



THE DATA GAME Glossary

на
български



Съфинансирано от
Европейския съюз

Изразените възгледи и мнения са единствено на автора(ите) и не отразяват непременно тези на Европейския съюз или на OeAD-GmbH. Нито Европейският съюз, нито предоставящият орган могат да бъдат държани отговорни за тях.
Номер на проекта: 2023-1-AT01-KA220-ADU-000157050

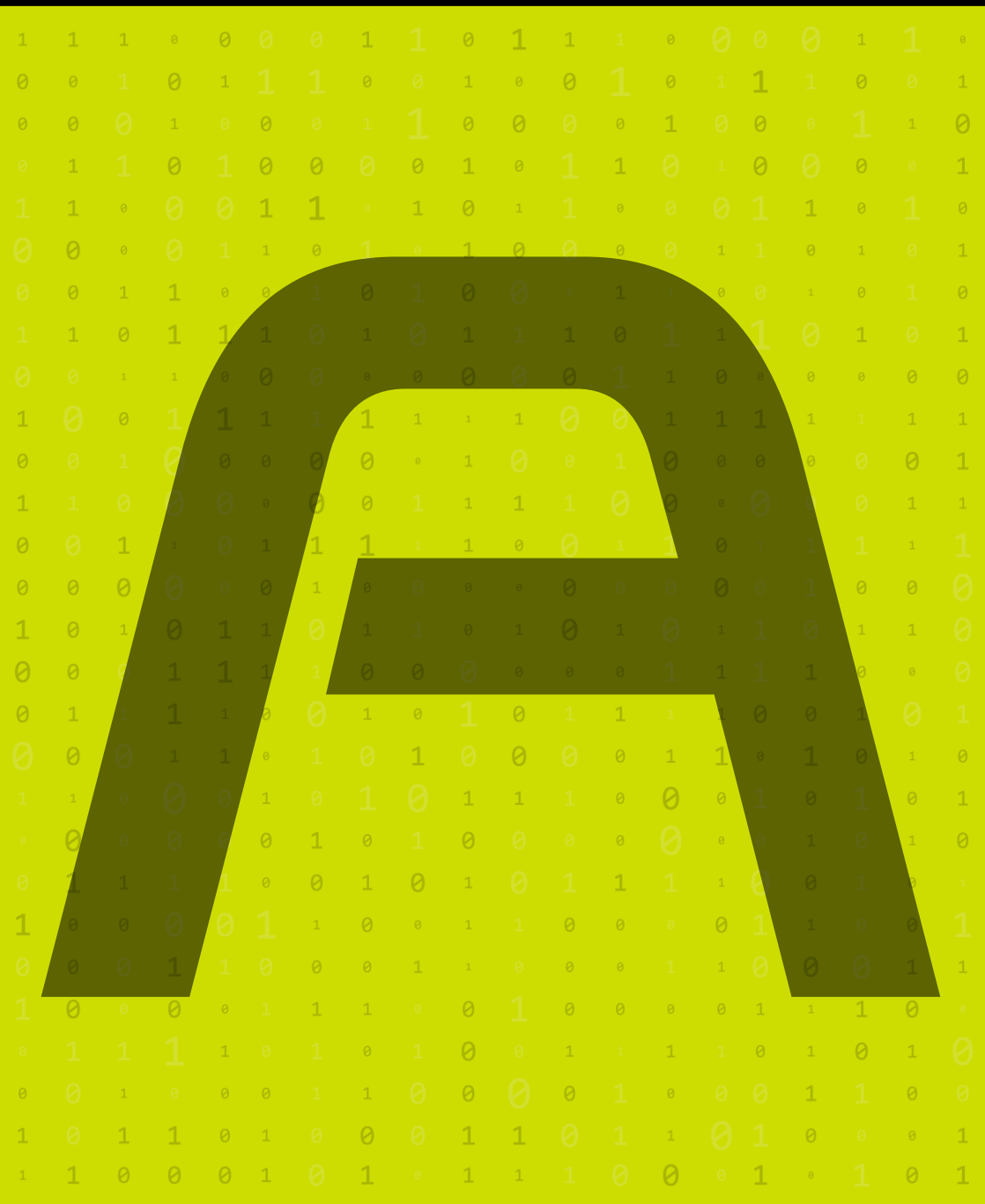


Тук ще намерите описанието на всеки непознат английски термин, на който може да се натъкнете в начинанията Ви в областта на поверителността и защитата на личните данни. Очаквайте скоро речника на български език!

И да, наистина сме взели този речник толкова сериозно, че да обясним термина „интернет“.

. . . Ами ако идвате от друга планета?





Z

"A"



Access Control - Mechanisms and policies that regulate who can view or use resources in a computing environment.

Access Control List (ACL) - A list of permissions attached to an object that specifies which users or systems are allowed to access it and what actions they can perform.

Access Management - The process of managing user access to resources and data within an organization.

Accountability - The principle that an organization or individual is responsible for their actions and decisions, especially concerning data privacy and security.

Active Directory - A Microsoft service for managing permissions and access to network resources within a domain environment.

Administrator Account - A user account with elevated privileges that allows the management of system settings and user accounts.

Advanced Encryption Standard (AES) - A symmetric encryption algorithm widely used to secure data, considered highly secure and efficient.

Advanced Persistent Threat (APT) - A prolonged and targeted cyberattack where an attacker gains unauthorized access to a network and remains undetected for an extended period.

Adware - Software that automatically displays or downloads advertising material (often unwanted) when a user is online.


Anomaly Detection - The process of identifying unusual patterns or deviations from normal behavior that may indicate a security threat.

Anonymisation - The process of removing personally identifiable information from data sets so individuals cannot be easily identified.

Anti-Malware - Software designed to detect, prevent, and remove malicious software, including viruses, worms, and spyware.

Antiphishing - Techniques and tools used to prevent phishing attacks, which attempt to deceive individuals into revealing sensitive information.

API Security - The practice of securing application programming interfaces to prevent unauthorized access and data breaches.



Application Security - The practice of protecting applications from threats and vulnerabilities throughout their lifecycle.

Application Vulnerability - A weakness in an application that can be exploited by attackers to compromise security or access sensitive data.

Application Whitelisting - A security measure that allows only approved applications to run on a system, blocking all others.

Asymmetric Encryption - A type of encryption that uses a pair of keys (public and private) for secure data transmission, where one key encrypts the data and the other key decrypts it.

Artificial Intelligence (AI) in Security - The use of AI technologies to enhance security measures, such as threat detection, risk assessment, and incident response.

Asset Management - The process of managing and securing an organization's physical and digital assets, including hardware, software, and data.

Attack Surface - The total area or set of entry points in a system or network that could be exploited by attackers.

Attack Vector - The method or pathway used by attackers to gain unauthorized access to a system or network.

Audit - A systematic examination of a system or process to ensure compliance with security policies and identify areas for improvement.

Audit Log - A detailed record of system events, including user actions and system changes, used for security monitoring and compliance.

Audit Trail - A chronological record of events, actions, or changes in a system that helps in tracking and monitoring user activities.

Authentication - The process of verifying the identity of a user or system, often through passwords, biometrics, or other methods.

Authentication Token - A digital object used to prove a user's identity and provide secure access to a system, often in the form of a hardware device or software-based code.

Authorisation - The process of determining whether a user or system has the right to access or perform certain actions on a resource.

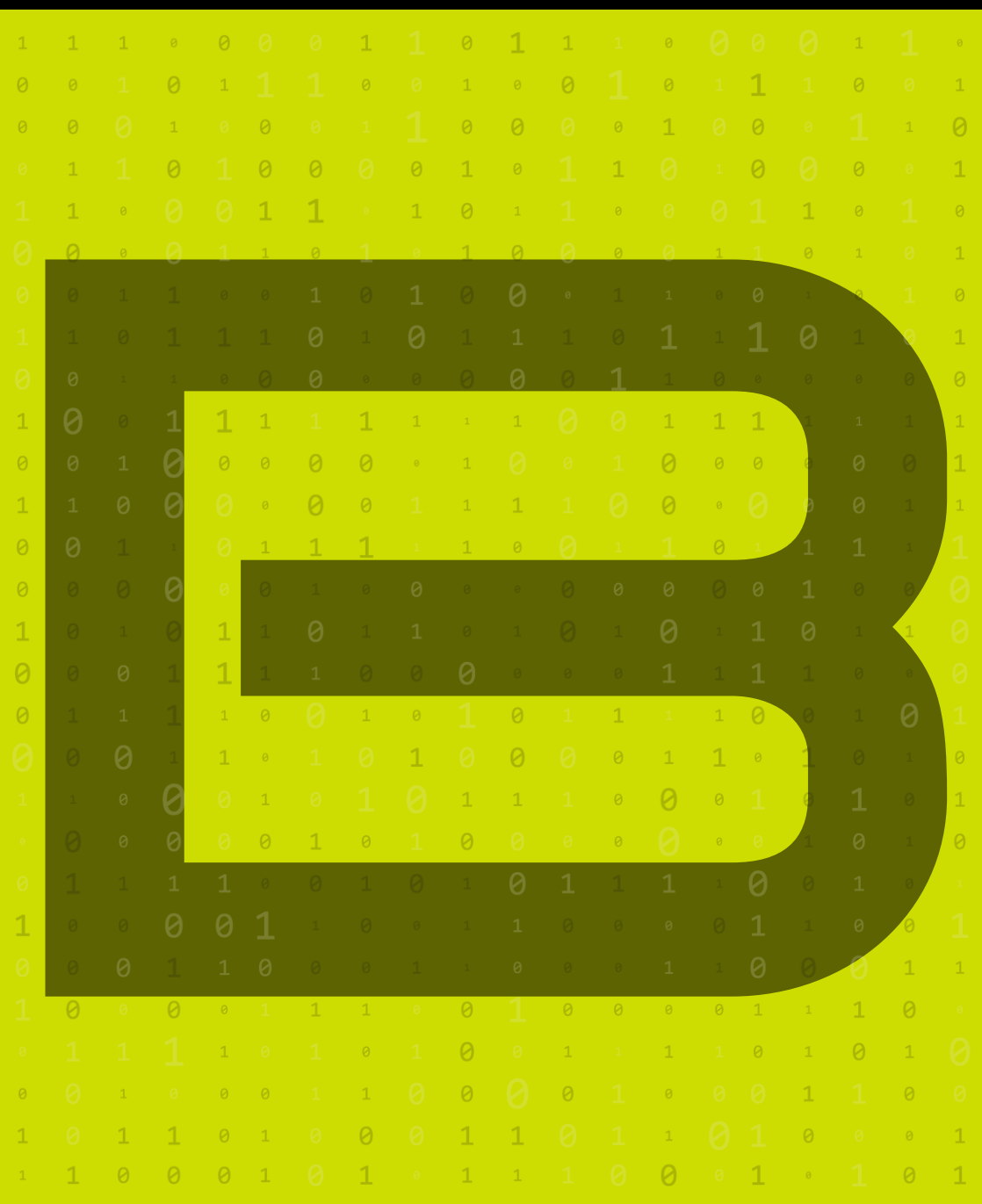



Authorization Protocol - A set of rules and procedures for determining and enforcing permissions for accessing resources and performing actions.

Automated Backup - A backup process that is scheduled and executed automatically, reducing the need for manual intervention.

Automated Threat Detection - The use of automated tools and technologies to identify and respond to potential security threats in real-time.

Availability - The assurance that data and resources are accessible to authorized users when needed, part of the CIA (Confidentiality, Integrity, Availability) triad in information security.





Backdoor - A hidden or unauthorized method of accessing a system or network, often created by attackers or malicious software to bypass normal security controls.

Backup - A copy of data or system files stored separately to prevent loss in case of a failure or data loss event.

Backup and Recovery - Processes and technologies used to create backups of data and restore them in the event of data loss or corruption.

Backup Encryption - The practice of encrypting backup data to ensure its confidentiality and prevent unauthorized access.

Backup Frequency - The interval at which backups are performed, which can range from hourly to annually, depending on the data's criticality.

Backup Integrity - The assurance that backup data is complete, accurate, and reliable, and has not been tampered with or corrupted.

Backup Policy - A set of guidelines and procedures for creating, managing, and restoring backups to ensure data integrity and availability.

Backup Solution - A comprehensive system or service designed to create, store, and manage backups to ensure data protection and recovery.

Backup Testing - The process of regularly verifying the effectiveness and reliability of backup procedures to ensure that data can be successfully restored when needed.

Baseline Security - The minimum level of security measures and practices required to protect an organization's assets and data from known threats and vulnerabilities.

Behavior-Based Detection - A security approach that identifies threats by analyzing patterns of behavior rather than relying solely on known signatures or patterns.

Behavioral Analytics - The analysis of user and system behavior patterns to detect anomalies and potential security threats.

Biometric Authentication - A method of verifying identity based on unique biological traits, such as fingerprints, facial recognition, or iris scans.

Biometric Authentication Systems - Systems that use biometric data (i.e., fingerprints, facial recognition) to verify and authenticate user identities.



Biometric Data - Information related to an individual's unique biological traits, used for authentication and identification purposes.

Biometric Verification - The process of confirming an individual's identity using biometric characteristics, such as fingerprints, voice, or iris patterns.

Biohacking - The practice of using biological techniques and technologies to enhance or manipulate human capabilities, which may raise privacy and security concerns.

Blacklist - A list of entities or IP addresses that are denied access to a system or network due to known malicious behavior or security risks.

Black Hat - A term used to describe hackers or security professionals who use their skills for malicious purposes, such as stealing data or disrupting systems.

Black Hat SEO - Malicious techniques used to manipulate search engine rankings unethically, which can be used to distribute malware or phishing attacks.

Blockchain - A decentralized digital ledger technology that records transactions across multiple computers, enhancing security and transparency.


Blockchain Security - The measures and protocols implemented to ensure the integrity, confidentiality, and security of blockchain transactions and data.

Blue Team - The team responsible for defending and securing an organization's systems and networks against cyberattacks and other security threats.

Bot Detection - Techniques and tools used to identify and block automated bots that may be used for malicious purposes, such as scraping data or launching attacks.

Bot Detection and Mitigation - Strategies and tools used to identify and counteract malicious bots that may compromise data security or disrupt services.

Botnet - A network of compromised computers or devices controlled by a malicious actor, often used for coordinated attacks or spreading malware.



Branded Malware - Malware that is designed to mimic legitimate software or services, often using familiar branding or names to deceive users.

Breach - An incident where unauthorized access or disclosure of data occurs, potentially compromising data privacy and security.

Breach Detection - Techniques and tools used to identify and respond to unauthorized access or data breaches in a timely manner.

Breach Notification - The process of informing affected individuals and relevant authorities about a data breach, as required by regulations and laws.

Brute Force Attack - A type of cyberattack where an attacker systematically tries all possible combinations of passwords or encryption keys until the correct one is found.

Browser Isolation - A security technique that isolates web browsing activity from the rest of the system to prevent malware infections and data breaches.

Browser Security - Measures and practices designed to protect web browsers from security threats, such as malware, phishing, and data breaches.

Buffer Overflow - A vulnerability that occurs when a program writes more data to a buffer than it can hold, potentially allowing an attacker to execute arbitrary code.

Buffer Zone - A security measure that creates a protected area around a critical system or network to prevent unauthorized access or attacks.

Business Associate - A person or entity that performs certain functions or activities on behalf of a covered entity, involving the use or disclosure of protected health information.

Business Associate Agreement (BAA) - A contract between a healthcare provider and a third-party service provider that outlines how the third party will protect sensitive health information in compliance with HIPAA.

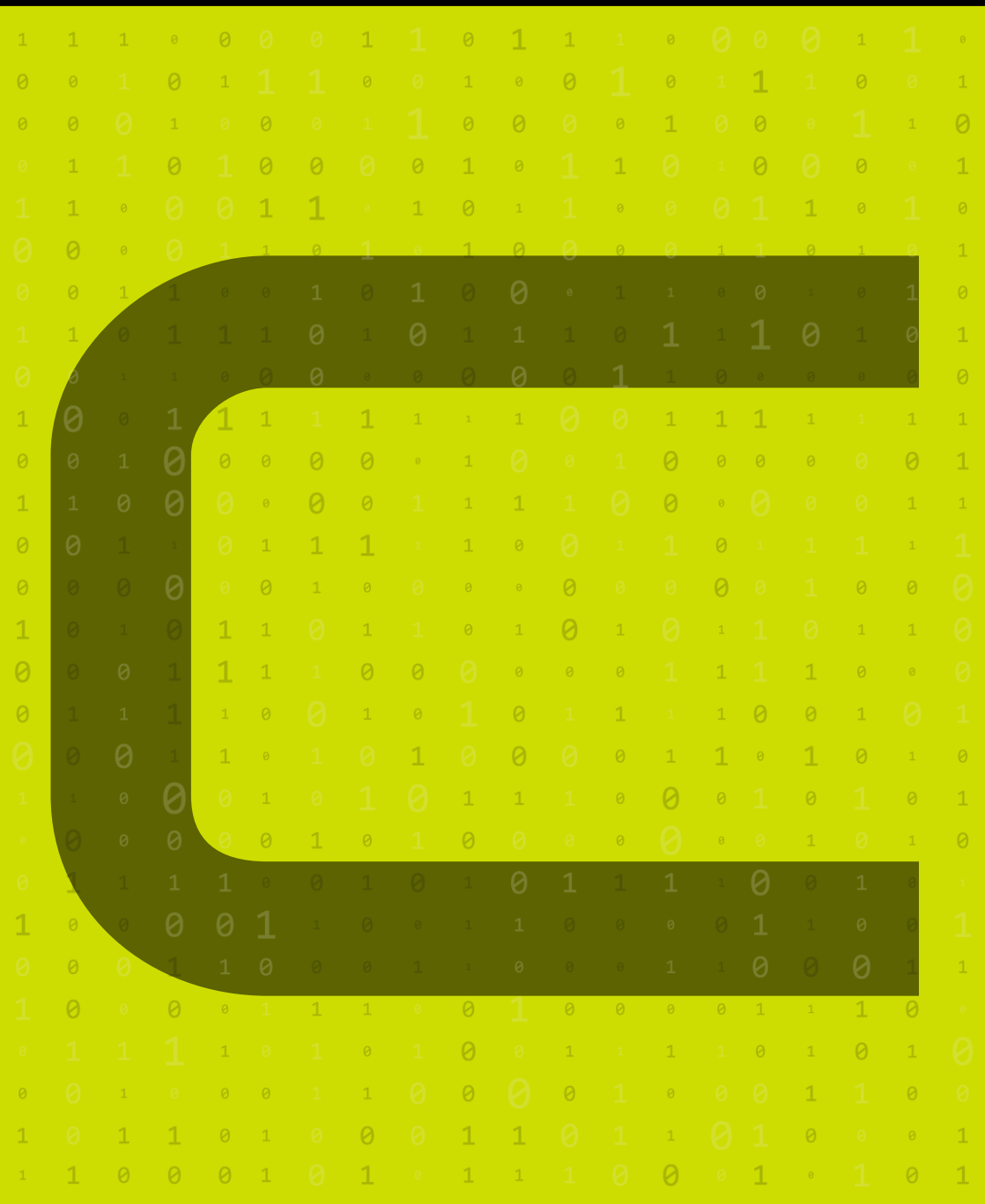
Business Continuity Planning (BCP) - The process of creating systems and procedures to ensure that critical business functions can continue during and after a disruption.




