ScotlandIS Cyber Security Terminology Catalogue

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

ScotlandIS, the membership and cluster management organisation for the digital technologies sector is building, supporting and enabling the digital technology ecosystem. ScotlandIS is at the heart of Scotland's digital economy, shaping, changing and driving it forward.

ScotlandIS works with members and partners to support the wider digital transformation of business and society. Digital technologies underpin modern business and are critical to Scotland's economic success. The digital technologies industry in Scotland employs over 70,000 people, offering a wide range of skills and professional services from niche specialised companies to global players. ScotlandIS membership includes technology businesses across a wide range of sectors covering telecoms, software, IT services, infrastructure specialists and digital media companies, in addition to universities, the public sector, financial services, energy industries and specialist providers.

ScotlandIS Cyber, Scotland's Cyber Cluster Management Organisation aims to bring together the cyber security community and wider ecosystem in order to support and grow the cyber security sector in Scotland and to promote our strengths in cyber security internationally (and domestically) to build our visibility and reputation globally.

In response to the increasingly complex landscape of cybersecurity threats, ScotlandIS recognises that it has become essential to provide accessible resources for both industry professionals and the wider community.

By creating a cybersecurity catalogue that helps to clarify intricate cyber capabilities in straightforward terms, we hope to be able to help empower businesses, organisations, and individuals to better understand and mitigate cybersecurity risks.

As we continue to take steps to build a cyber resilient Scotland, this catalogue aims to not only enhances and knowledge but also encourage a culture of proactive cybersecurity measures, which will ultimately contribute to a safer and more resilient digital Scotland.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Penetration Testing	Pen Testing White Hat Attacks Ethical Hacking	Penetration testing, commonly known as pen testing, is a simulated cyberattack on a computer system, network, or application to evaluate its security and identify vulnerabilities that could be exploited by malicious hackers. This process involves authorised security professionals, known as penetration testers, attempting to exploit vulnerabilities in the system's defences using the same tools and techniques as attackers. The goal is to uncover weaknesses in security controls, assess the potential impact of a real attack, and provide recommendations for remediation to enhance the overall security posture of the system. Penetration testing typically follows a	Perhaps the easiest way to consider what this is, is by imaging a digital version of your home. Just like with a house, there are clever people out there who try to find ways to break in. Penetration testing is like hiring a digital detective to play the role of a cyber intruder. They'll use all their skills to try and sneak into your home, not to cause harm, but to find any weak spots or vulnerabilities. If they succeed, it's a wake-up call for you to reinforce your defences and make your virtual home even stronger against real cyber threats.

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		systematic approach, including reconnaissance, scanning, exploitation, post-exploitation, and reporting.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Threat Hunting	Threat detection Cyber threat hunting Proactive threat detection Threat intelligence gathering Cyber threat analysis Adversary hunting Intrusion detection Security incident hunting Threat reconnaissance Cyber threat identification	Threat hunting is a cyber security practice that involves actively searching for signs of malicious activity or security breaches within an organisation's network infrastructure. It goes beyond traditional security measures such as firewalls and antivirus software by proactively seeking out potential threats that may have bypassed initial detection. Threat hunters use a variety of techniques, including data analysis, anomaly detection, and behavioural analysis, to uncover hidden threats and vulnerabilities. The goal of threat hunting is to identify and eliminate security risks before they can cause damage or disrupt operations.	Imagine your computer is like a castle, and you are responsible for its protection. Threat Hunting is like sending out your knights to search every corner of the castle to make sure no sneaky intruders have snuck in. These knights use special tools to look for clues, like footprints or open windows, that might show someone is trying to break in. If they find anything suspicious, they sound the alarm so you can take action to keep your castle safe. It's all about staying one step ahead of potential threats and keeping your digital "castle" safe and secure.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Threat Intelligence Analysis	Cyber Threat Intelligence Analysis Security Threat Analysis Threat Assessment Risk Analysis Threat Detection and Analysis Cyber Threat Assessment Threat Monitoring and Analysis Threat Research and Analysis Security Intelligence Analysis Adversary Intelligence Analysis	Threat Intelligence Analysis is the process of collecting, analysing, and interpreting information about potential and current cyber threats to identify patterns, trends, and indicators of compromise (IOCs) that may pose risks to an organisation's cyber security posture. This involves gathering data from various sources such as internal security logs, external threat feeds, open-source intelligence, and dark web monitoring. The information is then analysed to understand the tactics, techniques, and procedures (TTPs) used by threat actorstheir motives, and potential impact on the organisation's assets. The goal of Threat Intelligence Analysis is to proactively identify and mitigate security risks, enhance incident	Threat intelligence analysis is like being a detective for the digital world. Imagine you're trying to protect your home from burglars. You'd want to know where they might come from, what tools they might use, and what signs to look out for to know if they've been snooping around. In the digital world, threat intelligence analysts do something similar. They gather information about potential cyber threats, like hackers or viruses, from different sources. Then, they piece together this information to understand how these threats work, where they might come from, and what they might do. This helps organisations stay one step

