Security Forensics with EndaceProbe™ and Cisco Firepower™

Combining Endace network recording with Cisco Firepower's Next Generation Intrusion Prevention Systems (NG-IPS) streamlines investigation workflows for rapid response to security threats.

When it comes to investigating security incidents, access to an accurate, detailed and complete history of network traffic is an unparalleled resource. Detailed packet history provides definitive evidence of what happened, how it happened and what was compromised. It provides the context behind the security alerts raised by Cisco Firepower's NG-IPS and lets analysts investigate events quickly and respond with the confidence of knowing exactly what took place.

Deploying EndaceProbe Network Recorders alongside Cisco Firepower NG-IPS appliances ensures a complete, hi-fidelity history of network activity is immediately available for security investigations. Packets are timestamped to nanosecond level accuracy, ensuring accurate event reconstruction even for ultra-short-lived events.

The Endace Fusion Connector for Cisco Firepower delivers a seamless click-through workflow from security events in the Cisco Firepower Management Console directly to the related network history recorded on EndaceProbes. This streamlined workflow dramatically reduces the time required to investigate and respond to security events, increasing the effectiveness of SecOps teams, lowering costs and improving the security of the enterprise.

Access to a 100% accurate record of network history, and a streamlined investigation workflow, enables SecOps analysts to quickly identify, prioritize and respond to real threats and flag false positives for detection tuning.

Solution Details

Cisco Firepower NG-IPS products provide continuous threat protection before, during and after an attack. The Cisco Firepower Management Console (FMC) is the "nerve center" of the Firepower system. It correlates attacks with real-time network and user intelligence and centrally manages network security and operational functions, including event monitoring, incident prioritization, forensic analysis and reporting. Deploying EndaceProbes and Cisco Firepower NG-IPS side by side at strategic points across the network provides 100% accurate, complete recording of network history at any network speed (1 - 100Gbps).

PRODUCTS

EndaceProbe Network Recorders

Cisco Firepower Management Console

Endace Fusion Connector for Cisco Firepower

BENEFITS

- Accurate, granular and complete network history provides definitive evidence for security analysts
- Streamlined investigation workflow improves SecOps efficiency and ensures faster investigations
- More effective detection tuning reduces false-positives
- Network packets provide a definitive evidentiary trail

FURTHER INFORMATION

https://www.endace.com/cisco-firepower.html

Leveraging the open architecture of the EndaceProbes, the Endace Fusion Connector for Cisco Firepower allows users to select an event in the Firepower Management Console dashboard and drill down instantly to related packet-level network history for analysis. Via the Pivot to Packets integration with Cisco Firepower, EndaceProbes provide single-click access to the network history relating to potential intrusions, allowing SecOps staff to investigate threats quickly and shut them down.

Where analysts need to gain context around an event before conducting packet-level analysis, Pivot to Vision provides single-click access from a Cisco Firepower alert to EndaceVision™, a built-in network visualization tool. Analysts can zoom in to examine a specific subset of the alert data, or zoom out to look at precursor and post event activity. From the visualizations, recorded packets can be analyzed directly, using the built-in EndacePackets™ packet decode application. They can also be downloaded for analysis using Wireshark or other tools, or archived for evidentiary purposes.

Conclusion

Recorded network history provides the high-fidelity packet-level detail necessary for the conclusive investigation of security incidents. The combination of EndaceProbe Network Recorders and Cisco Firepower NG-IPS delivers a powerful, end-to-end detection, alerting and investigation solution. It gives SecOps teams industry-leading security monitoring and alerting, with access to the detailed data they need for fast, conclusive threat investigation and response.

How it works

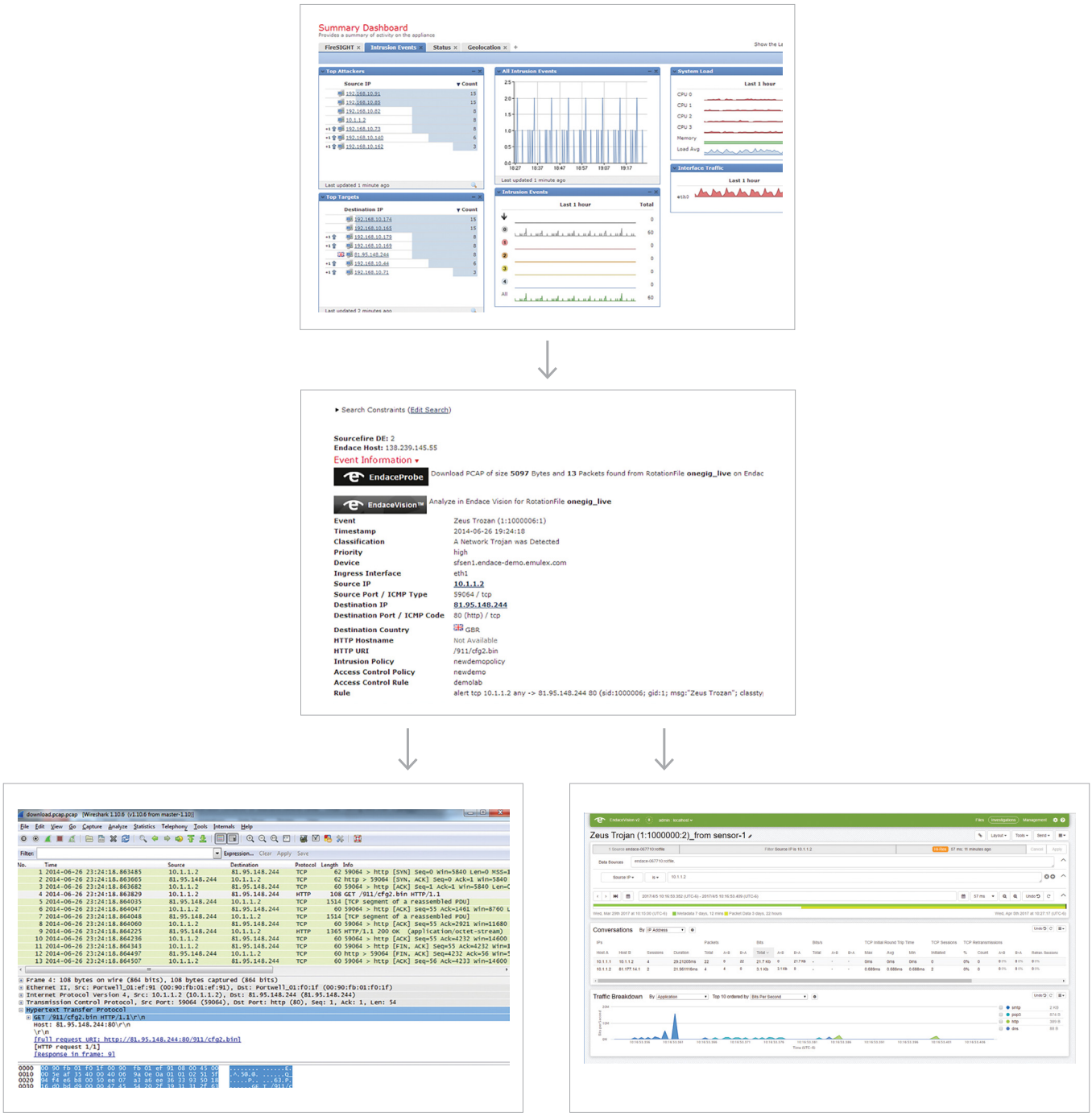

Figure 1 - Streamlined workflow from an alert in the Cisco Firepower console, to the alert detail, to related packets or network visualizations.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com