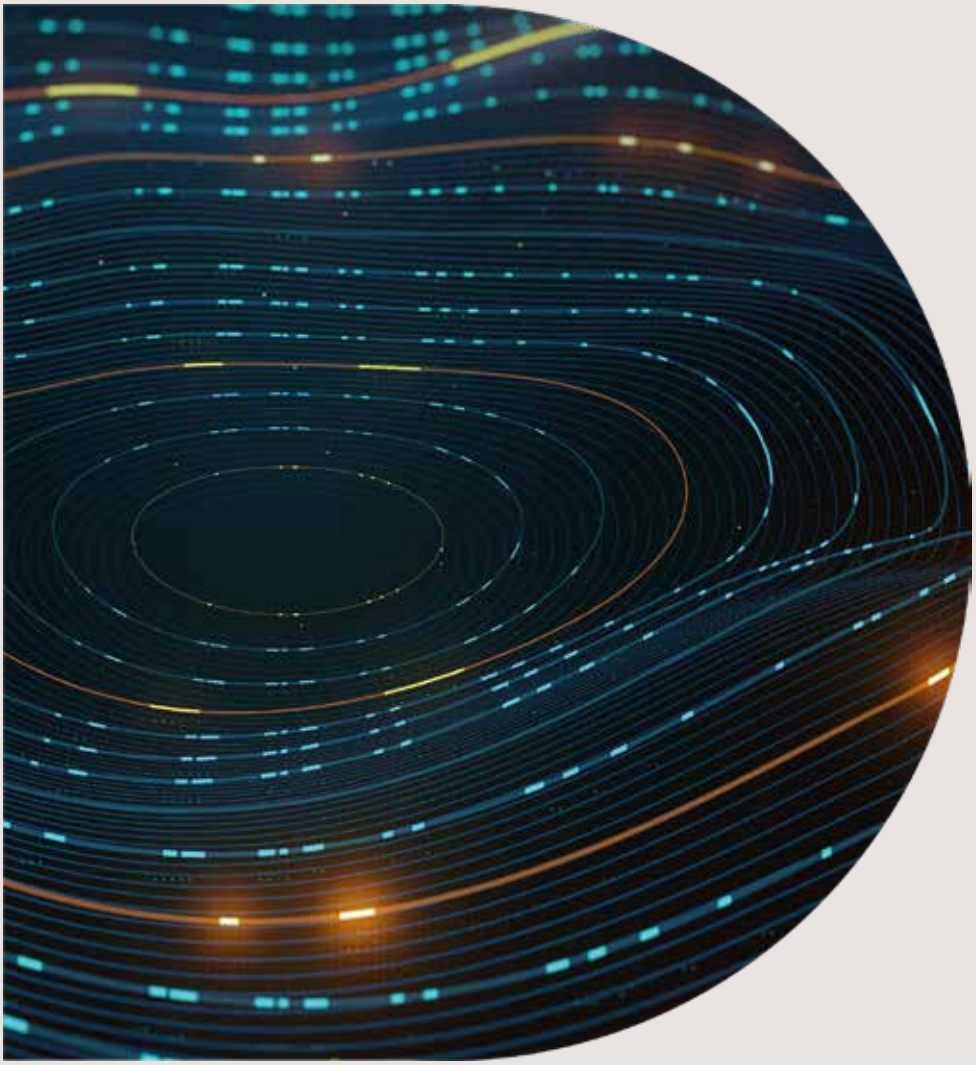
Enterprise Cyber Security

Portfolio Overview



Digital Intelligence

BAE SYSTEMS

Introduction

All organisations today are digitally dependent: their people, data, systems, physical infrastructure and business operations rely on technology to run successfully. To derive maximum advantage from this digital world, enabling connectivity and the flow of information between people, systems, and business partners is key.

However, organisations face challenges including a continually changing threat landscape, limited resources, a scarcity in cyber skills and expertise, and new dependencies that accompany digital operations. As such, many are reluctant to fully embrace a technology vision that could transform their operations by enabling greater efficiencies, effectiveness and success.

At BAE Systems Digital Intelligence, we understand the dilemma this poses to large organisations, particularly those in Critical National Infrastructure (CNI), government, and defence sectors. Over three decades of working with such customers, we have developed and grown into an independent premier provider of enterprise cyber products and services. For customers who need support in mastering areas where they do not possess sufficient internal expertise, we offer an extensive catalogue of solutions and capabilities that augment existing network defence measures.

