SC MEDIA LAB APPROVED One year later

We take another look at a premier tool

NIKSUN NetDetectorLive

When we started using NetDetectorLive a few years back, we developed our own approaches to getting the most out of it. Those approaches evolved as the tool evolved.

SC MEDIA LAB APPROVED

NetDetectorLive is not a SIEM, or really, a UTM. NetDetectorLive is, well, a NetDetector. It monitors the network but then it does some very sophisticated (but not sophisticated-look) analysis tasks. It can take threat intelligence feeds and apply them to its analysis. But the thing that we found most useful is application reconstruction. NIKSUN pioneered this functionality and it still does it better than just about any other tool we've used.

NetDetectorLive constantly is collecting meta-data and storing it. You can pull reconstructed events very rapidly and play them back much as you would using a VCR. But this is not just a VCR for past events. There is a lot of intelligence gleaned from the reconstructions that you probably would miss trying to analyze in real time. It also is much more complete than static snapshots. However, you are not limited to the playback of the event. The users associated with it, all the external indicators such as IP addresses, domains, applications, data exfiltration and, of course the actual packets. You can step through the event for a complete analysis from the collected and forensically preserved data.

Everything that NetDetectorLive does is rule-based and, although it ships with a very comprehensive package of pre-written rules, writing your own is quite straightforward. One use to which we have put the tool is creating special policies to test other tools or to catch particular types of attacks for further analysis.

You also can use NetDetectorLive for several data exfiltration tasks. It identifies exfiltration and reconstructs the entire exfiltration process with all the indicators: users, IPs, domains, data exfiltrated, method of exfiltration, among other things.

One of the tool's great strengths, in our view, is its event analysis forensics. This is as close to a one-tool network forensics device as we've seen. Network forensics is a tough bone to chew. It generally takes several individual tools.

For example, we look at such things as packet captures, source and destination IP/domain analysis, payload analysis and the results of several threat intelligence feeds. NetDetectorLive does all of that for you and it retains the complete information package in a forensically sound manner for future reconstruction to show repeatability and for presentation in court if necessary. In short, this is a complete network security/forensic analysis tool with the added benefit that it can alert you when a policy has been violated.

Support from NIKSUN is at the top of our positive response. We never have had to wait more than a couple of hours regardless of the complexity of the problem. There are two levels of support available: Platinum Care and Standard Care.

Pricing is based upon the configuration and there is a wide variety of possibilities that scale to tens of petabytes with possibility external storage arrays to extend well beyond that. It can reconstruct in the hundreds of applications with more being added regularly. This, plus policy and rule sets, is the product's greatest strength in our view. The tool, with its 100GigE top end fiber interface, can drink from just about any firehose you want.

– Peter Stephenson, technology editor

DETAILS

Product NetDetectorLive

Company NIKSUN

Web niksun.com

Price Depends on configuration

What it does Application reconstruction, real-time network monitoring and forensics

What we liked Policy and rule sets, application reconstruction, intelligent, forensically sound data analysis and reconstruction.

The bottom line This is, unquestionably, the top network forensics tool available.

NIKSUN

NIKSUN
457 North Harrison Street
Princeton, NJ 08540
www.niksun.com
info@niksun.com