STARA®

Security Threat and Risk Assessment

Full-spectrum defence against advanced threat actors

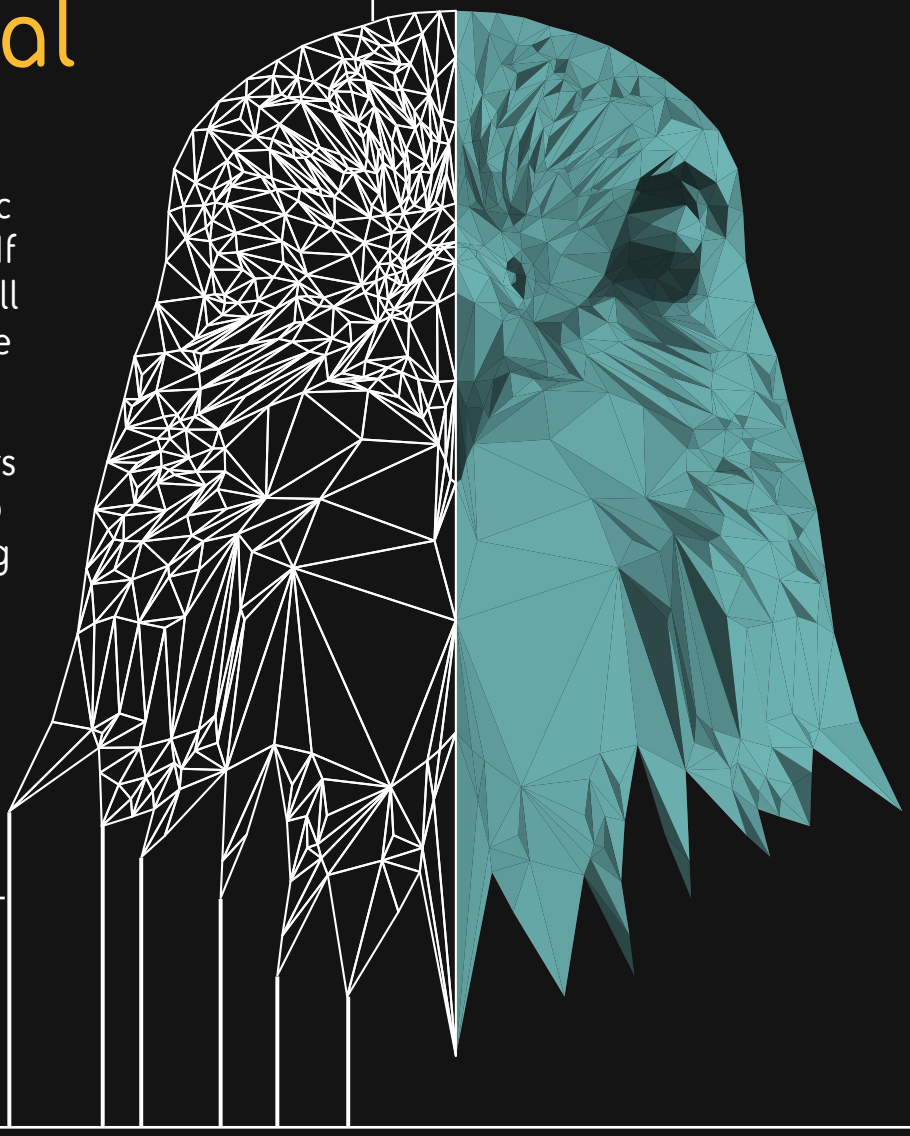
Digital Intelligence

BAE SYSTEMS

Looking beyond digital

Across all sectors, organisations today are operating in a dynamic and diverse threat environment. If attackers fail in one area, they will choose a different path to achieve their aims.

As such, there are multiple factors to keep in mind when it comes to protecting against and mitigating the impact of security threats.



The security of an organisation, its people or its business processes can be enhanced through the implementation of different safeguards and strategies. While cyber security is certainly a key component, it is often viewed in isolation.

We believe a new approach to enhancing security and reducing risk is required. The key stakeholders within organisations - including Chief Information Security Officers (CISOs), Chief Risk Officers (CROs) and Heads of Security - must be prepared to look beyond digital; to remove silos and take an all-inclusive view of their security posture.

Introducing STARA®

The BAE Systems Security Threat and Risk Assessment framework

Leveraging expertise gained from decades of experience working with Government and National Security organisations, we have developed a holistic approach to assessing security threats and risks covering the full spectrum of attack types. Our teams not only help organisations understand the maturity of their security against advanced threat actors, but also how best to deploy resources and controls to increase the depth and breadth of their defence.

STARA® is a unique and repeatable framework of services and tools designed to deliver actionable insights into an organisation's true vulnerability to specific technical and physical threats.

