Enabling Network Forensics in Security Breach Investigations

Savvius Vigil integrates with Cisco FirePower NGIPS to store the entire "packet environment" of hundreds, even thousands, of security alerts every day, more than the largest incident response team could investigate.

Enterprises, under constant attack, deploy highly effective systems to detect and prevent security threats. However, not even the most comprehensive and sophisticated security system can prevent all attacks from making it through. When a security incident occurs, investigation into the breach must be timely and comprehensive so you can rapidly understand, contain, and remediate the current issue, and better prevent future ones.

Investigations without access to the original network packets that carried the intrusion are invariably less effective. Network packets carry malware as binaries that, once assembled on an enterprise's server, cover their tracks — altering logs, changing resources, and modifying their identity — as the first order of business.

The challenge enterprises face is that attacks often remain undetected for weeks or months. This lets attacks inflict the most damage while at the same time altering logs and taking other steps to disguise themselves. This means that access to the original intrusion's network packets is vital. Yet the sheer volume of network traffic means that network packets are usually only available for a brief time.

Solution Overview

Savvius Vigil™, a high-performance security appliance, enhances the effectiveness of security breach investigations by storing months of relevant network traffic. One of the techniques Savvius Vigil uses to define "relevant network traffic" is to capture and store network packets around security alerts from prevention and detection systems.

Cisco FirePower® is a Next Generation Intrusion Prevention System which sets a new standard for advanced threat protection. It integrates real-time contextual awareness, full-stack visibility, and intelligent security automation for industry-leading security effectiveness.

Savvius Vigil integrates with Cisco FirePower NGIPS to store the entire "packet environment" of hundreds, even thousands, of security alerts every day, more than the largest incident response team could investigate.

Investigators can use Savvius Omnipeek™, included with Savvius Vigil, to view and investigate the original attack.

savvius Vigil™

Savvius Vigil is a 3U hardware appliance that stores 64 terabytes of packet data and has interfaces for 1 and 10 Gbps networks.

Making network packet data available to security breach investigations requires preparation, and that's where Savvius Vigil comes in.

How it works

Savvius Vigil analyzes all incoming network traffic against alerts from Cisco FirePower NGIPS. Vigil stores all relevant network packets from five minutes before the alert to five minutes after (or a different time range the user defines), as well as conversations with the IP addresses that triggered the alert. The network security team can use these network packets for immediate investigations, and they are stored for later use.

Savvius Vigil includes powerful search capabilities for zeroing in on the packets associated with specific alerts. Once security analysts have identified packets of interest, they can export them into a standard pcap format. Omnipeek forensics software, included with Savvius Vigil, is a superior solution for investigating packets in detail, including examining packet payloads and details of network conversations.

About Cisco

Cisco is the worldwide leader in IT that helps companies seize opportunities by proving that amazing things can happen when you connect the previously unconnected. At Cisco customers come first, and an integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success.

About Savvius

Savvius offers a range of powerful software and hardware products that maintain network performance and enhance security investigations. Trusted by network and security professionals at over 6,000 companies in 60 countries around the world, Savvius packet intelligence delivers intuitive visualization and effective forensics for faster resolution of network and application performance issues. For more information about Savvius Omnipliance®, Savvius Omnipeek®, Savvius Vigil™, and Savvius Insight™, and to learn about Savvius technology and channel partners, visit www.savvius.com.