Working closely and in partnership with our customers is part of who BAE Systems are. This ensures we understand the business or mission objectives, and help achieve their required outcomes.

Why is effective cyber defence still a challenge?

Effective cyber defence requires intelligence, robustness and resilience.

On the one hand, organisations need to have insight into the threats they face, along with how their adversaries operate, their motives and attack methods. At the same time, effective cyber defence requires clear control and understanding over their own organisation, assets, processes, systems and people.

Organisations must be able to maintain a defensive posture in the face of rapidly evolving technologies and threats, and in many cases transformational organisational change through acquisitions, divestments, mergers or new ways of working. They must also have the robustness to enable defences – technological, process and people based – to slow down, frustrate and thwart attacks. Rapid and effective detection is vital in order to mitigate attacks before harm is done.

Organisations also need to develop resilience and agility to be able to respond to attacks when they do occur, minimise the impact, and recover quickly – all while maintaining enterprise operations. This applies to government departments, transport infrastructure service providers, banks, telcos and other forms of enterprise network owners.

For many organisations, maintaining insight into their own infrastructure, systems, services and people is not straightforward. Keeping pace with vulnerabilities and exploits, and how attackers are actively exploiting these to attack enterprises, remains a monumental challenge.

Why BAE Systems Digital Intelligence?

At BAE Systems Digital Intelligence, we are specialists at operating across national security, government, and commercial sectors. Unlike other businesses where these would be strictly separate divisions, we embrace the benefits in bringing the best practices from one to the other, and our customers recognise and value this unique position.

At the core of our cyber business is a deep understanding of the threat landscape, derived from over a decade of research and providing incident response services following complex attacks. Many of these involve state actors or organised criminal groups – both adept at evading traditional security controls in enterprise networks.

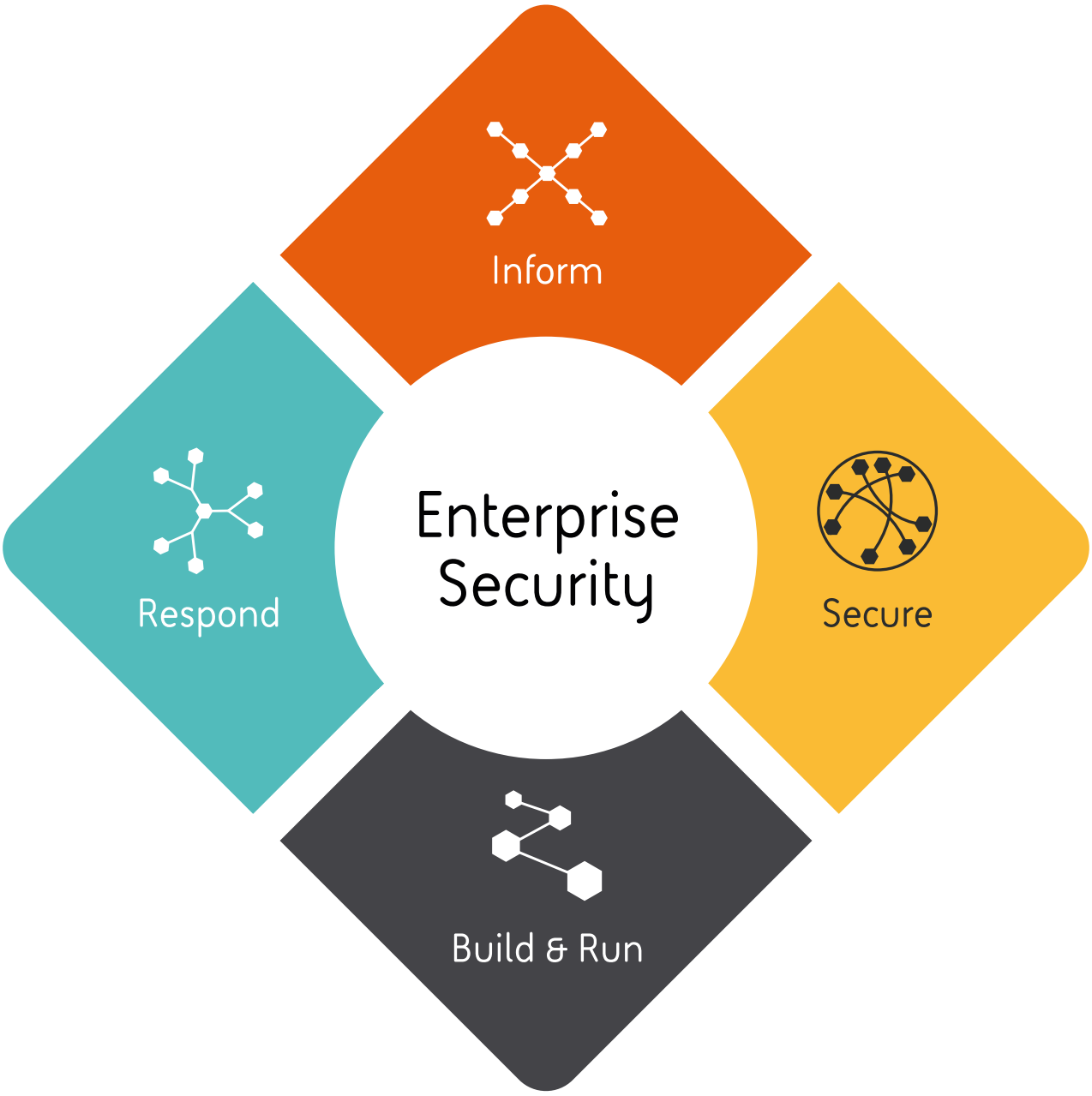
Our customer base for enterprise security services include organisations in transport, financial services, energy and utilities, telecommunications, healthcare, law enforcement, industry and technology. We also work with government and defence departments, agencies and functions to ensure they understand and are protected against the threats they face, while helping them exploit the connected digital world.

