Fortify Threat Detection and Response with Gigamon and Vectra AI

Introduction

The current state of cyberattacks has changed. Despite a strong perimeter defense with next-generation firewalls (NGFWs), an intrusion detection system (IDS), and malware sandboxes, cyberattackers will still get into your network and adapt to infiltrate even the toughest defenses. Without visibility into the network, detecting and mitigating these cyberattacks is nearly impossible.

Gigamon and Vectra AI provide a joint solution that fortifies threat detection and response by simplifying access to critical traffic from an infrastructure.

The Gigamon Deep Observability Pipeline lets you access East-West traffic across hybrid cloud infrastructure and sends the packets simultaneously to all tools. This centralized approach to accessing visibility lets you efficiently monitor and secure lateral, East-West traffic.

Gigamon also uses deep packet inspection to extract insightful metadata from accessed traffic. Teams use these capabilities to understand the applications currently communicating in East-West traffic and filter out low-risk traffic from the stream sent to tools.

This creates the opportunity to establish security postures that simplify access to critical intelligence, limit the creation of blind spots, and focus resources on only high-risk traffic.

Vectra AI receives traffic from Gigamon and automatically detects cyber threats hidden in approved applications and encrypted traffic, correlates those threats to the hosts that are under attack, and delivers unique context about what attackers are doing, enabling security teams to quickly prevent or mitigate damage.

Challenges

Teams are challenged by a myriad of different obstacles including:

- Constantly evolving infrastructures that create visibility blind spots
- Noisy dashboards that lead to information overload
- Cost of effective, East-West visibility
- Inability to address new security risks and methods since prevention systems like NGFWs use signatures and reputation lists that can only detect known threats
- Lack of visibility into network infrastructures
- Overwhelming amount of alerts and logs from legacy security technologies that bog down SOC analysts
- Dependence on logs, which provide only a limited view into what is occurring
- Reliance on outdated security systems due to inconsistent organizational investments

The Solution

The Gigamon Deep Observability Pipeline communicates with taps sitting across an infrastructure to access East-West traffic. Physical taps are used within physical data centers. Virtual taps are used in virtual environments like private cloud, public cloud, and containers.

Once East-West traffic is accessed by taps, a copy of the traffic is taken and sent to either GigaVUE HC Series appliances in physical data centers or mirrored to GigaVUE® V Series visibility nodes in virtual environments for aggregation, deep packet inspection, and traffic filtering.

The GigaVUE HC Series appliances and the visibility nodes are then programmed to simultaneously present customized, filtered streams of intelligence to each tool being used for monitoring and security in a team's stack.

Once the Vectra AI Platform receives its customized stream of intelligence from Gigamon, it is automatically correlated with detected threats and prioritized on the user interface.

Key Features

- Extract metadata from accessed traffic close to 6,000 L4–L7 application-related attributes to create customized streams of metadata intelligence
- Centralized visibility into all lateral, East-West traffic across on-premises, virtual, public cloud, and container environments
- Simplified delivery of network-derived intelligence totools
- Observability into the applications currently communicating in your network
- Combined data science, machine learning, and behavioral analysis to detect all phases of a cyberattack
- Over 90 percent coverage of relevant MITRE and ATT&CK techniques

Key Benefits

Here are a few security use cases enabled by the joint Gigamon–Vectra AI solution:

- **Complement log usage:** Combine intelligence received from logs with metadata extracted from network traffic to create dashboards that provide deep insights
- **Pinpoint applications and protocols:** Gain an understanding of known and unknown applications and protocols currently communicating in your infrastructure, including crypto mining, non-standard port usage, FTP, SMBv1, and NTP
- **Simplify implementation:** Bypass an intermediary to feed network traffic into the Vectra AI Platform with Gigamon Deep Observability Pipeline

- **Real-time network visibility:** Detect in-progress cyberattacks on physical and virtual networks and respond with confidence and speed
- **Fortify secure posture:** Strengthen your existing security posture by complementing your current use of logs with application intelligence use cases, such as observation of lateral movement, geographic location of source and destination of traffic, vulnerable systems, and compute that can be targeted by malware

Summary

Gigamon plus Vectra AI helps you gain a deeper understanding of what is occurring in your infrastructure to mitigate security issues faster.

Teams can now adequately address current challenges that impede them from creating an effective security posture by implementing a joint solution that gives them complete visibility, a deeper understanding of what is occurring, and an automated, AI-driven approach toward addressing security risks.

Put your organization in control even as infrastructures become more complex and threat actors become more sophisticated.

About Vectra

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

For more information on Gigamon and Vectra please visit
Gigamon.com | Vectra.com

Gigamon®

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

08.24_01