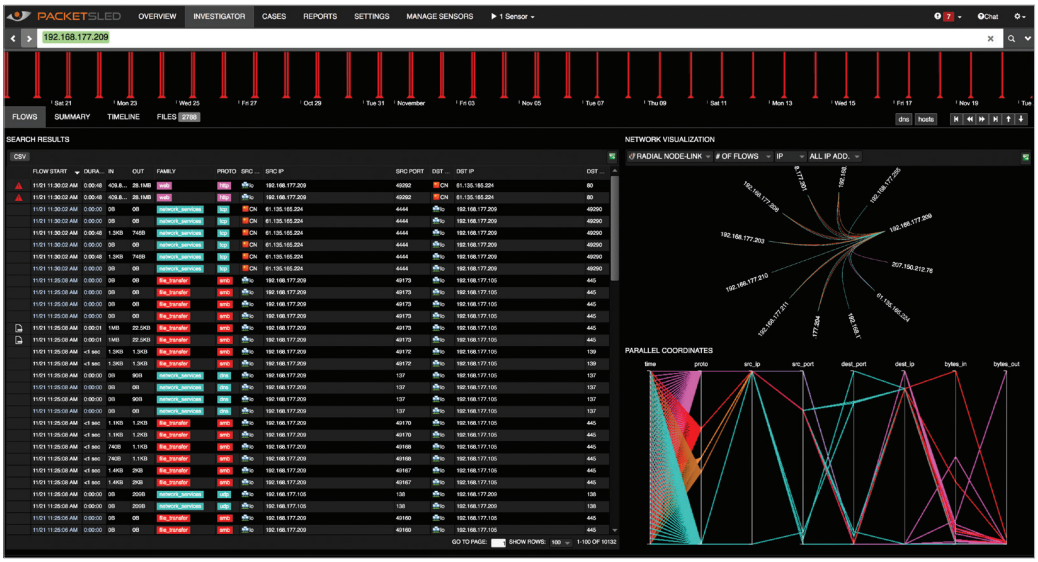
SC MEDIA
INDUSTRY INNOVATOR

Next-generation security monitoring and analytics

Packetsled



DETAILS

Vendor PacketSled
Flagship product PacketSled platform
Price Cloud packages start at $25,000 per year and range based on consumption and retention. Partners should contact PacketSled directly for on- premise packages; and for IR and MssP pricing.
Web packetsled.com
Innovation Strong application of advanced analytics, machine learning and flexibility with a powerful query language.
Greatest strength Vision and very strong technology along with a clear understanding of what the people who use the tool(s) really need to do their jobs.

Last year we introduced Packetsled as one of the tools we use in the Labs. Packetsled has some distinct advantages for us as we analyze activity against our honeynet and our deception network. Probably the biggest for us is the combination of an excellent query language and the ability to create alerting chains of events based upon IoCs very easily using IRES (Incident Response Expert System). We have several of the customized alerts and they have worked well for us, particularly since we deployed a TOR relay node. Using Packetsled we can learn a lot about a particular data stream. We also have used the customizing capability to create unique tests that we want to apply during an experiment. While you may not be experimenting as we do in the Labs, you may have repeated attacks that you want to trigger off. This lets you do that very easily.

This innovator has built the tool around Bro, the cyber security language and intrusion detection monitor. We like that because we can extract Bro logs and use them as part of our analysis. However, probably a better reason is that, even though it is open source, it is fairly standardized and reliable.

Visualizations are very straightforward and there is a lot of drill-down. This year there has been more emphasis on the kill-chain and we have found that quite useful. In addition to the sensor deployed at the Labs, we have had the opportunity to work with a deployment at a small financial institution where five sensors are deployed. It is a core tool for the security team there.

Earlier this year the innovator deployed a specialized version of the tool aimed at incident responders. It is a lightweight sensor package that is easy to deploy and have running in minutes. The available forensics is excellent and we had fine results using the tool in conjunction with such typical techniques as log analysis.

– Peter Stephenson, technology editor