Working closely and in partnership with our customers is part of who we are. This ensures we understand the business or mission objectives, and help achieve their required outcomes.

BAE Systems Enterprise Security

As threats and wider business, technology, and regulatory landscapes evolve, so do the risks. In the face of this, it is necessary to adapt and optimise defence measures to ensure they remain operationally effective.

Our Enterprise Security catalogue spans four main areas of activity, as shown below in Figure 1.



Inform

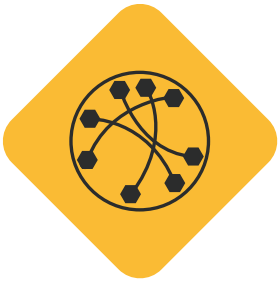
We help customers understand the risks and threat landscape in order to make more informed business and strategy decisions.

We inform customers of their cyber risk through understanding the impact of cyber attacks, the threats they face, and any specific vulnerabilities. These form key parts of cyber risk management (where cyber risks are a function of Impact, Threat and Vulnerability) and enable customers to make better risk balanced decisions for their cyber defence and resilience.

Our delivery is based on decades of experience packed into reusable methodologies and tools used across our products and services – altogether enabling a enable repeatable, traceable and actionable assessment of risk.

Our services in this area include: Security Threat and Risk Assessment (STARA®), Threat Intelligence, Security Testing, and wider cyber advisory services.

Secure



We help customers secure their enterprises, operations, systems and data from cyber threats.

Securing data and networks continues to be the cornerstone of network defence. We offer specialist solutions to enable communication between high-trust to low-trust networks, via high-assurance gateways. This area includes hardware appliances as well as expert consultants on secure network segmentation.

Our services in this area include: Cross Domain Solutions and Security Architecture.

Build & Run

We implement, manage and operate cyber security for our customers.

Many organisations are faced with the challenge of transforming, managing, or operating their existing cyber security function. This is particularly difficult when skilled resources are limited. Our consultants have expertise in the security tools and processes used in large enterprises, and we are hands-on in running aspects of customer security for dozens of organisations across the UK, Europe, Asia Pacific, and Australia.

Our services in this area include: Security Transformation programme management and implementation, SOC Design & Build, and hands-on operation of security functions such as security risk management, security architecture, and supplier security risk management.