Business Process Outsourcing (BPO) - The practice of contracting third-party service providers to handle certain business functions, which requires careful management of data privacy and security.

Business Risk Management - The process of identifying, assessing, and mitigating risks that could impact business operations, including cybersecurity and data privacy risks.

Bypass - An action or method used to circumvent security measures or controls, often to gain unauthorized access or exploit vulnerabilities.





Case Studies - Detailed examinations of specific instances or scenarios related to data privacy challenges and solutions.

Certificate Authority (CA) - An entity that issues digital certificates used to verify the authenticity of websites, software, and communications.

Certified Information Systems Security Professional (CISSP) - A globally recognized certification for information security professionals demonstrating expertise in various cybersecurity domains.

Cloud Computing - The delivery of computing services over the internet, including storage, processing, and applications, which requires robust security measures.

Cloud Encryption - The process of encrypting data stored in or transmitted through cloud services to protect it from unauthorized access.

Cloud Security - The set of policies, technologies, and controls designed to protect data, applications, and systems hosted in cloud environments.

Compliance - Adherence to laws, regulations, standards, and policies related to data protection and cybersecurity.

Compliance Audit - A systematic review of an organization's adherence to data protection laws, regulations, and internal policies.


Compliance Management - The process of ensuring that an organization meets its legal and regulatory obligations related to data privacy and security.

Confidentiality - The principle of ensuring that information is accessible only to those authorized to have access, protecting it from unauthorized disclosure.

Confidentiality Agreement - A legal contract in which parties agree to keep certain information private and not disclose it to unauthorized individuals.

Configuration Management - The process of managing and maintaining system settings and configurations to ensure security and compliance.

Consent - The voluntary agreement of an individual to process their personal data for specific purposes.



Container Security - The practice of securing containerized applications and their associated data and configurations to prevent unauthorized access and vulnerabilities.

Content Filtering - The practice of blocking or allowing access to specific types of content on a network or system to protect users from harmful or inappropriate material.

Continuous Monitoring - The ongoing process of assessing and analyzing security events and vulnerabilities to detect and respond to threats in real-time.

Controlled Access - The practice of limiting access to systems, data, or resources to authorized individuals or entities only.

Cookie - A small piece of data stored on a user's device by a web browser, used to track user activity and preferences.

Cookies - Small pieces of data stored on a user's device by a website, used to track user activity and preferences.

Cross-Border Data Transfers - The movement of data across international borders, which may require compliance with specific regulations.

Cross-Site Scripting (XSS) - A vulnerability in web applications allowing attackers to inject malicious scripts into webpages viewed by other users.

Cryptographic Key - A piece of information used in cryptographic algorithms to encrypt or decrypt data.


Cryptography - The practice of using mathematical algorithms to encrypt and decrypt data, ensuring its confidentiality and integrity.

Cryptojacking - The unauthorized use of someone else's computing resources to mine cryptocurrency.

Critical Data - Information that is essential to an organization's operations and requires heightened protection due to its sensitivity.

Critical Infrastructure - The essential systems and assets that are vital to an organization's operations and whose disruption could have significant consequences.

Cyber Attack - An attempt by hackers or malicious actors to disrupt, damage, or gain unauthorized access to computer systems or networks.



Container Security - The practice of securing containerized applications and their associated data and configurations to prevent unauthorized access and vulnerabilities.

Content Filtering - The practice of blocking or allowing access to specific types of content on a network or system to protect users from harmful or inappropriate material.

Continuous Monitoring - The ongoing process of assessing and analyzing security events and vulnerabilities to detect and respond to threats in real-time.

Controlled Access - The practice of limiting access to systems, data, or resources to authorized individuals or entities only.

Cookie - A small piece of data stored on a user's device by a web browser, used to track user activity and preferences.

Cookies - Small pieces of data stored on a user's device by a website, used to track user activity and preferences.

Cross-Border Data Transfers - The movement of data across international borders, which may require compliance with specific regulations.

Cross-Site Scripting (XSS) - A vulnerability in web applications allowing attackers to inject malicious scripts into webpages viewed by other users.

Cryptographic Key - A piece of information used in cryptographic algorithms to encrypt or decrypt data.

Cryptography - The practice of using mathematical algorithms to encrypt and decrypt data, ensuring its confidentiality and integrity.

Cryptojacking - The unauthorized use of someone else's computing resources to mine cryptocurrency.

Critical Data - Information that is essential to an organization's operations and requires heightened protection due to its sensitivity.

Critical Infrastructure - The essential systems and assets that are vital to an organization's operations and whose disruption could have significant consequences.

Cyber Attack - An attempt by hackers or malicious actors to disrupt, damage, or gain unauthorized access to computer systems or networks.



Cyber Incident Response - The process of managing and addressing a cybersecurity incident to mitigate its impact and prevent further damage.

Cyber Insurance - A type of insurance designed to protect organizations from the financial impact of cyberattacks, data breaches, and other cybersecurity incidents.

Cyber Law - The body of laws and regulations governing activities related to cybersecurity, data protection, and digital communications.

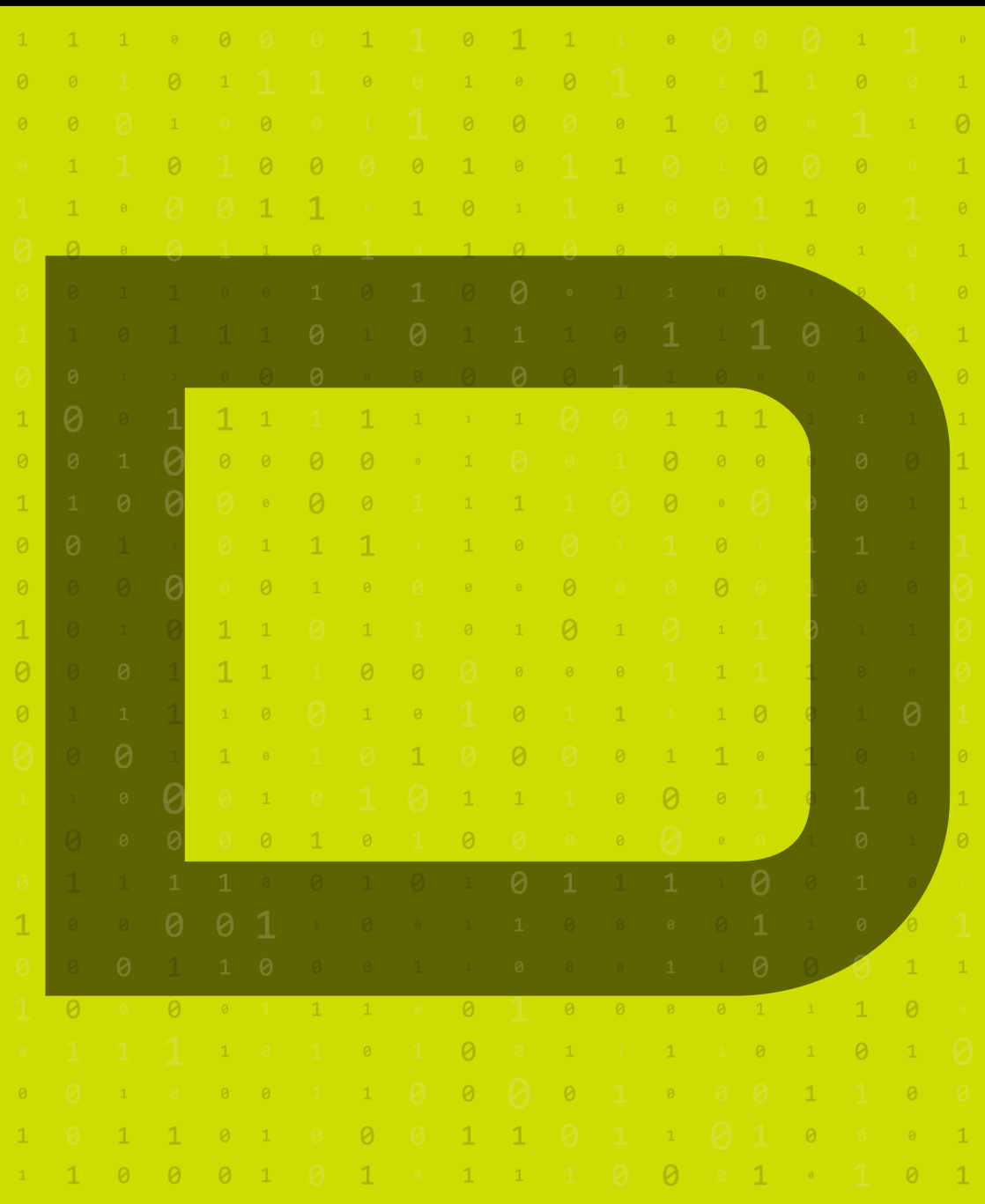
Cyber Resilience - The ability of an organization to withstand and recover from cyberattacks and other disruptions while maintaining essential operations.


Cybersecurity - The practice of protecting systems, networks, and data from digital attacks, theft, and damage.

Cybersecurity Framework - A set of guidelines and best practices designed to help organizations manage and reduce cybersecurity risk.

Cybersecurity Policies - Guidelines and rules designed to protect an organisation's digital assets from cyber threats.

Cyber Threat - A potential or actual malicious attack or activity that targets an organization's information systems or data.





Data Access Logs - Records of who accessed data, when, and what actions were taken.

Data Accuracy - The degree to which data correctly represents the real-world object or concept it is intended to model.

Data Aggregation - The process of combining data from multiple sources to analyze and extract useful information.

Data Aggregation Tools - Technologies used to combine data from various sources for analysis and reporting.

Data Anonymization - The process of transforming personal data so that the individual to whom the data relates can no longer be identified.

Data Breach - An incident where sensitive, confidential, or protected information is accessed, disclosed, or stolen by unauthorized individuals.

Data Breach Notification - The requirement to inform affected individuals and relevant authorities when a data breach occurs, often governed by regulations like the GDPR.

Data Breach Notification Regulations - Laws that require organizations to notify affected individuals and regulators in the event of a data breach.

Data Classification - The process of organizing data into categories based on its sensitivity and importance to ensure appropriate security controls.

Data Collection - The process of gathering data from various sources for analysis or processing.

Data Compliance Audit - An assessment conducted to ensure that data handling practices meet legal and regulatory standards.

Data Controller - An entity that determines the purposes and means of processing personal data, as defined by data protection laws like GDPR.

Data Destruction - The process of permanently erasing or destroying data to ensure it cannot be recovered or reconstructed.

Data Encryption - The process of converting readable data into an encoded format that can only be read by authorized users with the correct decryption key.



Data Encryption Standards - Protocols and guidelines for encrypting data to ensure its security.

Data Governance - A framework for managing data availability, usability, integrity, and security within an organization through policies, procedures, and controls.

Data Handling - The management of data throughout its lifecycle, including collection, storage, transfer, and deletion, in compliance with security and privacy standards.

Data Integrity - The accuracy and consistency of data throughout its lifecycle, ensuring it remains unaltered during transfer or storage.

Data Leakage - The unauthorized transmission of sensitive data from within an organization to an external or unauthorized recipient.

Data Lifecycle Management - The process of managing data from creation and storage to deletion or archiving.

Data Loss - The accidental or malicious destruction or deletion of data, which can occur due to hardware failures, cyberattacks, or human error.

Data Loss Prevention (DLP) - A set of tools and processes designed to detect and prevent the unauthorized use, transfer, or disclosure of sensitive data.

Data Masking - The process of obscuring specific data within a dataset to protect sensitive information while preserving its usability for authorized purposes.

Data Minimisation - The principle of collecting and retaining only the minimum amount of personal data necessary for a specific purpose, reducing privacy risks.

Data Portability - The ability to transfer personal data from one organization to another.

Data Portability Rights - The right of individuals to obtain and reuse their personal data across different services.

Data Processing - The operations performed on data, including collection, storage, modification, and deletion.



Data Processing Principles - Core principles governing how personal data should be processed, including lawfulness, fairness, and transparency.

Data Protection - The legal and technical measures designed to safeguard personal and sensitive data from unauthorized access, use, or disclosure.

Data Protection Authority (DPA) - A regulatory body responsible for overseeing the enforcement of data protection laws, such as GDPR.

Data Protection Impact Assessment (DPIA) - A risk assessment process that organizations use to evaluate the potential privacy risks associated with processing personal data.

Data Protection Officer (DPO) - An individual appointed to oversee and ensure compliance with data protection laws and practices, and ensure the proper handling of personal data.

Data Quality - The measure of data's accuracy, completeness, and reliability.

Data Redaction - The process of editing or blacking out sensitive information in a document before sharing it, to protect privacy or confidentiality.

Data Residency - The physical location where data is stored, which may have implications for compliance with data protection laws based on jurisdiction.


Data Retention - The policies and practices for storing data for a specified period before it is deleted or archived.

Data Retention Policy - A formal guideline that defines how long an organization retains data and the process for securely deleting it once it's no longer needed.

Data Sanitisation - The process of securely erasing or destroying data from a system to prevent it from being recovered.

Data Security - The protective measures taken to safeguard data from unauthorized access, corruption, or theft, ensuring its confidentiality, integrity, and availability.

Data Security Breach - An incident where unauthorized access, disclosure, alteration, or destruction of data occurs, compromising its confidentiality, integrity, or availability.



Data Sovereignty - The concept that data is subject to the laws and regulations of the country where it is stored.

Data Storage Solutions - Technologies and methods used to store data securely, including physical and cloud-based options.

Data Subject - An individual whose personal data is processed by an organization, as defined by data protection regulations like GDPR.

Data Subject Access Request (DSAR) - A request made by an individual to an organization to access the personal data it holds about them, in accordance with data protection laws.

Data Subject Access Requests (DSARs) - Requests made by individuals to access their personal data held by an organization.

Data Tokenisation - The process of replacing sensitive data with unique identification symbols or "tokens" that retain essential information without exposing the original data.

Data Transfer - Moving data from one system or location to another, which may involve compliance with data protection laws.

Data Transfer Agreement (DTA) - A legal document outlining the terms and conditions for transferring data between organizations, ensuring compliance with privacy and security regulations.


Data Use - How collected data is applied within an organization, including for analysis, reporting, and decision-making.

Data Validation - The process of ensuring that data is accurate, complete, and valid before it is processed or used.

Data Wiping - The process of securely erasing data from storage devices to prevent recovery, often used during decommissioning or hardware recycling.

Deep Packet Inspection (DPI) - A network monitoring method that examines the contents of data packets as they pass through a checkpoint, often used for identifying and mitigating threats.

Denial of Service (DoS) Attack - A cyberattack in which the attacker floods a network or service with excessive requests, rendering it unavailable to legitimate users.



Digital Certificate - An electronic document used to prove the identity of a website or user, often used in conjunction with encryption to secure online communications.

Digital Footprint - The trail of data an individual leaves behind when using digital platforms.

Digital Forensics - The process of collecting, analyzing, and preserving digital evidence from computers, networks, and devices in the investigation of cybercrimes or incidents.

Digital Identity - A set of attributes and credentials that define a user's identity in digital interactions, often verified through authentication methods like passwords or biometrics.

Digital Signature - An electronic, cryptographic signature used to verify the authenticity and integrity of a message, document, or transaction.

Disaster Recovery (DR) - A plan and process for restoring IT systems and data following a major disruption or disaster, ensuring business continuity.

Distributed Denial of Service (DDoS) Attack - A type of cyberattack where multiple systems overwhelm a target with a flood of traffic, causing service outages.

DNS Spoofing - A type of cyberattack where a hacker intercepts and alters DNS queries to redirect users to malicious websites without their knowledge.

Domain Name System (DNS) - The hierarchical system used to translate domain names (e.g., www.example.com) into IP addresses, making internet navigation possible.

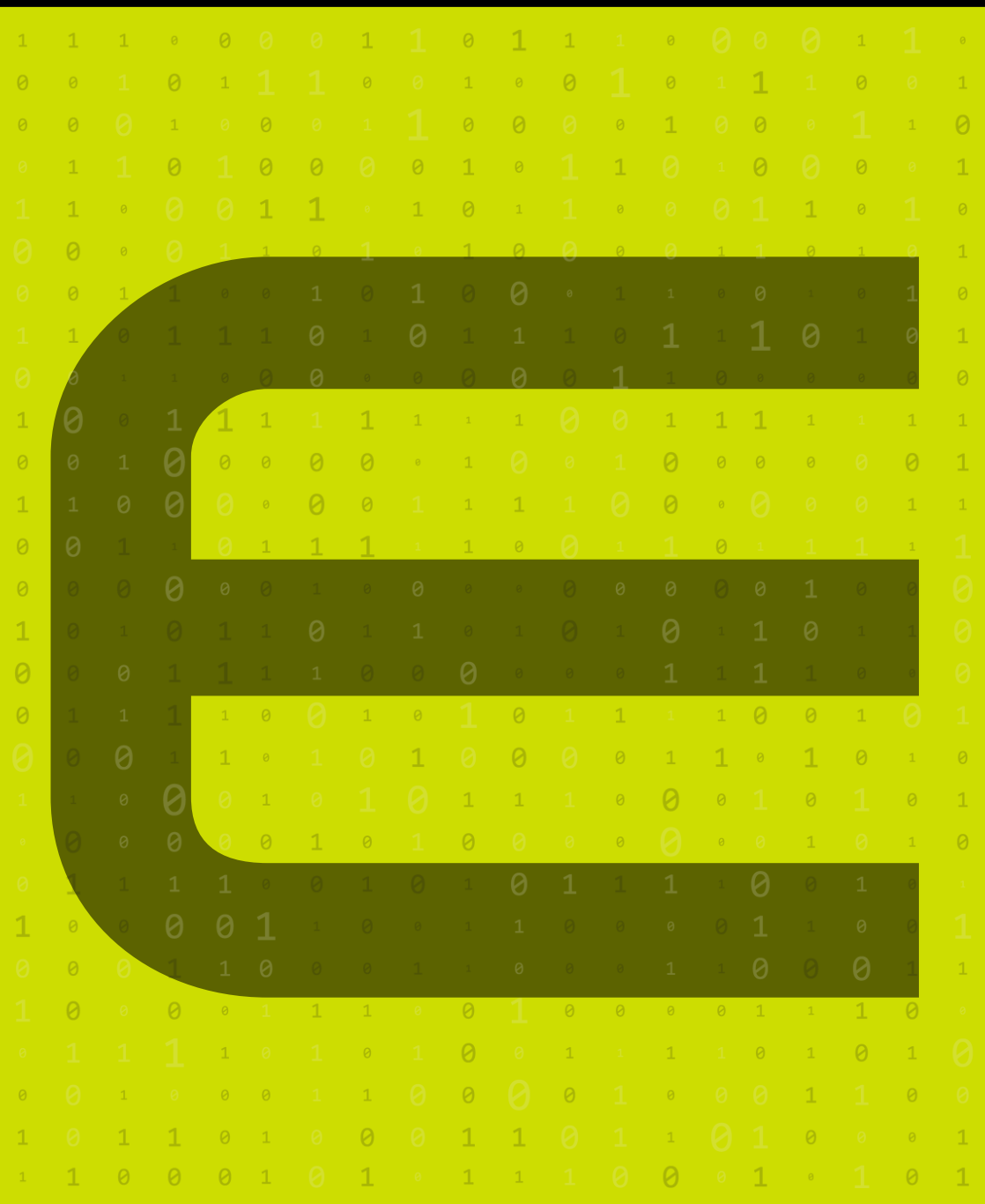
Domain-based Message Authentication, Reporting & Conformance (DMARC) - An email authentication protocol used to protect against spoofing and phishing by verifying the sender's domain.

