THALES
Building a future we can all trust

G-Cloud 15
PENETRATION TESTING

Doc Ref No: ThalesGC1510

INTRODUCTION

Comprehensive technical assessment of systems to identify vulnerabilities that could be exploited by adversaries to compromise, steal, or corrupt data or to otherwise prevent normal business or system operations

The Thales Penetration Testing is a set of modular work packages that can be combined or used stand-alone to assess the cyber-security of a system, solution, or organisation. Each of the work packages is designed to find vulnerabilities in a system that could allow a cyber-attack to become successful.

USE CASE

Penetration testing is of value to any individual managing IT systems, especially those that are risk owners. A test may be required for any number of reasons, including:

- To a schedule proscribed by the system's Cyber Security Management Plan
- In response to newly identified vulnerabilities or attacks against similar systems
- At specific review stages during the development of a new system.

The following is a short list of example government use cases:

Web Application Security for Citizen Services

- **Who:** Departments providing online portals for tax filing, benefits, licensing
- **Why:** To ensure web applications are secure against common attacks (e.g., SQL injection, cross-site scripting) protecting sensitive citizen data and maintaining public trust.

Internal Network Hardening

- **Who:** IT security teams in government ministries or agencies
- **Why:** Modular network penetration tests help identify weaknesses in internal infrastructure, enforce least privilege access, and protect against insider threats.

Mobile and Remote Workforce Security

- **Who:** Human resources and IT departments
- **Why:** To test VPNs, remote access points, and mobile endpoints ensuring secure connectivity for government employees working remotely, especially important given increased telework.

Cloud Security Assessment

- **Who:** Cloud infrastructure managers within government IT divisions
- **Why:** To verify the security of cloud-hosted systems by testing access controls, configurations, and APIs, ensuring compliance with government cloud security mandates.

Compliance and Regulatory Audits

- **Who:** Compliance officers and auditors in government bodies
- **Why:** Modular penetration testing aligned with specific regulations (e.g., GDPR for data protection or FISMA in the US) to help maintain compliance and avoid penalties.

New System or Application Deployment

- **Who:** Project managers and system architects within government IT departments
- **Why:** Conducting modular tests on new systems or applications before going live to catch and fix vulnerabilities early in the development lifecycle (DevSecOps).

Inter-agency Data Sharing Platforms

- **Who:** Security officers managing inter-agency collaborations
- **Why:** Testing security controls on shared platforms or data exchanges to prevent unauthorized access and data leaks between government entities.

Physical and IoT Security Testing

- **Who:** Departments overseeing government facilities or smart city initiatives

- **Why:** To assess vulnerabilities in IoT devices, surveillance systems, or physical security controls that could be exploited to gain network access or disrupt services**.**

FEATURES AND BENEFITS

Features

The penetration testing service includes the following features:

- IT systems penetration testing
- A modular and phased testing service
- Infrastructure and Application penetration testing
- A customisable scope to allow selection of specific system components
- Flexible engagement levels from basic vulnerability assessment to full penetration test
- Integration with other Thales service like risks assessment or training
- Expert advice per module with analysis and recommendations.

Benefits

The benefits of choosing a Thales penetration test include:

- Reduces the risk of cyber attacks
- Identifies vulnerabilities and weaknesses in systems, networks, and applications
- Increases the resilience of systems to attack
- Ensures compliance with regulatory standards that require regular testing
- Tests incident response processes
- Minimises the risk of data breaches
- Validates that security systems and controls are operating as intended
- Protects reputation by avoiding security incidents
- Saves costs by identifying and mitigating security vulnerabilities
- Supports wider risk management processes.

DETAILED SERVICE OVERVIEW

The Thales Penetration Testing service is delivered in three key phases – scoping, delivery, and reporting. The covers the definition of the test – what will be tested, why is it being tested and how. Delivery is the actual testing itself, and reporting is analysis of the testing and production of a report.

Scoping

The scoping phase involves Thales working with the customer to define the objectives and requirements of the testing, and then to determine the actual elements of the system that would be tested and which work packages would be used. The scoping will define the actual work and duration as well as what is needed to support testing and the location of testing.

The scoping will identify whether only a single methodology is required, multiple methodologies or some form of hybrid testing that selects different elements. Where required a custom, specialised, methodology may be developed.