Delivered in a modular format that allows customers to invest at their own pace, our subject matter experts define the real threats facing an organisation and assess how these threats materialise as risk.

This includes table-top analysis of the technical operations, human behaviours, physical facilities and supply chain - all enriched by our Threat Intelligence insights. The findings are then demonstrated and proven on the ground as our experts undertake highly targeted, intelligence-led physical and cyber intrusion testing within the organisation.

STARA® delivers results in easy to consume reports with clear descriptions of findings and actionable recommendations for change.

A holistic approach to helping organisations determine and assess security threats and risks covering the full spectrum of attack types

- Physical
- Personnel
- IT (Information Technology)
- OT (Operational Technology)
- Valuable Assets

STARA® overview

The table below illustrates how the different phases of the STARA® framework enable a methodical approach to the analysis of security threats and associated risks. Each stage, carried out in partnership with the customer, consists of modular operations dependent on specific requirements.

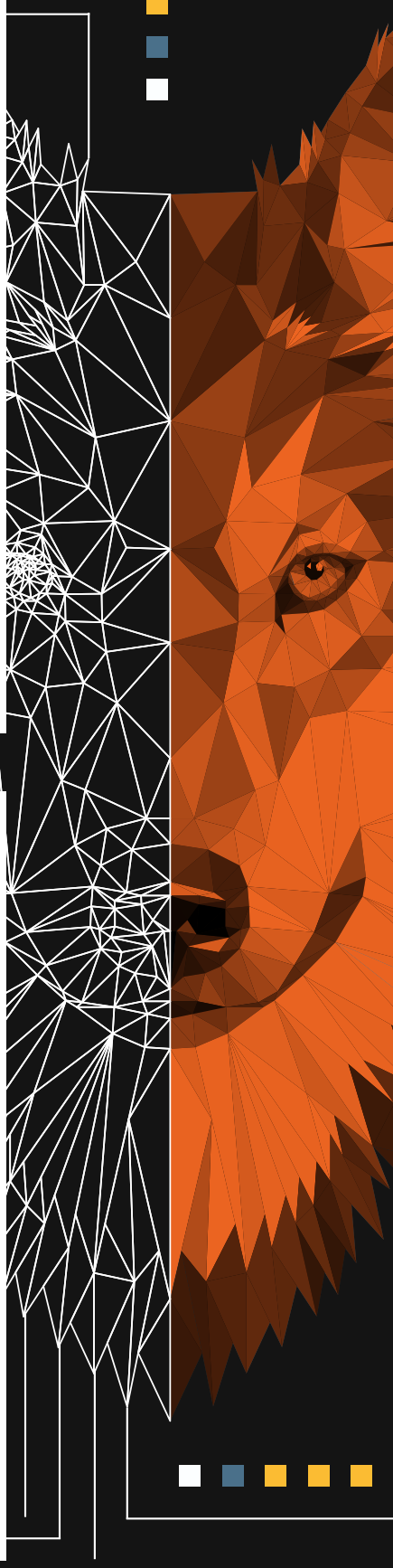
STARA High Level Programme		Core Deliverables	Output
PHASE 1 Identify Threats	We will identify, understand and define the current threat landscape in which the organisation operates, whilst modelling the delivery of its core strategy, mission and operations.	1. Threat Workshop 2. Threat Assessment 3. External Facing Attack Surface Model	• Client is aware of threat environment and engagement with NPSA & NCSC • Organisational and Technical Model • Security Strategy review
PHASE 2 Understand the Organisation	We will review and understand all documentation and physical, people and logical assets in order to understand their criticality to the organisation and its operational environment.	1. Business Impact Assessment, Workshop and report 2. Security Governance Review 3. Asset & Criticality Register	• Understand criticality of assets • Update of current BCP • Gap Analysis of Security Governance • Baseline maturity of corporate security • Compliance against HMG Standards
PHASE 3 Measure Maturity & Vulnerability	We will measure the potential attack surface of the identified assets and model realistic threat scenarios, vulnerabilities and risks in line with ISO 27001, NIST and NCSC CAF. Validating your maturity against industry best practice.	1. Technical, Physical, and socio-Technical Architecture Assessment 2. Attack Path Analysis 3. Red Team (Testing Vulnerability)	• Vulnerability of establishment, people & assets • Validation of security culture • Attack path generation • Test of incident response process • Alignment to NIST/CAF/ISO27001
PHASE 4 Report & Remediate	We will bring together the outputs and ensure that your stakeholders are engaged in a collaborative process to understand the findings of the assessment and the context in which they are made so that we can build a security improvement plan with buy-in from all key stakeholders.	1. Risk workshop and Register 2. NIST CSMA and NCSC CAF 3. Final Report 4. Executive Briefing 5. Security Improvement Plan	• Holistic understanding of Threat, Risks and Vulnerabilities of organisation • Understanding of compliance • Completed NCSC CAF • Body of evidence for change • Comprehensive Security Improvement Plan