Drive-by Download - A type of cyberattack where malicious software is automatically downloaded onto a user's device without their consent, typically by visiting a compromised website.

Dual-Factor Authentication (2FA) - A security process that requires two separate forms of identification (e.g., a password and a fingerprint) to verify a user's identity.



Dumpster Diving - A physical security threat where attackers search through discarded materials, such as paper documents or old hardware, to find sensitive information.





E-discovery (Electronic Discovery) - The process of identifying, collecting, and producing electronically stored information (ESI) for legal proceedings or investigations.

EdTech (Education technology) - the practice of introducing information and communication technology tools into the classroom to create more engaging, inclusive and individualized learning experiences.

Eavesdropping - The act of secretly listening to private communications, typically over unsecured networks, to gather sensitive information.

Email Authentication - Techniques used to verify the authenticity of email messages, ensuring they are from legitimate sources and not forged.

Email Encryption - The process of encrypting email messages to protect their content from unauthorized access while in transit or at rest.

Email Filtering - Software or hardware-based tools used to block or flag unwanted or suspicious emails, such as spam or phishing attempts.

Email Spoofing - A cyberattack technique where the sender of an email forges the sender address to make it appear as though it comes from a legitimate source.

Embedded Systems Security - The practice of securing the hardware and software components of embedded systems, which are specialized computer systems within larger systems (e.g., medical devices, cars).


Encryption - The process of converting readable data (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access, typically reversible only with a decryption key.

Endpoint - Any device connected to a network, such as computers, smartphones, or IoT devices, which can be vulnerable to security risks and attacks.

Endpoint Detection and Response (EDR) - A cybersecurity solution that continuously monitors and collects data from endpoints (e.g., computers, mobile devices) to detect and respond to potential security threats.

Endpoint Encryption - The use of encryption techniques on endpoint devices (e.g., laptops, mobile phones) to protect sensitive data stored or transmitted by these devices.

Endpoint Security - The practice of securing endpoints (devices) from cyber threats, using tools like antivirus software, firewalls, and intrusion prevention systems.



Enhanced Security Administrative Environment (ESAE) - A dedicated, isolated administrative environment designed to protect against privileged account attacks in sensitive or high-risk networks.

Enterprise Information Security Architecture (EISA) - A comprehensive framework that aligns security strategies with business objectives, helping organizations implement robust information security practices.

Enterprise Mobility Management (EMM) - A set of tools and technologies used to manage mobile devices, applications, and data to ensure security, particularly in corporate environments.

Ethical Hacking - The practice of intentionally probing systems or networks for vulnerabilities with permission, to identify security weaknesses before malicious hackers exploit them.

Exfiltration - The unauthorized transfer or theft of data from a network, often performed by hackers after breaching a system.

Exploit - A specific method/technique used by hackers to take advantage of a vulnerability or weakness in a system to carry out malicious activities.

Exploit Kit - A toolkit used by cybercriminals to identify and exploit vulnerabilities in software and deliver malware or other malicious code.

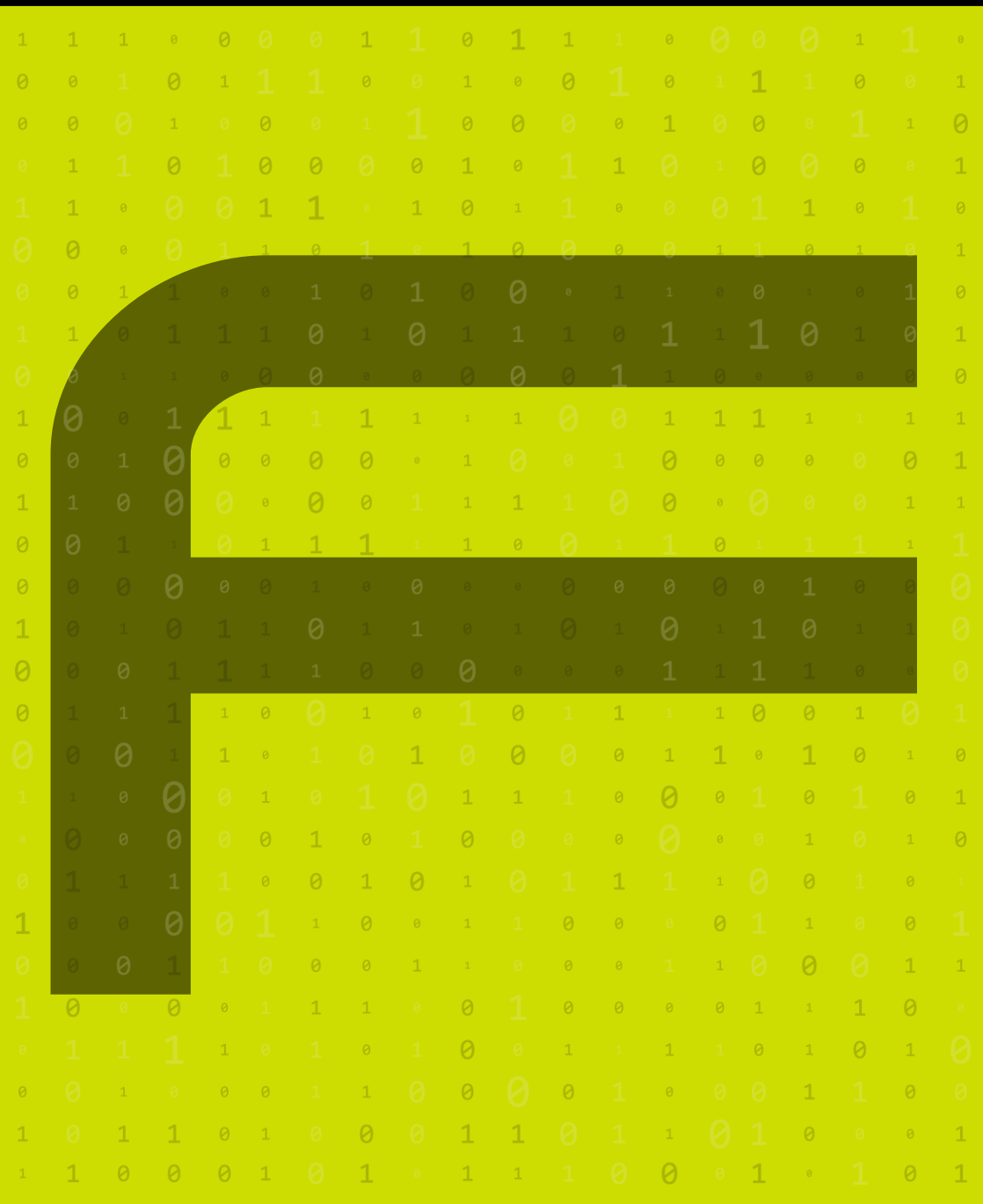
Extended Detection and Response (XDR) - A cybersecurity technology that integrates data from multiple security layers (e.g., endpoints, networks, servers) to provide a more comprehensive detection and response capability.

External Penetration Testing - A type of security testing conducted by ethical hackers or cybersecurity professionals to evaluate the security of a system or network from an external perspective.

External Threat - Any threat to a system or organization that originates from outside its own network, such as hackers, phishing attempts, or malware distributed online.

Extensible Authentication Protocol (EAP) - An authentication framework commonly used in wireless networks and point-to-point connections, providing various methods for authenticating devices.

Extensible Markup Language (XML) Encryption - A standard for encrypting the data contained within an XML document, used to secure information exchanged between systems, often in web services.





False Alarm - An alert generated by a security system that indicates a potential threat that does not actually exist.

False Negative - An error where a test or security system fails to identify an actual threat.

False Positive - An error where a test or security system incorrectly identifies a benign condition as a threat.

Federated Identity Management (FIM) - A system for managing user identities across multiple domains or organizations using a single set of credentials.

Federated Search - A search method that retrieves data from multiple, diverse sources in a unified search result.

Federation - The use of common protocols and standards to allow interoperability and single sign-on across different systems or organizations.

File-Based Ransomware - Ransomware that targets and encrypts specific files or file types rather than the entire system.

File Encryption - The process of converting files into a secure format that can only be accessed with a decryption key.

File Integrity Monitoring (FIM) - A process of detecting unauthorized changes to files to ensure their integrity.

Firewall - A network security device that monitors and controls incoming and outgoing network traffic based on security rules.

Firewall Policy - A set of rules and guidelines defining how network traffic should be allowed or blocked by a firewall.

Firewall Rule - A specific condition or policy set within a firewall to control traffic flow and enforce security measures.

Firmware - Software that is embedded in hardware devices to control and manage hardware functions.

Forensic Analysis - The detailed examination and investigation of digital data to uncover evidence of cybercrime or other security incidents.



Forensics (Digital Forensics) - The practice of collecting, preserving, analyzing, and presenting digital evidence for legal investigations.

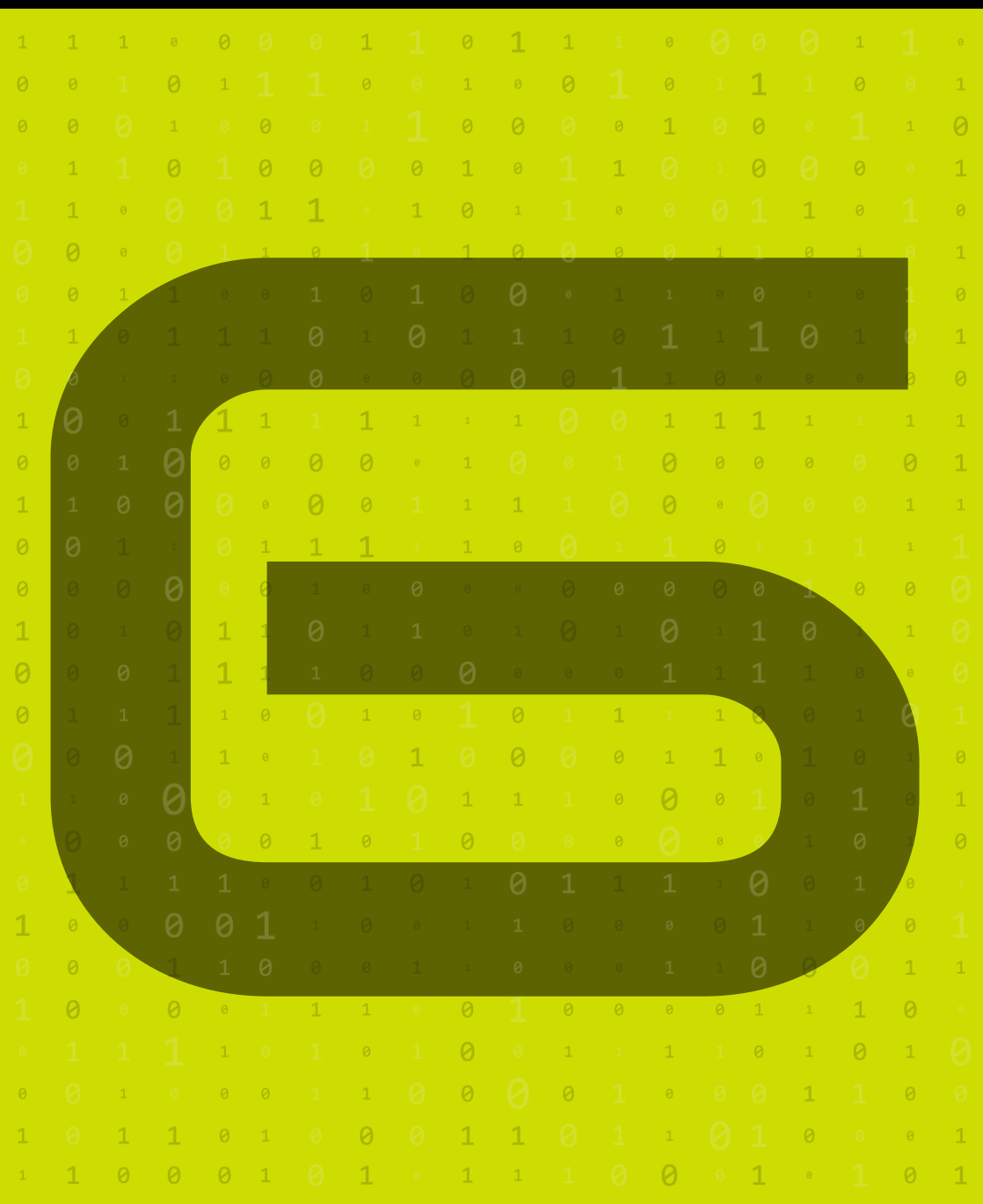
Fraud Detection - Techniques and systems used to identify and prevent fraudulent activities or transactions.


Frequency Analysis - The study of the frequency of letters or groups of letters in a ciphertext to break encryption.

Fuzz Testing - A testing technique where random data is fed into a program to discover vulnerabilities and bugs.

Fuzzy Logic - A form of many-valued logic that deals with approximate reasoning, useful in certain types of security systems and anomaly detection.

Functional Security - Security measures designed to protect the functionality and performance of a system or application.





Galos/Counter Mode (GCM) - A mode of operation for symmetric-key cryptographic block ciphers that provides both encryption and message authentication, commonly used in secure communication protocols.

Garbage Data - Data that is incorrect, irrelevant, or unnecessary, often used in cybersecurity as a tactic to mislead attackers or mask real data.

General Data Protection Regulation (GDPR) - A comprehensive regulation enforced by the European Union (EU) to protect the personal data of individuals within the EU and govern the data privacy practices of organizations handling such data.

Geo-blocking - The practice of restricting access to internet content based on a user's geographical location, often used for security, compliance, or licensing purposes.

Geofencing - A security technology that creates virtual boundaries (geofences) around a physical location, enabling alerts or actions when devices enter or leave the defined area.


Geolocation - The process of determining the physical location of a device (e.g., smartphone, laptop) based on GPS, IP address, or other location-detecting methods, often used in cybersecurity to detect anomalous activity.

Gartner Hype Cycle - A graphical representation developed by Gartner that tracks the maturity, adoption, and social application of emerging technologies, often used in cybersecurity to evaluate the development of new security technologies.

Governance, Risk, and Compliance (GRC) - A strategy for managing an organization's overall governance (decision-making processes), risk management (identification and mitigation of risks), and compliance (adherence to laws, regulations, and internal policies) in cybersecurity and data privacy contexts.

Gray Hat Hacker - A hacker or security expert who operates between ethical (white hat) and unethical (black hat) behavior, often finding and exploiting vulnerabilities without malicious intent but without full permission either.

Greenfield Network Security - Refers to network security practices applied to new, freshly built networks, where security measures are designed and implemented from the ground up without the limitations of legacy systems.



Greylist - A security mechanism where suspicious email messages or IP addresses are temporarily delayed or flagged until their legitimacy can be confirmed, commonly used in email filtering to fight spam.

Guard Bandin - A method used in wireless security that reserves part of the frequency spectrum to prevent interference between communication channels, contributing to a more secure communication environment.

Guarded Fabric - A security mechanism used in virtualization environments, particularly with Hyper-V, to ensure that virtual machines (VMs) are protected from unauthorized access and tampering.

Guardrails - Security policies or guidelines implemented within an organization to prevent actions that could lead to vulnerabilities or security breaches, ensuring a safe operational environment.

Guided Cybersecurity Simulation - A training or learning activity where participants engage in simulated cybersecurity scenarios under guidance, designed to improve awareness, skills, and response to real-world cybersecurity threats.

