services were accepted from March 10 to May 15, 2020. More than 90 offerings, spanning a broad range of categories, were submitted.

Solutions that targeted the top 5 cyber risks identified by participating insurers were encouraged: ransomware, supply chain/vendor management, cloud migration/management, social engineering, and privacy regulation/data management.

The insurers evaluated eligible solutions along six criteria:

1. Reduction of cyber risk.
2. Key performance metrics.
3. Viability.
4. Efficiency.
5. Flexibility.
6. Differentiation.

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight insurers, which voted independently. Marsh did not participate in the Cyber Catalyst designation decisions.

More Information

The next Cyber Catalyst program will occur in 2021.

For more information on the 2020 Cyber Catalyst designated solutions, or the 2019 class of Cyber Catalyst solutions, visit the Cyber Catalyst pages on the Marsh website: www.marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit www.marsh.com, or contact your Marsh representative.