

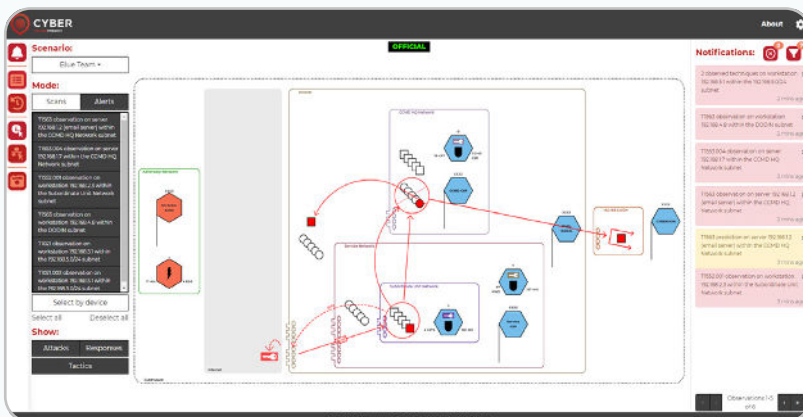


CyberAware | Cyber security and autonomous cyber defence

Powered by



PRODUCT SCREENSHOT



Key features

- › Intuitive dashboard with APP-6 / MIL-STD-2525 extended symbology.
- › Integrated with SO2 for real-time network monitoring using Zeek and Suricata.
- › Network weaknesses mapped using National Vulnerability Database (NVD) feeds.
- › Predictions underpinned by Common Attack Pattern Enumeration and Classification (CAPEC), MITRE ATT&CK and Unified Kill Chain (UKC).

Benefits

- › Predict both future cyber-attacks and the next steps of evolving attacks in real-time.
- › Mitigate the next steps of cyber-attacks before they happen.
- › Convey mission-relevant information to commanders unfamiliar with the technical details of cyberspace.
- › Developed in partnership with Dstl and DASA using feedback from CPTs.

Product overview

Traditional cyber security methods only respond to known threats, allowing defenders to react at best in real time, or at worst forensically after an attack.

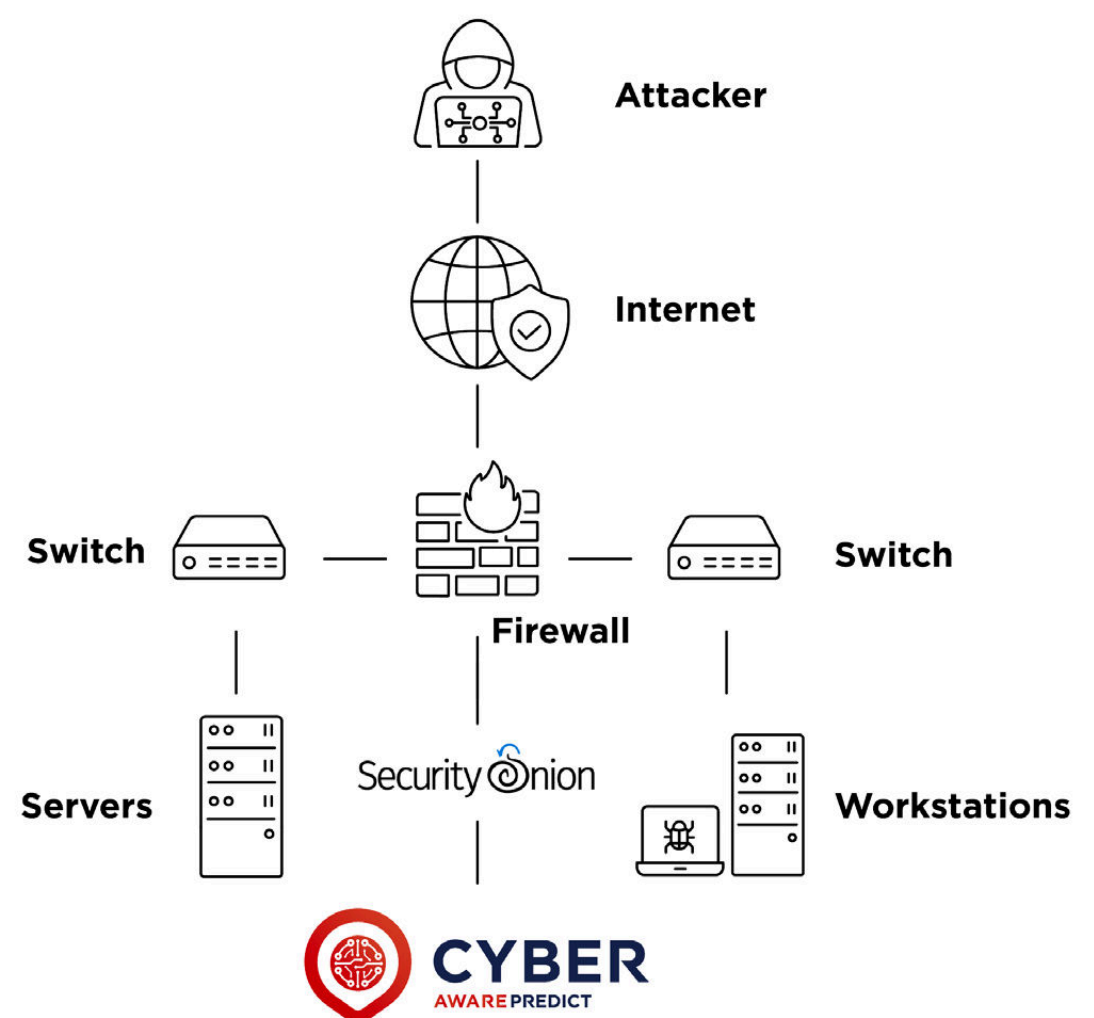
CyberAware Predict is an advisory dashboard that can predict both future cyber-attacks and the next steps of evolving attacks based on network scans, real-time monitoring and threat intelligence.