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		response capabilities, and improve overall cyber security posture.	ahead and protect themselves from cyber attacks.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Incident Response	Cyber incident response Security incident response Incident handling Incident management Security incident management	Incident response, in a technical context, refers to the organised approach and process of addressing and managing the aftermath of a security breach or cyber attack. It involves identifying, containing, mitigating, and recovering from security incidents to minimise their impact on an organisation's operations and assets. This typically includes steps such as detection and analysis of the incident, containment to prevent further damage, eradication of the threat, recovery of affected systems and data, and lessons learned for future prevention. The goal of incident response is to effectively handle security incidents in a timely manner, reduce their impact, and	Incident response can be explained as the process of dealing with and recovering from unexpected events that threaten the security of computer systems or networks. It's like having a plan in place for when something bad happens, such as a cyber attack or data breach. Just like how firefighters respond to a fire, incident responders work to identify and contain the problem, minimise damage, and restore things back to normal as quickly as possible. It's all about being prepared and taking action to protect against potential threats to computer systems and data.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		restore normal operations as quickly as possible.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Malware Reverse Engineering	Malware Analysis Malware Reverse Analysis Malware Reverse-Code Engineering Reverse Malware Engineering Malware Deconstruction Malware Code Reversal Malware Code Analysis Malware Code Inspection Malware Code Disassembly Malware Code Examination	Malware reverse engineering is the process of analysing malicious software (malware) to understand its functionality, behaviour, and structure. It involves dissecting the malware's code, examining its components, and identifying its purpose, such as data theft, system compromise, or other malicious activities. Reverse engineering techniques are employed to uncover how the malware operates, including its infection vectors, command and control mechanisms, and evasion tactics. This analysis helps security professionals develop counter measures, signatures, and mitigation strategies to detect, prevent, and remediate malware infections effectively.	Malware reverse engineering is like investigating a puzzle to figure out how it works. Imagine you find a strange object on your computer that you suspect is causing problems, slowing it down or stealing information. Reverse engineering is like taking that object apart, examining each piece, and trying to understand what it does and how it does it. By doing this, experts can learn how to stop the object from causing harm and protect other computers from similar problems in the future.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Network Forensics	Network traffic analysis Packet sniffing Network packet forensics Network intrusion analysis Network security analysis	Network forensics refers to the process of capturing, recording, and analysing network traffic and activity to uncover evidence of security incidents, intrusions, or malicious activities within a computer network. It involves examining network packets, logs, and other data to reconstruct events, identify vulnerabilities, detect anomalies, and determine the scope and impact of security breaches. Network forensics enables investigators to understand how an attack occurred, track the movements of attackers, and gather evidence for legal or disciplinary action.	Network forensics is like being a detective for computer networks. Imagine your computer network is like a busy street, and every piece of information traveling through it is like a car on that street. Network forensics is the process of watching and analysing those cars (or data packets) to figure out if something bad happened, like a cyber attack. We look for clues in the traffic to understand what happened, who did it, and how they did it. It's like investigating a crime scene, but in the world of computers and networks.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Endpoint Detection and Response	EDR Endpoint Security Platform Endpoint Threat Detection and Response (ETDR) Endpoint Protection and Response (EPR) Endpoint Security Detection and Remediation (ESDR). Endpoint Threat Management (ETM Endpoint Incident Response (EIR) Host-based Intrusion Detection and Response (HIDR) Endpoint Security Analytics and Response (ESAR)	Endpoint Detection and Response (EDR) is a specialised security solution that continuously monitors and analyses endpoint activity within a network to detect and respond to advanced threats and malicious activities. It provides visibility into endpoint behaviour, detects suspicious activities or indicators of compromise, and enables rapid response to mitigate potential security incidents. EDR solutions typically involve deploying lightweight agents on endpoints, collecting telemetry data, and using advanced analytics and machine learning algorithms to identify and respond to security threats in real-time.	Endpoint Detection and Response (EDR) is like having a security guard for your computer. Just like a security guard keeps an eye on things to make sure everything is safe, EDR software watches your computer to catch any bad guys trying to do harm. It looks for signs of trouble, like strange behaviour or suspicious activity, and then takes action to stop it before it causes any damage. So, think of EDR as your computer's personal bodyguard, always on the lookout for danger and ready to spring into action to keep you safe.

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

	Endpoint Security Monitoring and Response (ESMR) Device Threat Detection and Response (DTDR)		

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Security Information and Event Management	SIEM Security Operations Center (SOC) Security Event Management (SEM) Log Management Security Analytics Platform Threat Detection and Response Platform	Security Information and Event Management (SIEM) is a software solution that aggregates and analyses security events and logs from various sources across an organisation's IT infrastructure. It provides real-time monitoring, correlation, and analysis of security-related data to identify potential security threats, breaches, or abnormal activities. SIEM systems collect data from network devices, servers, applications, and other sources, normalise and correlate this data, and then generate alerts or reports to help security teams detect, investigate, and respond to security incidents effectively. Additionally, SIEM platforms often include features such as log management, incident response automation, and	Security Information and Event Management (SIEM) is similar to having a digital security guard for your computer systems. It keeps an eye on everything happening in your network, who's logging in, what programs are running, and if any files are being accessed. If it notices something suspicious, like a hacker trying to get in or a virus spreading, it alerts you so you can take action to stop it. It's a watchful eye that helps keep your digital world safe and secure.

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		compliance reporting to help organisations improve their overall security posture and meet regulatory requirements.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Identity and Access Management	IAM Access Control User Authentication User Provisioning Single Sign-On (SSO) Privileged Access Management (PAM) Identity Governance and Administration (IGA) Credential Management User Lifecycle Management Authentication and Authorisation Management User Identity Management	Identity and Access Management (IAM) is a framework of policies, processes, and technologies that ensures the appropriate individuals within an organisation have the right access to the right resources at the right time. It involves the management of digital identities, including user authentication, authorisation, and provisioning, as well as the management of privileges and permissions associated with those identities. The goal of IAM is to maintain security while enabling efficient access to resources and applications across an organisation's IT infrastructure.	Identity and Access Management (IAM) is similar to having a digital key to access different rooms in a building. Just as you need a specific key to enter certain rooms, IAM helps make sure that only the right people in a company can access certain parts of its computer systems. It keeps things secure by giving each person the right "key" (or digital access) to the right "rooms" (or parts of the computer system) they need to do their job. Like a digital bouncer that checks everyone's ID before letting them into the party.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Zero Trust Architecture	Zero Trust Security BeyondCorp Perimeterless security Continuous verification Least privilege access Micro-segmentation Network segmentation Adaptive access control Continuous authentication Identity-centric security	Zero Trust Architecture is a cyber security approach that assumes all users, devices, and network traffic are untrusted, regardless of whether they are inside or outside the corporate network perimeter. It is based on the principle of "never trust, always verify." In zero trust architecture, access controls are strictly enforced through continuous authentication, least privilege access, and micro-segmentation. This means that users and devices must authenticate themselves and their activities are continuously monitored and verified before granting access to resources or data. Zero trust architecture aims to enhance security by reducing the attack surface and minimising	Zero Trust Architecture is a fortress for your computer network. Imagine you have a castle, and instead of just having big walls around it, you also have guards at every door and window. But these guards don't just let anyone in. They check everyone who wants to come in, making sure they are who they say they are and that they're allowed to enter. Similarly, in a computer network with Zero Trust Architecture, every person or device trying to connect to the network has to prove they're trustworthy before they're allowed in. This extra layer of security helps keep the network safe from bad guys

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		the impact of potential security breaches.	who might try to sneak in and cause trouble.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Data Loss Prevention	DLP Data Leakage Prevention Data Leak Prevention Information Leak Prevention Information Leakage Prevention Data Loss Protection Data Leak Detection Information Loss Prevention Data Loss Protection	Data loss prevention (DLP) is a set of tools, processes, and policies designed to prevent sensitive data from being lost, stolen, or exposed to unauthorised individuals or entities. It involves identifying and classifying sensitive data, monitoring and controlling its movement both within and outside an organisation's network, and taking proactive measures to prevent data breaches and leaks. DLP solutions typically include features such as data encryption, access controls, monitoring of user activities, and policies for data handling and sharing. The goal of DLP is to protect confidential information, maintain regulatory compliance, and safeguard the reputation and integrity of an organisation.	You could describe data loss prevention (DLP) as a way to keep important information safe and secure. It's like having a lock on your door to prevent burglars from getting into your house and stealing your valuables. DLP tools and systems work behind the scenes to make sure that sensitive data, like personal information or company secrets, doesn't get into the wrong hands. They keep an eye on where data is going, who's accessing it, and if anyone is trying to take it without permission. Overall, DLP helps businesses and individuals keep their private information safe and protect against data breaches.

