**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. 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 and automates its alerts. 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. Swimlane establishes integration as a means to accommodate highly automated, complex incident response workflows. 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-sized 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. 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 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.

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. 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.

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.