BLUVECTOR®
A COMCAST COMPANY

BluVector Automated Threat Hunting™

Hunt Down Threats Faster

BluVector Automated Threat Hunting™ (ATH) gives security operations teams actionable insights so they can focus on hunting, not data.

Network security teams are encountering an increasingly broad-spectrum of cyber threats from novel attack vectors. The tools used for threat identification and response have not kept up.

What does BluVector ATH™ do?

Automated Threat Hunting and Analysis

Automates the time-consuming analysis of security events and augments the impact from proactive hunting of threats.

Automatic Campaign Identification

BluVector ATH correlates behaviors and detections and presents a synthesized view of the entire attack campaign rather than individual alerts. The Attack Campaigns feature automates security detections by connecting the dots of related attacker behaviors and exposing the relationship between entities (users / hosts) across internal detections, external advanced command-and-control detections, and connectivity to common command-and-control infrastructures.

Malicious Intent Detection, Post Compromise Recon and Lateral Movement

BluVector ATH expands Situational Awareness by detecting post compromise recognizance and lateral movement with streaming behavior detection, real-time collection, storage and processing of rich network metadata, and relevant logs including data from Cloud Service Providers

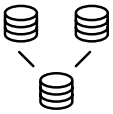
Provide Actionable Insight To Reduce Alert Fatigue

BluVector ATH correlates all behavioral detections generated by the system to the associated entities (user / host). The correlated alerts include an abundance of contextual information such as a related detection timeline, mapping to MITRE ATT&CK techniques, and related compromised entities involved.

How BluVector ATH™ solves common hunting problems.

BluVector Automated Threat Hunting™ (BluVector ATH™) focuses on finding threats already inside your environment, including insider threats.

Shows the complete story of what happened with suspicious user, host and over all enterprise behaviors, even if the clues are subtle and spread out over time.



Analyzes behaviors within your network over time by examining log data generated from the security stack, identifying potential campaigns, and enabling automated threat hunting and analysis.

Learns what is normal for your network environment and alerts analysts at the earliest possible moment of anomalous behavior or activity using advanced analytics that has reached a user defined level of interest.

Provides rich information about the wide variety of hosts and users in your network.

Uses AI to widen your security team's capability by processing massive amounts of data quickly and alert them to indicators of potential indicators of compromise (IoCs) – even ones that have never been seen before.

What makes BluVector ATH™ unique?

Actionable Insights

Security Analysts can view the narrative of what happened in a cybersecurity incident. For example, analysts can see human-readable reasons for concern, the device, and the associated country, along with event information of what occurred before, during, and after an incident. From the captured history of events, ATH joins the dots and provides actionable insight by categorizing bad actor techniques to the MITRE ATT&CK® framework.

Open Platform

Advanced security operations teams understand their infrastructure and have purpose-built analytics to meet their threat hunting requirements. BluVector ATH is an open platform providing full flexibility and multiple options for security teams to get the benefits of a purpose-built solution at a fraction of the required time and effort.

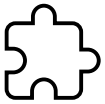
Campaign Identification

Threats are detected in entities (users, hosts) in real time through streaming behavior analytics. ATH synthesizes security alerts related to the high-risk entities into a Campaign graph/story on a periodic basis and tracks the evolution of the campaign graph/story.

SDK

BluVector ATH provides a software development kit that provides advanced security operations teams capability to build custom analytics as a fully embedded plugin, or by subscribing to the same message queues as ATH built-in analytics. Existing analytics can also be integrated into BluVector ATH using a 'shim' layer and/or RESTful APIs

Security operations teams can:



Build custom analytics with the SDK as a fully embedded plugin

Build custom analytics by subscribing to the same message queues as the BluVector ATH built in analytics

Use existing analytics and integrate them into BluVector ATH using a 'shim' layer and/or RESTful APIs.

How BluVector ATH™ Works

Comprehensive network activity data from multiple sources is streamed into ATH where it is categorized and correlated to entities (users and hosts). Activities are analyzed for suspicious behaviors resulting in analytic hits. Once, identified these suspicious behaviors elevate the risk score related to entities. An informational view provides insight into all the factors that contributed to an elevated risk score and a likely attack, including identified hosts, users, and external domains.

All activity data is recorded in an easy-to-read format with the ability to replay the data like a Network DVR. The platform knows how to track the same entity (user, host) if its IP address or name or observables change during the entity's life cycle, handling network temporality to significantly reduce false positives.

The scoring method is configurable using simple, fixed or multiple critical factors of the entities based on the analytic hits.

BluVector ATH automatically researches the entities (users, hosts) with high-risk scores to identify potential attack campaigns. All of the relevant data is stored for future use, accessible via a user interface or sent to an external system for additional analysis or response actions using SOAR or open standards.

Product Benefits

Threat hunting at scale:

Improved analyst workload by automating Hypothesis-based threat hunting approach, suppressing false positives, showing prioritized risk scores, and performing automated research using AI and not relying on threat intelligence to identify threats that were not blocked.

Extend your analytics capabilities:

Pluggable analytics framework with a software development kit that organizations can leverage to integrate with customer-built / pre-existing machine learning analytics.

Mind the gap:

Enables security teams in identifying dangerous visibility gaps and avoid detection gaps. Improved analyst efficiency and detection with feedback to the SOC from threat hunting teams using the product.

Data to information to actionable insight:

Advanced machine learning models enable real-time streaming anomalous host or user behavior detection. Security teams can monitor behaviors, not just streams of alerts. Enables security teams to hunt down unknown threats leading to better visibility, better discovery, and ultimately better defense.

Purpose Built & Flexible deployments:

Deployable to any environment – on-premises, in the cloud, and even air-gapped without requiring information sharing to a centralized back-end.

BluVector
4501 North Fairfax Drive, Arlington, VA 22203
www.bluvector.io

BLUVECTOR® A COMCAST COMPANY | COMCAST