The Necessity of Full Packet Capture (FPC)

Why do cyber threats persist despite significant investment to counteract them?

The fundamental reason that many cyber attacks still get through is because all traditional security sensors still rely upon known vectors. While many solutions claim to supply us with "all the data," it is important to inquire whether it is really "all of it" or just "all of that which they are aggregating."

For example, log aggregation solutions may suggest "we have all the data" and, indeed, they can supply us with every log that has been made. However, let us think about how the logs are generated in the first place. In the example of a computer, the logs that are generated are a result of someone determining what is important to log in the first place. It is fundamentally restricted by some input that dictates what to log and what not to log.

The same problematic input is required in event data collection. Someone, or some configuration, has determined the conditions under which an event is generated. SIEM tools then collect all these events and present them to the user for analysis. So yes, they do have "all the data," only if the definition of the data is "all events."

Similarly with flow data, it is determined what flows to log and how much metadata to include in the flow record.

Inevitably, when we implement a solution where we believe we have "all the data," we need to fundamentally understand if it is "all" or some subset category of the greater "all."

It should now be clear how zero day attacks succeed. We may think we have "all the data" but we actually are only given "all the logs or events" that we are collecting. Hackers, or to be precise crackers, know that this is what we are doing. They design their attacks to go around the visibility that we have into logs and events. In other words, they find a way around these known methods by operating in the "dark" parts of our networks.

So how can we succeed here? In order to understand what solutions might actually work, we can turn to the physical world to gain some insights. In this realm, for example, buildings have access logs. Collecting all access logs may lead us to conclude that we have "all the data," but in reality, it is not sufficient to prove who did what, when, where, and how. While access logs may help us look for a correlation between when someone entered and what occurred, such a task often requires a supremely time consuming investigation and yet can never be 100% definite if there are multiple personnel that may match our search criteria.

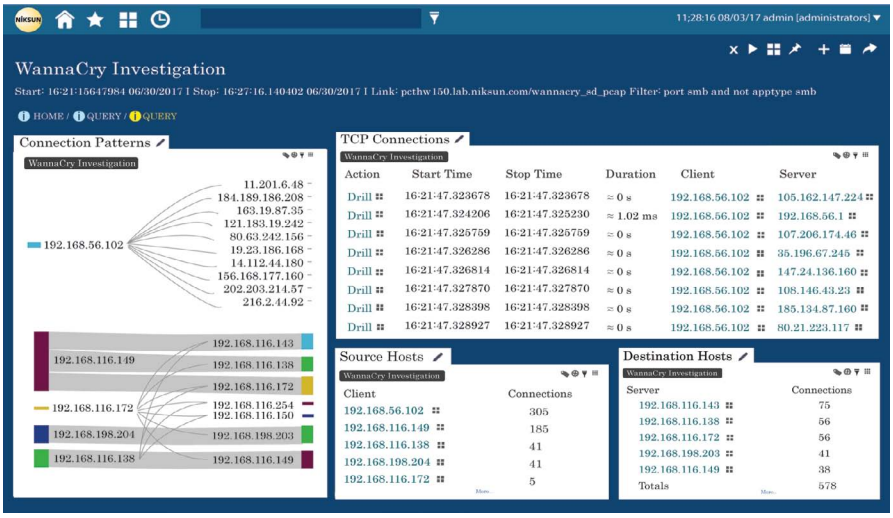
If a robbery takes place, how can we know that, without a doubt, it was a particular individual who is responsible? How can we prove what they did, when, where, and how they did it? The answer to this is to place security cameras that monitor and record the entire building, 24/7. Not only can we then immediately rewind back in time to see any incident that has taken place, we can also watch video feeds in real-time and stop security breaches as they occur. In fact, we can also set up image processing software that can look for patterns and behaviors and send out alerts, lock doors to trap the intruder, and more.

"Unquestionably the Top Network Forensics Tool"

Dr. Peter Stephenson
Technology Editor at SC Magazine

So the obvious answer to our problem of stopping and investigating cyber threats, including even zero day attacks, is to create something like a security camera that watches over every transaction. This is exactly what NIKSUN has been doing and perfecting over two decades. NIKSUN integrates full (or partial if required for privacy, etc.) packet capture with complete analytics at the packet, session, and all the way to the application layer. With NIKSUN, zero day attacks cannot be hidden from surveillance because it has already captured all actual activity of the malware. The malware has no way to circumvent being captured if it is deposited via the network or if it conducts any activity on the network.

Metadata, flow-data, malware, and APT analysis, as well as anti-virus programs and system patches, are proven now to be insufficient to combat such attacks. While such tools are useful in their own right (and all of these types of analysis are also included in NIKSUN's solution suite), they cannot provide answers to unknown threats that operate in the "dark" part of your network – the part that we aren't collecting logs and events about. Analysis can only be done with pre-known knowledge, so zero-day attacks and worms which hide under the typical radar are not easily detected and resolved. Anti-virus programs also rely on having the signature of an attack prior to it occurring, while system patches are only a retroactive fix and cannot find malware that was deposited while doors were open.



With its "Google-like" technology, NKSUN NikOS Everest provides one click for the who, what, where, when, and how

Given that NIKSUN has the ability to record a vast amount of information, the question becomes if we can find the information that we are looking for quickly. If we were to take continuous, 24/7 footage of a vault, for example, it would be useless without being able to easily search through it to find notable events. This fundamental difficulty is exactly what NIKSUN has solved and why it is the pioneer and industry leader in this space. NIKSUN's singular mission is to record all data at the highest rates without dropping a single packet and at the same time also indexing all the data in real-time to allow for extremely fast searching.

But can anyone, not just heavily specialized cybersecurity experts, use such a tool? Over the course of its existence, NIKSUN has made this possible as well. NIKSUN operates with a plain-English (as well as advanced expression for the experts) search, provides an extremely user friendly GUI, expert tools, and point and click analysis that is a game changer in the industry. It boils investigation down to just one or two clicks and visualizes everything that we need to know for easy and rapid forensics even if the user is not a forensics expert.

For a demo of this in action, please visit niksun.com/demo.

457 North Harrison St. • Princeton • NJ 08540 • USA
t: +1.609.936.9999 • toll free: +1.888.504.3336
f: +1.609.419.4260
info@niksun.com • www.niksun.com