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Security Orchestration, Automation, and Response	SOAR Incident Response Automation Threat Management Platform Security Automation and Orchestration (SAO) Security Operations Automation Security Incident and Event Management (SIEM) with Automation Incident Lifecycle Management Threat Intelligence Orchestration Automated Incident Handling Security Workflow Automation Cyber Defence Orchestration	Security Orchestration, Automation, and Response (SOAR) is a strategic approach to cyber security operations that combines orchestration, automation, and response capabilities to improve the efficiency and effectiveness of security teams in detecting, investigating, and responding to security incidents. **Orchestration**: Refers to the coordination and integration of disparate security tools, processes, and workflows to ensure seamless communication and collaboration among them. Orchestration allows for the automated execution of predefined workflows, such as incident response playbooks, across multiple security systems and technologies.	Imagine you are protecting your home from potential intruders. You have security cameras, motion sensors, and an alarm system in place to detect any suspicious activity. Now, imagine if you could have a smart system that not only detects a break-in but also automatically takes action to stop it and alerts the authorities if needed, all without you having to do anything. Security Orchestration, Automation, and Response (SOAR) is like that smart system but for your digital security. It's a way for organisations to better protect

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		Automation: Involves the use of technology to automate repetitive and manual security tasks, such as alert triage, enrichment, and containment actions. Automation helps to accelerate incident response times, reduce human error, and free up security analysts to focus on more complex tasks that require human judgment. **Response**: Encompasses the actions taken by security teams to mitigate and remediate security incidents. This includes both automated responses triggered by predefined playbooks as well as manual interventions guided by the analysis and decision-making of security analysts. Effective response capabilities ensure that security incidents are contained and resolved in a timely manner to	their digital assets from cyber threats. **Orchestration**: Just like your smart system coordinates different security devices at home, SOAR coordinates different security tools and systems in a company's network. It ensures they work together seamlessly, sharing information and acting in concert. **Automation**: Think of this as the "auto-pilot" feature of your smart security system. It automatically handles routine tasks and responses to security alerts. For example, if a suspicious file is detected, the system can automatically quarantine it or shut down access to affected areas,

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		minimize impact and prevent future occurrences. Overall, SOAR platforms serve as centralized hubs that enable security teams to orchestrate and automate their incident response processes, leveraging integrations with existing security tools, threat intelligence feeds, and workflows to enhance the organisation's overall security posture.	saving time and reducing the risk of human error. **Response**: This is like having a security team ready to respond immediately to any threat. SOAR helps security teams quickly investigate and respond to security incidents, whether it's isolating a compromised device, blocking a malicious website, or notifying relevant authorities.SOAR is like having a digital security guard that not only watches out for threats but also takes action to stop them, all while keeping you informed about what's happening. It's a way for organisations to stay one step ahead of cyber criminals and protect their valuable data and systems.

Funded by The Scottish Government

Capability	Also Known As	Definition	Clarification
Cloud Security	Cloud Security Posture Management (CSPM) Cloud Security Governance Cloud Access Security Broker (CASB Cloud Compliance Cloud Data Protection Cloud Identity and Access Management (Cloud IAM) Cloud Encryption Cloud Workload Protection Cloud Security Services DevSecOps (Development, Security, Operations)	Cloud security refers to the set of practices, technologies, policies, and controls implemented to protect data, applications, and infrastructure within cloud computing environments. It encompasses various security considerations, including confidentiality, integrity, availability, authentication, authorisation, and accountability, aimed at safeguarding cloud-based resources from unauthorised access, data breaches, and other cyber threats. **Data Protection**: Ensuring the confidentiality, integrity, and availability of data stored, processed, and transmitted in the cloud through encryption, access controls, data loss prevention (DLP),	Imagine the cloud as a vast digital space where you can store your files, run programmes, and do all sorts of things online. Just like you want to keep your physical belongings safe and secure, you also need to protect your stuff in the cloud. Cloud security is like having a set of digital locks and guards to keep your things safe in this virtual space. It's all about making sure that only the right people can access your files and programmes, and that they stay safe from hackers and other bad actors. Here's what cloud security involves in simpler terms:

Funded by The Scottish Government

		and backup and recovery mechanisms. **Identity and Access Management (IAM)**: Managing user identities, permissions, and access controls to cloud resources to ensure that only authorized users and devices can access sensitive information and perform permitted actions. **Network Security**: Securing network communications and traffic within cloud environments using firewalls, intrusion detection/prevention systems (IDS/IPS), virtual private networks (VPNs), and other network security measures to prevent unauthorised access and data exfiltration. **Application Security**: Protecting cloud-based applications and APIs against common vulnerabilities and threats, such as injection	**Locking the Door**: Just like you lock your house to keep intruders out, cloud security involves setting up virtual locks to keep unauthorised people from accessing your data and programmes. **Checking IDs**: Imagine needing a special key or password to get into a secret club. Cloud security involves making sure that only the right people have the right keys or passwords to access your stuff in the cloud. **Keeping an Eye Out**: Security guards watch over your house to make sure everything's okay. In the cloud, security measures keep an eye out for any suspicious activity, like someone trying to break in,

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		attacks, cross-site scripting (XSS), and unauthorised access, through secure coding practices, vulnerability assessments, and runtime protection mechanisms. **Compliance and Governance**: Ensuring compliance with regulatory requirements, industry standards, and internal policies within cloud environments, including data privacy regulations, industry-specific mandates, and contractual obligations. **Security Monitoring and Incident Response**: Implementing continuous monitoring, threat detection, and incident response capabilities to identify and mitigate security incidents, such as unauthorised access attempts, data breaches, and malicious activities, in a timely manner.	and alert you so you can take action. **Making Sure Everything's Safe**: Cloud security also involves things like making sure your files and programmes don't get messed up or stolen. It's like putting your valuables in a safe to keep them protected. **Following the Rules**: Just like there are rules to keep everyone safe on the road, there are rules and regulations for keeping things secure in the cloud. Cloud security helps make sure everyone follows these rules to keep the digital space safe for everyone. Think of cloud security as your digital security guard, keeping watch over your virtual