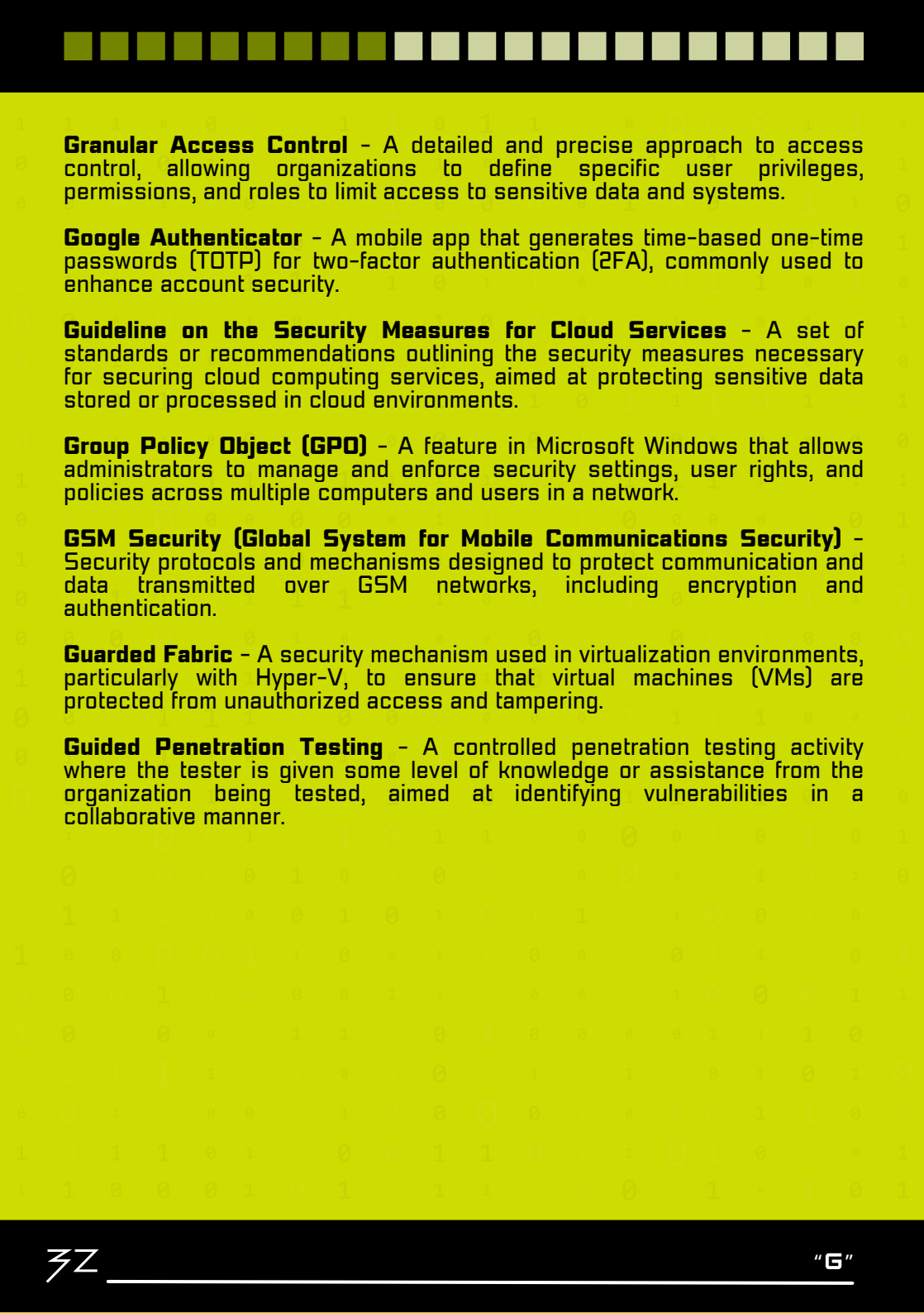
Guided Social Engineering Attack - A form of social engineering attack where the attacker provides subtle hints or guidance to manipulate the target into divulging confidential information or taking harmful actions.

GUI (Graphical User Interface) Security - Security mechanisms that focus on safeguarding the user interfaces of systems and applications to prevent unauthorized access or exploitation of vulnerabilities in the design or implementation of the interface.

Guest Access - A temporary, restricted form of network or system access given to users who do not have regular accounts or credentials, commonly used in corporate or public environments to ensure secure access for visitors.

Guest Isolation - A security feature in networking where guest users are isolated from the main internal network, preventing unauthorized access to sensitive internal resources.

Golden Ticket Attack - A sophisticated cyberattack targeting Kerberos authentication systems where attackers forge authentication tickets, giving them virtually unrestricted access to resources within the compromised network.



Granular Access Control - A detailed and precise approach to access control, allowing organizations to define specific user privileges, permissions, and roles to limit access to sensitive data and systems.

Google Authenticator - A mobile app that generates time-based one-time passwords (TOTP) for two-factor authentication (2FA), commonly used to enhance account security.

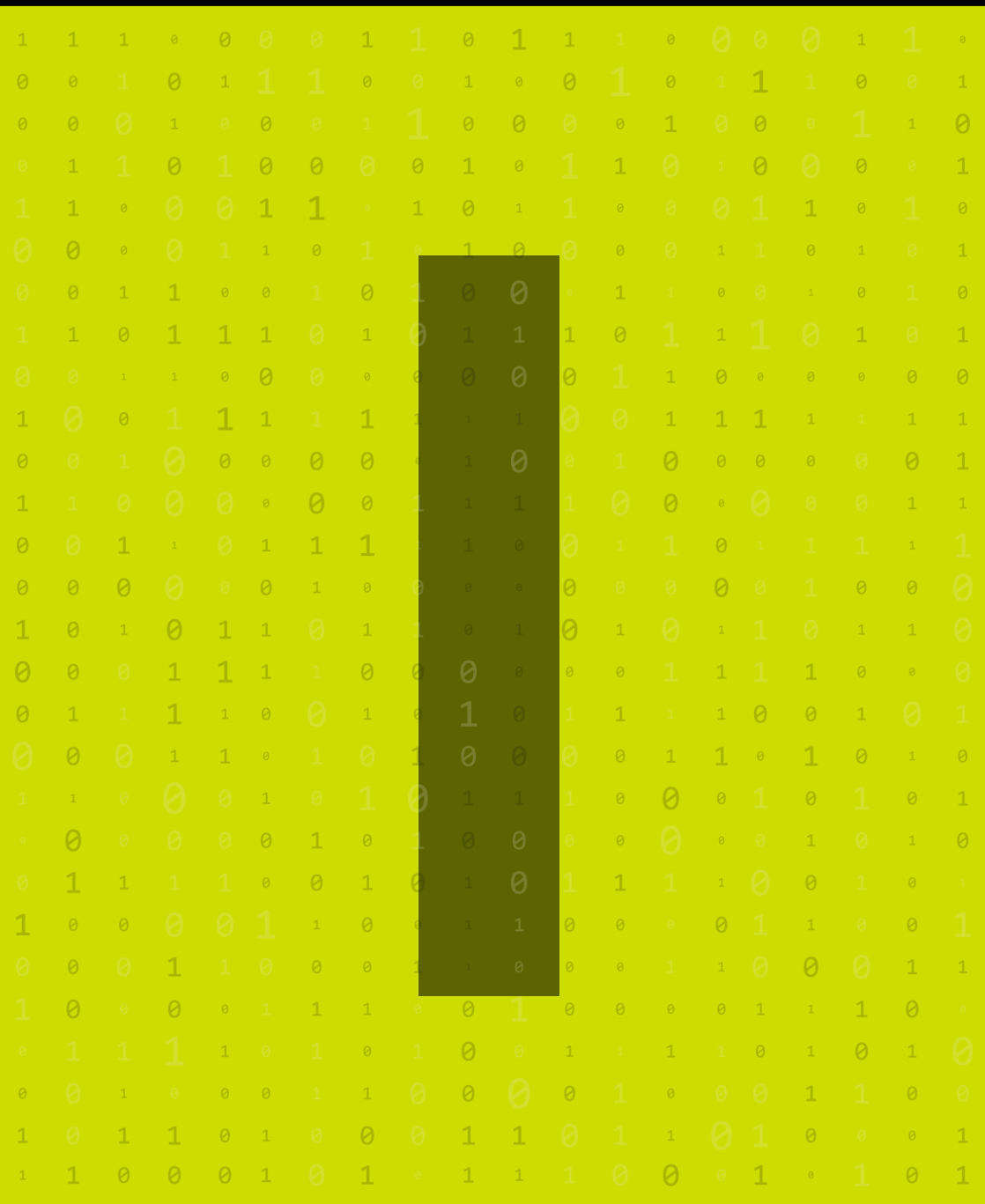
Guideline on the Security Measures for Cloud Services - A set of standards or recommendations outlining the security measures necessary for securing cloud computing services, aimed at protecting sensitive data stored or processed in cloud environments.


Group Policy Object (GPO) - A feature in Microsoft Windows that allows administrators to manage and enforce security settings, user rights, and policies across multiple computers and users in a network.

GSM Security (Global System for Mobile Communications Security) - Security protocols and mechanisms designed to protect communication and data transmitted over GSM networks, including encryption and authentication.

Guarded Fabric - A security mechanism used in virtualization environments, particularly with Hyper-V, to ensure that virtual machines (VMs) are protected from unauthorized access and tampering.

Guided Penetration Testing - A controlled penetration testing activity where the tester is given some level of knowledge or assistance from the organization being tested, aimed at identifying vulnerabilities in a collaborative manner.





IAM (Identity and Access Management) - A framework of policies and technologies used to manage and secure access to organizational resources, ensuring the right individuals have the correct access levels.

ICANN (Internet Corporation for Assigned Names and Numbers) - A non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the internet.

ICS (Industrial Control System) - Systems used to control industrial processes such as manufacturing, power generation, and other infrastructure services. Securing ICS is a significant aspect of cybersecurity.

Identity Federation - The process of linking a user's digital identity across multiple domains or organizations to allow single sign-on (SSO) and other identity management services.

Identity Fraud - A type of fraud where an attacker uses someone else's personal information without their permission, often to commit crimes or make unauthorized purchases.

Incident Management - The process of identifying, responding to, and mitigating data breaches and other security incidents.

Incident Reporting Mechanism - The process and system for reporting data breaches and security incidents within an organization.

Incident Response - The process of handling and managing the aftermath of a security breach or attack, focusing on limiting damage, recovering affected systems, and preventing future incidents.

Incident Response Plan - A plan detailing the steps to be taken in response to a data breach or security incident.

Incident Response Team (IRT) - A group of professionals responsible for managing and responding to data breaches and security incidents.

Indicator of Compromise (IoC) - Forensic evidence that suggests a system has been compromised, such as unusual login patterns or the presence of malware.

Information Assurance (IA) - The practice of ensuring the confidentiality, integrity, and availability of information, particularly in government and military contexts.



Information Lifecycle Management (ILM) - Strategies and practices for managing information throughout its lifecycle, from creation to disposal.

Information Security (InfoSec) - The practice of protecting information by mitigating risks and vulnerabilities in systems, software, and processes.

Information Security Management System (ISMS) - A systematic approach to managing sensitive information to keep it secure.

Infrared Intrusion Detection System - A physical security device that uses infrared technology to detect unauthorized physical access or movement in restricted areas.

Infrastructure as Code (IaC) - The management of IT infrastructure through code and automation, ensuring consistent and secure configurations for cloud and on-premise resources.

Injection Attack - A type of cyberattack where malicious code is inserted into a program or query, such as SQL injection or command injection, allowing unauthorized access or manipulation of data.

Insider Threat - A security risk that comes from individuals within an organization, such as employees or contractors, who have access to critical systems and data.

Integrity - A key principle of cybersecurity that ensures that data remains accurate, complete, and unaltered, both at rest and in transit.

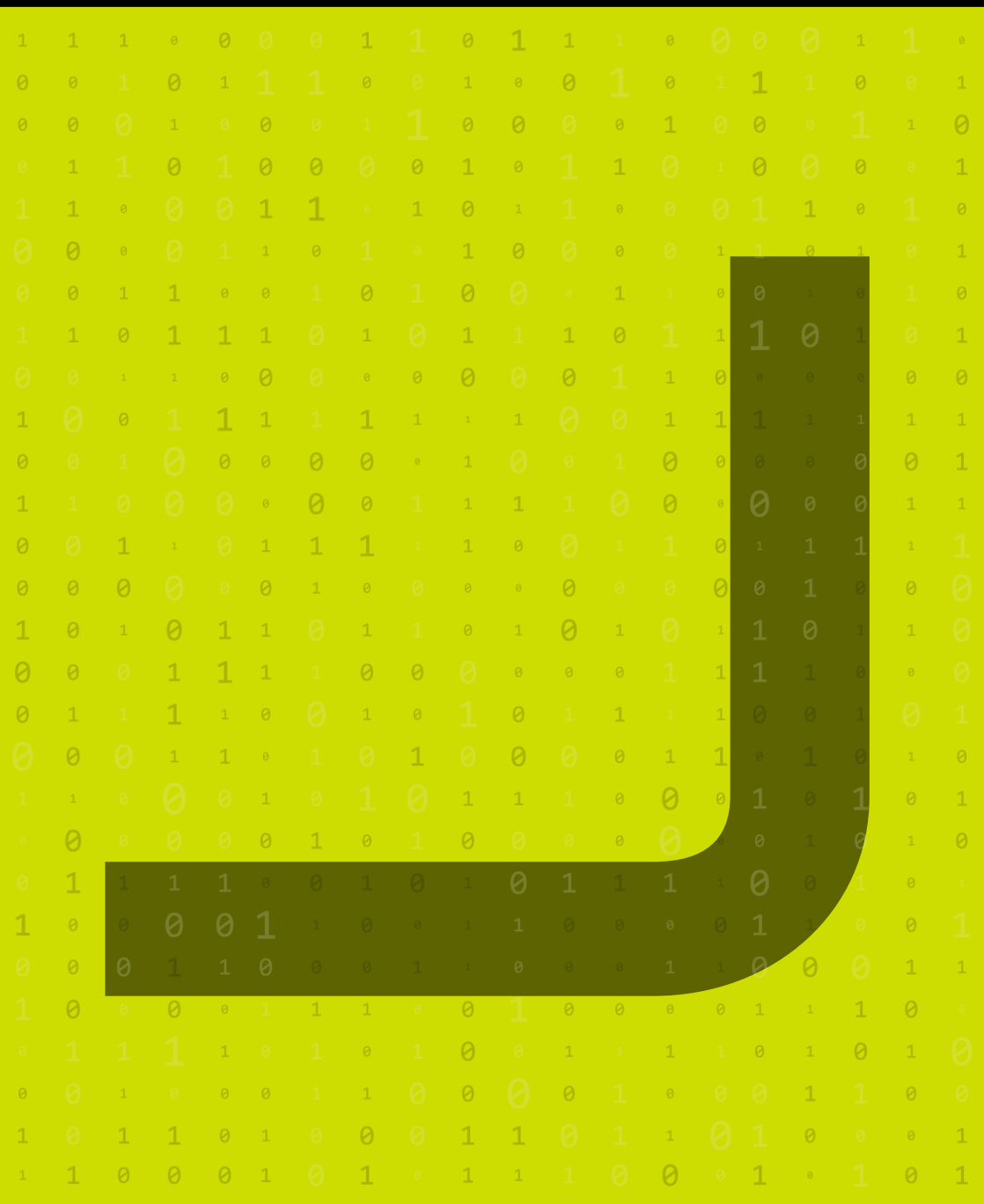
Internet - That intricate web of information and connectivity that allows you to read this Glossary, watch cat and dog videos, or pay by card for your hot chocolate on a rainy Sunday morning.


Internet of Things (IoT) Security - The practice of securing the vast array of internet-connected devices that form the IoT, ensuring they are protected from hacking, privacy violations, and unauthorized access.

Intrusion Detection System (IDS) - A device or software application that monitors network or system activities for malicious actions or policy violations.

Intrusion Prevention System (IPS) - Similar to IDS, but with the ability to actively block or prevent detected threats.

Intellectual Property - Creations of the mind for which exclusive rights are recognized, including data and software.





Jailbreaking - The process of removing software restrictions imposed by the manufacturer on devices such as smartphones, often exposing the device to security risks.

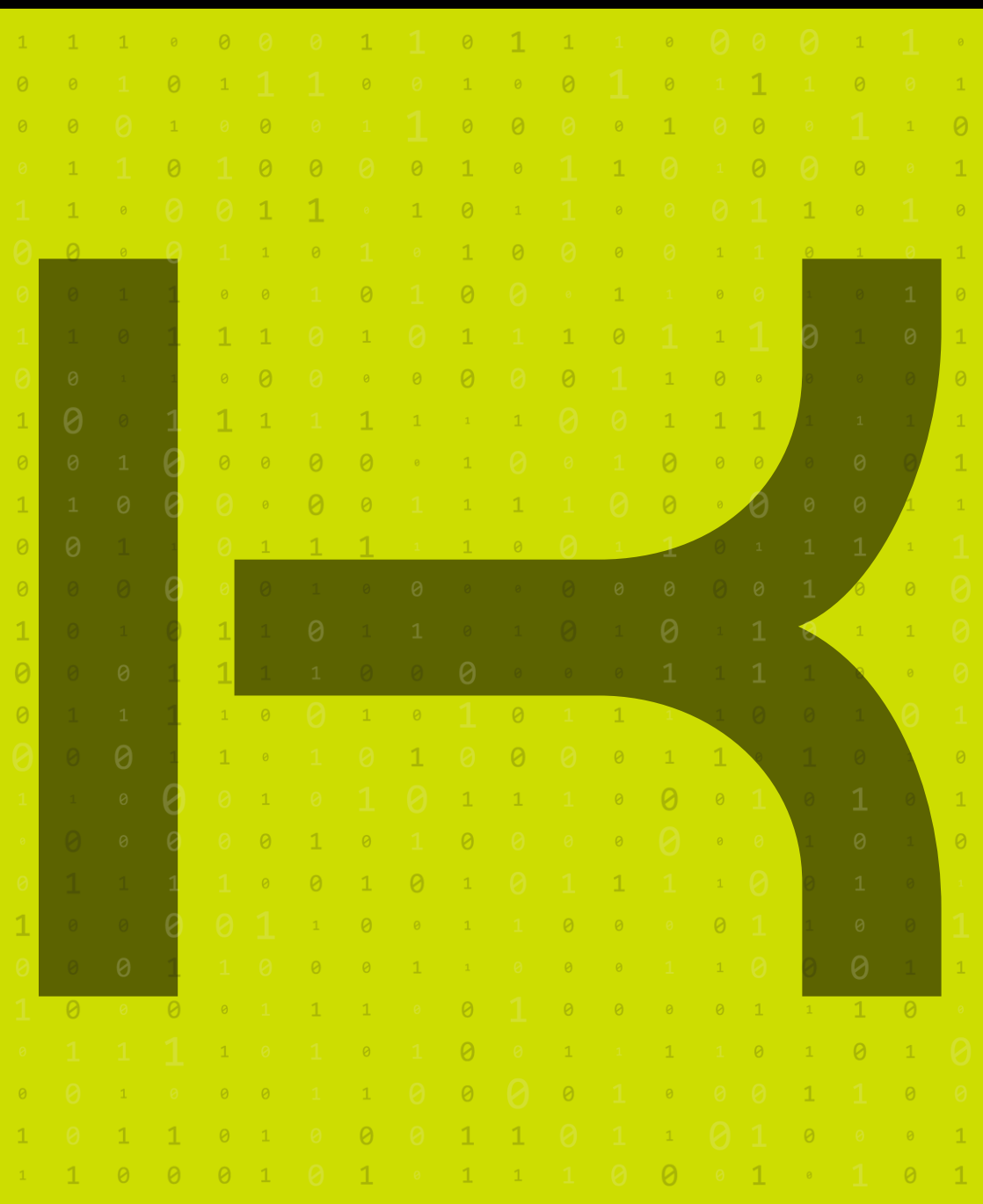
JavaScript Injection - A type of injection attack where malicious JavaScript code is injected into a website, often used in cross-site scripting (XSS) attacks.


Joint Authorization Board (JAB) - A group within the U.S. government responsible for reviewing and authorizing cloud service providers for federal use under the FedRAMP program.

Jitter - A network performance issue where data packets experience varying delays, potentially affecting the quality of VoIP or video conferencing services.

Just-in-Time (JIT) Access - A security concept that allows users temporary and limited access to critical systems or data, ensuring they have just enough time to complete a task before access is revoked.