Respond

When the worst happens, organisations need to be able to turn to someone they trust to help them investigate an incident or breach. We have over 20 years of experience running digital forensics and incident response investigations, including responding to major attacks against enterprise networks. Our team is CREST certified and our services are accredited as part of the UK's NCSC CIR scheme.

Our services in this area include: Incident Response.

How do we do this? Our Enterprise Cyber Assessment services

BAE Systems offers a broad range of cyber assessments to our enterprise customers, which include:

	**Security Threat and Risk Assessment (STARA®)**	STARA is our holistic framework for assessing risk and exposure at an organisational level to attack across the logical, socio-technical and physical domains. Outputs include visibility and demonstration of risks and vulnerabilities, along with recommendations and prioritised delivery of quick wins.
	**Cyber Diagnostic & Maturity Assessment**	We assess how your organisational cyber maturity aligns with your risk appetite, and the specific threats to your organisation. Our Diagnostic and Maturity Assessments are typically delivered against the NIST cyber maturity levels.
	**Security Supply Chain Maturity Assessment**	We assess how effective your organisation is at managing its supply chain, and the associated security risks.
	**Ransomware Controls Assessment**	We assess your organisation's protection against ransomware, based on our experience in helping customers respond to ransomware attacks. Our assessment framework is aligned to NIST & MITRE ATT&CK.
	**Security Operations Maturity Assessment (SOCMA)**	We assess the maturity of your Security Operations against our SOC blueprint model, enabling you to improve your SOC capability to align with your threats and risk appetite.
	**Quantum Readiness Assessment**	We assess your organisational readiness and cyber exposure to quantum technology, and help put measures in place to protect against this.
	**Threat Hunting / Compromise Assessment**	We conduct threat hunting investigations of customer networks, identifying signs of compromise or intrusion using our threat research and expertise in incident investigation, forensics and threat detection.
	**SWIFT CSCF Independent Assessment**	We assess your organisational implementation of the SWIFT Customer Security Controls Framework (CSCF), to support SWIFT compliance attestations.

Case Studies

Organisation Cyber Capability Assessments across the NHS

BAE Systems Digital Intelligence has been the Department of Health and Social Care (DHSC)'s strategic partner for cyber capability assessments since 2018. Our programme over the past 5 years has supported numerous DHSC Executive Agencies that own and operate CNI in the UK's health sector, including through the most difficult periods of the COVID pandemic.

In working with the DHSC, we've used HMG Functional Standards and recognised international standards (including ISO27001 and NIST SP800-53) as the foundation of our approach, augmenting these with best practices from our experiences working across different sectors. In addition, our STARA® Framework was the basis for understanding each organisation's threat landscape and security maturity, where we undertook a variety of assessments of the organisation's critical functions, socio-technical architecture (the human interaction with technology, processes, procedures and policies) and physical security architecture.

In addition, individual targeted vulnerability assessments were also undertaken to assess specific critical assets and systems in detail, understand their cyber risks and vulnerabilities, and provide remediation recommendations.

> "The STARA programme genuinely surpassed expectations in terms of the benefits it conferred to us, the reduction in risk that we are exposed to, and the value for money that we received.
>
> Owing to the work of STARA we, as well as the wider organisations across Health and Care, are able to deliver critical services to the NHS and the wider public in a de-risked, more secure, and sustainable manner."

Dan Jeffery
Deputy CIO and CISO
NHS Blood and Transplant

Global telco cyber detection & response testing

Telenor Group is a multinational telecommunications company, headquartered in Norway. It has a federated structure, with businesses operating locally in Norway, Denmark, Finland, Sweden, Thailand, Malaysia, Bangladesh, and Pakistan.

Telenor identified a gap in its understanding of the cyber maturity across its business units and required a partner who could engage in assessing this, as well as produce recommendations for improvements.

BAE Systems Digital Intelligence was selected following a competitive tender process in December 2020. The alignment and compatibility of BAE Systems' capabilities and Telenor's own security programme made for a strong proposition.

The initial tasks under this contract consisted of a series of maturity assessments around security operations, as well as attack simulation assessments. Using our defined methodologies for both, our teams were able to produce consistent reports and actionable recommendations for all business units that underwent the assessments.