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		Security Architecture and Design: Designing and implementing secure cloud architectures and configurations based on security best practices and industry standards to minimise security risks and vulnerabilities throughout the cloud lifecycle. Cloud security is a shared responsibility between cloud service providers (CSPs) and cloud customers, with CSPs responsible for securing the underlying cloud infrastructure and customers responsible for securing their data, applications, and configurations within the cloud environment. Effective cloud security requires a holistic approach, integrating technical controls, organizational policies, and user awareness to address the evolving threat	belongings and making sure they stay safe and sound in the cloud.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		landscape and mitigate security risks in cloud computing.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Container Security	Containerisation Security Container Security Posture Management (CSPM Container Runtime Container Image Security Kubernetes Security Microservices Security DevSecOps (Development, Security, Operations) Cloud-Native Security Immutable Infrastructure Security Runtime Protection	Container security is a set of practices, processes, and technologies aimed at securing containerised applications and the container runtime environment against various threats, vulnerabilities, and risks. **Image Security**: Container images, which contain the application code and dependencies, need to be scanned for vulnerabilities, misconfigurations, and malware before deployment. Image security involves using tools to analyse container images for known vulnerabilities and ensuring that only trusted and verified images are used. **Runtime Security**: Once containers are deployed and running, runtime security measures are employed to	Imagine you're running a restaurant with a lot of different dishes being prepared in the kitchen. Each dish has its own ingredients and recipe.Now, think of each dish as a container and the kitchen as your computer system. **Keeping Ingredients Safe**: Just like you want to make sure your ingredients are fresh and safe to use, container security ensures that the "ingredients" used to create your containers (like software code and libraries) are free from anything harmful, like bugs or viruses. **Watching Over the Cooking Process**: As your dishes are

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		protect against runtime threats. This includes monitoring container behaviour, enforcing access controls, and detecting and preventing unauthorised access, privilege escalation, and abnormal activities within the container runtime environment. **Isolation**: Containers should be isolated from each other and from the underlying host system to prevent container escapes and minimise the impact of security breaches. Techniques such as namespace and group isolation, as well as container network segmentation, are used to achieve this. **Network Security**: Containerised applications communicate with each other and with external systems over networks. Network security measures, such as network	being prepared, you want to keep an eye on the cooking process to make sure everything is going smoothly. Container security does the same thing—it monitors what's happening inside each container to ensure that nothing strange or unexpected is going on. **Preventing Cross-Contamination**: You wouldn't want one dish to accidentally mix with another?? Container security helps prevent this kind of mixing by keeping each container separate from the others, so they can't interfere with each other's "cooking." **Locking the Kitchen Doors**: Just like you'd lock the doors to your kitchen to keep unwanted guests out, container security

Funded by The Scottish Government

		policies, firewalls, and encryption, are implemented to secure container-to-container communication and protect against network-based attacks. **Orchestration Platform Security**: Container orchestration platforms, such as Kubernetes, manage the deployment, scaling, and lifecycle of containers. Securing the orchestration platform involves configuring access controls, securing API endpoints, and implementing security best practices to protect against unauthorised access and control plane attacks. **Identity and Access Management (IAM)**: Proper authentication and authorisation mechanisms are crucial for controlling access to containerized resources. IAM solutions are used to manage user	puts digital locks on your containers and the system they run on, so only authorised users can access them. **Checking the Recipe**: Before serving a dish, you'd check the recipe to make sure everything is done correctly. Similarly, container security checks to make sure each container follows the right "recipe" (or configuration) to keep it secure and working properly. **Keeping Records**: Finally, container security keeps records of everything that happens in the kitchen—what ingredients were used, who cooked what, and so on. This helps you keep track of any problems and fix them quickly.

Funded by The Scottish Government

		identities, assign permissions, and enforce access controls within containerised environments. **Logging and Monitoring**: Comprehensive logging and monitoring are essential for detecting and responding to security incidents in containerised environments. Logging tools capture container logs, audit trails, and security events, while monitoring solutions provide real-time visibility into container activity and performance metrics. **Compliance and Governance**: Containerised environments must adhere to regulatory requirements, industry standards, and organisational policies. Compliance and governance frameworks are implemented to ensure that container deployments meet security and compliance	Container security is like having a team of digital chefs and security guards in your kitchen, making sure that each dish (container) is prepared safely and served without any surprises. It's all about keeping your digital "kitchen" running smoothly and securely.

Funded by The Scottish Government

		objectives, with regular audits and assessments conducted to verify adherence.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Web Application Firewall	WAF Application Firewall Web Security Gateway Web Firewall HTTP Firewall Layer 7 Firewall Intrusion Prevention System (IPS) Content Security Policy (CSP) Web Application Shield	A Web Application Firewall (WAF) is a security tool designed to protect web applications from a variety of online threats and attacks by filtering and monitoring HTTP/HTTPS traffic between a web application and the Internet. Here's a more detailed technical definition: **Filtering and Monitoring**: WAFs inspect incoming and outgoing web traffic to and from a web application, analyzing each HTTP request and response for signs of malicious activity, anomalies, or violations of security policies. **Rule-Based Security Policies**: WAFs use a set of predefined rules, signatures, or policies to identify and block known attack patterns,	Imagine you're the owner of a shop with a big glass window facing the street. People passing by can see everything inside your shop. Now, think of your shop as a website or an online store, and the window as the connection between your website and the internet. A Web Application Firewall (WAF) is the same as having a security guard stationed at your shop's window. Their job is to watch out for any suspicious characters passing by and make sure they don't try to disrupt your storefront, like throwing rocks or trying to break in. **Keeping an Eye Out**: The WAF security guard watches all the

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		such as SQL injection, cross-site scripting (XSS), command injection, and other common web application vulnerabilities. **Behavioral Analysis**: Advanced WAFs may employ behavioral analysis techniques to detect anomalies in web traffic, such as unusual patterns of requests or suspicious user behavior, which may indicate a potential attack. **Virtual Patching**: WAFs can provide virtual patches for known vulnerabilities in web applications by blocking malicious requests targeting those vulnerabilities, thereby mitigating the risk until a permanent fix can be applied. **Logging and Reporting**: WAFs generate logs and reports of web traffic activity, including blocked requests, security incidents, and	people (web traffic) passing by your shop (website). They keep an eye out for anyone who looks like they might cause trouble. **Spotting Trouble**: If the security guard sees someone acting suspiciously, like trying to peek into the shop or tamper with the window, they'll step in and stop them before they can do any harm. **Blocking Bad Stuff**: Sometimes, the security guard might see someone trying to throw rocks or spray graffiti on your shop window. In web terms, these could be hackers trying to steal data or break into your website. The WAF can block these attacks to keep your website safe.