Jurisdiction - The geographical area within which data protection laws and regulations apply.





Key Derivation Function (KDF) - A cryptographic function used to derive keys from a base value, often used in password hashing and encryption.

Key Escrow - A system where cryptographic keys are held in escrow, often by a third party, to allow access in cases of emergency or regulatory requirements.

Key Management Interoperability Protocol (KMIP) - A standardized protocol used to manage encryption keys across different systems and environments, improving security and compliance.

Key Rotation Policy - A security policy that defines how often cryptographic keys should be rotated or changed to minimize the risk of key compromise.

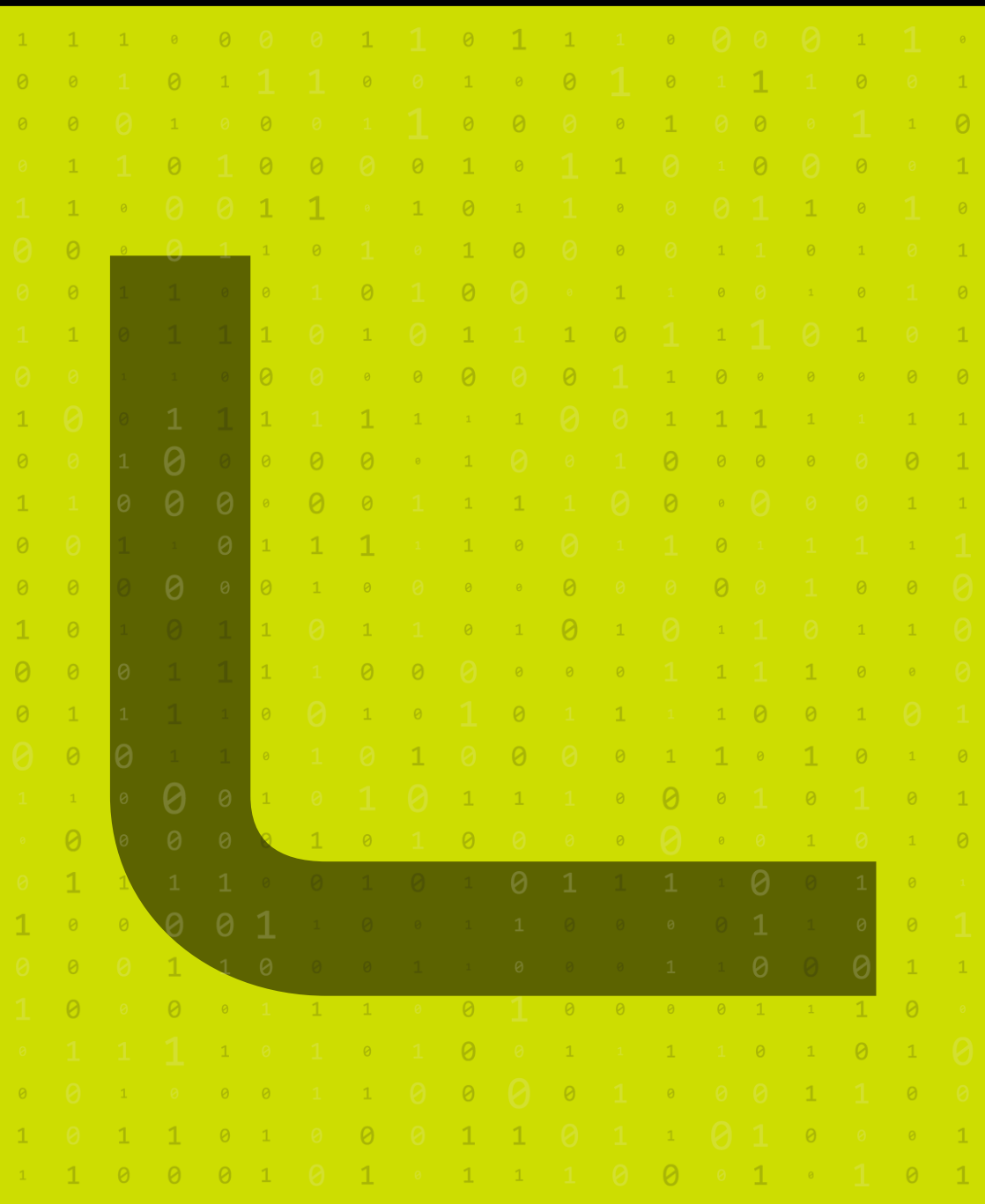
Keystroke Encryption - A method of encrypting keystrokes between the keyboard and the application to prevent keylogging attacks.


Kill Process Attack - An attack where malicious code forces critical processes or applications to terminate, often leading to system crashes or vulnerabilities.

Knowledge Discovery in Databases (KDD) - The process of discovering useful information and patterns from large datasets, often used in security analytics to identify potential threats.

Known Plaintext Attack (KPA) - A cryptanalysis technique where the attacker has access to both the plaintext and its corresponding ciphertext, using this information to uncover the encryption method.

Krack Attack - A vulnerability in the WPA2 Wi-Fi encryption protocol that allows attackers to intercept and manipulate traffic between devices and wireless networks.





LAN (Local Area Network) -A network that connects computers within a limited area such as a home, school, or office, often secured through firewalls and encryption.

LDAP (Lightweight Directory Access Protocol) - A protocol used to access and manage directory information services over an IP network, often employed in centralized authentication and authorization systems.

Lawful Basis for Processing - The legal grounds under which an organization can process personal data, as defined by data protection laws.

Legal Basis for Data Processing - The justification required under data protection laws to process personal data, such as consent or contractual necessity.

Legal Compliance - The process of ensuring that an organization adheres to relevant laws, regulations, and guidelines related to data privacy, cybersecurity, and data protection (e.g., GDPR, HIPAA).

Legislative Framework - The body of laws and regulations that govern data privacy and protection.

Letterbomb - A type of email or message-based attack that contains malicious code designed to exploit vulnerabilities when opened by the recipient.

Library Injection - A method of inserting malicious code into the software library of a program to alter its normal behavior or gain unauthorized access to system resources.

Linux Security Modules (LSM) - A framework in the Linux operating system that enables the enforcement of mandatory access controls, allowing administrators to define and implement security policies.

Log Aggregation - The process of collecting and centralizing log data from various systems and applications into a single location for security analysis and monitoring.

Log Management - The practice of recording, storing, and analyzing logs generated by software, hardware, and network devices for troubleshooting and security purposes.

Log Retention Policy - A set of guidelines that define how long log data should be retained before being archived or deleted, often required for compliance with data privacy regulations.

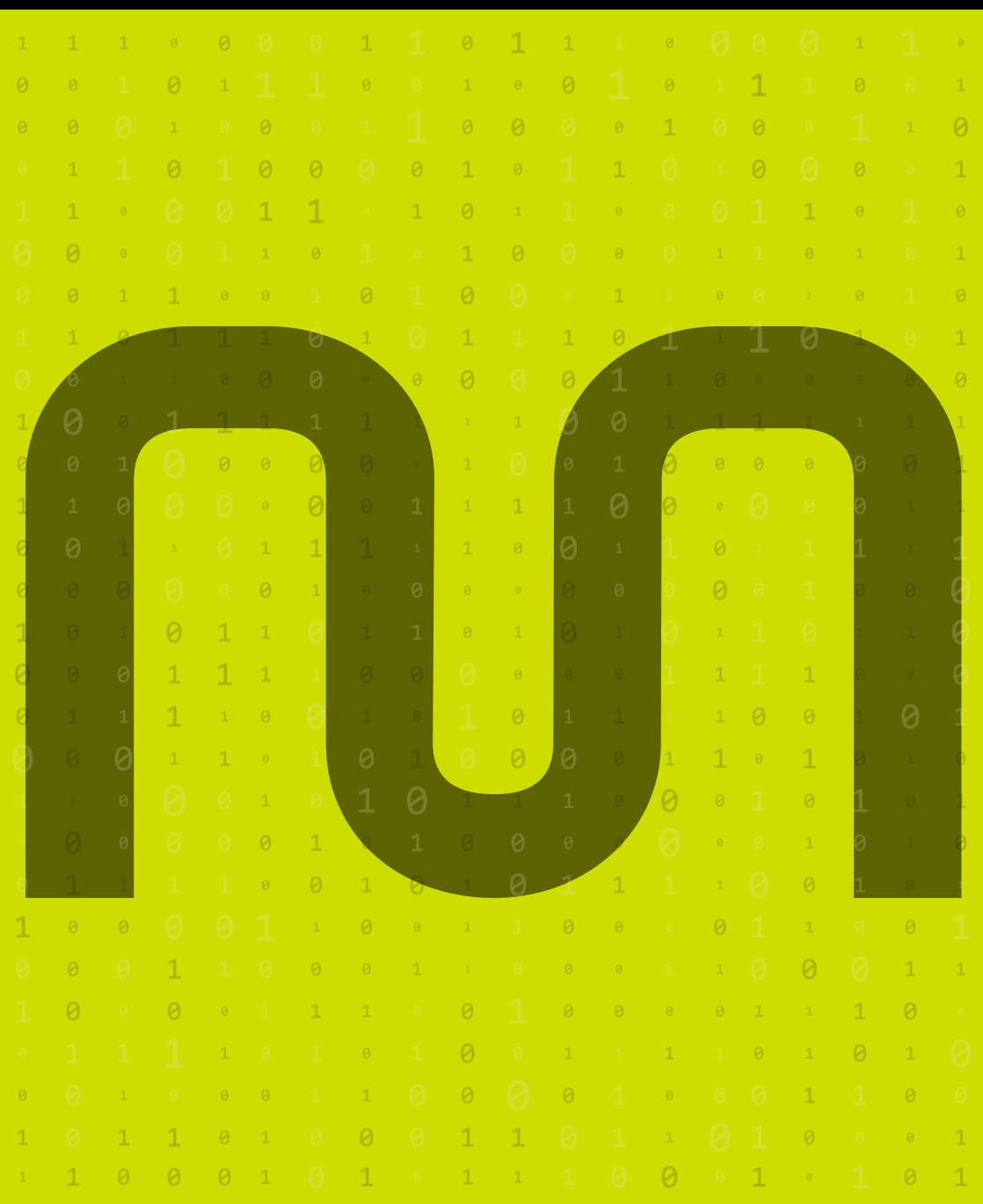



Logical Access Control - Security mechanisms that restrict access to data or resources based on predefined rules, typically managed through authentication and authorization systems.

Logic Bomb - A malicious program or code that lies dormant in a system until triggered by specific conditions, at which point it activates and causes harm.

Long-Term Persistence Attack - A type of cyberattack where an attacker maintains undetected access to a system over an extended period, allowing them to gather information or carry out further attacks.

Lua-based Security - Security measures and controls implemented using the Lua scripting language, often used in embedded systems and games for security features like script authentication.





MAC (Mandatory Access Control) - A type of access control where access to resources is granted based on policies determined by a central authority, typically in highly secure environments.

MAC Address (Media Access Control Address) - A unique identifier assigned to network interfaces for communication at the data link layer of a network, often used in device identification and network security.

Machine Learning - A type of artificial intelligence that enables systems to learn and make decisions from data without being explicitly programmed.

Machine Learning Security - The application of machine learning algorithms to detect anomalies, predict threats, and improve cybersecurity defenses based on large data sets.

Malicious Code - Any code or software designed to harm, exploit, or otherwise compromise a system, including viruses, worms, Trojan horses, ransomware, and spyware.

Malware (Malicious Software) - A term that refers to software specifically designed to disrupt, damage, or gain unauthorized access to a system or network.


Man-in-the-Middle Attack (MITM) - An attack where a malicious actor intercepts and potentially alters communication between two parties without their knowledge, often used to steal sensitive data.

Mandatory Encryption - A policy requiring that all sensitive data be encrypted both at rest and in transit to ensure its confidentiality and integrity.

Manual Penetration Testing - The process of manually testing a system or network for vulnerabilities by simulating real-world attack scenarios, as opposed to using automated tools.

Master Boot Record (MBR) Virus - A type of virus that infects the master boot record of a hard drive, allowing it to load before the operating system starts and making it difficult to detect.

MD5 (Message Digest Algorithm 5) - A widely used cryptographic hash function that produces a 128-bit hash value, commonly used to verify data integrity but is no longer considered secure due to vulnerability to collision attacks.



Memory Corruption - A software vulnerability where the contents of a computer's memory are unintentionally modified, potentially allowing an attacker to exploit the system.

Memory Dump - A file that captures the contents of memory at a given time, often used for forensic analysis during incident response to investigate attacks.

Message Integrity - A security concept ensuring that a message or data has not been altered in transit, typically achieved through hashing or digital signatures.

Metadata - Data that provides information about other data, such as file size or creation date.

Metadata Security - The protection of metadata (data about data), which could reveal sensitive information about systems, files, or communications even if the underlying data is encrypted.

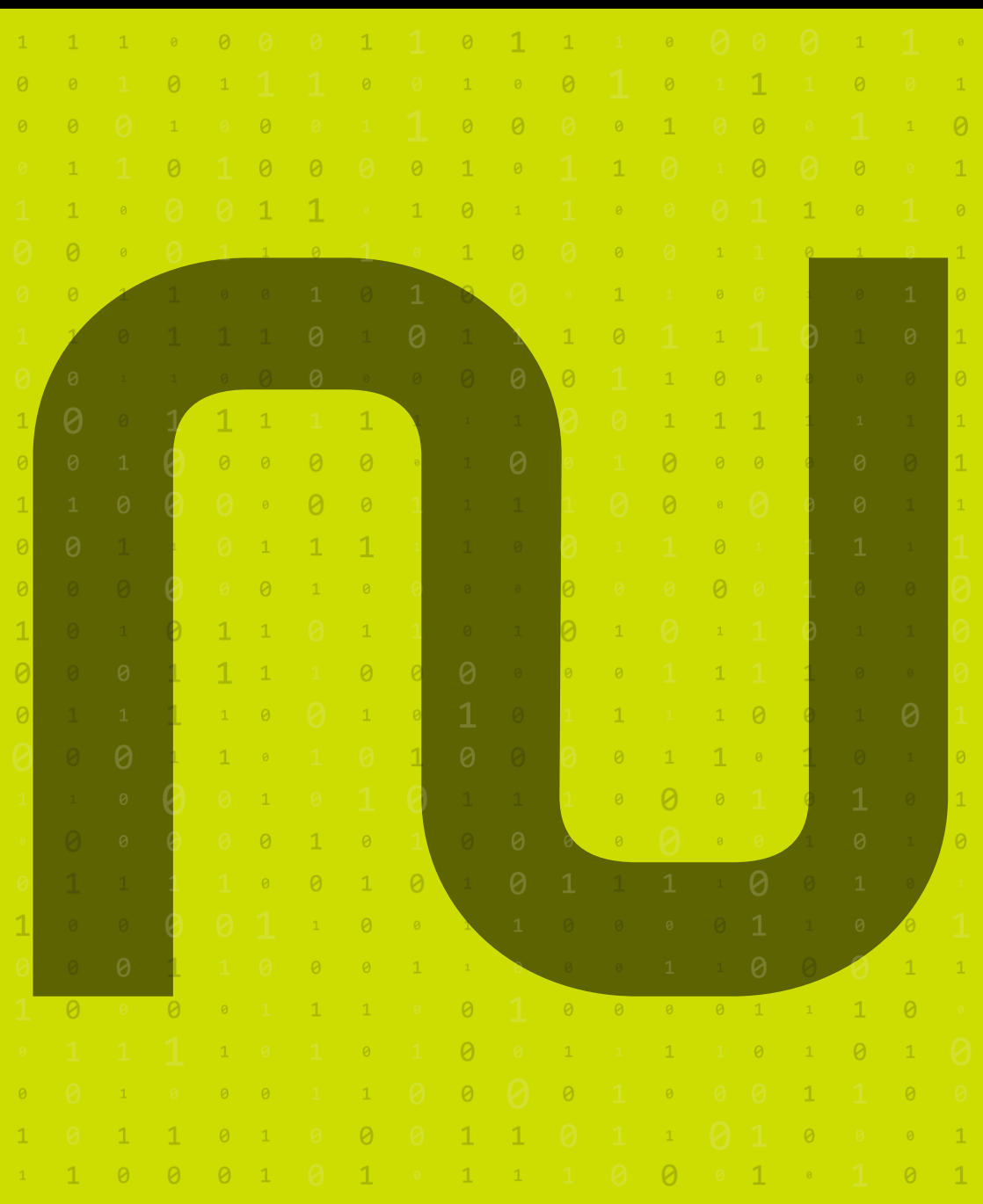
Microsite - A microsite is built for a specific purpose and is not a website or landing page. Microsites are small, but that doesn't mean they're small company websites. Instead, microsites are sub-websites that focus on a campaign, product, or service rather than the entire company and its offerings.


Mitigation - The process of reducing the severity, impact, or likelihood of a cybersecurity threat or vulnerability through various security measures.

Mobile Device Management (MDM) - A software solution used by organizations to manage, monitor, and secure mobile devices such as smartphones and tablets, ensuring compliance with security policies.

Multi-Factor Authentication (MFA) - A security process that requires users to provide two or more verification factors to gain access to a system, adding an extra layer of security beyond just passwords.

Mutual Authentication - A security process where both the user and the system authenticate each other to ensure that both parties are legitimate, often used in secure communications.





NAC (Network Access Control) - A security solution that restricts unauthorized devices from accessing a network by enforcing security policies and compliance checks.

National Institute of Standards and Technology (NIST) - A U.S. federal agency that develops and promotes standards, including cybersecurity frameworks, to ensure data security and protect critical infrastructure.

Network Address Translation (NAT) - A technique used in networking to translate private IP addresses within a local network to a public IP address, enabling multiple devices to share a single IP address.

Network Forensics - The process of capturing, recording, and analyzing network traffic to investigate and understand network-based security incidents or crimes.

Network Intrusion Detection System (NIDS) - A system that monitors network traffic for suspicious activity and potential threats, typically deployed at strategic points within a network.

Network Intrusion Prevention System (NIPS) - A system designed to detect and prevent potential threats by monitoring network traffic and blocking malicious activities before they can harm the system.


Network Mapping - The process of discovering and visualizing the layout of a network, including devices, connections, and configurations, often used for security assessments and management.

Network Policy - Rules and guidelines that govern the management, configuration, and security of network resources, including access controls and usage policies.

Network Security - The measures and practices used to protect a network from unauthorized access, attacks, and misuse, including the use of firewalls, intrusion detection systems, and encryption.

Network Segmentation - The practice of dividing a computer network into smaller, isolated sub-networks to reduce the attack surface and prevent attackers from moving laterally within the network.

Network Traffic Analysis - The process of examining data moving through a network to monitor performance, detect anomalies, and identify potential security threats.