The objectives for each assessment on a given entity were:

- Evaluate the performance of internal and outsourced activities
- Guide the business units' and strategic vendor's security improvements
- Harmonise and uplift security operations across the business

These objectives then fed into the broader goal of enhancing the Telenor Group's cyber capabilities through:

- Improved understanding of security operations quality
- Identification of improvement areas and roadmap creation
- Enabling better vendor management for operational services
- Capability harmonisation to enable common operations

> "During my professional career I have never experienced the true partner spirit that BAE Systems has been able to create between Telenor and BAE Systems. All the initiatives we have are working flawlessly."

CSAT feedback from Tommy Waldenstrøm
Head of Global Security Solutions
Telenor

Recovering a government department from Ransomware

In October 2019, the health sector in Victoria, Australia was hit by a massive ransomware attack. Following a phishing campaign, the attackers compromised a large network of hospitals and executed Ryuk ransomware. The malware was installed on thousands of servers and computers across 25 critical care hospitals, with over 220 systems encrypted by the time the BAE Systems Incident Response team was activated.

Despite the targeted attack causing widespread damage to health sector assets and disruption to clinical services, our team was able to quickly contain the incident and support workaround measures to get basic healthcare services working again. The timeline for this incident response activity was as follows:

Within 4 days of activating our IR team, the full attack scope was understood

Within 9 days all known malware had been eradicated from the 25 hospitals and the IR team was confident that control of the network was restored

At 10 days internal Department of Health cloud systems were reconnected to provide system access to critical hospital functions like Accident & Emergency

At 4 weeks the entire network environment had been re-architected and hardened to mitigate future attacks. Selected internet based systems were enabled in a controlled manner

By 6 weeks general internet connectivity, browsing, and email services were restored to all 25 hospitals.

Achieving this response and recovery from such a major cyber attack, required us to lead the management of dozens of resources from over 15 organisations. This was only possible through the scale of our local and global teams, and the breadth of experience and skills they possess across all facets of cyber security.

> This was the largest cyber attack in Victorian Government history, and we would absolutely not have been able to stop the attack and recover the hospitals without BAE Systems.

Ensuring organisational defence against ransomware

We were approached in 2022 by a leading professional services organisation who needed to understand the likely impact of ransomware on its operational stability, and to be informed of possible protection and controls against this.

In response, BAE Systems delivered a ransomware controls assessment, aimed at identifying and assessing the controls the organisation already had in place to prevent the intrusion, spread and execution of ransomware.

The outcome of this short 4 week engagement was a clear picture of the organisation's defences against a ransomware attack, with visibility of potential areas for improvement and strengthening which would reduce the likelihood of a successful attack.

Following our report, we supported the customer in establishing a security and risk improvement programme. Post implementation, despite frequent attempted attacks against its systems, the organisation has yet to suffer an incident with any material impact.