Funded by The Scottish Government

		compliance violations, to provide visibility into the security posture of the protected web applications. **SSL/TLS Inspection**: Some WAFs support SSL/TLS decryption and inspection to analyze encrypted HTTPS traffic for potential threats, ensuring comprehensive protection even for encrypted communications. **Integration with Security Ecosystem**: WAFs may integrate with other security tools and platforms, such as SIEM (Security Information and Event Management) systems, intrusion detection/prevention systems (IDS/IPS), and security analytics platforms, to enhance threat detection and response capabilities.	**Alerting the Owner**: If something unusual happens, (a crowd suddenly gathering outside your shop, the security guard will alert you so you can take action. Similarly, the WAF will notify you if it detects any suspicious activity on your website, so you can investigate and fix any problems. In simple terms, a Web Application Firewall is like having a vigilant security guard protecting your online shop from potential troublemakers and keeping your website safe and secure for your customers.

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		Customisation and Tuning: WAFs often provide options for customising security policies, creating custom rules, and fine-tuning the behavior of the firewall to suit the specific security requirements and application architecture of each web application. Overall, a Web Application Firewall serves as a critical security control for protecting web applications from a wide range of threats and vulnerabilities, helping to safeguard sensitive data, prevent unauthorized access, and ensure the availability and integrity of web services.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Threat Modelling	Risk Assessment Security Architecture Review Attack Surface Analysis Security Requirements Analysis Vulnerability Assessment Security Risk Management Security Controls Evaluation Adversarial Simulation Threat Intelligence Analysis Secure Design Review	Threat modelling is a systematic approach to identifying and evaluating potential security threats and vulnerabilities in systems, applications, or processes. It involves analysing the architecture, design, and implementation of a system to understand potential attack vectors and assess the associated risks. Here's a more technical breakdown of threat modelling: **Asset Identification**: The first step in threat modelling is to identify the assets that need protection, such as data, infrastructure components, or critical business processes.	Imagine you're building a fortress to protect your treasure. You want to make sure it's safe from thieves and other dangers. Threat modelling is like having a plan to identify and block any potential threats to your treasure. **Knowing What's Important**: First, you need to figure out what exactly you're trying to protect. In our case, it's the treasure. In the digital world, it could be your personal information, your company's data, or even your favourite online game account. **Thinking Like a Thief**: Next, you need to put yourself in the shoes of a thief and think

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		Threat Enumeration: Next, potential threats are systematically enumerated, considering various threat sources, including malicious actors, insiders, or environmental factors, and potential attack methods, such as unauthorised access, data manipulation, or service disruption. **Vulnerability Assessment**: Threat modelling involves identifying and assessing vulnerabilities or weaknesses in the system that could be exploited by the identified threats. This includes analysing the security controls, design flaws, configuration errors, or implementation weaknesses that could facilitate attacks. **Risk Analysis**: Once threats and vulnerabilities are identified, a risk analysis is conducted to evaluate the likelihood and potential impact	about all the ways someone might try to steal your treasure. This could include sneaking in through a window, breaking down the door, or digging a tunnel underneath. **Finding Weak Spots**: Once you've imagined all the ways a thief might try to get in, you need to look for weak spots in your fortress. Maybe there's a window that doesn't latch properly or a door that's easy to pick open. In the digital world, these weak spots might be things like outdated software or a password that's easy to guess. **Making a Plan to Protect**: Finally, armed with knowledge of the potential threats and weaknesses, you can make a plan to protect your treasure.

Funded by The Scottish Government

		of each threat scenario on the organization's assets and operations. This involves assessing the severity of the threat, the likelihood of occurrence, and the potential business impact if exploited. **Mitigation Planning**: Based on the identified threats and vulnerabilities, threat modelling aims to develop mitigation strategies and security controls to reduce the risk exposure and mitigate the potential impact of security incidents. This may involve implementing technical controls, improving security processes, or enhancing security awareness and training. **Documentation and Communication**: Threat modelling findings, recommendations, and mitigation strategies are	This might involve installing stronger locks, adding security cameras, or hiring guards to patrol the perimeter. In the digital world, it could mean things like updating your software regularly, using strong passwords, and installing antivirus software. **Keeping Watch and Adapting**: Threat modelling isn't a one-time thing—it's an ongoing process. Just like you'd keep watch over your fortress to make sure no new threats emerge, you need to stay vigilant in the digital world too. That means staying up-to-date on the latest security threats and adapting your defences accordingly. In simple terms, threat modelling is having a plan to

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		documented in a formal report or documentation that can be shared with relevant stakeholders, such as security teams, developers, architects, and business owners. Effective communication of threat modelling results is essential for ensuring that security risks are understood and addressed appropriately. Overall, threat modelling provides a structured approach for organisations to proactively identify and address security risks, helping to strengthen their security posture and resilience against cyber threats. It is an essential component of cybersecurity risk management and is often integrated into the software development lifecycle and system design processes to build security into systems from the outset.	protect your treasure by thinking like a thief, finding weak spots, and putting measures in place to keep it safe. It's all about staying one step ahead of the bad guys to keep what's important to you secure.

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Cryptography	Encryption Decryption Cryptanalysis Cryptology Ciphertext Plaintext Cryptosystem Key Management Digital Signature Hash Function Public-Key Cryptography Symmetric Cryptography Asymmetric Cryptography	Cryptography is the science and practice of securing communication and data through the use of mathematical techniques and algorithms. It encompasses various methods for encrypting information to ensure confidentiality, integrity, authenticity, and non-repudiation. Here's a more detailed technical definition of cryptography: **Encryption**: Cryptography involves the process of converting plaintext (unencrypted data) into ciphertext (encrypted data) using cryptographic algorithms and keys. Encryption ensures that only authorised parties with the appropriate decryption keys can	Imagine you have a secret message you want to send to your friend, but you're worried someone might intercept it and read it along the way. Cryptography is like putting your message in a special lockbox before sending it. Only you and your friend have the keys to open the lockbox and read the message. **Locking the Message**: Before you send your message, you use a special code to lock it up, making it unreadable to anyone who doesn't have the key. This process is called encryption. **Sending the Locked Message**: Now that your message is safely locked up, you can send

