

Cybersecurity: Definition and Goals

Cybersecurity is the practice of protecting computers, networks, systems and data from unauthorized or malicious digital actions cisco.com cisa.gov. It encompasses technologies, processes and policies to defend against attacks that seek to steal, alter or disrupt information. The fundamental goals of cybersecurity are the **CIA triad: Confidentiality** (preventing unauthorized disclosure of data), **Integrity** (ensuring information is accurate and unaltered), and **Availability** (ensuring authorized users have reliable access to information)

nccoe.nist.gov techtarget.com. These three pillars guide security strategies in organizations. For example, encryption and access controls enforce confidentiality, digital signatures and checksums maintain integrity, and backups and redundancy preserve availability nccoe.nist.gov techtarget.com. In today's digital world, strong cybersecurity is essential to protect sensitive data and critical services from rapidly evolving threats (e.g. nation-state espionage, ransomware, etc.) across all industries cisco.com nccoe.nist.gov.

Key Threats and Attack Categories

Cyber threats take many forms. Common categories include:

- **Malware:** Malicious software (worms, viruses, trojans, spyware, etc.) that infects systems to steal data, damage networks or facilitate other attacks. For example, malware "is any software used to gain unauthorized access to IT systems in order to steal data, disrupt services or damage networks" cisa.gov. Malware can be delivered via infected downloads, email attachments, or drive-by website downloads.
- **Ransomware:** A specialized type of malware that encrypts files or systems and demands payment (usually cryptocurrency) for the decryption key. Ransomware "is a type of malware identified by specified data or systems being held captive by attackers

until a form of payment or ransom is provided” [cisa.gov](#) . Ransomware attacks on enterprises and institutions have surged in recent years, impacting hospitals, governments, and businesses.

- **Phishing and Social Engineering:** Deceptive attacks that trick users into revealing credentials or sensitive data. Phishing typically occurs via email or messaging, “enticing users to share private information using deceitful or misleading tactics” [cisa.gov](#) . Examples include fake emails that mimic a bank to steal login details, or voice phishing (“vishing”) calls asking for credit card info. Because phishing exploits human trust, it remains one of the most common breach vectors.
- **Distributed Denial-of-Service (DDoS):** Attacks that overwhelm a server, network or service with massive traffic, rendering it unavailable to legitimate users. A DDoS “is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target...with a flood of Internet traffic” [cloudflare.com](#) . Attackers typically use botnets of compromised devices to launch the flood. Well-known incidents include DDoS attacks on DNS providers or online retailers that caused widespread outages.
- **Insider Threats:** Security risks originating from within an organization. These involve employees, contractors or business partners who misuse legitimate access. CISA defines an insider threat as an insider “using their authorized access, intentionally or unintentionally, to do harm” to the organization’s systems or data [cisa.gov](#) [cisa.gov](#) . Insider threats can be **malicious** (e.g. an employee stealing data or planting malware)

Threat

Category	Description	Example/Impact
Malware	Software designed to harm, infiltrate or control systems cisa.gov . Includes viruses, worms, spyware, etc.	Infection of computers to steal data, create botnets, or delete
Ransomware	A type of malware that encrypts files or systems and extorts payment for recovery cisa.gov .	Attackers encrypt hospital patient data, demand bitcoin to restore access
Phishing	Social engineering attack (often via email) that tricks users into revealing credentials or clicking malicious links cisa.gov .	Fake email appearing from a colleague, credential theft.
DDoS	Overloading a network/service with traffic to deny service to legitimate users cloudflare.com .	Botnet flood on an online retailer during a sale.
Insider Threat	Risk from authorized users who misuse access (maliciously or accidentally) cisa.gov .	Employee with access to customer data unwittingly installs malware.

•

or **unintentional** (e.g. an employee falling for a phishing scam or accidentally exposing data). Studies show that human error – including insider mistakes – contributes to roughly 74% of data breaches [infosecinstitute.com](https://www.infosecinstitute.com).

