CISCO FirePOWER

Joint Solution Brief

Performance Management with Effective Threat Prevention

The Challenge

Today's intrusion prevention systems (IPS) are effective at detecting anomalous, and often malicious traffic, but do not provide views of what was occurring on the network before and after an event. This detail is critical for investigating attack origins, identifying compromised data, understanding hacker behavior, and fine-tuning signatures.

Integrated Solution

Security teams that use Cisco FirePOWER Management Console and IPS appliances can now access Observer GigaStor long-term packet capture and analysis right from the existing UI. The integrated workflow takes you from a snapshot view of the FirePOWER-triggered event to replaying the entire attack in full context of all network activity and application conversations. Easily assess what occurred during the event, and how sensitive data was impacted.

Joint Solution Benefits

- Gain context and proof to assess and resolve security issues, inside the IPS solution – with easy access to transaction data.
  - Quickly understand key attack details, how it was perpetrated, phishing messages or exploits sent, and which systems or intellectual property was compromised.
  - Get immediate access to network conversations from within the IPS without learning new interfaces.
- Fine tune and improve signatures by using network traffic to validate intrusions or attacks.
- Reduce investigation time by automating steps and eliminate toggling between two solutions. Find the correct conversations, extract, and begin analysis.
- Apply advanced filtering to drill down to the specific conversations in question, rather than sorting through millions of packets.

Introduction

Network security and threat detection have changed significantly over the past several years. According to a recent study by the Ponemon Institute, mean per-business loss worldwide from cybercrime exceeds $7.7 million annually — a 19 percent increase in just one year. In the U.S. this number jumps to $15.4 million per company.[1]

Not only are the costs of these attacks rising, but the number of successful breaches has also jumped 46 percent in the past four years. Faster detection and remediation of these malicious events can determine in some cases whether a company remains profitable or even survives.[2]

One way that enterprises can stay ahead of these threats is to proactively monitor network resources, capturing and then accessing packets post-event. Network traffic analysis provides additional insight to determine not only where the attack originated, but also what impact it had, or continues to have on the network.

The Cisco FirePOWER and Observer GigaStor Joint Solution

Now you can gain total visibility to everything on your network and at the perimeter, including physical and virtual hosts, operating systems, applications, questionable network behavior, malicious attacks, and more with the Cisco FirePOWER management center and Observer GigaStor from Viavi Solutions.

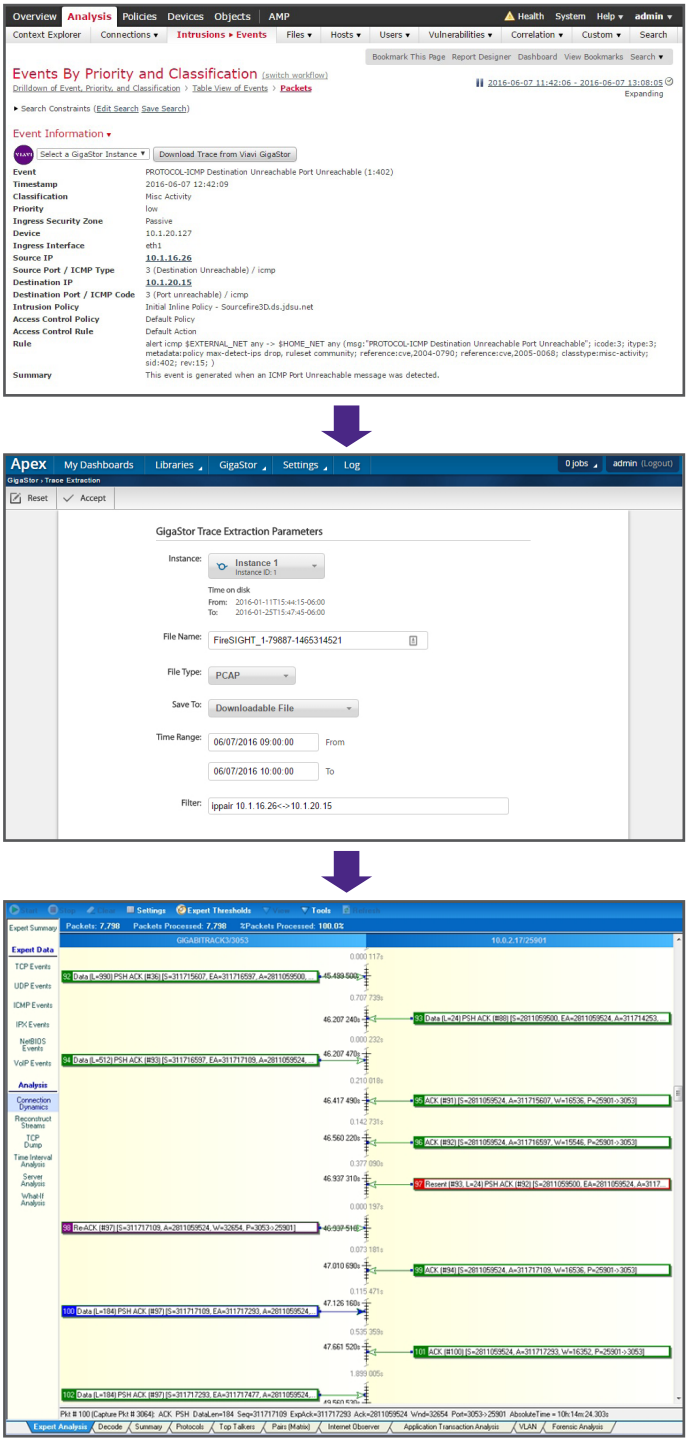
The integration uses REST APIs to create a workflow from the FirePOWER intrusion prevention system (IPS), to the long-term packet capture appliance, GigaStor. When FirePOWER detects a threat, security professionals investigating the potential attack can review network and application traffic specific to their investigation, via GigaStor. This includes all the conversations on the wire before, during, and after an event occurred.

The integration provides teams with a comprehensive, intuitive approach to:

- Network activity and context around the attack
- Improve awareness at the time of an IPS alert with a full record of network activity
- Rule out false positives to save time and zero in on critical issues
- Easily access hard-to-find packet data from a single console

Deploying FirePOWER with GigaStor ensures that the platform has access to all the relevant traffic information that it can effectively use at the time of an investigation. Set triggers, automate troubleshooting, and improve mean time to resolution.

1 http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states
2 http://www.forbes.com/sites/moneybuilder/2015/10/17/an-average-cyber-crime-costs-a-u-s-company-15-4-million/#3a2d22fe1a22



Achieve seamless workflows from FirePOWER security alerts directly to session data and packets in GigaStor. Visualize network and application flows and apply analytics for greater context to investigations.

Benefits of Security Forensics

Security investigations are facilitated by the integration with a focus on improving the time it takes to recognize threats. From the first IPS alert or suspicious event, detailed session conversations can be extracted and analyzed to determine its source. Identifying anomalous traffic and tracking this activity allows both network and security teams to better understand the event, quantify which assets were compromised, and take necessary steps to remediate. This also enables the enterprise to reduce costs associated with large-scale data breaches and diversify IT spends between network and security teams.

Learn More

For more information on the Viavi and Cisco FirePOWER solution, contact:

CISCO FirePOWER

www.cisco.com

www.viavisolutions.com

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you, visit www. viavisolutions.com/contacts.

Firepower-js-ec-nse-ae
30179837 900 0616