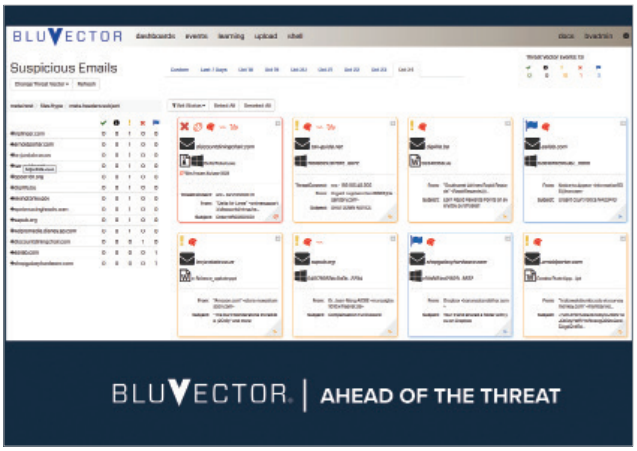
SC MEDIA
INDUSTRY INNOVATOR

Next Generation Security Monitoring and Analytics

BluVector



DETAILS

Vendor BluVector
Flagship product BluVector
Price Starting at $1,000/mo
Web bluvector.io
Innovation Analysis of the incoming data stream to identify malicious code before it enters the enterprise
Greatest strength Persistence and vision to see a need, develop a response to it and keep innovating along the way and going forward.

Last year we characterized BluVector as an on-the-wire hunting tool. The idea was that by being on the wire a measure of proactive hunting occurs before the malicious traffic even gets inside the enterprise and starts to do its damage. It turns out that in its current incarnation it is somewhat more than that. In fact, the company – and BluVector spun out of its prior owners to become fully independent this past year – describes the tool as, among other things, a next generation intrusion detection system. We think that is something of an oversimplification. It does that but BluVector excels as a proactive hunting tool.

Over the past year this innovator has done some interesting things. For example, it has developed what it calls a speculative execution engine for zero-data malware detection. This consists of high speed emulation where it examines the scripting code/language of suspected malware and enumerates possible malicious activity. Doing this at wire speeds is quite an accomplishment. To do this the company has invested 8 years in training its patented, machine learning-based detection and intelligent decision support engines to enable security analysts to find, confirm, and contain the newest and most sophisticated threats.

The company has added new engines for several other rule sets and third-party threat intelligence feeds. This all is part of creating a next generation network intrusion detection system with new analytics paradigms such as Yara and suricata, giving better visibility across the entire attack life cycle. Over the past year 90% of this innovator's efforts have focused on expanding on core competencies such as fast detection. BluVector also has focused on simplifying use for mid-markets and managed services providers. The company now has a virtual machine (for VMWare ESXi 6.0 and above) with cloud-based management that leaves data on customer's premises.

The company is growing and adding employees regularly now that it has spun off as an independent company. This is the starting point for new ways to view malicious behavior coming at the enterprise. More than a next gen NIDS, BluVector is the next generation of threat hunting tools that hunt the threat before it can enter the enterprise.

– Peter Stephenson, technology editor

BLUVECTOR®

BluVector
4501 North Fairfax Drive
Arlington, VA 22203
571.565.2100
https://bluvector.io