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		access and understand the original plaintext. **Decryption**: Cryptography also includes the process of reversing encryption, converting ciphertext back into its original plaintext form using the corresponding decryption keys. Decryption allows authorised recipients to access and interpret encrypted data. **Cryptographic Algorithms**: Cryptography relies on various mathematical algorithms and techniques for encrypting and decrypting data. These algorithms include symmetric encryption algorithms (e.g., AES, DES) that use a single shared secret key for encryption and decryption, as well as asymmetric encryption algorithms (e.g., RSA, ECC) that use	it through the mail, over the internet, or any other way you like. Even if someone tries to peek at it while it's being sent, they won't be able to understand it because it's all scrambled up inside the lockbox. **Unlocking the Message**: When your friend receives the locked message, they use their special key to unlock the lockbox and reveal the original message. This process is called decryption. In simple terms, cryptography is like using a secret code to protect your messages from prying eyes while they're being sent from one place to another. It's a way to keep your communications private and

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		pairs of public and private keys for encryption and decryption. **Key Management**: Cryptography involves the generation, distribution, storage, and protection of cryptographic keys used for encryption, decryption, and other cryptographic operations. Key management practices ensure the secure handling of keys to prevent unauthorized access and maintain the confidentiality and integrity of encrypted data. **Cryptographic Hash Functions**: Cryptography includes the use of cryptographic hash functions, which are mathematical algorithms that convert input data into a fixed-size hash value or digest. Hash functions are used for data integrity verification,	secure, even in a world full of potential eavesdroppers.

Funded by The Scottish Government

		password hashing, and digital signatures. **Digital Signatures**: Cryptography encompasses digital signature techniques, which provide a way to verify the authenticity, integrity, and origin of digital messages or documents. Digital signatures use asymmetric cryptography to generate and verify signatures, ensuring non-repudiation and message integrity. **Cryptographic Protocols**: Cryptography includes the design and implementation of cryptographic protocols, such as SSL/TLS for secure communication over the Internet, SSH for secure remote access, and IPsec for secure network communication. Overall, cryptography plays a crucial role in ensuring the security	

Funded by The Scottish Government

		and privacy of communication, data storage, and digital transactions in various domains, including cybersecurity, information technology, and telecommunications. It provides essential tools and techniques for protecting sensitive information and mitigating security risks in modern computing environments.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Security Testing	Penetration Testing (Pen Testing) Vulnerability Assessment Ethical Hacking Security Auditing Security Review Code Review (or Secure Code Review Red Teaming Threat Modelling Risk Assessment Security Validation	Security testing is a systematic evaluation process conducted to assess the security posture of systems, applications, networks, or other digital assets. It involves identifying, analysing, and mitigating security vulnerabilities, weaknesses, and threats to safeguard against unauthorized access, data breaches, and other security incidents. Here's a more detailed technical definition of security testing: **Identification of Security Risks**: Security testing involves identifying potential security risks and threats that could compromise the confidentiality, integrity, or availability of digital assets. This includes assessing the security architecture, design, and	Security testing is similar tochecking the locks on your house to make sure they're strong enough to keep out burglars. Just as you want your home to be safe and secure, security testing ensures that your digital belongings , like websites, apps, and computer networks, is protected from hackers and other bad actors. **Checking for Weak Spots**: Like a burglar might look for a weak spot in your house, security testing looks for weaknesses, called vulnerabilities, in your digital house. These could be things like open windows (unsecured network ports), flimsy locks

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		implementation of systems or applications to identify potential vulnerabilities and attack vectors. **Evaluation of Security Controls**: Security testing assesses the effectiveness of security controls, mechanisms, and countermeasures implemented to protect digital assets against security threats. This includes evaluating access controls, encryption mechanisms, authentication mechanisms, intrusion detection systems, and other security defences. **Detection of Security Vulnerabilities**: Security testing aims to detect and identify security vulnerabilities, weaknesses, and misconfigurations that could be exploited by attackers to compromise systems or applications. This may involve	(weak passwords), or hidden spare keys (backdoor access). **Testing the Locks**: Security testing tries to break into your digital home, just like a burglar might try to break into your house. But instead of using crowbars and lockpicks, security testers use special tools and techniques to find and exploit vulnerabilities. This helps identify areas where your security measures need to be strengthened. **Fixing the Weaknesses**: Once vulnerabilities are found, security testing helps you figure out how to fix them. This might involve installing stronger locks (updating software), adding security cameras (firewalls and intrusion detection systems),

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		using automated scanning tools, manual analysis, and penetration testing techniques to identify common vulnerabilities, such as SQL injection, cross-site scripting (XSS), or insecure configuration settings. **Validation of Security Compliance**: Security testing ensures that systems, applications, or networks comply with security standards, best practices, regulatory requirements, and industry-specific security guidelines. This includes assessing compliance with standards such as ISO 27001, NIST Cybersecurity Framework, PCI DSS, HIPAA, or GDPR. **Remediation and Mitigation**: Security testing provides actionable insights and recommendations for remediating identified security vulnerabilities	or hiring a security guard (security professionals) to keep watch. **Keeping Watch**: Security testing isn't a one-time thing—it's an ongoing process. Just like you might check your locks regularly to ensure they're still working, security testing helps you stay vigilant and keep your digital home safe from new threats that might emerge over time. In simple terms, security testing is similar to having a digital security guard checking your locks and windows to make sure your online home stays safe and secure from cyber intruders.

Funded by The Scottish Government

		and mitigating security risks. This may include implementing security patches, applying configuration changes, enhancing security controls, or updating security policies and procedures to address identified weaknesses. **Risk Management**: Security testing contributes to the overall risk management process by identifying, assessing, and prioritising security risks based on their likelihood and potential impact. This allows organisations to allocate resources effectively and prioritise security initiatives to mitigate the most critical risks. Overall, security testing is a critical component of cybersecurity risk management, helping organisations proactively identify and address security vulnerabilities and threats to protect digital assets	

Funded by The Scottish Government

		and mitigate the risk of security incidents. It encompasses a range of testing techniques, methodologies, and tools to assess the security posture of systems, applications, and networks comprehensively.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Mobile Device Management	MDM Enterprise Mobility Management (EMM) Unified Endpoint Management (UEM) Mobile Application Management (MAM) Bring Your Own Device (BYOD) Management Mobile Security Management Mobile Content Management (MCM) Device Enrolment Programme (DEP) Android Enterprise Remote Device Management Mobile Device Security	Mobile Device Management (MDM) is a security software solution that enables organizations to manage and secure mobile devices (such as smartphones, tablets, and laptops) deployed across their workforce. It provides administrators with centralised control and visibility over mobile devices, allowing them to enforce security policies, configure device settings, distribute applications, and remotely monitor and manage devices. **Device Enrolment**: MDM facilitates the enrolment of mobile devices into the organization's management system, typically through an enrolment process that establishes a trusted relationship between the device and the MDM server. This allows administrators to	Imagine you're running a big organisation with lots of employees who use smartphones and tablets for work. Now, keeping all those devices safe and organised is a big job. That's where Mobile Device Management (MDM) comes in. Here's a simple way to understand it: **Keeping Track of Devices**: MDM helps you keep track of all the smartphones and tablets your employees use for work. Having a list of all your company's devices, along with who's using them and what they're being used for.

