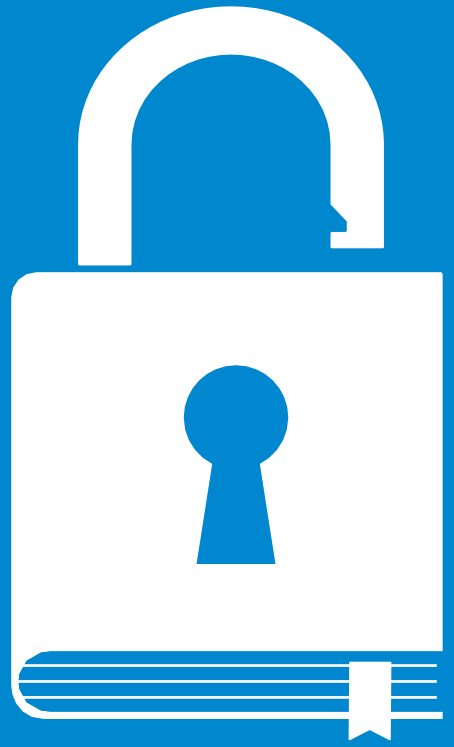
Computer Troubleshooters™

TECHNOLOGY SOLVED

Powered by Barracuda MSP

Barracuda Dictionary

Cybersecurity from A to Z



YOUR KEY TO MASTERING CYBERSECURITY LINGO

2024 edition

Introduction

Navigating the ever-changing cybersecurity landscape can often feel like decoding a foreign language. This cybersecurity dictionary is your comprehensive guide to unraveling the mysteries of cybersecurity terminology. Learn about these 150 seriously important terms in a fun way.

Whether you are looking to enhance your career, safeguard your organization, or simply stay informed about the latest cyberthreats, this dictionary is the key to unlocking the language of cybersecurity.

Index

2FA

(Two-factor Authentication)

/ too fak-ter aw-then-ti-key-shuhn /

Authentication.

Two locks are better than one. This is a security measure that requires two different forms of authentication to access an account or system.

Access Control

/ ak-ses kuhn-trohl /

Access.

The process of playing master gatekeeper to a digital domain by regulating who can access specific resources or data within a system or network. It involves authentication mechanisms to ensure that only authorized users or entities can access sensitive information or perform certain actions.

Account Takeover

/ uh-kount teyk-oh-ver /

Access.

When cybercriminals gain unauthorized access to a user's online account by exploiting weak passwords, phishing attacks, or other vulnerabilities. It's also one of the many reasons you should refrain from using your birthday as a password.

Advanced Penetration Testing

/ ad-vanst pen-i-trey-shuhn test-ing /

Practice.

A cyberattack simulation that takes your security system out for a spin. This can help discover security weaknesses in a system, network, or application.

Advanced Encryption Standard

(AES)

/ ad-vanst en-krip-shuhn stan-derd /

Encryption.

The secret handshake of the digital world. Advanced Encryption Standard (AES) is a widely used encryption algorithm to secure sensitive data, ensuring that it can only be accessed with the correct decryption key.

Air Gap

/ air gaap /

Security.

An air gap is like a moat around a castle. It's a physical separation used to prevent unauthorized data transfer between computer systems, networks or devices. It enhances cybersecurity by reducing potential malware, ransomware and other types of attacks.

Advanced Threat Protection

/ ad-vanst thret pruh-tek-shuhn /

Security.

A multilayered security approach that goes beyond traditional security to prevent zero-day attacks.

Anna Kournikova Virus

/ ah-nuh kor-nick-khova vahy-ruhs /

Attacks.

An infamous computer worm that spread via email in the early 2000s. Named after the Russian tennis player Anna Kournikova, it tricked users into opening an email attachment by promising a picture of the celebrity. When opened, it infected the victim's computer.

Anti-malware

/ an-tahy mal-wair /

Security.

A superhero software that detects, prevents and removes harmful malware from computer systems, protecting them against viruses, spyware, and other damaging programs.

Anti-spam

/ an-tahy spam /

Security.

Got spam? No problem. This type of solution identifies and filters out unwanted emails and reduces the likelihood of users falling victim to phishing attacks or other scams.

Application Firewall

/ ap-li-key-shuhn fahyuhr-wawl /

Practices.

A security solution that monitors and controls incoming and outgoing network traffic to and from an application, protecting it from unauthorized access, attacks, and vulnerabilities.

As a Service

/ az uh sur-vis /

Technologies and Tools.

“As a Service” (aaS) delivers services or resources via the internet on a subscription basis, removing the need for local infrastructure management.

Attack Surface

/ uh-tak sur-fis /

Practices.

If your system or application were a fortress, this would refer to potential entry points, like secret trapdoors, that attackers can exploit. That includes vulnerabilities, interfaces, and network connections. For security reasons, keeping the attack surface as small as possible is important.

Backdoor

/ bak-dawr /

Attacks.

Have you ever heard of a secret entrance to a computer system? No? Well, hackers have. This is a method used by attackers to access a system or encrypted data that bypasses the system’s usual security mechanisms. In short, it is like a secret trapdoor for hackers, giving them the ultimate backstage pass to a digital party they weren’t invited to!

Backup

/ bak-uhp /

Security.

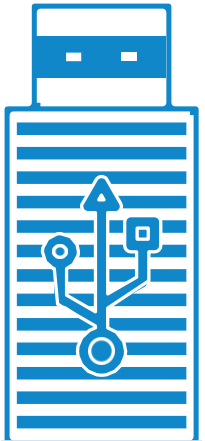
A digital replica of data and configuration set up in the event of a disaster, ensuring the recovery of digital data, files or systems.

BadUSB

/ bad yoo-es-be /

Attacks.

There are good USBs, and there are bad USBs. The bad ones are malicious devices that can infect computers with various types of malwares.



Biometric Authentication

/bahy-uh-me-trik aw-then-ti-key-shuhn /

Authentication.

The future is here! This is a type of authentication that uses unique physical or behavioral characteristics, such as fingerprints or facial features, to verify the identity of users and provide secure access to systems.

Black Hat Hacker

/ blak hat hak-er /

Teams and Roles.

The evil guys in the hacker community. A blackhat is a cybercriminal who breaks into computer networks with malicious intent, such as releasing malware to destroy files, holding computers hostage or stealing personal information.

Blue Team

/ bloo teem /

Teams and Roles.

A team of security analysts in charge of defending and protecting a company from cyberthreats — always ready to swoop in and save the day!

Bot Attacks

/ bot uh-taks /

Attacks.

Attacks that involve the use of automated software (bots) to perform malicious activities, such as data theft or unauthorized access. Let's just hope hackers don't accidentally unleash the robot uprising!

Botnet

/ bot-net /

Attacks.

A network of compromised computers or devices controlled by a single entity. It's the supervillain of the cyber world, launching attacks left and right.

Broken Access Control

/ broh-kuhn ak-ses kuhn-trohl /

Access.

When users venture into forbidden territory and gain access to restricted resources or perform unauthorized actions due to improper configuration or vulnerabilities.

Browser Hijacker

/ brou-zer hahy-jak-er /

Attacks.

Have you ever felt like your web browser has had a mind of its own? That can result from a type of malware that alters web browser settings without user permission, resulting in potential redirection to malicious websites or displaying unwanted content.

Brute Force Attack

/ broot-fawrs ah-tak /

Attacks.

Simple, yet effective. This is a method where an attacker systematically tries all possible combinations of passwords or encryption keys until they find the correct one.

Buffer Overflow Attack

/ buhf-er oh-ver-floh ah-tak /

Attacks.

Things can get overwhelming even in the digital world. This is an attack that targets vulnerabilities in software by overloading a program's memory buffer, potentially allowing an attacker to execute malicious code or gain control of the system.

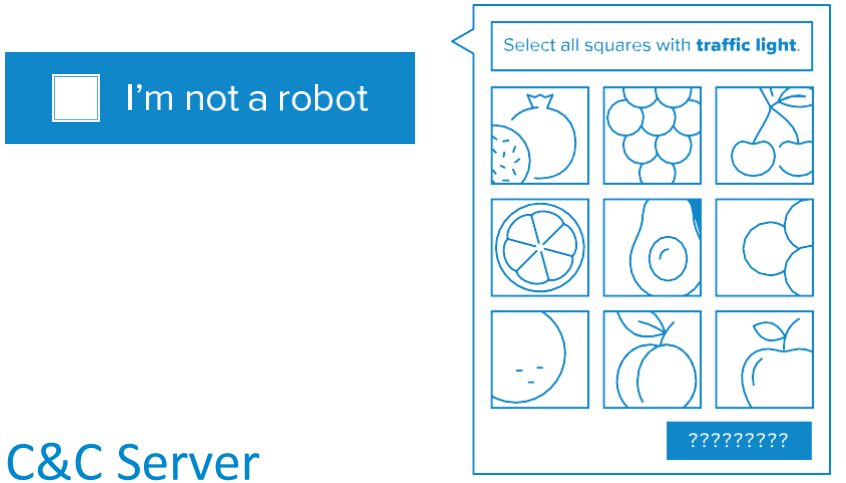
CAPTCHA

(Completely Automated Public Turing test to tell Computers and Humans Apart)

/ kap-chuh /

Security.

A security measure used on websites to determine whether a user is a human or a bot, typically involving solving some kind of puzzle. While the tests are supposed to be easy for humans to decode, we all know how anxiety-inducing it can be to select the correct photos of a traffic light.



C&C Server

(Command and Control)

/ kuh-mand and kuhn-trohl /

Attacks.

A centralized system cybercriminals use to manage and control compromised computers or devices within a botnet, playing puppet master and issuing commands for various malicious activities. Everything from DDoS attacks and data theft to malware distribution and click fraud. Watch out!

Cerber Ransomware

/ sur-ber ran-suhm-wair /

Attacks.

A type of ransomware* that encrypts a victim's files and, like a digital kidnapper, demands a ransom payment in exchange for the decryption key. It spreads through phishing emails or malicious websites and installs itself on the user's device.

Certificate-based Authentication

/ ser-tif-i-kit-beyst aw-then-ti-key-shuhn /

Authentication .

Think of certificate-based authentication as the high-tech key to the digital kingdom. Digital certificates play the role of the knight guarding the castle, ensuring only the rightful heroes can enter and enjoy secure communication.

Clickjacking

/ klik-jak-ing /

Attacks.

Have you ever accidentally clicked on an ad thinking it was the "download" button? This a technique where attackers trick users into clicking on something different from what they perceive, often leading to unintended actions or the exposure of sensitive information.

Cloud-to-cloud Backup

/ kloud-to-kloud bak-uhp /

Practices.

A backup strategy that involves copying data directly from one cloud service to another. It's like having a backup plan for your backup plan.

Cold Data

/ kohld dey-tuh /

Data Management.

Older or less frequently accessed data is stored in a lower- tier system to optimize storage costs and performance while maintaining availability. Kind of like the clothes at the back of your closet!

Command Injection

/ kuh-mand in-jek-shuhn /

Attacks.

A cyber illusionist's performance, where mischievous commands are the rabbits pulled out of the digital hat. Command injection involves inserting malicious commands into input fields or data sent to a system, manipulating it to execute unintended actions or gain unauthorized access.

Code Injection

/ kohd in-jek-shuhn /

Attacks.

A sneaky cyberattack where malicious code is inserted into a vulnerable software application, exploiting security flaws to execute unauthorized commands. One could say, it evokes the feeling of trypanophobia (fear of needles) but in the digital world.

Common Vulnerabilities and Exposures (CVE)

/ kom-uhn vuhl-ner-uh-bil-i-tee and ik-spoh-zher /

Security.

The ultimate guidebook, or database, of publicly disclosed security vulnerabilities and exposures. CVEs help track and communicate security issues across the cybersecurity community.

Cookie Theft

/ kook-ee theft /

Attacks.

An attack where the cyber version of an unauthorized cookie monster intercepts or steals a user's web session cookies. As the cookies contain sensitive session data, attackers swipe the digital crumbs to impersonate the victim and gain access to their accounts.

Credential Stuffing

/ kri-den-shuh stuhf-ing /

Authentication.

This is when cyber attackers use stolen login credentials to access multiple accounts due to people's habit of reusing the same passwords. A kind reminder to switch it up occasionally!

Credentials

/ kri-den-shuhl /

Access.

Information used to verify a user's identity, often including usernames and passwords, granting access to secure systems or services. Like the digital version of showing your membership card for an exclusive club.

Cross-Site Scripting (XSS)

/ kraws sahyt skripting /

Attacks.

The cyber equivalent of planting a secret trapdoor in a website's code. An XXS is a web vulnerability where malicious code is injected into a website, allowing attackers to execute scripts in the context of unsuspecting users, potentially stealing information or spreading malware.

CTB Locker

/ see-tee-bee lock-er /

Attacks.

Curve-Tor-Bitcoin Locker (CTB Locker) is a type of ransomware* that plays hide-and-seek with your files. It encrypts files on a victim's computer and demands a ransom in Bitcoin for the decryption key. This digital extortion tactic is known for its encryption strength and ability to target a wide range of file types.

Cryptographic Key

/ kripto-graf-ik kee /

Data Management.

The master key of the digital world: a piece of information used in cryptographic algorithms to transform plain data into secure, encrypted data and vice versa. These keys are crucial for ensuring the confidentiality of sensitive information.

Cryptography

/ krip-toh-gruh-fee /

Practice.

The science and practice of securing communication and data by creating a secret language so only authorized parties can decipher it. It involves algorithms and techniques for encrypting and decrypting information to protect it against eavesdropping and nosy parkers.

Cyber Insurance

/ sigh-ber in-shur-uhns /

Practices.

An insurance that protects businesses financially recover from cybersecurity incidents like cyberattacks and data breaches. You hope you never have to use it, but you're glad you have it if you do.

Cyber Resiliency

/ sigh-ber ri-zil-yen-see /

Practices.

An organization's force field against cyberattacks and security breaches. It involves not only preventing attacks but also planning for effective response and maintaining business continuity.

Cyberattack

/ sigh-ber uh-tak /

Attacks.

The surprise guests at the tech soiree, crashing in uninvited to steal data, make a digital mess, or even turn off the music – they're the party poopers of the cyberworld!

Cybersecurity Framework

/ sigh-ber-see-kyoo-rih-tee fraym-werk /

Practices.

The ultimate cybersecurity playbook. A structured set of guidelines, best practices, and standards designed to help organizations establish effective security measures.

Daemon

/ day-mun /

Technologies and Tools.

A daemon is like a supernatural computer program that runs as a background process, performing various tasks or functions. As it plays a role in managing system components, it can sometimes be exploited for malicious purposes.

Data Audit

/ day-tuh aw-dit /

Data Management.

Digital data are like students in a class, and audits are like surprise quizzes. By examining data and records to assess their accuracy, security, and compliance, audits help identify vulnerabilities and ensure data integrity.

Data Breach

/ day-tuh brech /

Access.

A breach is the unauthorized access, acquisition, or disclosure of sensitive or confidential information. It can result in the exposure of personal data, financial loss, and damage to an individual or organization's reputation. Or, in other words, time to call the cybersecurity hotline!

+44 (0) 1256 833 499

Data Encryption

/ day-tuh in-krip-shun /

Encryption.

The process of converting plaintext data into ciphertext using cryptographic techniques. Encryption ensures that even if data is intercepted, it remains unreadable without the appropriate decryption key. It's like using a secret code only you and the intended recipient can decipher!

Data in Transit

/ day-tuh in trans-it /

Encryption.

Like a train carrying its passengers to their destinations, this refers to data being transmitted between devices, networks or systems. Encryption is often used to protect data while it's in transit, safeguarding it from interception and unauthorized access.

Data Loss

/ day-tuh loss /

Data Management.

A digital vanishing act where information is unintentionally destroyed, corrupted, or compromised due to hardware failures, software errors, human mistakes, or cyberattacks.

Data Loss Prevention

/ day-tuh loss pri-ven-shun /

Practices.

Strategies, policies, and technologies that prevent everything from top-secret files to embarrassing selfies from being leaked, lost, or shared inappropriately.

Data in Transit Encryption

/ day-tuh in trans-it in-krip-shun /

Encryption.

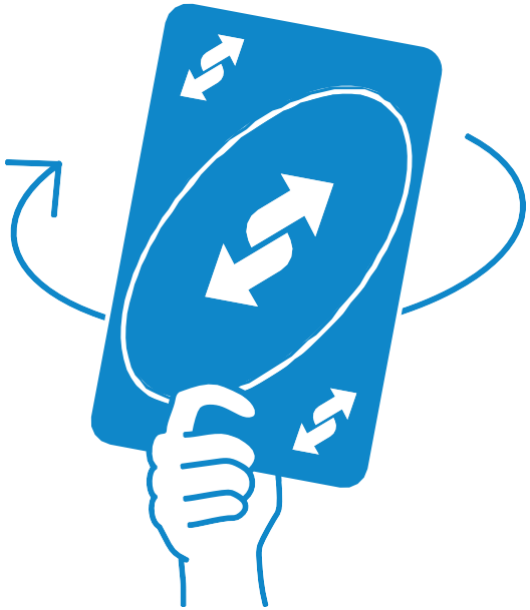
A security measure that protects sensitive information while it's being transmitted over networks. Like a virtual equivalent of a cloak of invisibility, it ensures that data is encrypted, making it unreadable to unauthorized users during transit.

Data Wiping

/ day-tuh wip-ing /

Data Management.

Say goodbye to your data forever! This is the secure erasure of data from storage devices to ensure it cannot be recovered. It's typically performed before repurposing or disposing of devices to prevent data leaks.



Decryption

/ dee-krip-shun /

Security.

Like unscrambling eggs, this is the process of converting encrypted data back into its original, readable form. It is typically performed using a decryption key or algorithm that reverses the encryption process.

DDoS (Distributed Denial of Service)

/ dis-trib-yoot-ed de-nigh-ul of ser-vis /

Attacks.

A digital flood in which multiple compromised computers are used to drown a target system, network, or website with excessive traffic, causing it to become inaccessible.

DNS Attack

/ dee-en-es at-tak /

Attacks.

A cyber criminal's attempt to mess with the internet's address book. This type of attack targets the Domain Name System to disrupt or manipulate the resolution of domain names, leading to various security vulnerabilities.

Domain Hijacking

/ do-main hij-ack-ing /

Attacks.

The act of cybercriminals pulling a domain heist! They take control of a domain name without permission, which can result in harmful activities such as website defacement or phishing attacks.

DomainKeys Identified Mail (DKIM)

/ do-main-keys i-den-ti-fied mayl /

Security.

A method that helps verify the authenticity of an email message – the fingerprints of the digital world. It uses cryptographic signatures to ensure that the email hasn't been altered in transit and that it came from the claimed sender, not some deceitful impersonator.

Drive-By Download

/ drive-by down-load /

Attacks.

A type of cyberattack where malware is automatically downloaded onto a user's computer without their consent when visiting a compromised website. The attacks often exploit vulnerabilities in web browsers or plugins, regular software updates are your trusty ghostbusters, keeping these digital phantoms at bay and your computer safe and sound!

Dyreza

/ dy-rey-zuh /

Attacks.

A sophisticated banking Trojan malware designed to act as a virtual pickpocket, stealing sensitive financial information from victims. It typically spreads through phishing emails or malicious downloads and can capture personal data to facilitate financial fraud.

Email Bomb

/ ee-meyl bomb /

Attacks.

A cyberattack that'll make you wish you never signed up for anything online. The attack floods a target's inbox with an overwhelming volume of spam emails, causing the server to become overloaded. It can temporarily disrupt communication and an individual or organization's email services – keep an eye out!

Email Encryption

/ ee-meyl in-krip-shun /

Encryption.

The practice of encrypting the content of email messages, like sealing them in a digital envelope, to protect them from unauthorized access. It safeguards sensitive information in emails, ensuring that only the intended eyes can read it.

Email Fraud

/ ee-meyl fraud /

Practice.

The age-old practice of sending deceitful emails to trick recipients into taking harmful actions, like sharing sensitive information or transferring funds to unauthorized accounts.

Encryption

/ in-krip-shun /

Encryption.

The process of converting plain, readable data (plaintext) into a coded form (ciphertext) using cryptographic algorithms. This is done to ensure the confidentiality and authenticity of the data — where only authorized parties with keys can access the original plaintext. Basically, it serves as the high-security vault of data protection.

End-to-End Encryption

/ end-to-end in-krip-shun /

Encryption.

Imagine end-to-end encryption as your digital version of the secret code you and your buddy invented for passing notes in class. It's like having your very own super-secret decoder ring, ensuring that only the two of you can unravel the message, while keeping it hidden away from the prying eyes of the world.

Endpoint Security

/ end-point see-kyoo-ri-tee /

Security.

Security measures designed to give your gadgets, such as computers and phones, VIP-treatment of protection against malware, unauthorized access, and other threats.

Ethical Hacking

/ eth-i-kuhl hak-ing /

Practice.

Why let the bad guys have all the fun? Authorized and controlled attempts to exploit vulnerabilities in computer systems, networks or applications. Ethical hackers use their skills to identify weaknesses that malicious hackers might exploit, with the goal of helping organizations improve their security measures.

Exploit

/ ek-sploit /

Attacks.

The ultimate hacker's tool. This is a program, or piece of code, that takes advantage of a security flaw in an application or a computer system.

False Flag

/ fawls flag /

Attacks.

Taken straight out of a mystery novel, this is a deceptive tactic used by cybercriminals or nation-state actors to make their actions appear as though they were carried out by someone else. This involves using techniques or tools to obscure their true identity and intentions, making attribution and response more challenging for investigators.

Firewall

/ fai-er-wawl /

Security.

Imagine a cyber bouncer that monitors network traffic to prevent unauthorized access and attacks, leaving any partygoers not on the list outside in the digital cold.

Formjacking

/ form-jak-ing /

Attacks.

The cyber version of robbing a bank vault. This cyberattack involves cybercriminals injecting malicious code into a website's payment or data entry forms. The code captures sensitive information, such as credit card details, entered by users without their knowledge.

Geo-blocking

/ jee-oh-blok-ing /

Security.

The borders of the digital universe. It's a technique that restricts access to digital content or services based on the user's geographical location. It limits access to certain websites, videos, or online services based on the user's IP address — often employed to comply with regional licensing agreements or legal requirements.

Gray Hat Hacker

/ gray hat hak-er /

Teams and Roles.

A hacker that operates in a morally ambiguous gray area between white hat and black hat hackers. They may uncover and disclose vulnerabilities without authorization but typically do so with the intent of helping organizations.

Green Team

/ gre-en team /

Teams and Roles.

A group of experts who venture into the digital jungle to conduct proactive security assessments and testing within an organization. They work alongside the blue (defensive)* and red (offensive)* teams to enhance security posture.

Hardening

/ har-den-ing /

Practices.

The process of enhancing the security of a system by reducing its attack surface and minimizing vulnerabilities. This involves configuring the system, network, or software, such as disabling unnecessary services or regularly updating software — staying one step ahead of cybercriminals.

Honeypot

/ huh-nee-pot /

Practices.

A decoy system to bait cyber attackers in their natural habitat. This way, security experts can observe cyber threats without the risk of getting bitten.

Impersonation Attack

/ im-per-soh-nay-shun uh-tak /

Attacks.

An attacker dresses up and pretends to be a trusted entity to deceive users into sharing sensitive information or performing specific actions.

Incident Response

/ in-suh-dent ri-spons /

Practices.

The organized approach taken by an organization to manage and mitigate the impact of a cybersecurity incident. It outlines the necessary steps, from identifying the incident's scope to enhancing future response efforts. Managing a cybersecurity incident is like playing a game of chess: always think ahead!

Intrusion Detection System (IDS)

/ in-troo-zhun dih-tek-shun sis-tem /

Practices.

The cyberspace version of an alarm system. IDS is a security technology that monitors network traffic and system activities to detect unauthorized access or malicious activities. It can identify anomalies indicating a security breach and raise alerts for further investigation.

Insider Threat

/ in-sigh-der thret /

Practices.

The call is coming from inside the house! The risk posed to an organization's cybersecurity by individuals within the organization, such as employees or contractors, who misuse their access privileges.

Intrusion Prevention System

(IPS)

/ in-troo-zhun pri-ven-shun sis-tem /

Practices.

A security solution designed to detect and prevent unauthorized or malicious activities within a network or system. With its keen eye for detecting suspicious activity and lightning-fast reflexes, IPS takes proactive measures to block or mitigate potential threats — making it the ultimate defender in cyberspace.

IoT (Internet of Things)

/ in-ter-net of thihngs /

Technologies and Tools.

IoT refers to the network of interconnected physical devices, objects, and sensors that can collect and exchange data over the internet, anything from smart appliances and wearables to industrial machines and connected cars. It's like a high-tech family reunion, where you'll find everything from talking toasters and stylish wearables to super-smart machines and chatty cars, all mingling in the digital universe!

IoT Exploitation

/ in-ter-net of thihngs ek-sploi-tey-shun /

Technologies and Tools.

When cybercriminals play hide and seek with IoT devices. They find vulnerabilities and sneak in undetected to gain unauthorized access, control, or steal data from these devices.

IP Reputation

/ i-p re-pyoo-tey-shun /

Security.

Similar to a credit score system, a reputation is a measure of the trustworthiness of an IP address based on its past behavior and activity. It is often used in email filtering and cybersecurity to identify and block IP addresses associated with spam, malware, or other malicious activities.

Keychain

/ kee-cheyn /

Authentication.

As the word suggests, this is a storage system on a computer or mobile device that holds cryptographic keys, passwords, and certificates. Like a digital vault, it helps protect these credentials, ensuring secure communication and authentication.

Keylogger

/ kee-log-er /

Attacks.

A type of software a secret agent would use. It records a user's keystrokes on a computer or mobile device without their knowledge and can capture sensitive information such as passwords, credit card numbers, and personal messages.

Kovter

/ kuhv-ter /

Attacks.

A constantly evolving and evasive fileless malware designed to attack the Windows operating system. A master at playing hide-and- seek, it avoids detection by traditional antivirus software by storing its configuration data on the computer's registry.

Lateral Movement

/ la-ter-uhl moo-vmuhnt /

Attacks.

Techniques cyber attackers use to sneak their way deeper into a network or system after gaining initial access. The attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges.

Least Privilege

/ leest pri-vuh-lij /

Practices.

Least privilege is like the office keycard system, granting employees access to specific rooms or resources based on their roles, while keeping the executive suite off-limits to interns and visitors. This reduces the potential for unauthorized access or misuse of resources.

Link Encryption

/ link in-krip-shun /

Encryption.

A security measure that protects data transmitted over a network or communication channel by encrypting the entire data link or connection, preventing interception or decryption by snooping eavesdroppers.

Logic Bomb

/ lah-jik bahm /

Practices.

A piece of code that is intentionally inserted into a computer system to execute a harmful action when certain conditions are met, like a specific date or time. It can cause data loss or other forms of damage and is often used by insiders or attackers with knowledge of the target system. It's the cyber equivalent of a surprise party that nobody wants!

Malicious Email

/ muh-lish-us ee-meyl /

Attacks.

An email that is up to no good. This type of email contains harmful content or intends to deceive the recipient, often carrying malware attachments, phishing links or fraudulent requests.

Malicious Links

/ muh-lish-us links /

Attacks.

Not all links lead to Rome. These links are embedded URLs in emails, websites, or messages that direct to harmful destinations. Clicking on them can trigger cyberattacks, such as phishing, malware downloads, or potentially compromising the user's device or privacy.

Malware

/ mal-wair /

Attacks.

An umbrella term for any type of evil software designed with malicious intent. It includes viruses, worms, trojans and other harmful programs that can infect and damage computers, steal data, or perform other actions.

Malware-as-a-Service (MaaS)

/ mal-wair-az-a-ser-viss /

Attacks.

Who needs streaming platforms when you can subscribe to a virus instead? MaaS is a model in which cybercriminals offer malware-related services or tools on a subscription or pay-per-use basis. It enables less technically skilled individuals to access and deploy malware for malicious purposes.

Managed Service Provider (MSP)

/ man-ayjd ser-vis pro-vy-der /

Security.

MSPs are your trusty IT sidekicks, here to lend a hand (and a cape) when businesses need help. They offer outsourced IT services, including cybersecurity, and stand guard over your IT kingdom with proactive protection and round-the-clock support. It's a bit like having a tech-savvy fairy godmother!

Man-In-The-Middle (MITM) Attack

/ man-in-the-mid-ul ah-tak /

Attacks.

When an attacker becomes the third wheel by intercepting and possibly altering the communication between two parties without their knowledge — allowing them to eavesdrop and steal personal information.

Mitre ATT&CK (ATT&CK)

/ my-ter at-tak /

Practices.

Mitre ATT&CK, or simply ATT&CK, is a framework developed by Mitre Corporation that categorizes and describes tactics, techniques, and procedures (TTPs) commonly used by cyber adversaries. It helps organizations understand and defend against cyber threats.

Multifactor Authentication

/ mul-tee-fak-ter auth-en-ti-kay-shun /

Authentication.

A security process that requires users to provide two or more forms of identification before gaining access to a system or account. This enhances security by combining different factors like passwords or biometrics — keeping your account safe and sound!

Network Detection and Response

/ net-wurk dih-tek-shun and ri-spons /

Practices.

With this security approach focusing on real-time monitoring, detection, and response to threats within a network environment, you'll always be one step ahead of cybercriminals.

Network Intrusion Protection System (NIPS)

/ net-wurk in-troo-zhun pro-tek-shun sis-tem /

Practices.

Your digital watchdog, patrolling the virtual streets and barking loudly when it senses trouble. In reality, a security solution designed to monitor and analyze network traffic for signs of unauthorized or malicious activity. Identifies and responds to intrusion attempts in real-time, safeguarding the network from cyber threats and attacks.

Network Segmentation

/ net-wurk sehg-men-tay-shun /

Security.

The method of dividing a network into smaller, isolated segments to enhance security and control. By separating different parts of the network, the attacker's ability to move laterally and access other segments is restricted even if one of them is compromised. You know what they say: divide and rule!

Network Sniffing

/ net-wurk snif-ing /

Practices.

No, not cute doggy kind. This is the practice of intercepting and analyzing data packets as they traverse a network. While often used for legitimate purposes like network troubleshooting, it can also be exploited maliciously to capture sensitive information, making it a concern for cybersecurity.

Packet Sniffer

/ pak-it snif-er /

Technologies and Tools.

No, still not the four-legged, furry, magical creature. A sniffer is a tool or software that captures and examines data packets traveling through a network. It helps analyze network traffic for diagnostic or security purposes but can also be misused to intercept unencrypted information.

Password Cracking

/ pass-word krak-ing /

Attacks.

When hackers put on their Sherlock Holmes hats and attempt to guess or decrypt passwords through various methods. A common technique attackers use to gain unauthorized access to accounts.

Passwordless

/ pass-word-less /

Authentication.

A method that eliminates the traditional use of passwords for user authentication. Instead, it relies on alternative practices such as biometrics, hardware tokens or mobile push notifications for more secure and user-friendly access. It's like they say: less is more!

Patch

/ pach /

Technologies and Tools.

A software update or modification that works like a bandaid. It's designed to fix vulnerabilities, bugs or security flaws in a program or operating system. Applying patches is essential to keep systems udated, as it addresses known weaknesses that could be exploited.

Patch Management

/ pach man-ayj-ment /

Technologies and Tools.

The process of acquiring, testing and applying updates to software, applications, and operating systems. This helps address vulnerabilities and security flaws. It's like brushing your teeth: not the most exciting task, but it protects your systems against bugs and cyberattacks.

Penetration Testing

/ pen-uh-tray-shun tes-ting /

Practices.

A digital security drill where cyberattacks are simulated to identify system vulnerabilities and assess security measures, with the goal of strengthening defenses proactively.

Perimeter Security

/ pe-rim-uh-ter se-kyoo-ri-tee /

Practices.

You know what they say about good fences making good neighbors? Well, the same goes for network security. These are protective measures implemented at the boundary of a network to defend against unauthorized access and cyber threats, like a firewall, for example.

Pharming

/ far-ming /

Attacks.

The sneakiest game in the digital arcade, where cyber attackers hold all the cards in the deck. Mastering the art of twisting domain names and sneakily editing hosts files, guiding unsuspecting users straight into their pixelated trap of malicious websites.

Phishing

/ fish-ing /

Attacks.

A deceptive tactic where attackers send fraudulent emails, messages, or websites to trick recipients into revealing sensitive information, such as passwords or credit card details.

Ransomware

/ ranz-um-wair /

Attacks.

Have you ever had your files held hostage by a digital thug? As the term implies, this malicious software encrypts a user's files or locks them out of their own system. Attackers then demand a ransom payment in exchange for providing the decryption key or restoring access.

Red Team

/ red teem /

Teams and Roles.

A group of skilled cybersecurity experts who simulate real-world cyberattacks on an organization's systems, networks, and physical security. The goal of the red team is to identify vulnerabilities that might be missed by regular security measures. Go, Red Team!

Remediation

/ reh-mee-dee-ay-shun /

Security.

Imagine if you had a doctor examining your computer system. This is the process of identifying and addressing vulnerabilities, weaknesses or issues found during security tests. It involves taking corrective actions to mitigate the risks and improve security.

Remote Monitoring and Management (RMM)

/ reh-moht mon-it-or-ing and man-ayj-ment /

Security.

Think of Remote Monitoring and Management (RMM) as the magic wand in the toolkit of MSPs*, their digital wizard's apprentice. RMM allows for real-time monitoring, troubleshooting, and maintenance of network devices to ensure security and performance. It's the enchanted key to success for MSPs!

Rootkit

/ root-kit /

Attacks.

A particularly nasty type of software designed to gain unauthorized access to a computer system or network by concealing its presence, granting a hacker "root"-level (administrative) privileges. It is often used to hide other malware or provide persistent access for cybercriminals, making it difficult to detect and remove.

Sandboxing

/ sand-box-ing /

Practices.

Think of it like a science experiment: you isolate an application, software, or process within a controlled and secure environment to be able to analyze its behavior. This is commonly used to test potentially malicious files or programs to understand their actions, without risking harm to the rest of the system.

SCADA

/ skah-duh /

Practices.

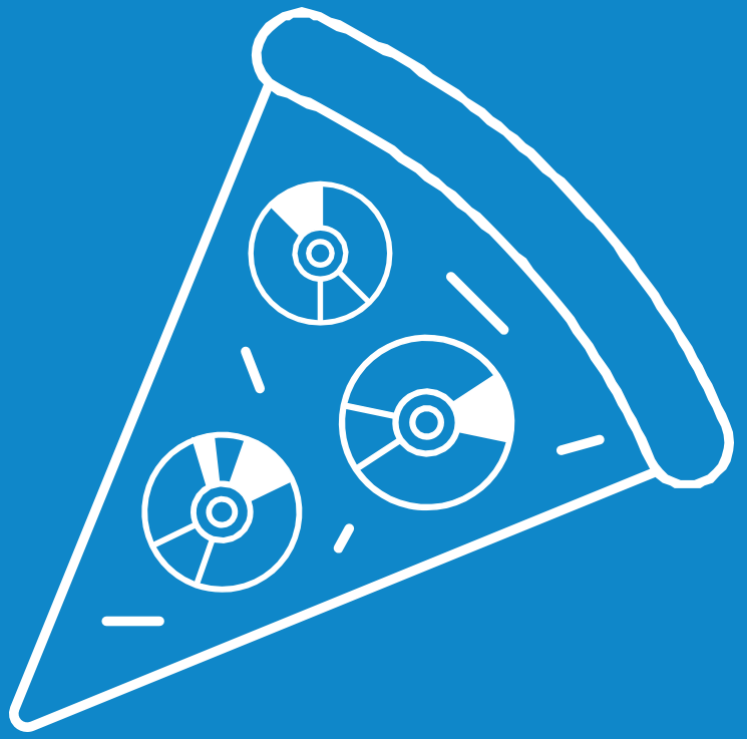
SCADA, which stands for Supervisory Control and Data Acquisition, refers to a system used to monitor and control industrial processes and critical infrastructure. The industry superhero we all need to keep the lights on, the machines humming, and the water flowing, making our world a better, safer, and more fun place to be!

Script Kiddie

/ skript ki-dee /

Teams and Roles.

A derogatory term used to describe amateur hackers with limited technical skills who use readily available hacking scripts or tools to launch cyberattacks. While part of the junior league, they shouldn't be underestimated, as their reckless attacks and lack of experience can cause actual damage.



Salami Fraud

/ sa-lah-mee frod /

Attacks.

A cybercrime technique often used in financial or accounting fraud schemes, where the perpetrator embezzles tiny fractions of money from transactions or accounts, hoping to fly under the radar. Sneaky, but not very savory.

SD-WAN

/ es-dee-wan /

Security.

Imagine if your internet had a personal trainer. This technology uses software to centrally manage and optimize the performance of wide-area networks, improving connectivity and security.

Secure Access Service Edge (SASE)

/ seh-kyoor ak-sess ser-vis ej /

Security.

SASE is a cloud-based security framework that combines network security and wide-area networking (WAN) capabilities to provide secure and scalable access to network resources for remote and branch office users. The Swiss Army knife for network security!

Security Awareness Training

/ seh-kyoor-i-tee uh-wair-nis trayn-ing /

Practices.

An educational program for employees and individuals to raise awareness of cybersecurity threats and best practices. Like a virtual self-defense class, it aims to help people recognize and respond effectively to security risks.

Security Operations Center (SOC)

/ seh-kyoor-i-tee op-uh-ray-shunz sen-ter /

Practices.

Your cybersecurity SWAT team, dedicated to vigilant oversight, monitoring, and expert management of your data. Whether operating within your organization or across the digital realm, these cyber guardians maintain a cutting-edge stance, protecting your data like the digital superheroes they are!

Security Information and Event Management (SIEM)

/ seh-kyoor-i-tee in-fur-may-shun and i-vent man-ayj-ment /

Practices.

SIEM is a comprehensive cybersecurity solution that combines security information management (SIM) and security event management (SEM). The Sherlock Holmes of cybersecurity, merging the powers of a detective and an event coordinator. It collects and analyzes security data from various sources to detect, and springs into action to thwart cyber threats.

Security Policy

/ seh-kyoor-i-tee pol-uh-see /

Practices.

Picture a security policy as the digital constitution of your organization, laying down the law on how to protect and manage IT treasures. It’s the user-friendly map that guides us through the cyber jungle!

Security Token

/ seh-kyoor-i-tee toh-ken /

Authentication.

Meet the security token, a cyberspace gadget used to authenticate a user's identity. The token, either physical or digital, generates temporary, one-time codes or cryptographic keys, adding an extra layer of security to the login process.

Session Hijacking

/ sesh-un hi-jak-ing /

Attacks.

An attack where a person joins the party uninvited to take control of a user's session on a computer system or web application. This can lead to unauthorized access or manipulation of the victim's account.

Single Sign-On (SSO)

/ sin-guhl sain-ahn /

Authentication.

Who else is tired of trying to keep track of a million different usernames and passwords? This method allows users to access multiple applications or services with a single set of login credentials, enhancing convenience and security.

Smishing

/ smish-ing /

Attacks.

A form of phishing that occurs through messaging platforms. In these attacks, cybercriminals slide into people's DMs with deceptive and manipulative messages to trick recipients into revealing sensitive information, clicking on malicious links or downloading harmful attachments.

Social Engineering

/ soh-shul en-juh-neer-ing /

Attacks.

A technique cybercriminals use to trick individuals into divulging confidential information or performing actions that compromise security. Like a high-tech game of mind control, it often involves psychological manipulation through impersonation or deceit.

SQL Injection

/ es-kew-el in-jek-shun /

Attacks.

A cyberattack where someone tries to sneak some unwanted SQL code into the party. The malicious code is inserted into web application inputs, potentially compromising the associated database.

SQL code: Structured Query Language (SQL) code is a set of instructions used to interact with and manage relational databases, allowing you to perform tasks like retrieving, updating, and manipulating data. Like a wizard's spellbook for talking to databases – watch out for unwanted spells!

Spear Phishing

/ speer fish-ing /

Attacks.

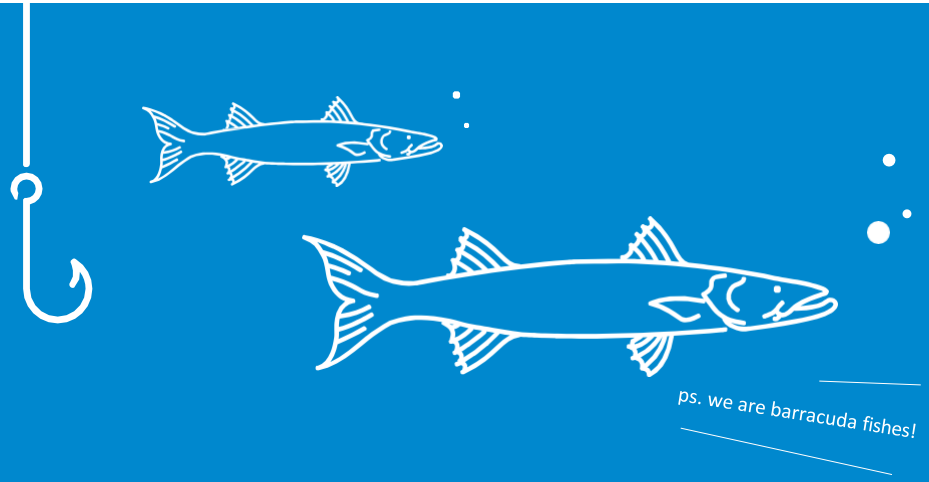
This is a tactic where cyber attackers create personalized messages to trick one or a select number of people into sharing sensitive information. So don't fall for it; your boss wouldn't ask you to purchase gift cards.

SSL Encryption

/ es-es-el in-krip-shun /

Attacks.

A trick used to turn secrets into a secret code. This process secures and protects data during transmission by converting it into an unreadable format that can only be deciphered by authorized parties.



SSL/ TLS (Secure Socket Layer)

/ seh-kyoor sawk-it lay-er /

Attacks.

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are cryptographic protocols used to secure data transmission over networks, commonly used for secure web browsing, email, and other online communications. TLS is the cool new kid on the block, the successor to SSL.

Threat Vector

/ thret vek-tor /

Attacks.

A threat vector is like the secret passage cybercriminals use to sneak into computer systems and networks without going through the main entrance. Cybersecurity professionals study these methods to pinpoint and neutralize potential weaknesses, helping to keep digital fortresses secure from unwanted intruders. It's all about knowing where the hidden trapdoors are!

Trojan

/ tro-jun /

Attacks.

An ancient attack in digital form. This is a type of malicious code or software disguised as legitimate, designed to damage, disrupt, steal, or inflict other harmful actions on your data or network.

VPN

/ vee-pee-en /

Security.

A cloak of invisibility for your online activity. This technology (even though considered slightly outdated) provides a secure and encrypted connection over a public network, enabling users to access private networks or the internet with enhanced privacy and security.

Vulnerability

/ vul-nuh-ra-bil-i-tee /

Practices.

A weakness or flaw in a computer system, software, or network that attackers can exploit to gain unauthorized access, disrupt operations, or steal data. Proof that no one is perfect – not even computer systems!

Web Application Firewall (WAF)

/ web ap-luh-kay-shun fai-er-wawl /

Technologies and Tools.

A WAF is like the vigilant guardian of your website, standing at the digital gate and scrutinizing incoming web traffic. Its mission? To shield your web applications from sneaky cyber threats like SQL injection, cross-site scripting (XSS), and other crafty application-layer attacks.

Whaling

/ wayl-ing /

Attacks.

A targeted form of phishing* attack aimed at high-profile individuals or senior executives within organizations. In this ultimate game of cat and mouse, cybercriminals craft sophisticated and convincing messages to deceive these individuals to gain access to sensitive company data, financial information or intellectual property.

White Hat Hacker

/ wyt hat hak-er /

Teams and Roles.

The antithesis of black hats*. Also known as an ethical hacker, a cybersecurity professional who legally and ethically tests systems and networks for vulnerabilities. They help organizations improve their security by identifying weaknesses and recommending fixes.

Whitelisting

/ wyt-list-ing /

Access.

The equivalency of having a VIP guest list for your network. This strategy involves creating a list of trusted applications, devices or users. Any entity not on the whitelist is denied access, enhancing security by only allowing known elements to interact with the system.

XDR

/ eks-dee-ar /

Extended Detection & Response.

Your multi-talented bodyguard. A holistic managed security service that integrates multiple security tools to detect and respond to threats across an organization's digital environment, such as endpoint, email, cloud, network, and server.

Zero Trust

/ zeer-oh truhst /

Practices.

A cybersecurity framework with some serious trust issues. It's like your digital bouncer, constantly checking IDs at the cyber club's door. No more VIP passes for sneaky cyber-criminals – everyone's got to earn their access, one byte at a time!

Zero-day

/ zeer-oh-day /

Attacks.

By the time you see it, it's already too late. This is a kind of software flaw that attackers exploit before a fix is available, leaving zero days of protection.

ZTNA

/ zee-tee-en-ay /

Authentication.

This security framework is like a cyber-hotel where your data checks in, but only you hold the key. Just like you need your lift key card to reach your floor, you need that digital pass to access your private room in the digital realm, ensuring no unwelcome guests crash your virtual party!

About Computer Troubleshooters Indooroopilly

Our offers of IT Services to you are based on your needs. We customise the services you need to keep your business protected and supported. We don't have a one model fits everyone, but based on our proven technologies and Vendors we can offer a tailored solution to fit your requirements and budget.

We should be your first call when you have security questions, when your network breaks down, when your machine or software needs to be upgraded, or when viruses, spyware, and other malware rear their ugly heads. You don’t need to have a long-term maintenance contract although that’s a service that we provide to many of our clients. In fact, no matter who you are and no matter what your needs, all you have to do is pick up the phone and your problem is as good as solved, your questions are good as answered.

MSP Barracuda
Your journey, secured.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP’s partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information. @BarracudaMSP | LinkedIn: BarracudaMSP | blog.barracudamsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com

CYBERSECURITY DICTIONARY - 2024 EDITION -