Splunk Attack Analyzer

Automatically analyze the most complex credential phishing and malware threats

Product Benefits

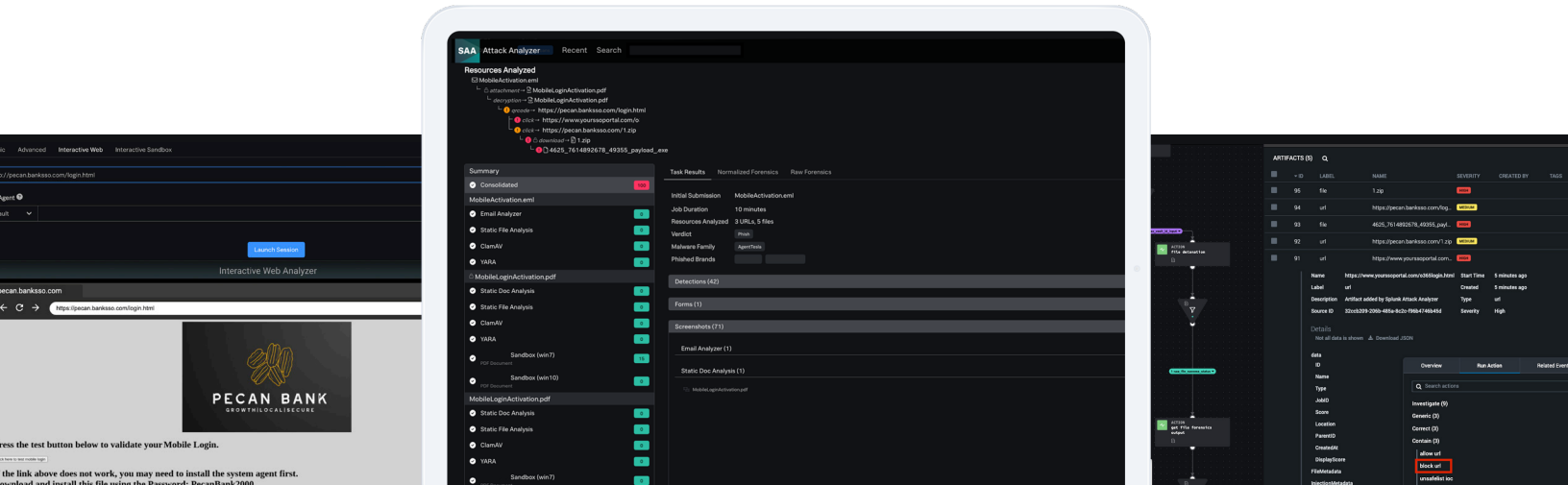
Follow and analyze complex attack chains that would otherwise require cumbersome manual workflows

View detailed threat forensics showing the technical details of attacks

Seamlessly investigate suspected threats by automatically accessing associated technical context

Security operations center (SOC) analysts work across many security tools to help them understand and address threats targeting their organization. These tools tend to be disparate and disjointed, failing to provide analysts with the full picture of malicious activity or the contextual awareness of a series of coordinated threats. Security analysts often turn to traditional sandboxes for analysis and detection purposes, but these tools require a large amount of manual work for analysts to access malicious content safely and usually do not present conclusive results. During an investigation, analysts must manually synthesize data, files, or URLs to formulate insights, and then take the time to draw conclusions and take corrective action. This process is inefficient, which leads to slower response times and wasted analyst cycles. While detection-based products play a crucial role in alerting SOCs to an attack, analysts need additional visibility and context to fully understand the scope of an incident to decide on an appropriate response.

Splunk Attack Analyzer is a critical informational component of an organization's overall threat detection, investigation, and response (TDIR) capabilities. It provides automated threat analysis and associated digital forensics of files and URLs to deliver consistent high-quality analysis of potential threats, save analysts time, and help SOCs achieve the operational efficiency needed to outpace adversaries. The solution uses proprietary technology to extract malicious content from text, images, macro source code, website content, and more to automatically analyze credential phishing and malware threats. With Splunk Attack Analyzer, analysts achieve unparalleled detection efficacy with accuracy, confidence, and ease.



Take the manual work out of threat analysis

The technology automatically navigates through varying delivery vectors, such as decoding QR codes, visiting malicious content, extracting attachments and embedded files, or even entering passwords for archives by pulling them from images or emails to get to the final payload which can then be analyzed.

Analysts are provided a visualization, built in real time, which showcases the step-by-step actions of the threat, along with associated intelligence and context. This insight provides analysts with a clear and rapid view into how threat actors are operating and eliminates the need to manually synthesize data in order to draw conclusions, ultimately saving time and ensuring an iron-clad response. Analysts can also identify if the enterprise is at risk of any future attack with existing policies and procedures based on how threat actors are bypassing security measures.

Fully automate end-to-end threat analysis and response workflow

Paired with Splunk SOAR, Splunk Attack Analyzer conducts automated analysis of identified indicators without SOC analysts having to perform manual investigative tasks or write complex playbooks utilizing multiple threat analytics products. Once Splunk Attack Analyzer has rendered informed verdicts on imminent threats, Splunk SOAR will execute the appropriate response playbook. The combination of Splunk SOAR and Splunk Attack Analyzer provides world-class analysis and response capabilities, empowering SOC and IR teams to proficiently triage and respond to the multitude of active threats encountered daily with unrivaled speed and precision.

Gain consistent, comprehensive, high-quality threat analysis

Splunk Attack Analyzer's proprietary technology safely executes the intended threat while providing analysts a consistent, comprehensive view showing the technical details of an attack. When a sample is submitted to Splunk Attack Analyzer, analysts are provided a visualization of where malicious content is embedded. The insight provides analysts with a clear and rapid view into how threat actors are operating. Whether in a URL or deep within several PDF files, analysts can keep up with the continual shift of threat actor TTPs in order to protect the enterprise and ensure security operational protocols are in place.

Interact with malicious content in a dedicated, unattributable environment

Analysts, regardless of tier, have the capability to seamlessly generate non-attributed environments directly within Splunk Attack Analyzer in order to access malicious content without compromising the safety of the analyst or the enterprise. The ability to directly access potential phishing sites or files enables analysts to thoroughly conduct an investigation and remain confident their identity is concealed; and the consistent, high-quality analysis of threats enables valuable learning for tier 1 analysts and reduces escalations to tier 3 analysts.

Read More >

Watch Webinar >

Take a Tour >

splunk>

Contact us: www.splunk.com/asksales

www.splunk.com