CERTIFIED CYBER COP

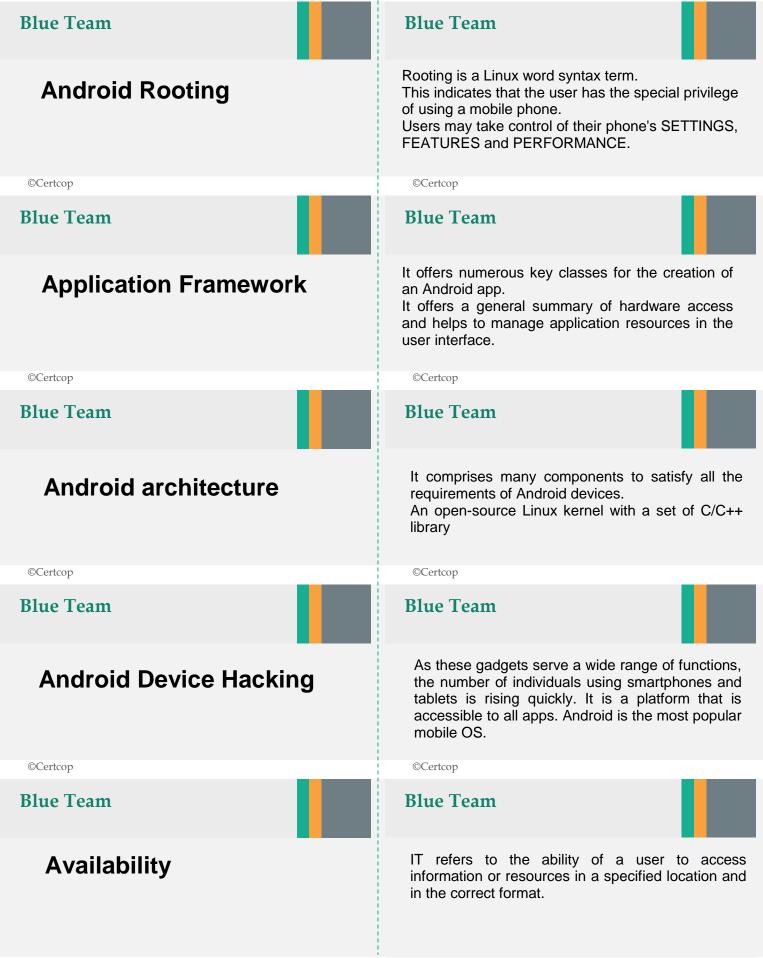
57

Blue Team Certcop CertTips

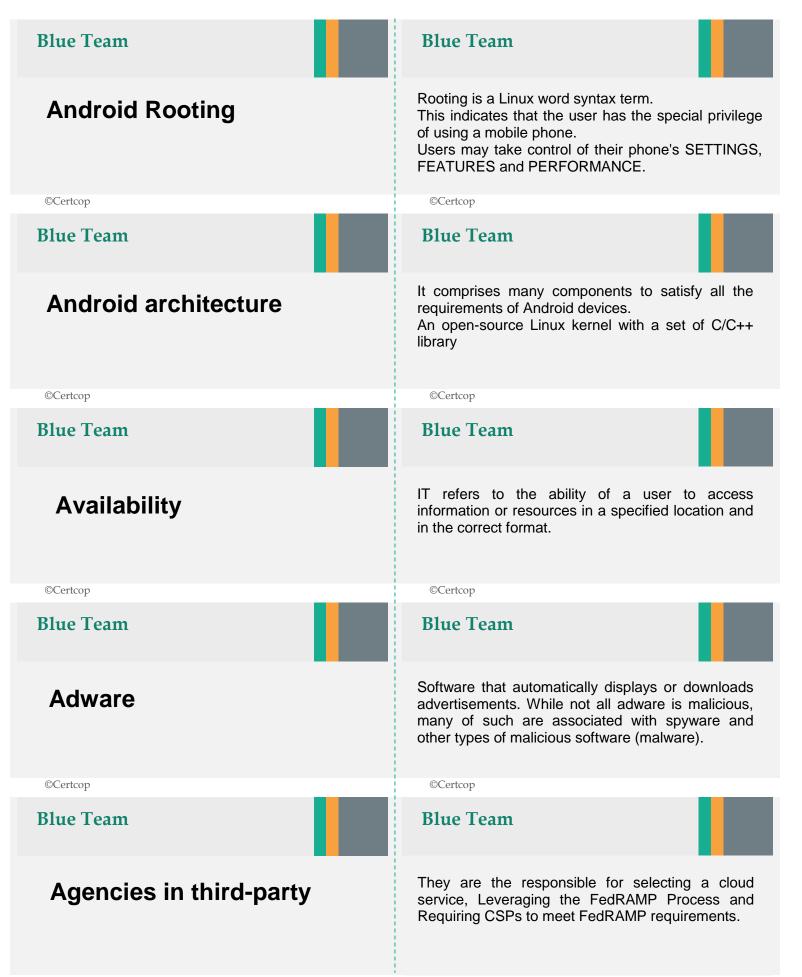
www.Certcop.com

Copyrights @ 2022 Certcop, All rights reserved





Blue Team	Blue Team
Android OS	The Android operating system is a Google mobile operating system. Its design allows users to intuitively use mobile devices, Google uses Android software also with a distinct user experience for TVs, automobiles and wristwatches.
©Certcop	©Certcop
Blue Team	Blue Team
Android OS Architecture	Android architecture comprises many components to satisfy all the requirements of Android devices. An open-source Linux kernel with a set of C/C++ library.
©Certcop	©Certcop
Blue Team	Blue Team
Active Network Threats	An active attack is one in which an attempt is made to make unauthorized changes to the system. Modifications to transmitted or stored data, as well as the formation of new data.
©Certcop	©Certcop
Blue Team	Blue Team
Application-level filtering	Email filters and web proxies are examples of application level filters. These act as proxies for one or more services.
©Certcop	©Certcop
Blue Team	Blue Team
Anomaly Detection	These systems that look for unusual changes in behaviour patterns to detect uncatalogued attacks.



Awareness and Training (AT) in security control

©Certcop

Blue Team

Audit and Accountability (AU)

©Certcop

Blue Team

Access Control (AC)

©Certcop

Blue Team

Asset Inventory

©Certcop

Blue Team

Asset management systems

Blue Team



Employees are educated about the cyber security landscape through Security Awareness Training. Security Awareness Training uses a variety of learning methodologies to help raise awareness of cyber security dangers, lower the risks associated with cyber-attacks, and cement a security compliance culture in your organization.

©Certcop

Blue Team



The Audit and Accountability (AU) objective's goal is to make sure there are enough controls in place to give auditable evidence for system transactions and that key records are kept for a long enough time.

©Certcop

Blue Team



The selective restriction of access to a place or other resource is known as access control (AC), while the process is known as access management. Consuming, entering, or using are all words that can be used to describe the process of accessing. Authorization is the process of gaining access to a resource.

©Certcop

Blue Team



It is critical to understand where information is stored in order to protect it. The physical and logical components must be included in the asset inventory. For each piece, it should describe the location, business processes

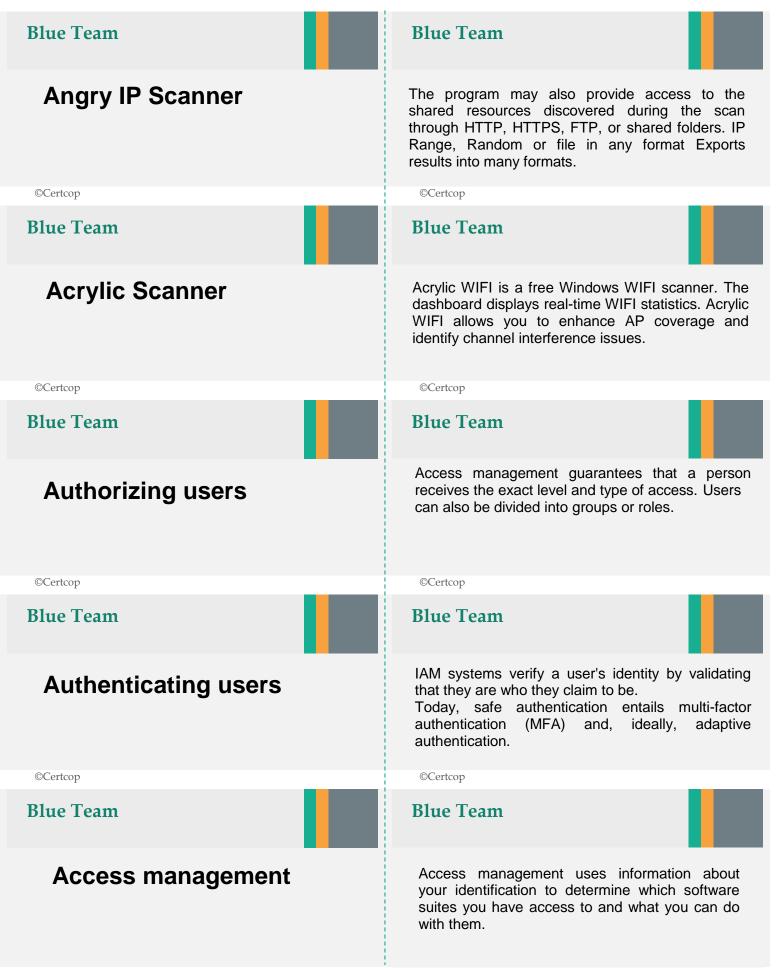
©Certcop

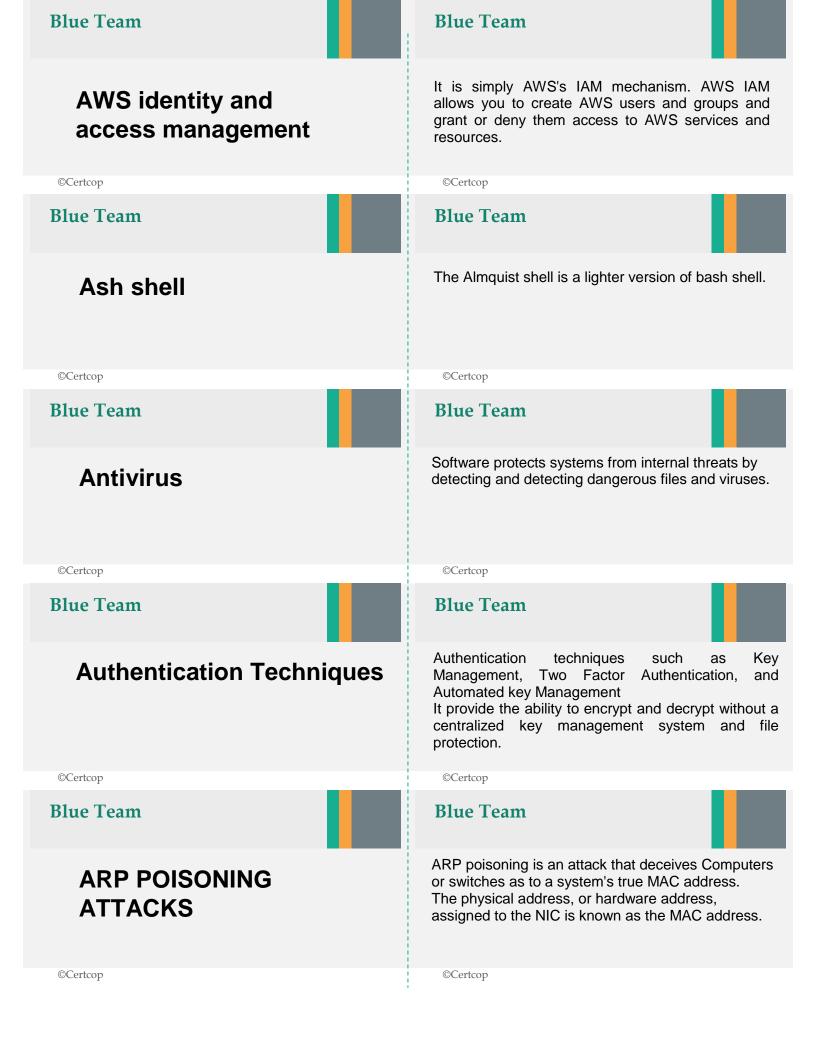
Blue Team

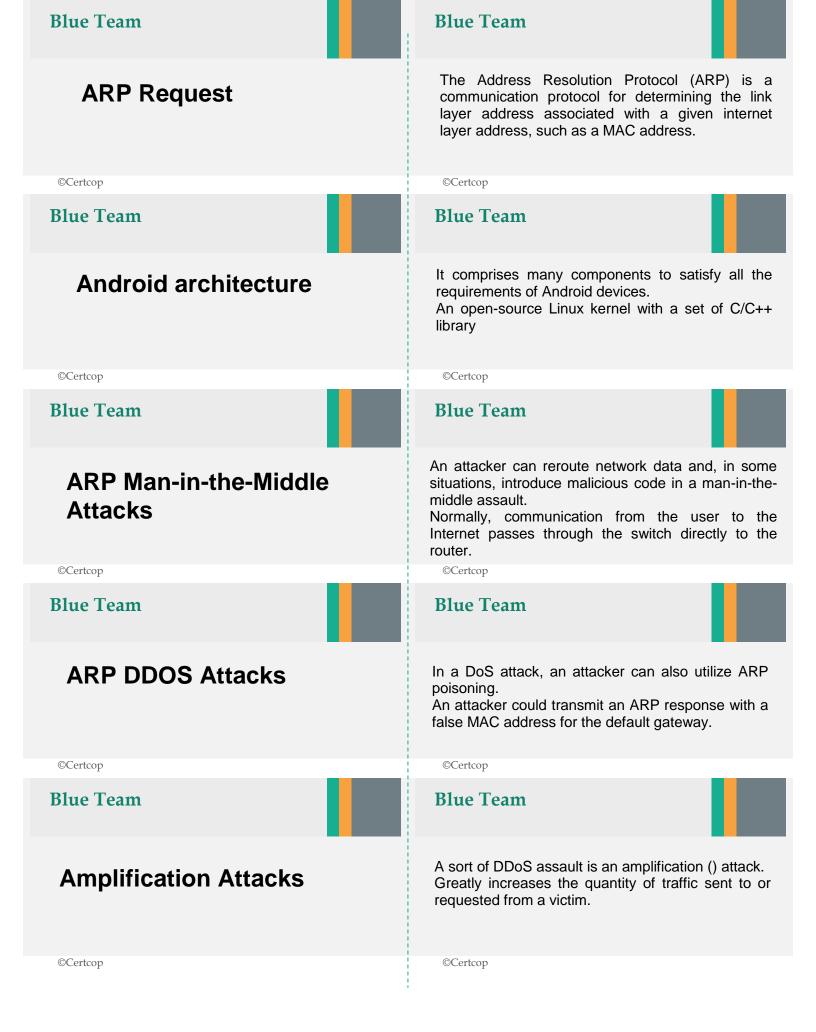


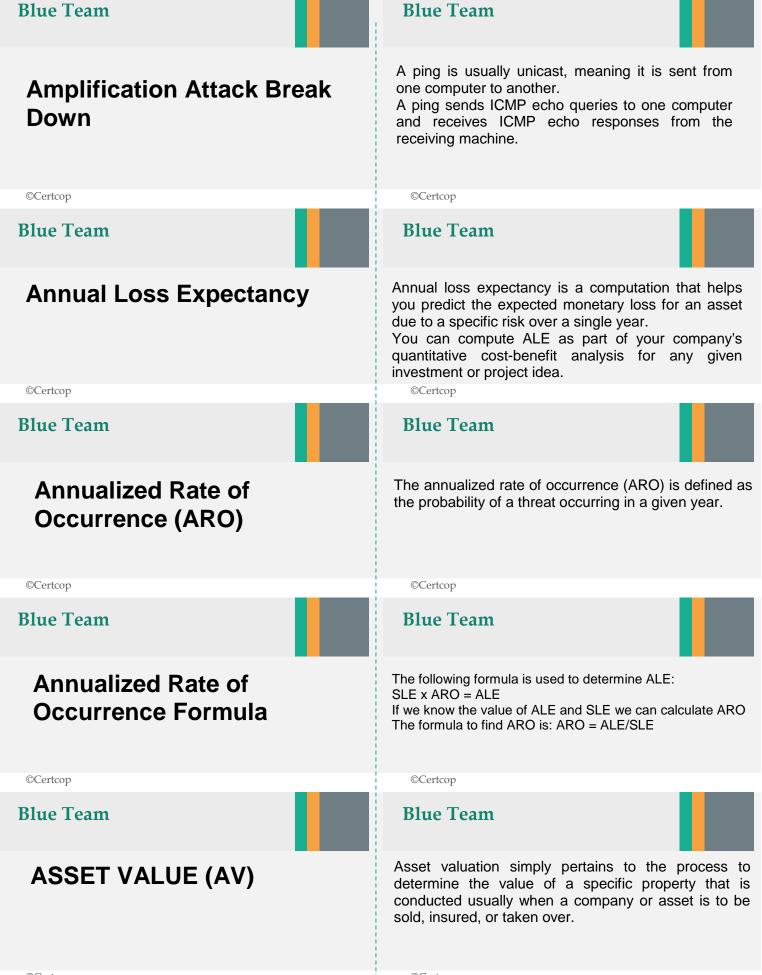
The Asset Management System (AMS) is a collection of tools and procedures for establishing asset management policies and objectives.