Transforming security for a UK Airport

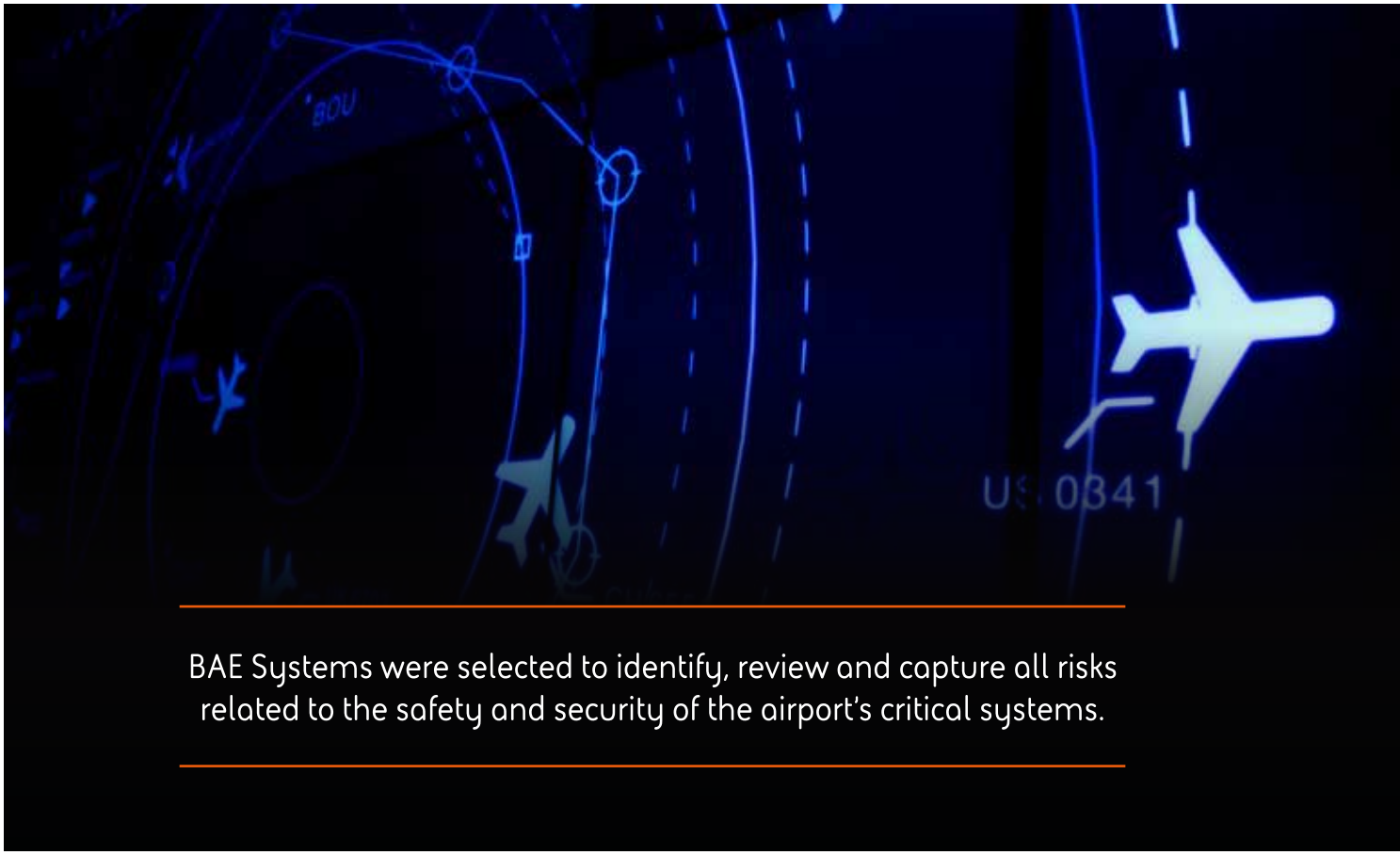
BAE Systems Digital Intelligence supported the identification and development of a robust cyber security transformation programme for the UK's Gatwick airport (one of Europe's top-ten busiest airports at the time).

This included reviewing and developing the risk mitigation programme for the airport covering a wide range of critical systems, establishing the cyber security methodology, and developing policy.

We worked with Gatwick Airport to develop cyber security documentation aligning to ISO 27001, NIST and NIS-D. Our consultants worked with the UK Civil Aviation Authority (CAA) and the UK National Cyber Security Centre (NCSC) to establish the 2020 CAF 3 (CAP 1574) standard for the UK NIS-D CAA Aviation Standards, attending focus group meetings with the CAA.

As a result, we were selected to undertake the 2020 NIS-D submission for the airport, identifying, reviewing and capturing all risks related to the safety and security of the airport's critical systems.

Our work had a fundamental impact in lowering the number of outstanding cyber security support tickets. This saw a reduction from several hundred support tickets to less than ten per day, significantly reducing operating cost whilst at the same time improving security posture.



BAE Systems were selected to identify, review and capture all risks related to the safety and security of the airport's critical systems.

Advanced Security Operations Centre

BAE Systems provided an Advanced Security Operations Centre solution to a UK government department, providing a new monitoring capability and transforming an existing operation.

The solution comprised of new hardware and software, as well as a range of services. These were broken into several work-stream areas:

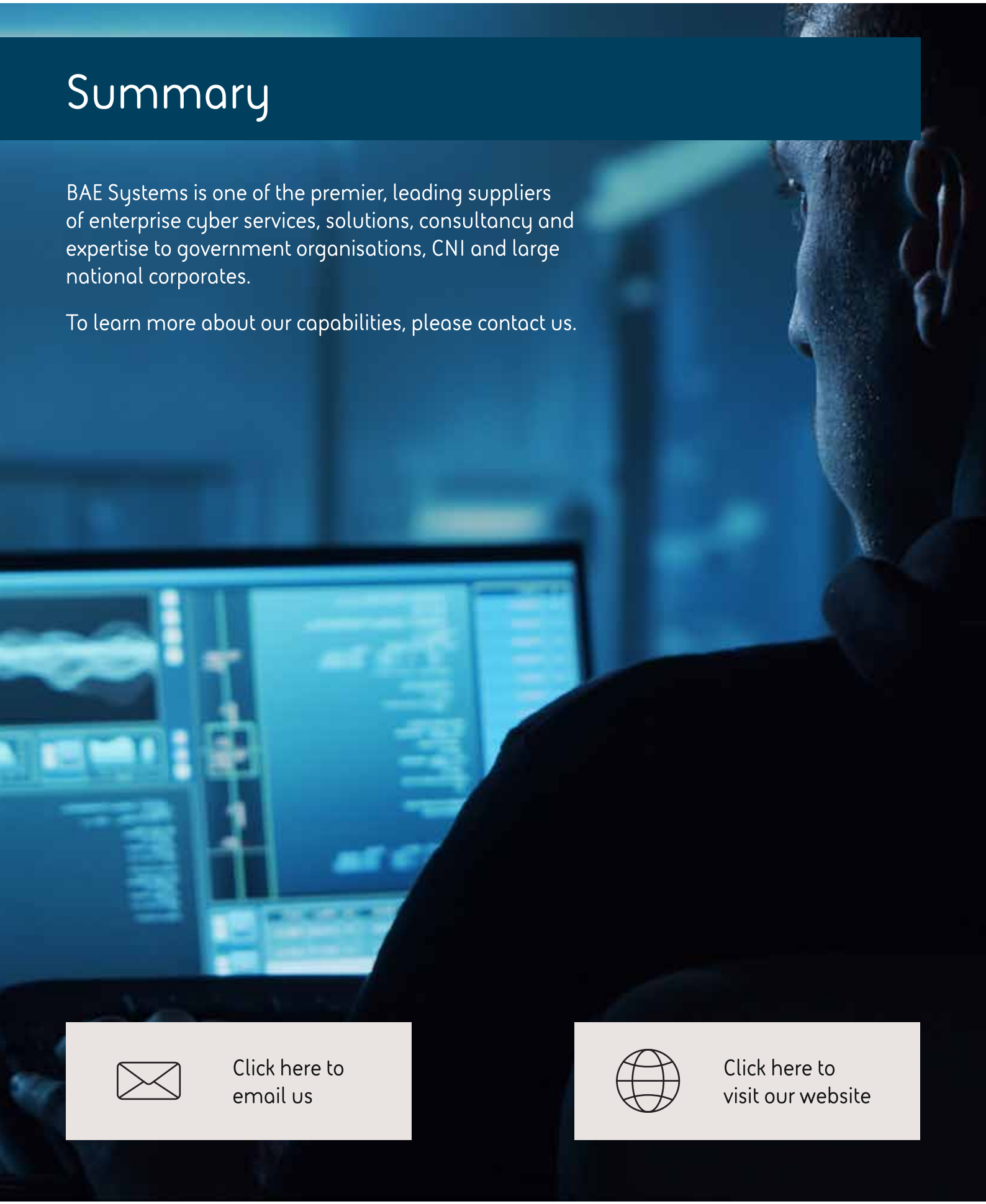
- **Hardware and software provision**
- **Infrastructure Services:**
  - Design, configuration, testing
- **Programme Management and Business Change**
- **Technical Services:**
  - Information Assurance
  - Threat Intelligence
  - Incident Response
- **On-boarding of security event data sources**
- **Professional Development Programme**
- **ICT Support and Maintenance**
- **Strategic Skills Transfer (including SOC skillset capture, knowledge transfer and mentoring)**

The capability significantly enhanced the effectiveness of the customer's security operations. This enabled the customer to identify multiple ongoing intrusions against its networks, which we were able to support by investigating and remediating alongside the customer.

Summary

BAE Systems is one of the premier, leading suppliers of enterprise cyber services, solutions, consultancy and expertise to government organisations, CNI and large national corporates.

To learn more about our capabilities, please contact us.



Click here to email us

Click here to visit our website

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.

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

BAE Systems Digital Intelligence
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

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 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

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