Solution Brief

Symantec Technology Integration Partner: HP

Business Challenge

A threat event is often just the start of an intense incident response process. When such an event occurs, the security team must move quickly to verify a compromise, prevent malware propagation, and most importantly, block extraction of sensitive data. However, taking such action requires more context than is typically included in the records of the HP ArcSight Enterprise Security Manager (ESM). How was the user manipulated into clicking a malware link? After the download, did the client connect to a botnet and was sensitive data leaked? Quickly understanding what happened before, during, and after an attack event is critical to effective incident response.

Solution Overview

Symantec Security Analytics provides the HP ArcSight ESM with the context that incident response teams need to quickly respond to threats with targeted precision. Security Analytics extracts and reconstructs every detail associated with advanced malware and threats – including source and destination IPs, every packet, flow, file, application, and server information. Combining Security Analytics with Symantec Malware Analysis provides ArcSight ESM with details of previously unknown malware that has been thoroughly analyzed by next-generation sandboxing and malware detonation. Security Analytics also leverages the Symantec Global Intelligence Network – aggregated threat intelligence from 15,000 customers and 75 million users to provide instant, actionable intelligence on web, email, or file-based threats. Armed with this analysis, incident response teams can assess damage, contain malware, mitigate data loss, and prevent subsequent attacks by fortifying the network.

Integration Certified
Security–ArcSight

Partner: HP

Partner Product: HP ArcSight ESM

Symantec Product: Security Analytics

How it Works

Symantec Security Analytics acts like a security camera on the network, using network taps or span ports to record and index full packet captures of all activity – even on today's fastest networks. This packet capture data can then be analyzed to provide context that enables rapid response to HP ArcSight ESM attack alerts. For example, when an ArcSight ESM generates a high-priority alert within the ArcSight ESM user interface, event parameters are seamlessly passed to Security Analytics, which responds with a complete analysis detailing what occurred before, during and after the event. The ArcSight ESM user can even recreate actual artifacts (documents, executables, etc.) from stored packet data.

Many security events are suspicious, but not definitive attacks. For example, an ArcSight ESM event may indicate executable shell-code download. This may be an attack, or it may be legitimate. To clarify, Security Analytics provides an immediate reputation analysis of the captured file that includes scan results from third-party virus databases and the Symantec Global Intelligence Network. If the file is not known to the Global Intelligence Network or virus databases, it can be forwarded to Malware Analysis or third party sandboxing solution for deeper analysis. In either case, the response team is armed with the data it needs to verify and isolate threats within minutes.

Symantec

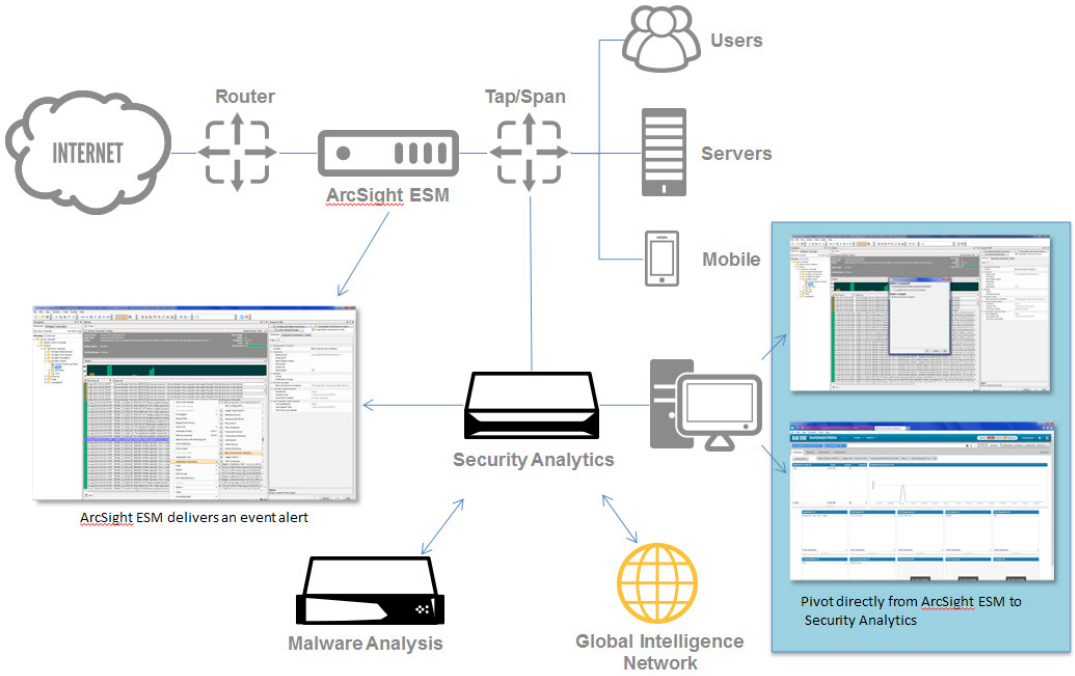
By reconstructing what happened before a compromise, Security Analytics determines the root cause and provides the intelligence needed to prevent others from falling victim to the same attack. For example, Security Analytics analysis of host activity prior to a malware download may reveal that the root cause was a bogus Facebook URL sent to users via instant messaging (IM). In this case, Security Analytics identifies the source IM account, IM content, bogus URL, URL reputation, and more. It can also use captured HTML to recreate the bogus Facebook page as it appeared at the time of the incident. With this context, the incident response team can prevent recurrences by shutting down the source IM account, blocking IM traffic, and blocking the malicious URL. They can even prevent recurrence by educating employees with sample IM content and screen shots of the bogus Facebook page.

By reconstructing what happened after an ArcSight ESM event, Security Analytics can assess damage that may have already occurred within the corporate network and prevent data loss going forward. Did a compromised host connect to a botnet and if so, did it send sensitive data? Did it connect to other internal hosts to collect data or spread malware? Security Analytics quickly answers these and other post-event questions across thousands of hosts without manually collecting and analyzing data from each individual host.

When new malware is found, it is critical to quickly determine whether other hosts may have been impacted by the same threat. For example, a newly deployed IPS signature may identify malware delivery to a single host. Since the signature is new, it is possible that the same malware infected other hosts prior to signature deployment. To find any such hosts, Security Analytics can search days, weeks, or months worth of captured traffic to determine if any hosts downloaded the same file prior to the signature becoming available.

Threat Detection

In addition to accelerating incident response, Security Analytics can serve as an ArcSight ESM event source. These threat events are delivered to ArcSight ESM in Common Event Format (CEF) where they are correlated with other events and prioritized for incident response.



Benefits of the joint Symantec and HP solution:

- Save critical time and effort by quickly determining false positive alerts in networks
- Significantly reduce the manual effort involved in identifying, isolating and remediating potential threats
- Identify the root cause, significantly reduce the time-to-resolution and contain malicious threats such as unknown malware before any serious network damage is done
- Prevent sensitive network data loss and ensure compliance with regulations such as HIPAA, PCI and SOX

About HP

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in its hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats. For more information on HP TippingPoint solutions, please visit www.hp.com/go/tippingpoint. To learn more about HP Enterprise Security, please visit www.hpenterprisesecurity.com.

For More Information

Learn more about Symantec Technology Integration Partners on our website.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.
SYMC_sb_TechPartner_HP_ArcSight_EN_v1a