Network Vulnerability Scanner - A tool used to scan networks for known vulnerabilities and security weaknesses, helping to identify and address potential risks before they can be exploited.

Non-Compliance - Failure to adhere to data protection laws and regulations.

Non-Repudiation - A security concept that ensures the authenticity and integrity of communications, making it impossible for the sender to deny having sent a message or transaction.

Nonce - A random or unique value used in cryptographic communication to ensure that old communications cannot be reused in replay attacks.

Null Cipher - A method of concealing messages within a block of non-secret information, where the message is extracted using a predetermined pattern or key.

Null Encryption - A term referring to encryption that is effectively non-existent, often due to weak or broken encryption algorithms that do not provide adequate protection.

Null Session - A type of unauthorized connection to a Windows system that can allow attackers to enumerate shares, users, and other sensitive information.

Nullification - The process of rendering data or a security feature ineffective, often used in the context of security bypass attacks or revocation of access.

NVRAM (Non-Volatile Random Access Memory) Security - Security mechanisms applied to NVRAM storage to protect critical configuration data from tampering or unauthorized access.

Normalisation - The process of standardizing data to a common format to improve consistency, usability, and analysis, often used in database management and data processing.

NoSQL Database - A type of database that provides a mechanism for storage and retrieval of data modeled in ways other than tabular relations used in SQL databases, often used for handling large volumes of unstructured data.

Node - A network device or point where data is processed or transmitted, such as a computer, router, or switch, within a network infrastructure.

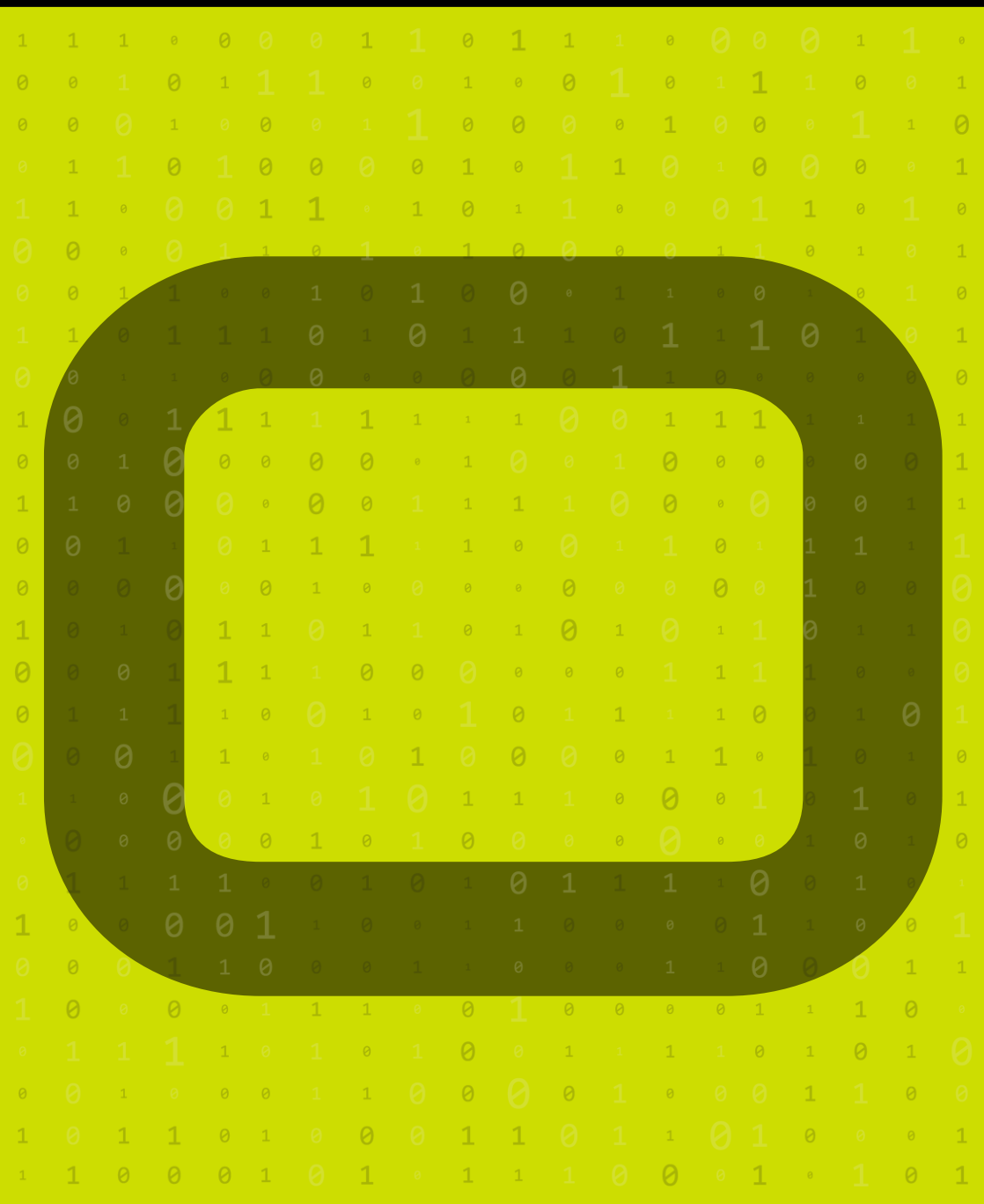



Node Authentication - The process of verifying the identity of a node (e.g., a device or system) within a network to ensure it is authorized to access or communicate with other nodes.

Neural Network Security - The application of neural network-based techniques to enhance cybersecurity, such as using artificial neural networks for anomaly detection and threat prediction.

Non-Secure Protocol - A communication protocol that does not provide encryption or other security measures to protect data during transmission, such as HTTP (as opposed to HTTPS).

Non-Disclosure Agreement (NDA) - A legal contract between parties to protect sensitive information from being disclosed to unauthorized individuals or entities.





OAuth (Open Authorization) - An open standard for token-based authentication and authorization on the internet, often used to allow third-party applications access to user information without exposing passwords.

Obligations of Data Controllers - Responsibilities held by organizations that determine the purposes and means of data processing.

Obligations of Data Processors - Responsibilities held by organizations that process data on behalf of data controllers.

Object-level Security - Security measures applied to individual objects, such as files or database records, to ensure that only authorized users can access or modify them.

Offensive Security - A branch of cybersecurity focused on simulating attacks to identify vulnerabilities and improve the defensive posture of a system or network.

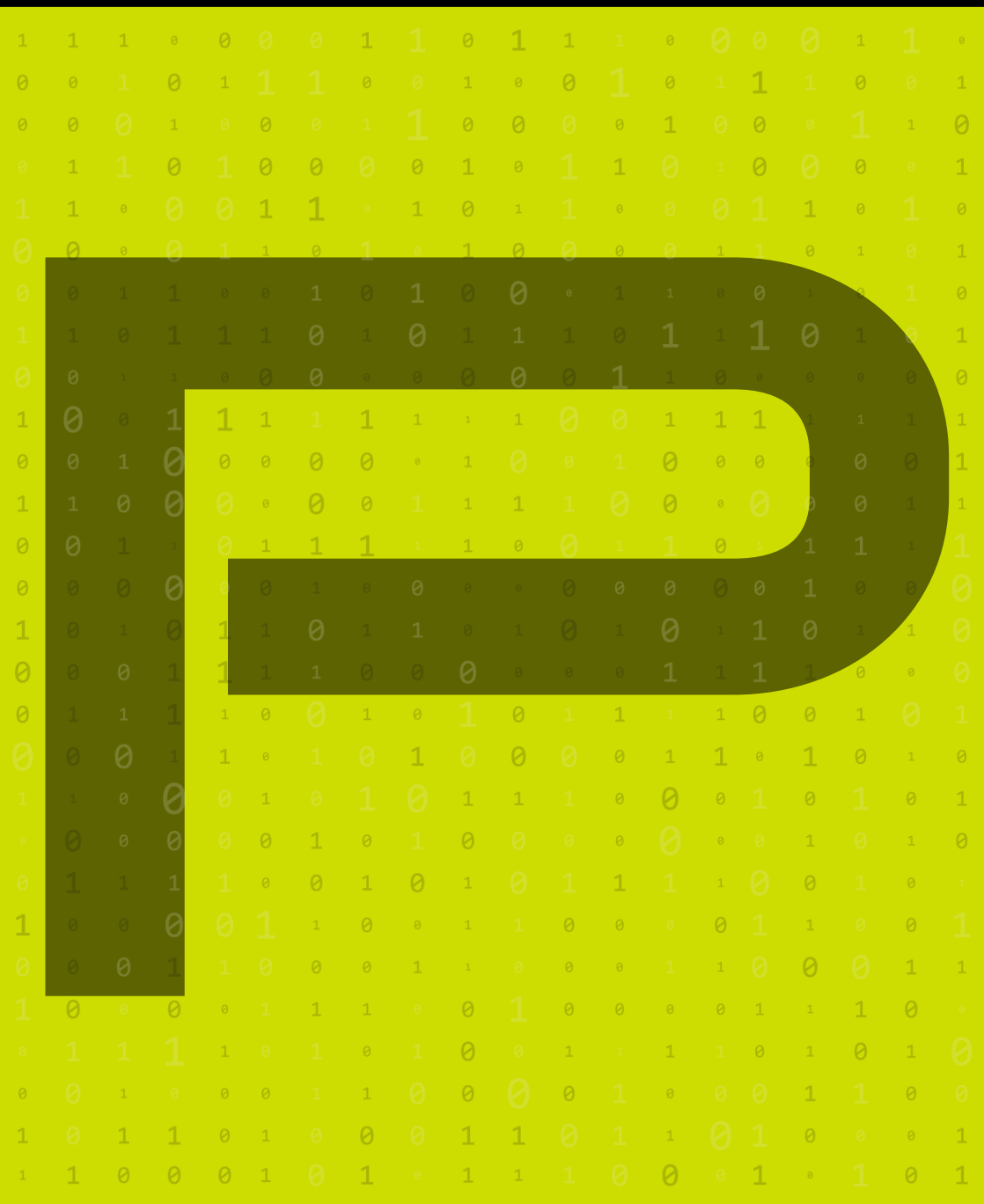
One-Time Pad (OTP) - A theoretically unbreakable encryption method where a random key, used only once, is combined with the plaintext to produce the ciphertext.


Open Source Intelligence (OSINT) - The practice of collecting and analyzing publicly available data from open sources (such as social media, public records, and websites) for cybersecurity and threat intelligence purposes.

Operating System Hardening - The process of securing an operating system by reducing its attack surface, such as disabling unnecessary services, applying patches, and configuring security settings.

Over-The-Air (OTA) Update Security - Security measures that protect software updates delivered wirelessly to devices like smartphones and IoT devices, ensuring that the updates are authentic and have not been tampered with.

Obfuscation - The process of deliberately making code or data harder to understand or reverse-engineer, often used to protect sensitive information or prevent analysis of malware.





Packet Filtering - A firewall technique that examines the headers of data packets and allows or blocks them based on predefined rules, such as source and destination IP addresses.

Password Cracking - The process of recovering passwords from data stored in or transmitted by a computer system, typically done through methods like brute force or dictionary attacks.

Password Policy - A set of rules enforced by an organization to enhance security by defining requirements for creating and maintaining secure passwords.

Patch Management - The process of managing software updates and patches, ensuring that vulnerabilities are fixed to maintain system security.

Penetration Testing (Pentest) - A security testing method where ethical hackers simulate attacks on a system to identify and exploit vulnerabilities, providing insights for remediation.

Personally Identifiable Information (PII) - Any information that can be used to identify an individual, such as names, social security numbers, and addresses, which must be protected under data privacy regulations.

Pharming - A cyberattack technique where traffic is redirected from a legitimate website to a fraudulent one to steal sensitive information, often through DNS poisoning.


Phishing - A social engineering attack where attackers pose as trustworthy entities to trick individuals into revealing sensitive information, such as passwords or financial details.

PII (Personally Identifiable Information) - Any data that could identify a specific individual, such as names, social security numbers, or email addresses, often targeted in data breaches.

Pirate Box - A device used to share files and data over a local network without an internet connection, often designed to be anonymous.

Plaintext - Data that is readable and not encrypted, making it vulnerable to interception and unauthorized access if transmitted insecurely.

Platform as a Service (PaaS) - A cloud computing model where a third-party provider delivers hardware and software tools over the internet, allowing users to develop, run, and manage applications without the complexity of building and maintaining the underlying infrastructure.



Port Scanning - A method used by attackers to discover open ports on a system, which may indicate potential entry points for attacks.

Privilege Escalation - A type of attack where a user gains higher access privileges than initially granted, enabling them to perform unauthorized actions on a system.

Public Key Infrastructure (PKI) - A framework for managing digital certificates and public-key encryption to secure communications and authenticate users.

PUP (Potentially Unwanted Program) - Software that may not be malicious but is often unwanted by the user, such as toolbars or adware, which can pose security risks if left unchecked.

Pwn - A slang term derived from "own," often used in hacking culture to describe taking control of or defeating a system or target.

Personal Data - Information relating to an identified or identifiable individual.

Personal Data Protection Regulations - Laws and standards designed to safeguard personal data from misuse and unauthorized access.

Privacy by Design - The principle of integrating data protection measures into the design of systems and processes.

Privacy Impact Assessment (PIA) - An assessment to evaluate the impact of a project or system on privacy and data protection.

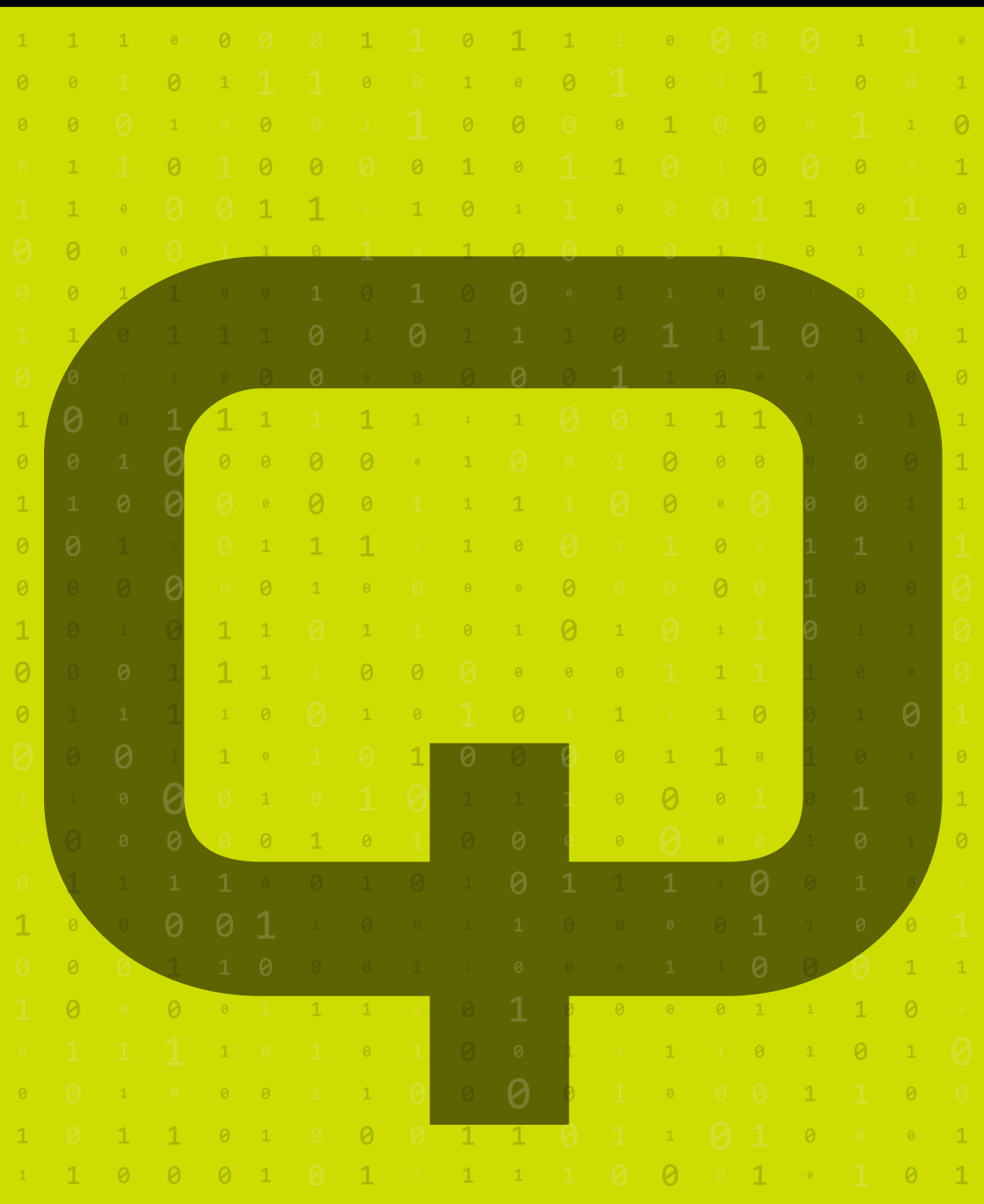
Privacy Notices - Documents provided to individuals explaining how their data will be collected, used, and protected.


Privacy Policies - Documents outlining how an organization collects, uses, and protects personal data.

Privacy Shield Framework - A framework designed to protect personal data transferred between the European Union and the United States (Note: replaced by other agreements after invalidation).

Profiling - The automated processing of personal data to evaluate certain aspects of an individual's behavior or characteristics.

Pseudonymisation - The process of replacing identifiable information with pseudonyms to protect individual identities.





