CounterFlow ai

ThreatEye Recorder

CASE STUDY

Leveraging Splunk For Complete and Seamless Network Visibility

splunk>

CHALLENGE

While Splunk collects a substantial amount of data, it does not provide the full recording of what has been sent and received on the network. Security and Network Operations Centers therefore need a tool to further investigate suspicious events.

SOLUTION

The API integration of Splunk with the Counterflow AI ThreatEye Recorder allows all captured data to be accessed quickly and easily for forensic investigation.

BENEFITS

ThreatEye Recorder provides insights in mere seconds, allowing the Splunk user to determine the full scope of the event and provide timely remediation. ThreatEye can be seamlessly integrated with any existing Splunk solution, which enables enterprises to leverage earlier investments.

Challenge

As one of the most versatile event management tools on the market, Splunk is utilized across industries to collect data from security, network, and server assets throughout the corporate infrastructure. To provide the needed insight into network security and performance, any unusual activity registered by Splunk must be analyzed and prioritized.

This task is typically managed by Security and Network Operations Centers (SOCs and NOCs) working to condense billions of log notifications to the highest priority actionable events. But while Splunk collects a substantial amount of event data, it does not provide the needed visibility of what has been sent and received on the network. SOCs and NOCs therefore need a way to corroborate and resolve any events that look suspicious.

> “The average cost of time wasted responding to inaccurate and erroneous intelligence can average $1.27 million annually.”
>
> Ponemon Institute Survey

Solution

This is where Counterflow AI ThreatEye Recorder can help. ThreatEye is a scalable capture-to-disk solution with hardware-accelerated capture and reconfigurable storage. It captures, stores and retrieves all network data on demand, enabling teams to retrospectively provide PCAP evidence for a multitude of tasks, including forensic analysis or operational troubleshooting. ThreatEye provides full continuous capture that can be matched to Splunk events or any other anomaly observed.

Case 1

In our first use case, an SOC security engineer working for a financial services firm is investigating a Splunk event, sent by Suricata, with a suspicious domain name. A corresponding event from the firewall indicates that a connection was attempted to the resolved address. To further investigate this activity, the SOC engineer clicks on the event in Splunk, uses the ThreatEye workflow, and in just a few seconds sees the full packet record corresponding to the name.

Without this information, the decision to report or disregard the event would have been based on assumption alone. But by analyzing the packet data, the SOC engineer can determine exactly what was sent/received to the suspicious address, whether a harmful document was downloaded, and if any information was sent out of the infrastructure. So the Splunk event can be resolved for severity and impact without conjecture or incomplete info.

> “
> An organization can receive an average of nearly 17,000 malware alerts in a typical week. The time to repsond to these alerts is a severe drain on an organization’s financial resources and IT security personnel.”
>
> Ponemon Institute Survey

Case 2

In our second use case, an NOC analyst working at a social media agency sees an application alert in Splunk for slow/no response and needs to identify the exact area of concern; an exercise which could prove time consuming and complex. But with the ThreatEye/Splunk integration, the NOC analyst can simply click on the event, search for packets, and quickly determine which infrastructure area is likely at fault: network, server or database. Inevitably, the stakeholders in each of these areas would only have visibility of their own domain and would tend to claim that there is “no trouble found”. But with this solution, the raw packet data will conclusively show which part of the organization needs to action the event and provide a root cause analysis.

Case 3

In our third use case, an Incident Responder working for a major Defense Contractor notices that a network security device has sent an alert into Splunk indicating suspicious SSL traffic. In this case, the server may be vulnerable to “heartbleed”, where the vulnerability exposes information in memory from recent web transactions, including cleartext usernames and passwords. The Incident Responder clicks on the event in Splunk and by analyzing the packets he can directly determine:

1. Whether the bug seems to have been exploited successfully.
2. Exactly what information was obtained through the vulnerability.

Benefits

Counterflow AI ThreatEye Recorder provides an extremely easy workflow. By clicking on any event in Splunk, the operations user can immediately get the full network packet trace that corresponds to the Splunk event. Thanks to its industry leading search speed, ThreatEye provides an answer in mere seconds, allowing the Splunk user to determine the full scope of the event and instantly provide the needed remediation.

ThreatEye can be seamlessly integrated with any existing Splunk solution, allowing businesses to leverage earlier investments and realize substantial savings.

LEARN MORE AT: **www.CounterFlowAI.com**

About CounterFlow AI, Inc.

CounterFlow AI is a cybersecurity software company offering an AIOps platform for network forensics. The flagship product, ThreatEye®, integrates advanced security technologies into a streaming machine learning pipeline to identify network faults, anomalies, and threats at wire speed. ThreatEye® is built for hybrid cloud deployments to easily extend customer network and security operations.

CounterFlow AI, Inc.
6181 Rockfish Gap Turnpike, Crozet, VA 22932
info@counterflowai.com