Vectra and Gigamon Provide Rapid Detection of Supply Chain Attacks
Rapidly Detect and Stop Attacks by Analyzing Network Activity Across All IT Operations

THE CHALLENGE
+ 100 percent network visibility
+ Network traffic aggregation
+ Rapid attack detection on trusted supply chain software

THE SOLUTION
+ Gigamon Visibility and Analytics Fabric™
+ GigaSMART applications
+ Vectra Cognito Platform

JOINT SOLUTION BENEFITS
+ Eliminate cybersecurity monitoring blind spots
+ Automated detection of cyberthreats hidden in approved applications
+ A more effective approach to defend against this class of attack

SolarWinds Orion and Detecting New Supply Chain Threats

Supply chain attacks pose a great risk against federal networks. Unprotected federal departments and branches have suffered a severe breach with the trusted SolarWinds Orion application being weaponized against them in a new type of supply chain attack. What other trusted application are vulnerable? And how can agencies enable early detection of this new type of attack?

Vectra provides rapid detection and response by examining behavior on the network to detect changes in application communications, while Gigamon provides Vectra with visibility into data-in-transit across all IT operations, including cloud and virtualized infrastructure, to eliminate monitoring blind spots.

The Vectra Cognito Platform

The Vectra Cognito Platform automatically detects cyberthreats hidden in approved applications and encrypted traffic in hybrid, on-premise and cloud deployments with learning behavioral models that understand both hosts and identities — tracking and stopping attackers earlier in the kill chain.

By leveraging a unique combination of data science, machine learning and behavioral analysis, it offers real-time early warning and continuous visibility across the attack progression from on-premise to cloud — without dependency on indicators of compromise (IoCs), signatures or other model updates. All of this works to identify and stop attacks like SolarWinds before damage is done.

The Vectra Cognito Platform correlates threats to the hosts and accounts under attack, and it delivers unique context about what attackers are doing, enabling security teams to quickly address and mitigate loss.
Gigamon Extends Vectra Visibility Across All IT Operations

The Gigamon Visibility and Analytics Fabric™ (VAF) establishes complete visibility into data-in-transit across all IT operations — physical networks, virtual networks, private and public clouds — eliminating cybersecurity monitoring blind spots. Gigamon collects and aggregates the IP packet-level traffic and applies intelligent processing in real-time, including packet de-duplication, header stripping and application traffic identification and filtering. Gigamon then forwards custom sets of monitoring data to Vectra to optimize Vectra coverage and effectiveness.

The Gigamon VAF can be deployed using physical chassis/taps or as a 100 percent virtual solution in AWS, Microsoft Azure, Google or OpenStack-based clouds, or within a micro-segmented environment on the network, such as VMware, Nutanix, Kubernetes, IBM/RedHat or Cisco ACI. The instantiation of visibility, data aggregation, processing and forwarding is controlled from the GigaVUE-FM fabric manager interface.

Gigamon Extends Vectra Visibility Across All IT Operations

Gigamon VAF

Countering the attack on SolarWinds Orion with Vectra and Gigamon

The hack on SolarWinds Orion demonstrates the utility — and necessity — of network monitoring when taking steps to detect breaches that have bypassed preventative security and to protect data. Network-based technologies are critical when countering the increasing sophistication of threats. Preventative security and endpoint controls, while raising the bar, are insufficient, and legacy, signature-based systems have again been proven ineffective when detecting new attacks where IoCs do not yet exist. Leveraging network detection and response — where the network is defined broadly as everything outside of the endpoint — is a more effective approach for defending against this class of attack.

Together, Vectra and Gigamon close the dangerous cybersecurity gap between perimeter defenses and post-breach analysis by providing network visibility and real-time detection of the fundamental actions and behaviors that supply chain attackers perform when they spread and steal inside networks. This gives IT security teams the speed and agility needed to stop well-funded and deeply motivated threat actors before they cause harm.

For more information on Gigamon and Vectra, visit: www.gigamon.com and vectra.ai.

© 2021 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.