A Technical Executive Summary on

Automation of Malware Forensic Triage in SOC

Security teams are frequently overwhelmed by the manual review of security alerts and the coordination of multiple security systems. Sifting through the high volume of false positives is a resource drain, but as previous breaches have demonstrated, the potential impact of missing a real attack makes it a necessity. Traditional anti-malware products can be effective in detecting known malware, but they can fail when faced with new or evolving malware types.

SOAR (Security Orchestration, Automation, and Response) is a solution stack of compatible software programs that allow an organization to collect data about security threats from multiple sources and respond to low-level security events without human assistance. SOAR employs a combination of technical capabilities and built-in processes to automate previously manual and time-consuming security management tasks. A SOAR platform delivers centralized security operations by orchestrating incident response tasks through a two-way integration with a broad range of third-party security tools.

SOAR solutions enable the security team to automate its existing alert responses by modeling and orchestrating the workflow steps across multiple tools. SOAR speeds up alert response workflows by automating and orchestrating timeconsuming and repetitive tasks, such as updating tickets, creating reports, logging into multiple systems, entering incident information, and sending email alerts. A SOAR solution can implement security controls like updating SIEM watch lists, disabling user accounts, and so forth.

An effective SOAR solution offers a comprehensive set of functionality in one platform.

These include:

- Automation – The ability to execute a sequence of tasks related to a security workflow without a human user.
- Orchestration – The invoking of functionality from multiple, independent security systems to execute a security workflow.
- Case management – A centralized capability for managing all aspects of a security incident or alert.
- Reporting and analytics – A built-in, or integrated, third-party tool that enables the security team to report on incidents or cases in progress, alert levels, threat intelligence and so forth.

Splunk:

An analyst can quickly detect malware across the organization using domain-specific dashboards, correlation searches, and reports included with Splunk Enterprise Security. Use log data from an endpoint security product and web proxy servers. Data from endpoint systems is vital to maintain an accurate view of malware infections in your environment.

Using the information surfaced from by Splunk Enterprise Security, an analyst can take the critical steps to act on the threat of a malware outbreak by quarantining and cleaning infected hosts, blacklisting the suspicious domain, and identifying the suspicious files that delivered the malware payload. The notable events provided the starting point for the investigation and an analyst can use additional dashboards and detail to locate the entry point for the malware infection.

Elastic Stack

Elastic Stack can be used to quickly detect signatures related to the download, infection, spread, and kill switch activity of ransomware, helping to gain insight into the state of infection within your infrastructure, during initial triage.