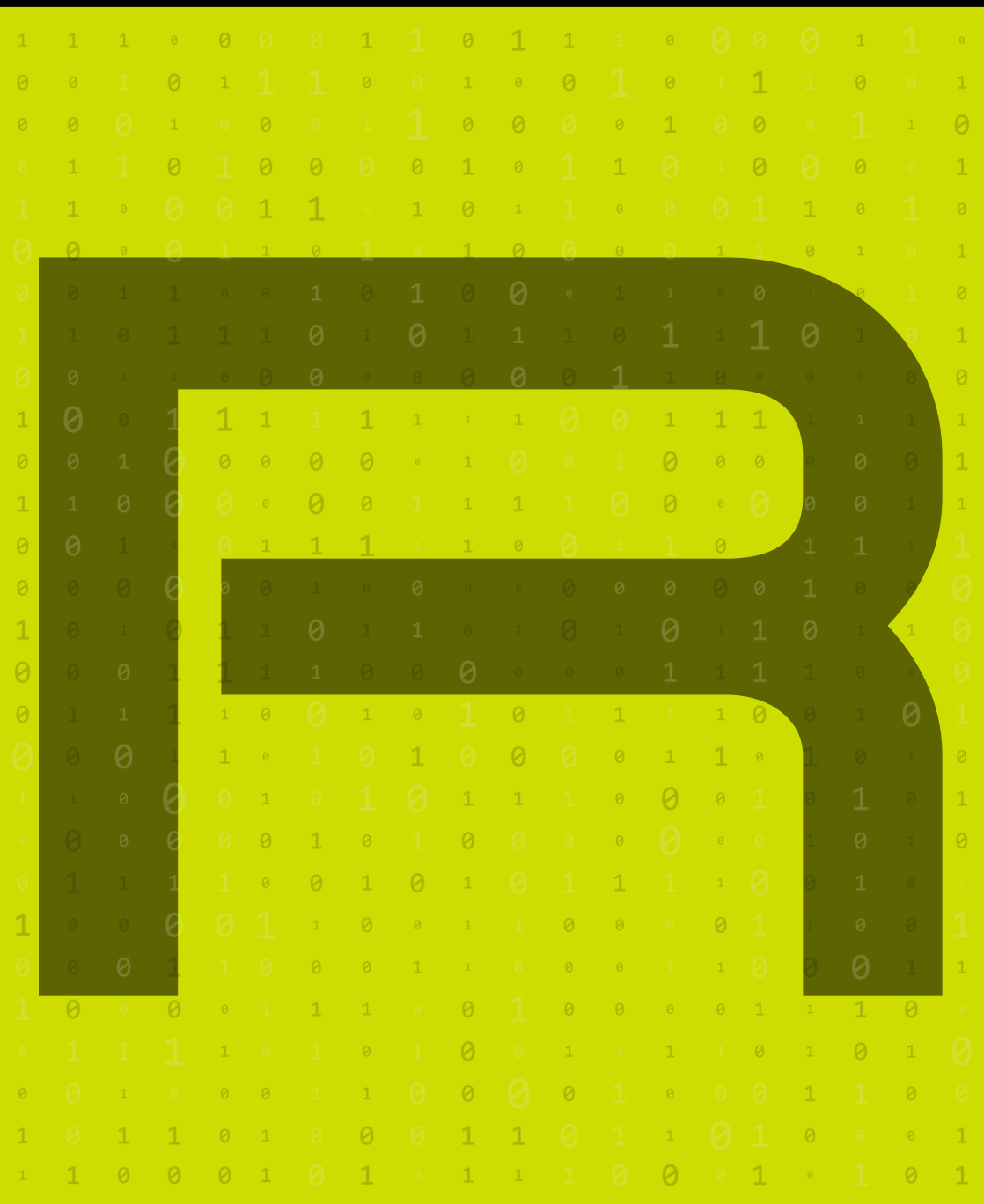
Quantum Cryptography - A method of encryption that uses the principles of quantum mechanics to secure data, potentially making it unbreakable by classical computing methods.


Quarantine - The isolation of potentially harmful files or systems to prevent them from causing damage, typically used in antivirus software to handle detected malware.

Query Flood Attack - A type of denial-of-service attack that overwhelms a target system by sending a high volume of queries or requests, rendering it unresponsive.

Quick Response (QR) Code Security - Security measures for protecting against malicious QR codes that can redirect users to harmful websites or initiate unintended actions.

Quorum-based Access Control - A security mechanism that requires multiple parties to approve or authorize access to sensitive resources or operations, enhancing protection against misuse.





Ransomware - A type of malicious software that encrypts a victim's data or locks their system, demanding payment (usually in cryptocurrency) for the decryption key or access restoration.

Red Teaming - A cybersecurity exercise where an independent group (the Red Team) simulates real-world attacks to test the effectiveness of an organization's security defenses.

Reflected XSS (Cross-Site Scripting) - A type of web application vulnerability where malicious scripts are reflected off a web server and executed in a user's browser, often used to steal sensitive information.

Remote Access Trojan (RAT) - A type of malware that allows attackers to remotely control an infected system, often used for espionage, data theft, or system manipulation.

Remote Code Execution (RCE) - A security vulnerability that allows an attacker to execute arbitrary code on a remote machine, often leading to full system compromise.

Replay Attack - A type of network attack where valid data transmission is maliciously or fraudulently repeated or delayed, allowing attackers to impersonate or disrupt communication.

Resident Virus - A type of computer virus that installs itself in the memory of a system, allowing it to infect files and programs whenever they are accessed.


Retina Scan - A biometric security measure that uses unique patterns in an individual's retina for identification and authentication purposes.

Reverse Engineering - The process of analyzing software or hardware to discover its design, architecture, or source code, often used in vulnerability research or malware analysis.

Risk Assessment - The process of identifying, analyzing, and evaluating risks to an organization's information systems and data, often followed by measures to mitigate or eliminate these risks.

Role-Based Access Control (RBAC) - A security model that assigns access rights based on the roles assigned to users within an organization, ensuring that they only have access to the data necessary for their role.

Rootkit - A collection of malware tools that enable an attacker to gain and maintain control of a system undetected, often by hiding its presence.



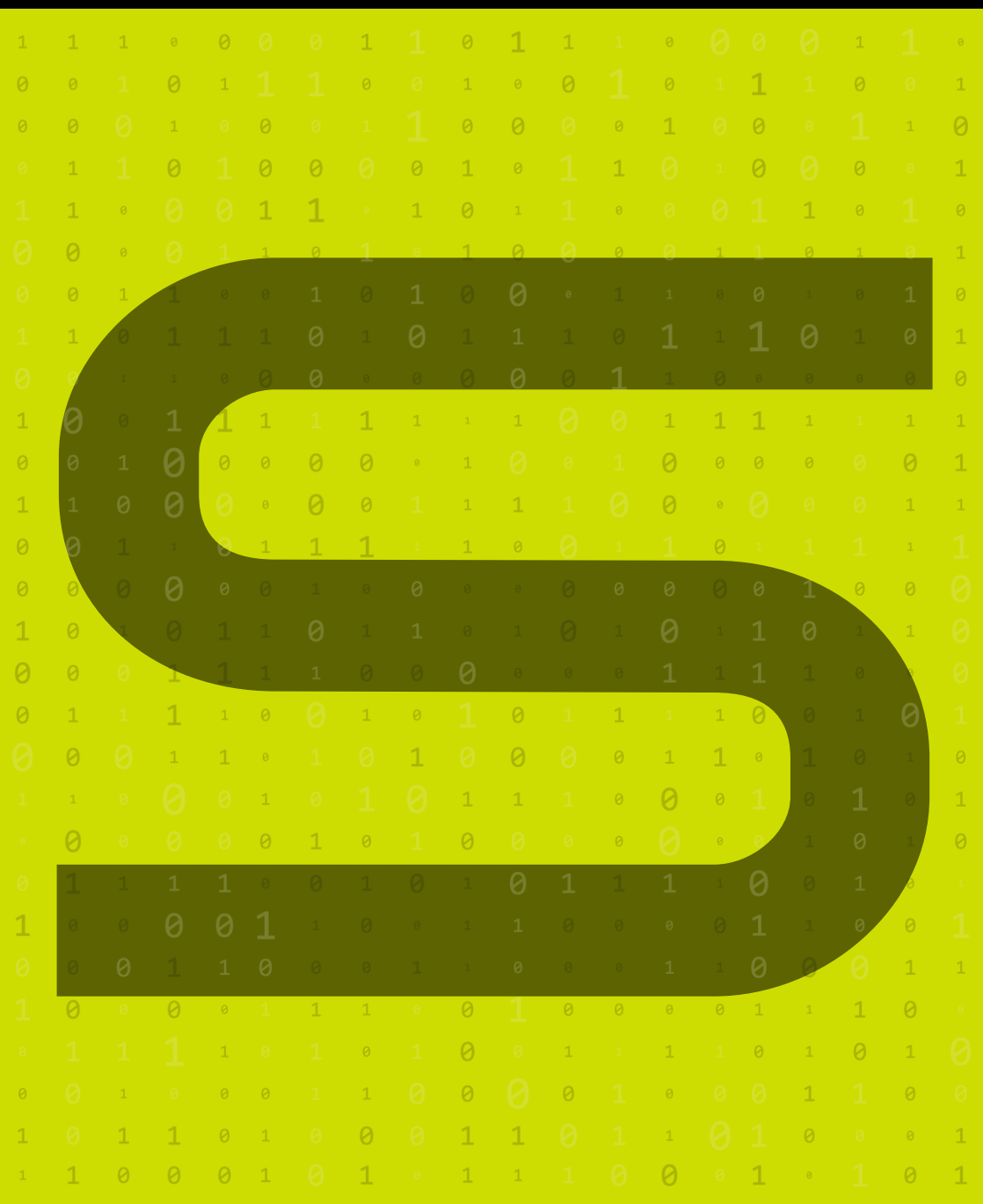
RSA (Rivest-Shamir-Adleman) - A widely-used public key cryptosystem for secure data transmission, named after its inventors and known for its role in encrypting and securing sensitive information.


Regulatory Compliance - Adherence to laws and regulations governing data protection and privacy.

Regulatory Requirements - Obligations imposed by laws and regulations that organizations must follow to ensure data protection.

Risk Management Framework - A structured approach to identifying, assessing, and managing risks related to data protection.

Risk Tolerance - The level of risk an organization is willing to accept while managing data protection and security.





Salami Attack - A type of cyberattack that involves stealing small amounts of money or data over time, often too small to be noticed in individual transactions but adding up to significant losses.

Sandboxing - A security mechanism used to isolate potentially harmful programs or code from critical systems, allowing them to run in a restricted environment without risking damage to the larger network.

Scareware - Malicious software designed to trick users into believing their computer is infected with malware, often leading to the purchase of fake security software or revealing personal information.

Script Kiddie - A derogatory term for an inexperienced hacker who uses pre-written scripts or tools to carry out cyberattacks without fully understanding how they work.

Secure Boot - A security standard for ensuring that a device only boots using trusted software, preventing the loading of unauthorized or malicious operating systems.

Secure Socket Layer (SSL) - A security protocol used to encrypt data transmitted over the internet, commonly used in HTTPS to protect sensitive information like login credentials and credit card numbers.

Security Awareness Training - Programs designed to educate employees or users about cybersecurity best practices, social engineering threats, and how to recognize and prevent cyberattacks.


Security Breach Notification - The requirement to inform affected individuals and regulators about a data breach.

Security Certifications - Official recognition that an organization's data protection practices meet specific standards.

Security Incident Management - The processes and procedures for handling and mitigating security incidents.

Security Information and Event Management (SIEM) - A system that collects, analyzes, and correlates security events from various sources in real-time, helping organizations detect and respond to threats more effectively.

Session Hijacking - A type of attack where an attacker takes over a user's session on a website or application, often by stealing the session token or cookie.



Shoulder Surfing - A physical security threat where an attacker observes a user entering sensitive information, such as passwords or PINs, by looking over their shoulder or using surveillance equipment.

Side-channel Attack - A type of attack that exploits physical or implementation-specific characteristics of a system (such as power consumption or timing information) to gain access to sensitive data.

Signature-based Detection - A method used in antivirus and intrusion detection systems that identifies threats based on predefined patterns or "signatures" of known malware.

Single Sign-On (SSO) - A user authentication process that allows a user to log in once and gain access to multiple applications or systems without having to log in again for each one.

Smishing - A phishing attack that is carried out over SMS (text) messages, where the attacker attempts to trick the victim into revealing personal information or clicking on a malicious link.

Sniffing - The act of intercepting and analyzing network traffic, often used by attackers to capture sensitive data such as login credentials or credit card numbers.


Social Engineering - A manipulation technique used by attackers to trick individuals into revealing confidential information or performing actions that compromise security, such as clicking on malicious links.

Spear Phishing - A targeted phishing attack directed at a specific individual or organization, often using personalized messages and details to increase the likelihood of success.

Spoofing - The act of impersonating another user, device, or system to gain unauthorized access to a system or manipulate communication.

Spyware - Malicious software that secretly monitors and collects information from a user's system, such as browsing habits or personal data, often without the user's knowledge.

SQL Injection - A type of attack where an attacker exploits vulnerabilities in an application's database query interface by inserting malicious SQL code to gain unauthorized access to or manipulate data.



State-sponsored Attack - A cyberattack carried out or supported by a government, typically targeting other nations, organizations, or individuals for espionage, sabotage, or other strategic purposes.

Steganography - The practice of hiding information within other data, such as embedding a message within an image or audio file, often used for covert communication.

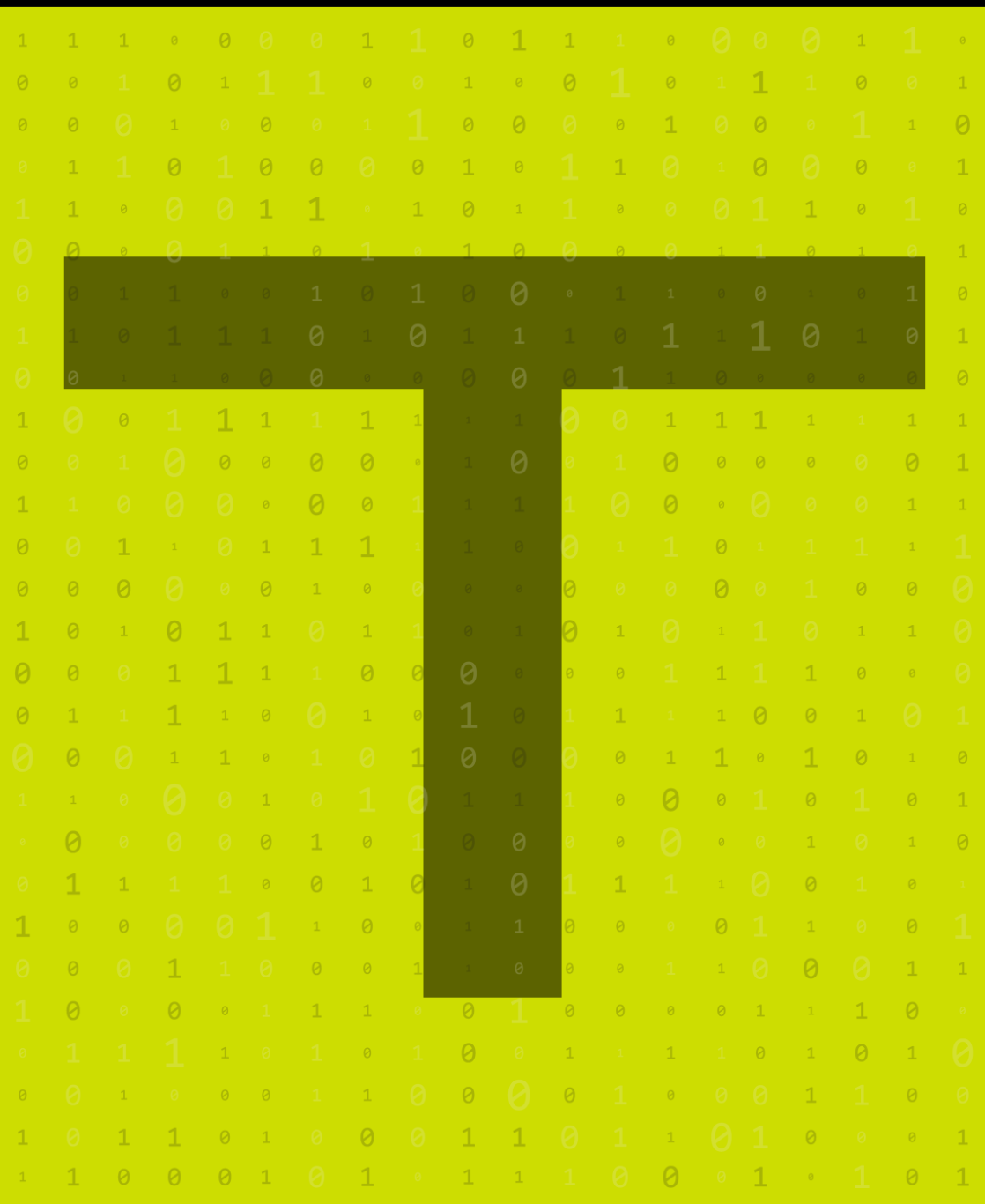
Supply Chain Attack - A type of attack where an attacker targets less secure elements in the supply chain, such as third-party vendors or service providers, to compromise the security of a larger organization.


Symmetric Encryption - A type of encryption where the same key is used for both encrypting and decrypting the data, often used in secure communication protocols.

Sensitive Data - Personal data that requires additional protection due to its nature, such as health information or financial details.

Social Engineering - Techniques used to manipulate individuals into divulging confidential information.

Standard Contractual Clauses (SCCs) - Legal agreements used to ensure adequate data protection when transferring data outside the European Economic Area (EEA).





Tails (The Amnesic Incognito Live System) - A security-focused Linux-based operating system designed for anonymous internet usage and privacy protection. It runs from a USB stick or DVD and leaves no trace on the machine.

Tamper Detection - A security feature that identifies unauthorized alterations or attempts to manipulate systems or data, often triggering alerts when tampering is detected.

Technical and Organisational Measures (TOMs) - Measures taken to ensure the security of personal data, including technical solutions and organizational practices.

Technical Vulnerabilities - Weaknesses in a system that could be exploited to gain unauthorized access to data.

Terms of Service - Legal agreements that outline the rules and conditions for using a service or product.

Third-Party Risk Management - The process of assessing and managing risks associated with third-party vendors who handle data.

Third-Party Vendors - External organizations or individuals that provide services or products to a company, which may involve handling data.

Threat Actor - An individual or group engaged in malicious activities, such as cyberattacks, with the intent to compromise systems, steal data, or disrupt operations.

Threat Hunting - A proactive cybersecurity practice where security professionals actively search for threats or indicators of compromise (IoCs) within a network before they lead to a breach.

Threat Intelligence - Information about current or potential cyber threats gathered from various sources to help organizations identify, prevent, and respond to attacks.