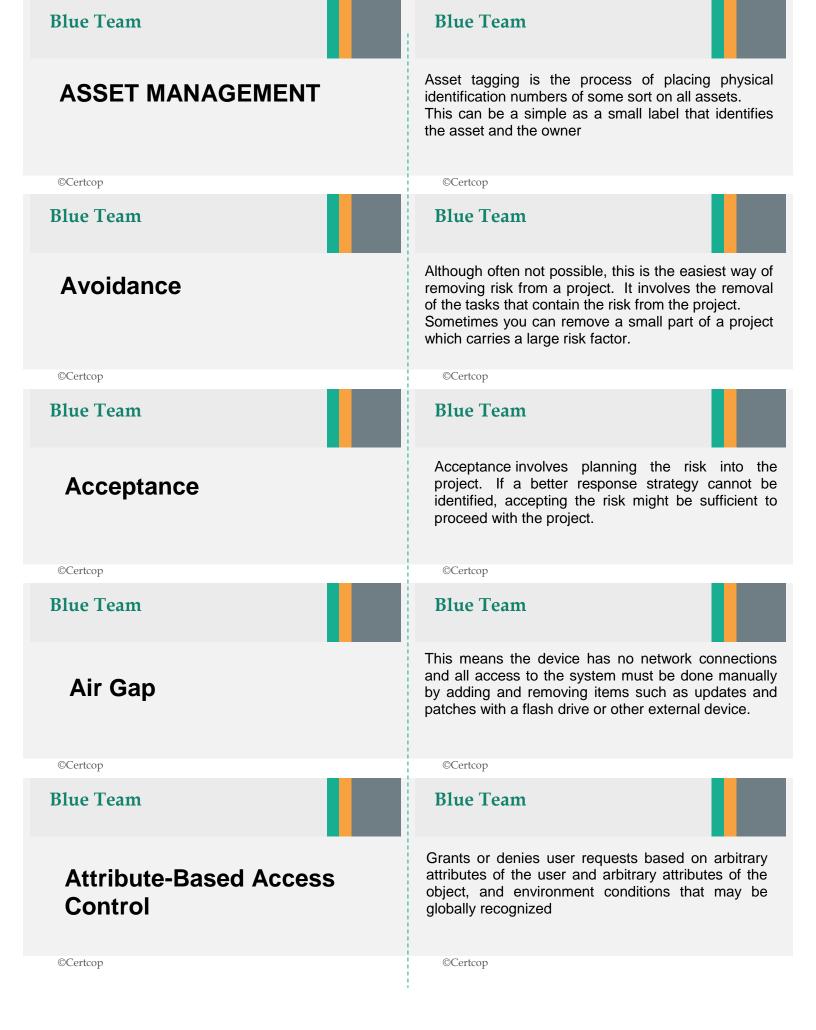


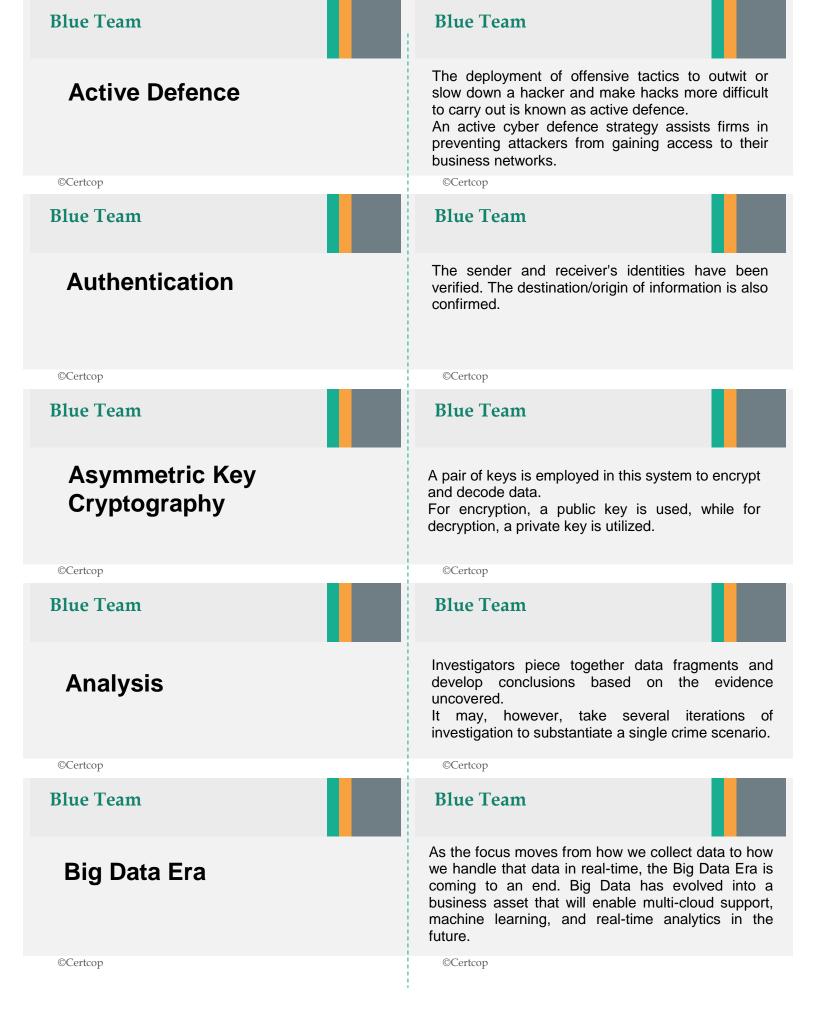








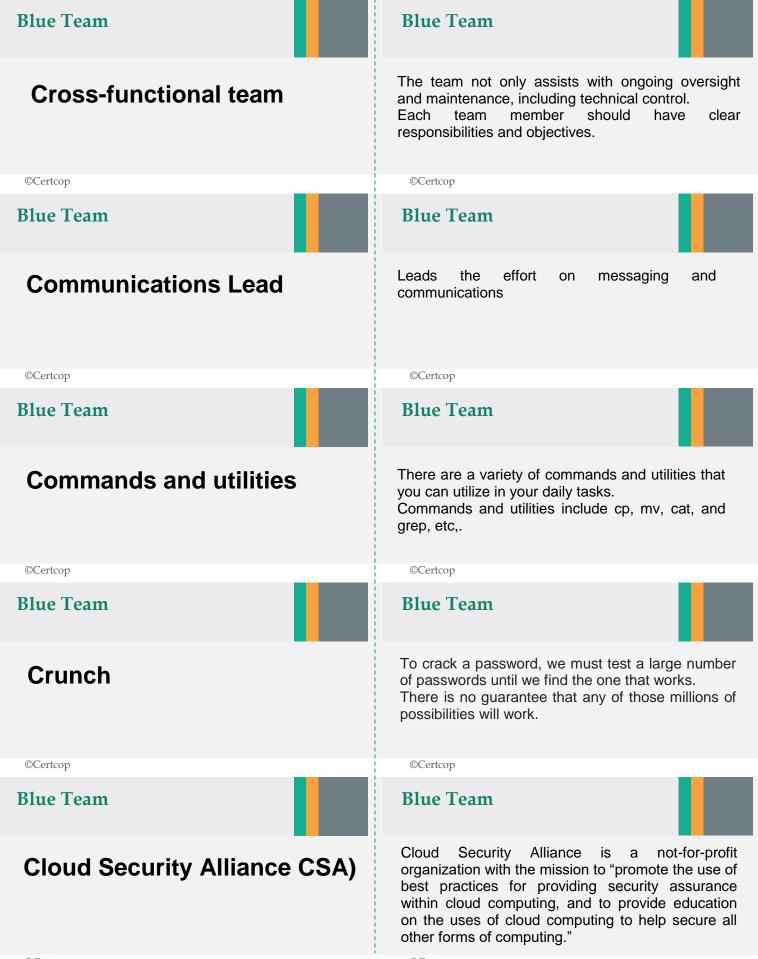






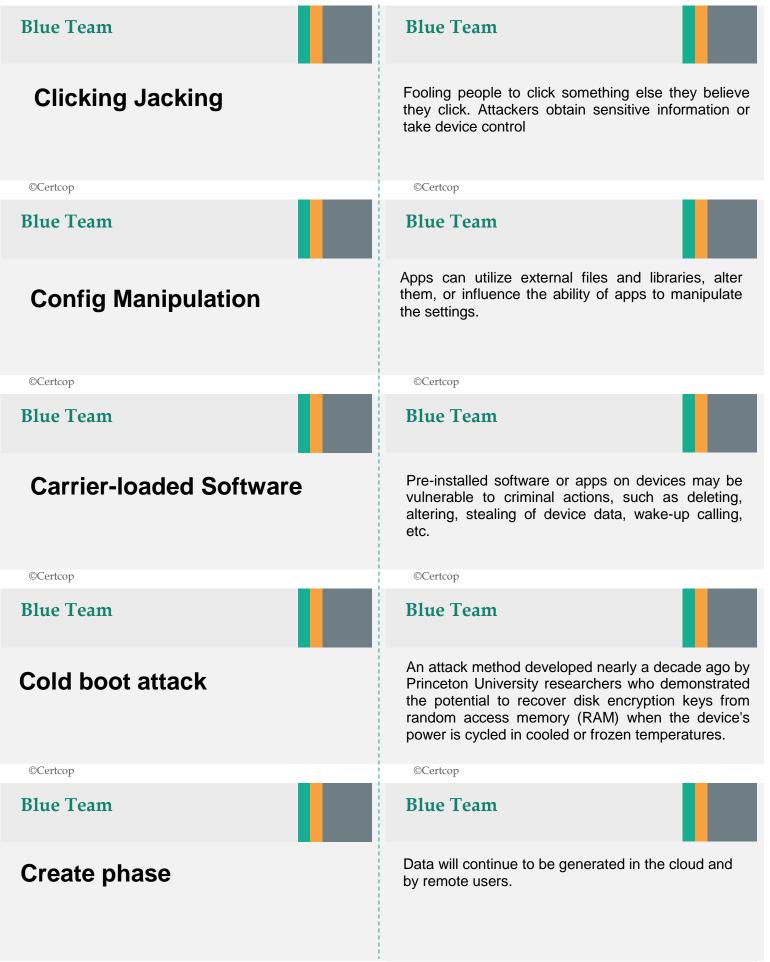


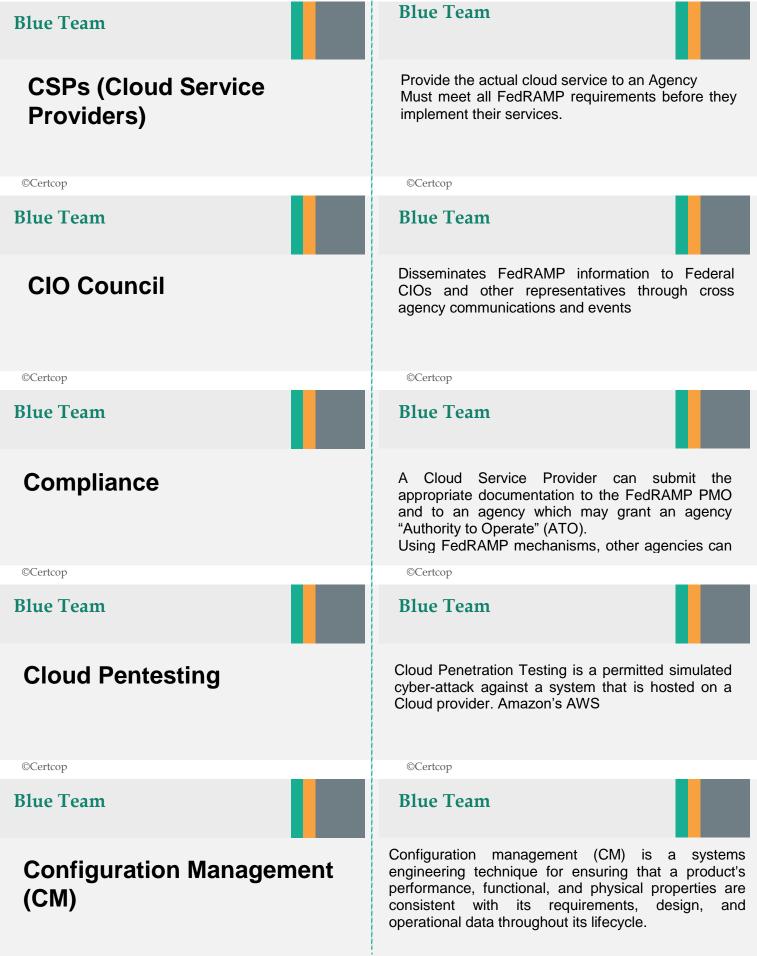
Blue Team	Blue Team
Birthday Attack	A birthday attack is a form of cryptographic attack that takes advantage of the probability theory mathematics underpinning the birthday problem. This assault can be used to manipulate two or more parties' communication.
©Certcop	©Certcop
Blue Team	Blue Team
Buffer Overflow	When an application receives more or different input than it expected, a buffer overflow occurs. As a result of the error, system memory that would normally be protected and inaccessible is exposed.
©Certcop	©Certcop
Blue Team	Blue Team
Blanket Purchase Agreement (BPA)	A Blanket Purchase Agreement (BPA) is a simplified method of filling anticipated repetitive needs for supplies or services by establishing "charge accounts" with qualified contractors.
©Certcop	©Certcop
Blue Team	Blue Team
Computer Forensics	Data from personal computers, laptops, and storage computing devices is collected, identified, preserved, and analyzed in computer forensics. Computer forensics experts are usually involved in investigations of computer crimes, although their services are also required in civil lawsuits and the data recovery process.
©Certcop	©Certcop
Blue Team	Blue Team
Cloud Carrier	A cloud carrier serves as an intermediary between cloud consumers and cloud providers, providing connectivity and transfer of cloud services.

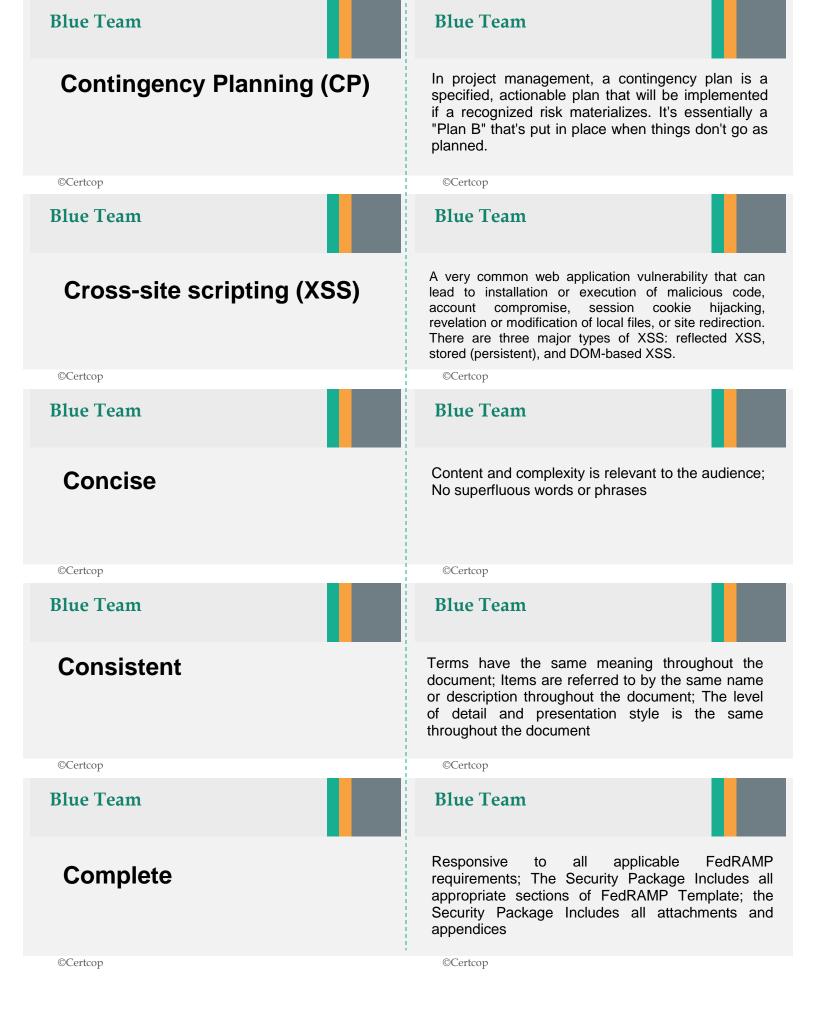


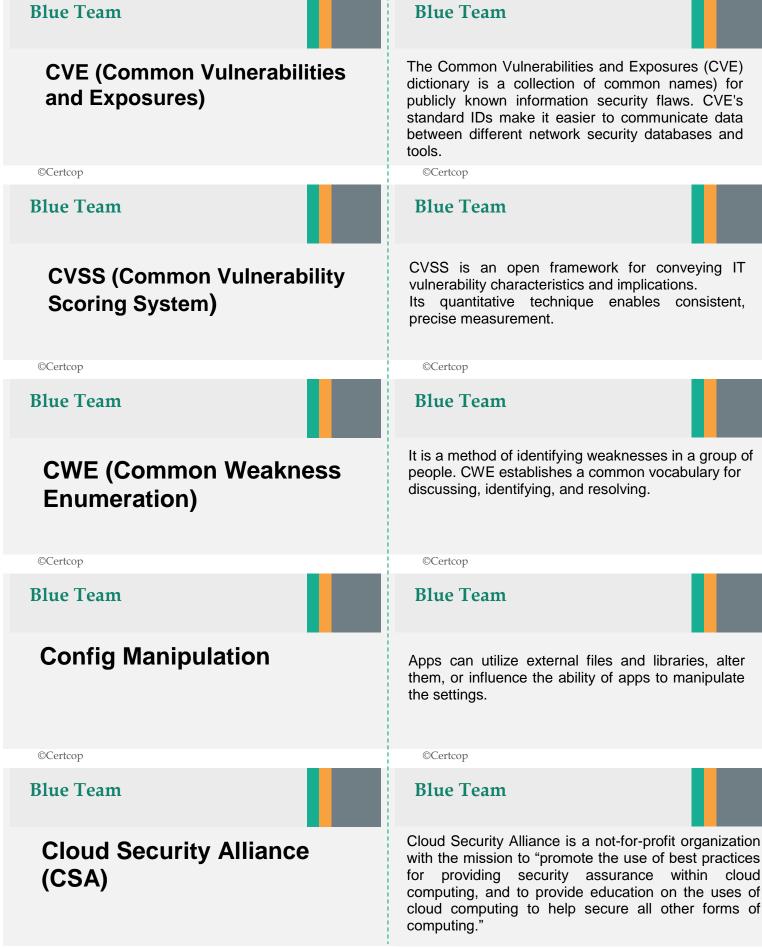
©Certcop

Blue Team	Blue Team
Creating a File	The touch command is used to create empty files. We can create multiple empty files by executing it once. Command : Touch <file name=""></file>
©Certcop	©Certcop
Blue Team	Blue Team
Changing Permissions	To change the file or the directory permissions, you use the chmod (change mode) command. Each permission is assigned a value, as the following table shows, and the total of each set of permissions provides a number for that set.
©Certcop	©Certcop
Blue Team	Blue Team
Changing Owners and Groups	While creating an account on Unix, it assigns a owner ID and a group ID to each user. All the permissions mentioned above are also assigned based on the Owner and the Groups.
©Certcop	©Certcop
Blue Team	Blue Team
chown	The chown command stands for "change owner" and is used to change the owner of a file.
©Certcop	©Certcop
Blue Team	Blue Team
chgrp	The chgrp command stands for "change group" and is used to change the group of a file.
©Certcop	©Certcop









©Certcop

Blue Team

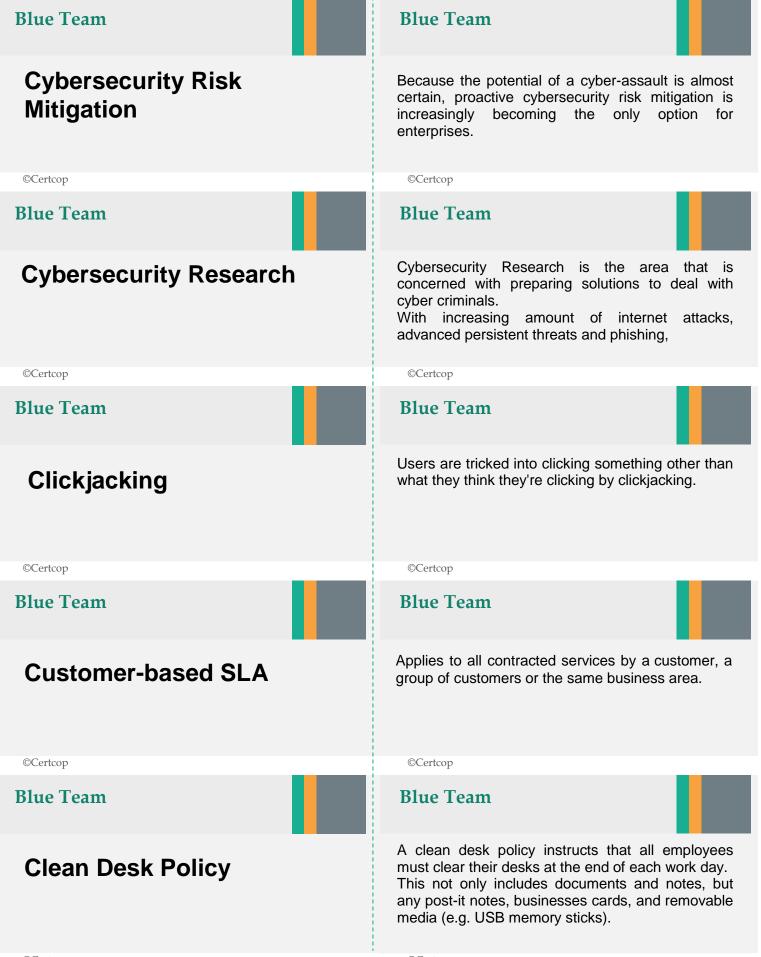
Conduct Root Cause Analyses

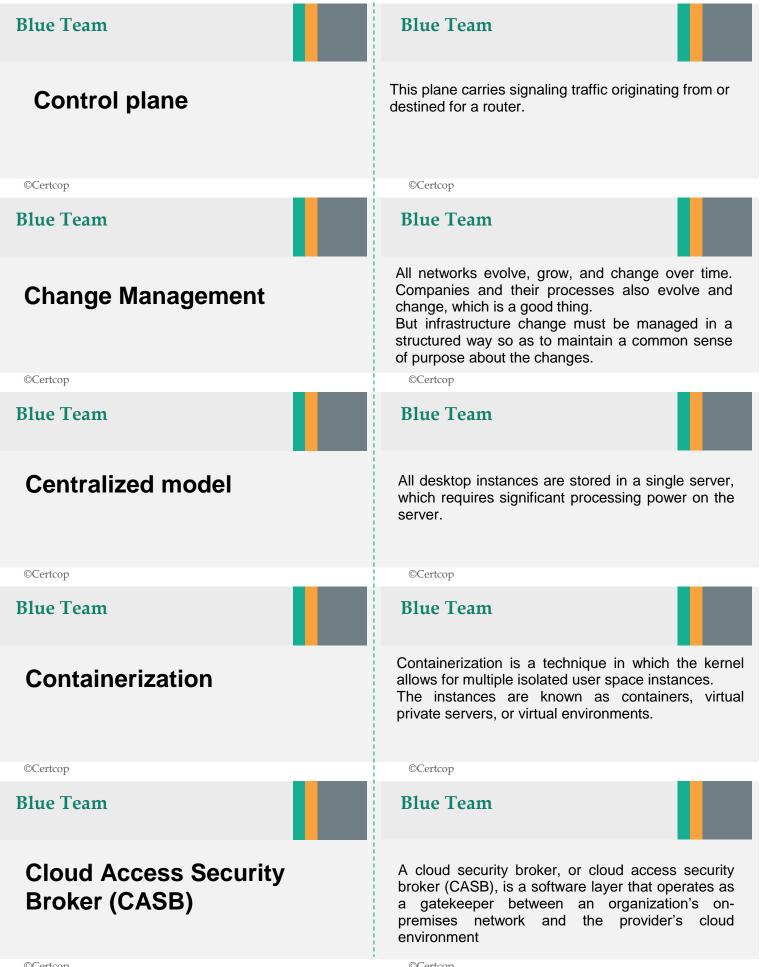
Blue Team

temporary fixes.

Spend more time searching for root causes of equipment failures instead of engaging in

©Certcop	©Certcop
Blue Team	Blue Team
Condition-Based Maintenance (CBM)	This maintenance strategy uses technology-based diagnostics—vibrations, temperature, pressure, speed,
©Certcop	©Certcop
Blue Team	Blue Team
Central identity management	IAM takes place in a single environment with centralized identity management. In a professional environment, this would entail a person logging into a single workspace to gain access to all of the programs and tools they require.
©Certcop	©Certcop
Blue Team	Blue Team
C shell	The C shell was developed by Bill Joy for the Berkeley Software Distribution Its syntax is modelled after the C programming language.
©Certcop	©Certcop
Blue Team	Blue Team
Controlling Jobs	Job control is a command shell capability that allows many commands to be run and managed from a single shell instance. A parent shell forks a child process to run a command without job control, sleeping until the child
	process terminates.

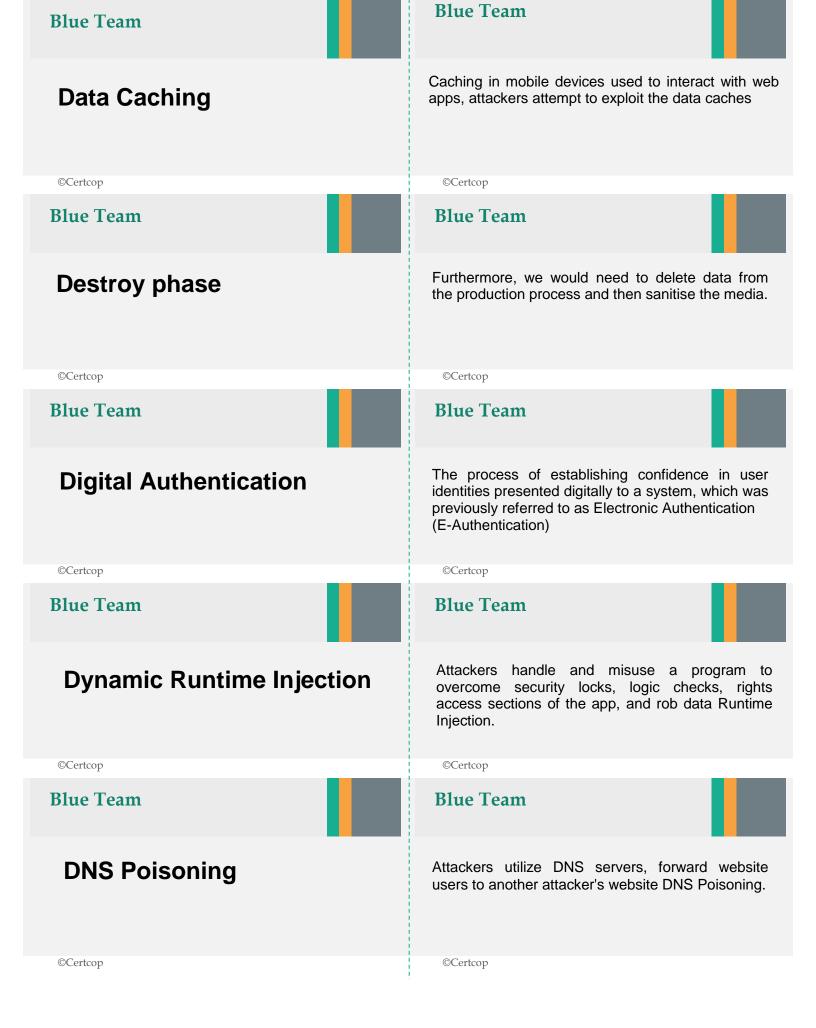




©Certcop

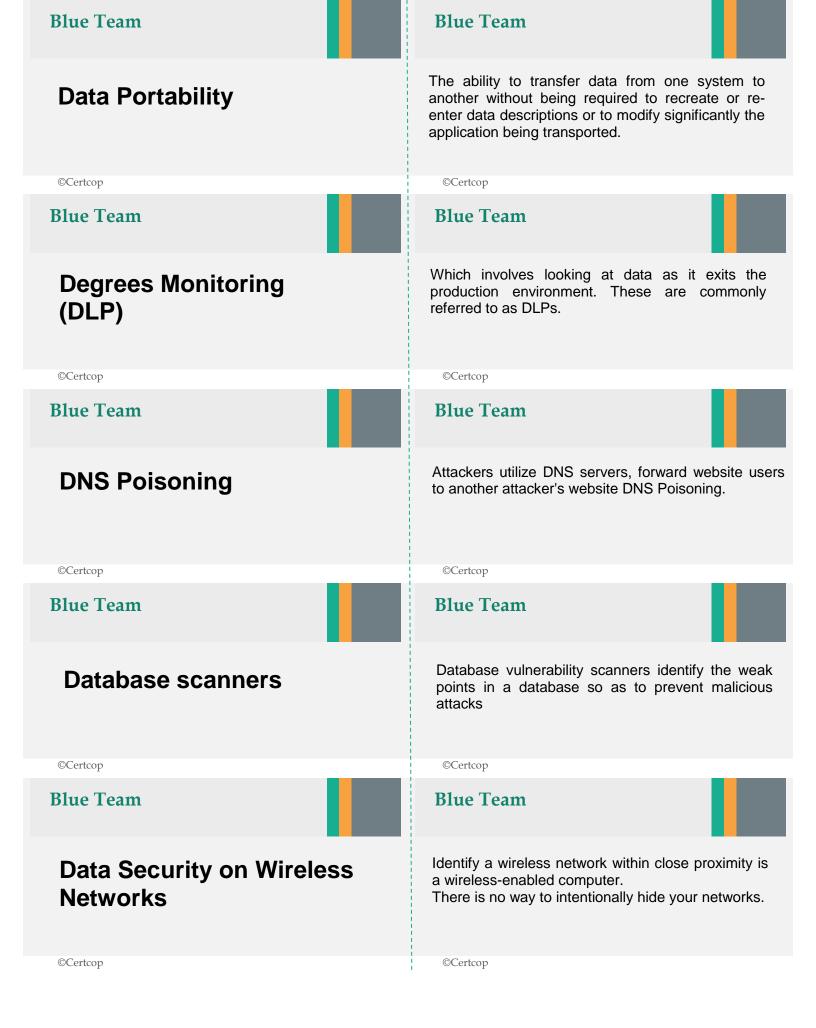






Blue Team	Blue Team
Data Centers	A data center is a physical location where businesses keep their mission-critical programs and data. The design of a data center is built on a network of computer and storage resources that allow shared applications and data to be delivered.
©Certcop	©Certcop
Blue Team	Blue Team
Data Dumping	A memory dump (sometimes called a core dump or system dump) is a snapshot of computer memory data taken at a certain point in time. A memory dump can contain important forensic information about the condition of the system prior to an
©Certcop	©Certcop
Blue Team	Blue Team
Dr.Fone	Dr. Fone was the first company in the world to offer iOS and Android data recovery software, and it has saved a lot of people. With over a decade of expertise providing top-rated software and services to individuals,
©Certcop	©Certcop
Blue Team	Blue Team
Denial-of-Service	Denial-of-Service (DoS) attacks prevent a company or organization from using its own resources. In a typical DoS attack, the culprit floods the target network with invalid authentication requests or pings.
©Certcop	©Certcop
Blue Team	Blue Team
Database models	Describes relationships between data elements Used to represent the conceptual organization of data Formal methods of representing information
©Certcop	©Certcop

Blue Team	Blue Team
Distributed Database models	Client-server type of DB located on more than one server distributed in several locations Synchronization accomplished via a two-phase commit or replication methods.
©Certcop	©Certcop
Blue Team	Blue Team
Data dictionary	A Data Dictionary is a list of names, definitions, and properties for data elements in a database, information system, or research project.
©Certcop	©Certcop
Blue Team	Blue Team
Data Marts	Often regional collection of information from databases.
©Certcop	©Certcop
Blue Team	Blue Team
Data Warehouse	A data warehouse is a sort of data management system that is intended to facilitate and assist business intelligence (BI) and analytics activities. Data warehouses are designed mainly for querying and analysis, and they frequently store vast
©Certcop	©Certcop
Blue Team	Blue Team
Data mining	Data mining is a technique for extracting and detecting patterns in huge data sets that combines machine learning, statistics, and database systems.
©Certcop	©Certcop
*	*



