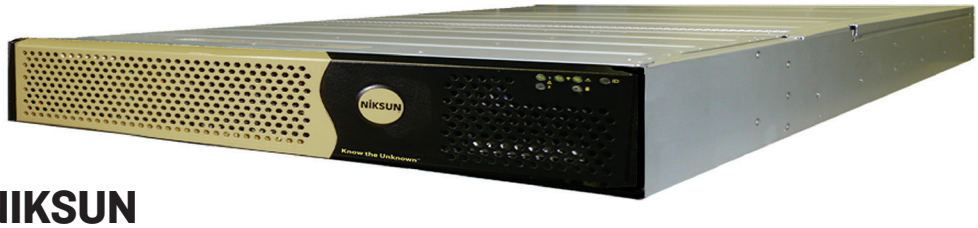

NIKSUN
NetDetectorLive NikOS Everest

NIKSUN has been a staple in our lab for several years and has always been one of our dependable workhorses. This latest version is no exception. However, there's a lot that's new here and we were impressed immediately. The most obvious update is to the user interface. But, we're getting ahead of ourselves.

When we received the appliance we installed it in our test bay. We fired it up and started through the initial configuration. Nothing. Dead on arrival. A panic call to NIKSUN support brought an engineer from the New Jersey offices to our lab in Michigan. Verdict was that the boot disk was damaged in transit. A new disk, a new OS image, and we were on the road. We finished configuration, connected it into our honeynet - the sensor port with no IP to our network tap and the management port to our internal network. Slick and quick.

Then we went to our lab computer and browsed to the management network. Yes... browsed. For those of you who are long NIKSUN users, that is a foreign term. NIKSUN now supports a slick UI called NikOS Everest - web based - that allows the user to create whatever desktop he or she wants. That means any desktop. Since the product sees everything as a report, all you need to do is drag in what you want - onto the screen, with no icons or code to write - and save it as your own report. Once you have the screens you want - and they may include the NIKSUN out-of-the-box reports - you have a fully customized UI to meet your needs. That could include specialized monitors that have your custom drill-downs.

We set up a suite of reports after we enabled the event monitoring - all events are defined using SNORT rules - and settled in on a particular project we are working on in our honeypot. We ran several other monitors - each with its own purpose - and we hoped that NetDetectorLive would give us a deeper dive into what the bad guys were doing as they attacked and probed us. We were not disappointed. Drill-downs got us exactly where we wanted to be and we were able to collect some interesting artifacts. Since we can reproduce an attack down to the bit level, we had about as good a picture as you're likely to get.

NetDetectorLive moved right into our lab, settled in between our PacketSled and our open source Maltrail and started giving us good data immediately. Once we had the dead disk replaced and the box up, it took us under a half-hour to configure and start collecting data. We monitor our honeypots 24/7 and this tool is going to give us exactly what we need to decode attacks and probes in detail. We can say with pretty firm assurance that just about anything you have in your SOC will give you more in the context of NetDetectorLive. This tool can stand on its own or it can augment your other monitors to give you a much deeper dive.

One of the nice things that we found was that since we monitor several open sources of indicators of compromise and some of them produce specific SNORT rules for particular indicators, we can copy/paste those SNORT rules into NetDetectorLive and that adds to our event detection and capture.

Support is superb, cost is very reasonable. You can go from the small system we have to a fully loaded box with lots of mass storage and there are virtual versions as well. The website gives you what you need to deploy and make the best use of the tool.

– Peter Stephenson, technology editor

DETAILS

Vendor NIKSUN

Price Depends on configuration.

Contact niksun.com

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

OVERALL RATING ★★★★★

Strengths Its new UI is its strongest feature in that it gives extremely flexible access to the rest of the strong functionality.

Weaknesses None that we found.

Verdict NetDetector always has been a good series for NIKSUN, but this new version tops everything they've done so far – except, perhaps, for the Supreme Eagle (see our First Look review, October 2015). Again this year, we bring the NetDetectorLive into the lab as SC Lab Approved, our highest award.

NIKSUN, Inc.
457 North Harrison St., Princeton, NJ 08540
609-936-9999 • info@niksun.com • www.niksun.com