Detect and identify
the threats that put your organisation at risk

STARA® phases in detail

PHASE 1: Understand the Threats

- Run stakeholder workshops to understand what your organisation does and how it conducts its operations.
- Leverage our Threat Intelligence and Open Source Intelligence (OSINT) expertise to capture evidence and assess the sector and environment in which you operate.
- Define your current threat landscape and assess its relationship to your organisation's core strategy, mission and operations.
- Establish your attitude to risk (e.g. acceptance, avoidance) and approach to corporate security.
- In recognition of the above, we consider the personas and motivation of threat actors who may be motivated to attack your organisation, and evaluate your current security focus.
- Validate the existing threat landscape by postulating principle attack vectors that threat actors may utilise to breach and attack your organisation.



PHASE 2: Predict the Risks

- Conduct stakeholder interviews, workshops, and document reviews to gain a detailed understanding of your operational environment, and physical, personnel and digital assets and their criticality.
- Carry out a detailed gap analysis to assess your baseline controls against industry standards.
- Review asset criticality against CNI categories/classifications in relation to your mission and core operations.
- Assess and validate effects of concern and their impact on your organisation through collaborative workshops with stakeholders and industry experts.
- Define your security architecture, attack surface, the vulnerabilities of your people, assets and processes that could be exploited, and any attack vectors which they may enable.
- Assess the maturity and effectiveness of your current security posture against industry standards (e.g. NIST, CSMA).

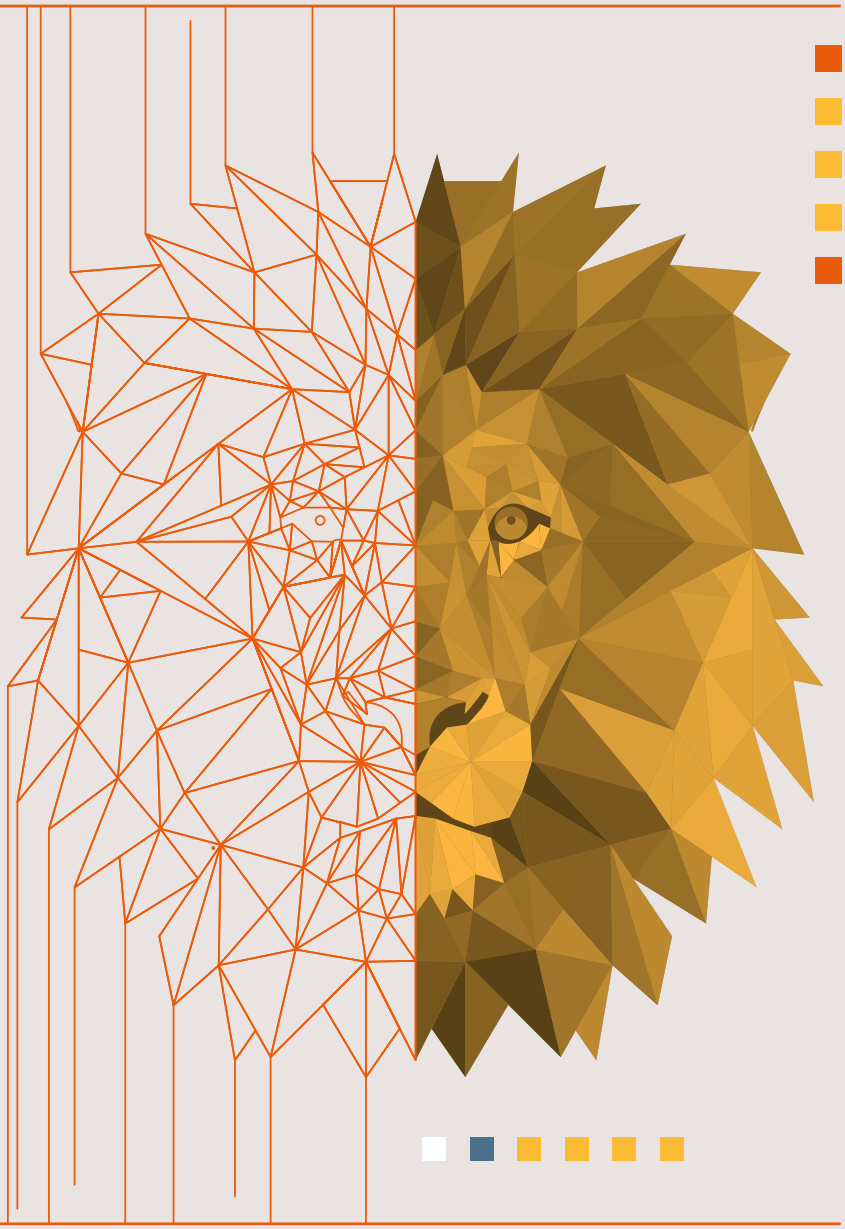
PHASE 3: Prove the Vulnerabilities

- Build on any vulnerability analysis, as well as our earlier consideration of the threat actors who may be encountered, through intelligence-led security testing
- Measure the potential attack surface of the identified assets and model realistic threat scenarios, vulnerabilities and risks in line with ISO 27001, NIST and NCSC CAF.
- Carry out physical penetration tests of facilities to show how non-technical attacks could result in system compromise or data exfiltration.

