BLUVECTOR®

BLUVECTOR® CORTEX™

RELEASE 3.1 OVERVIEW

Release 3.1 of BluVector Cortex introduces new capabilities across the product, with features that improve detection coverage and enable automated investigation.

BluVector Cortex is an AI-driven sense and response network security platform. Designed for mid-sized to very large organizations, the platform makes it possible to accurately and efficiently detect, analyze and contain sophisticated threats including fileless malware, zero-day malware, and ransomware in real time.

Release 3.1 of BluVector Cortex introduces a series of "no-click" investigation features and detection coverage enhancements to the award-winning platform, allowing customers to sense and respond to even the most advanced threats earlier in the kill chain.

Major New Features and Enhancements
Cloud Email Analysis Including Office 365 and Google for Business
Detection of Malicious VBScripts
Dynamic Malware Analysis in the Cloud
Event Reporting Dashboard
Expanded Threat Intelligence

Detection Coverage Enhancements

Cloud Email Analysis

BluVector Cortex can analyze any cloud-based IMAP email service including Office 365, Google for Business and other major providers. The platform identifies threats in milliseconds with minimal noise and extremely low false positive rates, providing detection of phishing, spear-phishing, ransomware, and credential-phishing attacks that evade traditional defenses.

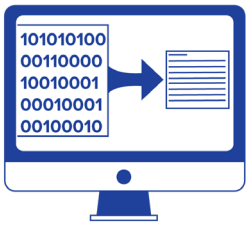
Detection of Malicious VBScripts

BluVector Cortex examines all files to look for and analyze embedded malicious VBScript, an increasingly common attack vector. This detection capability comes as a new classifier of the patented Machine Learning Engine (MLE) of BluVector Cortex. Like BluVector MLE's other classifier engines, this new engine is pre-trained to detect malicious scripts upon deployment.

No-Click Investigation Features

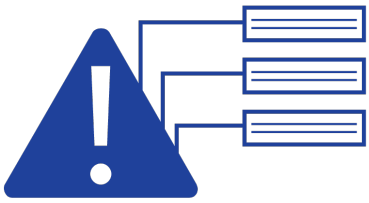
Dynamic Malware Analysis in the Cloud

With the introduction of the new Dynamic Malware Analysis Cloud, BluVector Cortex users will be able to automate secondary analysis of flagged malware content. Additional context associated with the inner workings of the captured malware is added to the battle card, making it possible for analysts to gain a deep understanding of how the malware was constructed.



Event Reporting Dashboard

With Release 3.1, BluVector Cortex provides a new reporting dashboard that provides even greater visibility into network traffic. This dashboard automatically translates the rich network traffic data generated by BluVector Cortex into easily understandable insights.



Expanded Threat Intelligence

Threat intelligence feeds have long been used by BluVector to provide context around suspicious events, as well as to identify lateral movement post-breach. With release 3.1, BluVector Cortex comes with its own integrated threat intelligence feed, further improving customer ROI.

BLUVECTOR®

GET AHEAD OF THE THREAT

BluVector is revolutionizing network security with state-of-the-art AI, sensing and responding to the world's most sophisticated threats in real time. Stop waiting for breaches to happen. Get ahead of the threat.

www.bluvector.io | 571.565.2100