The output of the scoping phase is a scoping document describing the following:

- Objectives of the testing including any specific scenarios to be evaluated
- The elements of the system to be tested

- The testing work packages to be used
- Specific requirements
- Estimated testing timeline.

Delivery

The delivery stage is the actual testing of the system in scope, on customer site, at a Thales cyber lab, or remotely. The testing team will engage with the Customer's point of contact and carry out the activities described in the scoping document. As testing progresses and vulnerabilities or issues are identified the testing team will ensure that the point of contact is informed, and a wash-up meeting will be held as required at the end of every day.

Detailed logs of activities that are conducted are recorded to provide evidence of activities and to ensure that the Customer is able to reproduce issues themselves.

Reporting

Upon the completion of the Assignment, Thales shall deliver to the Customer a written report containing:

- An executive summary presenting the main identified security risks
- All the findings, annotated with appropriate references to standards like CVE, CWE or CVSS risk computation methodology
- All the necessary proofs and methodology used that will allow the client to confirm the vulnerabilities
- A remediation plan for all Critical vulnerabilities identified, with a suggested priority based on the calculated risk.

Infrastructure Testing Modules

Work Package: Infrastructure Testing

Infrastructure testing focuses on assessing the security posture of network devices, servers, firewalls, routers, switches, and other hardware components within an organisation's IT environment. The goal is to identify and exploit vulnerabilities to determine potential risks and impacts on the infrastructure.

This assessment includes:

- **Network and System Reconnaissance**: Identification of networked devices and the services that are exposed on the network
- **Vulnerability Identification:** Use of automated tools to identify potential vulnerabilities in the network and infrastructure components
- **Vulnerability Exploitation:** Attempts to exploit identified vulnerabilities to determine the extent of access and potential impact. This includes testing for misconfigurations, weak passwords, outdated software, and unpatched vulnerabilities
- **Privilege Escalation and Lateral Movement:** Assess the level of access gained and potential data exposure. Evaluate the ability to move laterally within the network.

Work Package: Network Access Control (NAC) Assessment

Network Access Control (NAC) assessments evaluate the effectiveness of an organisation's NAC solutions. These solutions are designed to control access to network resources by enforcing security policies on devices when they attempt to access the network. The assessment aims to identify vulnerabilities, misconfigurations, and compliance issues within the NAC implementation.

This assessment will comprise:

- **Environment Setup**: Prepare the testing environment, including setting up test devices and ensuring access to the NAC solution management interfaces
- **Policy Review**: Review existing NAC policies and configurations to understand the rules and controls in place
- **Access Control Testing**: Evaluate the effectiveness of NAC policies by attempting to connect various devices (e.g., compliant, non-compliant, rogue) to the network and observing the NAC responses
- **Bypass Testing**: Attempt to bypass NAC controls using various techniques such as MAC spoofing, VLAN hopping, and rogue device connections
- **Authentication and Authorisation Testing**: Verify that authentication mechanisms (e.g., 802.1X, RADIUS) are correctly implemented and that authorisation policies are enforced as intended.

Work Package: IT Health Check (non-CHECK)

An IT Health Check (non-CHECK) is an assessment aimed at evaluating the overall security posture of an organization's IT systems, networks, and applications. Unlike formal CHECK tests, which are certified by the UK National Cyber Security Centre (NCSC), non-CHECK health checks are performed without formal CHECK certification but follow similar principles to identify vulnerabilities and provide actionable recommendations for improvement.

This test will comprise:

- **Reconnaissance**: Perform passive and active information gathering to understand the IT environment
- **Vulnerability Assessment**: Use automated tools and manual techniques to identify potential security weaknesses across systems, networks, and applications
- **Configuration Review**: Assess configurations of key systems and devices to ensure they follow security best practices
- **Penetration Testing**: Conduct limited penetration testing on identified vulnerabilities to evaluate their exploitability and potential impact
- **Compliance Check**: Review adherence to relevant security policies, standards, and best practices.

Work Package: Cloud Security Audit

A Cloud Security Audit is a comprehensive assessment of a cloud infrastructure and its associated services and configurations to ensure compliance with security best practices, industry standards, and regulatory requirements. The objective is to identify misconfigurations, insecure deployments, access control issues, and potential vulnerabilities in cloud environments.

This test will comprise:

- **Access Review**: Assess identity and access management (IAM) configurations, roles, permissions, and authentication mechanisms
- **Configuration Review**: Evaluate configurations of cloud resources for adherence to security best practices, including storage access controls, encryption, firewall rules, and logging settings
- **Network Security Review**: Examine cloud networking components such as virtual networks, subnets, gateways, and security groups
- **Logging and Monitoring**: Review audit logs, logging configurations, and monitoring tools for evidence of visibility and incident response readiness

- **Compliance Mapping**: Check alignment with relevant security standards (e.g., CIS Benchmarks, ISO 27001, NIST, GDPR).

Work Package: Stolen Device Assessment

A Stolen Device Assessment evaluates the security risks and potential impact on an organization if an employee's device (such as a laptop, smartphone, or tablet) is lost or stolen. This assessment focuses on understanding the vulnerabilities associated with data stored on the device, potential access to corporate networks, and the effectiveness of data protection mechanisms like encryption and remote wipe capabilities.

This assessment will comprise:

- **Device Acquisition:** Obtaining a test device that closely matches the configuration and security measures of actual devices used by the Customer
- **Baseline Data Collection:** Documenting the device's initial state, including installed applications, data storage, and security configurations.
- **Security Testing:**
  - Data Extraction: Attempt to access sensitive data stored on the device using common data recovery techniques
  - Network Access Simulation: Test for potential unauthorised access to corporate networks and services, examining stored credentials, VPN configurations, and cached sessions
  - Bypass Security Measures: Try to circumvent security features such as encryption, password protection, and biometric authentication.
- **Remote Management Evaluation**: Assess the capability and effectiveness of remote wipe or device lock features.

Work Package: Wireless Network Testing

Wireless Network Testing is a comprehensive evaluation of the security and performance of wireless communication technologies, including WiFi, Bluetooth (BLE), and radio frequencies. The objective is to identify vulnerabilities, assess the effectiveness of security controls, and ensure the reliability and robustness of wireless networks against unauthorised access, eavesdropping, and other threats

This test will comprise:

- **Reconnaissance**: Perform passive and active scanning to discover wireless networks, access points, and devices. Gather information on signal strength, SSIDs, encryption methods, and other relevant data
- **Vulnerability Assessment**: Use automated tools and manual techniques to identify vulnerabilities in wireless networks, such as weak encryption, default credentials, misconfigurations, and insecure protocols
- **Penetration Testing**: Exploit identified vulnerabilities through techniques such as cracking WEP/WPA/WPA2 encryption, spoofing MAC addresses, and launching man-in-the-middle (MITM) attacks
- **Bluetooth and Radio Testing**: Evaluate the security of Bluetooth (BLE) and radio communication by scanning for devices, sniffing traffic, and testing for vulnerabilities such as insecure pairing and data leakage
- **Performance Testing**: Assess the performance and reliability of wireless networks under various conditions, including signal interference and load testing.

Build and Configuration Review Modules

Work Package: Host Build Review

Host Build Review is a security assessment process that involves evaluating the configuration and setup of servers, workstations, and other host systems. The purpose is to identify vulnerabilities, misconfigurations, and security weaknesses that could be exploited by malicious actors. This test ensures that hosts are securely configured according to best practices and organisational security policies.

This test will comprise:

- **Configuration Review:**
  - examine the system configurations, including file system permissions, user accounts, installed software versions, and security settings
  - review system logs and audit trails for signs of unauthorized access or anomalous activities.
- **Vulnerability Assessment:**
  - use automated tools and manual techniques to identify known vulnerabilities in the host's software and configurations
  - assess the effectiveness of security patches and updates applied to the system.
- **Security Control Assessment:**
  - evaluate the effectiveness of implemented security controls such as firewalls, antivirus software, encryption, and access controls
  - review system hardening measures and compliance with security benchmarks (e.g., CIS Benchmarks).

Work Package: Network Device Configuration Review

A Network Device Configuration Review is a security assessment method focused on evaluating the configuration settings of network devices such as routers, switches, firewalls, and other network appliances. The goal is to identify misconfigurations, weaknesses, or non-compliance with security best practices that could expose the network to potential threats.

This test will comprise:

- **Configuration Data Collection:**
  - Accessing network devices to collect configuration data. This may include manually reviewing configurations via administrative interfaces or exporting configuration files for analysis.
- **Configuration Analysis:**
  - Analysing the collected configuration data against industry best practices, security standards, and organizational policies. Areas of focus include access control, logging, network segmentation, protocol usage, and firmware versions.
- **Risk Identification:**
  - Identifying potential vulnerabilities and misconfigurations, such as weak passwords, open ports, outdated firmware, or improper network segmentation.

Work Package: Pre-Hardening Assessment

A Pre-Hardening Assessment is a security evaluation performed on systems, applications, or networks before they undergo hardening processes. The goal is to identify existing vulnerabilities, misconfigurations, and potential security weaknesses, providing a baseline for

subsequent hardening efforts. This ensures that all necessary security controls are implemented effectively.

This test will comprise:

- **Baseline Configuration Review**: Examine the current configurations of systems, applications, and network devices to identify deviations from security best practices
- **Vulnerability Scanning**: Use automated tools to scan for known vulnerabilities and security issues in the environment
- **Manual Analysis**: Perform manual checks and validations to identify configuration issues and potential security risks that automated tools might miss
- **Risk Assessment**: Evaluate the identified vulnerabilities and misconfigurations to determine their potential impact and likelihood of exploitation.

Embedded Systems Modules

Work Package: Embedded Systems Penetration Test & Audit

Embedded Systems Penetration Testing comprises a thorough security assessment of hardware and software components that constitute embedded systems. These systems typically include specialized computer systems designed to perform dedicated functions, often within larger systems. The purpose of this test is to identify and exploit potential vulnerabilities within embedded devices, which may include IoT devices, industrial control systems (ICS), medical devices, automotive systems, and other specialized hardware. The objective is to assess the security posture, uncover vulnerabilities, and provide recommendations to mitigate identified risks.

This test will comprise:

- **Information Gathering**: Collect detailed information about the embedded system. This may involve reverse engineering the device, extracting firmware, and analysing system documentation. Techniques such as firmware extraction, hardware interfacing, and sniffing communication channels may be employed
- **Vulnerability Analysis**: Identify potential vulnerabilities in the hardware, firmware, and software components. This includes static analysis of the firmware, dynamic analysis of the running system, and checking for known vulnerabilities in software libraries and protocols used by the device
- **Exploitation:** Attempt to exploit identified vulnerabilities to determine their potential impact. This phase may involve gaining unauthorised access, escalating privileges, manipulating device functionality, or extracting sensitive information
- **Post-Exploitation and Analysis**: Analyse the implications of successful exploitation. This includes determining the potential impact on data integrity, system availability, and confidentiality. The Assessment Team will also assess the ability to persist within the system or network.

Application Testing Modules

Work Package: Desktop Application Binary/Deployment Testing

Desktop application binary/deployment penetration testing involves evaluating the security posture of a desktop application's executable files and deployment mechanisms. This type of testing focuses on identifying vulnerabilities in the application's binaries, configurations, and deployment procedures such as reverse engineering, code analysis, and configuration reviews. The goal is to uncover potential security weaknesses that could be exploited by attackers to gain unauthorized access, execute malicious code, or compromise sensitive information.

This test will comprise:

- **Static Analysis:**

- perform reverse engineering of the application's binaries to understand the underlying code and logic
- analyse the binary code for hardcoded credentials, insecure APIs, and other potential security flaws
- review configurations for misconfigurations that could lead to vulnerabilities.

- **Dynamic Analysis**:
  - execute the application in a controlled environment to observe its behaviour
  - monitor network communications, file system interactions, and other system activities for signs of insecure practices
  - attempt to exploit any identified vulnerabilities in a safe and controlled manner.
- **Configuration** and Deployment Review:
  - assess the security of deployment procedures, including installer packages and update mechanisms
  - verify that the deployment process follows best practices, such as secure code signing and integrity verification.

Work Package: Web Application Testing

Web Application penetration tests simulate real-world attacks against a web application to identify security flaws, vulnerabilities, and implementation weaknesses. The aim is to assess the application's resilience to threats such as injection attacks, authentication bypasses, insecure configurations, and session management flaws.

This test will comprise:

- **Reconnaissance**: Perform OSINT, gather server headers, enumerate directories, and identify exposed APIs or endpoints
- **Automated Scanning**: Use scanners to identify common issues such as XSS, SQLi, outdated components, and misconfigurations
- **Manual Testing**: Validate automated results and manually test for business logic flaws, privilege escalation, IDOR (Insecure Direct Object References), CSRF, and other complex vulnerabilities
- **Authentication Testing**: Assess session management, token security, password policies, and multi-factor enforcement
- **Exploitation (Controlled)**: Where permitted, exploit identified flaws to demonstrate potential impact without causing disruption.

Work Package: Restricted Environment Breakout Testing

Restricted Environment Breakout refers to the process of testing the security measures in place to prevent unauthorized access or privilege escalation within a controlled or restricted computing environment. This type of testing is designed to identify vulnerabilities that could allow an attacker to bypass security controls, escape from restricted environments (such as sandboxes, kiosk modes, virtual machines, or locked-down user accounts), and gain unauthorized access to more sensitive parts of a system or network.

This test will comprise:

- **Initial Environment Assessment**: The testing team will review the environment's architecture, configurations, and security controls to understand the scope and potential weaknesses

- **Environment Access:** Testers will gain access to the restricted environment, typically through user-level accounts or interfaces with limited permissions
- **Testing Execution:** The team will employ various techniques to attempt to break out of the restricted environment. This may include:
  - Exploiting misconfigurations or software vulnerabilities
  - Leveraging scripting or command execution capabilities
  - Testing the effectiveness of sandboxing, containerization, and other isolation mechanisms
  - Attempting privilege escalation to gain higher-level access.
- **Monitoring and Documentation:** All testing activities will be closely monitored and documented, including methods used, findings, and evidence of successful breakouts.

Work Package: Custom Protocol Fuzz Testing

Custom Protocol Fuzz Testing is a method of assessing the security and robustness of proprietary or non-standard communication protocols by sending malformed, unexpected, or random data to the protocol's implementation. The objective of the testing is to uncover vulnerabilities, crashes, memory leaks, and other weaknesses in the protocol handling.

This test will comprise:

- **Environment Setup**: Prepare a controlled testing environment that includes the implementation of the protocol under test. This can involve setting up servers, clients, and any necessary network infrastructure
- **Fuzzing Setup**: Configure fuzzing tools to generate and send malformed or random data based on the protocol specifications. This involves defining the protocol structure, message formats, and communication patterns
- **Initial Baseline Testing**: Perform baseline tests using valid protocol messages to establish normal operation and behaviour
- **Fuzz Testing Execution**: Execute the fuzzing process by sending malformed inputs to the protocol implementation and monitoring its behaviour. Record any crashes, hangs, or unexpected responses
- **Analysis and Debugging**: Analyse anomalies detected during fuzzing to determine the root cause. Debug the protocol implementation to pinpoint specific vulnerabilities or weaknesses.

Work Package: Code Review and Audit

Code review and audit is a process of systematically examining source code to identify and rectify potential security vulnerabilities, coding errors, and adherence to coding standards. This testing regime aims to improve code quality, enhance security, and ensure compliance with best practices and regulatory requirements.

This test will comprise:

- **Automated Code Review**: Use automated tools to perform an initial scan of the codebase, identifying common vulnerabilities, code smells, and compliance issues
- **Manual Code Review**: Conduct a detailed manual review of the code by experienced developers and security experts. Focus on complex logic, critical security areas, and sections flagged by automated tools
- **Security Audit**: Evaluate the code for security vulnerabilities such as SQL injection, cross-site scripting (XSS), buffer overflows, and insecure API usage. Assess the implementation of security controls and data handling practices
- **Compliance Check**: Verify that the code adheres to relevant coding standards, guidelines, and regulatory requirements. Check for proper documentation and comments.

Work Package: Binary Fuzz Testing

Binary fuzz testing is a dynamic analysis technique used to discover vulnerabilities in binary executables by providing random or malformed inputs to the program. The goal is to identify bugs, crashes, memory leaks, and other security weaknesses that can be exploited by attackers.

This test will comprise:

- **Environment Setup:** Preparation of a controlled environment to execute the fuzz testing, including setting up virtual machines or isolated test systems to prevent any impact on production environments
- **Fuzzing Setup**: Configure fuzzing tools to generate random, malformed, or semi-valid inputs. Define input vectors and execution parameters
- **Initial Baseline Testing**: Run the binary with known good inputs to establish a baseline for normal operation and behaviour
- **Fuzz Testing Execution**: Execute the fuzzing process, feeding the binary with generated inputs and monitoring its behaviour. Record any crashes, hangs, or unexpected behaviours
- **Analysis and Debugging**: Analyse the recorded anomalies to identify the root cause of crashes or unexpected behaviours. Debug the binary to pinpoint specific vulnerabilities.

ABOUT THALES

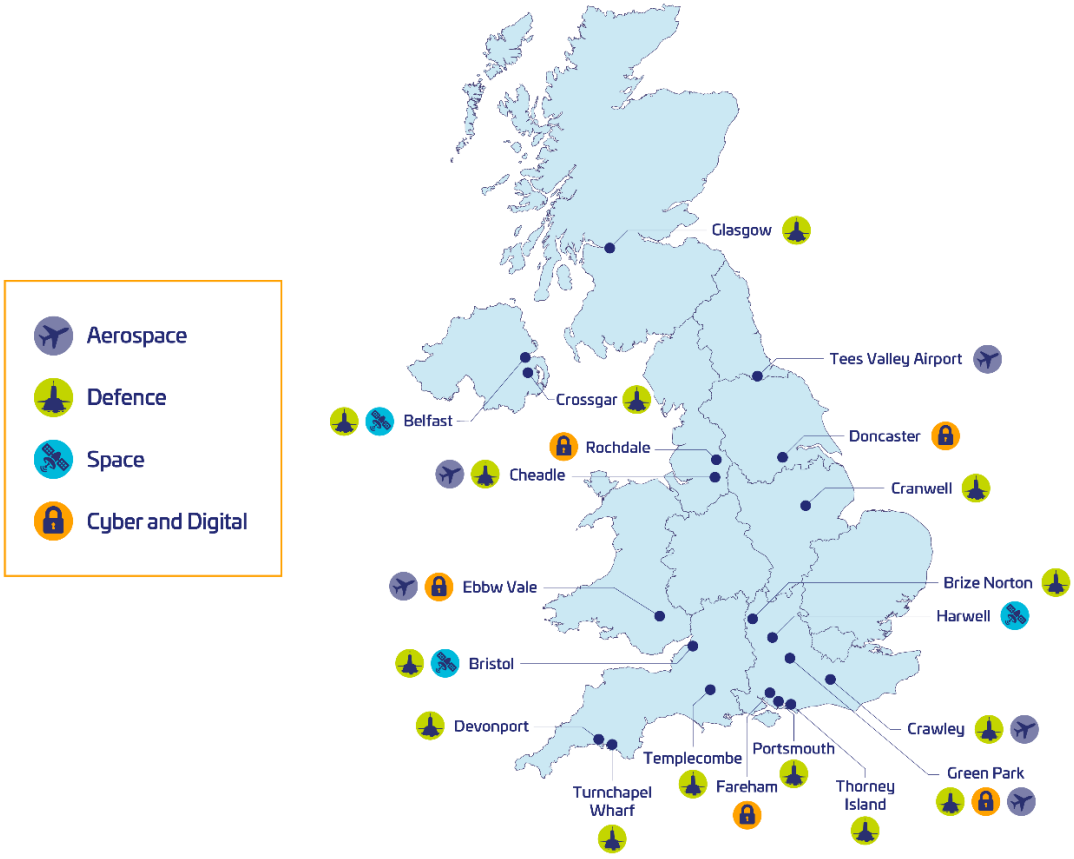
Thales in the UK has been harnessing technology to benefit the nation for over a century. Across all walks of life, you will find us securing and protecting every moment. We develop world-leading capabilities to help our customers think smarter and act faster.

Thales collaborate with partners in both government and industry, providing cutting-edge technologies to the civil and defence markets.

Thales has a significant presence across the UK, with locations strategically positioned in England, Wales, Northern Ireland, and Scotland. This geographic reach enables us to effectively support the diverse needs of local communities while contributing to the economic prosperity of all four nations. Our key facilities, along with several customer-facing sites, extend from the South West of England to Glasgow, reinforcing our commitment to regional investment and development.

The most trusted organisations in the world rely on Thales for cybersecurity solutions that keep critical assets safe. With more than 6,000 cybersecurity experts worldwide, our portfolio protects applications, data and identities, including services that close compliance gaps, detect and monitor threats and strengthen defences.

For further information, please see https://www.thalesgroup.com/en/worldwide/united-kingdom


Aerospace
Defence
Space
Cyber and Digital
Glasgow
Tees Valley Airport
Crossgar
Belfast
Doncaster
Rochdale
Cheadle
Cranwell
Ebbw Vale
Brize Norton
Harwell
Bristol
Devonport
Crawley
Templecombe
Portsmouth
Green Park
Fareham
Thorney Island
Turnchapel Wharf