**Automation of Malware Forensic Triage in SOC**

A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. 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. These days ransomware has occupied the news headlines. Protecting digital assets requires the right tools and processes for the security team to handle the workload efficiently. This is becoming a greater challenge as the volume and seriousness of threats continue to grow. Security teams are frequently overwhelmed by the manual review of security alerts and 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. So, how can a security team offer the most robust protection and efficiently react to serious threats, despite being inundated by false alarms? This is the realm of security orchestration, automation and response (SOAR). 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 two-way integration with a broad range of third-party security tools. For instance, using a SOAR solution, a security manager can view a single console to monitor, interpret and respond to data generated by a broad range of platforms including SIEMs, IDS/IPSs, FWs, EDRs, UEBAs, malware and sandbox analysis, and others. SOAR solutions enable the security team to automate its existing alert responses by modeling and orchestrating the workflow steps across multiple tools. For example, an incident response process might call for a suspicious binary to be manually uploaded into a malware analysis system for evaluation. The SOAR platform will automate the submission step on its own and centralize the results to initiate additional actions, like opening a trouble ticket and/or quarantining an infected endpoint without requiring human intervention. SOAR speeds up alert response workflows by automating and orchestrating time-consuming and repetitive tasks, such as updating tickets, creating reports, logging into multiple systems, entering incident information and sending email alerts. SOAR also includes workflows, like incident investigation involving log gathering and analysis, and can review and analyze threat intelligence sources. By automating these tasks, SOAR solutions allow analysts to focus their full attention on more advanced security threats. One of SOAR’s main value propositions is making security teams more productive. This means that usability is a major factor in the success of a SOAR solution. The best SOAR platforms are easy to deploy and manage, with a simple, intuitive user experience for administrators and users alike. Ideally, the user interface (UI) and user experience (UX) is flexible to suit the work styles of a range of users, including power users, security analysts and executives. Since each user type has different requirements, an adaptable UI/UX will make the solution as beneficial as possible to each kind of user. Swimlane establishes integration as a means to accommodate highly automated, complex incident response workflows. There is more to automation than simply laying out an ABC set of steps and instructing the solution to execute them. A SOAR solution ought to drive playbook execution of security response workflows to reduce time and overhead. In that sense, the automation capabilities need to be smart. They need to be able to adapt to how the best team members handle security challenges and then mimic the response through an automated sequence of tasks. For medium- and large-sized security organizations, it’s especially critical that they are not forced to rely on generic “templates” but are able to build highly customized playbooks that document and replicate their exact workflows to fit their existing people, processes, and technologies.A SOAR solution’s automation capabilities can (and should) go beyond preventive measures. Security benefits from automated triggering of additional investigative measures. Similarly, some SOAR solutions can update monitoring platforms on an automated basis. Swimlane’s automation is designed to capture security best practices from its user team. The resulting standardization enables the team to learn and resolve security tasks quickly. Swimlane is at the forefront of the growing market of security automation, orchestration and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane’s solution helps organizations address all security operations (SecOps) needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization.

Elastic Stack can be used during the triage phase of a malware outbreak to identify potential infections within the organisation. The ability to quickly search through network and operating system events can enable the rapid identification of machines which have been compromised, given our knowledge of specific malware signatures. The Elastic Stack cannot prevent infection - that requires a combination of people, process, and other technology - or exhaustively identify new malware attack vectors, but it lets you gain rapid insight into your current situation. It can be used to quickly detect signatures related to the download, infection, spread, and kill switch activity of the WannaCry ransomware, helping to gain insight into the state of infection within your infrastructure, during initial triage. It will work as follows: First it will detect any malware download, then it will explore and detect its execution to help with triaging of the threats. It will detect the infection spread, outbound activities and the behaviour of the malware.

Detecting malware and investigating malware-infected hosts is a common task for a security operations team that helps improve the security posture of their organization. Traditional anti-malware products can fail when faced with new or evolving malware types. So, another possible solution can be using Splunk Enterprise Security (ES) 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. Using data from the endpoint systems and proxy server logs, Splunk Enterprise Security identifies notable events when hosts get infected with malware and requests downloads from a suspicious domain. The notable events provide the starting point for the investigation and an analyst can use additional dashboards and detail to locate the entry point for the malware infection. After analyzing the data and pivoting to search results, an analyst could identify the hosts that requested downloads from suspicious domains. 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.

Use the following search:

*index=\* tag=attack tag=malware | transaction maxpause=1d RiskName | where mvcount(ComputerName)>3 | table Occurrences, RiskName, RequestedAction, ActualAction, SecondaryAction, ApplicationHash, HashType, ComputerName, Source, UserName, Confidence, Disposition, File\_Path, Prevalence, \_time*

# In searches, replace the asterisk in index=\* with the name of the index that contains the data. By default, Splunk stores data in the main index. Therefore, index=\* becomes index=main. Use the OR operator to specify one or multiple indexes to search.

When you see the same malware on multiple systems, it is important to understand how the malware is spreading so you can stop the threat. For example, if WannaCry is spreading through an unpatched SMB vulnerability, you need a network or patching response. Phishing campaigns require that you remove messages from mailboxes and filter them. Drive-by download responses require an entirely different set of actions. Perform all standard malware incident response actions, such as updating definitions, reimaging systems, and so on.