PHASE 4: Report and Action

At the end of the assessment phases, BAE Systems Digital Intelligence will provide appropriate reporting and recommendations to remediate any issues found:

- We assess the different risks identified across all the domains investigated, including your risk profile, then create a report to explain our findings and reasoning to you.
- We evaluate the findings with you, and jointly agree a set of recommendations that outline what you should do to mitigate risks, remediate vulnerabilities and enhance your secure posture.
- We support the development of a Security Improvement Plan to enact the recommendations and rapidly improve your security posture.

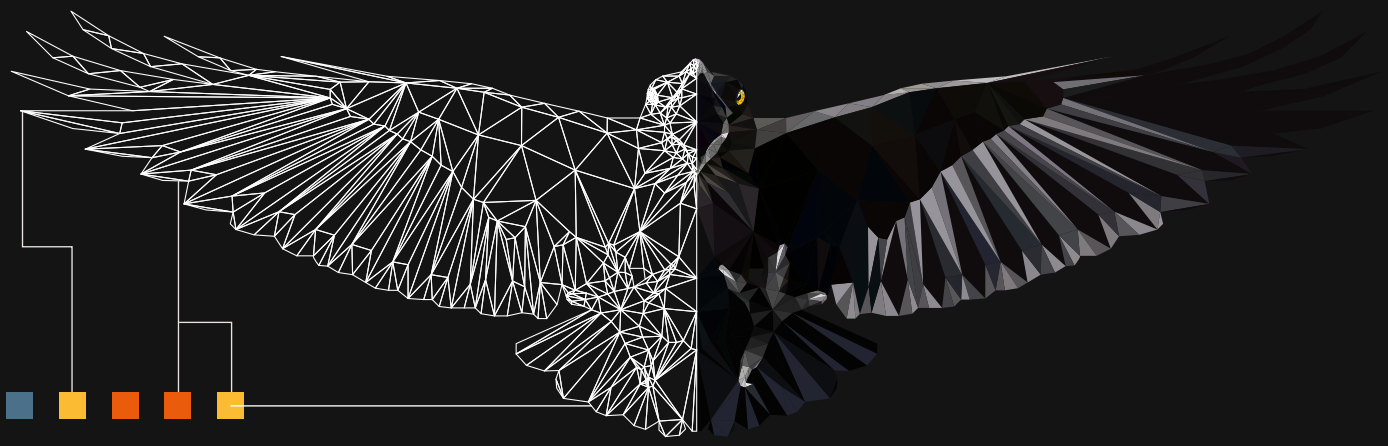


Our STARA® framework is a tried and tested methodology which has been validated by the UK and other governments.

Why BAE Systems Digital Intelligence?

Through STARA®, we employ a unique threat-led and evidence-based approach. This is derived from our experiences protecting some of the world's largest and most targeted organisations from cyber-attacks, our own Threat Intelligence services, and over a decade of experience in helping CNI organisations reduce their risk and enhance security.

The success of the STARA® programme is, we believe, down to our philosophy that organisations must be viewed as a whole in order to truly understand all sources of threats, risks and vulnerabilities. We adopt a holistic mindset rather than the traditional layered approach to security.



Our STARA® framework is a tried and tested methodology that has been validated by the UK and other governments around the world. We bring a unique mix of specialist skills including counter intelligence, covert methods of entry, RFID hacking, surveillance, hostile reconnaissance, forensics and malware analysis. We have also developed the only OFQUAL accredited Covert Operations and Threat Management (COTM) course, a standard to which all of our testing team are certified. Moreover, our Physical Penetration Testing is one of only a handful to be certified by both CREST1 and The Security Institute.

Our Red Team considers all hazards and threats, not only those you would expect to find. Consequently, our approach is both proactive (looking for threats, vulnerabilities and risks), and reactive.

For CNI organisations, the STARA® programme has a further, immediate advantage: we already have a rich heritage of experience gained from having embedded teams investigating and mitigating security threats for many other CNI organisations. Based upon this experience, we have templates, artefacts and processes which are ready for immediate deployment.

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

Learn more

We provide a flexible set of modular options for STARA® to meet your organisation's security requirements. This ranges from a rapid programme - STARA LITE - to a full assessment and many options in between.

Get in touch to find out how we can help you enhance your security posture.

baesystems.com/STARA

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS