Essential Guide

Automated Threat Analysis

Automate analysis, accelerate investigations and achieve rapid resolution of active credential phishing and malware threats.

splunk>

In an era where cyber threats evolve at an unprecedented rate, the ability to rapidly analyze and respond to potential incidents is critical for maintaining organizational security. Security operations centers (SOCs) face the daunting task of analyzing and responding to threats swiftly and effectively in an environment where attackers constantly devise new strategies. Analysis of threats often requires security teams to work across disparate tools to manually review the results of each analysis, capture secondary artifacts and synthesize the data to formulate insights and draw conclusions to take corrective action. This process leads to slower response times and wasted analyst cycles.

Phishing and malware threats in particular have become a significant concern for businesses. These threats continue to grow in volume quarter over quarter and have evolved in sophistication, leveraging advanced techniques to bypass traditional security measures. Phishing attacks have become more targeted using social engineering tactics to trick users into divulging sensitive information and putting businesses at risk. The rise in remote work and increased digital transactions have further amplified these threats, making cybersecurity a top priority. The growing volume of cyber threats underscores the critical need for advanced analysis and rapid response mechanisms. Robust, automated security solutions are essential to gaining comprehensive insights into threats, removing the manual burden, ensuring minimal disruption and maintaining continuous operational security.

What is automated threat analysis?

Automated threat analysis is a novel approach in cybersecurity, where advanced software tools and algorithms are employed to identify and assess potential security threats without the need for extensive human intervention. Traditional threat analysis methods rely heavily on manual processes conducted by cybersecurity professionals, which are time-consuming and prone to human error. In contrast, automated threat analysis analyzes data at scale and speed that is unattainable by human analysts. This allows organizations to respond to threats more quickly and effectively.

Furthermore, automated threat analysis systems are constantly evolving to keep up with new tactics, techniques and procedures (TTPs), such as obfuscation techniques and attack chain patterns, to automatically take the steps needed for deep analysis that traditional tools do not have the architecture to support.

Limitations of traditional cybersecurity tools in the face of evolving threats

When dealing with credential phishing and malware threats, security teams use a variety of traditional tools: perimeter protection tools such as secure email gateways and endpoint detection and secondary defense mechanisms like abuse mailbox monitoring solutions and traditional sandboxes. However, with the increasing complexity and sophistication of cyber threats, the shortcomings of traditional tools are becoming more evident.

Secure email gateways

Secure email gateways (SEGs) are a vital tool in an organization's cybersecurity arsenal, designed to filter incoming emails to prevent spam, phishing and malware from reaching users' inboxes. They typically employ various techniques to allow or deny emails and signature-based detections to identify and block malicious content. However, analyzing every email in each mailbox will inevitably result in some missed threats. Additionally, the effectiveness of SEGs in detecting sophisticated threats is increasingly challenged as cybercriminals are becoming more adept at crafting emails that bypass traditional detection methods utilizing things like QR codes, custom malware, password protected files and multi-stage URLs.

Abuse mailbox monitoring solutions

To help combat phishing threats, abuse mailbox monitoring is a common practice where businesses set up dedicated email addresses to streamline the process for employees to report suspicious emails. This method relies on the vigilance of employees to identify and report suspicious emails. With 3.4 billion phishing emails being sent daily, phishing is one of the most serious threats to businesses. However, 61% of employee-reported phishing emails end up being false positives, which leaves security teams overwhelmed with high email volumes that are hard to keep up with using manual analysis and tools. The high volume of false positives strains resources, leads to wasted time investigating benign emails and results in alert fatigue.

61% of employee-reported phishing emails end up being false positives.

Endpoint detection and response tools

Endpoint detection and response (EDR) tools are designed to continuously monitor endpoints for suspicious activities and generate alerts when potential threats are detected. These tools generate vast amounts of data, resulting in false positives and false negatives. EDR tools can also sometimes miss critical stages of an attack. EDR threat verdicts, while useful for initial identification, often provide limited actionable intelligence, leaving security teams without sufficient context or guidance for effective response.

Traditional sandboxes

Security analysts typically turn to traditional sandboxes for analysis and detection purposes. While they provide a controlled environment to execute and analyze suspicious content, these tools require a lot of manual work for analysts to access malicious content safely and usually do not present conclusive results. Generally, they are not designed to detect the latest complex attacks that utilize varying delivery vectors, and certainly not in an automated way at scale. Traditional sandboxes also do not provide an immediate, comprehensive explanation of threat behaviors. All of this leads to inefficient, incomplete and misleading investigations. Additionally, utilizing open source tools in conjunction with traditional sandboxes to create custom malware analysis pipelines brings about significant challenges, primarily due to the extensive time and expertise required to develop, integrate and maintain the systems.

While these tools are integral to cybersecurity efforts, limitations necessitate more advanced and proactive solutions to augment their capabilities with automated phishing and malware analysis.

5 essential capabilities of automated threat analysis

1. Attack chain following

Following an attack chain is paramount for understanding and mitigating threats effectively. An attack chain outlines the sequence of events or stages used by an attacker to infiltrate and compromise a system, and it provides crucial insights into the TTPs employed. A key component of automated threat analysis is the ability to navigate the varying delivery vectors in order to execute the entire attack chain, regardless of complexity.

2. Consistent, comprehensive analysis

Comprehensive insight into the actions taken by threat actors means that analysts are no longer required to piece together the intended tactics of a threat manually. And with consistent, high-quality automated analysis, security teams can achieve operational efficiency that would otherwise be lacking due to inconsistent processes and outcomes between individual analysts, as well as gain a deeper understanding of complex threats. Comprehensive analysis is vital not only for responding to ongoing threats but also for proactively strengthening defenses against future attacks.

3. Interactive sandbox

A secure and unattributable environment to submit potentially malicious URLs or files offers the ability to scrutinize suspicious content without risking the integrity of the business. This environment allows analysts to execute and observe the behavior of suspected malware or phishing links in real time, providing a deeper understanding of their mechanisms and potential impact. This is particularly important as modern threats often employ sophisticated evasion techniques that can be difficult to detect with static analysis methods. Furthermore, insights gained from sandbox analysis can be used to update defensive strategies and educate users about emerging threats.

4. Interactive web browser

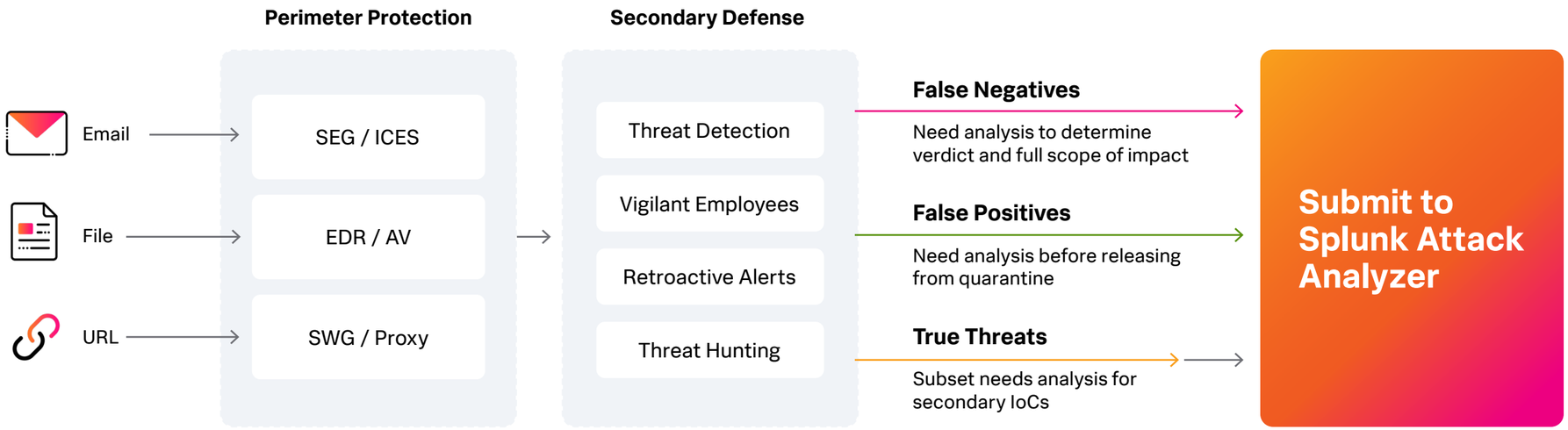
For analysis that requires human intervention (e.g., entering credentials to get past an attacker's login page), an interactive web browser can interact with URLs or HTML files to deal with data that needs to be investigated manually.

5. End-to-end automated threat analysis and response workflow

The pairing of automated threat analysis with security orchestration, automation and response (SOAR) capabilities significantly advances threat analysis workflows. This synergy allows security teams to keep up with today's fast-paced digital landscape. Automated threat analysis excels in quickly identifying and dissecting potential threats, while SOAR solutions streamline and automate the response process. By combining these two powerful tools, teams can immediately translate threat analysis into actionable response strategies.

Automated threat analysis strategies to enhance security defenses

As a component of an organization's security operations, automated threat analysis helps teams manage threats that make it past perimeter edge and secondary defenses. The most impactful results that security teams can gain with automated threat analysis are through incident triage and incident analysis of existing workflows.



Email analysis

Managing potential email threats takes up a large amount of SOC resources each day, but the percentage of actual threats is relatively low, so teams have to sort through a lot of noise. Automated threat analysis can be incorporated into email analysis workflows to help teams more efficiently handle employee-reported emails, customer-reported brand fraud and retroactive email alerts when perimeter detection systems are delayed in detecting potential malicious threats.

- For employee-reported emails, automated threat analysis drastically reduces the manual work required from analysts to determine if the content is malicious, and when paired with a SOAR solution, triage can be done without any human intervention to cut down the noise security teams are dealing with.
- Analysis of customer-reported brand fraud allows businesses to understand how they are being impersonated and take the necessary steps to initiate phishing takedowns to reduce the uptime of phishing URLs.
- For emails initially deemed safe by perimeter detection systems but later discovered to be malicious, automated threat analysis helps teams eliminate any potential false positives or find secondary indicators of compromise (IoCs) beyond what was caught by the detection system.

Endpoint detection and response or antivirus alerts

The context that automated threat analysis provides to understand the full scope of an incident can help reduce the number of false positives generated by EDR and antivirus (AV) tools and make better informed decisions about the severity of alerts so analysts can prioritize and tackle the most pressing issues first. With the ability to fully execute the entire attack chain, automated analysis can also provide secondary analysis of threats quarantined by EDR and AV tools to find additional IoCs, confirming false positives before being released from quarantine. Furthermore, automated analysis can help address the subtle and evasive threats that may slip through EDR and AV tools as false negatives.

Web and proxy alerts

Automated analysis of URLs and IPs can help security teams better manage the volume and complexity of alerts from tools like secure web gateways (SWGs). Analysis results can help make swift decisions about handling URL categorization and inform proxy site block or unblock requests. Teams can also use automated analysis to proactively analyze web referrer logs to identify any suspicious traffic patterns or potential threats targeting their organization.

In addition to these workflow examples, automated threat analysis supports overall threat hunting efforts. The insights from thorough threat analysis empower hunters to make data-driven decisions, tailor their hunting strategies and adapt to the evolving threat landscape.

By integrating automated threat analysis into existing workflows, security teams can enhance the efficiency, accuracy and speed of analyzing and responding to threats.

Enter Splunk

Splunk offers automated threat intelligence for businesses to tackle credential phishing and malware threats. **Splunk Attack Analyzer** is designed to meet the challenges of security teams head-on, delivering full-scope insights to enable a deeper understanding of complex threats and rapid resolution.

Take the manual work out of threat analysis

SOC analysts work across many security tools, including threat intelligence platforms or malware sandboxes, to help them understand and address threats targeting the organization. These tools tend to be disparate and disjointed and do not provide analysts with conclusive results to see the complete picture of malicious activity or the contextual awareness of a series of coordinated threats. With automated threat analysis, security teams can move away from manual, time-consuming analysis to an automated solution that can keep up with the ever-increasing volume and sophistication of threats. Splunk Attack Analyzer automatically performs the actions required to fully execute complex attack chains, including clicking and following links, extracting attachments and embedded files and dealing with archives. The solution then renders a verdict and extracts forensics to provide analysts with the associated intelligence and context of the active threat for a clear and rapid view into how threat actors are operating.

Gain consistent, comprehensive, high-quality threat analysis

Staying ahead of threat actors is an ongoing challenge, especially with the persistent shortage of skilled cybersecurity professionals. Threat actors relentlessly pursue new attack vectors and tactics, often leveraging cutting-edge technology and sophisticated techniques to evade detection. As threat actors constantly adapt to security measures and exploit vulnerabilities, security teams perpetually play catch-up with understaffed teams. Skilled tier-3 cybersecurity analysts bring years of experience and a deep understanding of evolving threats. In their absence, organizations often rely on less-experienced tier-1 analysts, limiting the ability to deliver high-quality analysis of threats as junior analysts may need more nuanced knowledge and contextual understanding compared to senior analysts.

Splunk Attack Analyzer safely executes the intended threat while providing analysts with a consistent, comprehensive view of an attack's technical details. This ensures a baseline standard of analysis job results regardless of the analyst completing the task. Thorough technical forensics provide valuable learning for tier-1 analysts, reduce escalations to tier-2 and tier-3 analysts, and give seasoned analysts more time to focus on higher value, more productive and intellectually challenging tasks.

Interact with malicious content in a dedicated, unattributable environment

When accessing malicious samples, it is critical that analysts maintain anonymity and not expose the business to any risk. The interactive web browser and interactive sandbox features of Splunk Attack Analyzer allow analysts to quickly launch an unattributable environment to interact with URLs and HTML files or detonate malware without compromising the safety of the analysts or the organization.

Build intelligent automation for end-to-end threat analysis and response

When SOCs combine Splunk Attack Analyzer and Splunk SOAR, they gain unique, world-class analysis and response capabilities that make the SOC more effective and efficient by responding to threats at machine speed. Splunk SOAR can identify events from SIEM solutions like Splunk Enterprise Security and user-reported phishing to open cases and pass potentially malicious files or URLs to Splunk Attack Analyzer. Splunk Attack Analyzer conducts automated analysis of credential phishing threats, and Splunk SOAR uses the rendered verdict to execute the appropriate response playbook to automate first-level triage or protect the enterprise. All of this is delivered to customers through out-of-the-box playbooks.

Splunk Attack Analyzer is a pivotal tool for modern cybersecurity. By seamlessly integrating with existing security infrastructures, it not only enhances the capabilities of the SOC to analyze and respond to credential phishing and malware threats but also helps reduce cyber risk. With its advanced features of comprehensive attack chain following, interactive sandboxing, and SOAR integration capabilities for end-to-end threat analysis and response workflows, Splunk Attack Analyzer is essential for any organization looking to fortify its defenses against the ever-evolving threat landscape. Embracing this powerful tool is a step towards a more secure, resilient and proactive cybersecurity strategy.

Splunk SOAR

Splunk SOAR excels in case management, initial enrichment, and orchestration to identify events from the SIEM and user-reported phishing, and open cases.

- Case Management
- Orchestration
- Automation
- Event Management
- Collaboration
- Reporting and Metrics

Splunk Attack Analyzer

Splunk Attack Analyzer conducts automated analysis of identified indicators without SOC analysts having to perform manual investigative tasks.

- Static and Dynamic Analysis
- Attack Chain Following
- Rich Forensics
- Malware and Credential Phishing Detection

Splunk SOAR

Once Splunk Attack Analyzer has confirmed an active threat, Splunk SOAR executes the appropriate response playbook to protect the enterprise.

- Case Management
- Orchestration
- Automation
- Event Management
- Collaboration
- Reporting and Metrics

Get Started.

Are you ready to learn more about how automated threat analysis can help modernize your SOC? Speak with a Splunk expert now.

splunk>

23-432247-Splunk-The Essential Guide to Automated Threat Analysis-EB-109