BluVector® Advanced Threat Detection (ATD)

State of Threat

As cybersecurity threat actors improve their efforts with sophisticated technologies and tactics, enterprises are faced with the reality that their security stack lacks the capabilities to effectively detect, prevent, or respond to all attacks. Current enterprise prevention techniques such as next generation firewalls and endpoint protection are effective only against known threats. Next generation detection techniques such as sandboxes cannot keep up with increasing network speeds, resorting to sampling.

In response, enterprises have largely shifted from detecting exploits to hunting for threats already inside their network. In 2019, the dwell time of the average threat from compromise to discovery was 56 days. Enterprise threat hunting teams are accelerating detection but averages still outpace the window threat actors can inflict damage and/or steal information. Impacts organizations cannot afford.

Advanced Threat Detection Solution

Machine-learning offers the chance to shrink the threat detection window to within the attackers' OODA loop; allowing threats to be eradicated prior to impact. BluVector's Advanced Threat Detection solution leverages supervised machine-learning to analyze **every** file transitioning an enterprise network and determines the file's malignancy. The result of over ten years of research, BluVector includes over 40 content-specific, supervised machine-learning classifiers that detect malware with efficacies in the 98+ percentile.

Benefits and Features

- **Network Defense Teams shift detection of threat actors from within enterprise to enterprise edge**
  - BluVector's Machine-learning determines the malignancy of all content on enterprise networks
- **Cyber Analysts rapidly triage to orient themselves to extant threats**
  - Extensive content-layer logging by BluVector's Machine-learning combined with Zeek's network and application logging provide extensive visibility into network events
- **Pre-breach discovery empowers Incident Response teams to stop threat actors prior to causing harm in the enterprise**
  - BluVector discovers threats at the enterprise edge at wire speed and with high efficacy; Responses can be automated to stop attacks
- **AI-powered, in situ learning, enables sharing of zero days immediately across the enterprise**
  - Learning is shared and managed solely on premise

Realized Customer Value

Accelerate Detection

By focusing our Machine-learning on malware detection at the network, BluVector detects threat actors' initial delivery, prior to execution and impact. Even the most sophisticated computer network defense teams routinely catch threat actors on the "way out" when they connect to command and control domains that are known. BluVector catches threat actors on the "way in". Detection this early in the attack chain minimizes the potential impact of threat actors who make it past network defenses.

Accelerate Triage

BluVector delivers our patented Machine-learning Engine atop the best of class Zeek Network Security Monitoring tool. Zeek's extensive network and application logging is elevated by BluVector's content-layer logging equipping analysts and threat hunters with comprehensive insight into threat actors' actions. This combination typically replaces existing enterprise investments in NetFlow, intrusion detection systems, and in some cases, full packet-capture thus saving resources while still providing the insight network defense teams require.

Accelerate Response

By analyzing **all** network data, presenting analysts with comprehensive insight and operating at network wire-speed, BluVector equips network defense teams to react to threat actors at the delivery or pre-breach stage of the kill chain. Enterprises can push previously unknown malware signatures to endpoint protections to block execution or add previously unknown delivery domains to firewalls to block further downloads. All of these can happen prior to the threat actor executing their malware within an enterprise.

BLUVECTOR®
A COMCAST COMPANY

Technical Overview

BluVector Advanced Threat Detection deploys as a 1Gbps to 20Gbps speed network appliance to packet brokers, IMAP (email), TAP, or SPAN ports on major network choke points such as connections to the Public Internet or inter-organizational connections. It leverages the Zeek Network Security Monitor software to acquire, identify, reassemble, and log network traffic. It can also input pcap files from other network collection systems. Network and application layer traffic is analyzed by a bundled instance of the Suricata Intrusion Detection System. All network content is analyzed by bundled ClamAV and Yara anti-malware engines. Uniquely, all network content is analyzed by BluVector's patented Machine-learning Engine to produce static analysis metadata and flag malignancy. Specific content used by fileless malware techniques is analyzed by BluVector's patented Speculative Code Execution engine to determine malignancy. Customer provided Threat Intelligence feeds, Active Directory probes, and Domain information can further illuminate traffic insight. Integrations with endpoint protection and security orchestration technologies enable automated and manual response to stop threats.

BluVector's system operates wholly without connection to the public Internet. Customer data is never shared with BluVector. Also, manual remediation feed back to the Machine-learning engine is used to retrain in place via a patented technique called In-Situ retraining. *This ensures an ever, increasing level of detection accuracy that remains wholly-owned and controlled by the client*.

Market Traction

BluVector's solution has been around for almost a decade and operates within a Fortune-50 Company: Comcast. Comcast is both the company owner and BluVector's largest client. Comcast relies upon BluVector to monitor over 130Gbps of Internet Traffic with deployments that will bring the number to over 300Gbps. BluVector has enterprise-wide deployments within the US Department of Defense and US Treasury, Municipal Law Enforcement, and commercial customers in manufacturing, finance, and telecommunications.

- 2018 – Best performing Advanced Threat Detection platform per DHS after a 10-month test of over 100 technologies
- 2018 – Selected as the best performing machine-learning based advanced threat detection engine by MITRE
- 2018 – Selected as central analytical engine for DARPA's Cyber Hunting at Scale (CHASE) solution
- 2019 – Won CYBERCOM's Rapid Prototyping Exercise for Malware Identification
- 2019 – Comcast acquisition after testing for cyber initiatives
- 2019 – Best Network Security Appliance in National Cyber Range test conducted by ORNL
- 2019 -- 99.8% detection against the 2019 Miercom Malware Suite – 11.4% higher than the Industry Average of network security solution detection products

Draft – Proprietary & Confidential