AUTOMATION OF MALWARE FORENSIC TRAIGE IN SOC

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor.

Triage is the assessment of a security event to determine if there is a security incident, its priority, and the need for escalation. As it relates to potential malware incidents the purpose of triaging may vary.

Publication Details. Triage is the process of rapidly examining sick children when they first arrive in order to place them in one of the following categories: Those with EMERGENCY SIGNS who require immediate emergency treatment.

Cyber Triage is an automated incident response software any company can use to investigate their network alerts. When your SIEM or detection system generates an alert, you need to investigate endpoints to determine severity and scope.

Ransomware has become one of the most common and lucrative forms of malware, recently eclipsing even credit card theft incidents. With the potential for huge profits, you can be sure hackers will be coming up with even more effective and dangerous attacks. Recent ransomware attacks include data exfiltration, that is then held for ransom.

SPLUNK

We use Splunk Enterprise Security with Splunk Enterprise to detect malware-infected hosts. An analyst can quickly detect malware across the organization using domain-specific dashboards, correlation searches and reports included with Splunk Enterprise Security.

Enterprise Security provides statistics and interesting events on security domain specific dashboards. Using the dashboards together, you can build a workflow for investigating threats by reviewing the results, isolating the events that require attention, and using the contextual information provided to drill down into the issue.

ELK OR ELASTIC STACK

ELK or Elastic stack is an open source tool (well, more like a set of open source tools) that enable the collection and analysis of large amounts of data (there are applications that handle data volumes on the order of few PBs) One of the most common uses of ELK is probably for the collection and analysis of logs from various sources.

A slightly different use case for the ELK stack would be to collect logs and alerts from security and IT related devices and applications for the purpose of detecting and investigating cyber related attacks.

SOAR

SOAR stands for Security Orchestration, Automation, and Response. ... Threat and vulnerability management (Orchestration) covers technologies that help amend cyber threats, while security operations automation (Automation) relates to the technologies that enable automation and orchestration within operations.

Comprehensive, automated static analysis on files entering an organization. This rich, highly relevant file intelligence enhances correlation and visibility of malware, enriching any SIEM or SOAR, and promotes a more effective and efficient malware identification and incident response process.

By taking alerts you already receive, SOAR can automate the malware analysis process to determine if further action is required. This process seems simple at first, but if you take into account the huge number of distinct services that are alerting you of potential malicious behavior then you can quickly see why you need a security automation and orchestration platform.

Once integrated into your current services, you can use both internal (e.g. Cuckoo Sandbox, etc.) or external (e.g. Hybrid-Analysis, SNDBOX, Joe Sandbox, McAfee Advanced Threat Defense, etc.) sandbox/analysis processes to automate the triaging of alerts related to potentially malicious files and URLs.