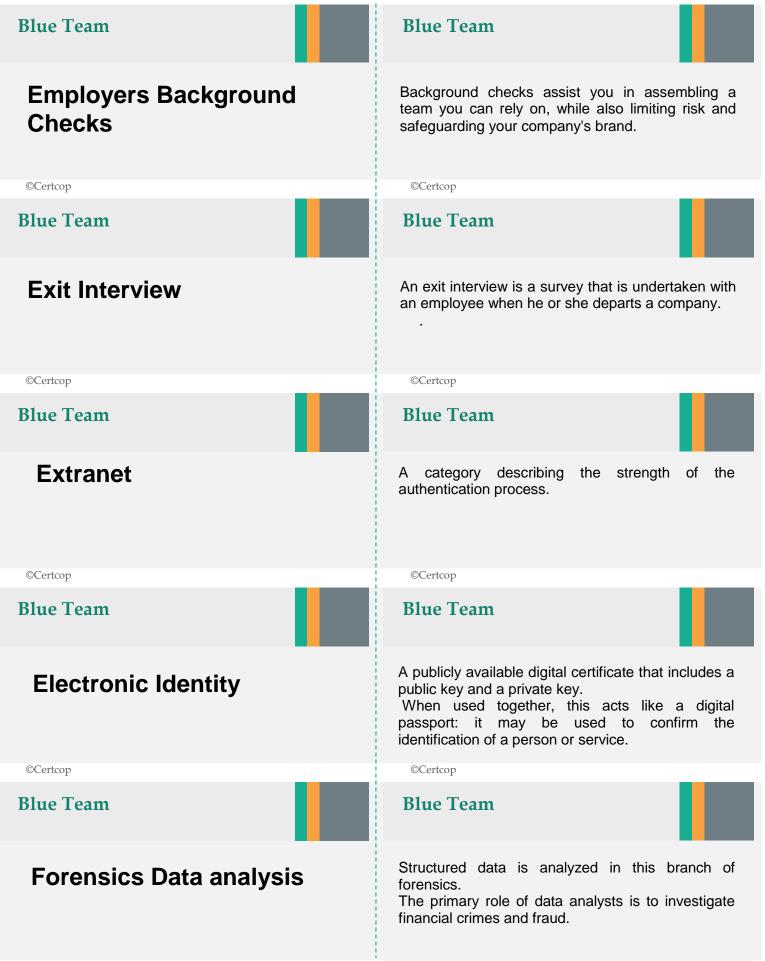


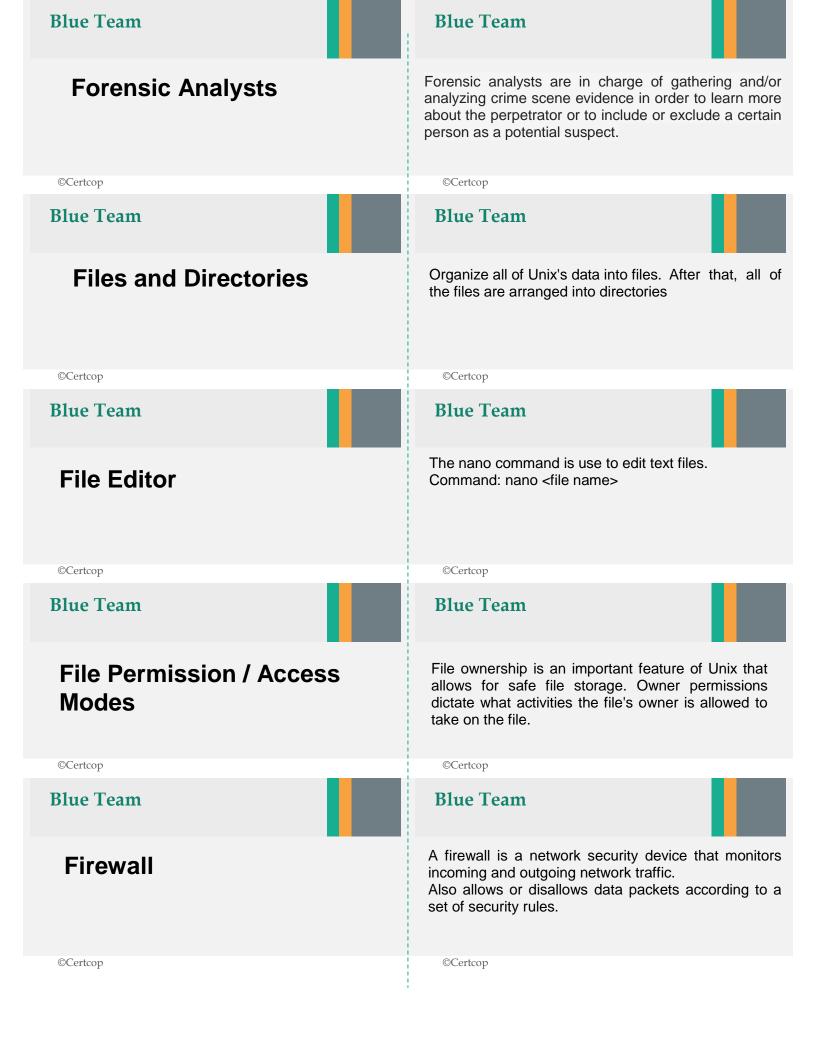


Blue Team	Blue Team
DLL Injection	A DLL is a compiled set of code that may be used by a program without having to recreate it. Most programming languages, for example, include math-based DLLs.
©Certcop	©Certcop
Blue Team	Blue Team
Data Ownership Policy	The act of holding legal rights and total control over a single piece or set of data pieces is referred to as data ownership. It establishes and gives information on the legitimate owner of data assets, as well as the data owner's acquisition, use, and distribution policies.
©Certcop	©Certcop
Blue Team	Blue Team
Data plane	Also known as the forwarding plane, this plane carries user traffic.
©Certcop	©Certcop
Blue Team	Blue Team
Data Security	Throughout its lifecycle, data security refers to the process of securing data from illegal access and data corruption. Data encryption, hashing, tokenization, and key management are all data security strategies that safeguard data across all applications and platforms.
©Certcop	©Certcop
Blue Team	Blue Team
Dissemination	Intelligence and Security Informatics has more information. This refers to the active dissemination and dissemination of all types of information to the users or audiences that deserve it.
©Certcop	©Certcop
	1 Contraction of the second

Blue Team Blue Team A digital certificate is a file that contains a variety of **Digital Certificate** data, including identifying information, a serial number, and expiration dates. It also contains the digital signature of the certificate authority that issued the certificate. ©Certcop ©Certcop **Blue Team Blue Team** Analysts that specialize in email forensics extract **Email Forensics** valuable information from emails. Senders and receivers, the content of the messages, time stamps, sources, and metadata are all examples of this information. ©Certcop ©Certcop **Blue Team Blue Team** Evasi0n7 is an iPhone, iPod touch, iPad, and iPad Evasi0n7 mini devices running iOS 7.0 to 7.0.6 is suitable as a junk tool (Devices that have been updated Over the Air [OTA] should be restored with iTunes first). ©Certcop ©Certcop **Blue Team Blue Team** When it comes to tracing the attacker and **Evidence Collection** comprehending the attack's procedure, evidence collecting is important. As a result, incident responders should know where to look for evidence and how to gather it. ©Certcop ©Certcop **Blue Team Blue Team Escalated privileges** Attackers engage in escalation privilege assaults that take advantage of design flaws, programming mistakes, bugs, etc.

Blue Team **Blue Team** Electricity The movement of electrical power or charge is referred to as electricity. Electricity can be generated using renewable or non-renewable energy sources, yet electricity is neither renewable nor nonrenewable. ©Certcop ©Certcop **Blue Team Blue Team** Eavesdropping attacks are comparable to sniffing Eavesdropping attacks, but they're usually more passive, easier to conduct out. An attacker listens to data travelling between networks in order to obtain private information. ©Certcop ©Certcop **Blue Team Blue Team Eavesdropping attacks** Involve a weaker link between the client and the server, allowing the attacking entity to transfer network traffic to itself. Tools used to carry out these attacks include Wireshark, tcpdump, and Ettercap. ©Certcop ©Certcop **Blue Team Blue Team** Encoding data to hide it from anyone who isn't Encryption authorized to see it. A decryption key can be used to access or decrypt encrypted data. ©Certcop ©Certcop **Blue Team Blue Team** Attackers obtain a wireless access point and **Evil Twin** configure it to function as the current network. One of the simplest methods to prevent evil twins from stealing your organization's information is to use data encryption.

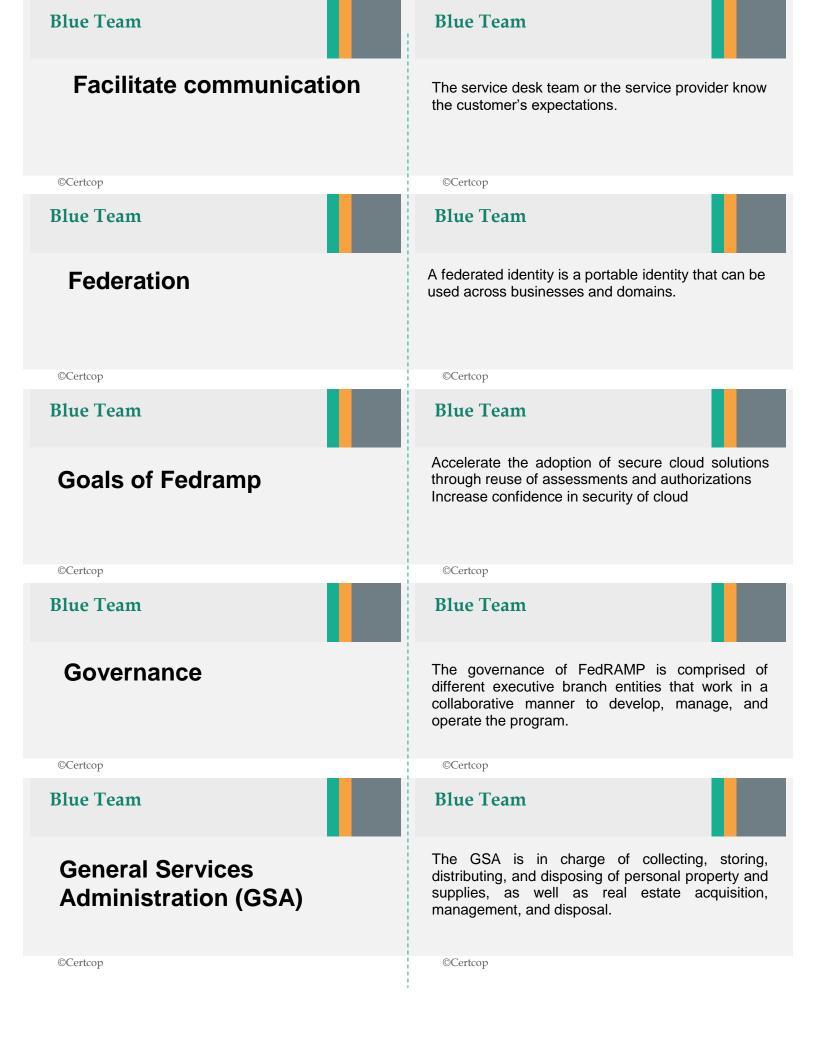


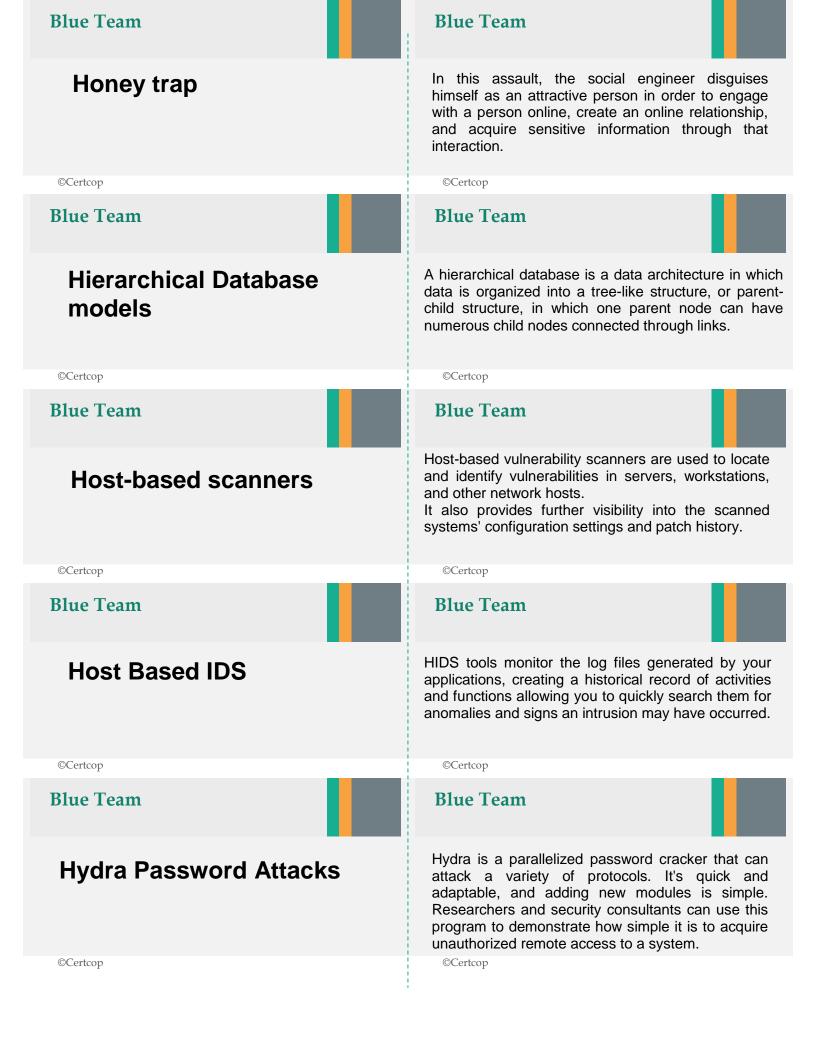


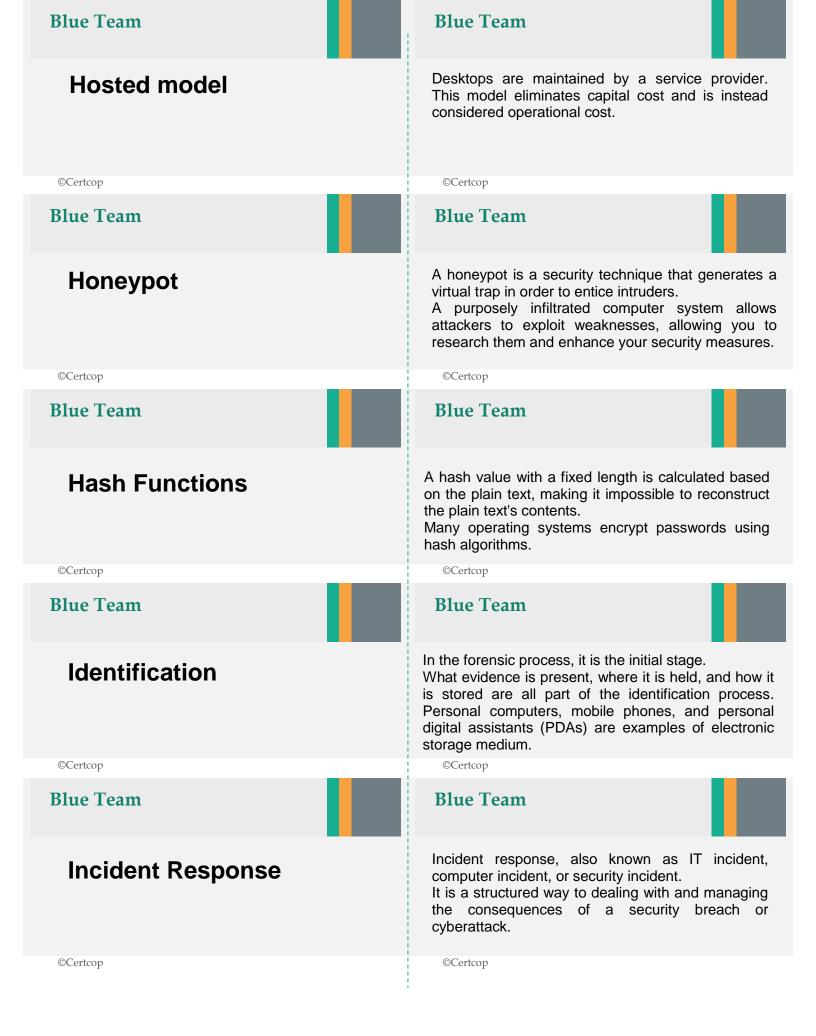


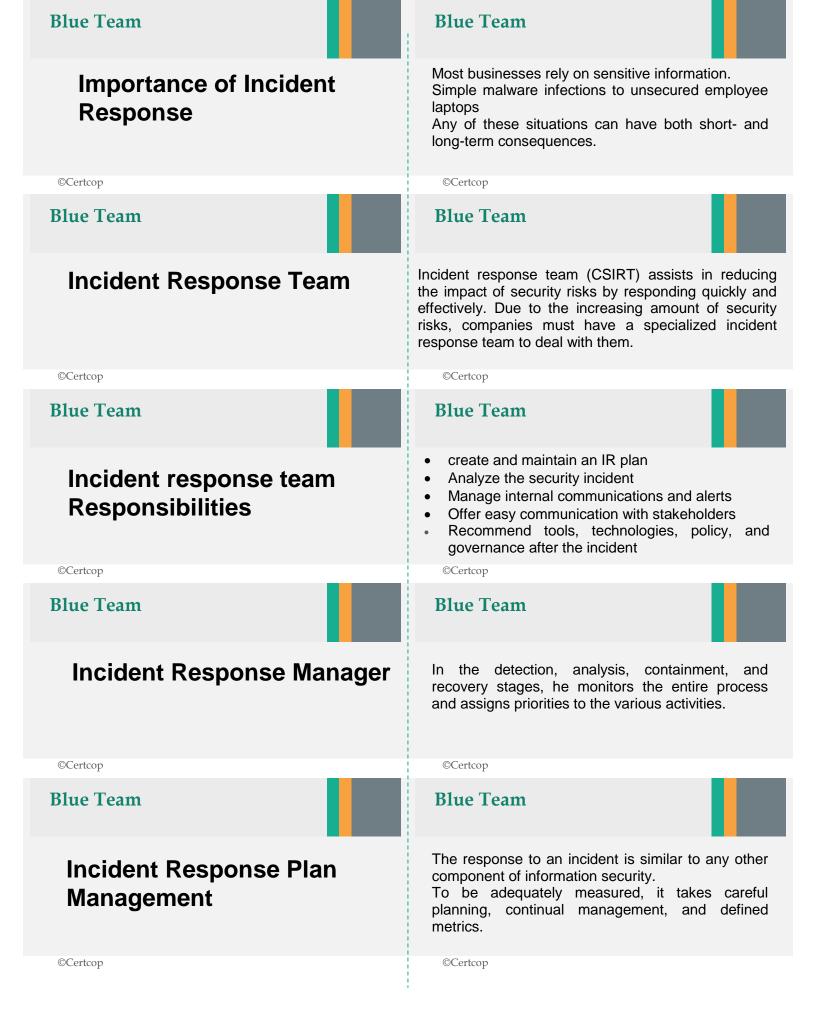
Blue Team	Blue Team
Foreign Keys	Foreign keys are structured as a shared component in a database that connects two tables. A foreign key must always relate to another primary key.
©Certcop	©Certcop
Blue Team	Blue Team
File	A file is a computer object that holds data, information, settings, or commands that are utilized with a software.
©Certcop	©Certcop
Blue Team	Blue Team
Fedramp	It is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
©Certcop	©Certcop
Blue Team	Blue Team
Fedramp Needed	The Federal Government spends hundreds of millions of dollars a year securing the use of IT systems Cloud solutions allow for faster processing
©Certcop	©Certcop
Blue Team	Blue Team
FedRAMP Program Management Office	Established within the GSA and responsible for the development of the FedRAMP program.
©Certcop	©Certcop
	•

Blue Team	Blue Team
FIPS 199	FIPS 199 mandates that federal agencies evaluate their information systems in terms of confidentiality, integrity, and availability, assigning a low, moderate, or high impact rating to each system in each category.
©Certcop	©Certcop
Blue Team	Blue Team
FedRAMP Assignments	The assignments are also documented in the "Parameter" sections of the Control Summary Information following the requirements. When multiple requirements are presented as in the case with AC-2 objective (f)
©Certcop	©Certcop
Blue Team	Blue Team
Factors that can affect RPO	Maximum tolerable data loss for the specific organization, Industry-specific factors—businesses dealing with sensitive information such as financial transactions or health records must update more often, Data storage options, such as physical files versus cloud storage, can affect speed of recovery,
©Certcop	©Certcop
Blue Team	Blue Team
Fish shell	This friendly interactive shell was written from scratch and isn't derived from any of the other shell families. It's intended to be user friendly. Amongst its many other perks, fish offers suggestions for commands based on your history and the contents of the current folder, similar to predictive text.
©Certcop	©Certcop
Blue Team	Blue Team
Foreground Processes	They run on the screen and require user input. For example Office Programs
©Certcop	©Certcop

