CERTCOP

CERTIFIED CYBER COP

Blue Team

Certcop CertTips

CERTCOP

BLUE TEAM CERTIFIED - DEFENSIVE SECURITY

www.Certcop.com

Android Rooting

Rooting is a Linux word syntax term.
This indicates that the user has the special privilege of using a mobile phone.
Users may take control of their phone's SETTINGS, FEATURES and PERFORMANCE.

Application Framework

It offers numerous key classes for the creation of an Android app.
It offers a general summary of hardware access and helps to manage application resources in the user interface.

Android architecture

It comprises many components to satisfy all the requirements of Android devices.
An open-source Linux kernel with a set of C/C++ library

Android Device Hacking

As these gadgets serve a wide range of functions, the number of individuals using smartphones and tablets is rising quickly. It is a platform that is accessible to all apps. Android is the most popular mobile OS.

Availability

IT refers to the ability of a user to access information or resources in a specified location and in the correct format.

Android OS

Blue Team

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

Blue Team

Android OS Architecture

©Certcop

Blue Team

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

Blue Team

Active Network Threats

©Certcop

Blue Team

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

Blue Team

Application-level filtering

©Certcop

Blue Team

Email filters and web proxies are examples of application level filters.These act as proxies for one or more services.

©Certcop

Blue Team

Anomaly Detection

©Certcop

Blue Team

These systems that look for unusual changes in behaviour patterns to detect uncatalogued attacks.

©Certcop

Blue Team

Android Rooting

Blue Team

Rooting is a Linux word syntax term.
This indicates that the user has the special privilege of using a mobile phone.
Users may take control of their phone's SETTINGS, FEATURES and PERFORMANCE.

Blue Team

Android architecture

Blue Team

It comprises many components to satisfy all the requirements of Android devices.
An open-source Linux kernel with a set of C/C++ library

Blue Team

Availability

Blue Team

IT refers to the ability of a user to access information or resources in a specified location and in the correct format.

Blue Team

Adware

Blue Team

Software that automatically displays or downloads advertisements. While not all adware is malicious, many of such are associated with spyware and other types of malicious software (malware).

Blue Team

Agencies in third-party

Blue Team

They are the responsible for selecting a cloud service, Leveraging the FedRAMP Process and Requiring CSPs to meet FedRAMP requirements.

Blue Team

Awareness and Training (AT) in security control

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.

Blue Team

Audit and Accountability (AU)

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.

Blue Team

Access Control (AC)

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.

Blue Team

Asset Inventory

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

Blue Team

Asset management systems

Blue Team

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

Blue Team

Application Scanner

Blue Team

Applications vulnerability scanners test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications.

Blue Team

Acunetix

Blue Team

It's a comprehensive web application security testing solution that can be used on its own or in conjunction with other tools in a complicated context.

Blue Team

Aircrack-ng

Blue Team

Aircrack-ng is a complete suite of tools to assess WiFi network security.

Blue Team

Attacking in Aircrack-ng

Blue Team

Replay attacks, de-authentication, fake access points and others via packet injection

Blue Team

Access Point (AP)

Blue Team

A wireless access point (AP) is a network device that sends and receives data via a wireless local area network (WLAN). The WLAN and a fixed wire network are connected through the wireless access point.

Blue Team

Angry IP Scanner

Blue Team

The program may also provide access to the shared resources discovered during the scan through HTTP, HTTPS, FTP, or shared folders. IP Range, Random or file in any format Exports results into many formats.

Blue Team

Acrylic Scanner

Blue Team

Acrylic WIFI is a free Windows WIFI scanner. The dashboard displays real-time WIFI statistics. Acrylic WIFI allows you to enhance AP coverage and identify channel interference issues.

Blue Team

Authorizing users

Blue Team

Access management guarantees that a person receives the exact level and type of access. Users can also be divided into groups or roles.

Blue Team

Authenticating users

Blue Team

IAM systems verify a user's identity by validating that they are who they claim to be.
Today, safe authentication entails multi-factor authentication (MFA) and, ideally, adaptive authentication.

Blue Team

Access management

Blue Team

Access management uses information about your identification to determine which software suites you have access to and what you can do with them.

Blue Team

AWS identity and access management

Blue Team

It is simply AWS's IAM mechanism. AWS IAM allows you to create AWS users and groups and grant or deny them access to AWS services and resources.

Blue Team

Ash shell

Blue Team

The Almquist shell is a lighter version of bash shell.

Blue Team

Antivirus

Blue Team

Software protects systems from internal threats by detecting and detecting dangerous files and viruses.

Blue Team

Authentication Techniques

Blue Team

Authentication techniques such as Key Management, Two Factor Authentication, and Automated key Management
It provide the ability to encrypt and decrypt without a centralized key management system and file protection.

Blue Team

ARP POISONING ATTACKS

Blue Team

ARP poisoning is an attack that deceives Computers or switches as to a system's true MAC address.
The physical address, or hardware address, assigned to the NIC is known as the MAC address.

ARP Request

Blue Team

The Address Resolution Protocol (ARP) is a communication protocol for determining the link layer address associated with a given internet layer address, such as a MAC address.

©Certcop

Blue Team

Android architecture

©Certcop

Blue Team

It comprises many components to satisfy all the requirements of Android devices.
An open-source Linux kernel with a set of C/C++ library

©Certcop

Blue Team

ARP Man-in-the-Middle Attacks

©Certcop

Blue Team

An attacker can reroute network data and, in some situations, introduce malicious code in a man-in-the-middle assault.
Normally, communication from the user to the Internet passes through the switch directly to the router.

©Certcop

Blue Team

ARP DDOS Attacks

©Certcop

Blue Team

In a DoS attack, an attacker can also utilize ARP poisoning.
An attacker could transmit an ARP response with a false MAC address for the default gateway.

©Certcop

Blue Team

Amplification Attacks

©Certcop

Blue Team

A sort of DDoS assault is an amplification () attack.
Greatly increases the quantity of traffic sent to or requested from a victim.

©Certcop

Amplification Attack Break Down

A ping is usually unicast, meaning it is sent from one computer to another.
A ping sends ICMP echo queries to one computer and receives ICMP echo responses from the receiving machine.

Annual Loss Expectancy

Annual loss expectancy is a computation that helps you predict the expected monetary loss for an asset due to a specific risk over a single year.
You can compute ALE as part of your company's quantitative cost-benefit analysis for any given investment or project idea.

Annualized Rate of Occurrence (ARO)

The annualized rate of occurrence (ARO) is defined as the probability of a threat occurring in a given year.

Annualized Rate of Occurrence Formula

The following formula is used to determine ALE:
SLE x ARO = ALE
If we know the value of ALE and SLE we can calculate ARO
The formula to find ARO is: ARO = ALE/SLE

ASSET VALUE (AV)

Asset valuation simply pertains to the process to determine the value of a specific property that is conducted usually when a company or asset is to be sold, insured, or taken over.

ASSET MANAGEMENT

Asset tagging is the process of placing physical identification numbers of some sort on all assets.
This can be a simple as a small label that identifies the asset and the owner

Avoidance

Although often not possible, this is the easiest way of removing risk from a project. It involves the removal of the tasks that contain the risk from the project.
Sometimes you can remove a small part of a project which carries a large risk factor.

Acceptance

Acceptance involves planning the risk into the project. If a better response strategy cannot be identified, accepting the risk might be sufficient to proceed with the project.

Air Gap

This means the device has no network connections and all access to the system must be done manually by adding and removing items such as updates and patches with a flash drive or other external device.

Attribute-Based Access Control

Grants or denies user requests based on arbitrary attributes of the user and arbitrary attributes of the object, and environment conditions that may be globally recognized

Active Defence

The deployment of offensive tactics to outwit or slow down a hacker and make hacks more difficult to carry out is known as active defence.
An active cyber defence strategy assists firms in preventing attackers from gaining access to their business networks.

Authentication

The sender and receiver's identities have been verified. The destination/origin of information is also confirmed.

Asymmetric Key Cryptography

A pair of keys is employed in this system to encrypt and decode data.
For encryption, a public key is used, while for decryption, a private key is utilized.

Analysis

Investigators piece together data fragments and develop conclusions based on the evidence uncovered.
It may, however, take several iterations of investigation to substantiate a single crime scenario.

Big Data Era

As the focus moves from how we collect data to how we handle that data in real-time, the Big Data Era is coming to an end. Big Data has evolved into a business asset that will enable multi-cloud support, machine learning, and real-time analytics in the future.

Buffer Overflows

Blue Team

A buffer overflow, also known as a buffer overrun, is a frequent software programming error that an attacker might use to obtain access to your computer..

©Certcop

Blue Team

Bootrom Exploit

©Certcop

Blue Team

A jailbreak bootrom may break all authentications at low levels such as file system, iBoot, and NOR (custom boot logos).

©Certcop

Blue Team

Backdoors

©Certcop

Blue Team

Usually created by software developers for an emergency entry into a system

©Certcop

Blue Team

Blue Keep

©Certcop

Blue Team

Blue Keep is a Microsoft RDP vulnerability that allows attackers to remotely log in to a victim's computer.

©Certcop

Blue Team

Business impact analysis (BIA)

©Certcop

Blue Team

A business impact analysis (BIA) is the process of assessing the criticality of business activities and the corresponding resource requirements in order to maintain operational resilience and continuity during and after a business disruption.

©Certcop

Business continuity planning

Blue Team

The process of developing a framework for preventing and recovering from potential risks to a corporation is known as business continuity planning (BCP).

©Certcop

Blue Team

Bash

©Certcop

Blue Team

Bash is a Unix shell and command language created by Brian Fox as a free software substitute for the Bourne shell for the GNU Project.

©Certcop

Blue Team

Bourne shell

©Certcop

Blue Team

The Bourne shell was one of the major shells used in early versions and became a de facto standard

©Certcop

Blue Team

Bashrc File

©Certcop

Blue Team

When a user signs in, the.bashrc file is executed as a script. The file itself contains a number of terminal session configurations. Coloring, completion, shell history, command aliases, and other features can all be set up or enabled in this way.

©Certcop

Blue Team

Background Processes

©Certcop

Blue Team

Background and do not require user involvement. As an example, consider antivirus software.

©Certcop

Blue Team

Birthday Attack

Blue Team

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

Blue Team

Buffer Overflow

©Certcop

Blue Team

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

Blue Team

Blanket Purchase Agreement (BPA)

©Certcop

Blue Team

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

Blue Team

Computer Forensics

©Certcop

Blue Team

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

Blue Team

Cloud Carrier

©Certcop

Blue Team

A cloud carrier serves as an intermediary between cloud consumers and cloud providers, providing connectivity and transfer of cloud services.

©Certcop

Cross-functional team

The team not only assists with ongoing oversight and maintenance, including technical control.
Each team member should have clear responsibilities and objectives.

Communications Lead

Leads the effort on messaging and communications

Commands and utilities

There are a variety of commands and utilities that you can utilize in your daily tasks.
Commands and utilities include cp, mv, cat, and grep, etc,.

Crunch

To crack a password, we must test a large number of passwords until we find the one that works.
There is no guarantee that any of those millions of possibilities will work.

Cloud Security Alliance CSA)

Cloud Security Alliance is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.”

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>

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

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

Blue Team

chown

The chown command stands for "change owner" and is used to change the owner of a file.

©Certcop

Blue Team

chgrp

The chgrp command stands for "change group" and is used to change the group of a file.

©Certcop

Blue Team

Clicking Jacking

Blue Team

Fooling people to click something else they believe they click. Attackers obtain sensitive information or take device control

Blue Team

Config Manipulation

Blue Team

Apps can utilize external files and libraries, alter them, or influence the ability of apps to manipulate the settings.

Blue Team

Carrier-loaded Software

Blue Team

Pre-installed software or apps on devices may be vulnerable to criminal actions, such as deleting, altering, stealing of device data, wake-up calling, etc.

Blue Team

Cold boot attack

Blue Team

An attack method developed nearly a decade ago by Princeton University researchers who demonstrated the potential to recover disk encryption keys from random access memory (RAM) when the device's power is cycled in cooled or frozen temperatures.

Blue Team

Create phase

Blue Team

Data will continue to be generated in the cloud and by remote users.

CSPs (Cloud Service Providers)

Provide the actual cloud service to an Agency
Must meet all FedRAMP requirements before they implement their services.

CIO Council

Disseminates FedRAMP information to Federal CIOs and other representatives through cross agency communications and events

Compliance

A Cloud Service Provider can submit the appropriate documentation to the FedRAMP PMO and to an agency which may grant an agency "Authority to Operate" (ATO).
Using FedRAMP mechanisms, other agencies can

Cloud Pentesting

Cloud Penetration Testing is a permitted simulated cyber-attack against a system that is hosted on a Cloud provider. Amazon's AWS

Configuration Management (CM)

Configuration management (CM) is a systems engineering technique for ensuring that a product's performance, functional, and physical properties are consistent with its requirements, design, and operational data throughout its lifecycle.

Contingency Planning (CP)

Blue Team

In project management, a contingency plan is a specified, actionable plan that will be implemented if a recognized risk materializes. It's essentially a "Plan B" that's put in place when things don't go as planned.

©Certcop

Blue Team

Cross-site scripting (XSS)

©Certcop

Blue Team

A very common web application vulnerability that can lead to installation or execution of malicious code, account compromise, session cookie hijacking, revelation or modification of local files, or site redirection. There are three major types of XSS: reflected XSS, stored (persistent), and DOM-based XSS.

©Certcop

Blue Team

Concise

©Certcop

Blue Team

Content and complexity is relevant to the audience; No superfluous words or phrases

©Certcop

Blue Team

Consistent

©Certcop

Blue Team

Terms have the same meaning throughout the document; Items are referred to by the same name or description throughout the document; The level of detail and presentation style is the same throughout the document

©Certcop

Blue Team

Complete

©Certcop

Blue Team

Responsive to all applicable FedRAMP requirements; The Security Package Includes all appropriate sections of FedRAMP Template; the Security Package Includes all attachments and appendices

©Certcop

Blue Team

CVE (Common Vulnerabilities and Exposures)

Blue Team

The Common Vulnerabilities and Exposures (CVE) dictionary is a collection of common names) for publicly known information security flaws. CVE's standard IDs make it easier to communicate data between different network security databases and tools.

Blue Team

CVSS (Common Vulnerability Scoring System)

Blue Team

CVSS is an open framework for conveying IT vulnerability characteristics and implications.
Its quantitative technique enables consistent, precise measurement.

Blue Team

CWE (Common Weakness Enumeration)

Blue Team

It is a method of identifying weaknesses in a group of people. CWE establishes a common vocabulary for discussing, identifying, and resolving.

Blue Team

Config Manipulation

Blue Team

Apps can utilize external files and libraries, alter them, or influence the ability of apps to manipulate the settings.

Blue Team

Cloud Security Alliance (CSA)

Blue Team

Cloud Security Alliance is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.”

Blue Team

Conduct Root Cause Analyses

Blue Team

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

©Certcop

Blue Team

Condition-Based Maintenance (CBM)

©Certcop

Blue Team

This maintenance strategy uses technology-based diagnostics—vibrations, temperature, pressure, speed,

©Certcop

Blue Team

Central identity management

©Certcop

Blue Team

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

Blue Team

C shell

©Certcop

Blue Team

The C shell was developed by Bill Joy for the Berkeley Software Distribution
Its syntax is modelled after the C programming language.

©Certcop

Blue Team

Controlling Jobs

©Certcop

Blue Team

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

Cybersecurity Risk Mitigation

Blue Team

Because the potential of a cyber-assault is almost certain, proactive cybersecurity risk mitigation is increasingly becoming the only option for enterprises.

Blue Team

Cybersecurity Research

Blue Team

Cybersecurity Research is the area that is concerned with preparing solutions to deal with cyber criminals.
With increasing amount of internet attacks, advanced persistent threats and phishing,

Blue Team

Clickjacking

Blue Team

Users are tricked into clicking something other than what they think they're clicking by clickjacking.

Blue Team

Customer-based SLA

Blue Team

Applies to all contracted services by a customer, a group of customers or the same business area.

Blue Team

Clean Desk Policy

Blue Team

A clean desk policy instructs that all employees must clear their desks at the end of each work day. This not only includes documents and notes, but any post-it notes, businesses cards, and removable media (e.g. USB memory sticks).

Control plane

This plane carries signaling traffic originating from or destined for a router.

Change Management

All networks evolve, grow, and change over time. Companies and their processes also evolve and change, which is a good thing.
But infrastructure change must be managed in a structured way so as to maintain a common sense of purpose about the changes.

Centralized model

All desktop instances are stored in a single server, which requires significant processing power on the server.

Containerization

Containerization is a technique in which the kernel allows for multiple isolated user space instances.
The instances are known as containers, virtual private servers, or virtual environments.

Cloud Access Security Broker (CASB)

A cloud security broker, or cloud access security broker (CASB), is a software layer that operates as a gatekeeper between an organization's on-premises network and the provider's cloud environment

Certificate Management

Blue Team

Certificate management is the process of managing digital security certificates.
Certificate authorities are responsible for certificate management and serve as a registration authority for subscriber certificates.

©Certcop

Blue Team

Cryptography

©Certcop

Blue Team

Cryptography is the use of codes to secure information and communications.
Only the individual to whom the information is directed can understand and process it.

©Certcop

Blue Team

Confidentiality

©Certcop

Blue Team

Only the individual for whom the information is meant has access to it, and no one else has access to it.

©Certcop

Blue Team

Digital Forensics

©Certcop

Blue Team

The process of preserving, identifying, extracting, and documenting computer evidence.
It is the science of extracting information from digital media.

©Certcop

Blue Team

Digital Evidence

©Certcop

Blue Team

Any type of data stored and gathered from any electronic storage device is referred to as digital evidence.
Wireless networks and random-access memory can also be used to recover digital evidence.

©Certcop

Documentation

Blue Team

This method necessitates the creation of a record of all visible data. It aids in the recreation and analysis of the crime scene.
It entails photography, sketching, and crime-scene mapping, as well as adequate documenting of the crime scene.

©Certcop

Blue Team

Database Forensics

©Certcop

Blue Team

Database forensic experts look into any database access and report any changes to the data.
Database forensics can be used to investigate large-scale financial crimes and verify business contracts.

©Certcop

Blue Team

Disk Forensics

©Certcop

Blue Team

The science of extracting forensic evidence from digital storage media such as hard disks, USB devices, CD, DVD, Flash drives, and floppy disks is known as disk forensics.

©Certcop

Blue Team

Disk analysis

©Certcop

Blue Team

Analysts that specialize in disk forensics ensure that all pertinent data is retrieved, processed, and presented as evidence.

©Certcop

Blue Team

Directories

©Certcop

Blue Team

Directories are used to organize both unique and common files.

©Certcop

Data Caching

Caching in mobile devices used to interact with web apps, attackers attempt to exploit the data caches

Destroy phase

Furthermore, we would need to delete data from the production process and then sanitise the media.

Digital Authentication

The process of establishing confidence in user identities presented digitally to a system, which was previously referred to as Electronic Authentication (E-Authentication)

Dynamic Runtime Injection

Attackers handle and misuse a program to overcome security locks, logic checks, rights access sections of the app, and rob data Runtime Injection.

DNS Poisoning

Attackers utilize DNS servers, forward website users to another attacker's website DNS Poisoning.

Blue Team

Data Centers

Blue Team

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.

Blue Team

Data Dumping

Blue Team

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

Blue Team

Dr.Fone

Blue Team

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,

Blue Team

Denial-of-Service

Blue Team

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.

Blue Team

Database models

Blue Team

Describes relationships between data elements
Used to represent the conceptual organization of data
Formal methods of representing information

Distributed Database models

Blue Team

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

Blue Team

Data dictionary

©Certcop

Blue Team

A Data Dictionary is a list of names, definitions, and properties for data elements in a database, information system, or research project.

©Certcop

Blue Team

Data Marts

©Certcop

Blue Team

Often regional collection of information from databases.

©Certcop

Blue Team

Data Warehouse

©Certcop

Blue Team

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

Blue Team

Data mining

©Certcop

Blue Team

Data mining is a technique for extracting and detecting patterns in huge data sets that combines machine learning, statistics, and database systems.

©Certcop

Data Portability

The ability to transfer data from one system to another without being required to recreate or re-enter data descriptions or to modify significantly the application being transported.

Degrees Monitoring (DLP)

Which involves looking at data as it exits the production environment. These are commonly referred to as DLPs.

DNS Poisoning

Attackers utilize DNS servers, forward website users to another attacker's website DNS Poisoning.

Database scanners

Database vulnerability scanners identify the weak points in a database so as to prevent malicious attacks

Data Security on Wireless Networks

Identify a wireless network within close proximity is a wireless-enabled computer.
There is no way to intentionally hide your networks.

Data Encryption

WPA and WPA2 are both viable options, but longer and more complicated passwords give better security
If You are putting your business or personal data at risk, encryption should be considered necessary.

Disaster recovery strategy

A disaster recovery plan (DRP), also known as a disaster recovery implementation plan or an IT disaster recovery plan, is a documented policy and/or process that helps an organization execute recovery processes in the event of a disaster.

Dash shell

The Debian Alquist Shell is the default shell script in Ubuntu.
While bash is the default login and interactive shell, dash is used to run system processes because it's much lighter than bash.

Data Caching

Caching in mobile devices used to interact with web apps, attackers attempt to exploit the data caches

DNS Attacks

DNS is a service that converts host names to IP addresses.
Users will no longer need to remember web site IP addresses as a result of this.
Reverse lookups are also available through DNS.

DNS Poisoning Attacks

Blue Team

DNS poisoning is a type of attack that tries to change or corrupt DNS results.
The rogue website's IP address is returned by the DNS server.

©Certcop

Blue Team

DDoS DNS Attacks

©Certcop

Blue Team

Individual systems are forced to become bots within huge botnets by Mirai.
They transmitted commands to millions of infected devices. It was instructing them to send queries to DNS servers over and over again.

©Certcop

Blue Team

Dictionary Attacks

©Certcop

Blue Team

One of the first password assaults was a dictionary attack. It makes use of a word dictionary and tries every word in it to check if it works.
A dictionary is essentially a list of words and letter combinations in this context.

©Certcop

Blue Team

Domain Hijacking

©Certcop

Blue Team

An attacker changes the registration of a domain name without the owner's permission in a domain hijacking assault.
Social engineering tactics are frequently used by attackers to get illegal access to the domain owner's email account.

©Certcop

Blue Team

Driver Manipulation

©Certcop

Blue Team

Drivers are used by operating systems to interact with hardware and software components.
An application may need to support an older driver on occasion.

©Certcop

DLL Injection

Blue Team

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

Blue Team

Data Ownership Policy

©Certcop

Blue Team

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

Blue Team

Data plane

©Certcop

Blue Team

Also known as the forwarding plane, this plane carries user traffic.

©Certcop

Blue Team

Data Security

©Certcop

Blue Team

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

Blue Team

Dissemination

©Certcop

Blue Team

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

Blue Team

Digital Certificate

Blue Team

A digital certificate is a file that contains a variety of data, including identifying information, a serial number, and expiration dates.
It also contains the digital signature of the certificate authority that issued the certificate.

Blue Team

Email Forensics

Blue Team

Analysts that specialize in email forensics extract valuable information from emails.
Senders and receivers, the content of the messages, time stamps, sources, and metadata are all examples of this information.

Blue Team

Evasi0n7

Blue Team

Evasi0n7 is 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).

Blue Team

Evidence Collection

Blue Team

When it comes to tracing the attacker and 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.

Blue Team

Escalated privileges

Blue Team

Attackers engage in escalation privilege assaults that take advantage of design flaws, programming mistakes, bugs, etc.

Blue Team

Electricity

Blue Team

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 non-renewable.

Blue Team

Eavesdropping

Blue Team

Eavesdropping attacks are comparable to sniffing 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.

Blue Team

Eavesdropping attacks

Blue Team

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.

Blue Team

Encryption

Blue Team

Encoding data to hide it from anyone who isn't authorized to see it.
A decryption key can be used to access or decrypt encrypted data.

Blue Team

Evil Twin

Blue Team

Attackers obtain a wireless access point and 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

Employers Background Checks

Blue Team

Background checks assist you in assembling a team you can rely on, while also limiting risk and safeguarding your company's brand.

Blue Team

Exit Interview

Blue Team

An exit interview is a survey that is undertaken with an employee when he or she departs a company.

.

Blue Team

Extranet

Blue Team

A category describing the strength of the authentication process.

Blue Team

Electronic Identity

Blue Team

A publicly available digital certificate that includes a public key and a private key.
When used together, this acts like a digital passport: it may be used to confirm the identification of a person or service.

Blue Team

Forensics Data analysis

Blue Team

Structured data is analyzed in this branch of forensics.
The primary role of data analysts is to investigate financial crimes and fraud.

Forensic Analysts

Blue Team

Forensic analysts are in charge of gathering and/or analyzing crime scene evidence in order to learn more about the perpetrator or to include or exclude a certain person as a potential suspect.

©Certcop

Blue Team

Files and Directories

©Certcop

Blue Team

Organize all of Unix's data into files. After that, all of the files are arranged into directories

©Certcop

Blue Team

File Editor

©Certcop

Blue Team

The nano command is use to edit text files.
Command: nano <file name>

©Certcop

Blue Team

File Permission / Access Modes

©Certcop

Blue Team

File ownership is an important feature of Unix that allows for safe file storage. Owner permissions dictate what activities the file's owner is allowed to take on the file.

©Certcop

Blue Team

Firewall

©Certcop

Blue Team

A firewall is a network security device that monitors incoming and outgoing network traffic.
Also allows or disallows data packets according to a set of security rules.

©Certcop

Firewall Types

Blue Team

- Software or hardware firewalls Jailbroken iPhones
- Packet-filtering firewalls Mobile Malware
- Next-generation firewalls (NGFW)
- Proxy firewalls
- Network address translation (NAT) firewalls

©Certcop

Blue Team

Filter Table

©Certcop

Blue Team

Filter is default table for iptables. So, if you don't define you own table, you'll be using filter table.

©Certcop

Blue Team

Framing

©Certcop

Blue Team

Website combined with iFrame components in HTML in another webpage
Drive By Downloading: unintentional Internet download of software. This exploit affects Android

©Certcop

Blue Team

FIDO Alliance

©Certcop

Blue Team

FIDO Authentication enables password-only logins to be replaced with secure and fast login experiences across websites and apps.

©Certcop

Blue Team

Formal methods developed

©Certcop

Blue Team

Formal methods are mathematical entities that are used to model complex systems. Designers can not only validate the system's attributes in a more thorough manner but also use mathematical proof.

©Certcop

Foreign Keys

Blue Team

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

File

Blue Team

A file is a computer object that holds data, information, settings, or commands that are utilized with a software.

©Certcop

Fedramp

Blue Team

It is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

©Certcop

Fedramp Needed

Blue Team

The Federal Government spends hundreds of millions of dollars a year securing the use of IT systems Cloud solutions allow for faster processing

©Certcop

FedRAMP Program Management Office

Blue Team

Established within the GSA and responsible for the development of the FedRAMP program.

©Certcop

FIPS 199

Blue Team

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

Blue Team

FedRAMP Assignments

©Certcop

Blue Team

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

Blue Team

Factors that can affect RPO

©Certcop

Blue Team

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

Blue Team

Fish shell

©Certcop

Blue Team

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

Blue Team

Foreground Processes

©Certcop

Blue Team

They run on the screen and require user input. For example Office Programs

©Certcop

Facilitate communication

The service desk team or the service provider know the customer's expectations.

Federation

A federated identity is a portable identity that can be used across businesses and domains.

Goals of Fedramp

Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations
Increase confidence in security of cloud

Governance

The governance of FedRAMP is comprised of different executive branch entities that work in a collaborative manner to develop, manage, and operate the program.

General Services Administration (GSA)

The GSA is in charge of collecting, storing, distributing, and disposing of personal property and supplies, as well as real estate acquisition, management, and disposal.

Blue Team

Honey trap

©Certcop

Blue Team

In this assault, the social engineer disguises himself as an attractive person in order to engage with a person online, create an online relationship, and acquire sensitive information through that interaction.

©Certcop

Blue Team

Hierarchical Database models

©Certcop

Blue Team

A hierarchical database is a data architecture in which data is organized into a tree-like structure, or parent-child structure, in which one parent node can have numerous child nodes connected through links.

©Certcop

Blue Team

Host-based scanners

©Certcop

Blue Team

Host-based vulnerability scanners are used to locate and identify vulnerabilities in servers, workstations, and other network hosts.
It also provides further visibility into the scanned systems' configuration settings and patch history.

©Certcop

Blue Team

Host Based IDS

©Certcop

Blue Team

HIDS tools monitor the log files generated by your applications, creating a historical record of activities and functions allowing you to quickly search them for anomalies and signs an intrusion may have occurred.

©Certcop

Blue Team

Hydra Password Attacks

©Certcop

Blue Team

Hydra is a parallelized password cracker that can attack a variety of protocols. It's quick and adaptable, and adding new modules is simple. Researchers and security consultants can use this program to demonstrate how simple it is to acquire unauthorized remote access to a system.

©Certcop

Hosted model

Blue Team

Desktops are maintained by a service provider. This model eliminates capital cost and is instead considered operational cost.

©Certcop

Blue Team

Honeypot

©Certcop

Blue Team

A honeypot is a security technique that generates a virtual trap in order to entice intruders.
A purposely infiltrated computer system allows attackers to exploit weaknesses, allowing you to research them and enhance your security measures.

©Certcop

Blue Team

Hash Functions

©Certcop

Blue Team

A hash value with a fixed length is calculated based on the plain text, making it impossible to reconstruct the plain text's contents.
Many operating systems encrypt passwords using hash algorithms.

©Certcop

Blue Team

Identification

©Certcop

Blue Team

In the forensic process, it is the initial stage.
What evidence is present, where it is held, and how it is stored are all part of the identification process. Personal computers, mobile phones, and personal digital assistants (PDAs) are examples of electronic storage medium.

©Certcop

Blue Team

Incident Response

©Certcop

Blue Team

Incident response, also known as IT incident, computer incident, or security incident.
It is a structured way to dealing with and managing the consequences of a security breach or cyberattack.

©Certcop

Importance of Incident Response

Most businesses rely on sensitive information.
Simple malware infections to unsecured employee laptops
Any of these situations can have both short- and long-term consequences.

Incident Response Team

Incident response team (CSIRT) assists in reducing the impact of security risks by responding quickly and effectively. Due to the increasing amount of security risks, companies must have a specialized incident response team to deal with them.

Incident response team Responsibilities

- create and maintain an IR plan
- Analyze the security incident
- Manage internal communications and alerts
- Offer easy communication with stakeholders
- Recommend tools, technologies, policy, and governance after the incident

Incident Response Manager

In the detection, analysis, containment, and recovery stages, he monitors the entire process and assigns priorities to the various activities.

Incident Response Plan Management

The response to an incident is similar to any other component of information security.
To be adequately measured, it takes careful planning, continual management, and defined metrics.

Indicators of Compromise (IOC)

Blue Team

These detect potentially malicious behaviour on a system or network
Information security and IT workers can use indicators of compromise.

Blue Team

Incident Response Tools

Blue Team

- SIEM (Security information and event management)
- Intrusion Detection Systems (IDS)
- Netflow Analyzers
- memdump

Blue Team

Intrusion Detection Systems (IDS)

Blue Team

If a server, a host-based intrusion detection system (HIDS), or a network-based intrusion detection system detects suspicious behavior or known assaults, the system will send an alert to the appropriate party (NIDS).

Blue Team

IP TABLES

Blue Team

Packet filtering and NAT rules are managed by the iptables firewall.
IP Tables is included in every Linux distribution.

Blue Team

Infecting the device

Blue Team

Mobile spyware infects the device on Android and iOS smartphones differently.

Infection with iOS

iOS requires physical mobile access. A null-day operation like the JailbreakME hack can also infect the device.

Interoperability

The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions

Installing a backdoor

For installing the backdoor, the rooting of Android devices and Apple jailbrakings requires admin access.
Despite rooting/jamming methods by device makers, mobile spyware may simply overcome them.

Improper SSL validation

Security Laps in applications The process of SSL validation can allow attackers to bypass data security

iOS Jailbreaking

Jailbreaking controls the iOS system used on Apple devices, the symmetry of rooting of Android devices in simple language.
It removes the device from Apple source dependencies and allows you to utilize non-existent third-party programs from the official app store.

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.

Ios 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

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.

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.

Inheritance

Objects inherit attributes and behaviors from super class

Identity Management

Blue Team

Identity management is the method of associating user rights with a given identity to grant individuals access to system services.

©Certcop

Blue Team

Input validation

©Certcop

Blue Team

Input validation ensures that only properly formed data enters an information system's process, preventing flawed data from remaining in the database and causing downstream components to malfunction.

©Certcop

Blue Team

Initial

©Certcop

Blue Team

Development based on Ad Hoc effort. No procedures in place and there is no assurance of consistency; thereby affecting software quality.

©Certcop

Blue Team

Interoperability

©Certcop

Blue Team

The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions

©Certcop

Blue Team

IOT Devices

©Certcop

Blue Team

IoT is an Internet-connected gadget which can interact with other devices and networks.
Depending on their design and functions, these gadgets may do a wide range of activities.

©Certcop

Identification of vulnerabilities

Vulnerability scanning is the most common method of detecting flaws, and the effectiveness of a scanner is determined by two factors:
The scanner's capacity to discover and identify devices, software, and open ports, as well as acquire other system data

IEEE 802.11b-1999 (802.11b)

This technology supports up to 11Mbps transmission and is backward compatible.

IEEE 802.11g-2003 (IEEE 802.11g)

This is a popular technology that offers up to 54Mbps and a range of 150 feet.

IEEE 802.11n-2009 (IEEE 802.11n)

This technology seeks to improve throughput in the 2.4GHz to 5GHz frequency band. It employs several antennas, which boosts data speeds.

inSSIDer

inSSIDer is comparable to the old Net Stumbler tool, except that it has been updated and works with Windows XP, Vista, and Windows 7.
The program detects wireless networks and reports on their kind, maximum transfer rate, and channel utilization.

IP addresses

Blue Team

The Internet Protocol (IP) is a set of standards and specifications for producing and transferring data packets, or datagrams, across networks. The Internet Protocol (IP) is a component of the Internet protocol suite's Internet layer.

©Certcop

Impact of Incidents

Blue Team

The impact and immediacy of an incident are frequently used to evaluate its priority.
The term 'Impact' refers to the scope of the Incident as well as the potential damage caused by the Incident before it can be remedied.

©Certcop

Improve PM Processes

Blue Team

An effective PM program can drastically increase MTBF

©Certcop

Identity and Access Management

Blue Team

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.

©Certcop

iBoot Exploit

Blue Team

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. This is used mostly for reducing iOS controls at low level.

©Certcop

Identity management

Blue Team

Identity management ensures that you are who you say you are and stores information about you. An identity management database stores information about your identity.

©Certcop

Integrate Overflow

Blue Team

An integer overflow attack tries to use or produce a numeric value that an application can't handle.
As a result, the application produces incorrect results.

©Certcop

Improve the service provided

Blue Team

Reduced incident resolution or request delivery times

©Certcop

Identify the hazards

Blue Team

The first step to creating your risk assessment plan is determining what hazards your employees and your business face

©Certcop

Intranet

Blue Team

An intranet is a private network within a corporation that allows employees to safely communicate information.

©Certcop

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.

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.

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.

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.

Jamming

The goal of jamming (also known as network interference) is to interrupt the network.
Interference is almost unavoidable due to the wireless characteristics.

John the ripper

It is a fantastic program for breaking passwords.
Well-known brute-force techniques such as dictionary and bespoke wordlist attacks.
It can also be used to crack hashes or passwords for zipped or compressed data, as well as locked files.

Blue Team

Job rotation

A policy that requires employees to rotate into various jobs, or at least rotate some of their responsibilities.
It provides numerous advantages for both the person and the organization.

©Certcop

Blue Team

Jump box

A jumpbox, or jump server, is a server that is used to access devices that have been placed in a secure network zone such as a DMZ.

©Certcop

Blue Team

Known Plaintext Attacks

If an attacker obtains samples of both the plaintext and the cipher text, he can execute a known plaintext assault.
Attacker can use the same decryption procedure on other cipher text if he succeeds.

©Certcop

Blue Team

Lead Investigator

Collects and analyses all evidence
Implements rapid system and service recovery.

©Certcop

LINUX+

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.

ls

You can use the ls command to list out all the files or directories available in a directory.
Command: ls

Linux Kernel

The core of the Android architecture is Linux Kernel.
It manages all drivers accessible, such as Display controls, Camera ports, etc.

Leveraging and Authorization

Shows the architecture, including the domain architecture, with the existing domain hierarchy, names, and addressing scheme; server roles; and trust relationships.

Logical deployment diagram

The process or action of confirming an identity used to interact with or log in to an information system.

Mobile Device Forensics

Blue Team

Data can be recovered from smartphones, SIM cards, mobile phones, GPS devices, tablets, PDAs, and gaming consoles by specialists in this sector.
This type of analysis is needed to recover audio and visual data, contacts, and call logs from devices used as evidence in court.

©Certcop

Blue Team

Malware Forensics

©Certcop

Blue Team

This branch's experts identify, analyse, and investigate various malware types in order to track down culprits and causes for the attack.
They also assess the extent of the damage produced by the attack and identify the malware's code.

©Certcop

Blue Team

Memory Forensics

©Certcop

Blue Team

Live acquisition is another term for this form of digital forensics. The data is retrieved from RAM.
Hackers can now leave no traces on hard drives thanks to recent advancements in cybercrime technology.

©Certcop

Blue Team

Malware infections

©Certcop

Blue Team

Malware can infiltrate your computer by exploiting known software flaws. A vulnerability is a flaw in your program that allows malware to get access to your computer. When you visit a website

©Certcop

Blue Team

Mangle Table

©Certcop

Blue Team

Iptables’s Mangle table is for specialized packet alteration. This alters QOS bits in the TCP header.

©Certcop

memdump

The memdump plugin is run against the memory image, with the output directed to the home folder

Multi-Tenant Security

Multi-tenancy is a software architecture that uses a single application to serve multiple customers. By using multi-tenancy, you can create one application and then deploy it to as many customers as you want.

Mobile Application Attack Vectors

An Attack Vector is defined as a process or technique used by a hacker to enter another device or network, to inject a so called 'bad code' which is usually termed payload.
This vector enables hackers use system faults

Man in the Middle

Attacker implants malicious code on victim's mobile device
An attacker has connections between two systems across the current network

Message replay

Usage of recorded data at a later period than intended in order to repeat an action that benefits the attacker. Such as the capture and replay of an instruction to transfer funds from a bank account under the attacker's control.

Message manipulation

Blue Team

Changing a packet header address to route it to an unexpected destination or modifying user data are examples of message manipulation.

©Certcop

Blue Team

Masquerade attacks

©Certcop

Blue Team

Masquerade attacks involve an entity adopting a false persona in order to get or manipulate information.
As a result, gain unjustified privilege status.

©Certcop

Blue Team

Manage patch application

©Certcop

Blue Team

A solid patch management policy will include regular tracking of patch releases for all software.

©Certcop

Blue Team

Misuse Detection

©Certcop

Blue Team

These systems that look for a signature or defining characteristic of an attack.

©Certcop

Blue Team

Masking

©Certcop

Blue Team

Hiding the data with useless characters; for example, showing only the last four digits of a Social Security number: XXX-XX-1234.

©Certcop

Metadata

Blue Team

"Data about data" gives the data its meaning/context

Blue Team

Mobile Device Security

Blue Team

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.

Blue Team

Monitoring and Reporting

Blue Team

Discovering and monitoring the virtual resources, monitoring cloud operations and events, and generating performance reports

Blue Team

Mitigating Controls

Blue Team

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.

Blue Team

Monitor Baseline

Blue Team

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

Monitoring

Blue Team

Packet capture and export of data to text files for further processing by third party tools

Blue Team

Mobility

Blue Team

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.

Blue Team

MAC address

Blue Team

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).

Blue Team

Mean Time between Failures (MTBF)

Blue Team

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.

Blue Team

Mean Time to Repair (MTTR)

Blue Team

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.

Blue Team

MTTR formula

©Certcop

Blue Team

(Total corrective maintenance time/ Number of repairs) =MTTR

©Certcop

Blue Team

Multi- factor authentication

©Certcop

Blue Team

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

Blue Team

Monitoring and Managing Processes

©Certcop

Blue Team

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.

©Certcop

Blue Team

Man-in-the-Browser

©Certcop

Blue Team

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

Blue Team

Memory Leak

©Certcop

Blue Team

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

Blue Team

Multilevel SLA

Blue Team

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.

Blue Team

Malvertising

Blue Team

The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.

Blue Team

Malware

Blue Team

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.

Blue Team

Metasploit

Blue Team

One of the most popular exploitation frameworks.

Blue Team

Mutual agreement.

Blue Team

The SLA is mutually accepted by the customer and the service provider.

Memorandum of Understanding (MOU)

Blue Team

A memorandum of understanding is an agreement between two or more parties outlined in a formal document.
It is not legally binding but signals the willingness of the parties to move forward with a contract.

©Certcop

Blue Team

Mandatory Vacations

©Certcop

Blue Team

Mandatory vacation regulations, like work rotation, serve as a disincentive to fraud.
Many companies will have a policy requiring employees in sensitive positions to take five or ten days off in a row.

©Certcop

Blue Team

Monitor and Prepare

©Certcop

Blue Team

Similar to accepting the risk, this response can be used for major risks that carry a high probability and/or severity, but must be accepted by the project.

©Certcop

Blue Team

Mitigation

©Certcop

Blue Team

Since risk is a function of probability and severity, both of these factors can be scrutinized to reduce the risk of project failure.

©Certcop

Blue Team

Multifactor Authentication (MFA)

©Certcop

Blue Team

Multifactor Authentication (MFA) uses a password and a code delivered to your smartphone to authenticate yourself is a frequent form of multi-factor authentication.

©Certcop

Mandatory Access Control

In mandatory access control (MAC), subject authorization is based on security labels.

Manual Review

Privileged accounts, regardless of the authentication method or architecture, must be monitored to ensure that these additional rights are not abused.

Monitoring and Logging

Monitoring, also known as application supervision, is the ability to have a global view of an application at any one time as well as a history of prior states for numerous elements:
Performance and response time of various server resources.

Network Forensics

The goal of network forensics is to track, record, and analyse all network activity.
In the event of security breaches, cyberattacks, or other cyber incidents, network specialists examine traffic and activities.

Netflow Analyzers

Actual traffic across border gateways and within a network is examined in this study A specific thread of activity may be tracked using Net flow, as can the protocol utilized on your network or the assets that are talking with one other.

Blue Team

New Directory

Blue Team

The mkdir command is used to create a new directory under any directory.

Command: Mkdir <name>

Blue Team

nano

Blue Team

The nano command is use to edit text files

Command: Nano <file name>

Blue Team

Next-generation firewalls (NGFW)

Blue Team

NAT gates hide individual IP addresses.
As a result, attackers scanning a network for IP addresses are unable to collect detailed details.
In the same way that proxy firewalls function as an intermediate between a group of computers and outside traffic, NAT firewalls do the same.

Blue Team

NAT Table

Blue Team

NAT table is essential for your internet connection. The network address translation (NAT) table is responsible for allowing devices on a private network to connect to a public network, such as the internet.

Blue Team

Network Based IPS

Blue Team

It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy Violations

No encryption / faint encryption

Unsecured or weakly encrypted data transmission applications are capable to attack, for example hijacking session

Network Based Attacks

Network-based attacks aim to compromise network security by intercepting and altering network traffic or spying on it.
These can be active assaults, in which the hacker alters network activity in real time

National Institute for Standards and Technology (NIST)

Advises FedRAMP on FISMA compliance requirements and assists in developing the standards for the accreditation of independent 3PAOs

Network Based IDS

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

NIDS: OSSEC

OSSEC is the world's most popular open-source host-based intrusion detection system (HIDS).

Blue Team

Network-based scanners

Blue Team

On wired or wireless networks, network-based vulnerability scanners discover potential network security assaults and vulnerable systems.
Network-based scanners help determine if there are unknown perimeter points on the network.

Blue Team

Netsparker

Blue Team

Netsparker is an automated, yet fully configurable, web application security scanner that allows you to scan and identify security flaws in websites, web applications, and web services.

Blue Team

Nikto

Blue Team

Nikto is a free command-line vulnerability scanner that looks for dangerous files/CGIs, outdated server software, and other issues on webservers. It runs generic and server-specific checks.

Blue Team

Network devices

Blue Team

In a wireless mesh network, a network device is a node. It can send and receive wireless HART data, as well as execute the fundamental network formation and maintenance activities. Field devices, router devices, gateway devices, and mesh hand-held devices are examples of network equipment.

Blue Team

NMAP

Blue Team

Nmap, or Network Mapper, is a free and open source network discovery and security auditing application.
Use it for activities like network inventory, service upgrade schedule management, and monitoring host or service uptime.

Blue Team

Next Generation Firewall

Blue Team

Next Generation Firewall that offers security intelligence to enterprises and enable them to apply best suited security controls at the network perimeter are also being worked on.

Blue Team

Non-Disclosure Agreement

Blue Team

A non-disclosure agreement (NDA) is a legally binding contract that creates a confidential connection.
The party or parties signing the agreement agree that sensitive information will not be shared with anyone else.

Blue Team

Network Architecture

Blue Team

The way network devices and services are arranged to serve the connectivity demands of client devices is referred to as network architecture. Switches and routers are common network hardware.

Blue Team

Non-repudiation

Blue Team

The creator/sender of information cannot later deny his or her intention to convey information.

Blue Team

Network based point

Blue Team

It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy Violations

New Directory

The mkdir command is used to create a new directory under any directory.

Command: Mkdir <name>

Objectives of Computer Forensics

It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.

It helps to postulate the motive behind the crime and identity of the main culprit.

Ordinary Files

An ordinary file is a file that holds data, text, or program instructions on a computer system.

OUTPUT chain

The output-chain command functions similarly to the next filter term in that it allows several levels of filtering on the interface in both the ingress and egress directions.

Obfuscation

The term "obfuscation" refers to the use of any of these techniques to make data less relevant, detailed, or readable in order to protect the data or the data's subject.

Blue Team

Object oriented technology

Blue Team

Keeps track of objects and entities that contain both data and action on the data
Designed for non-text data such as graphics, video and audio clips
A DB in which the operations carried out on data objects are considered part of their definition

Blue Team

Optimized

Blue Team

Integrated plans for continuous process improvement.

Blue Team

Ongoing Assessment & Authorization

Blue Team

Once an authorization is granted, ongoing assessment and authorization activities must be completed to maintain the security authorization.

Blue Team

Office of Management and Budget Policy (OMB)

Blue Team

The governing body that issued the FedRAMP policy memo which defines the key requirements and capabilities of the program

Blue Team

OBJECTIVES OF THE SSP

Blue Team

The SSP is the main document in which the CSP describes all the security controls in use on the information system and their implementation.
Provides a global view of how the system is structured

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.

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

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

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

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

Protect in Phases of the Incident Response

Developing and implementing suitable safeguards for better delivery of critical infrastructure services

passwd

Passwords are required on all Unix systems to ensure that your files and data remain private and that the system is safe from hackers and crackers. The steps to changing your password are as follows:

Permission Indicators

While using ls -l command, it displays various information related to file permission as follows

Packet-filtering firewalls

It examines packets and prevents them from passing if they do not comply with a set of security rules.
The source and destination IP addresses of packets are checked by this form of firewall.

Platform vulnerabilities

Exploiting vulnerabilities in the OS, Server software, or app modules running on the web server

Performance Audit

Blue Team

Systematic evaluation of a cloud system by measuring how well it conforms to a setoff established performance criteria

©Certcop

Blue Team

Platform Libraries

©Certcop

Blue Team

The Platform Libraries comprises several fundamental C/C++ libraries and Java-based libraries, such Media, Graphics, Surface Manager, OpenGL etc.

©Certcop

Blue Team

Pangu

©Certcop

Blue Team

The Pangu team comprises a number of prominent security scientists and focuses on mobile security research.
Team Pangu aggressively shares expertise and research with the community at well-known security conferences such as BlackHat, CanSecWest and Ruxcon.

©Certcop

Blue Team

Passive Network Threats

©Certcop

Blue Team

The passive attack is defined by the unmodified interception of messages.
The network data and systems are unaffected.

©Certcop

Blue Team

Packet Filtering

©Certcop

Blue Team

Allowing traffic only to certain port numbers.
Packet filtering refers to a firewall examining packet addresses and port numbers.
It ensure that traffic from IP addresses known to be "evil" is kept out.

©Certcop

Project Initiation

Decide on conceptual definition of project
Identify security requirements
Perform an initial risk analysis (analyze potential threats)

Polymorphism

Capability of different objects to respond differently to same message

Platform Libraries

Platform Libraries comprises several fundamental C/C++ libraries and Java-based libraries, such Media, Graphics, Surface Manager, OpenGL etc.

Phishing

When a malevolent entity sends a fraudulent email masquerading as a real email, frequently from a trustworthy source. The message's purpose is to dupe the receiver into disclosing financial or personal information or clicking on a link that installs malware.

Privacy Threshold Analysis (PTA)

A Privacy Threshold Analysis (PTA) is a questionnaire used to determine:
If an information technology system contains Personally Identifiable Information (PII),

Blue Team

Privacy Impact Analysis (PIA)

Blue Team

A privacy impact assessment (PIA) is a tool for detecting and assessing privacy concerns throughout a program's or system's development life cycle.
A privacy impact assessment explains what personally identifiable information (PII) is gathered and how that information is preserved, secured, and shared.

Blue Team

Platform vulnerabilities

Blue Team

Exploiting vulnerabilities in the OS, Server software, or app modules running on the web server

Blue Team

Penetration Testing

Blue Team

You can carry out penetration tests against resources on your AWS account per the policies and guidelines at Penetration Testing.

Blue Team

Persistent Threats

Blue Team

Attacks exploiting security vulnerabilities for financial gain and criminal agendas continue to dominate headlines.

Blue Team

Prioritization

Blue Team

Vulnerability and security configuration assessments can result in lengthy remedy task lists, which must be prioritized.
It is often find that a high proportion of systems have many vulnerabilities and security configuration problems.

Packet Sniffing

Networks are intended to facilitate and expedite information traffic.
To do this, information is delivered in packets over both wired and wireless networks.

Productivity in iam

When you log in to your primary IAM portal, your employee no longer has to worry about having the correct password or access.
Not only does every person have access to the best tools for their task.

Provisioning/de-provisioning users

Provisioning refers to the process of specifying. which tools and access levels should be granted to a user.

Policy-based control

Users should be given only the permissions they need to complete their responsibilities.
An IAM should be developed to grant users access to resources depending on their employment function, department, or any other relevant attributes.

Password Reuse

An old 3rd party database is compromised; your users are still using a compromised password
Users using the same password across many accounts

Privilege Escalation

When attackers first exploit a system, they generally get access with limited privileges.
To get greater and more access, they employ a variety of privilege escalation strategies.
.

Pharming Attacks

A pharming attack is another type of attack that manipulates the DNS name resolution process.
It aims to compromise either the DNS server or the DNS client.

Platform as a Service (PaaS)

Capability to deploy applications in the cloud,
Languages, libraries, services, some control by user

Password Hashes

Most systems do not save an account's real password.
They instead save a hash of the password.
Hash attacks target the hash of a password rather than the password itself.

Privileged user

A typical privileged user is a system administrator who is in charge of administering an environment, or an IT administrator who is in charge of certain software or hardware.

Blue Team

Purpose of a risk register

Blue Team

The main purpose of a risk register is to serve as the database for specific risks. These risks might be safety risks, commercial risks, financial risks
The risk register enables a project manager or company to list all possible or potential risks into rows, and then identify and outline important components of these risks in the associated columns.

Blue Team

Privilege Management

Blue Team

When users are given the ability to do something that typically only an administrator can do, they have been granted privileges and their account becomes a privileged account

Blue Team

Public Key Infrastructure

Blue Team

It is a technology used in the digital world to authenticate individuals and devices.
The basic idea is for one or more trusted parties to digitally sign papers confirming that a specific cryptographic key belongs to a specific user or device.

Blue Team

PKI Authentication

Blue Team

When a user attempts to authenticate their identity to a server, the server creates and sends random data to the user.
The user encrypts the data and sends it back to the server using their private key.

Blue Team

PKI Digital Signing

Blue Team

The first step is to compute a hash value for the document to be signed.
The hash value is produced using an algorithm, and the output is a digital fingerprint of the file's contents.

Qualitative Risk Analysis

A qualitative risk analysis uses a pre-defined grading scale to prioritize the discovered project risks.
Risks will be graded based on their likelihood of occurrence and the impact on project objectives if they occur.

Quantitative Risk Analysis

It is a further examination of the project's greatest priority hazards, during which a numerical or quantitative rating is assigned in order to construct a probabilistic analysis.

Remote Terminal Unit (RTU)

RTU is a microprocessor-controlled electronic device. This uses telemetry data and messages from its Master Supervisory System to control connected objects to interface objects.
Remote telemetry unit and remote control unit may also be used in other words for RTU.

Respond In Phases of the Incident Response

Developing and implementing strategies to respond to the detected incidents

Recover In Phases of the Incident Response

Developing and implementing a plan to restore the business operations after the occurrence of the incident

Blue Team

Remove file or Directories

Blue Team

To remove a directory and all its contents, including any subdirectories and files, use
command Rm <file name/directory>
-r recursive

Blue Team

RAW Table

Blue Team

Iptable's Raw table is for configuration exemptions. Raw table has built-in chains.

Blue Team

Rogue Access Points

Blue Team

Attackers build physically illegal wireless access points that enable them to access a secure network by depriving network users' connections

Blue Team

Redsn0w

Blue Team

Redsn0w is a jailbreaking tool for iOS devices that works on both OS X and Windows.

Blue Team

Reduce attack surface

Blue Team

Deleting all unneeded or unnecessary applications and services from all computer devices.
There is usually no reason for every workstation in your firm to be running a mail server, ftp server, and DNS.

Retirement/Disposal

Properly dispose of system
Move data to another system or discard accordingly
Repeat full cycle with a new project initiation

Relational Database models

A DB in the form of tables (rows & columns) related to each other
Stores data in such a way that a data manipulation language can be used independently on data
Uses a database engine (Oracle, Sybase, etc...)

Repeatable

A formal structure has been developed including quality assurance. However, no formal process models have been defined.

Risk Assessment (RA)

Risk assessment is a formal and systematic method for identifying and quantifying events, their frequencies / probabilities, and the amount of repercussions / losses to recipients as a result of exposure to hazards such as natural disasters and hardware, software, and human system failures.

Regulation

Many government and industry regulations, such as HIPAA-HITECH, PCI DSS V2 and Sarbanes-Oxley (SOX), mandate rigorous vulnerability management practices

Blue Team

Risk Management

Blue Team

Mature organizations treat it as a key risk management component.
Organizations that follow mature IT security principles understand the importance of risk management.

Blue Team

Risk Assessment

Blue Team

Larger issues should be articulated in risk-based language (e.g., ISO 27005), with the impact expressed in terms of business impact.
Considerations relating to risk reduction and policy compliance should be included in the business case for any remedial action.

Blue Team

Remediation

Blue Team

Only when mitigation activity is carried out as a result of the baseline and monitoring functions is security improved.
Cross-organizational processes and workflows aid in the remediation process.

Blue Team

Root Cause Analysis

Blue Team

It's critical to examine security and vulnerability evaluations.
Changes to user administration and system provisioning processes may be required to eliminate the fundamental cause of security flaws.

Blue Team

Radio Frequency (RF)

Blue Team

Radio frequency is abbreviated as RF. Any frequency in the electromagnetic spectrum that is linked with radio wave propagation is referred to as RF. RF field propagation is used in a lot of wireless technologies. The electromagnetic radiation spectrum includes these frequencies.

Rouge access point

Any illegal access point (AP) on a network is referred to as a rouge access point.
It might be caused by an attacker or a misunderstanding on the part of an employee.

RTO

The RTO is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs.
An RTO is measured in seconds, minutes, hours or days. It is an important consideration in a disaster recovery plan (DRP).

RECOVERY POINT OBJECTIVE (RPO)

Recovery point objective (RPO) is defined as the maximum amount of data that can be lost after a recovery from a disaster or a failure.
An RPOs determines the maximum age of the data in backup storage needed to be able to meet the objective specified by the RPO, when a network or computer system failure occur.

rbash

This Restricted bash shell provides minimal functionality to the person or script running in it.

Risk Mitigation

The application of security policies and processes to lower the overall risk or impact of a threat is known as risk mitigation.
Risk mitigation in cybersecurity can be divided into three components:

Blue Team

Rainbow Attack

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.

Blue Team

Replay Attack

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.

Blue Team

ROLE-BASED AWARENESS TRAINING

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.

Blue Team

Record your findings

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.

Blue Team

Review assessment and update if necessary

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.

RISK REGISTER

The Risk Register records and keeps track of practically all of the hazards that have been recognized and are related to the project.
As a result, it keeps track of dangers, including their status and history.

Remote virtual desktops model

An image is copied to the local machine, which means a constant network connection is unnecessary.

Rogue Access Points

Attackers build physically illegal wireless access points that enable them to access a secure network by depriving network users' connections

Role-based access control (RBAC)

It Is a commonly used in networks to simplify the process of assigning new users the permission required to perform a job role.

Revocation

Deleting all unneeded or unnecessary applications and services from all computer devices.
There is usually no reason for every workstation in your firm to be running a mail server, ftp server, and DNS.

Six-STEP INCIDENT RESPONSE PLAN

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

Security Analysts

Professionals in this field work to restore the network. In an IR team, there are two categories of security analysts:

SIEM (Security information and event management)

Collected log data from applications, host systems, networks, and security devices in the organization's technological infrastructure (e.g., antivirus filters and firewalls). Security issues are reported, including virus activity and unauthorized logins.

Shell

The shell is the application that handles your requests.
It analyses and invoke the commands
All commands in the shell follow standard syntax.

SYSTEM BOOTUP

If you have a computer with the Unix operating system installed, all you have to do is turn it on to get it up and running.
The system starts booting up as soon as you turn it on.Then it prompts you to log in.

Special Files

Access to hardware such as hard disks, CD-ROM drives, modems, and Ethernet adapters is provided by several special files.

Software or hardware firewalls

A software firewall is a program that is installed on each computer.
Whereas a physical firewall is a piece of hardware that is located between your network and gateway.

Stateful multilayer inspection (SMLI) firewalls

SMLI firewalls compare packets to known trusted packets at the network, transport, and application levels.
It examines the entire packet and only allows it to pass if each layer is passed.

Spare Phishing

It is a type of deception. This is similar to phishing, except the rootkit or malware is customized to a specific person or organization.

Sandboxing

Sandboxing is a cybersecurity practice in which code is executed, observed, and analyzed in a secure, isolated network environment that simulates end-user operating environments.

Blue Team

Sensitive data storage

Blue Team

Some applications utilize a poor security system in their database design, such that attackers may hack and steal sensitive user information.

Blue Team

SSLStrip

Blue Team

MITM type attack that leverages SSL/TLS implementation flaws

Blue Team

Session Hijacking

Blue Team

Attacker Steal DNS Poisoning Valid Session ID

Blue Team

SQL Injection

Blue Team

SQL injection is a type of online security flaw that allows an attacker to interfere with a web application's database queries. It allows an attacker to see data that they wouldn't ordinarily be able to see.

Blue Team

Sandboxing Attacks

Blue Team

Sandboxing helps to safeguard systems and users by restricting the resources available to the application on the mobile platform.

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.

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.

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.

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

Social engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime,

Blue Team

Spare Phishing

Blue Team

It is a type of deception. This is similar to phishing, except the rootkit or malware is customized to a specific person or organization.

Blue Team

Sensitive data storage

Blue Team

Some applications utilize a poor security system in their database design, such that attackers may hack and steal sensitive user information.

Blue Team

Software as a Service (SaaS)

Blue Team

Applications accessible from client devices, web browser, email, mobile, limited configuration

Blue Team

SMS phishing

Blue Team

A social engineering technique used to target victims through SMS messages and may use different motivational techniques like scarcity or fear to entice the victim to perform an action, like clicking on a malicious URL within the message.

Blue Team

Security Operational/Maintenance

Blue Team

Deleting all unneeded or unnecessary applications and services from all computer devices.
There is usually no reason for every workstation in your firm to be running a mail server, ftp server, and DNS.

Blue Team

Spyware

Blue Team

It is a secretly installed malicious code that is intended to track and report usage of a target system or collect data. Such data may include web browsing history, personal information, user names and passwords, and much more.

Blue Team

Security Assessment

Blue Team

The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.

Blue Team

SSP- System Security Plan

Blue Team

A formal document that summarizes an information system's security needs and details the security procedures in existence or intended to achieve those criteria.

Blue Team

System Inventory

Blue Team

This is a comprehensive inventory of all system components Hardware Software Network Port, Protocols, and Services

Blue Team

Security Assessment and Authorization (SA&A)

Blue Team

The process of obtaining and maintaining a management decision to authorize the operation of an information system or a service and to explicitly accept the residual risk of an agreed-upon set of security controls, as well as the results of continuous security assessment is known as security assessment and authorization (SA&A).

Blue Team

System and Communications Protection (SC)

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.

Blue Team

System and Information Integrity (SI)

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.

Blue Team

Service Dependency Mapping

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.

Blue Team

Switches

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).

Blue Team

Streamline Data Collection

Blue Team

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

Single Point of Failure (SPOF)

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.

Security in iam

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.

Service Dependency Mapping

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.

Single Sign-on

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.

Secure access

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.

Security Access Markup Language (SAML)

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.

System for Cross-domain Identity Management (SCIM)

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.

Shell

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

Scripting

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

Secured Protocol and Algorithms

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.

SYN Flood Attacks

Blue Team

A SYN flood is a type of denial-of-service attack in which an attacker establishes a connection to a server quickly but does not complete it.
The server must devote resources to waiting for half-opened connections, which might cause the system to become unresponsive to valid traffic.

©Certcop

Blue Team

Session Hijacking

©Certcop

Blue Team

Session hijacking makes use of cookie-stored session IDs.
When a person logs in to a website, the site frequently delivers a small text file with a session ID.

©Certcop

Blue Team

Service Level Agreement (SLA)

©Certcop

Blue Team

A service-level agreement (SLA) is a contract between a service provider and its clients..
It specifies the services that the provider will deliver and the service standards that the provider is required to meet.

©Certcop

Blue Team

Separation of Duties

©Certcop

Blue Team

The basic principle of separation of duties is that no individual person, role, or group, should be able to execute all parts of a transaction or process.

©Certcop

Blue Team

Streamline Data Collection

©Certcop

Blue Team

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

©Certcop

Systems Administrators Policy

Administrators have privileges and tasks that may require them to come into contact with sensitive, restricted, or personal information while doing their jobs.

System owner Policy

The system owner may also be a manager whose duty it is to oversee and maintain the computers that carry data.
As a result, in addition to physically securing an organization's hardware infrastructure, the system owner should patch and upgrade operating systems,

Social Media Policies

A social media policy essentially spells out how an organization and its personnel should behave online. It aids in the protection of your firm's online reputation and encourages employees to share information about the organization with their social media networks.

Single-Loss Expectancy

The expected monetary loss each time an asset is at risk is referred to as single-loss expectation (SLE).
It is most typically used during risk assessment and aims to assign a monetary value to each individual threat.

Single-Loss Expectancy Formula

Formula to calculate the Single Loss Expectancy is SLE = AV * EF

SEGMENTATION

One of the best ways to protect sensitive resources is to utilize network segmentation.
While there is no limit to the number of zones you can create in general, most networks have the zone types

System Isolation

Systems can be isolated from other systems through the control of communications with the device.

Software-Defined Networking

In a network, three planes typically form the networking architecture. Management plane
This plane administers the router.

Single Sign-On (SSO)

In an effort to make users more productive, several solutions have been developed to allow users to use a single password for all functions and to use these same credentials to access resources in external organizations.

Symmetric Key Cryptography

It is an encryption system in which the sender and receiver encrypt and decrypt communications using a single common key.
Symmetric Key Systems are faster and simpler, but the sender and receiver must exchange keys in a secure manner.

Threat Researchers

The Cyber Threat Researcher will be a member of a global team that will track and analyze threat campaigns.

Triage Analysts

They keep digital evidence preserved to conduct forensic investigation against the incident.

Threat actor

An individual or group that seeks to harm a business or organization and is motivated through financial, personal, or political gain.

Target Value

You may see all the available firewall rules on your system by running

iptables –list

There are no firewall rules specified on this system, as seen by the following iptables example.

TCP-level filtering

Reassembling and inspecting all the packets in each TCP session.

It can also be used for DNS filtering and traffic encryption.

It well as offers Virtual Private Network (VPN) capability.

Blue Team

Tuple

Blue Team

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.

Blue Team

Trojan

Blue Team

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.

Blue Team

Third-Party Assessment Organizations (3PAOs).

Blue Team

Perform initial and periodic assessment of CSP systems per FedRAMP requirements
Provide evidence of compliance
Have on-going role in ensuring CSPs meet requirements.

Blue Team

Tripwire

Blue Team

Tripwire provides a comprehensive, automated view of operational, regulatory, and security compliance throughout the data center's dynamic environment.

Blue Team

Tailgating

Blue Team

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.

TCP Tracer out

TCPTraceroute is a traceroute implementation that uses TCP packets.
TCPTraceroute follows routes via networks to determine what is obstructing traffic.

Threats

Threats can come from anywhere and are becoming more sophisticated all the time, making it increasingly difficult to be completely prepared for data breaches.

Threat Intelligence

There is a proactive response mechanism in place to deal with cyber threats.
Research and Development activities are already underway at various research organizations to fight threats in cyberspace.

Threat Protection

Through negligence or malicious intent, employees and third parties with stolen credentials can leak or steal sensitive data from cloud services.
To help pinpoint anomalous user behavior, CASBs can compile a comprehensive view of regular usage patterns and use it as a basis for comparison.

Type 1 hypervisor

A guest operating system runs on another level above the hypervisor.

Blue Team

Type 2 hypervisor

Blue Team

A Type 2 hypervisor runs within a conventional operating system environment.

Blue Team

Unix Architecture

Blue Team

This operating system has a four-layered design. Hardware, Kernel, System Call Interface (shell), and application libraries/tools, as well as utilities, are all part of it.

Blue Team

Unintended Permissions

Blue Team

Unknown applications sometimes allow attackers to enter doors by offering unknown permission.

Blue Team

Userland Exploit

Blue Team

A jailbroken user enables access at user-level but does not allow access at the iboot level.
This sort of exploit cannot be linked since recovery mode loops are not possible.
You can patch them using Apple.

Blue Team

Understand Aging Assets

Blue Team

Forty percent of unplanned downtime is caused by aging equipment.
But maintenance professionals can sometimes do more than they realize is possible to manage these failures.

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.

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.

Virus

Malicious code that spreads from a computer to computer via attaching itself to other files. The code executes when the attached files opened.

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.

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.

Vulnerability management process

The process of finding, analyzing, treating, and reporting security vulnerabilities in systems and the software that runs on them is known as vulnerability management.

Vulnerability databases

A vulnerability database (VDB) is a platform for storing, updating, and spreading information regarding computer security flaws that have been discovered.

Vendor vulnerability announcements

Unknown applications sometimes allow attackers to enter doors by offering unknown permission.

Vulnerability analysis

The goal of this stage is to determine the source and root cause of the vulnerabilities discovered in the previous step.
It entails determining which system components are responsible for each vulnerability.

Virtual

All the network segmentation components discussed thus far separate networks physically with devices such as routers and firewalls, a virtual local-area network (VLAN) separates them logically.

Virtual Desktop Infrastructure (VDI)

Hosts desktop operating systems within a virtual environment in a centralized server.

Wireless Forensics

Wireless forensics analyzes and investigates traffic in a wireless environment using specialized tools and procedures.
When computer crimes or cyberattacks are perpetrated by breaching security protocols in wireless networks, this type of study is critical.

whoami

While you're logged into the system, you might be willing to know: Who am I?
The easiest way to find out "who you are" is to enter the whoami command

Who is logged in?

Sometime you might be interested to know who is logged in to the computer at the same time.
There are three commands available to get you this information, based on how much you wish to know about the other users: users, who, and w.

Worms

Malicious code that spreads from computer to computer, within a network, on its own. It ultimately consumes network bandwidth.

Wireless Scanner

Wireless vulnerability scanners are used to identify rogue access points and also validate that a company's network is securely configured.

Blue Team

©Certcop

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

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

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

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

Wireess Networking

Connecting multiple devices without any physical connection.
Transfer data through Radio Frequency

Wireless Networks Works

Wireless networks use radio frequency (RF) technology
When an RF current is applied to an antenna, an electromagnetic field is generated.

Wireless Networks Standards

Wireless technology, like the technology connected with it, has changed over time. It's always a good idea to perform your own research before investing in any of these technologies.

WIRELESS NETWORKS BENEFITS

Voice over Internet Protocol (VoIP).
It has enabled mobility.
They are less expensive than wired networks
Data encryption methods

Wired Equivalent Privacy (WEP)

The first encryption system designed specifically for wireless networks
WEP, on the other hand, has several well-known security vulnerabilities, is complex to configure, and is readily cracked.

Blue Team

Wi-Fi Protected Access (WPA)

Blue Team

For encryption, most modern WPA implementations employ a pre-shared key (PSK).
To produce keys or certificates, WPA Enterprise use an authentication server.

Blue Team

Wi-Fi Protected Access (WPA2)

Blue Team

A wireless security standard based on the 802.11i wireless security standard, which was completed in 2004. The adoption of the Advanced Encryption Standard (AES) WPS assaults remains significant in contemporary WPA2-capable access points, as is the case with WPA.

Blue Team

Wireless Wizard

Blue Team

Wireless Wizard is a free tool that will assist you in getting the greatest performance out of your wireless network connection.
The program also includes a set of diagnostic tests that you can use to determine how well your wireless network is working.

Blue Team

Wireless Key Generator

Blue Team

It is a basic application for enhancing network security in the Wireless Key Generator.
It invites you to choose the security type and key strength that you use on your wireless network.

Blue Team

Zero-Trust Policy

Blue Team

A zero trust policy implies that an organization's IAM solution is always monitoring and securing the identification and access points of its users.
Zero-trust standards ensure that each employee is constantly identifiable and their access is regulated.

Zero trust centralized administration

This could imply transferring people from other systems or synchronizing your IAM with other user directories.

zsh

The Z shell is a modern take on the bash family of shells.
It offers neat improvements, like command spellchecks and suggested corrections.

Zero-Day Attacks

A zero-day vulnerability is a flaw or issue that has yet to be discovered.
A zero-day assault takes use of a previously unknown flaw.
Frequently, the vendor is unaware of the problem.

Application Based Attacks

The application layer is the most difficult to protect. The flaws found here frequently rely on complex user input scenarios that are difficult to define with an intrusion detection signature.

Application-level filtering

Email filters and web proxies are examples of application level filters.
These act as proxies for one or more services.
These filters are extremely costly, especially when applied to high-bandwidth web traffic.

Blue Team

Access control list (ACL)

Blue Team

In computer security, an access-control list is a list of permissions associated with a system resource.

Blue Team

Brute Force Attacks

Blue Team

A brute force attack tries to guess every conceivable combination of characters.
Online and offline brute force assaults are the two forms of brute force attacks.

Blue Team

Asset value (AV)

Blue Team

Asset value (AV) is the value per share as determined on a specific date or time.

Blue Team

Chief Information Officers (CIOs)

Blue Team

A chief information officer (CIO) is a company leader who is in charge of information and computer technology management, implementation, and usability.

Blue Team

Configuration Management Plan (CM Plan)

Blue Team

Throughout the lifecycle, the Configuration Management Plan establishes uniform CM techniques for managing system software, hardware, and documentation changes.

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that must be protected or disseminated in accordance with existing laws and regulations.

Control Definition

Each control objective (a-k) will need to be answered individually.
As a guide to understanding the requirements for each control, the Rev 4 Test Cases may be reviewed.

Configuration Standards by Device Role

It focuses on vulnerability assessment falls short of achieving.
One of the most important vulnerability management program goals:

Certificate Management

Certificate management is the process of managing digital security certificates.
Certificate authorities are responsible for certificate management and serve as a registration authority for subscriber certificates.

Data acquisition and duplication

Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim

Blue Team

Deep packet inspection (DPI)

Blue Team

Deep packet inspection examines the data within the packet itself.
While basic firewalls only look at packet headers.

Blue Team

Denial of service or interruption of availability

Blue Team

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.

Blue Team

Dynamic Host Configuration Protocol (DHCP)

Blue Team

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

Blue Team

evasi0n7

Blue Team

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).

Blue Team

EXIF

Blue Team

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

Blue Team

Exploit Impact

Blue Team

Any attack that takes advantage of weaknesses in programs, networks, operating systems, or hardware is referred to as an exploit.

Blue Team

Ethical hacker

Blue Team

A person who hacks into a computer network in order to test or evaluate its security rather than with malicious or criminal intent.

Blue Team

Establish Network Access Controls

Blue Team

First you have assessed your assets and identified high-priority problem areas.
Next step is to establish network access controls to help mitigate the risk of insider threats.

Blue Team

Exposure factor (EF)

Blue Team

Exposure factor (EF) is a percentage that measures the possible loss that could occur to an asset if a given threat occurs.

Blue Team

Evidence Collection

Blue Team

When it comes to tracing the attacker and 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.

Blue Team

IEEE 801.11

Blue Team

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.

Blue Team

ksh

Blue Team

The Korn Shell provides a particularly strong scripting language.

Blue Team

Media Protection (MP)

Blue Team

These policies define how to use, store, and transmit data while ensuring its confidentiality and integrity.

Blue Team

Manage user identities

Blue Team

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.

Blue Team

MTransference

Blue Team

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.

Blue Team

Nexpose Community

Blue Team

Nexpose is a popular vulnerability assessment tool. Nexpose Community Edition is a free application, while other Nexpose editions are charged.

Blue Team

Proxy firewalls

Blue Team

Traditional firewall technology is combined with extra features.
Such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more.

Blue Team

Switch spoofing

Blue Team

A type of VLAN hopping attack that occurs when an attacker can emulate a valid trunking switch on the network by speaking 802.1Q.

Blue Team

Process States

Blue Team

Each CPU (or CPU core) in a multi-tasking operating system can work on only one process at a time. As a process runs, its immediate CPU time and resource allocation requirements change.

Blue Team

Process Control Using Signals

Blue Team

A signal is a type of software interrupt that is provided to a process.
Signals communicate events to a running application.
Events that trigger a signal can be a mistake, external events, or explicitly requested events.

Blue Team

Rootkits

Blue Team

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.

Blue Team

SolarWinds

Blue Team

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

Blue Team

Secure Hash Algorithm 3. (SHA-3).

Blue Team

A user then logs in using a username and password.

Blue Team

Wireless Networks Threats

Blue Team

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.

Blue Team

Zero-day exploits

Blue Team

Start an attack on a mobile OS or app, taking advantage of an undiscovered vulnerability.

Zero-day assaults

Blue Team

Given the impossibility of flawless security, businesses should supplement vulnerability management and shielding with more effective monitoring.

©Certcop