Funded by The Scottish Government

		manage and monitor enrolled devices remotely. **Configuration Management**: MDM enables administrators to remotely configure and manage device settings, such as Wi-Fi and VPN configurations, email and account settings, device passcode requirements, and security policies. Configuration profiles can be deployed to devices over-the-air (OTA) to ensure consistent settings across the organization. **Application Management**: MDM allows administrators to distribute, manage, and update mobile applications (both in-house and third-party apps) on enrolled devices. This includes installing, updating, and removing apps, as well as controlling access to enterprise app stores and	**Making Sure Devices are Secure**: Just like you'd want to make sure your company's building is secure, MDM helps you make sure all those devices are safe from hackers and other threats. It helps you set up things like passwords and encryption to keep your company's information safe. **Managing Apps and Settings**: MDM lets you control what apps your employees can use on their devices and how those devices are set up. You can make sure everyone has the right tools they need to do their jobs, without worrying about them downloading anything harmful. **Fixing Problems Remotely**: If something goes wrong with one of the devices, if it gets

Funded by The Scottish Government

		blacklisting or whitelisting apps based on security policies. **Security Management**: MDM helps organizations enforce security policies and controls to protect sensitive data and mitigate security risks on mobile devices. This includes enforcing device encryption, enforcing passcode policies, enforcing device compliance rules, and remotely locking or wiping lost or stolen devices. **Monitoring and Reporting**: MDM provides administrators with visibility into the status and usage of enrolled devices through monitoring and reporting capabilities. This includes tracking device inventory, monitoring device health and compliance status, generating usage reports, and	lost or stops working properly, MDM lets you fix it remotely. You can lock it down so no one else can use it, or even wipe it clean to protect your company's data. **Keeping Everything Organized**: Overall, MDM helps you keep all those devices organised and running smoothly. It's like having a digital manager who takes care of all the little details so you can focus on running your business. In simple terms, Mobile Device Management is similar tohaving a digital assistant that helps you keep all your company's smartphones and tablets safe, organised, and working smoothly, so your

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		detecting security incidents or policy violations. **Remote Management**: MDM enables administrators to perform remote management tasks on enrolled devices, such as remote troubleshooting, remote support, remote lock, remote wipe, and remote configuration changes. This helps organisations maintain control over mobile devices even when they are not physically accessible. **Integration with Enterprise Systems**: MDM solutions often integrate with other enterprise systems and tools, such as directory services (e.g., Active Directory), identity and access management (IAM) systems, email servers, and security information and event management (SIEM) systems, to streamline device	employees can focus on getting their work done.

Funded by The Scottish Government

		management and enhance security posture.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	**Also Known As**	**Definition**	**Clarification**
Network Segmentation	Network Isolation Subnetting Microsegmentation Zone-based Security VLAN Segmentation Perimeter Security Network Access Control (NAC) Zero Trust Architecture Software-Defined Networking (SDN Firewall Rulesets	Network segmentation is a security practice that involves dividing a computer network into smaller subnetworks or segments to improve security, control access, and optimize network performance. It aims to restrict the flow of network traffic between different parts of the network based on security policies and access controls, reducing the potential attack surface and limiting the impact of security incidents or breaches. Here's a more detailed technical definition of network segmentation: **Division of Network into Subnetworks**: Network segmentation involves dividing a	Imagine your computer network is like a big city with different neighbourhoods. Each neighbourhood has its own rules, borders, and security guards to keep things safe. Network segmentation is like dividing the city into smaller neighbourhoods, each with its own set of rules and security measures. This helps control who can go where and prevents problems from spreading too far if something goes wrong. **Creating Neighbourhoods**: Just like you'd split a city into neighbourhoods, network

Funded by The Scottish Government

		larger computer network into smaller logical or physical segments, known as subnetworks or segments. This can be achieved through various means, including VLANs (Virtual Local Area Networks), subnetting, or physical network segmentation using routers or switches. **Isolation of Traffic**: Once the network is segmented, each segment operates as a separate network entity with its own set of security policies, access controls, and communication boundaries. This isolation helps contain network traffic within specific segments and prevents unauthorised access between segments. **Implementation of Access Controls**: Network segmentation enables the implementation of access controls and security	segmentation splits your computer network into smaller parts, called segments. Each segment might include certain computers, servers, or devices that need to communicate with each other. **Setting Rules and Borders**: In each neighbourhood, there are rules about who can come in and what they can do. Similarly, network segmentation sets up rules and boundaries for how data can move between different segments of the network. This helps keep sensitive information safe and prevents unauthorised access. **Adding Security Guards**: Think of security guards as the protective measures in each neighbourhood. Network

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		policies to regulate the flow of traffic between segments. This includes defining firewall rules, access control lists (ACLs), and security zones to restrict or allow communication between different segments based on criteria such as IP addresses, port numbers, or protocols. **Enhanced Security**: By limiting communication between segments, network segmentation reduces the attack surface and mitigates the risk of lateral movement by attackers within the network. It helps contain security incidents or breaches to specific segments, limiting their impact on the overall network infrastructure. **Optimised Performance**: Network segmentation can improve network performance by reducing broadcast traffic, congestion, and	segmentation adds security measures, like firewalls and access controls, to each segment of the network. These guards keep an eye on who's trying to enter or leave and make sure everything stays safe. **Preventing Problems from Spreading**: If there's a problem in one neighbourhood, like a fire or a burglary, you don't want it to spread to the whole city. Similarly, network segmentation helps contain problems within their own segment, so they don't affect the entire network. This limits the damage and makes it easier to fix things. In simple terms, network segmentation is dividing your computer network into

Funded by The Scottish Government

		latency within individual segments. It allows organisations to prioritie critical applications or services and allocate network resources more efficiently to meet performance requirements. **Compliance and Regulatory Requirements**: Network segmentation helps organisations achieve compliance with regulatory requirements and industry standards by implementing segmentation controls to protect sensitive data, such as personally identifiable information (PII), financial data, or healthcare records. **Dynamic Segmentation**: Advanced network segmentation techniques, such as software-defined networking (SDN) and micro segmentation, enable dynamic and policy-driven segmentation	smaller, more manageable parts, each with its own rules and protections. It helps keep your data safe, prevents problems from spreading, and makes your network more secure overall.

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		based on contextual factors, such as user identity, device type, or application behaviour. Overall, network segmentation is a fundamental security strategy that plays a crucial role in protecting organisational assets, enhancing network performance, and ensuring compliance with security requirements and industry standards.	