Table: Threat Categories and Characteristics

Essential Practices and Principles

Effective cybersecurity relies on multiple best practices and design principles:

- **Zero Trust Architecture:** Treat **no user or device as inherently trusted**, even inside the network perimeter [ibm.com](https://www.ibm.com). The Zero Trust model enforces strict identity verification (“never trust, always verify”) for every user and device, typically on a per-connection basis [ibm.com](https://www.ibm.com). For example, every login attempt requires authentication and authorization checks, and network access is segmented so that each resource requires explicit permission. Many organizations are adopting Zero Trust to counter threats from remote work and cloud-based services [ibm.com](https://www.ibm.com).
- **Encryption:** Use strong cryptography to protect data both **at rest** (on disks/storage) and **in transit** (across networks). Encryption transforms data into coded form so that “unauthorized third parties...cannot understand the data” if intercepted [techtarget.com](https://www.techtarget.com). It is a cornerstone for confidentiality. Best practices include HTTPS/TLS for web traffic, VPN or encrypted tunnels, disk/file encryption, and secure key management. Many compliance standards (e.g. PCI-DSS, GDPR) explicitly require encryption of sensitive data.
- **Multi-Factor Authentication (MFA):** Require two or more independent authentication factors (something you know – e.g. password, something you have – e.g. security token or SMS code, and/or something you are – e.g. fingerprint) for login. MFA adds “extra layers of protection beyond what passwords alone can offer” [ibm.com](https://www.ibm.com). Even if a password is compromised, a second factor (like a one-time code or biometric) can prevent unauthorized login [ibm.com](https://www.ibm.com). Modern identity platforms strongly encourage or mandate MFA for all accounts, especially for privileged or remote access.
- **Network Segmentation:** Divide the network into smaller, isolated segments or zones to contain breaches and limit lateral movement [illumio.com](https://www.illumio.com). Network segmentation (e.g.

VLANs, subnets, access control rules) “breaks a large network into smaller, separate sections to stop the spread of breaches” illumio.com. Sensitive resources (databases, critical servers) are placed in their own segments with tight access controls. This way, if an attacker compromises one segment, they cannot easily access the entire network.

- **Least Privilege Principle:** Grant users and systems only the **minimum permissions** needed to perform their tasks. The principle of least privilege (POLP) “gives users limited access rights based on the tasks necessary to their job” crowdstrike.com. By restricting administrative rights and file access, the damage from a compromised account is minimized. Administrators should also implement just-in-time privilege elevation and regularly review access rights.
- **Defense in Depth (Layered Security):** Employ multiple, overlapping security controls (firewalls, antivirus, intrusion detection, access controls, monitoring, etc.) so that a failure of one control is mitigated by others. For instance, use both network firewalls and hostbased firewalls, endpoint protection plus email filtering, etc. This “onion” approach ensures attackers face multiple hurdles.
- **Regular Patching and Vulnerability Management:** Keep software and systems up-to-date. Unpatched vulnerabilities are a common exploit vector (e.g. EternalBlue, Log4j). Effective patch management processes identify, test and apply patches in a timely manner to close security holes. Likewise, routine vulnerability scanning and penetration testing help find and fix security gaps before attackers do.
- **Security Policies and Training:** Establish clear security policies (e.g. password policies, BYOD policies) and enforce them. Complement policies with regular security awareness training for all staff, emphasizing phishing awareness, secure usage, and incident reporting. Since human error causes the majority of breaches infosecinstitute.com, educating employees is a fundamental practice.

Key Technologies and Tools

Organizations deploy a range of security technologies. Major categories include:

- **Firewalls:** Hardware or software gateways that monitor and control traffic between networks (e.g. between an internal network and the Internet). A firewall “prevents unauthorized access to a network by inspecting incoming and outgoing traffic using a

•

set of predetermined security rules” [techtarget.com](#) . Firewalls can be traditional (packetfiltering), stateful (tracking connection state), or next-generation (with intrusion prevention, application awareness, etc.). They are often the first line of defense at network perimeters.

- **Antivirus/Anti-Malware:** Endpoint security programs that scan for, detect and remove known malware signatures. Antivirus software is “designed to prevent, detect, search and remove viruses and other types of malware from computers, networks and other devices” [techtarget.com](#) . Modern solutions include next-generation antivirus (NGAV) which use behavior analysis and machine learning to spot zero-day threats.

Endpoint Detection and Response (EDR): Advanced tools for monitoring and responding to threats on endpoints (desktops, laptops, servers). EDR continuously monitors end devices, logs system behaviors, and uses analytics to detect suspicious activity [crowdstrike.com](#) . It also provides rapid response capabilities like isolating an infected endpoint. EDR complements traditional antivirus by catching stealthy attacks (e.g. fileless malware) and enabling security teams to investigate incidents with detailed forensic data [crowdstrike.com](#) .

- **Security Information and Event Management (SIEM):** Centralized platforms that **collect, correlate and analyze** log and event data from across an organization’s IT infrastructure. SIEM solutions “help organizations recognize and address potential security threats and vulnerabilities before they...disrupt business operations” [ibm.com](#) . They aggregate logs from firewalls, servers, applications, etc., and use rules or AI to flag anomalies. SIEM is the backbone of a Security Operations Center (SOC), enabling realtime monitoring and incident response through alerts and dashboards [ibm.com](#) .

Technology/Tool	Function/Role
Firewall	Inspects and filters network traffic at boundaries techtarget.com . Enforces access rules to unauthorized connections.
Antivirus / Anti-Malware	Scans devices for malicious software and removes or quarantines it techtarget.com . Protects from known virus, trojans, spyware, etc.
EDR (Endpoint Detection & Response)	Continuously monitors endpoint activities to detect and investigate threats in real-time. Provides rapid containment and forensic data on compromises.

- Intrusion Detection/Prevention Systems (IDS/IPS):** Systems that monitor network or host activity for signs of intrusions. An IDS “monitors network traffic and devices for known malicious or suspicious activity” ibm.com, alerting administrators when a threat is detected. An IPS extends this by automatically **blocking** or mitigating detected threats
ibm.com. Signature-based IDS uses databases of attack patterns, while anomaly-based IDS uses behavior baselines. Today, IDS/IPS capabilities are often built into firewalls and intrusion appliances.
- Other Tools:** Additional categories include **email/web gateways** (filter spam/malicious links), **Web Application Firewalls (WAFs)** (protect web apps from attacks like SQL injection), **Data Loss Prevention (DLP)** systems (prevent exfiltration of sensitive data), **Encryption tools** (for email or disk encryption), **Identity and Access Management (IAM)** platforms (manage user accounts, single sign-on, MFA) and **cloud security tools** (CASB, cloud workload protection). Threat intelligence platforms, network anomaly detectors, honeypots and forensic tools also play roles.

Table: Key Cybersecurity Technologies and Their Functions

Technology/Tool	Function/Role
SIEM (Security Information & Event Management)	Aggregates logs/events from across IT systems for correlation and analysis. Detects and alerts security teams <small>ibm.com</small> . Supports incident response and compliance reporting
IDS/IPS (Intrusion Detection/Prevention)	Monitors network/host traffic for attack signatures or anomalies <small>ibm.com</small> . IDS alerts a suspicious activity; IPS can also block harmful traffic automatically <small>ibm.com</small> .
Web/App Security	(e.g. WAF, API security) Protects web applications and APIs from attacks like SQL injection, abuse, etc.
IAM & Authentication	Manages user identities, roles, and authentication (including MFA). Ensures only authorized systems and data.
Other	(e.g. VPN, DLP, CASB, Threat Intelligence platforms, Encryption tools) – each adds specific capabilities (secure remote access, data leakage prevention, cloud visibility, etc.).

Current and Emerging Trends

The cybersecurity landscape is rapidly evolving. Key trends include:

- **AI and Machine Learning:** AI is a double-edged sword in cyber. Attackers use AI to automate and enhance attacks (e.g. "AI-supercharged" malware generation, automated phishing) explodingtopics.com, while defenders deploy AI/ML in threat detection and response. Modern SIEMs and EDRs incorporate ML for anomaly detection. Generative AI is also beginning to be used for automated code analysis and creation of advanced attack tools. Conversely, cyber defenders are developing AI-driven models to predict and respond to threats faster paloaltonetworks.com paloaltonetworks.com. Industry forecasts predict AI/ML will play an increasing role in identifying sophisticated threats and automating mitigation paloaltonetworks.com.
- **Cloud Security:** As more data and applications move to public clouds, securing cloud environments is paramount. A 2024 survey found ~65% of organizations list cloud security as a top concern (projected 72% soon) cloudsecurityalliance.org. Attacks on cloud infrastructure (misconfigurations, stolen cloud keys) are rising cloudsecurityalliance.org. Trend drivers include multi-cloud adoption and SaaS proliferation cloudsecurityalliance.org. Defenses involve cloud-native controls (e.g. IAM for cloud resources, encryption of cloud data, Cloud Access Security Brokers), as well as shared responsibility models. The human factor remains critical: a significant portion of cloud breaches are due to misconfiguration or human error cloudsecurityalliance.org.
- **Quantum Computing Threats:** Advances in quantum computing pose a future threat to conventional cryptography. Powerful quantum computers could break widely used algorithms (RSA, ECC) that underlie current encryption. Experts warn such a breakthrough could arrive within the next decade nist.gov. In anticipation, standards bodies are developing **post-quantum cryptography**. In mid-2024, NIST finalized the first set of PQC algorithms designed "to withstand the attack of a quantum computer" nist.gov. Organizations are advised to begin planning migration to these quantum-resistant algorithms to protect long-term data confidentiality.

- **Cyber Warfare and Nation-State Attacks:** Geopolitical tensions have elevated state-sponsored cyber operations. Hostile nation-states increasingly conduct espionage, sabotage and influence campaigns via cyber means. Critical infrastructure (power grids, elections, defense systems) is a major target. For example, security experts predict “state-sponsored cyberattacks will remain a significant concern...as nation-states continue to target critical infrastructure” splashtop.com. High-profile incidents (industrial control system attacks, infrastructure breaches) underscore that cyber warfare requires robust national and corporate defense strategies. Collaboration between government and private sector (sharing threat intelligence, coordinated defense) is a growing priority to build resilience.
- **Zero Trust and Perimeterless Security:** The “cloud-first” and remote-work era has eroded traditional network perimeters. The Zero Trust philosophy (described above) is now being widely embraced across industries. Many governments even mandate it (e.g. the U.S. Executive Order of 2021 on cybersecurity directs federal agencies to adopt Zero Trust). Zero Trust is often cited as a critical trend to safeguard distributed systems and workforces (see Sec. 3).
- **IoT and 5G Security:** The explosion of Internet-of-Things (IoT) devices – many with weak built-in security – is creating new vulnerabilities. As 5G networks expand, billions of IoT/IoT devices will come online, vastly increasing the attack surface. Trend reports emphasize securing IoT at device and network levels and applying network segmentation and authentication. For example, organizations must secure IoT endpoints and apply rigorous network monitoring, as compromising IoT devices can provide attackers with network entry points.
- **Cybersecurity Automation and CaaS:** To cope with the overwhelming volume of alerts and talent shortage, many organizations are turning to automation and **Cybersecurity-as-a-Service (CaaS)**. Managed security services, orchestration tools (SOAR), and AI-driven automation are trending to improve efficiency. Supply chain security (e.g. vetting third-party vendors, use of SBOMs) is another major focus, as attacks like SolarWinds have shown.

•

In summary, the emerging trends are characterized by **increased automation (AI), migration to the cloud, new threat landscapes (quantum, IoT), and rising geopolitical cyber conflict**. Staying current means integrating advanced analytics (AI/ML), adopting cloud-native security, preparing for post-quantum cryptography, and collaborating on cyber defense strategies paloaltonetworks.com nist.gov splashtop.com .

Standards and Compliance Frameworks

Organizations worldwide follow various standards and regulations to guide cybersecurity controls and ensure legal compliance. Key examples include:

- **NIST Cybersecurity Framework (CSF)** – A voluntary U.S. framework providing guidelines to manage cyber risk. It organizes activities into five functions (Identify, Protect, Detect, Respond, Recover) and is widely adopted by government and industry. (See NIST Cybersecurity Framework for details.) NIST also publishes detailed security control catalogs (e.g. SP 800-53) and guidance (e.g. Risk Management Framework) used globally.
- **ISO/IEC 27001 (and ISO 27000 series)** – International standards for Information Security Management Systems (ISMS). ISO 27001 sets requirements for establishing, implementing and improving an ISMS. Organizations certified to ISO 27001 demonstrate systematic risk-based security programs. Complementary standards (ISO 27002, 27017, 27018, etc.) provide best-practice controls (e.g. for cloud or privacy).
- **GDPR (General Data Protection Regulation)** – European Union regulation (effective since 2018) that governs the protection of personal data of EU citizens. GDPR mandates “appropriate security of personal data” through technical and organizational measures crowdstrike.com, and requires breach notification within 72 hours. Non-compliance can incur

hefty fines (up to €20 million or 4% of global revenue). GDPR’s impact is global – any organization (even outside the EU) handling EU personal data must comply.

- **HIPAA (Health Insurance Portability and Accountability Act)** – U.S. law that includes the Security Rule, setting national standards for protecting **electronic protected health information (ePHI)**. Covered

Framework / Regulation	Scope / Region	Purpose
NIST Cybersecurity Framework (CSF)	U.S. (widely adopted globally)	Voluntary framework for managing cybersecurity risk (Identify, Protect, Detect, Respond, Recover functions).
ISO/IEC 27001	International	Standard for Information Security Management Systems (ISMS). Specifies requirements for a risk-based security program.
GDPR	European Union (global effect)	Regulation on personal data protection. Mandates safeguards (e.g. consent, reporting, data minimization) and high fines for non-compliance.
HIPAA	United States	Law protecting health information. Requires safeguards for ePHI (administrative, physical, technical) to ensure patient data privacy and security.
PCI-DSS	Global (for payment card data)	Security standard for organizations handling credit card data. Specifies secure payment processing (encryption, access control, logging, etc.).
Others (e.g. CMMC, FISMA)	Industry/Government	Various sector-specific requirements (e.g. government contractors, federal agencies, etc.) that mandate cybersecurity controls and maturity levels.

Entities (healthcare providers, insurers) must implement safeguards (access controls, audit logging, encryption, etc.) to ensure confidentiality, integrity and availability of patient data. Violations of HIPAA can lead to civil and criminal penalties.

Other Compliance Regimes: Industry-specific standards also influence cybersecurity. For example, **PCI-DSS** governs payment card data security; **SOX** affects financial data controls; **NERC CIP** addresses bulk electric system security; and **CMMC** (Cybersecurity Maturity Model Certification) is emerging for U.S. defense contractors. Many organizations implement cybersecurity controls in alignment with multiple frameworks to satisfy regulatory and customer requirements.

Table: Examples of Cybersecurity Standards and Regulations

These standards provide baselines. For instance, NIST publishes detailed guidelines (e.g. SP 800-53, SP 800-171) that map to CSF controls, and ISO 27001's Annex A lists control objectives. Adhering to such frameworks not only improves security posture but also helps meet legal obligations and customer trust.

The Human Factor: Training and Awareness

Humans remain both a critical defense layer and a vulnerability in cybersecurity. A welltrained workforce can prevent many attacks; untrained users often cause breaches. Key points:

- **Security Awareness Training:** Regular training programs educate employees about common threats (phishing, social engineering, safe web/email habits, password hygiene, etc.). Because human error underlies the majority of breaches (e.g. clicking phishing links, misconfigurations) infosecinstitute.com, effective training is essential. Training often includes simulated phishing campaigns to reinforce vigilance. Many guidelines (e.g. NIST SP 800-50) emphasize training as a fundamental control.
- **Social Engineering Risks:** Attackers exploit human trust and error. *Social engineering* encompasses tactics like phishing, spear-phishing (targeted), pretexting (fraudulent scenarios), baiting, vishing (voice phishing) and smishing (SMS phishing). For example, phishing "entices users to share private information using deceitful tactics" cisa.gov. Awareness programs teach users to verify requests for sensitive information and report suspicious communications.
- **Culture and Policies:** Organizations should promote a security-conscious culture. This includes clear policies (e.g. no sharing of credentials, reporting incidents promptly) and leadership support. Encouraging a "see something, say something" environment helps catch threats early. Regular reminders, posters and security champions can reinforce best practices.

- **Incident Drills and Response Training:** Beyond prevention, training also prepares staff for incident response (e.g. whom to notify, how to preserve evidence). Tabletop exercises and red-teaming (ethical hacking simulations) help test plans and human reactions.

In short, technology alone cannot solve security; **people** need to be informed, vigilant and engaged. Ongoing awareness campaigns and user training reduce the chance that attackers succeed through deception or carelessness infosecinstitute.com .

Career Paths and Certifications

The cybersecurity field offers diverse career paths, from technical specialist to managerial roles. Key roles include Security Analysts, Penetration Testers, Security Engineers, Security Architects, Incident Responders, Governance/Risk/Compliance (GRC) professionals, and Chief Information Security Officers (CISOs). Each role often benefits from specific industry certifications. Major certifications include:

- **CISSP (Certified Information Systems Security Professional)** – Offered by (ISC)², CISSP is a broad, advanced certification covering security management, architecture, engineering and more isc2.org . It is often regarded as the “gold standard” for experienced security professionals. CISSP requires at least five years of relevant experience and validates knowledge across eight domains (e.g. Security Risk Management, Asset Security, Network Security, etc.) isc2.org isc2.org . It suits roles like Security Manager, Architect or Consultant.
- **CEH (Certified Ethical Hacker)** – Offered by EC-Council, CEH focuses on penetration testing and ethical hacking techniques. It teaches how to think like an attacker, covering tools and methods for vulnerability identification, exploitation, and countermeasures. CEH is popular among Penetration Testers and Red Team members. (EC-Council also offers OSCE, ECSA etc. for advanced offensive skills.)

Certification	Issuing Body	Focus / Career Path	Experience Req. (min.)
CISSP	(ISC) ²	InfoSec management and architecture	5 years in security (2 dom
CEH	EC-Council	Ethical hacking and penetration testing	None formally required (years IT)
Security+	CompTIA	General cybersecurity fundamentals	None (recommended 2 y

-
- **CompTIA Security+** – A vendor-neutral entry-level certification covering fundamental cybersecurity concepts: threats, architecture, identity management, cryptography, etc. Security+ is widely recognized for junior security roles (e.g. Security Analyst, junior admin) and has no formal prerequisites (though 2 years IT experience is recommended). It validates baseline skills and is often required by employers or government DoD for Level 1 positions.
- **CISM (Certified Information Security Manager)** – Offered by ISACA, CISM is geared toward information security management and governance. It certifies ability to design and manage an enterprise security program. CISM requires at least five years of experience in security management, and is valued for roles such as Security Manager, CISO or IT Auditor. Domains include Security Governance, Incident Management, and Program Development.
- **Other Notable Certifications:** CISSP Associates, CCSP (cloud security), CRISC (risk and IT control), CISA (audit), GIAC and SANS certifications (e.g. GSEC, GPEN for technical specialists), OSCP (offensive pen-testing), and vendor-specific (e.g. Cisco CCNA Security). Career advancement often combines technical expertise with leadership (CISO) or specialization (e.g. forensic investigator).

Table: Common Cybersecurity Certifications


Issuing

Earning these certifications demonstrates expertise and can improve job prospects and salary. For example, CISSP-certified professionals often qualify for senior roles and are in high demand. The field also values practical skills: many professionals boost credentials through hands-on experience (labs, CTFs, projects) alongside certifications. Continuous learning (through training, conferences, and recertification) is necessary, as cyber threats and technologies constantly evolve.

Sources: Authoritative cybersecurity references and industry reports have been used throughout (e.g. NIST publications nccoe.nist.gov nist.gov, CISA guidance cisa.gov cisa.gov, and reputable tech media techtarget.com techtarget.com) to provide current, comprehensive information.


Certification	Body	Focus / Career Path	Experience Req. (min.)
CISM	ISACA	Security program management and governance	5 years in info security m
Other (CCSP, OSCP, CISA, etc.)	Various	Specialized domains (cloud, pen-test, audit, etc.)	Varies (1–5 years)
Citas			

 **What is cybersecurity? - Cisco** <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html>


 **What is Cybersecurity? | CISA** <https://www.cisa.gov/news-events/news/what-cybersecurity>


 **Executive Summary — NIST SP 1800-26 documentation**
<https://www.nccoe.nist.gov/publication/1800-26/VoIA/index.html>

 **What is the CIA Triad? | Definition from TechTarget**
<https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>

 **What is Encryption and How Does it Work? | Definition from TechTarget**
<https://www.techtarget.com/searchsecurity/definition/encryption>

 **Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency** <https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>

 **What is a distributed denial-of-service (DDoS) attack? | Cloudflare**
<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

 **Defining Insider Threats | CISA** <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>



Defining Insider Threats | CISA <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>



74% Data Breaches Are Due to Human Error | Infosec

<https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-databreaches/>



What Is Zero Trust? | IBM <https://www.ibm.com/think/topics/zero-trust>



What is Encryption and How Does it Work? | Definition from TechTarget

<https://www.techtarget.com/searchsecurity/definition/encryption>



What is MFA (Multifactor Authentication)? | IBM <https://www.ibm.com/think/topics/multi-factor-authentication>



Cybersecurity 101: Network Segmentation | Illumio

<https://www.illumio.com/cybersecurity-101/network-segmentation>



What is Principle of Least Privilege (POLP)? | CrowdStrike

<https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/principle-of-least-privilegepolp/>



What is a Firewall and Why Do I Need One? | Definition from TechTarget

<https://www.techtarget.com/searchsecurity/definition/firewall>



What is Antivirus Software? | Definition from TechTarget

<https://www.techtarget.com/searchsecurity/definition/antivirus-software>



What is EDR? Endpoint Detection & Response Defined | CrowdStrike

<https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-andresponse-edr/>



What is SIEM? | IBM <https://www.ibm.com/think/topics/siem>



What is an Intrusion Detection System (IDS)? | IBM

<https://www.ibm.com/think/topics/intrusion-detection-system>





What is an Intrusion Detection System (IDS)? | IBM


<https://www.ibm.com/think/topics/intrusion-detection-system>





7 AI Cybersecurity Trends For The 2025 Cybercrime Landscape


<https://explodingtopics.com/blog/ai-cybersecurity>


 **What are Predictions of Artificial Intelligence (AI) in Cybersecurity? - Palo Alto Netw...** <https://www.paloaltonetworks.com/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity>  **What are Predictions of Artificial Intelligence (AI) in Cybersecurity? - Palo Alto Netw...** <https://www.paloaltonetworks.com/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity>


 **What are Predictions of Artificial Intelligence (AI) in Cybersecurity? - Palo Alto Netw...** <https://www.paloaltonetworks.com/cyberpedia/predictions-of-artificial-intelligence-ai-in-cybersecurity>

 **Cloud Security in 2024: A Shifting Landscape | CSA**
<https://cloudsecurityalliance.org/blog/2024/06/27/cloud-security-in-2024-addressing-the-shiftinglandscape>


 **Cloud Security in 2024: A Shifting Landscape | CSA**
<https://cloudsecurityalliance.org/blog/2024/06/27/cloud-security-in-2024-addressing-the-shiftinglandscape>

 **Cloud Security in 2024: A Shifting Landscape | CSA**
<https://cloudsecurityalliance.org/blog/2024/06/27/cloud-security-in-2024-addressing-the-shiftinglandscape>

 **Cloud Security in 2024: A Shifting Landscape | CSA**
<https://cloudsecurityalliance.org/blog/2024/06/27/cloud-security-in-2024-addressing-the-shiftinglandscape>

 **NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST**
<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantumencryption-standards>

 **NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST**
<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantumencryption-standards>

 **Top 12 Cybersecurity Trends And Predictions For 2025**
<https://www.splashtop.com/blog/cybersecurity-trends-2025?srsltid=AfmBOoqtKgkoFAGjKm9wvjAhYSE5OzWd8aRj4QMA34y1bL05AiV75JgG>

 **The GDPR and Cybersecurity | CrowdStrike** <https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/general-data-protectionregulation-gdpr/>

 **CISSP Exam Outline**
<https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline>

2 CISSP Exam Outline

<https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline>

Todas las fuentes

