SC MAGAZINE First Look

BluVector

BluVector

BluVector is a threat hunting tool on steroids. It differs from other threat hunting tools in that it works on the data stream instead of seeking static code on the target platform. It operates at line speed and is capable of performing malware analysis on the fly. The heart of the tool is a souped-up BRO cluster. BRO is a threat intelligence framework with its own unique language. It was designed from the ground up to be what it is rather than being a re-jigging of another framework to work in the threat intelligence space.

BluVector connects to a SPAN port or tap and can support line speeds of up to 10 Gbps. It is an on-premises tool that lives in a 2U server appliance. When we connected with the server we dropped into a pretty vanilla dashboard. But looking at the statistics was anything but vanilla. This gave us a taste of why this is a significant entry into the threat hunter's tool kit. We noted that it had analyzed 1.9K events. Of those it found only 57 interesting enough to dig into more deeply. After that stage of the analysis it identified only 4 events as malicious. The amount of time and effort this saves the threat hunter is really impressive.

We were able to dig down to the events themselves and continue our analysis in a much more efficient manner than if we had to comb through 1900 events or, even, 57. The tool pulls in the network feed through a collector and then passes it to a scalable file analyzer. This looks at files on the fly and analyzes them and their associated possible events.

The brain behind BluVector is Hector, a proprietary malware analyzer that uses machine learning to isolate probable malicious events. It can analyze thousands of objects per second without losing anything through executing the object. Executing takes time and the resulting analysis would be extremely difficult – if not impossible given today's technology – at line speeds.

The tool integrates with a number third party systems including SIEMs, threat intelligence tools and feeds (including STIX), sandboxes and incident response tools. We especially liked the way it integrates with sandboxes such as Cuckoo, which we use in the lab. The use of these third party tools is a post-process that does not slow down the on-line analysis performed by BluVector itself.

This is not an inexpensive product at $188,440 but in our view it is worth every penny for those organizations that depend upon sensitive data and have large environments to protect. This is a case of knowing what your environment looks like, what data you need to protect and to what degree you need to protect it. Then, comparing that to your upstream liability in the case of a breach and data theft, you can work out the financial justifications fairly easily.

The web site is quite marketing-oriented without the usual support portal which we think that it needs. However, the company offers one and three-year support agreements that include software updates. This is definitely not for organizations that have very limited need for asset protection but for those that need rock-solid cyber threat protection this is without doubt a product that demands your attention.

AT A GLANCE

Product BluVector

Company BluVector

Price Starts at $188,440

What it does BluVector is a cyber hunting tool intended to detect very stealthy attacks.

What we liked This is a very serious threat hunting tool that unlike many others operates on the data stream.

The bottom line If you are a large organization or if you deal with very sensitive data – banks, hospitals, government agencies – you need to take a serious look at BluVector. It's not the attack that we know about that keep us up nights... it's the ones we don't even know occurred and that is what this tool is focused on.

BLUVECTOR®

8666 Veterans Highway
Millersville, MD 21108
1.855.672.4258
info@bluvectorcyber.com
www.bluvectorcyber.com