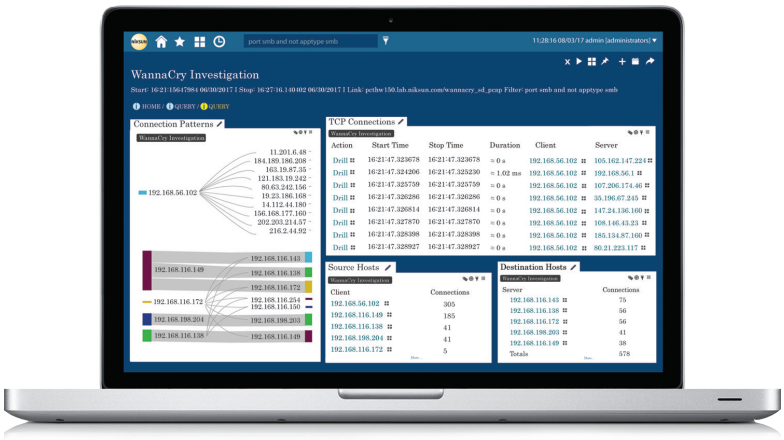

DETAILS

Vendor NIKSUN

Price Depends on configuration

Contact niksun.com

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Power and flexibility are key characteristics. We like the reports that come with the tool a lot but we really like the ease with which we can build our own..

Weaknesses None that we have experienced.

Verdict This is probably the best analytics tool we've seen and the notion of feeding with a SIEM is intriguing for its significant possibilities. We certainly will be doing that here in the Labs. NIKSUN has been SC Lab Approved since we started the program and we continue that for another year.

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

NIKSUN
NetDetector Suite

NetDetector Suite monitors all data flowing across the IP network and uses deep packet inspection techniques to accurately recognize, classify and analyze all applications, sessions and content traversing the network. Metadata is created in real-time on all content including email, IM, FTP, HTTP, and DNS. The tool alerts on suspicious traffic based on metadata content, for immediate notifications on policy violations, data exfiltration, malware and cyber attacks and records all data at the highest rates without dropping a single packet, and at the same time, also index all the data in real-time to allow for extremely fast searching. The tool provides robust analytics so spooling off data from a SIEM into the NetDetector provides enhanced analysis.

When you log into the system for the first time you will see quite a few windows. This is part of the html5 UI and you have a lot of options for what you see. One of the new features this year is a significantly increased suite of out of the box reports. One that we really liked was the security overview report. It is a sort of combination of many other relevant reports. In addition to the tabular drill-down, there is a good collection of graphical widgets. Just as from the tabular data, the drill-down is excellent. As with most NIKSUN reports you can drill down to the event and then past the event to the packet level.

Another report that we liked was the application forensics. The level of details is impressive. Drill-down gives greater detail. Searching is equally comprehensive, allowing RegEx searches. One of the widgets in this report is content type. NIKSUN does not believe the file extension so when it reports that a file that looks like a pdf is an executable, believe it.

This tool is aiming at becoming a network search engine with the objective of mining such data as metadata and string searches. These are remarkably fast given that the searches tend to be across large datasets. For example, using complex RegEx statements searches across the network for data in a DDOS attack revealed the IP address set for a botnet. The search took just a few seconds. Bounce diagrams show the back and forth activity and you can select a bounce diagram of the transactions of an event and drill down to the packet level.

When you select building a new report you get a menu of report components. Selecting the ones you want is all that is necessary and the tiles are created automatically. Then you can combine tiles into a full report page. Once you have built your report, you can cause the report to be sent to other users on a schedule. The reports show the power of the tool and the ability to create custom reports is limited only by your imagination.

They have markedly improved their use of intelligence feeds. Intelligence can be implemented from a URL, a file or a STIX/TAXII feed. The addition of STIX/TAXII is new. NIKSUN offers basic no-cost support and there are advanced, for-fee support packages as well. Documentation is excellent and pricing is reasonable.

– Peter Stephenson, technology editor