Funded by The Scottish Government

Capability	Also Known As	Definition	Clarification
Red Team and Blue Team Exercises	Red Team Operations (Red Teaming) Blue Team Operations (Blue Teaming) Purple Team Exercises Adversarial Simulation Tabletop Exercises Cyber Range Exercises Capture the Flag (CTF) Competitions Ethical Hacking Exercises Incident Response Drills	Red Team and Blue Team exercises are cyber security practices aimed at testing and improving an organisation's security posture through simulated adversarial attacks (Red Team) and defensive responses (Blue Team). Here's a more detailed technical definition for each: **Red Team Exercises (Red Teaming)**: • **Technical Definition**: Red Team exercises involve skilled cyber security professionals, known as Red Teamers, simulating real-world cyber attacks against an organization's systems, networks, and assets. The Red Team	**Red Team Exercises (Red Teaming)**: • Imagine a group of pretend bad guys (the Red Team) who try to sneak into a big fortress (your organisation's computer network). They use all sorts of tricks and tools to try and break through the fortress walls. • Their goal is to find weak spots in the fortress's defences. They might try to steal secret information, mess with

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		employs advanced techniques and tactics, similar to those used by actual threat actors, to identify and exploit security vulnerabilities, bypass security controls, and achieve specific objectives, such as gaining unauthorised access, stealing sensitive data, or disrupting operations. • **Objectives**: The primary objective of Red Team exercises is to assess the effectiveness of an organisation's security defences, detection capabilities, and incident response procedures by	important systems, or just cause chaos. • By pretending to be attackers, they help the fortress's defenders (the Blue Team) learn where they need to improve their defences. It's like a practice game where the bad guys test the good guys to make them stronger. **Blue Team Exercises (Blue Teaming)**: • Now, imagine the fortress has a team of guardians (the Blue Team) who are always on

Funded by The Scottish Government

		emulating the tactics, techniques, and procedures (TTPs) used by real-world adversaries. Red Team activities may include penetration testing, social engineering, phishing attacks, malware deployment, and physical security assessments. **Blue Team Exercises (Blue Teaming)**: • **Technical Definition**: Blue Team exercises involve cybersecurity defenders, known as Blue Teamers, responding to simulated cyber attacks initiated by the Red Team. The Blue	the lookout for trouble. When they hear the bad guys are coming, they spring into action. • The Blue Team watches for any signs that the bad guys are trying to break in. They use special tools and techniques to spot the tricks the bad guys are using. • If they catch the bad guys trying to sneak in, they jump in to stop them and fix any damage they've done. It's like a game of cat and mouse, but with

Funded by The Scottish Government

		Team is responsible for detecting, analysing, and mitigating security incidents, as well as implementing defensive measures to protect systems, networks, and data from compromise. Blue Teamers collaborate to identify indicators of compromise (IOCs), analyse attack patterns, and coordinate incident response efforts to contain and mitigate the impact of simulated attacks. • **Objectives**: The primary objective of Blue Team exercises is to assess the organization's ability to	computer systems. Overall, Red Team and Blue Team exercises are like a big game where one group pretends to be attackers trying to break in, while the other group pretends to be defenders trying to stop them. It's all about learning how to keep your computer systems safe from the bad guys by practicing what to do if they ever come knocking.

Funded by The Scottish Government

		detect, respond to, and recover from cyber attacks effectively. Blue Team activities may include network monitoring, log analysis, incident detection and response, malware analysis, forensic investigations, and security incident management. Together, Red Team and Blue Team exercises form a comprehensive approach to cyber security testing and training, enabling organisations to identify weaknesses, improve security controls, enhance incident response capabilities, and strengthen overall security resilience in the face of evolving	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		cyber threats. These exercises facilitate collaboration between offensive and defensive cyber security teams, promoting a proactive and adaptive approach to cyber security risk management.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

Capability	Also Known As	Definition	Clarification
Hacker	Cyber Intruder Cyber criminal Malicious Actor Security Threat Actor Black Hat Cracker Cyber Attacker Exploiter Intruder Digital Saboteur Threat actor	The term "hacker" has evolved over time and can have different meanings depending on context. In a technical sense, a hacker is an individual with advanced computer skills and knowledge who uses those skills to explore, modify, or exploit computer systems and networks. Here's a more detailed technical definition: **Technical Proficiency**: A hacker typically possesses advanced technical skills and expertise in various areas of computer science, including programming, networking, operating systems, and cyber security. **Exploration and Experimentation**: Hackers are curious by nature and often engage in exploration and experimentation with computer	Imagine a hacker as someone who's really good with computers. They're like the explorers of the digital world, always curious about how things work and what they can do. **Computer Whizzes**: Hackers are super smart when it comes to computers. They understand all the technical stuff, like coding, networks, and how different systems work together. **Curious Minds**: Like detectives, hackers are always investigating and experimenting with computer systems to see what they can

Funded by The Scottish Government
Scottish Government
Riaghaltas na h-Alba

		systems and networks to understand how they work and identify potential vulnerabilities or weaknesses. **Security Testing**: Some hackers use their skills for ethical purposes, such as security testing and vulnerability assessment, where they systematically identify, assess, and mitigate security risks in computer systems and networks. **Unauthorised Access**: In some cases, hackers may gain unauthorized access to computer systems or networks without permission, either for malicious purposes or to demonstrate security flaws and vulnerabilities. **Tool Development**: Hackers may develop or customize tools and software applications to assist in their exploration, analysis, or	find. They like to explore and figure out how things tick. **Playing by Their Own Rules**: Some hackers use their skills to help make computers safer. They're the good guys, finding and fixing problems before the bad guys can exploit them. **Ethical vs. Unethical**: But not all hackers are good guys. Some use their skills to break into computers or networks without permission. These are the bad guys, like the burglars of the digital world. Overall, hackers are the adventurers of the digital age, using their computer skills to explore, discover, and sometimes cause trouble in

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba

		exploitation of computer systems and networks. **Ethical Considerations**: The term "hacker" is often associated with both ethical and unethical behaviour, and it's essential to distinguish between "white hat" hackers (ethical hackers who use their skills for constructive purposes, such as security testing and research) and "black hat" hackers (malicious hackers who engage in illegal or unethical activities, such as unauthorised access, data theft, or system manipulation). Overall, the technical definition of a hacker encompasses individuals with advanced computer skills and knowledge who explore, experiment with, and sometimes exploit computer systems and networks for various purposes, including	the vast landscape of cyber space.

Funded by The Scottish Government

		security testing, research, or unauthorised access.	

Funded by The Scottish Government

Scottish Government
Riaghaltas na h-Alba