CYBER
AWARE RESILIENCE

PRODUCT SHEET

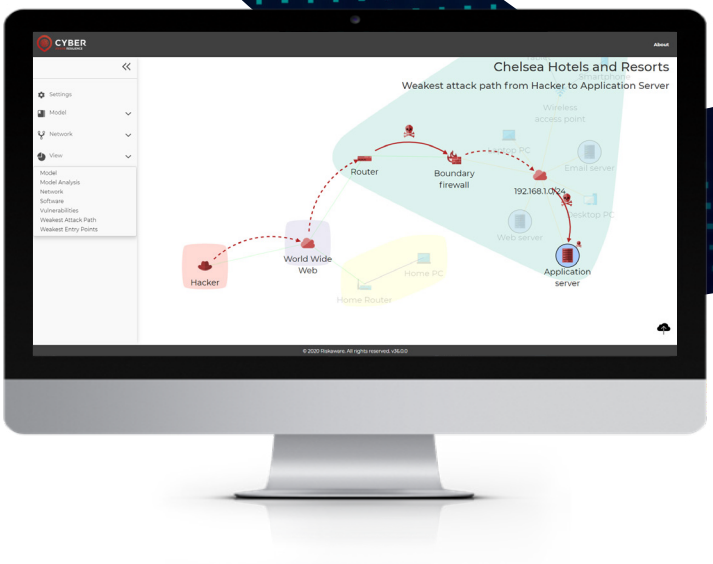
Multi-stage cyber attack and mission impact assessment analytics

OVERVIEW

CyberAware Resilience is a system that determines the potential impact of cyber attacks on missions or businesses. By integrating network scans, vulnerability feeds and mission or business models, it provides insights into complex scenarios that bridge the cyber and physical domains. This enables users to simulate, assess and mitigate network threats.

The intuitive web-based user interface produces in-depth analysis, giving cyber analysts an intimate understanding of their cyber terrain, cyber vulnerabilities, and viable cyber attack paths that adversaries could use to compromise critical assets.

CyberAware Resilience has a flexible impact assessment data model, built on detailed network topology and vulnerability information. It can be leveraged in a variety of sectors, from defence and critical national infrastructure, to finance and healthcare. The system can also be deployed as a standalone tool, or be integrated into existing cyber security platforms to provide detailed analytics that go beyond current cyber vulnerability assessments.



CREDENTIALS

Riskaware developed CyberAware Resilience to analyse and visualise the effect of a cyber attack on a mission, with initial funding from the UK Centre for Defence Enterprise. It was further developed and integrated as the core cyber-mission risk analytics component and cyber analyst user interface in the Joint User Mission Planning (JUMP) concept demonstrator for MoD, in collaboration with BMT and funded by Dstl. During that work, JUMP was tested at military exercises and presented at the NATO IST-153 Cyber Resilience Workshop and Operations Research and Analysis (OR&A) conference.

SOFTWARE DETAIL

CyberAware Resilience is a set of microservices underpinned by a scalable connected-graph database. It can import network scans, mission models and vulnerability feeds, as well as providing interactive editors to create and augment the data. The full suite of analytics is available either through a GraphQL Application Programming Interface (API) or an intuitive web front-end which provides visual analytics for enhanced cyber situational awareness.

CyberAware Resilience allows users and client applications to perform a topological vulnerability analysis of their networks. This computes an attack surface on which sophisticated, multi-stage cyber attacks can then be modelled.

The system can simulate attack paths that consider attacker sophistication and determine the weakest network entry points that would allow attackers to reach critical assets. Users can then conduct impact assessments that show the local and overall effect of each attack on the mission or business. Once potential attacks are identified, CyberAware Resilience gives users the opportunity to simulate patching before allocating time and effort to mitigation tasks.

With this information, mitigations can be targeted at mission or business-critical vulnerabilities. CyberAware Resilience allows users to optimise their patching strategy by prioritising the least complex attack paths to quickly improve mission or business resilience to cyber attack.

FEATURES

- Intuitive web-based interface with interactive visual analytics
- Network attack surface analysis using the National Vulnerability Database (NVD)
- Multi-stage cyber attack modelling
- Network entry point analysis
- Mission or business impact assessment
- Simple API and modular services for integrating into existing cybersecurity platforms

BENEFITS

- Quickly assess the cyber resilience of any mission or business
- Optimise patching strategies to defend mission or business-critical assets
- Import network details from scans or asset management systems and automatically map vulnerabilities
- Model missions or business processes at any level of detail
- Consultancy and integration support is available from our expert team

ABOUT RISKAWARE

Riskaware is a leading incident modelling solutions provider. With over 20 years' experience working with global government departments and science-led R&D partners, we deliver actionable insight on environmental, human and security challenges worldwide. Our scalable incident modelling platform solutions offer superior situational awareness and critical decision support to government and commercial organisations.

For more information or to discuss how we can work together, please contact us on:

Email
info@riskaware.co.uk

Phone
+44 (0) 117 929 1058

Whitefriars
Lewins Mead
Bristol
BS1 2NT

RISKAWARE