CYBERSECURITY DICTIONARY

A to Z

PROTECTED
HARBOR

Introduction

Navigating the ever-evolving cybersecurity landscape can often feel like deciphering a complex code. This cybersecurity dictionary is your go-to resource for demystifying essential cybersecurity terminology. Dive into these 150 critical terms in an engaging way. Whether you're aiming to advance your career, protect your organization, or stay updated on the latest cyber threats, this dictionary is your key to mastering the language of cybersecurity.

About Protected Harbor

As a dedicated managed service provider, Protected Harbor empowers IT service providers to deliver multi-layered security and data protection services to their clients. Through our award-winning products and purpose-built MSP management platforms, we provide robust, scalable solutions tailored to how managed service providers build and grow their businesses. Protected Harbor's partner-first approach emphasizes providing enablement resources, industry expertise, and comprehensive MSP solutions designed to support the unique needs of our partners.

LEARN MORE

Index

2FA
(Two-factor Authentication)

A security measure that requires two different methods of verification to access an account or system. Think of it like having two locks on your door—extra protection!

Access Control

The process of deciding who gets to enter a digital space. It regulates who can access certain resources or data within a system by using authentication methods to ensure that only authorized users can see or do certain things.

Account Takeover

When cybercriminals take control of a user's online account by exploiting weak passwords or using phishing attacks. It's a good reminder to avoid using easily guessed passwords like your birthday!

Advanced Penetration Testing

A simulated cyberattack to test the strength of your security system. It's like giving your defenses a test run to find any weaknesses.

Advanced Encryption Standard (AES)

A widely-used encryption method that secures sensitive data, ensuring that it can only be accessed with the right decryption key. It's like a secret handshake in the digital world.

Air Gap

A physical separation between computer systems, like a moat around a castle, used to prevent unauthorized data transfer and protect against cyber threats like malware and ransomware.

Advanced Threat Protection

A security approach with multiple layers that goes beyond standard defenses to protect against new, unknown attacks, like zero-day threats.

Anna Kournikova Virus

A notorious computer worm from the early 2000s, named after the tennis player Anna Kournikova. It spread through email by tricking users into opening an attachment that claimed to show a picture of the celebrity, but instead, it infected their computers.

Anti-malware

A protective software that acts like a superhero for your computer, detecting, preventing, and removing harmful programs like viruses, spyware, and other malware.

Anti-spam

A solution that filters out unwanted emails, helping to protect users from spam, phishing attacks, and other email scams.

Application Firewall

A security tool that monitors and controls the traffic going to and from an application, protecting it from unauthorized access, attacks, and vulnerabilities.

As a Service

A model where services or resources are delivered over the internet on a subscription basis, eliminating the need for managing local infrastructure.

Attack Surface

If your system were a fortress, the attack surface would be all the possible entry points—like secret doors—that attackers could exploit. This includes vulnerabilities, interfaces, and network connections. Keeping the attack surface small is key to better security.

Backdoor

A hidden way into a computer system that bypasses the usual security measures. It’s like a secret trapdoor that hackers use to access data or systems without permission.

Backup

A digital copy of your data or system, created as a safety net in case of disaster. It ensures that you can recover important information if something goes wrong.

BadUSB

A malicious USB device that can infect computers with harmful software. Not all USBs are created equal—some are designed to do more harm than good.

Biometric Authentication

The future is now! This authentication method uses unique physical traits, like fingerprints or facial features, to verify identity and securely access systems.

Black Hat Hacker

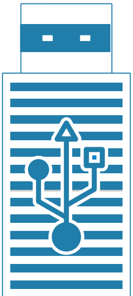
The villains of the hacking world. Black hat hackers break into networks with malicious intent, often spreading malware or causing damage.

Blue Team

The heroes of cybersecurity! A team of security experts responsible for defending a company against cyberthreats, always ready to protect and respond.

Bot Attacks

These attacks use automated software (bots) to perform harmful activities like stealing data or gaining unauthorized access. Let’s hope they don’t start a robot rebellion!



Botnet

A network of hijacked devices controlled by a single attacker, often used to launch large-scale cyberattacks—like the supervillain of the internet.

Broken Access Control

When users gain unauthorized access to restricted areas due to security flaws or misconfigurations, leading to potential breaches.

Browser Hijacker

A type of malware that changes your browser settings without permission, redirecting you to unwanted sites or displaying annoying content.

Brute Force Attack

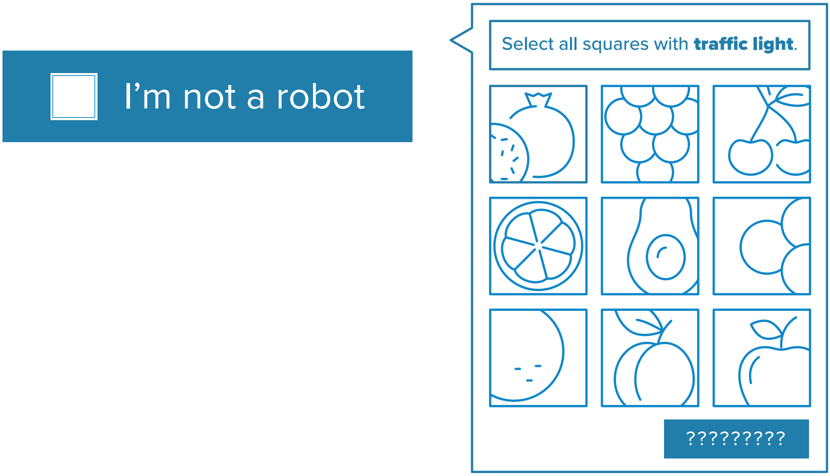
An attack where a hacker tries every possible password combination until they find the right one—simple but effective.

Buffer Overflow Attack

This attack overwhelms a program's memory, potentially allowing a hacker to execute malicious code and take control of the system.

CAPTCHA

A security test on websites to distinguish humans from bots, usually by solving a puzzle. It’s meant to be easy for humans but can sometimes be frustrating.



C&C Server (Command and Control)

A central system used by cybercriminals to control compromised devices in a botnet, directing them to perform harmful activities like DDoS attacks or data theft.

Cerber Ransomware

A type of ransomware that encrypts a victim’s files and demands a ransom for the decryption key, spreading through phishing emails or malicious websites.

Certificate-based Authentication

A security method where digital certificates act as the key to secure access, ensuring only authorized users can enter and communicate safely in the digital world.

Clickjacking

A deceptive technique where attackers trick users into clicking something different from what they think, often leading to unintended actions or exposure of sensitive information.

Cloud-to-Cloud Backup

A backup strategy that transfers data directly between cloud services, providing an extra layer of protection for your data.

Cold Data

Older or less frequently accessed data stored in a lower-tier system to optimize storage costs and performance, much like storing seasonal clothes in the back of your closet.

Command Injection

An attack where malicious commands are inserted into input fields, manipulating a system to execute unintended actions or gain unauthorized access.

Code Injection

A cyberattack where malicious code is inserted into a software application to exploit security flaws and execute unauthorized commands.

Common Vulnerabilities and Exposures (CVEs)

A database of publicly disclosed security vulnerabilities and exposures that helps track and communicate security issues across the cybersecurity community.

Cookie Theft

An attack where session cookies are intercepted or stolen, allowing attackers to impersonate users and gain access to their accounts.

Credential Stuffing

A technique where stolen login credentials are used to access multiple accounts due to the reuse of passwords.

Credentials

Information used to verify a user's identity, such as usernames and passwords, granting access to secure systems or services.

Cross-Site Scripting (XSS)

A vulnerability where malicious code is injected into a website, allowing attackers to execute scripts in the context of unsuspecting users.

CTB Locker

A ransomware that encrypts files on a victim's computer and demands a Bitcoin ransom for the decryption key, known for its strong encryption and wide file type targeting.

Cryptographic Key

A piece of information used in cryptographic algorithms to encrypt and decrypt data, crucial for ensuring data confidentiality.

Cryptography

The practice of securing communication and data through encryption, creating a secret language for authorized parties to decipher.

Cyber Insurance

Insurance that helps businesses recover financially from cyberattacks and data breaches, providing a safety net in case of cybersecurity incidents.

Cyber Resiliency

A strategy to protect against cyberattacks and security breaches by preventing attacks, planning effective responses, and ensuring business continuity.

Cyberattack

Uninvited digital intruders aiming to steal data, cause disruptions, or damage systems, making them the unwelcome guests of the cyberworld.

Cybersecurity Framework

A structured set of guidelines and best practices designed to help organizations implement effective security measures and protect their systems.

Daemon

A background process or program that performs various tasks on a computer system. While it helps manage system components, it can also be exploited for malicious purposes.

Data Audit

An examination of data and records to assess accuracy, security, and compliance, helping to identify vulnerabilities and ensure data integrity.

Dark Web

A hidden part of the internet accessible only through specialized browsers, often associated with illegal activities.

Data Breach

Unauthorized access or disclosure of sensitive information, leading to potential exposure of personal data and damage to reputation.

Data Encryption

The process of converting plaintext into unreadable ciphertext using cryptographic techniques, ensuring that only authorized parties can access the data.

Data in Transit

Information being transmitted between devices or networks, protected by encryption to prevent interception and unauthorized access.

Data Loss

The accidental destruction, corruption, or compromise of information due to hardware failures, software errors, human mistakes, or cyberattacks.

Data Loss Prevention

Policies and technologies designed to prevent the leakage, loss, or inappropriate sharing of sensitive information.

Data in Transit Encryption

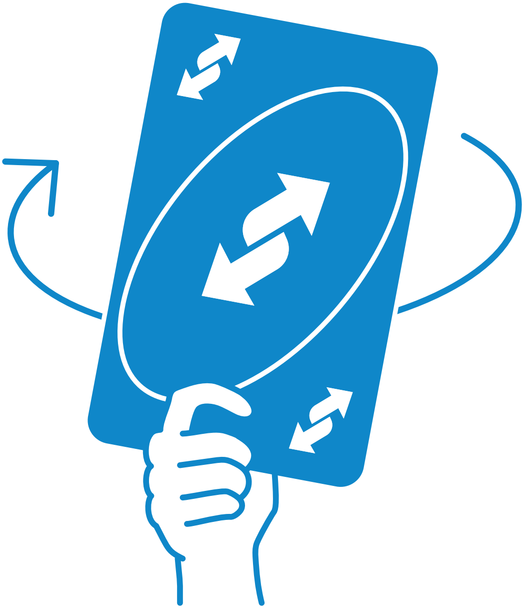
A security measure that protects information while it is being transmitted over networks, ensuring it remains unreadable to unauthorized users.

Data Wiping

Say goodbye to your data forever! Data wiping is the secure erasure of information from storage devices, ensuring it cannot be recovered. It’s often done before repurposing or disposing of devices to prevent data leaks.

Decryption

Like unscrambling eggs, decryption is the process of converting encrypted data back into its original, readable form using a decryption key or algorithm.



DDoS (Distributed Denial of Service)

A digital flood where multiple compromised computers overwhelm a target system, network, or website with excessive traffic, rendering it inaccessible.

DNS Attack

A cyber criminal's attempt to tamper with the internet's address book, targeting the Domain Name System to disrupt or manipulate domain name resolution, leading to security vulnerabilities.

Domain Hijacking

A cyber heist where criminals take control of a domain name without permission, potentially leading to harmful activities like website defacement or phishing attacks.

DomainKeys Identified Mail (DKIM)

The fingerprints of the digital world, DKIM helps verify the authenticity of an email using cryptographic signatures, ensuring it hasn’t been altered in transit and came from the claimed sender.

Drive-By Download

A type of cyberattack where malware is automatically downloaded onto a user’s computer without consent when visiting a compromised website. Regular software updates are key to staying safe.

Dyreza

A sophisticated banking Trojan designed to steal sensitive financial information from victims. It spreads through phishing emails or malicious downloads and can facilitate financial fraud.

Email Bomb

A cyberattack that floods a target's inbox with an overwhelming volume of spam emails, potentially disrupting communication and overloading email servers.

Email Encryption

Like sealing a letter in a digital envelope, email encryption protects the content of your messages from unauthorized access. It ensures that only the intended recipient can read sensitive information in emails.

Email Fraud

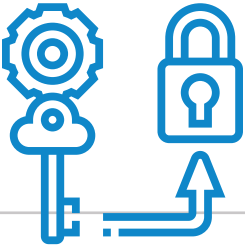
The classic scam of sending deceptive emails to trick recipients into sharing sensitive information or transferring funds to unauthorized accounts. It's the digital version of a con artist's playbook.

Encryption

Encryption turns readable data (plaintext) into a coded form (ciphertext) using cryptographic algorithms. This process protects the data, ensuring only authorized parties can unlock the original information, much like a high-security vault.

End-to-End Encryption

Think of end-to-end encryption as a secret code shared between you and a friend. It ensures that only you two can read the message, keeping it hidden from anyone else trying to peek.



Endpoint Security

Your devices, like computers and phones, get VIP protection with endpoint security. These measures safeguard against malware, unauthorized access, and other cyber threats.

Ethical Hacking

Ethical hacking is like a controlled heist where the hacker is hired to break into a system to find vulnerabilities before the bad guys do. The goal is to improve security by identifying and fixing weaknesses.

Exploit

An exploit is a hacker's secret weapon: a program or code that takes advantage of a security flaw in a system or application, allowing unauthorized actions or access.

False Flag

Straight out of a spy thriller, a false flag is a deceptive tactic where cybercriminals or nation-state actors disguise their actions to appear as though they were carried out by someone else, making it harder for investigators to trace the real culprit.

Firewall

Picture a cyber bouncer at a digital nightclub, only letting in the right guests while keeping out unauthorized intruders. That's what a firewall does for your network.

Formjacking

The cyber equivalent of a heist, formjacking involves injecting malicious code into a website's forms to secretly capture sensitive information, like credit card details, entered by users.

Geo-blocking

Geo-blocking is the digital equivalent of border control, restricting access to content based on your geographical location. It's often used to comply with regional laws or licensing agreements.

Gray Hat Hacker

A gray hat hacker walks the line between good and bad. They may expose vulnerabilities without permission but usually aim to help organizations improve their security.

Green Team

A specialized group of security experts who dive into the digital jungle to conduct proactive security assessments and testing. They collaborate with the blue (defensive) and red (offensive) teams to enhance an organization's overall security posture.

Hardening

The process of fortifying a system's defenses by reducing its attack surface and minimizing vulnerabilities. This involves configuring systems, networks, or software by disabling unnecessary services and regularly updating them, staying one step ahead of cybercriminals.

Honeypot

A decoy system set up to lure cyber attackers. By attracting threats, security experts can study their tactics and behaviors in a controlled environment without risking real systems.

Impersonation Attack

An attack where the cybercriminal pretends to be a trusted entity to deceive users into sharing sensitive information or performing specific actions. It's like a digital con artist in disguise.

Incident Response

A systematic approach for managing and mitigating the impact of a cybersecurity incident. It includes identifying the incident's scope, containing the damage, eradicating the threat, and enhancing future response efforts. Handling a cyber incident is akin to playing chess — always planning several moves ahead.

Intrusion Detection System (IDS)

The digital equivalent of an alarm system. IDS monitors network traffic and system activities to detect unauthorized access or malicious activities, raising alerts for further investigation if anything suspicious is detected.

Insider Threat

The risk posed by individuals within an organization, such as employees or contractors, who misuse their access privileges. It's a situation where the threat comes from inside the house, potentially causing significant harm.

Intrusion Prevention System (IPS)

A proactive security solution designed to detect and prevent unauthorized or malicious activities within a network or system. IPS identifies suspicious activity and takes immediate action to block or mitigate potential threats, serving as a frontline defender in cyberspace.

IoT (Internet of Things)

A network of interconnected physical devices, objects, and sensors that can collect and exchange data over the internet. From smart appliances and wearables to industrial machines and connected cars, IoT is like a high-tech family reunion of devices all communicating in the digital universe.

IoT Exploitation

When cybercriminals exploit vulnerabilities in IoT devices to gain unauthorized access, control, or steal data. It’s a game of hide and seek where the attackers try to sneak in undetected to manipulate or extract valuable information from these connected devices.

IoT Exploitation

When cybercriminals exploit vulnerabilities in IoT devices to gain unauthorized access, control, or steal data. It’s a game of hide and seek where the attackers try to sneak in undetected to manipulate or extract valuable information from these connected devices.

IP Reputation

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

Keychain

A digital vault on a computer or mobile device that securely stores cryptographic keys, passwords, and certificates. It helps protect these credentials, ensuring secure communication and authentication.

Keylogger

A type of spyware that secretly records a user’s keystrokes on a computer or mobile device, capturing sensitive information such as passwords, credit card numbers, and personal messages.

Kovter

A sophisticated and evasive fileless malware that attacks Windows operating systems. Kovter hides its configuration data in the computer’s registry, making it difficult for traditional antivirus software to detect and remove.

Lateral Movement

Techniques used by cyber attackers to move deeper into a network or system after gaining initial access. This allows them to explore the environment, gain increased privileges, and potentially access more sensitive information.

Least Privilege

A security practice that grants users the minimum level of access necessary to perform their roles. It’s like giving employees keycards that only allow them into specific areas, reducing the risk of unauthorized access or misuse of resources.

Link Encryption

A security measure that encrypts the entire data link or connection, protecting data transmitted over a network from being intercepted or decrypted by unauthorized parties.

Logic Bomb

A piece of malicious code inserted into a computer system that is triggered by specific conditions, such as a certain date or time. It can cause data loss or other damage, often being used by insiders or attackers with knowledge of the target system.

Malicious Email

An email with harmful intent, often containing malware attachments, phishing links, or fraudulent requests aimed at deceiving the recipient.

Malicious Links

URLs embedded in emails, websites, or messages that lead to harmful destinations. Clicking on these links can trigger cyberattacks, such as phishing, malware downloads, or compromising the user's device or privacy.

Malware

A broad term for any type of malicious software, including viruses, worms, trojans, and other harmful programs designed to damage computers, steal data, or perform other malicious actions.

Malware-as-a-Service (MaaS)

A cybercrime model where malware-related services or tools are offered on a subscription or pay-per-use basis, allowing individuals, even those with limited technical skills, to deploy malware for malicious purposes.

Managed Service Provider (MSP)

MSPs are your reliable IT allies, always ready to step in when businesses need support. They deliver outsourced IT services, including cybersecurity, and ensure your IT environment remains secure with proactive protection and 24/7 monitoring. It’s like having a tech-savvy guardian angel! Protected Harbor offers comprehensive cybersecurity solutions tailored for MSPs and their clients. Our platform, solutions, and 24/7 SOC empower you to deliver Cybersecurity-as-a-Service in a time of escalating threats and limited talent. In addition to providing security services, we're dedicated to helping you educate your customers, increase sales, and grow your business.

Man-In-The-Middle Attack

A scenario where an attacker secretly intercepts and possibly alters the communication between two parties, effectively becoming an unnoticed third party. This allows the attacker to eavesdrop on the conversation and steal sensitive information.

Mitre ATT&CK

The Mitre ATT&CK framework, created by the Mitre Corporation, categorizes and details the tactics, techniques, and procedures (TTPs) that cyber adversaries commonly use. It's an invaluable tool for organizations to better understand and defend against cyber threats.

Multifactor Authentication

A security process that requires users to provide multiple forms of identification before gaining access to a system or account. By combining different factors like passwords, biometrics, or tokens, it significantly enhances security and keeps your account well-protected.

Network Detection and Response

A security strategy focused on real-time monitoring, detection, and response to threats within a network environment. It ensures that you stay one step ahead of cybercriminals, safeguarding your digital assets.

Network Intrusion Protection System

Your digital watchdog, vigilantly monitoring network traffic for signs of unauthorized or malicious activity. This security solution analyzes and responds to intrusion attempts in real-time, protecting your network from potential cyber threats and attacks.

Network Segmentation

A security strategy that involves dividing a network into smaller, isolated segments. By compartmentalizing the network, you limit an attacker's ability to move laterally, reducing the risk of widespread compromise even if one segment is breached. Think of it as "divide and conquer" for your network's defense.

Network Sniffing

The act of intercepting and analyzing data packets as they travel through a network. While often used for legitimate purposes like troubleshooting, it can also be exploited to capture sensitive information, making it a potential cybersecurity risk.

Packet Sniffer

Not your average dog! A packet sniffer is a tool or software that captures and examines data packets traveling across a network. It’s used for analyzing network traffic, diagnosing issues, or ensuring security, but it can also be misused to intercept unencrypted data.

Password Cracking

When attackers channel their inner detective to guess or decrypt passwords using various techniques. This common method is often employed to gain unauthorized access to accounts and systems.

Passwordless

A method that eliminates traditional passwords for user authentication. Instead, it uses alternatives like biometrics, hardware tokens, or mobile push notifications for more secure and user-friendly access. As they say, less is more!

Patch

A software update or modification that acts like a bandaid, designed to fix vulnerabilities, bugs, or security flaws in a program or operating system. Applying patches is crucial to keeping systems secure and up-to-date, as it addresses known weaknesses that could be exploited.

Patch Management

The process of acquiring, testing, and applying updates to software, applications, and operating systems. It’s like brushing your teeth: not the most thrilling task, but essential for protecting your systems against bugs and cyberattacks.

Penetration Testing

A digital security drill where simulated cyberattacks are conducted to identify system vulnerabilities and assess security measures. The goal is to proactively strengthen defenses before real attackers strike.

Perimeter Security

Like a sturdy fence around a network, perimeter security consists of protective measures implemented at the boundary to defend against unauthorized access and cyber threats. Firewalls, for example, serve as one of these crucial defenses.

Pharming

A deceptive cyberattack where malicious actors manipulate domain names or hosts files, redirecting unsuspecting users to fake websites. It's like a digital trap that lures victims into providing sensitive information, all while thinking they're on a legitimate site.

Phishing

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. It's like a digital bait-and-switch, luring victims into a trap.

Ransomware

A form of malicious software that holds your files hostage, encrypting them or locking you out of your system entirely. Attackers demand a ransom payment in exchange for the decryption key or restoring your access, leaving victims scrambling to regain control.

Red Team

A group of skilled cybersecurity experts who simulate real-world cyberattacks on an organization's systems, networks, and even physical security. Their mission? To uncover vulnerabilities that regular security measures might miss, strengthening defenses from within.

Remediation

The process of identifying and fixing vulnerabilities or weaknesses in a computer system. Much like a doctor treating a patient, remediation involves taking corrective actions to mitigate risks and improve overall security health.

Remote Monitoring and Management (RMM)

RMM is the MSP's* digital magic wand, enabling real-time monitoring, troubleshooting, and maintenance of network devices from afar. It's an essential tool for keeping systems secure and running smoothly, like having a watchful eye on your IT kingdom at all times.

Rootkit

A stealthy and dangerous type of software designed to gain unauthorized access to a computer system or network. Rootkits grant hackers "root"-level (administrative) privileges while concealing their presence, often hiding other malware or ensuring persistent access. Detecting and removing them is notoriously difficult.

Sandboxing

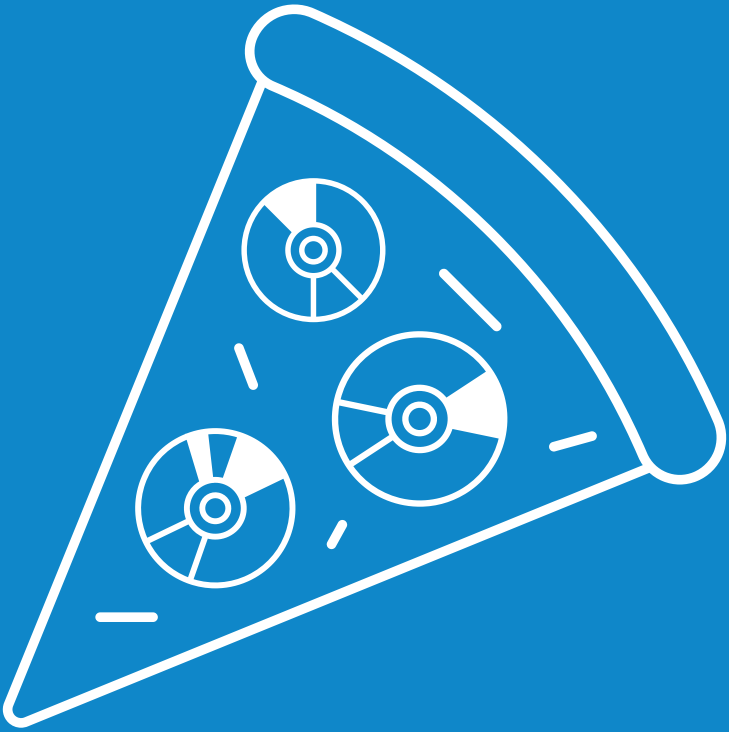
Imagine a science experiment where you can safely isolate and observe an application, software, or process within a controlled environment. Sandboxing allows you to analyze potentially harmful files or programs without risking damage to the rest of the system.

SCADA

SCADA, short for Supervisory Control and Data Acquisition, is the unsung hero of industrial systems. It monitors and controls critical infrastructure, ensuring that everything from power grids to water supplies runs smoothly, keeping our modern world functioning safely and efficiently.

Script Kiddie

A term used to describe amateur hackers with limited technical skills who rely on pre-made hacking scripts or tools. While they lack expertise, their reckless use of these tools can still cause significant damage.



A sneaky cybercrime tactic where small amounts of money are skimmed from numerous transactions or accounts, aiming to fly under the radar. It's a subtle, but potentially profitable, form of financial fraud.

SD-WAN

Think of SD-WAN as your internet's personal trainer. This technology uses software to manage and optimize the performance of wide-area networks, enhancing both connectivity and security.

Secure Access Service Edge (SASE)

SASE is a cloud-based security framework that merges network security and wide-area networking (WAN) capabilities into a single solution. It provides secure, scalable access for remote and branch office users, acting as the Swiss Army knife for network security.

Security Awareness Training

An educational program designed to arm employees with the knowledge to recognize and respond to cybersecurity threats. Like a digital self-defense class, it aims to improve awareness and encourage safe practices in the workplace.

Security Operations Center (SOC)

Your cybersecurity SWAT team, vigilantly monitoring and managing your organization's data. Whether in-house or outsourced, these cyber guardians are always on the front lines, ready to protect your digital assets from threats.

Security Information and Event Management (SIEM)

SIEM is the Sherlock Holmes of cybersecurity, combining the power of a detective and an event coordinator. It collects and analyzes security data from multiple sources to detect, investigate, and respond to cyber threats.

Security Policy

Think of a security policy as your organization's digital constitution. It sets the rules and guidelines for protecting and managing IT resources, providing a clear path through the complex cyber landscape.

Security Token

Think of a security token as a digital key fob for the cyber world. Whether physical or digital, it generates temporary, one-time codes or cryptographic keys that authenticate a user's identity, adding an extra layer of security to the login process.

Session Hijacking

An attacker secretly takes over a user's active session on a computer system or web application. This allows them to gain unauthorized access or control over the user's account, often leading to data breaches or identity theft.

Single Sign-On (SSO)

Tired of juggling multiple usernames and passwords? Single Sign-On (SSO) is here to help. This method lets users access multiple applications or services with just one set of login credentials, streamlining the process and boosting security.

Smishing

A cyber variant of phishing that targets you through text messages or other messaging platforms. Attackers use deceptive messages to trick recipients into revealing sensitive information, clicking on malicious links, or downloading harmful attachments.

Social Engineering

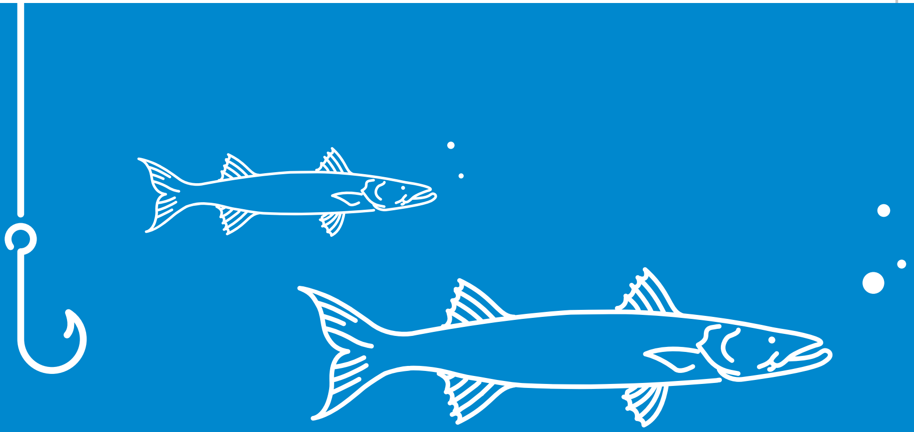
A cunning tactic where cybercriminals manipulate individuals into giving up confidential information or performing actions that compromise security. Often involving psychological tricks like impersonation or deceit, it's like mind control for the digital age.

SQL Injection

An attacker injects malicious SQL code into a web application's input fields, attempting to exploit vulnerabilities in the associated database. If successful, they can gain unauthorized access, manipulate data, or even take control of the entire system.

Spear Phishing

A highly targeted phishing attack where cybercriminals craft personalized messages aimed at specific individuals or groups. These deceptive messages often appear to come from a trusted source, like a boss or colleague, tricking victims into sharing sensitive information.



SSL/TLS (Secure Socket Layer)

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are protocols that encrypt data transmitted over networks, ensuring secure web browsing and online communication. TLS is the newer, more secure successor to SSL, often used to protect sensitive data.

SSL Encryption

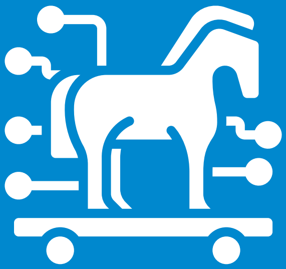
The process of encoding data during transmission to prevent unauthorized access. SSL encryption turns data into an unreadable format, ensuring that only authorized parties can decode and access the information, keeping it secure from eavesdroppers.

Threat Vector

The route or method used by cybercriminals to infiltrate a system, network, or device. Understanding these entry points allows cybersecurity professionals to identify and close vulnerabilities, strengthening defenses against potential attacks.

Trojan

A type of malicious software that disguises itself as legitimate to infiltrate a system. Once inside, it can damage, steal, or disrupt data, much like the infamous wooden horse from ancient times.



VPN (Virtual Private Network)

A technology that creates a secure, encrypted connection over a public network, acting like a cloak of invisibility for online activities. Though slightly outdated, VPNs are still widely used to ensure privacy and security when accessing private networks or the internet.

Vulnerability

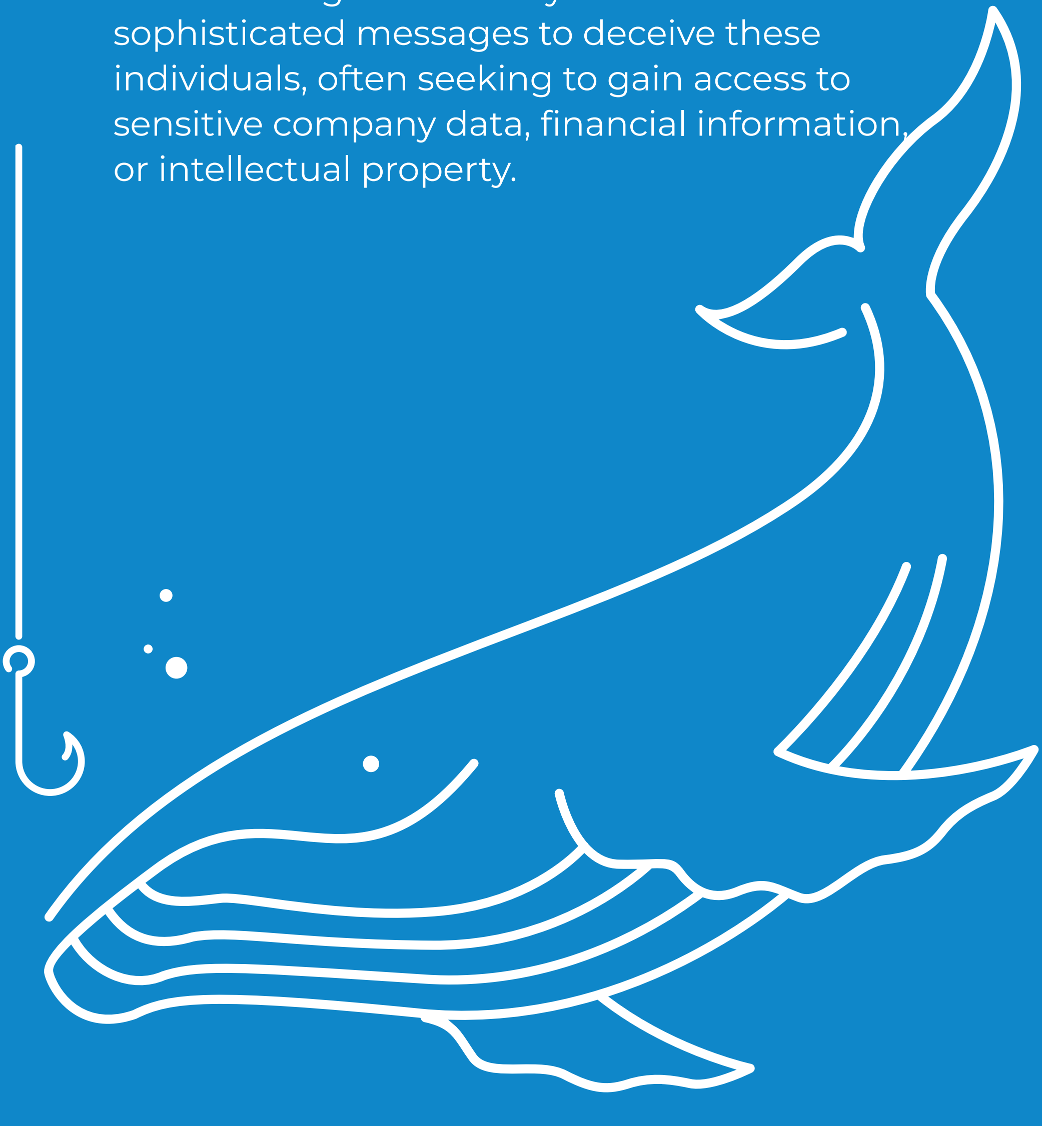
A flaw or weakness in a system, software, or network that can be exploited by attackers. Vulnerabilities are the digital equivalent of cracks in a fortress wall, and identifying them is crucial to prevent unauthorized access or damage.

Web Application Firewall (WAF)

A WAF acts as a vigilant guardian for your web applications, monitoring and filtering incoming traffic to protect against cyber threats like SQL injection, cross-site scripting (XSS), and other application-layer attacks. It stands at the front line, defending your digital assets.

Whaling

A highly targeted phishing attack aimed at senior executives or high-profile individuals within an organization. Cybercriminals craft sophisticated messages to deceive these individuals, often seeking to gain access to sensitive company data, financial information, or intellectual property.



White Hat Hacker

The ethical counterpart to black hat hackers. A White Hat Hacker is a cybersecurity professional who legally tests systems and networks for vulnerabilities. They help organizations strengthen their security by identifying weaknesses and providing recommendations for improvement.

Whitelisting

Similar to having a VIP guest list for your network, whitelisting is a security strategy where only pre-approved applications, devices, or users are granted access. This method enhances security by ensuring that only trusted entities can interact with the system.

XDR (Extended Detection & Response)

A comprehensive security service that acts like a multi-talented bodyguard, integrating various security tools to detect and respond to threats across an organization's digital environment, including endpoints, emails, cloud services, networks, and servers.

Zero Trust

A cybersecurity framework that operates on the principle of never trusting, always verifying. It's like a digital bouncer, ensuring that every user, device, and connection is continuously validated before being granted access, eliminating automatic trust within the network.

Zero-day

A type of cyberattack that exploits a software vulnerability before the developer has issued a patch or fix. The term "zero-day" refers to the fact that the software creator has had zero days to address the flaw, making these attacks particularly dangerous.

ZTNA (Zero Trust Network Access)

A security approach where access to network resources is granted only after the user's identity is thoroughly verified. Similar to a hotel where guests can only access their floor with a keycard, ZTNA ensures that only authenticated users can reach specific parts of the network, preventing unauthorized access.

PROTECTED HARBOR MANAGED SERVICE PROVIDER

PROTECTED
HARBOR