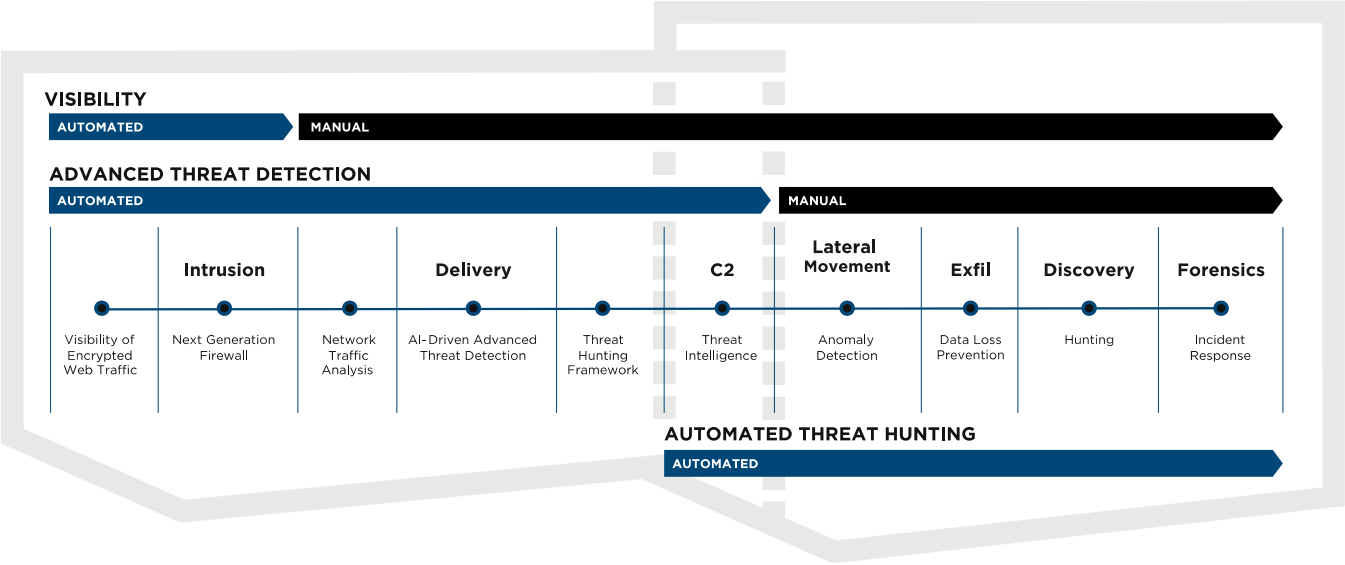
BLUVECTOR®
A COMCAST COMPANY

BluVector Capabilities Overview – Executive Summary

BluVector offers proven, supervised ML capabilities across the entire malware attack chain – we provide industry leading detection accuracy of unknown malware and insider threat/anomalous behavior, all at wire speed. Security analysts make faster, more accurate, more automated decisions and eliminate wasted time on false alerts.



Our supervised ML **detection** algorithms deploy **fully trained**. We **detect bad content, signature-less (zero-day) malware**. We are proven and deployed at:

- DHS, where we are Authorized to Operate (ATO) on the .gov domain.
- DISA, where we are at Full Operational Capability (FOC) and Interim ATO on the .mil domain (across multiple Internet Access Points, multiple continents).
- COMCAST, our country's largest ISP, where we currently provide coverage of over 4 billion events a day, at an aggregated throughput over 350 Gbps.

Our detection accuracy reduces sandboxing requirements. This benefit enabled COMCAST to **reduce its pre-existing security expenses by over $10 million per year**.

For the **threat hunting of bad behavior**, we offer capabilities proven in DARPA's Cyber Hunting At Scale (CHASE) program. Our hunting platform provides retrospective and real-time analysis across all class of enterprise users, devices, and behaviors. Key capabilities include:

- An open platform, enabling clients to see and control all facets of a hunting campaign, including a DVR playback feature for forensics and staff training.
- An open standards-based analytics framework with a software development kit (SDK) to develop your own unique mission-centric hunting analytics.
- A content management correlation engine enabling "best in class" detection accuracy across **all** users, entities, devices, and applications.

We can offer "best in class" detection accuracy evaluations (i.e., "bake off's") where we earned highest detection accuracy with:

DHS (twice by MITRE) DISA (for ID66) USCC (for RPE#5)
US Navy (PMW130) Miercom (3rd party)

POC: **Larry Gloss**, larry.gloss@bluvector.io