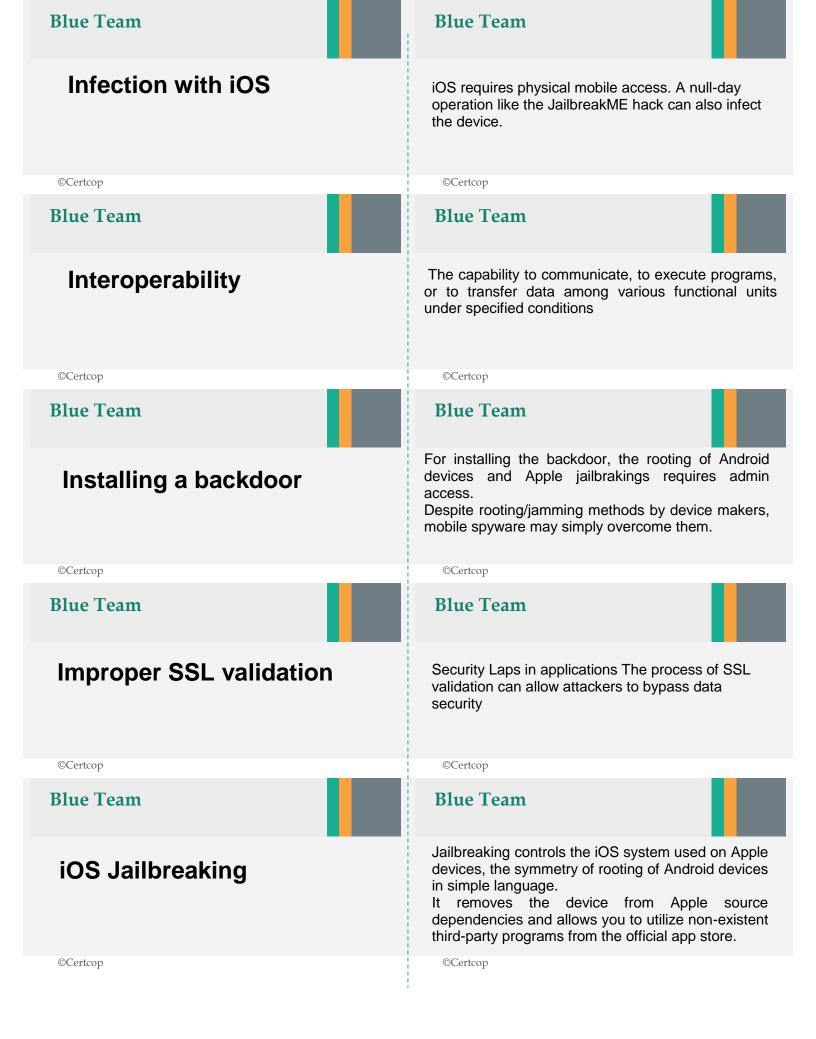




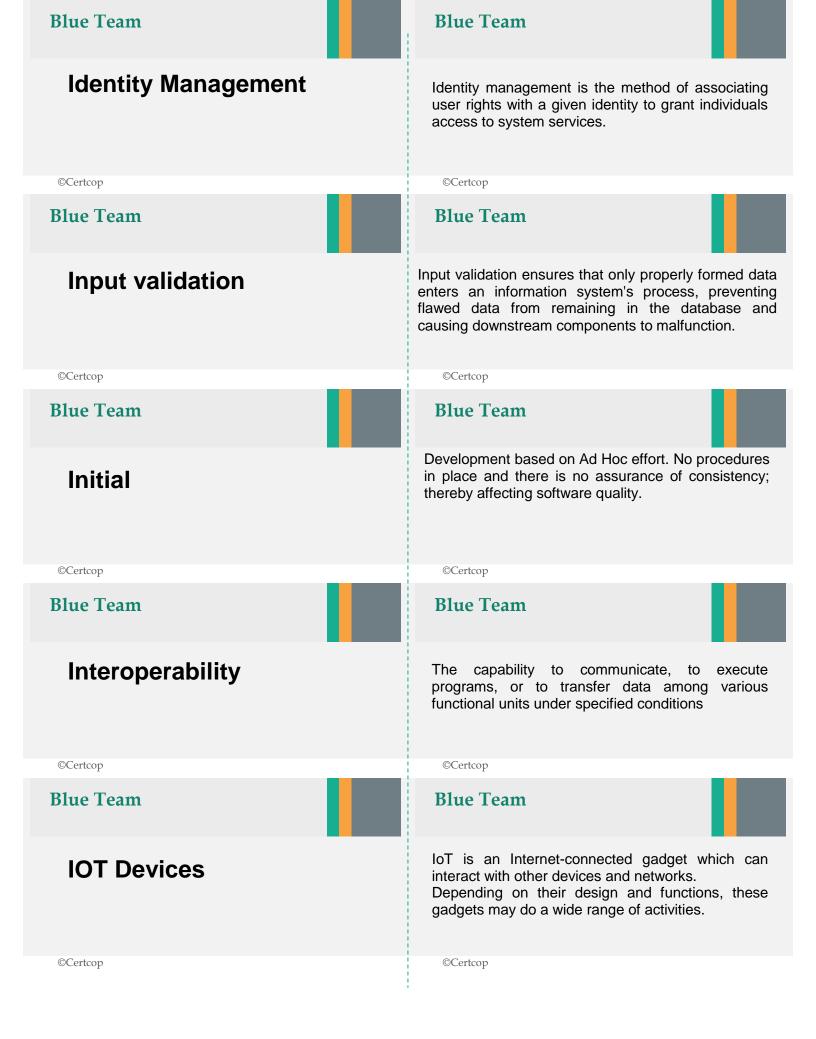


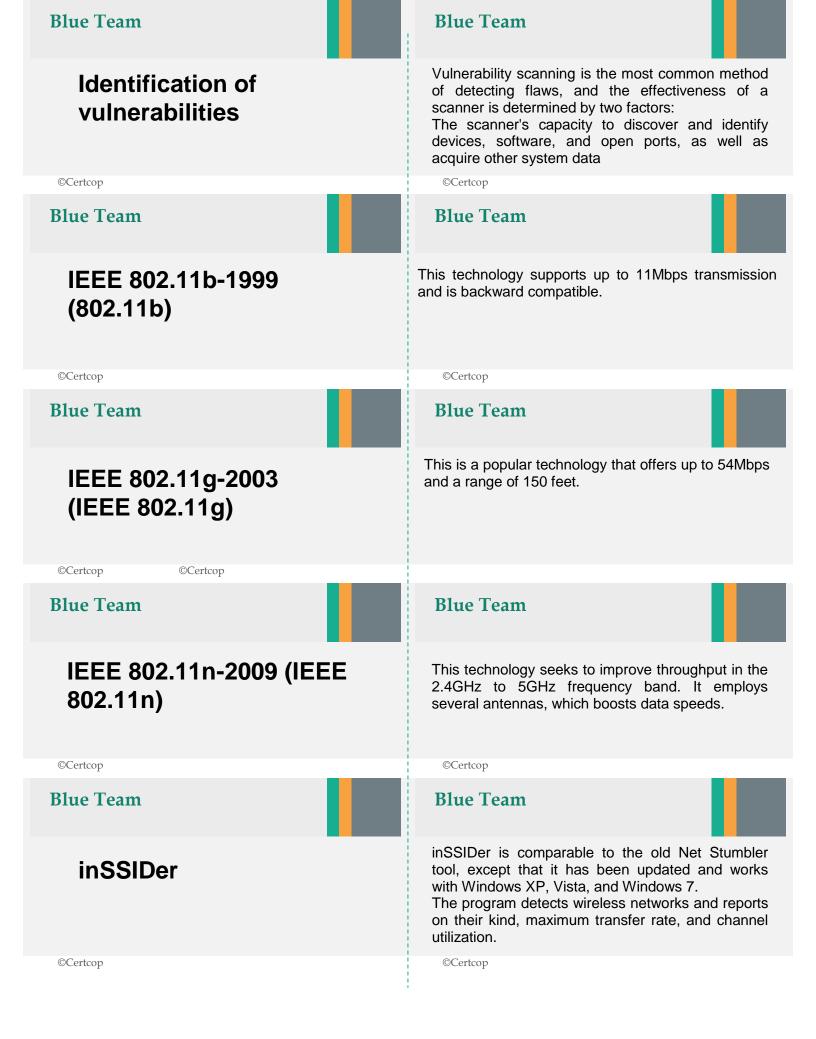




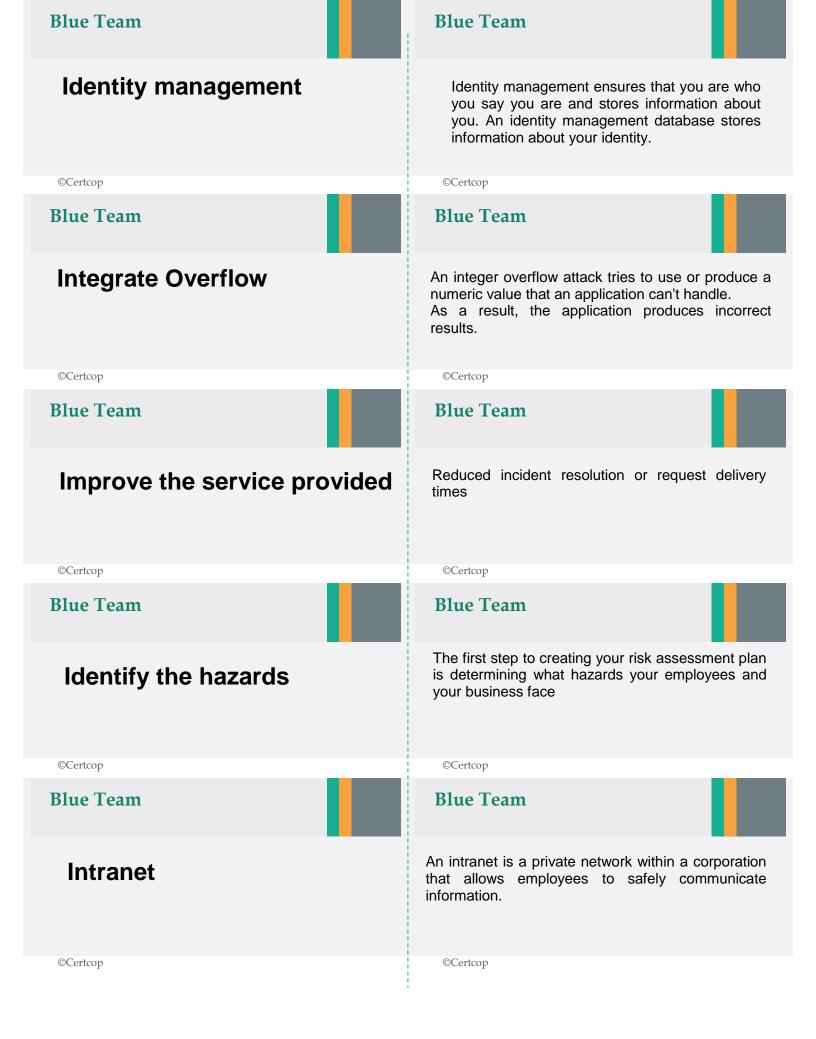


Blue Team	Blue Team
IRoot	Like Root Genius, iRoot has been built by Chinese folks for another strong root program. You can manage your Android phone or tablet only one click away.
©Certcop	©Certcop
Blue Team	Blue Team
los Device Hacking	Mobile Apple's operating system iOS operates devices including the iPhone, iPad and iPod Touch. Originally called the iPhone OS, with the launch of the iPad, the moniker was changed to iOS. The iPad has had a different OS
©Certcop	©Certcop
Blue Team	Blue Team
iBoot Exploit	A jailbreak iBoot permits access to the file system and level iboot. If a fresh boot-rom is in place, this sort of exploit can be semi-tethered.
©Certcop Blue Team	©Certcop Blue Team
	It poor of the network for indicators of communic
Intrusion detection	It search the network for indicators of compromise or an ongoing attack and alert the user if malicious behavior is discovered. Monitoring and detecting when a threshold is crossed is the most popular intrusion detection approach.
Certcop	an ongoing attack and alert the user if malicious behavior is discovered. Monitoring and detecting when a threshold is crossed is the most popular intrusion detection
	an ongoing attack and alert the user if malicious behavior is discovered. Monitoring and detecting when a threshold is crossed is the most popular intrusion detection approach.
©Certcop	an ongoing attack and alert the user if malicious behavior is discovered. Monitoring and detecting when a threshold is crossed is the most popular intrusion detection approach. ©Certcop



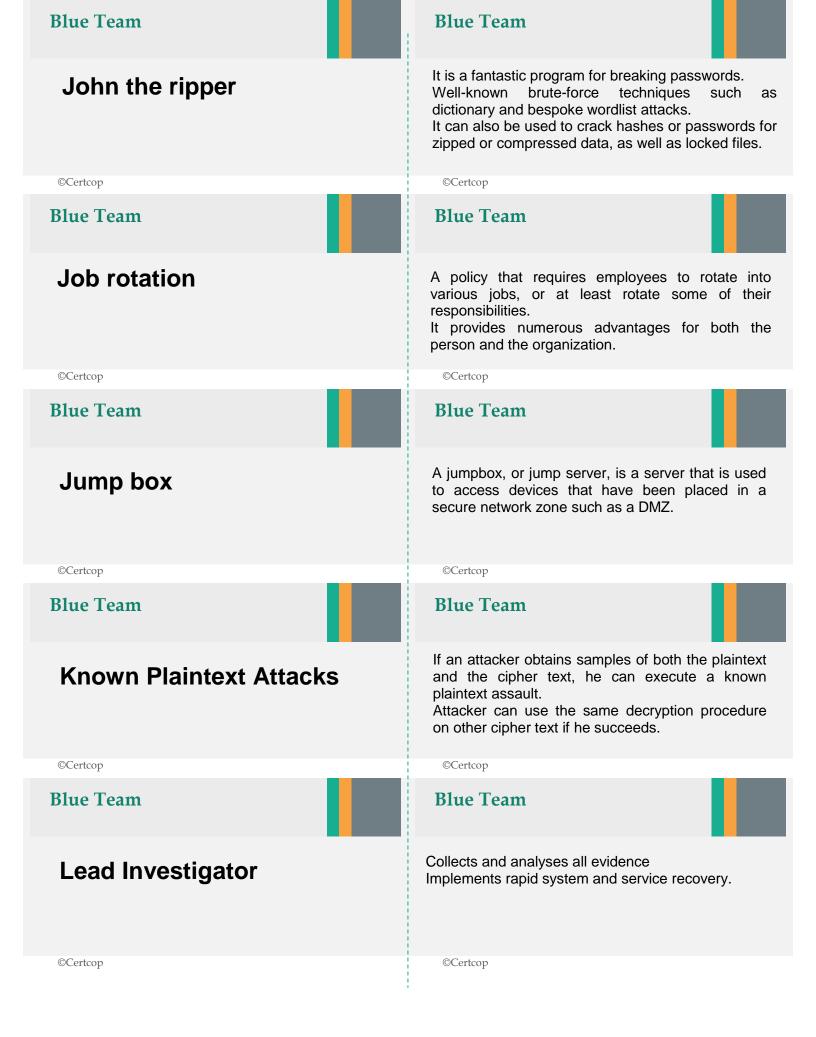




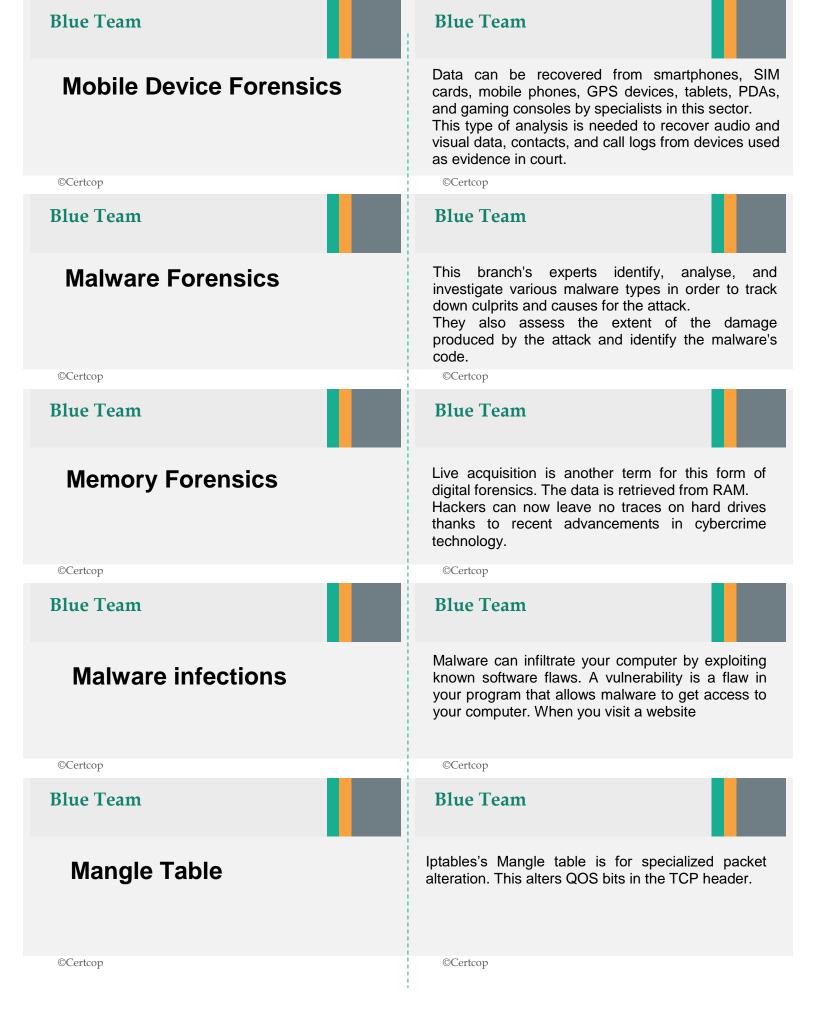


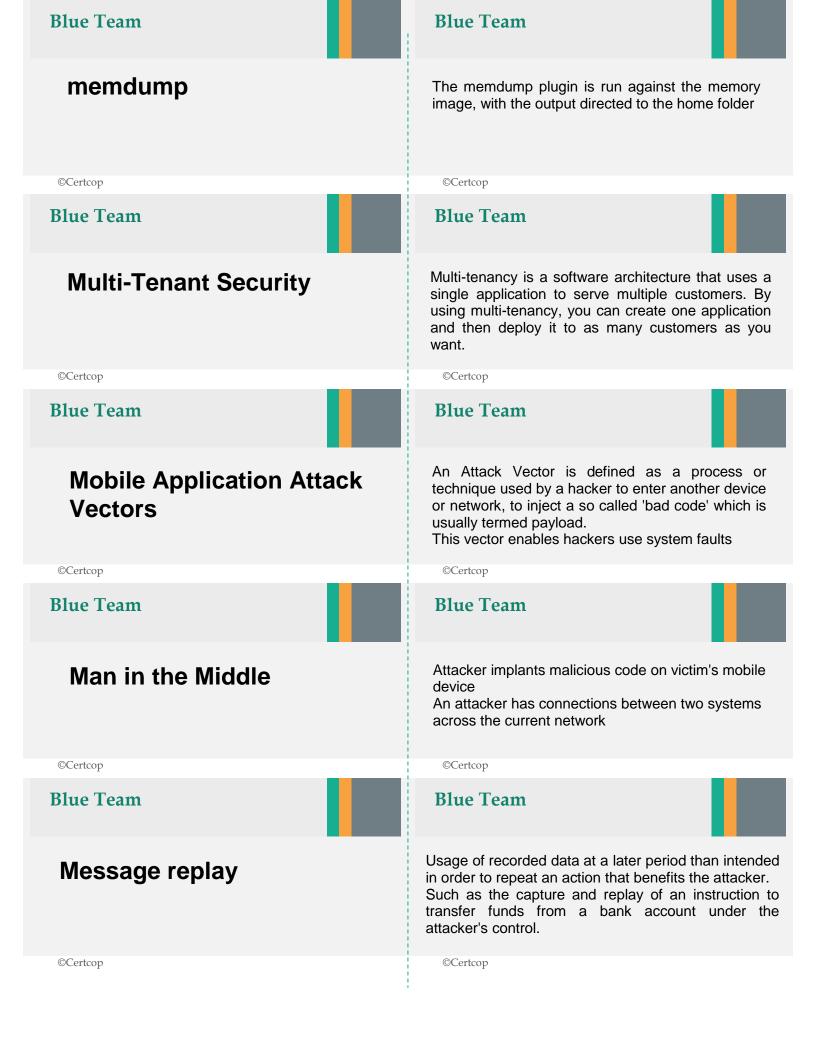
Blue I eam	Blue Team
Identity and Access Management	Ensuring the right people and job responsibilities (identities) in a company have access to the resources they need to execute their duties Identity and access management solutions allow your organization to manage a variety of identities, such as people, software, and hardware.
©Certcop	©Certcop
Blue Team	Blue Team
Integrity	Information cannot be updated in storage or during the transfer between the sender and the intended receiver without any modification to the information being detected.
©Certcop	©Certcop
Blue Team	Blue Team
Jump Bag- Forensic Toolkit	Response times should be as short as feasible when an issue occurs. As a result of every minute that passes, a danger artifact is lost, or the attackers cause additional harm.
©Certcop	©Certcop
Blue Team	Blue Team
Jump Bag	Response times should be as short as feasible when an issue occurs. As a result of every minute that passes, a danger artifact is lost, or the attackers cause additional harm.
©Certcop	©Certcop
Blue Team	Blue Team
Jamming	The goal of jamming (also known as network interference) is to interrupt the network. Interference is almost unavoidable due to the wireless characteristics.
©Certcop	

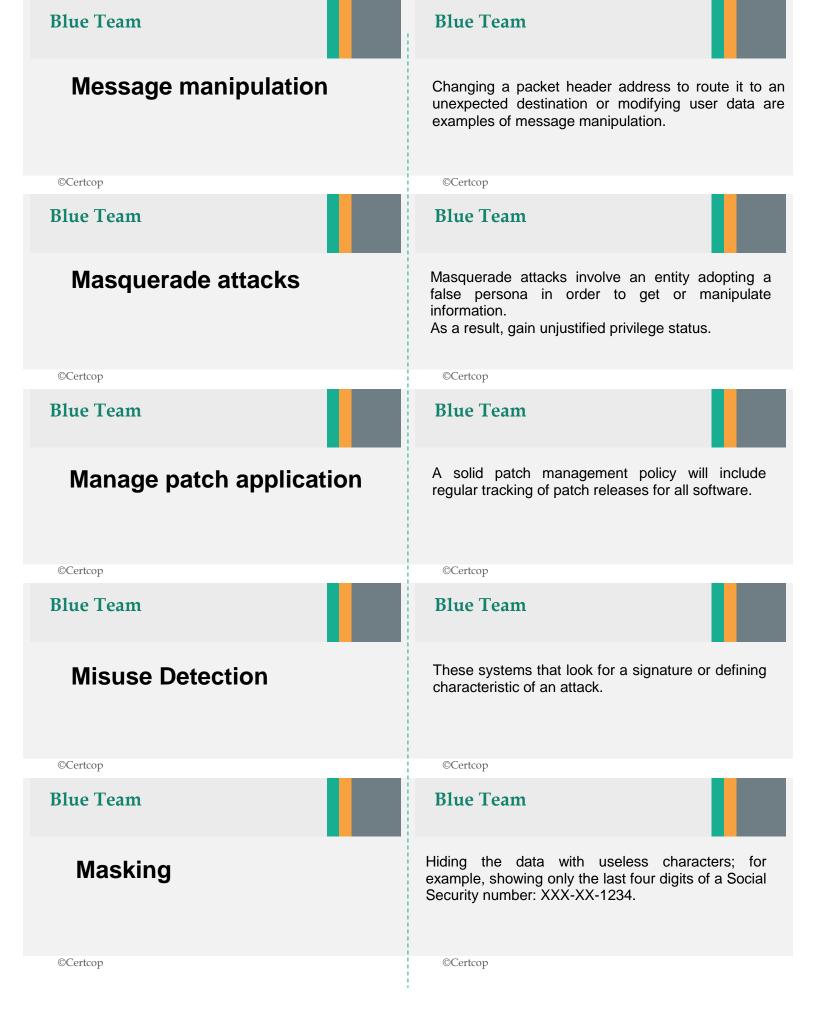
-



Blue Team	Blue Team
LINUX+ ©Certcop	The UNIX operating system is a collection of applications that serve as a conduit between the user and the computer. Kernel is a set of computer programs that distribute system resources and coordinate all aspects of the computer's internals.
Blue Team	Blue Team
ls	You can use the Is command to list out all the files or directories available in a directory. Command: Is
©Certcop	©Certcop
Blue Team	Blue Team
Linux Kernel	The core of the Android architecture is Linux Kernel. It manages all drivers accessible, such as Display controls, Camera ports, etc.
©Certcop	©Certcop
Blue Team	Blue Team
Leveraging and Authorization	Shows the architecture, including the domain architecture, with the existing domain hierarchy, names, and addressing scheme; server roles; and trust relationships.
©Certcop	©Certcop
Blue Team	Blue Team
Logical deployment diagram	The process or action of confirming an identity used to interact with or log in to an information system.
©Certcop	©Certcop







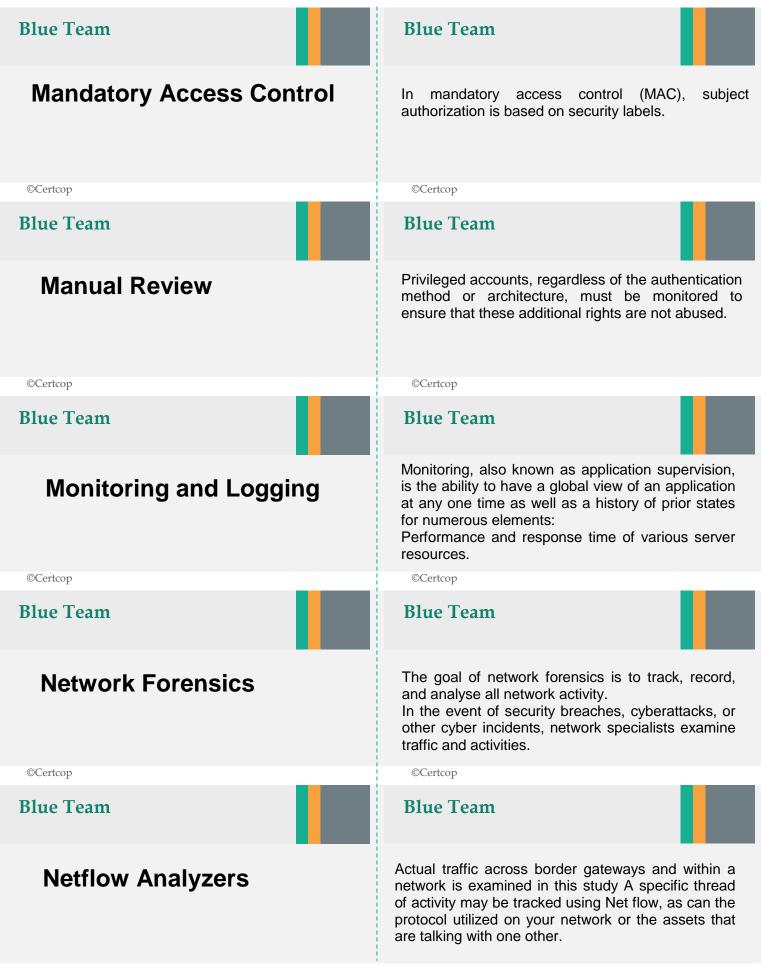
Blue Team	Blue Team
Metadata	"Data about data" gives the data its meaning/context
©Certcop	©Certcop
Blue Team	Blue Team
Mobile Device Security	Mobile Device Security refers to the safeguards put in place to protect sensitive data kept on and transferred by laptops, smart phones, tablets, wearable's, and other portable devices.
©Certcop	©Certcop
Blue Team	Blue Team
Monitoring and Reporting	Discovering and monitoring the virtual resources, monitoring cloud operations and events, and generating performance reports
©Certcop	©Certcop
Blue Team	Blue Team
Mitigating Controls	As stated in the definition, mitigating controls are procedures employed to lessen the overall impact of a danger. As a result, the mitigating controls are assigned to the appropriate dangers.
©Certcop	©Certcop
Blue Team	Blue Team
Monitor Baseline	Assessment and mitigation cannot entirely protect it. It's impossible to fix every system or eliminate every application flaw right away. Even if this were possible, users would continue to do
	things that permitted dangerous code to be installed on their systems.

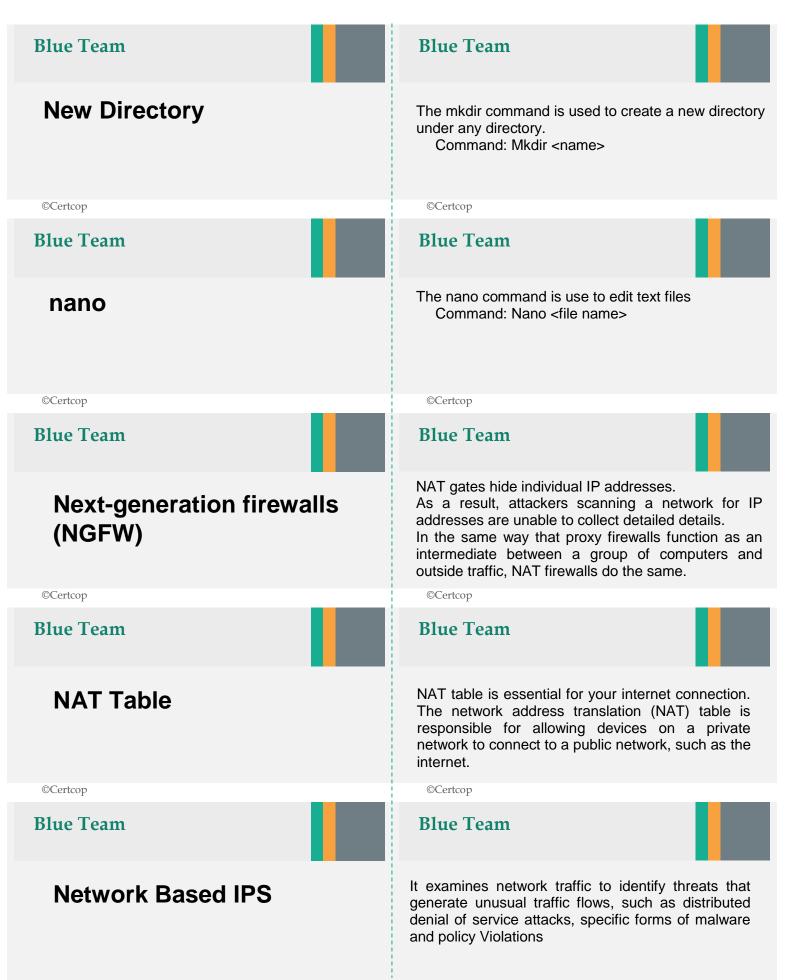
Blue Team	Blue Team
Monitoring	Packet capture and export of data to text files for further processing by third party tools
©Certcop	©Certcop
Blue Team	Blue Team
Mobility	Users of wireless networks can connect to existing networks and then roam freely. Because the phone connects the user via cell towers, a mobile phone user can travel kilometers in a single call.
©Certcop	©Certcop
Blue Team	Blue Team
MAC address	A unique identification assigned to a network interface controller (NIC) for use as a network address in communications inside a network segment is known as a media access control address (MAC address).
©Certcop	©Certcop
Blue Team	Blue Team
Mean Time between Failures (MTBF)	Mean time between failures (MTBF) is a prediction of the time between the innate failures of a piece of machinery during normal operating hours. MTBF helps businesses understand the availability of their equipment.
©Certcop	©Certcop
Blue Team	Blue Team
Mean Time to Repair (MTTR)	Mean time to repair (MTTR) is a maintenance metric that calculates the average amount of time required to troubleshoot and repair faulty equipment. It reflects how rapidly an organization can respond to and repair unplanned breakdowns.
	@C-steer

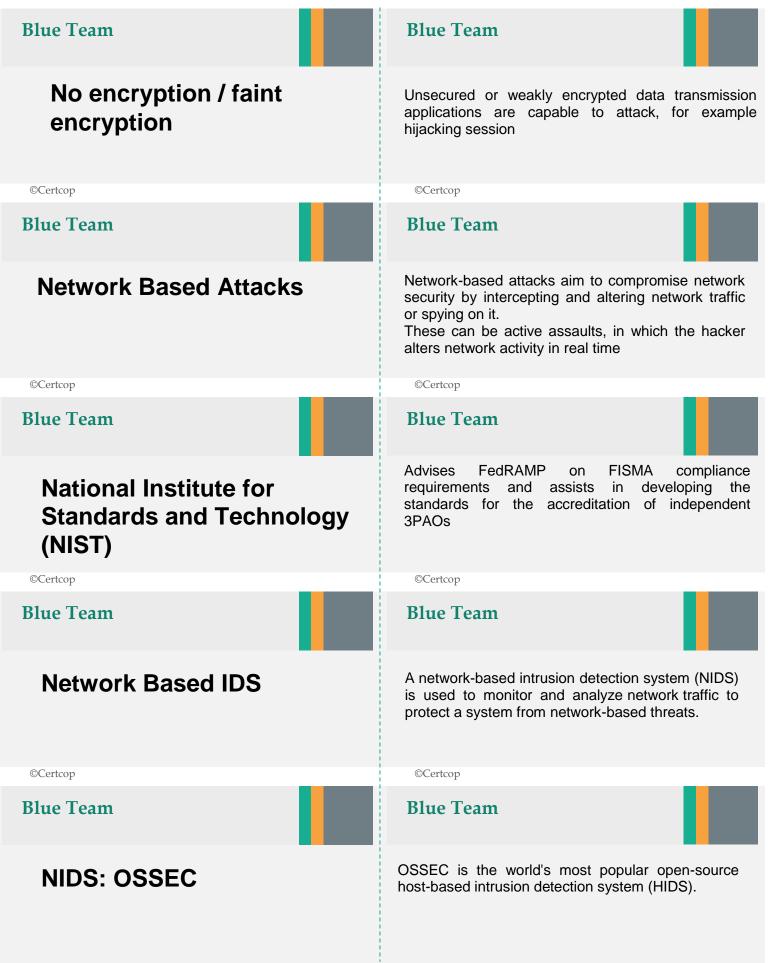
Blue Team	Blue Team
MTTR formula	(Total corrective maintenance time/ Number of repairs) =MTTR
©Certcop	©Certcop
Blue Team	Blue Team
Multi- factor authentication	When you use multi-factor authentication, your IAM provider requires more than one type of proof that you are who you say you are. A common example is the requirement of both a password and a fingerprint.
©Certcop	©Certcop
Blue Team	Blue Team
Monitoring and Managing Processes	When a system boots, the kernel launches a software called init. init executes shell scripts that launch all system services. Some of them merely run in the background and have no user interface. They are called to as daemon processes.
Blue Team	Blue Team
Man-in-the-Browser	It is a form of proxy Trojan horse that infects web browsers that are vulnerable. Browser session data can be captured by successful man-in-the-browser attacks.
©Certcop	©Certcop
Blue Team	Blue Team
Memory Leak	A memory leak is a flaw in a computer program that leads it to consume more and more memory as time goes on. The application can take so much memory that the operating system fails in the worst-case scenario.
©Certcop	©Certcop

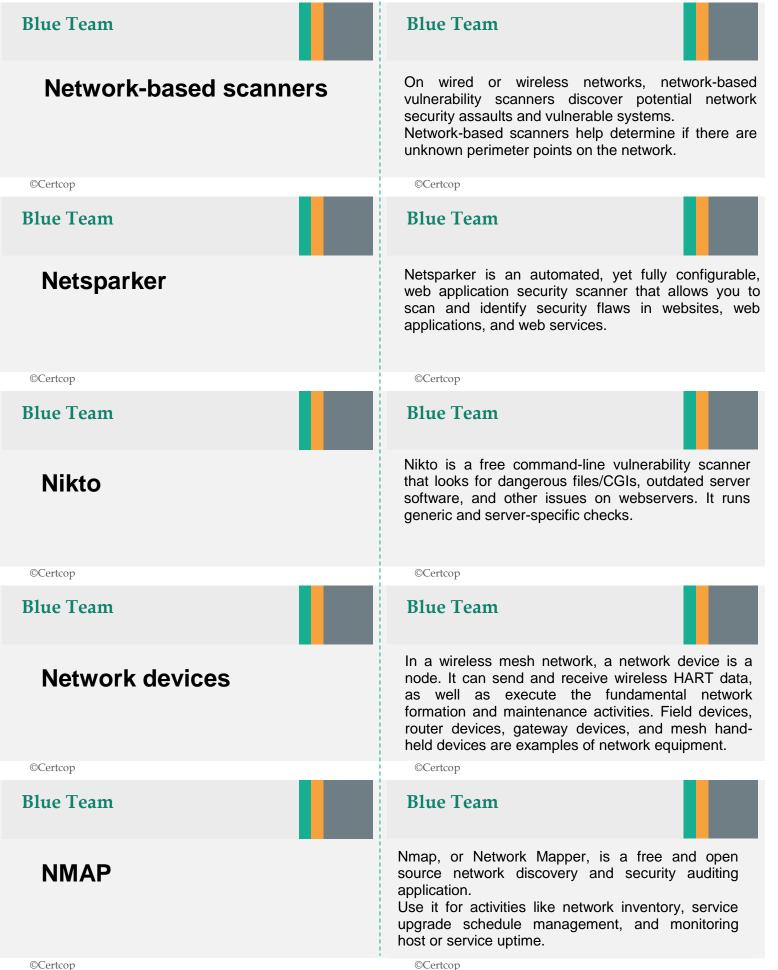
Blue Team	Blue Team
Multilevel SLA	Combines service and customer SLA, and applies at a corporate level for all users in an organization too. Multilevel SLAs avoid duplication and incompetence between several agreements, making it possible to integrate several conditions into the same system.
©Certcop	©Certcop
Blue Team	Blue Team
Malvertising	The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.
©Certcop	©Certcop
Blue Team	Blue Team
Malware	A computer program that is covertly placed onto a computer with the intent of compromising the privacy, accuracy, or reliability of the computer's data, applications, or operating system.
©Certcop	©Certcop
Blue Team	Blue Team
Metasploit	One of the most popular exploitation frameworks.
©Certcop	©Certcop
Blue Team	Blue Team
Mutual agreement.	The SLA is mutually accepted by the customer and the service provider.

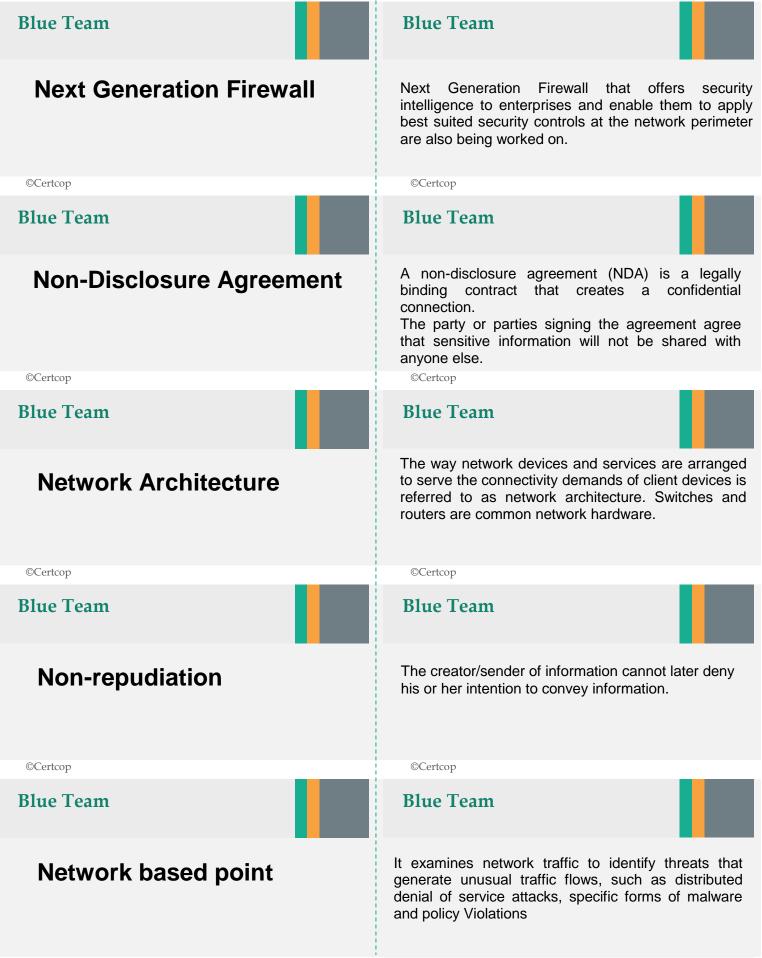


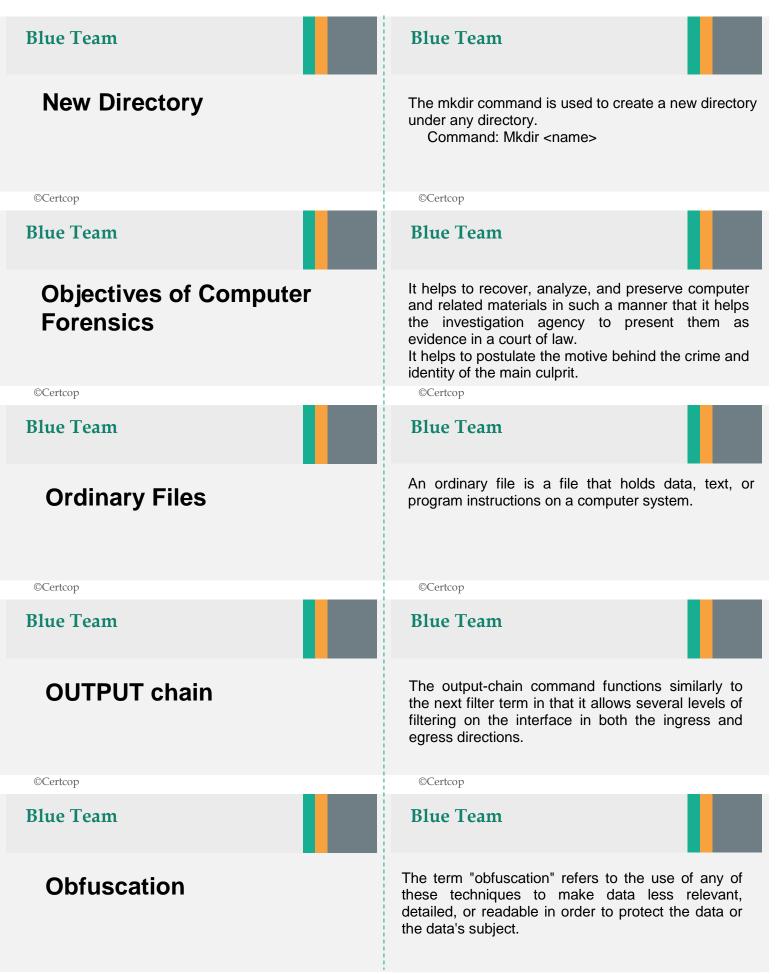


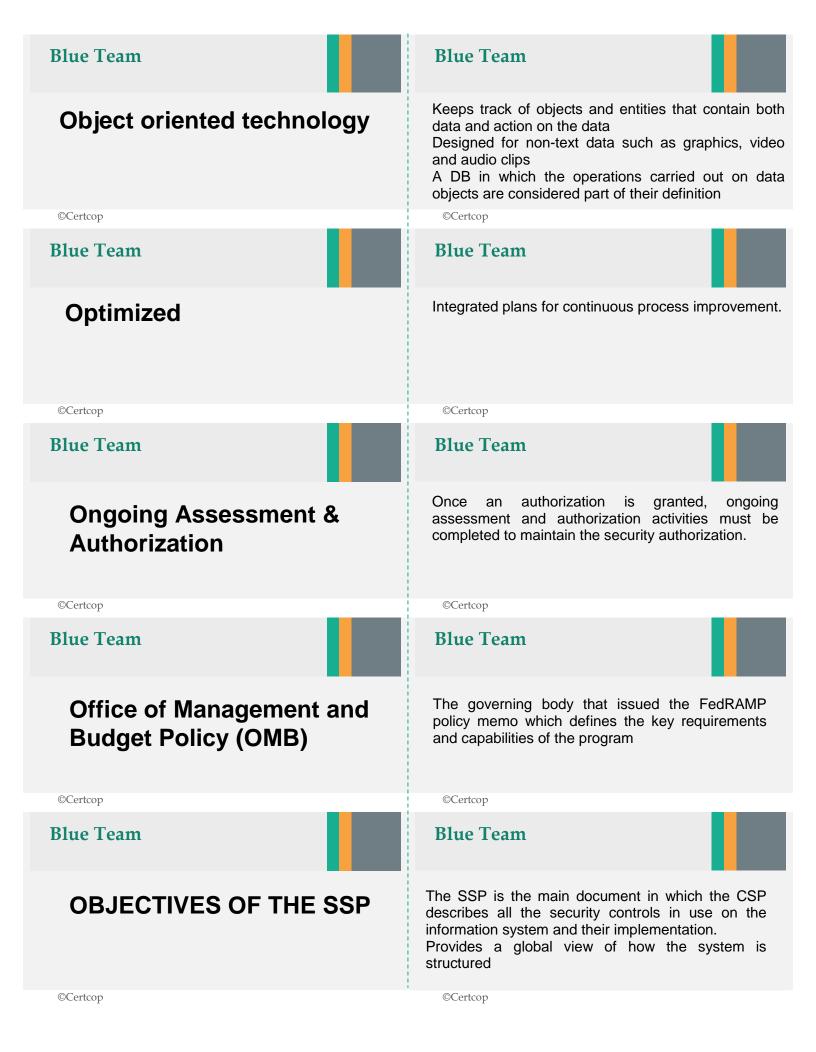




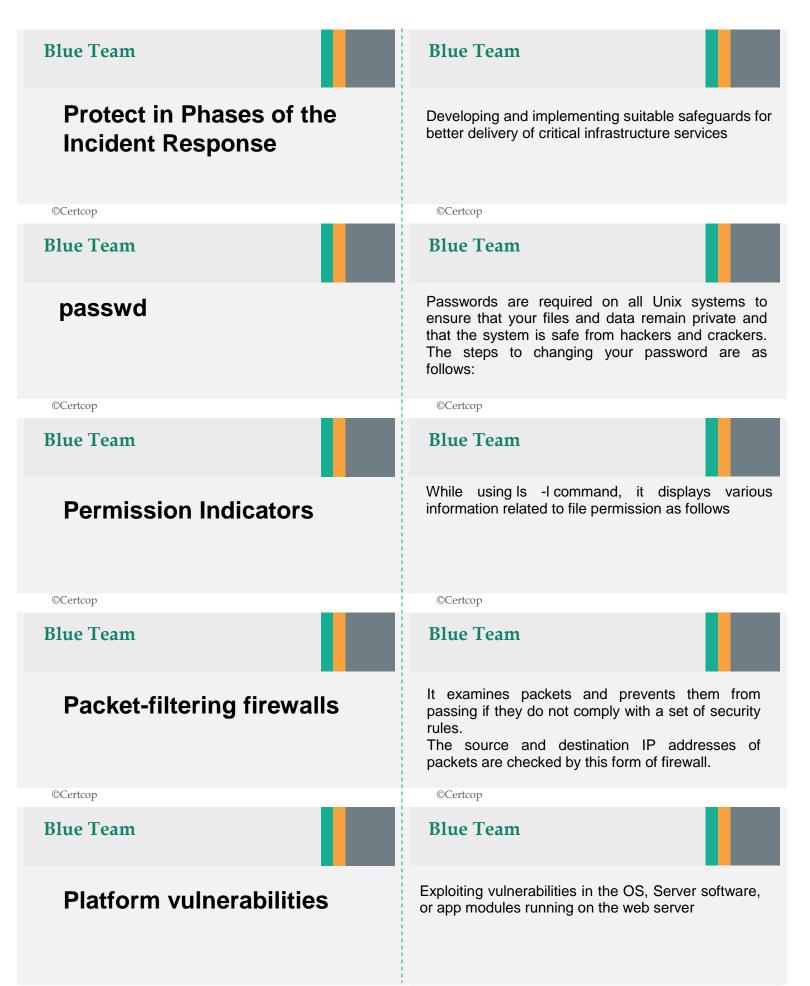




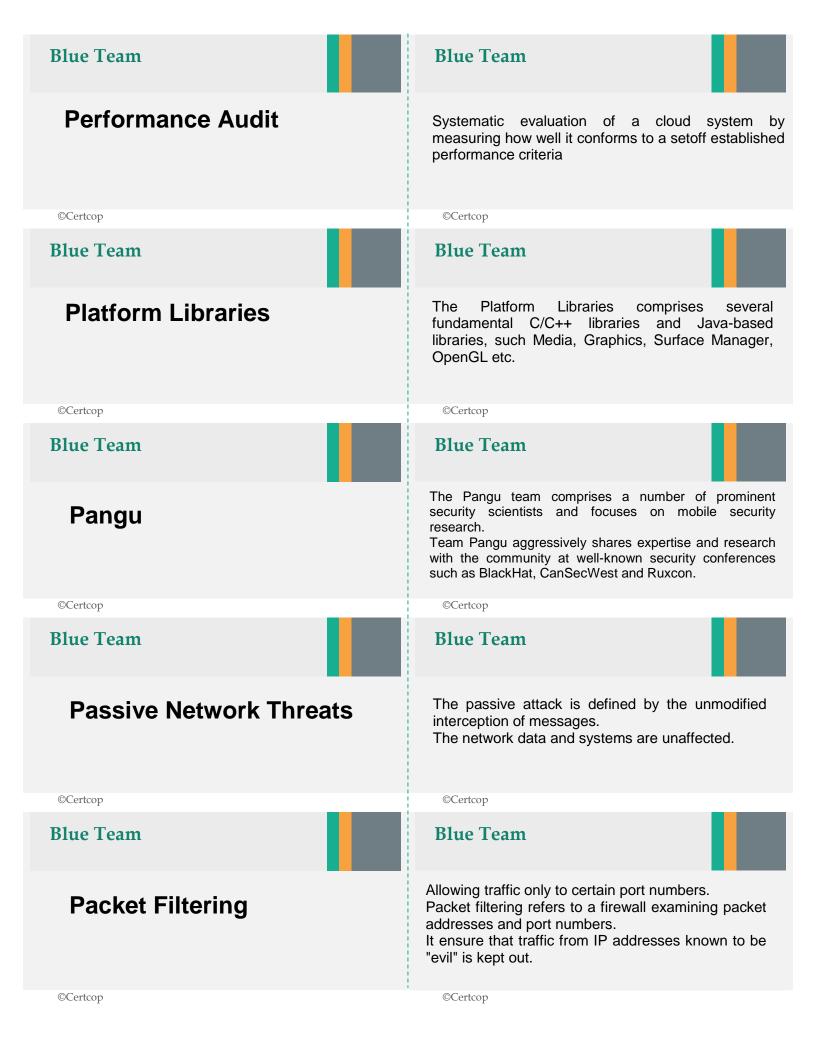


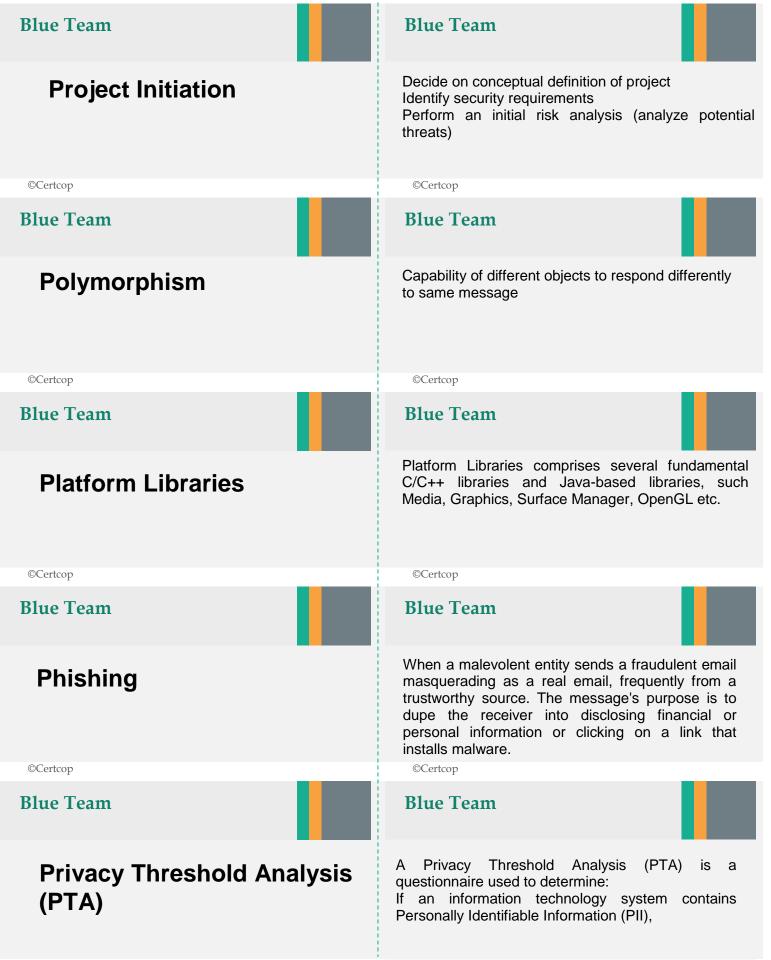


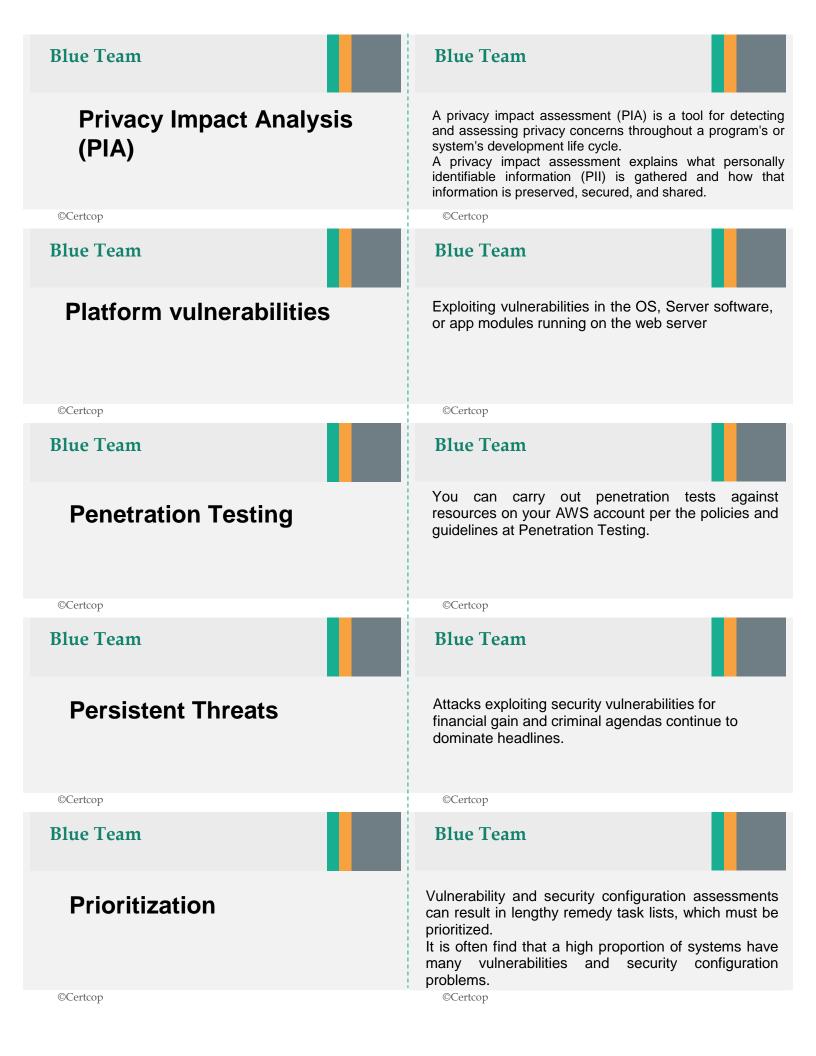
Blue Team	Blue Team
OpenVAS	OpenVAS is a vulnerability scanner with a lot of features. Unauthenticated and authenticated testing, different high-level and low-level internet and industrial protocol.
©Certcop	©Certcop
Blue Team	Blue Team
OpenID Connect (OIDC)	OIDC is a newer open standard that allows users to log in to their applications using an identity provider. It is extremely similar to SAML, however it is built on the OAuth 2.0 standards and uses JSON to communicate data rather than XML, like SAML does.
©Certcop	©Certcop
Blue Team	Blue Team
Onboarding	When a new employee joins a company, the on boarding process is defined as the person's first encounter with the company. As a result, you may assess whether the employee will continue with the company for a longer period of time in the first few days.
©Certcop	©Certcop
Blue Team	Blue Team
Preservation	Data is segregated, safeguarded, and preserved during this phase. It includes restricting people from utilizing the digital device in order to prevent tampering with digital evidence.
©Certcop	©Certcop
Blue Team	Blue Team
Presentation	The process of summarization and explanation of conclusions is completed in this final step. It should, however, be written in layman's words with abstracted terminologies. The precise details should be referenced in all abstracted terms.
©Certcop	@Certcon

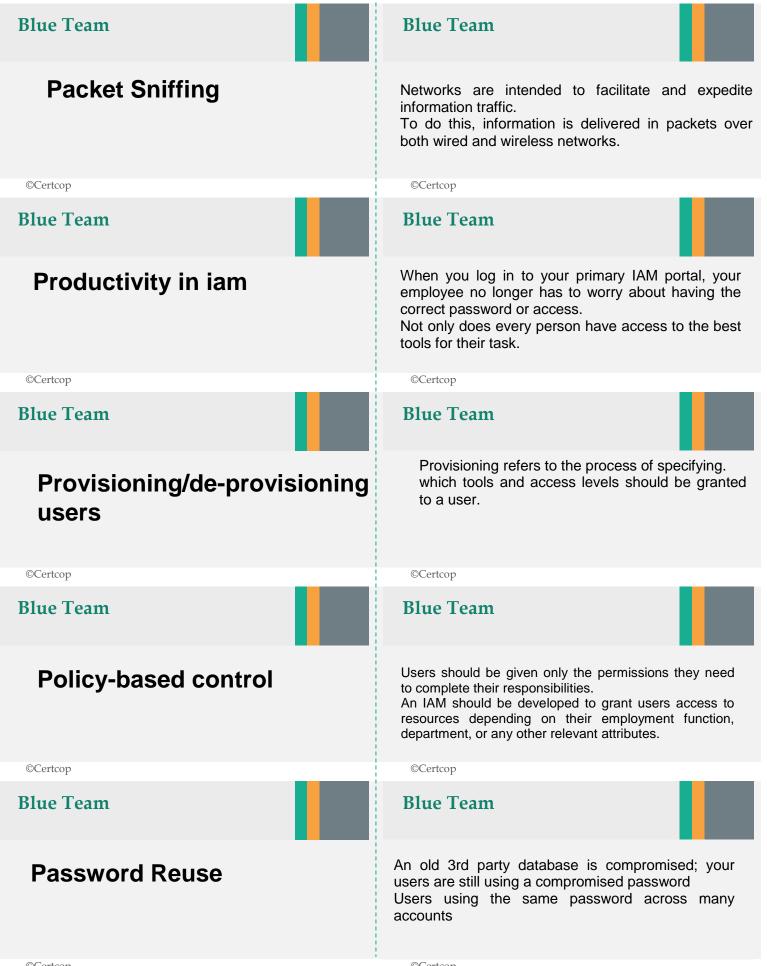


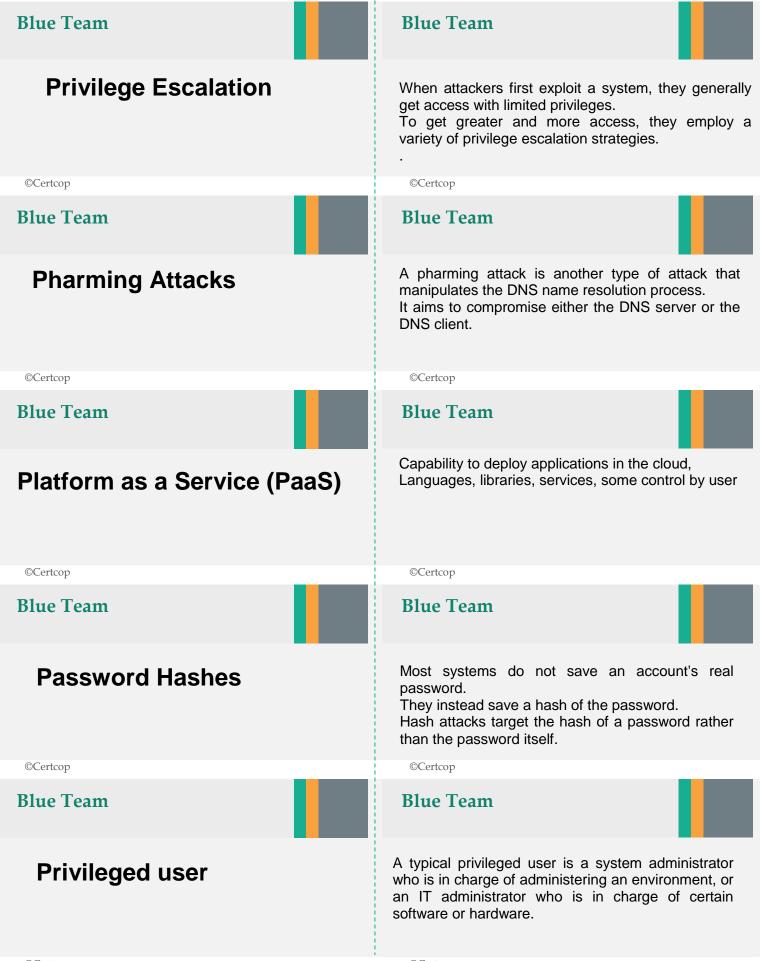
©Certcop

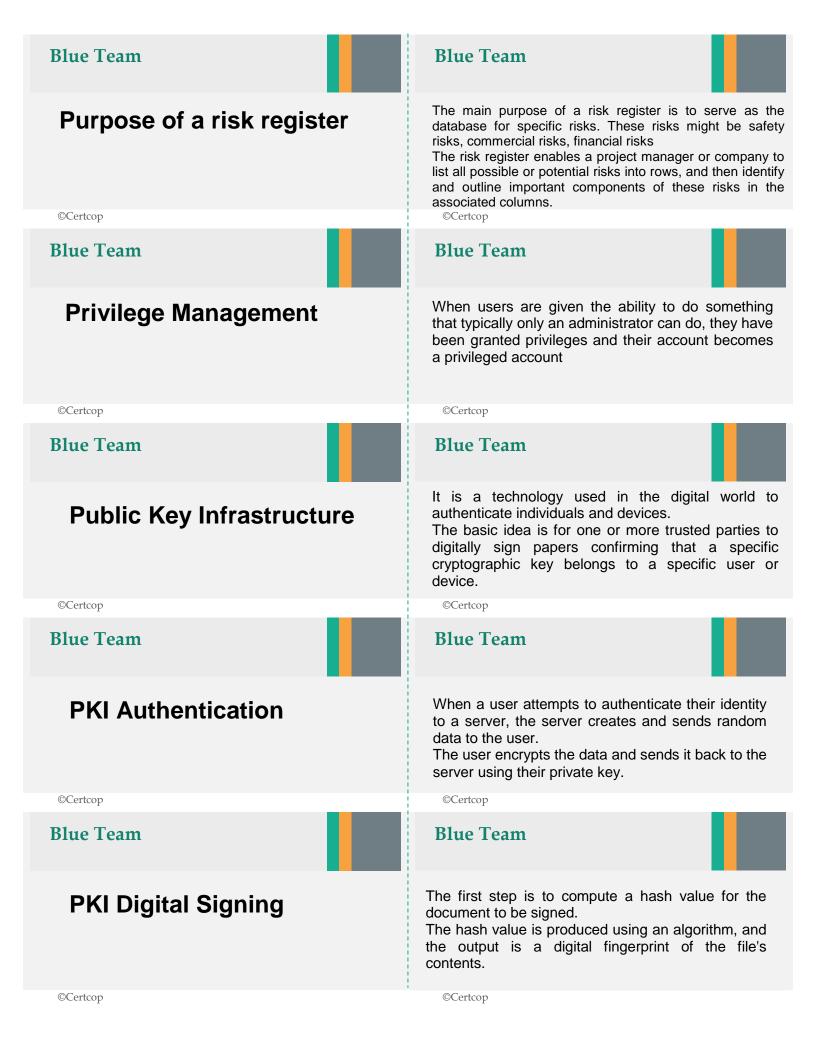


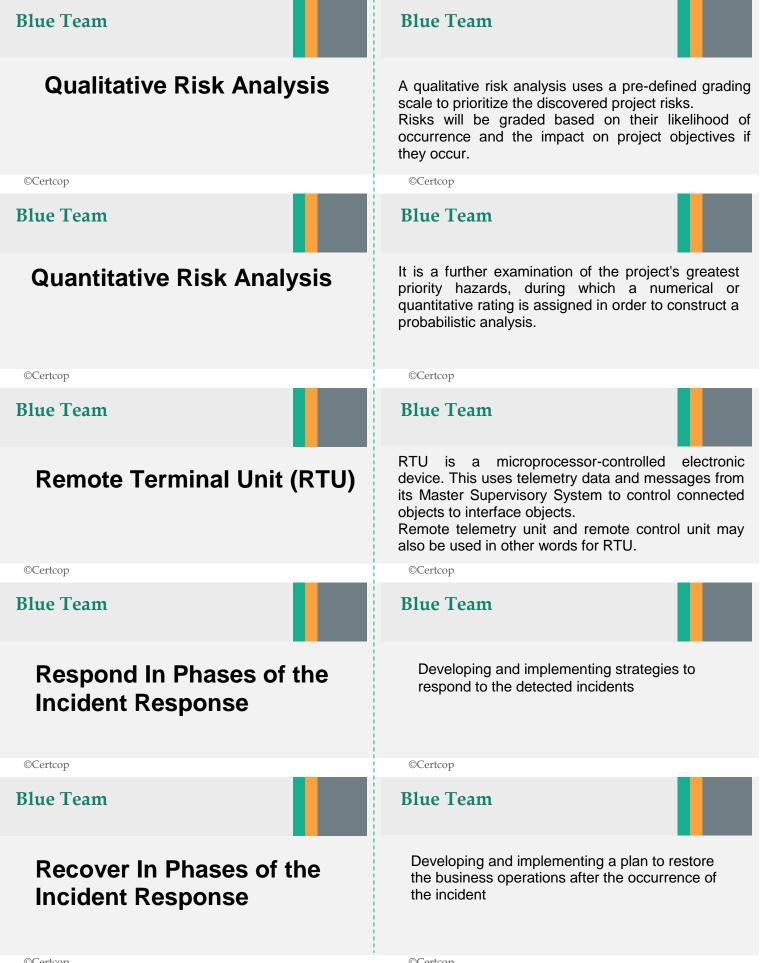


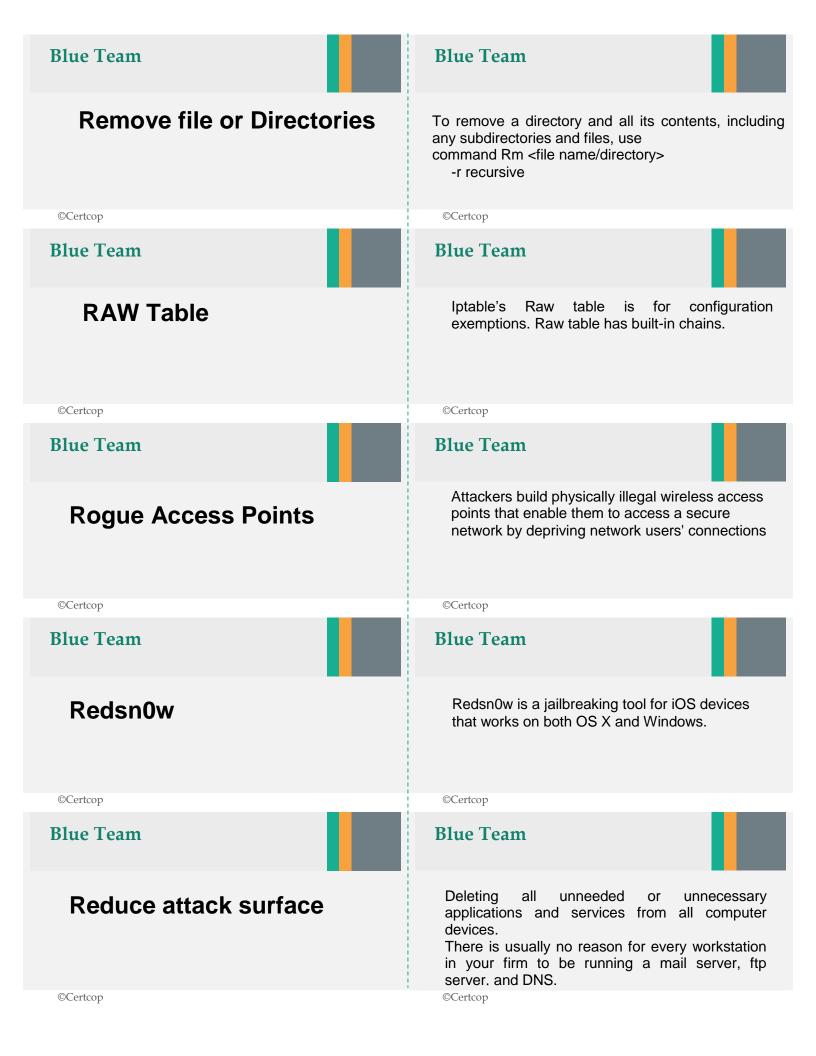


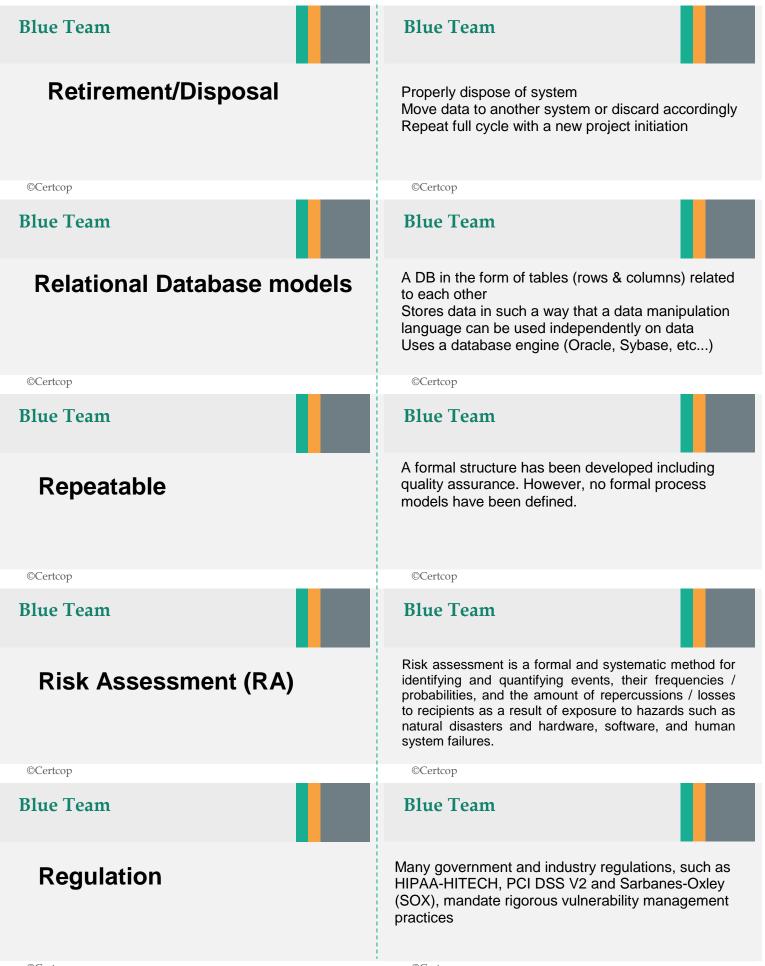




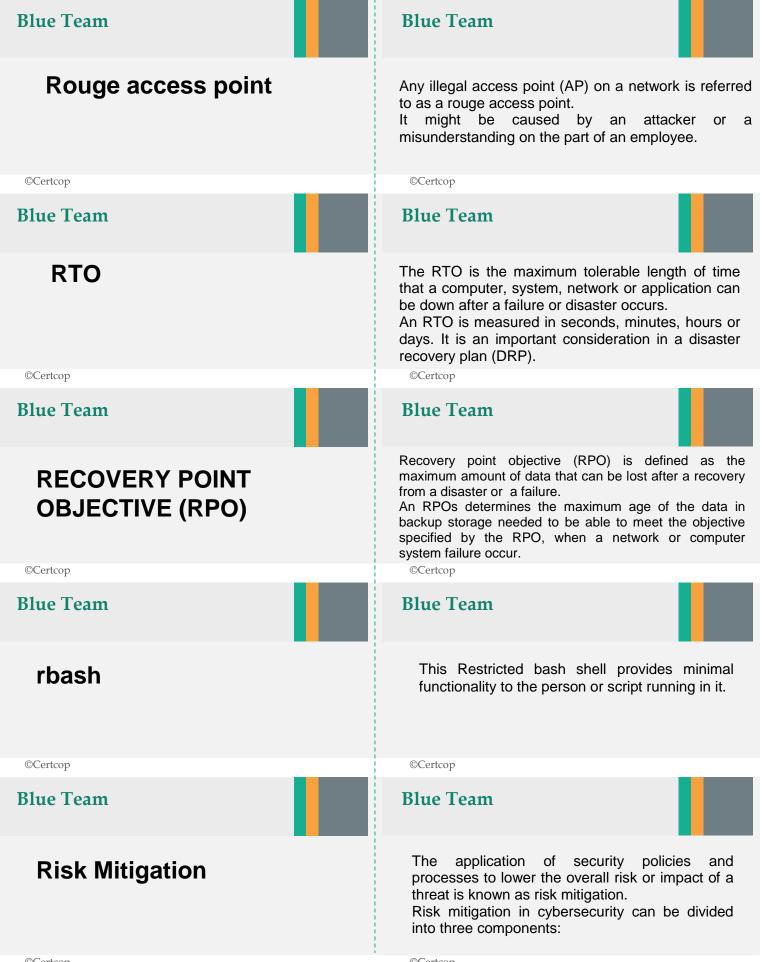












©Certcop

Blue Team

Rainbow Attack

©Certcop

Blue Team

Replay Attack

©Certcop

Blue Team

ROLE-BASED AWARENESS TRAINING

©Certcop

Blue Team

Record your findings

©Certcop

Blue Team

Review assessment and update if necessary

Blue Team



Rainbow table assaults are a sort of attack that tries to figure out the password by looking at the hash. A rainbow table is a large database of hashes that have already been generated.

©Certcop

Blue Team



A replay attack occurs when an attacker replays data from a communication session that has previously occurred.

A replay attack occurs when a third party tries to imitate a client who was present during the initial session.

©Certcop

Blue Team



If you have someone who is new to the organization, you might want to provide some role-based security awareness training.

This is typically a specialized sort of training that is tailored to the role that this individual user plays with this program or data.

©Certcop

Blue Team



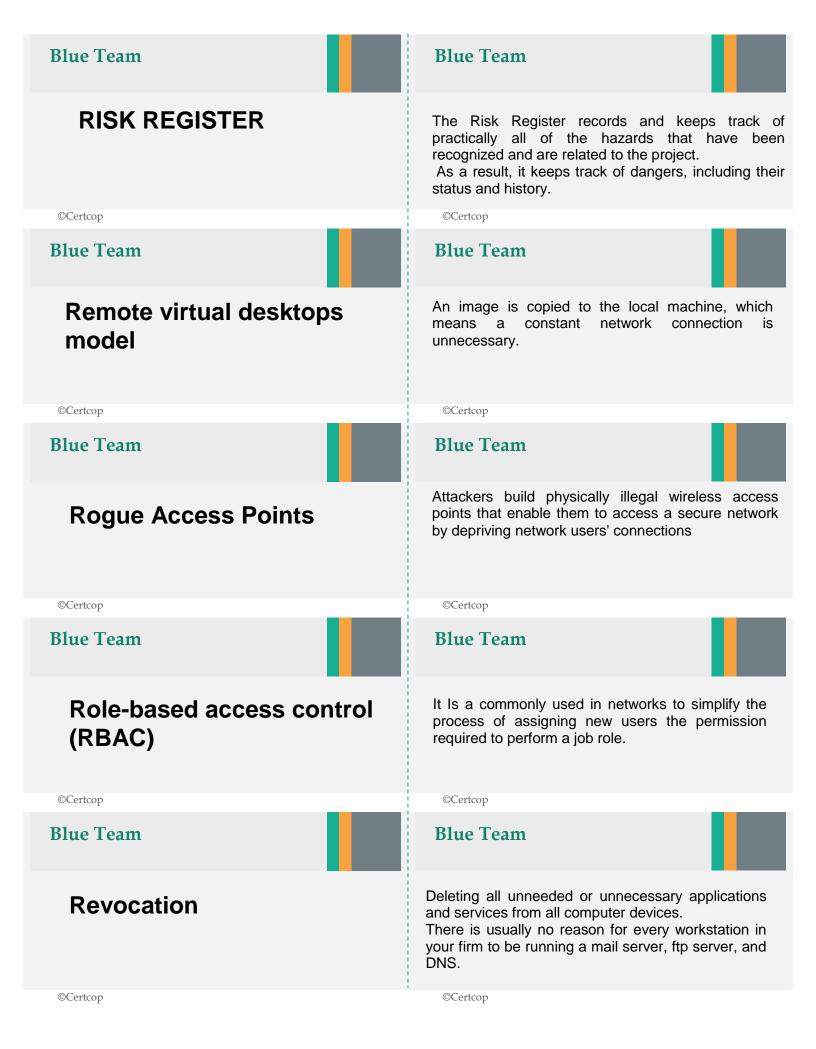
If you have more than five employees in your office, you are required by law to write down your risk assessment process. Your plan should include the hazards you've found, the people they affect, and how you plan to mitigate them.

©Certcop

Blue Team

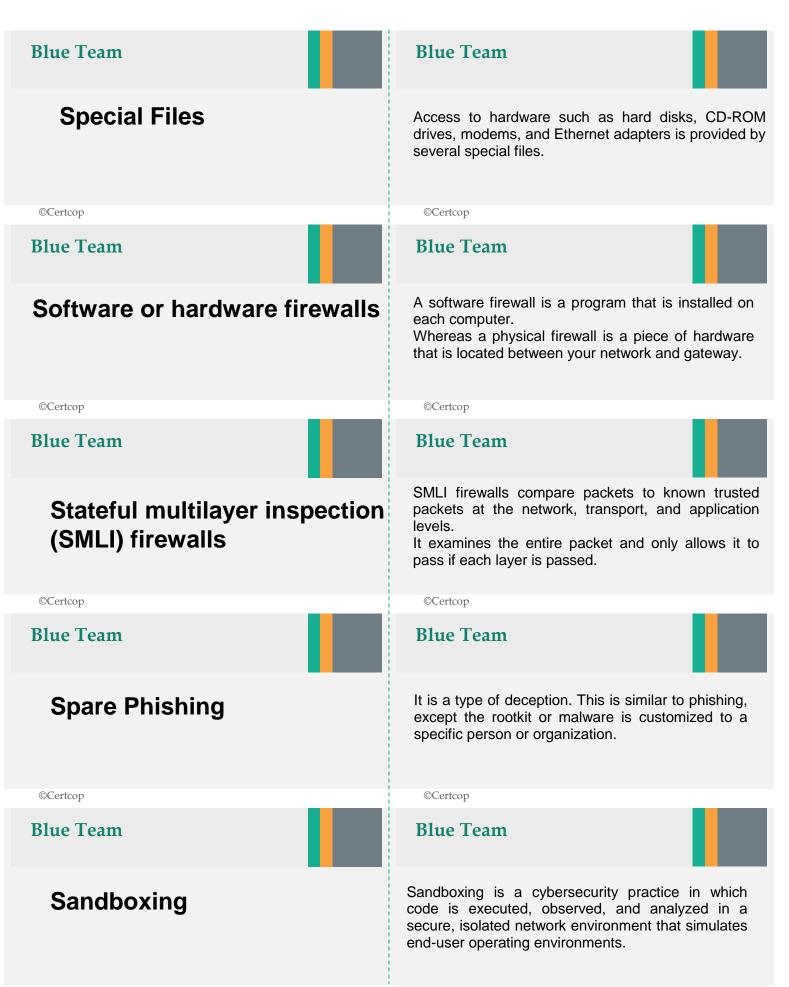


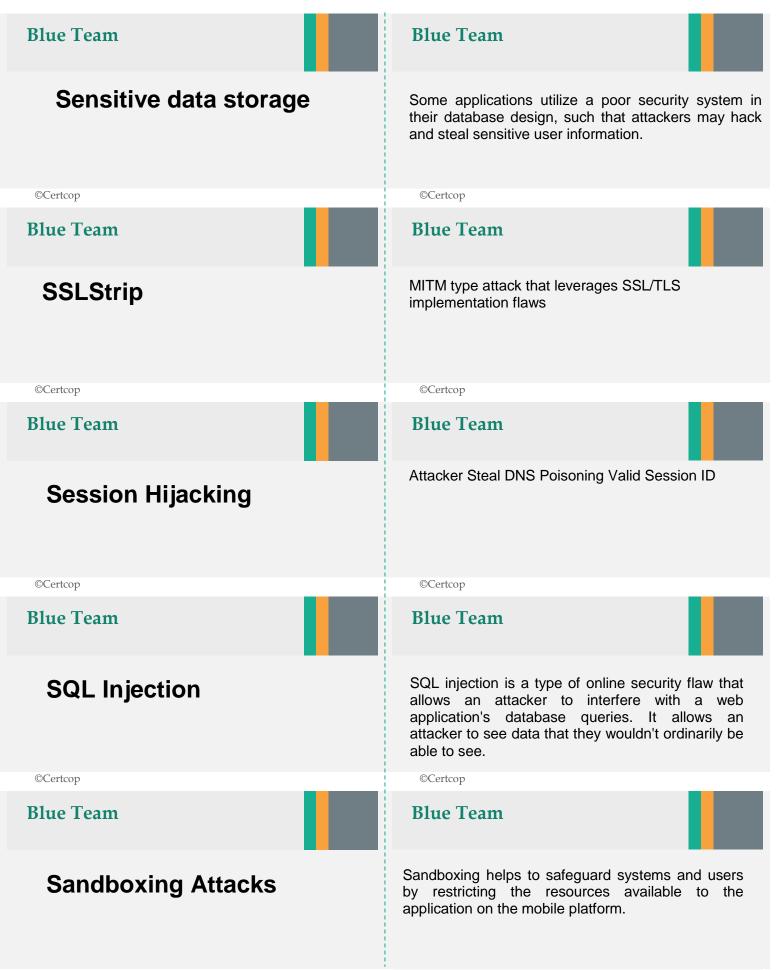
Your workplace is always changing, so the risks to your organization change as well. As new equipment, processes, and people are introduced, each brings the risk of a new hazard.



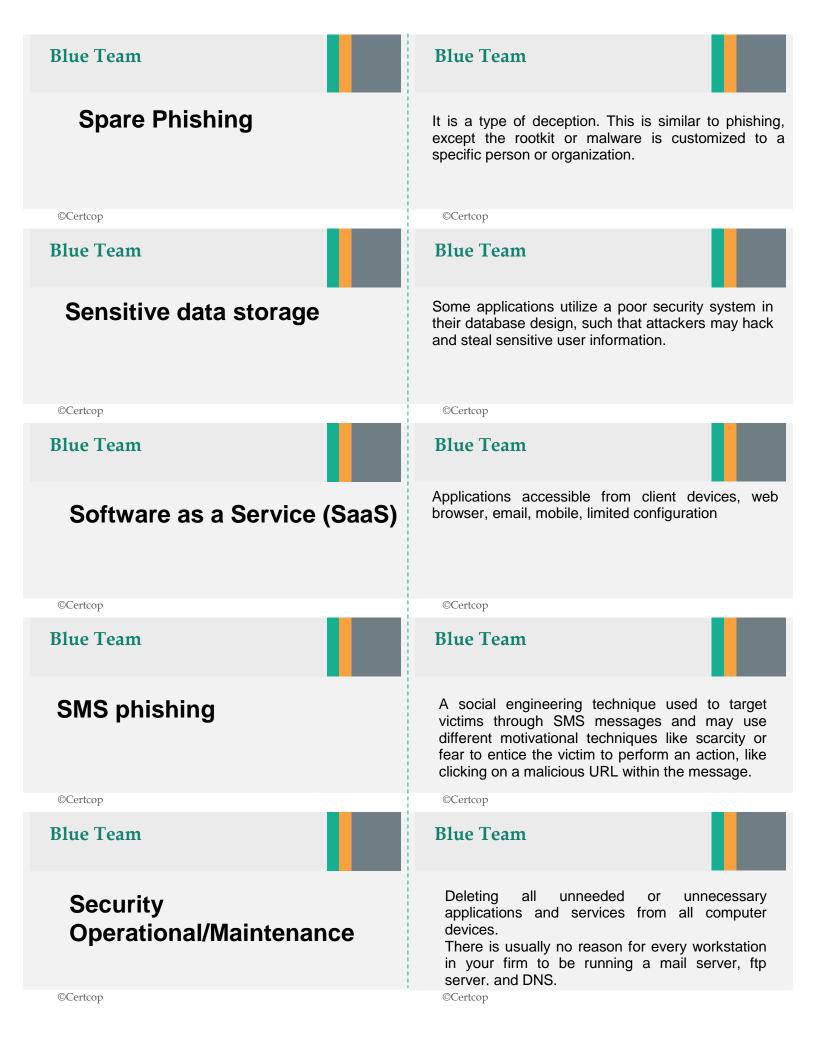


©Certcop





Blue Team	Blue Team
Sniffing	Attacker reads, monitors, or captures complete packets of data passing between a client and a server. An unencrypted network packet intercepted by a hacker might inflict significant damage to the company or institution.
©Certcop	©Certcop
Blue Team	Blue Team
Spoofing	Spoofing is the practice of a bad actor impersonating a legitimate entity or someone they are not. It usually refers to a computer faking an IP address, ARP, or DNS server.
©Certcop	©Certcop
Blue Team	Blue Team
Segment the network	Segment is one of the simplest ways for businesses to safeguard their networks. It refers to the practice of dividing a bigger network into smaller, self-contained networks. Organizations can also use segmentation to keep sensitive data more secure and restrict access to essential information. ©Certcop
Blue Team	Blue Team
Switch from default to secure configuration	Installed software's security settings to the most secure available configuration on a regular basis. New software is frequently used with default settings for lengthy periods of time. This results in security breaches that could have
©Certcop	©Certcop
Blue Team	Blue Team
Social engineering	Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime,





System and Communications Protection (SC)

©Certcop

Blue Team

System and Information Integrity (SI)

©Certcop

Blue Team

Service Dependency Mapping

©Certcop

Blue Team

Switches

©Certcop

Blue Team

Streamline Data Collection

Blue Team



The systems and communications protection policy defines the rules for effectively creating network segmentation and boundary protection across the company, as well as the essential regulations for implementing encryption.

©Certcop

Blue Team



System and information integrity ensures that the data being accessed has not been tampered with or harmed as a result of an information system fault.

©Certcop

Blue Team



The goal of this stage is to determine the source and root cause.

It entails determining which system components are responsible.

An obsolete version of an open source library.

©Certcop

Blue Team



A switch has a number of ports into which computers can be connected. When a data frame arrives at any port of a network switch, it is examined for the destination address, relevant checks are performed, and the frame is sent to the appropriate device (s).

©Certcop

Blue Team



Again, the most accurate equipment data stems from using sensory meters with CMMS platforms.

Single Point of Failure (SPOF)

©Certcop

Blue Team

Security in iam

©Certcop

Blue Team

Service Dependency Mapping

©Certcop

Blue Team

Single Sign-on

©Certcop

Blue Team

Secure access

Blue Team



It is a potential risk presented by a weakness in the design, implementation, or configuration of a circuit or system in which a single fault or malfunction causes the entire system to fail.

©Certcop

Blue Team



Traditional security frequently has a single point of failure - the password.

If a user's password or, worse, the email address used for password recovery is compromised, your organization becomes vulnerable to attack.

©Certcop

Blue Team



The goal of this stage is to determine the source and root cause.

It entails determining which system components are responsible.

An obsolete version of an open source library.

©Certcop

Blue Team



Authenticate their identities with a single portal. Once authorized, the IAM system serves as the source of identity truth for the user's other resources.

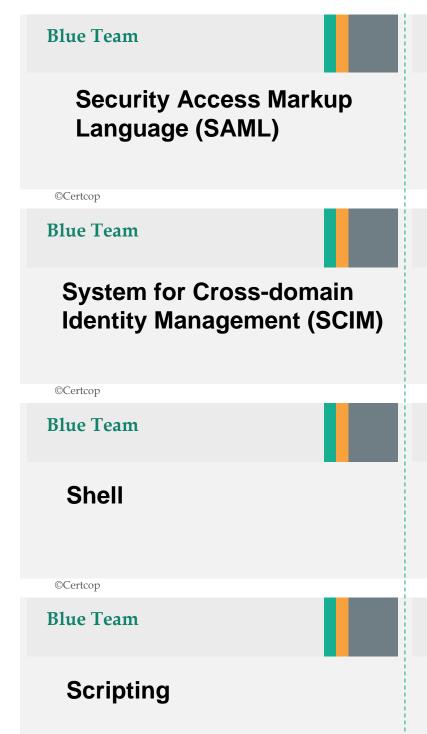
©Certcop

Blue Team



Securing at the identity level is critical; an IAM should ensure that the identities of those logging in are confirmed.

This could include implementing MFA and adaptive authentication.



©Certcop

Blue Team

Secured Protocol and Algorithms

Blue Team



SAML is an open standard that allows identity provider systems to communicate authentication and authorization information.

This is the most widely used technique for an IAM to provide a user access to an application.

©Certcop

Blue Team



SCIM is standard used to automatically exchange identity information between two systems.

When new users are assigned to the service, SCIM is utilized to maintain the user information up to date.

©Certcop

Blue Team



It is a macro processor which allows for an interactive or non-interactive command execution.

©Certcop





It allows for an automatic commands execution that would otherwise be executed interactively one-byone.

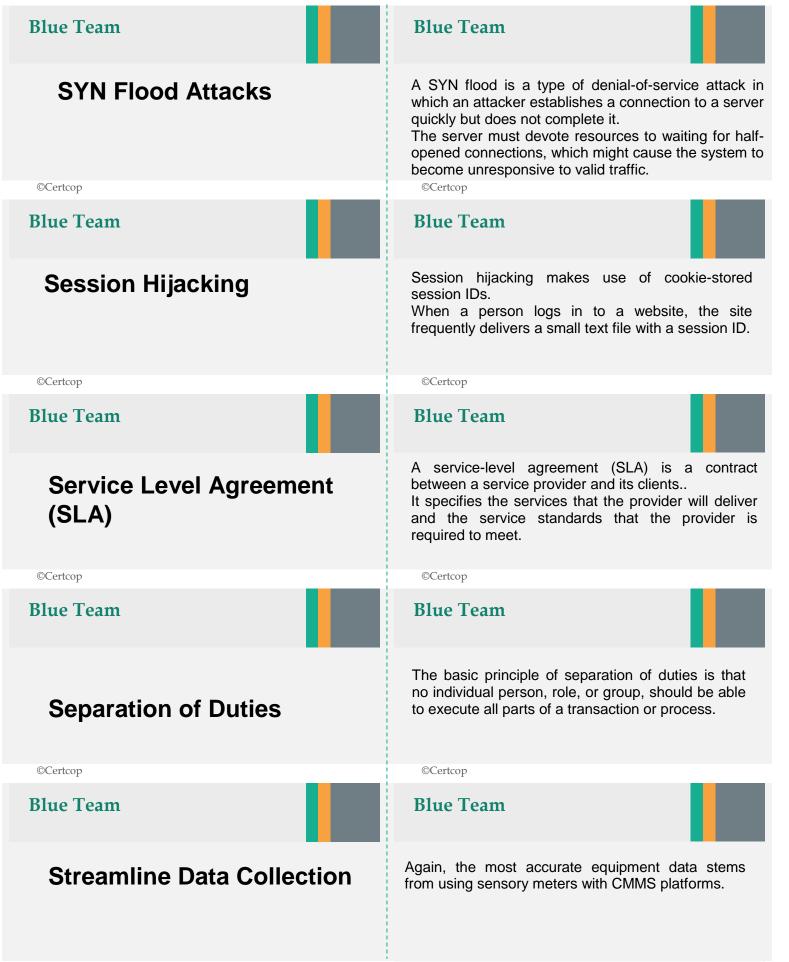
©Certcop

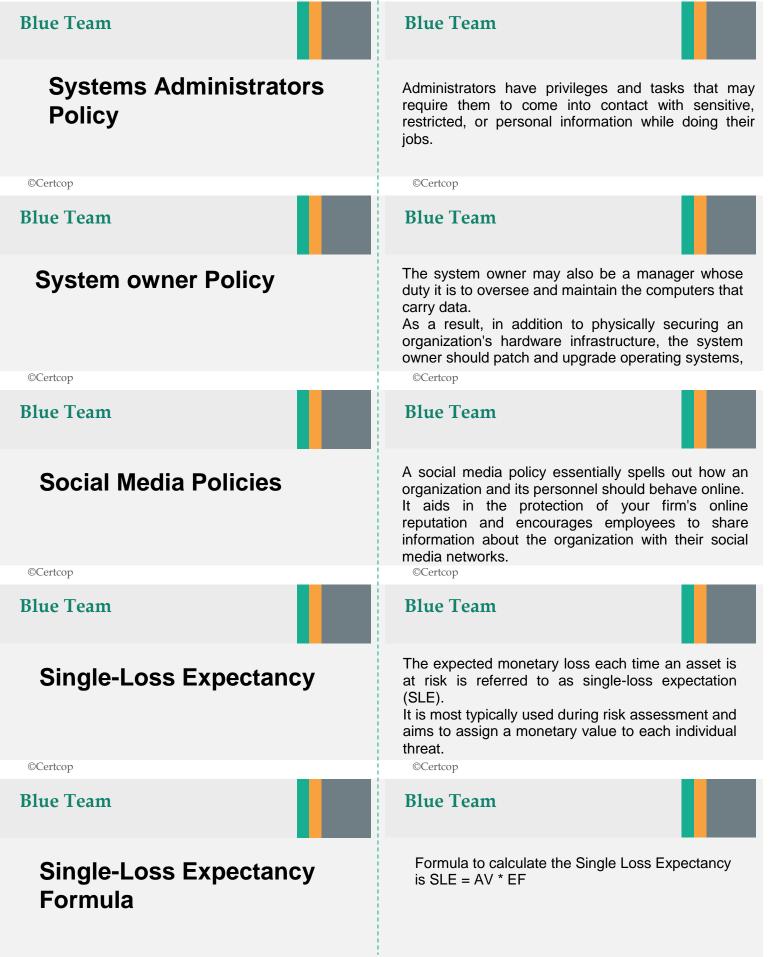
Blue Team

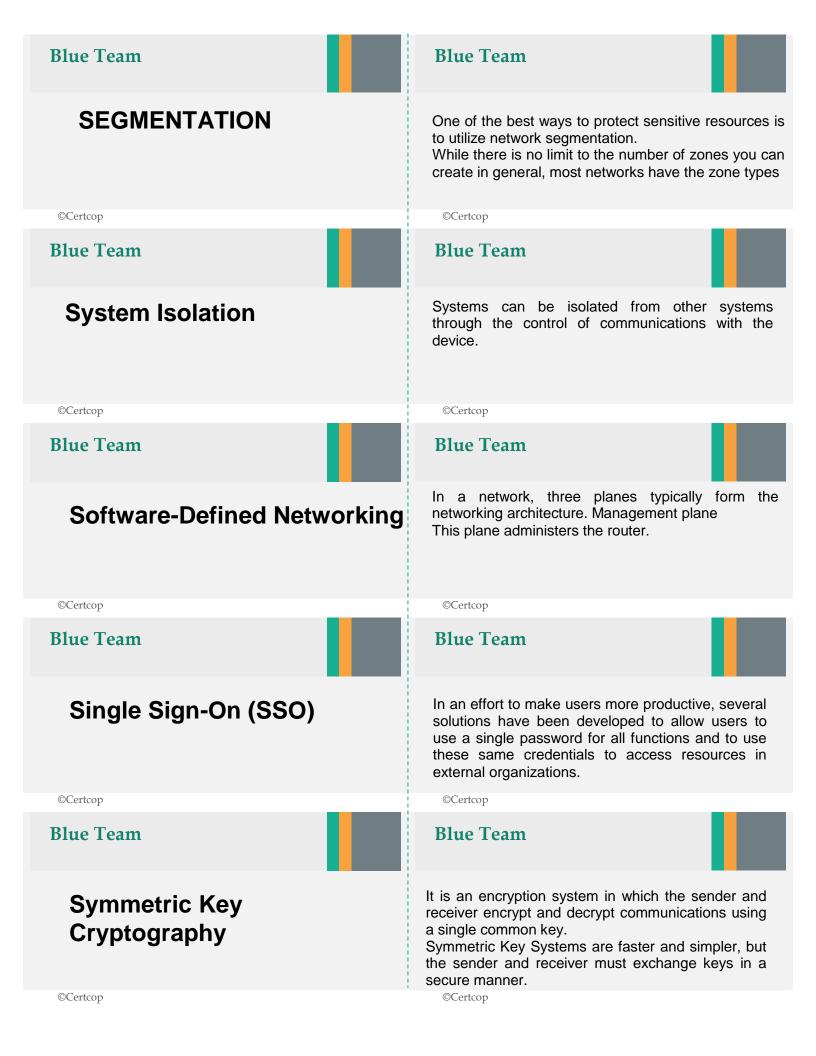


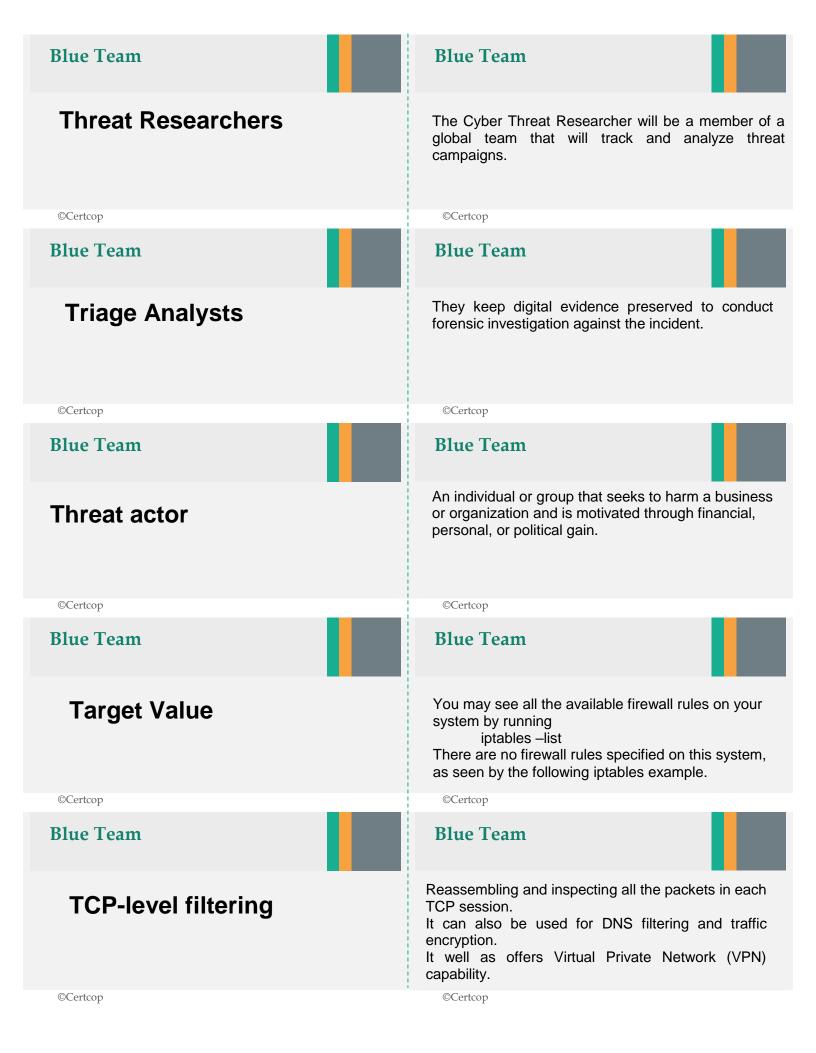
Research in protocols and algorithms is a significant phase for the consolidation of cybersecurity at a technical level.

It defines the rules for information sharing and processing over cyberspace.

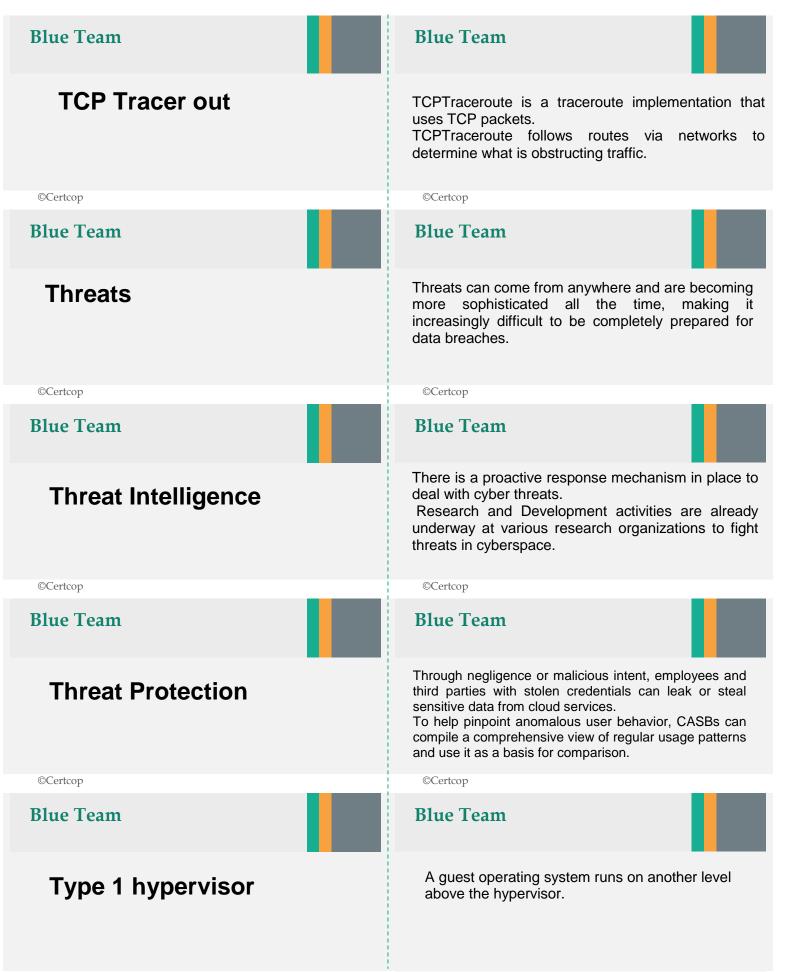


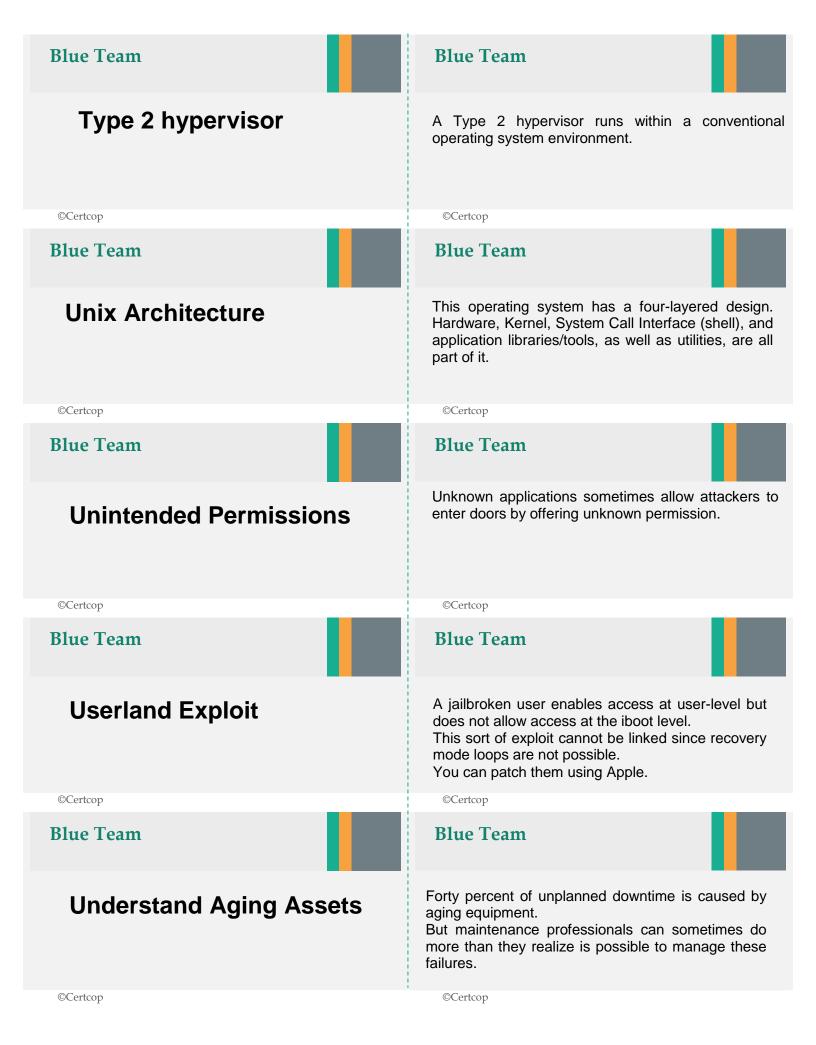




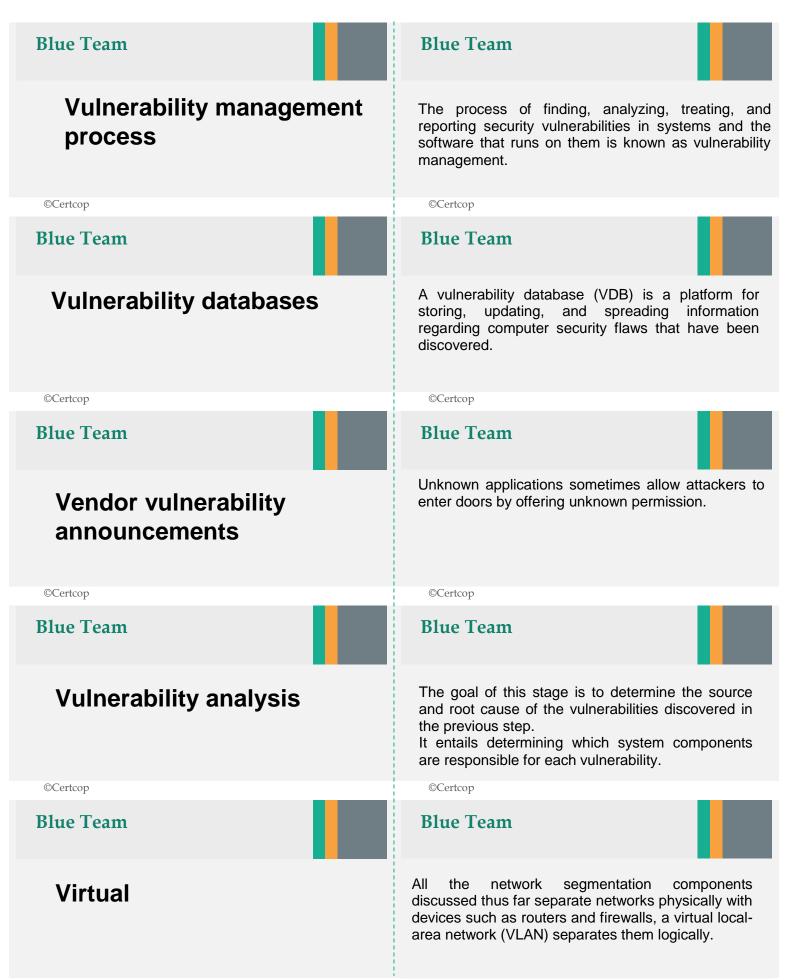


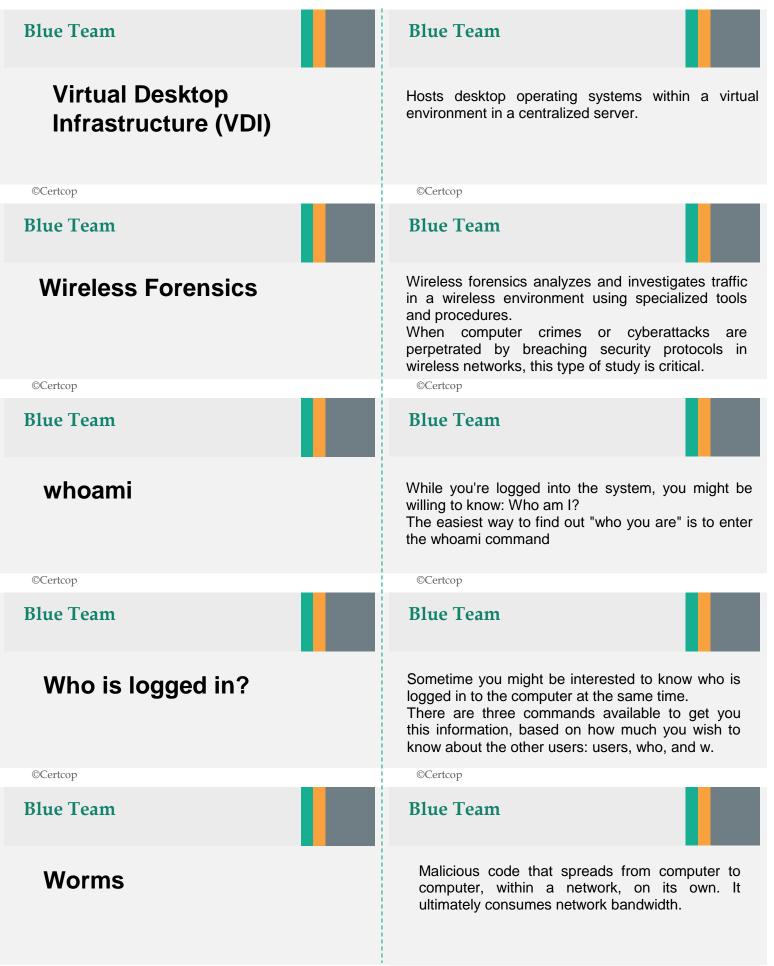
Blue Team	Blue Team
Tuple	A Tuple is a comma-separated collection of Python objects. In terms of indexing, nested objects, and repetition, a tuple is comparable to a list, but a tuple is immutable, whereas lists are mutable.
©Certcop	©Certcop
Blue Team	Blue Team
Trojan	Malicious code that masquerades as a harmless file. It usually performs a variety of actions, including key-logging, opening the computer to further attacks, destroying data or files, among others.
©Certcop	©Certcop
Blue Team	Blue Team
Third-Party Assessment Organizations (3PAOs).	Perform initial and periodic assessment of CSP systems per FedRAMP requirements Provide evidence of compliance Have on-going role in ensuring CSPs meet requirements.
©Certcop	©Certcop
Blue Team	Blue Team
Tripwire	Tripwire provides a comprehensive, automated view of operational, regulatory, and security compliance throughout the data center's dynamic environment.
©Certcop	©Certcop
Blue Team	Blue Team
Tailgating	Tailgating also known as piggybacking occurs when a hacker follows someone with an approved access card into a protected building. This assault assumes that the individual with valid access to the facility is kind enough to keep the door open for the person in front of them, presuming they are permitted to be there.



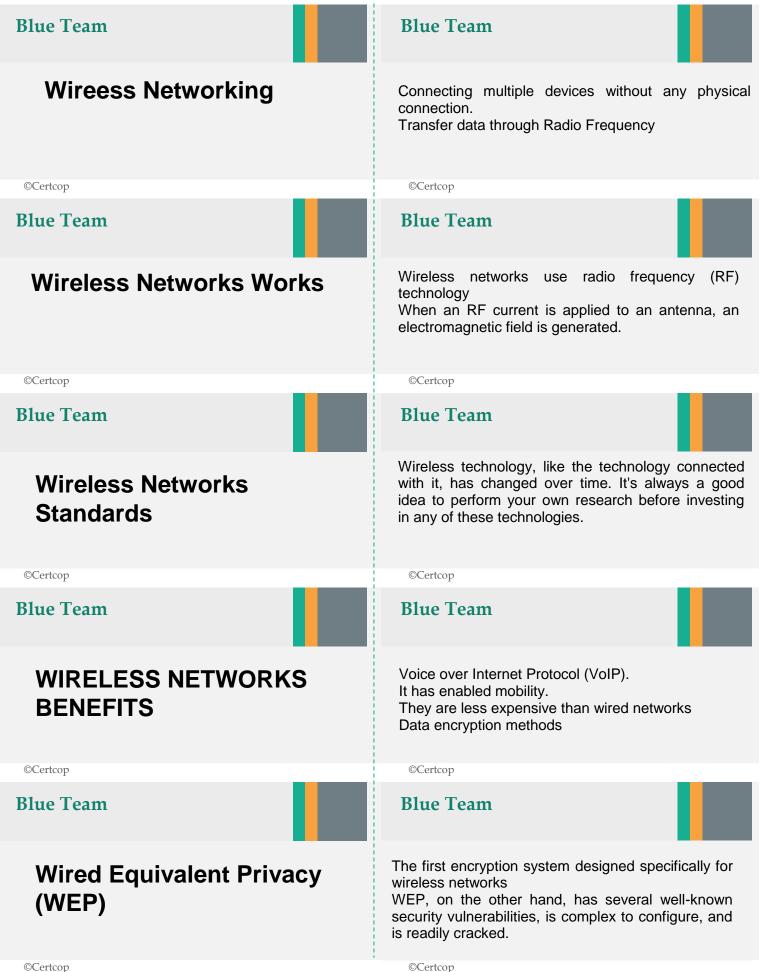


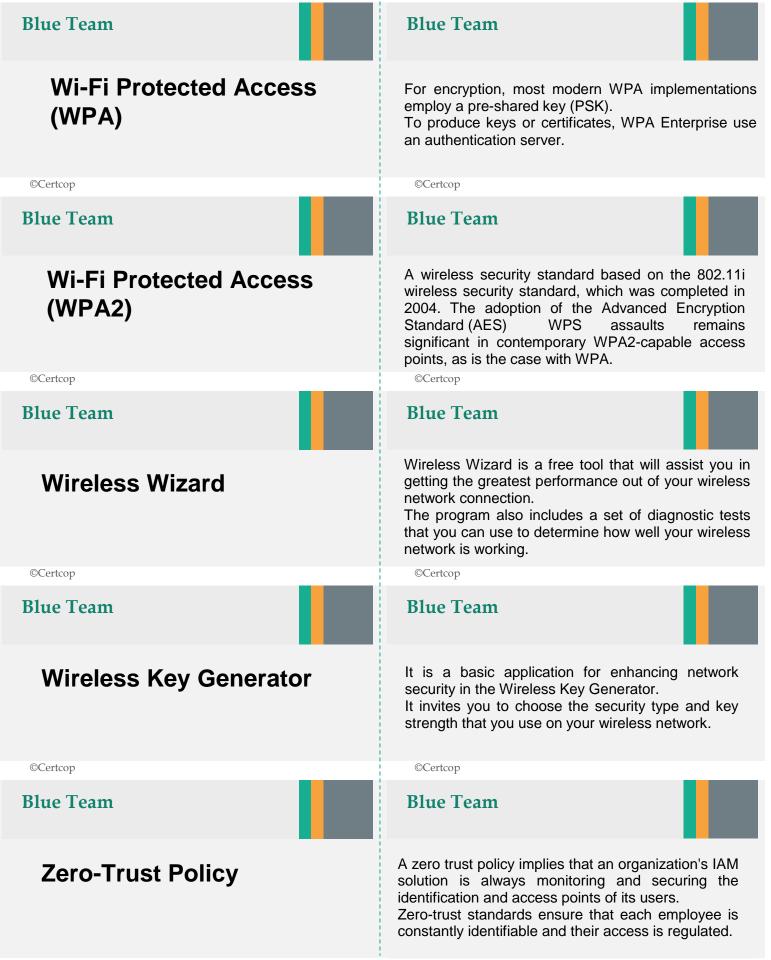
Blue Team	Blue Team
URL Hijacking	When someone buys a domain name that is similar to a valid domain name, this is known as typo squatting (also known as URL hijacking). People frequently do so with malice in mind.
©Certcop	©Certcop
Blue Team	Blue Team
User Policy	A user does not absolve someone of his or her responsibility to become acquainted with the organization's security policy and to uphold it by adhering to all security measures.
©Certcop	©Certcop
Blue Team	Blue Team
Virus	Malicious code that spreads from a computer to computer via attaching itself to other files. The code executes when the attached files opened.
©Certcop	©Certcop
Blue Team	Blue Team
Vulnerability Assessment	The next stage is to evaluate the environment for known vulnerabilities. This is performed by regular analyses of the environment's vulnerability and configuration. Network-based vulnerability assessment (VA) has been the primary method employed to baseline networks, servers and hosts.
©Certcop	©Certcop
Blue Team	Blue Team
Virtual machines	A virtual machine is a computer file that duplicates the behavior of a real computer. It can run as a distinct computing environment in a window, usually to run a different operating system.

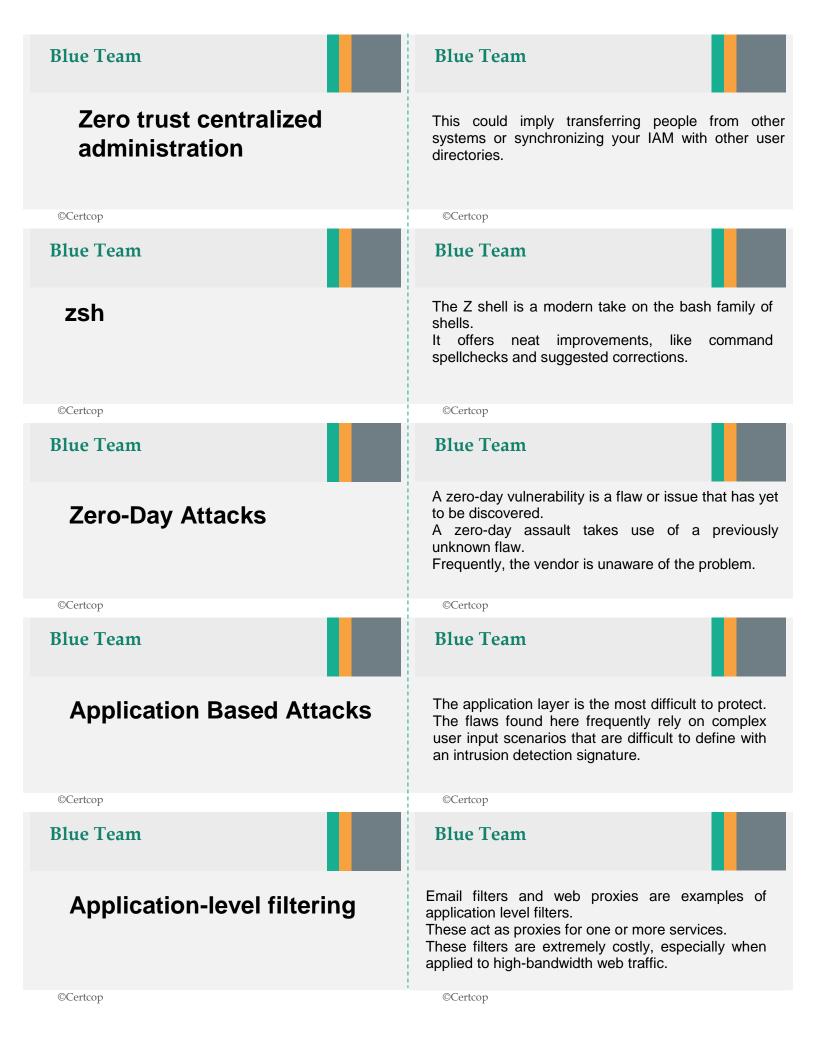


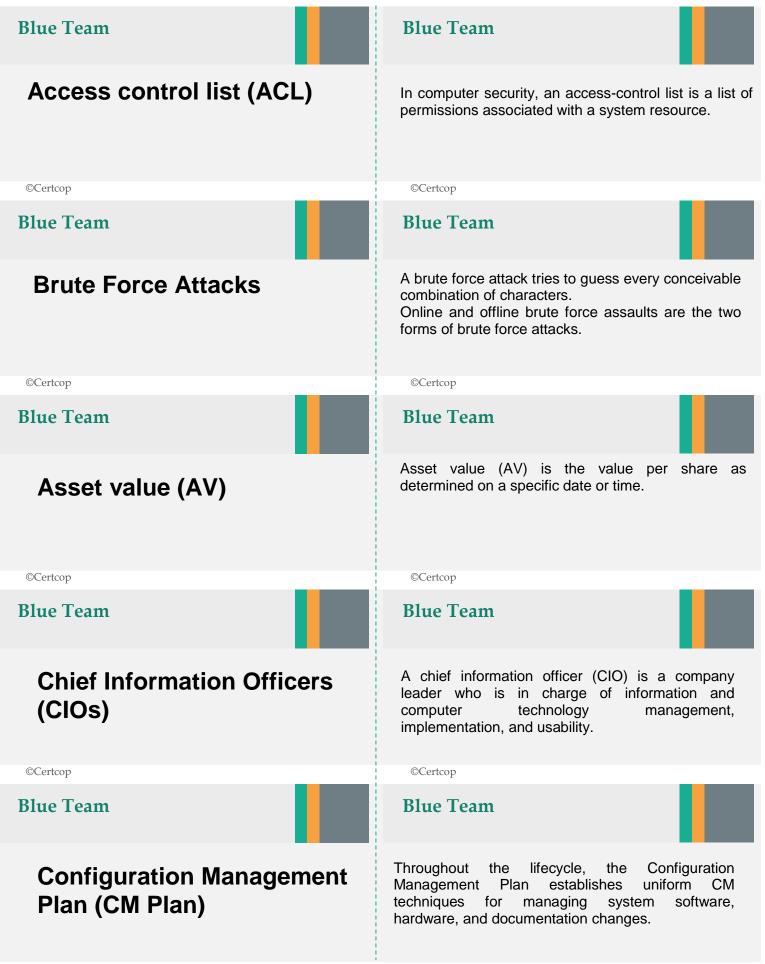


Blue Team	Blue Team
Wireless Scanner	Wireless vulnerability scanners are used to identify rogue access points and also validate that a company's network is securely configured.
©Certcop	©Certcop
Blue Team	Blue Team
Wireshark	Wireshark is a free and open source network protocol analyzer. It allows users to examine data traffic on a computer network in an interactive manner. The development effort was formerly known as Ethereal.
©Certcop	©Certcop
Blue Team	Blue Team
WLAN	WLAN is a network that connects two or more computers using a wireless distribution mechanism. They have high-frequency radio waves and an internet access point (AP).
©Certcop	©Certcop
Blue Team	Blue Team
WWAN	WWAN is a WAN with the addition of wireless connection. It offers wireless coverage on a regional, national, and global scale.
©Certcop	©Certcop
Blue Team	Blue Team
WMAN	WMAN is a wireless metropolitan area network capable of covering an entire city. It is larger than WLAN but smaller than WWAN. WMAN is controlled by any corporate or public entity.
©Certcop	©Certcop

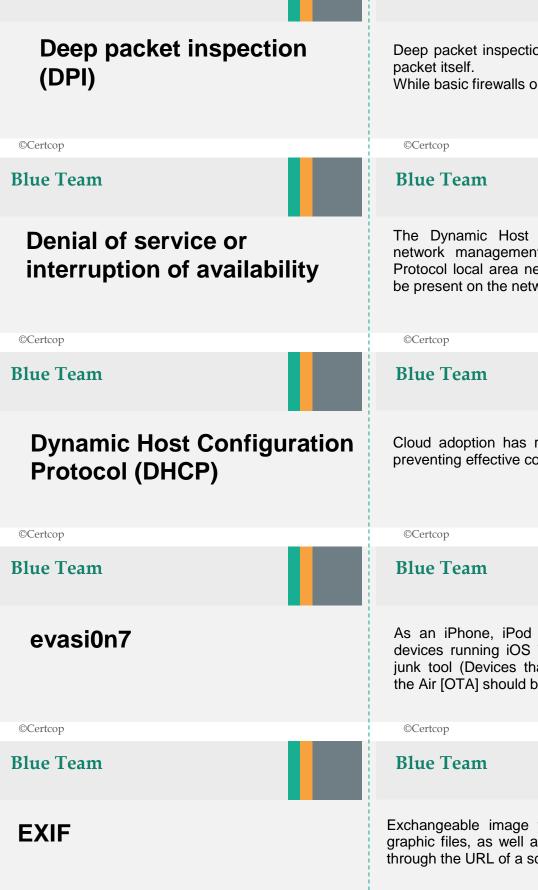












Blue Team



Deep packet inspection examines the data within the packet itself.

While basic firewalls only look at packet headers.



The Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol local area networks. A DHCP server must be present on the network.



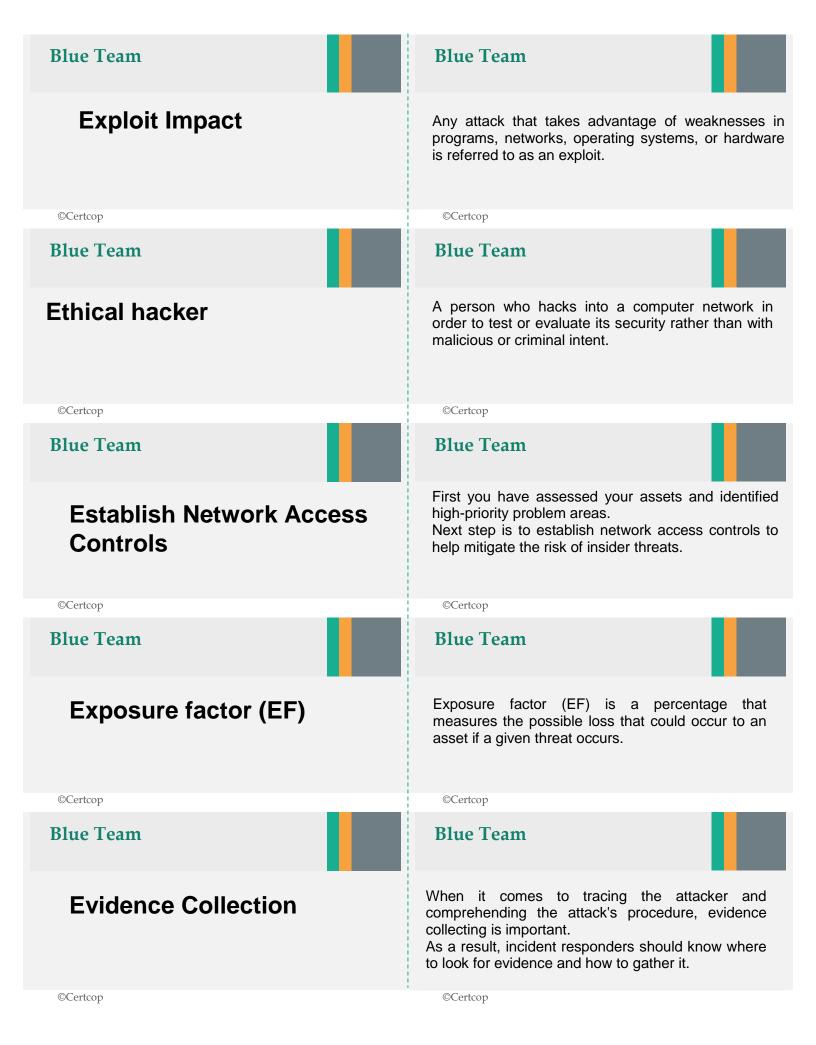
Cloud adoption has removed many of the barriers preventing effective collaboration at distance.

As an iPhone, iPod touch, iPad, and iPad mini devices running iOS 7.0 to 7.0.6 is suitable as a junk tool (Devices that have been updated Over the Air [OTA] should be restored with iTunes first).



Exchangeable image file format information from graphic files, as well as the information discovered through the URL of a scanned website.

Blue Team



Blue Team	Blue Team
IEEE 801.11	IEEE 802.11 refers to a set of standards that define wireless LAN communication (wireless local area networks, or WLANs). Consumers refer to the technology behind 802.11 as Wi-Fi.
©Certcop	©Certcop
Blue Team	Blue Team
ksh	The Korn Shell provides a particularly strong scripting language.
©Certcop	©Certcop
Blue Team	Blue Team
Media Protection (MP)	These policies define how to use, store, and transmit data while ensuring its confidentiality and integrity.
©Certcop	©Certcop
Blue Team	Blue Team
Manage user identities	IAM systems can be the sole directory used to create, change, and delete users. Identity and access management can also be used to generate new identities.
©Certcop	©Certcop
Blue Team	Blue Team
MTransference	Finally, you can transfer the risk onto another party. Naturally, this will usually require some form of trade-off (or cost). Shifting the consequence of a risk to a third party is not always easy but is often overlooked.
©Certcop	©Certcop



Blue Team	Blue Team
©Certcop	Malicious code that is intended to take full or partial control of a system at the lowest level (core or kernel). They often hide themselves from monitoring or detection and modify system files. Most rootkit infections install back trapdoors, spyware, or other malicious codes once they gain control of the target system. ©Certcop
Blue Team	Blue Team
SolarWinds	Easily scan your network devices' firmware for reported CVEs that can help to keep your network secure and compliant. Keep devices current and stay ahead of network vulnerabilities
©Certcop	©Certcop
Blue Team	Blue Team
Secure Hash Algorithm 3. (SHA-3).	A user then logs in using a username and password.
©Certcop	©Certcop
Blue Team	Blue Team
Wireless Networks Threats	Because of the ubiquitous usage of the internet, we can perform our business procedures online and without being constrained by cables and wires. Wireless networks are one of the relatively new technologies that the internet has introduced into our lives.
©Certcop	©Certcop
Blue Team	Blue Team
Zero-day exploits	Start an attack on a mobile OS or app, taking advantage of an undiscovered vulnerability.

Blue Team	Blue Team
Zero-day assaults	Given the impossibility of flawless security, businesses should supplement vulnerability management and shielding with more effective monitoring.
©Certcop	©Certcop