Using live network traffic, Intrusion Detection System (IDS) events and the latest software vulnerabilities, underpinned by the MITRE ATT&CK framework, CyberAware Predict advises analysts on how to detect and mitigate the next steps of attacks before they happen.

Using extensions to military symbology, the intuitive dashboard allows analysts to convey mission-relevant information to commanders unfamiliar with the technical details of cyberspace.

Software detail

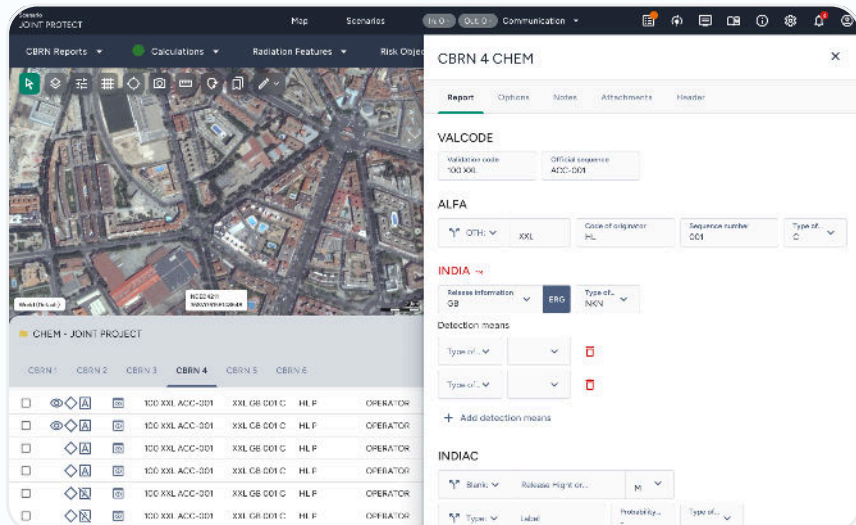
CyberAware Predict is a set of containerised microservices that integrate with Security Onion 2 (SO2). Zeek network traffic and Suricata IDS events from SO2 provide CyberAware Predict with real-time information, allowing it to learn network topology, observe the initial cyber-attack and infer network weaknesses. The analytics then considers software vulnerabilities, adversary attack patterns, adversary tactics and techniques, and kill chain progression to provide next-step predictions with associated confidences.



Credentials

CyberAware Predict has been developed in partnership with Dstl and the Defence and Security Accelerator (DASA) under the Predictive Cyber Analytics (PCA) programme. It has been developed across three separate phases and has been assessed in a relevant environment to Technology Readiness Level (TRL) 6. During development, hands-on feedback from Army, Navy and Air Force Cyber Protection Team (CPT) users has driven the design of the dashboard. Trialled at the NATO Locked Shields 2024 exercise with Swiss Cyber Command.

Related products



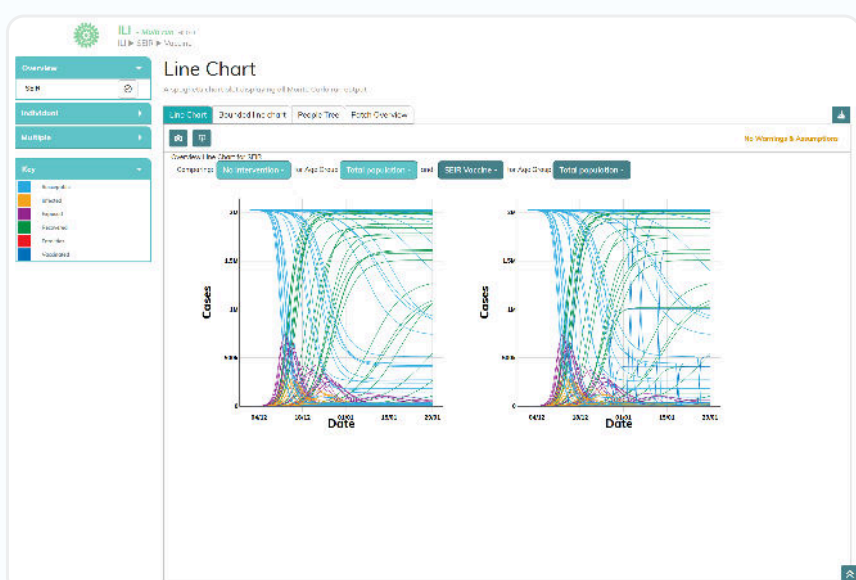
CBRN-Analys NG

- CBRN-Analys is an advanced, off-the-shelf software-based CBRN Knowledge Management Application that includes Hazard Prediction and Warning and Reporting.
- Configurable and modular, it provides commanders with rapid and accurate information to increase their CBRN situational awareness within an area where CBRN materials may be used.
- CBRN-Analys effectively supports and enhances risk-management in all phases of an operation, both in the planning and pre-deployment phase, in-theatre and in the post-conflict or recovery phase.



UrbanAware

- Optimise real-time decision making with superior situational awareness. UrbanAware is a next-generation CBRN Information Management (IM) tool for the military, first responders, and local government.
- Its aim is to provide lifesaving situational awareness and decision support in the context of urban CBRN and HazMat incidents, helping stakeholders to develop more effective response processes.



CrystalCast

- CrystalCast is a disease forecasting tool that combines multiple epidemiological models to predict outbreaks and anticipate impacts on the population.
- The software provides statistical outputs relating to “what-if” scenarios, allowing key stakeholders to weigh up uncertain conditions and parameters before taking appropriate action.

More information can be found at: www.bruhn-newtech.com.

