

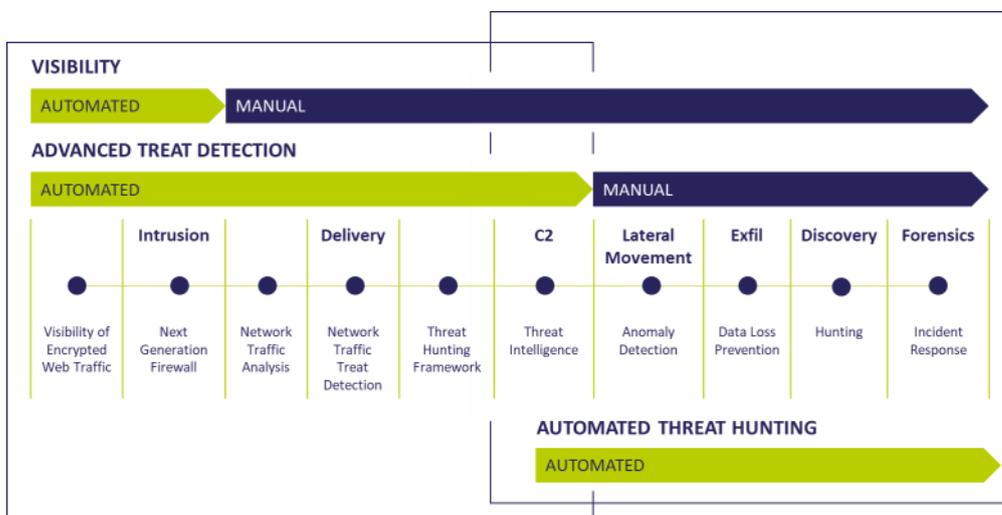


Responding quickly to cyber security threats is imperative

SA Group have partnered with BluVector to offer a highly accurate AI-powered Advanced Threat Detection system. Owned by American telecommunications company Comcast, BluVector are broadening their market into the UK and Europe by selecting SA Group as their mission partner.

This innovative solution includes built-in machine learning algorithms to increase cyber resilience, and uses intelligent edge software providing near real-time insight from data, whether it is seconds or years old.

Multiple layers of security controls and defence, both perimeter and endpoint, give the strongest protection of one IT system and safeguard valuable data and information. The system detects against the most modern, advanced threats including Nation-state and Polymorphic malware threats with ever-increasing resilience and accuracy to protect against developing threats.



Features

- Ever-increasing detection accuracy improves analyst response and decision making
- Automated workflow with full network visibility
- Built-in machine learning algorithms increases cyber resilience
- Integrates with existing customer threat detection systems

Benefits

- User-friendly interface, no need to understand Artificial Intelligence
- Less time spent chasing false alerts
- Faster detection and resolution
- Lower costs of alert management
- The easiest way to collect and analyse vast amounts of geographically distributed data

Award Winning

The product has been recognised for its innovation and unique technological approach, including selected as the best performing Advanced Threat Detection platform by the United States Department of Homeland Security after a ten-month test of over one hundred technologies

About BluVector

Well established in the US, BluVector is a trusted partner to both Fortune 500 companies and large government agencies working to tackle some of the nation's most critical challenges.

The company worked with the US Intel Community and their threat data for 8 years, and has the proven ability to protect against emerging threats an average of 13 months in advance.

Trusted by Government and Commercial

The product is actively in use across global Governments and commercial networks.

Comprehensive Threat Detection Coverage

100% network coverage with flexible deployment options and a modular design enabling scalability from remote offices to the data centre core.

Efficient and Cost Saving

Actionable events are prioritised with context to improve analyst efficiency and reduce operational costs.

Detection with Confidence

Quality threat indicators to help security analysts get answers.

Complements Current Security Monitoring Software

Complementary of software such as Zeek by offering many associated analytics including automated correlation of threat metadata, configurable analyst workflows along with threat scoping.

Eases Management of Mass Data

Aids customers to manage the volume, velocity and polymorphic nature of cybersecurity threats.



About SA Group

SA Group is a business management consultancy solving critical, highly complex challenges by designing, implementing and supporting secure mission critical infrastructure.

The company supports organisations in both the commercial and public sectors to deliver vital projects, including the challenging defence environment, working collaboratively with clients to create value, maximise growth and improve business performance. SA Group's experience of protecting mission critical infrastructure within Defence and Critical National Infrastructure complements BluVector's world-class Advanced Threat Detection capability proven within US Government and Defence and backed by Comcast who creates incredible technology and entertainment that connects millions of people.



SA Group Cyber professionals are highly experienced in designing solutions to protect digital infrastructure against cyber threats. When implementing Advanced Threat Detection (ATD) we start with a comprehensive review of current defence measures, identifying security vulnerabilities and advising in line with our Cyber blueprint the best way to deploy and maximise the capabilities of ATD (technology, people and processes) whilst ensuring compliance with ISO 27001, FFIEC, NIST, 10 Steps to Cyber and Cyber Essentials.

Scalable Performance - Designed to adapt to the customer's need. Advanced Threat Detection is offered as both a VM, as well as 1U-2U hardware appliances.

Not a Black Box - Every security team has invested time, effort and expense in tailoring their security stack to meet the needs of their business. With BluVector, security teams can continue to operate their custom Zeek/Bro scripts, Yara rules Suricata.

A Better Workflow - ATD presents dataflows within the context of an event and the analyst's broader workflow to reinforce each time saving feature. Events are correlated and scored, so analysts can more efficiently understand where they should focus. Information including network metadata targeted around the event, Active Directory user information, results from embedded sandbox, hex detail for fireless attacks and the actual content payload are all easily accessible.

