NIKSUN Alpine

The NIKSUN Alpine as tested is an appliance that combines the NIKSUN NetDetector and NetVCR. This is a general purpose network forensic tool with a solid history. From a simplistic perspective, the appliance monitors the network, detects anomalous traffic and then allows a deep dive into the nature of the traffic. But, there really is a lot more to this tool than that.

First, the monitoring is intelligent, meaning that it knows what anomalous traffic is. So, this is not simply a sniffer or IDS. It is designed from the ground up to be a true network forensic tool. The appliance we tested has four network interfaces and can use them independently to monitor four different networks. We set it up with two: one in front and one behind our firewall. This allows us to compare traffic in-bound for our gateway with traffic that manages to get through it.

This tool is an analyst's dream. By starting at the dashboard, users can pick out those events that seem worthy of interest. For example, we recently experienced a SYN flood attack against our perimeter. While unsuccessful, we still wanted to know what we could learn about it. We can search the database on the Alpine for the source address and then reconstruct the attack. That is the NetVCR piece of the product. In this case, reconstructing meant examining the packets in detail. However, in the case of an internal user abusing internet resources by going to disallowed sites, for example, we can replay the user's session from packets captured by the appliance.

It is important to understand that this is not a SIEM. SIEMs combine and correlate flow and event data from other devices on the enterprise. Alpine generates its own data from packets that it sees moving past its interface. It then analyzes and can replay, as well as providing drill-down for lots of detail. In the case of the attack against our perimeter, we had visibility at the packet level so analysis can view the payload as well as the header or metadata.

Once a user finds something of interest in the summary view, there are several other views available for deeper analysis. One of the chief issues in tools of this type is visualization. Because there is so much available data, views can become cluttered and difficult to figure out. Not so with Alpine. The approach NIKSUN has taken is a mix of the traditional listing by event and a more web-like UI.

NIKSUN has excellent documentation in the form of PDF files. We needed just a bit of support when we deployed due to the nature of our virtual environment. That said, like other network appliances, users need to know their network in order to place sensors appropriately. Alpine is no exception, albeit an installation will require the admin to think a bit about where to deploy in order to get the most useful results.

NIKSUN offers both eight-hours-a-day/five-days-a-week and 7/24 support options. The standard support offers phone, email, FAQ listing and a knowledge base. The platinum offering provides all the above plus a dedicated supportnet. In addition, if needed, NIKSUN provides its customers with a technical service manager (TSM) and a dedicated customer support representative (DCSR) dedicated to a client as a single point of contact when troubleshooting issues arise.

DETAILS

Vendor NIKSUN

Price Depends on configuration, contact vendor.

Contact niksun.com

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	N/A
OVERALL RATING	★★★★★

Strengths Comprehensive, easy-to-use network forensic tool.

Weaknesses None that we found.

Verdict Regardless of the size of the organization, Alpine can help identify and analyze network attacks easily and effectively. Well worth attention. SC Lab Approved.

NIKSUN

Corporate Headquarters
100 Nassau Park Blvd
Princeton, NJ 08540
P: +1.609.936.9999 Toll Free: +1.888.504.3336
F: +1.609.419.4260
Email: info@niksun.com