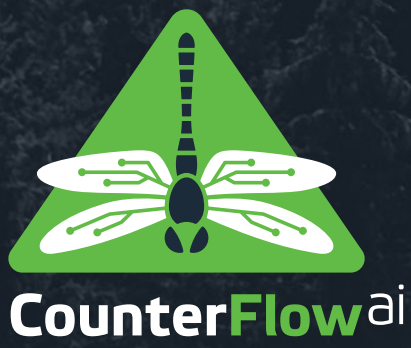

Got PCAP?

The Case for Full Packet Capture in a State Government SOC

POINT OF CONTACT

Sam Donnelly, Director of Federal Solutions

6181 Rockfish Gap Turnpike, Crozet, VA 22932

sd@counterflowai.com

910-331-4021

Consider these alarming trends impacting government cybersecurity teams today:

The volume of internet traffic will increase by 25% annually for the next three years[1]

The median dwell time of cyber-attacks in the US is 71 days[2]

The nationwide shortage of qualified security analysts will exceed 400,000 by the year 2022[3]

One particular state government has its security operations center (SOC) spending most of its waking hours sifting through potential network security events, triaging its workload, and trying to find and respond to threats before it's too late. With over 30,000 end points on this state's network, and given the challenges stated above, the SOC team members are facing a staggering challenge without new innovations.

In an effort to streamline its workflow and modernize its environment, this state SOC partnered with CounterFlow in late 2018. CounterFlow is a next-generation network forensics company that is revolutionizing the art of threat hunting by enabling SOC analysts to hunt, detect, and respond to threats within seconds or minutes, not weeks or months.

This state's cyber defense team was employing an alert-driven workflow from one of the best firewalls available today. However, true threat hunters need a way to dive deeper into proactive threat investigations.

According to the SANS Institute 2018 Threat Hunting Survey Results,

"One of the key elements not generally available across all [threat] hunts is full-packet captures. Hunters should place network sensors in specific locations with full-content packet interception enabled to add additional depth to network data collected and to provide for additional containment once found during incident response."[4]

Full packet capture provides the basic evidence – the "ground truth" - that is absolutely necessary for any substantial incident response or threat investigation.

Enter CounterFlow's Recorder, part of its ThreatEye™ product line.This solution is the cost-efficient platform of choice for ultra-fast, highly reliable, full packet capture, indexing, and federated search of network traffic.

The SOC analysts now have the detailed records of all network traffic, along with analytic tools to conduct retrospective threat forensics and diagnose suspicious network activity.

A key feature of CounterFlow's product line is its ability to integrate easily across a spectrum of cybersecurity tools, bolting on with SIEMs, firewalls, workflow enhancers and threat intel providers.

In this case, the state SOC enjoys a pivot-to-PCAP feature with Palo Alto Networks' (PAN) next generation firewall, as well with Suricata, an open-source intrusion detection system. These implementations use an API to correlate metadata from an alert to the stored location of the specifically related flows and packets on the ThreatEye™ Recordert.

With a single click, an analyst can pivot from an alert to a detailed view of the traffic that triggered it. Utilizing the ThreatEye™ packet analyzer, the analyst can further examine the captured file for a detailed report of threat analytics powered by CloudShark, yet another CounterFlow bolt-on option.

But don't just take our word for it; consider what this state SOC's Lead Analyst has to say:

> "CounterFlow technology has re-defined my daily workflow and made my life a lot easier."

The SOC has fully integrated CounterFlow tools into its daily workflow and formalized the process of threat response and investigation to include full packet inspection. The team has a few examples on how our technology helped:

> Within weeks of deploying CounterFlow's technology, a SOC analyst was able to identify a compromised end point on the State Government's network, isolate the end point by IP address, and take remedial action by removing the device from the network.

> The SOC team received a Palo Alto alert that incoming traffic was carrying a payload containing a malicious virus. However, activity logs did not provide the fidelity needed to locate and mitigate the virus. Using the pivot-to-PCAP feature, an analyst isolated an individual e-mail with a malicious attachment and notified the recipient before the recipient had a chance to open the message, preventing a potentially damaging compromise.

> Utilizing an open source IDS, an analyst received an alert of potentially nefarious activity. With a single click from the alert, the SOC team member was able to immediately analyze the PCAP to identify multiple attempts by an outside entity to log on to a host and install a malicious file.

> "Having this information at hand with just a single click from the alert allowed us to remediate an issue instantly that would have taken hours to discover... CounterFlow saves the day again!"

At CounterFlow, we make threat-hunters more effective. With high-performing full packet capture, intuitive search functions, and a wide array of integration options, we don't replace your suite of cybersecurity tools – we make them more effective. And as a result, we make organizations more secure.

About CounterFlow

CounterFlow's mission is to improve the efficiency and effectiveness of network forensics with AIOps. The company's flagship product, ThreatEye™, enables intelligent packet capture with a streaming machine learning engine that allows security teams to deploy scripts for real-time threat analysis and packet recording, at wire-speed up to 100Gbps.
For more information, visit https://counterflow.ai/.

[1] "Cisco Visual Networking Index: Forecasting and Trends, 2017-2022," 2018. Pages 2, 4.
[2] "Special Report: M-Trends 2018," by Mandiant, a FireEye Company, 2018. Pages 3-5.
[3] "Cybersecurity Jobs Report 2018-2021," https://cybersecurityventures.com/jobs/, 2017.
[4] "SANS 2018 Threat Hunting Survey Results," https://www.sans.org/reading-room/whitepapers/analyst/membership/38600