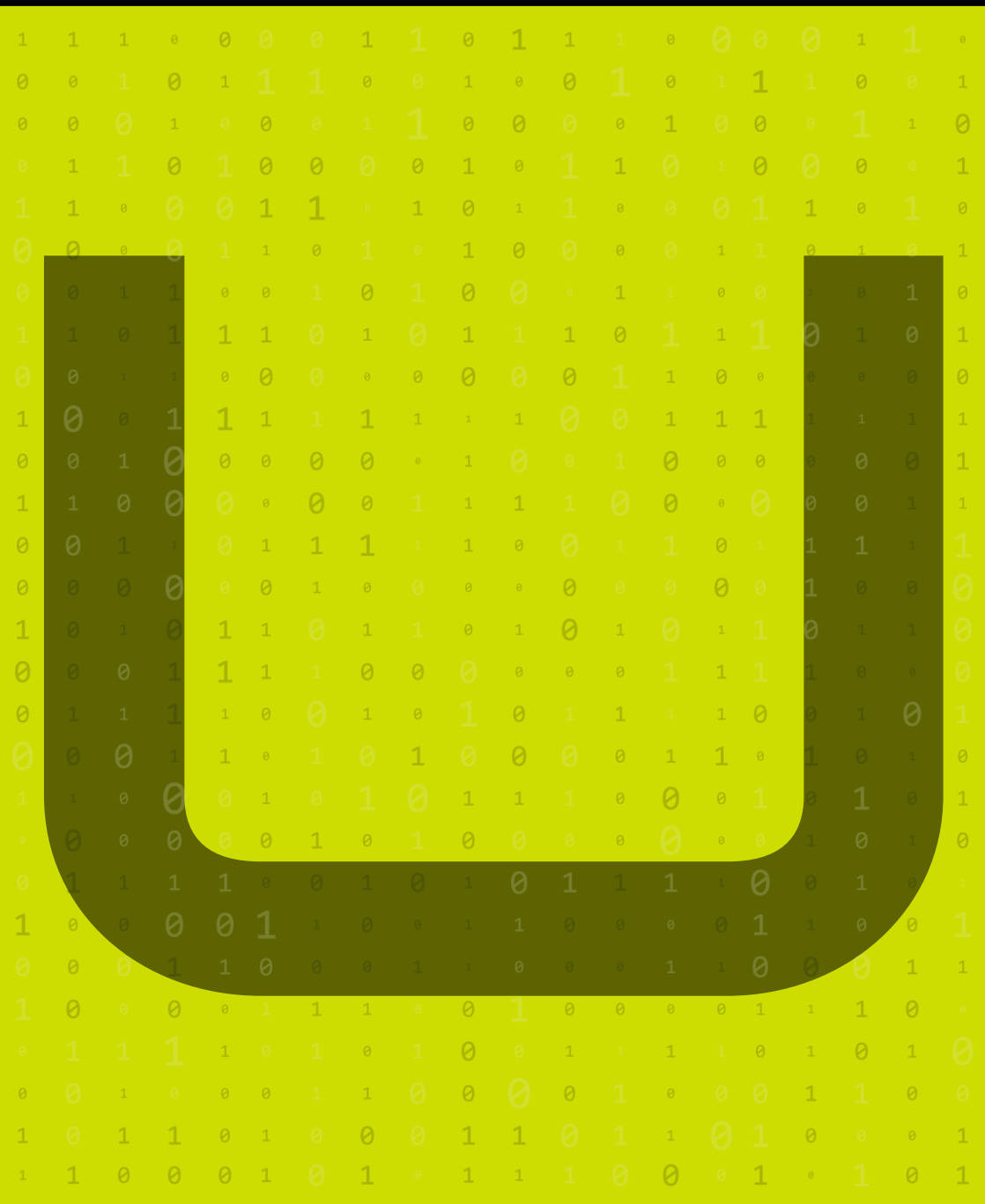
Tokenisation - A process that replaces sensitive data with a unique identifier or token, reducing the risk of exposing the actual data during storage or transmission.


Transparency - The principle of being open and clear about data collection practices and how data is used.



Two-factor Authentication (2FA) - A security process that requires two separate methods of verification (such as a password and a one-time code sent to a mobile device) to authenticate a user, enhancing account security.

Typo Squatting - A social engineering attack where cybercriminals create fake websites with domain names similar to popular ones, hoping that users will mistype the URL and land on the malicious site.





UDP (User Datagram Protocol) - A communication protocol used on the internet for fast, connectionless data transmission. It is often used in applications like streaming and VoIP but is less secure than TCP.

UEBA (User and Entity Behavior Analytics) - A cybersecurity technology that uses machine learning and analytics to detect anomalies in the behavior of users and entities, identifying potential threats or malicious insiders.

Underground Economy - A term referring to the black market where cybercriminals buy, sell, and trade illegal goods and services such as stolen data, malware, or hacking tools.

Uniform Resource Locator (URL) - A reference (address) used to access resources on the internet. Malicious URLs are often used in phishing attacks to redirect users to harmful sites.

Untrusted Network - A network that is not controlled by the organization and is considered insecure, such as public Wi-Fi, where communications may be vulnerable to eavesdropping or attacks.


URL Filtering - A security measure that blocks or allows access to specific websites based on URL addresses, often used to prevent users from accessing malicious or inappropriate content.

USB Security - The policies and measures to protect systems from security risks associated with USB drives, which can introduce malware or facilitate data exfiltration.

User Consent Management - Processes and tools for obtaining and managing individuals' consent for data processing activities.

User-Friendliness - The ease with which a tool or system can be used by its intended users.





Virus - A type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code, potentially causing damage to systems and data.

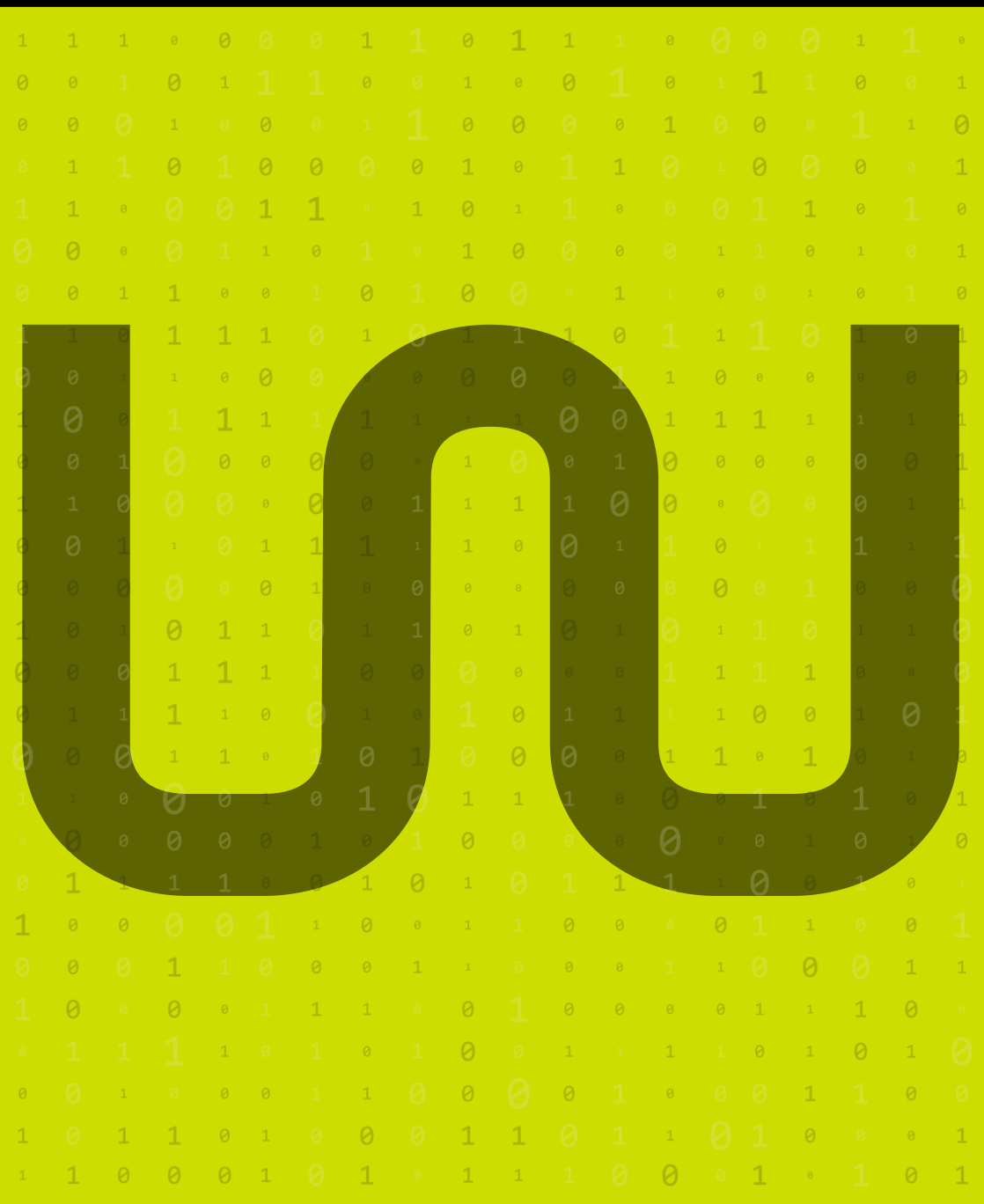
Virtual Private Network (VPN) - A service that encrypts internet traffic and hides the user's IP address, providing a secure connection between the user and a remote network. It is often used for privacy and security.


Vishing - A type of phishing attack conducted over the phone, where attackers impersonate legitimate entities to steal sensitive information like passwords or credit card details.

Vulnerability - A weakness or flaw in software, hardware, or procedures that can be exploited by an attacker to gain unauthorized access or cause harm.

Vulnerability Assessment - A systematic process of identifying, quantifying, and prioritizing the vulnerabilities in a system to understand the risks and address them before they are exploited.

Vulnerability Management - The continuous process of identifying, evaluating, treating, and reporting on vulnerabilities in systems, to reduce the window of opportunity for attacks.





Watering Hole Attack - A targeted attack where cybercriminals compromise a website frequently visited by their intended victims, injecting malware into the site to infect the visitors' devices.

Web Scrapping - The automated extraction of data from websites, often requiring compliance with data protection laws.

WEP (Wired Equivalent Privacy) - An outdated security protocol used to protect wireless networks. It has been replaced by more secure protocols like WPA due to its vulnerabilities.

Whaling - A form of phishing attack that specifically targets high-level executives or important individuals within an organization, often aiming to steal sensitive information or funds.

White Hat Hacker - An ethical hacker who uses their skills to identify and fix security vulnerabilities in systems with the owner's permission, often employed by organizations to improve security.

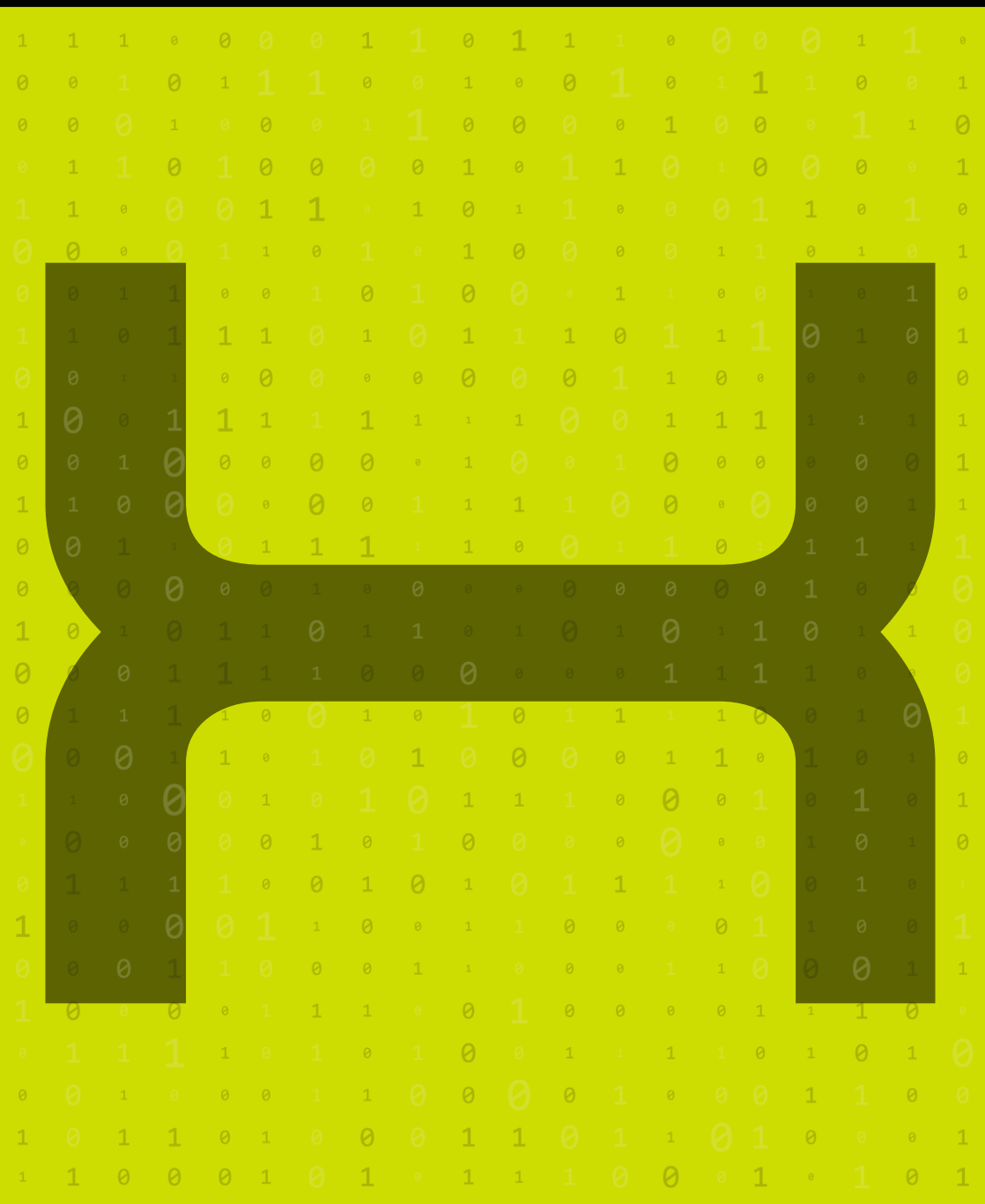
Whistleblowing - Reporting unethical or illegal practices, including data breaches or non-compliance with data protection laws.


Wi-Fi Protected Access (WPA/WPA2) - A security protocol used to secure wireless networks, providing stronger encryption than its predecessor WEP. WPA2 is currently the standard for secure Wi-Fi communication.

Worm - A type of self-replicating malware that spreads across networks by exploiting vulnerabilities, without the need for human interaction or attaching itself to files.

Workplace Privacy - The protection of personal data and privacy rights within the work environment.

WPA3 (Wi-Fi Protected Access 3) - The latest security protocol for wireless networks, designed to provide stronger data protection and secure encryption in both personal and enterprise environments.





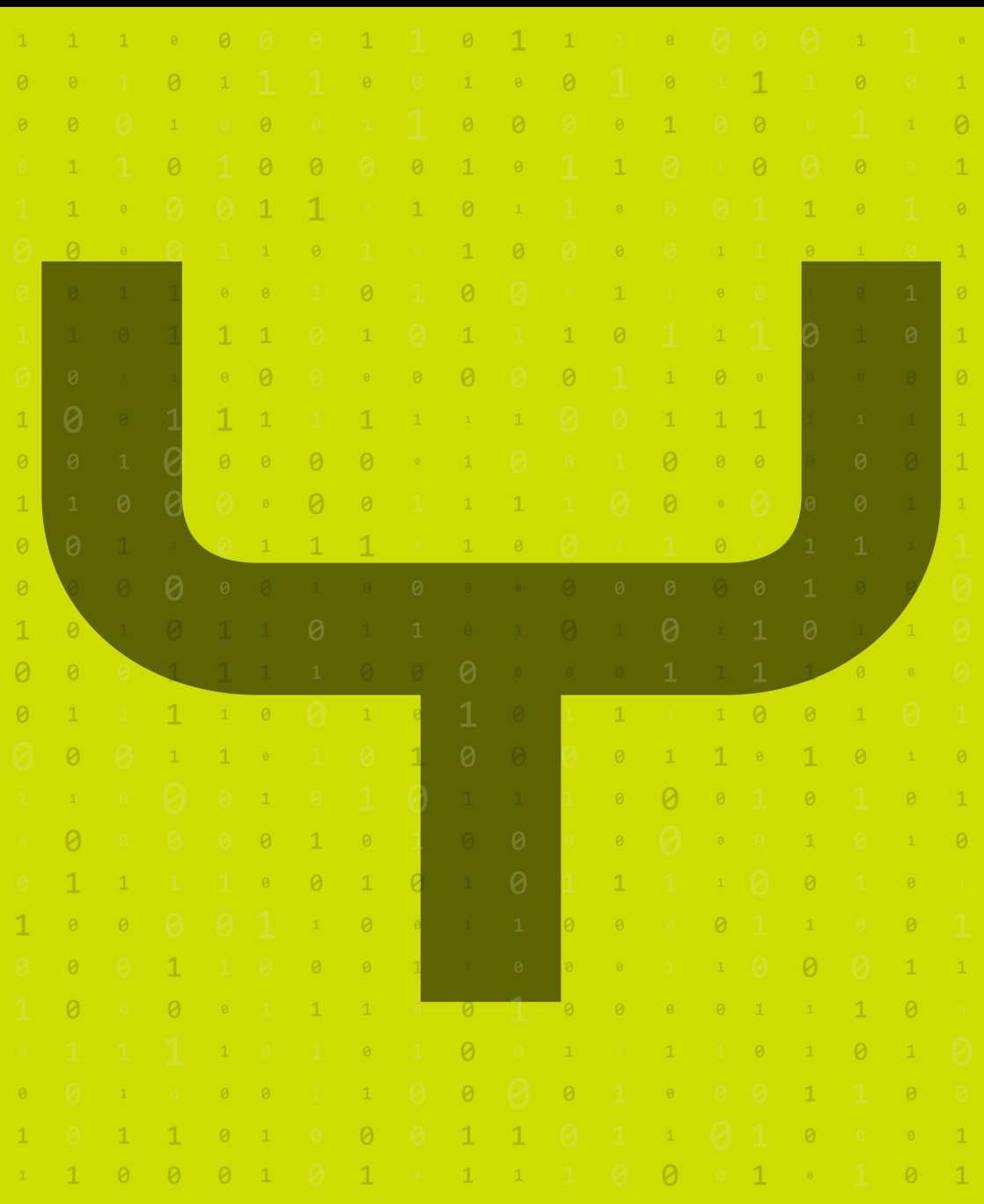
X.509 Certificate - A digital certificate that uses the X.509 public key infrastructure (PKI) standard to verify the identity of individuals, devices, and servers over the internet, ensuring secure communication.

XACML (eXtensible Access Control Markup Language) - An XML-based framework for defining and enforcing access control policies. It is commonly used to manage authorization in systems and networks.

XDR (Extended Detection and Response) - A security solution that integrates and correlates data from multiple security products to provide comprehensive threat detection, investigation, and response across an organization's network.

XML Encryption - A standard for encrypting the content of XML documents, ensuring that sensitive data transmitted in XML format is protected from unauthorized access.

XML Firewall - A security system designed to protect XML-based web services by filtering XML traffic, preventing attacks like XML injection or denial of service.

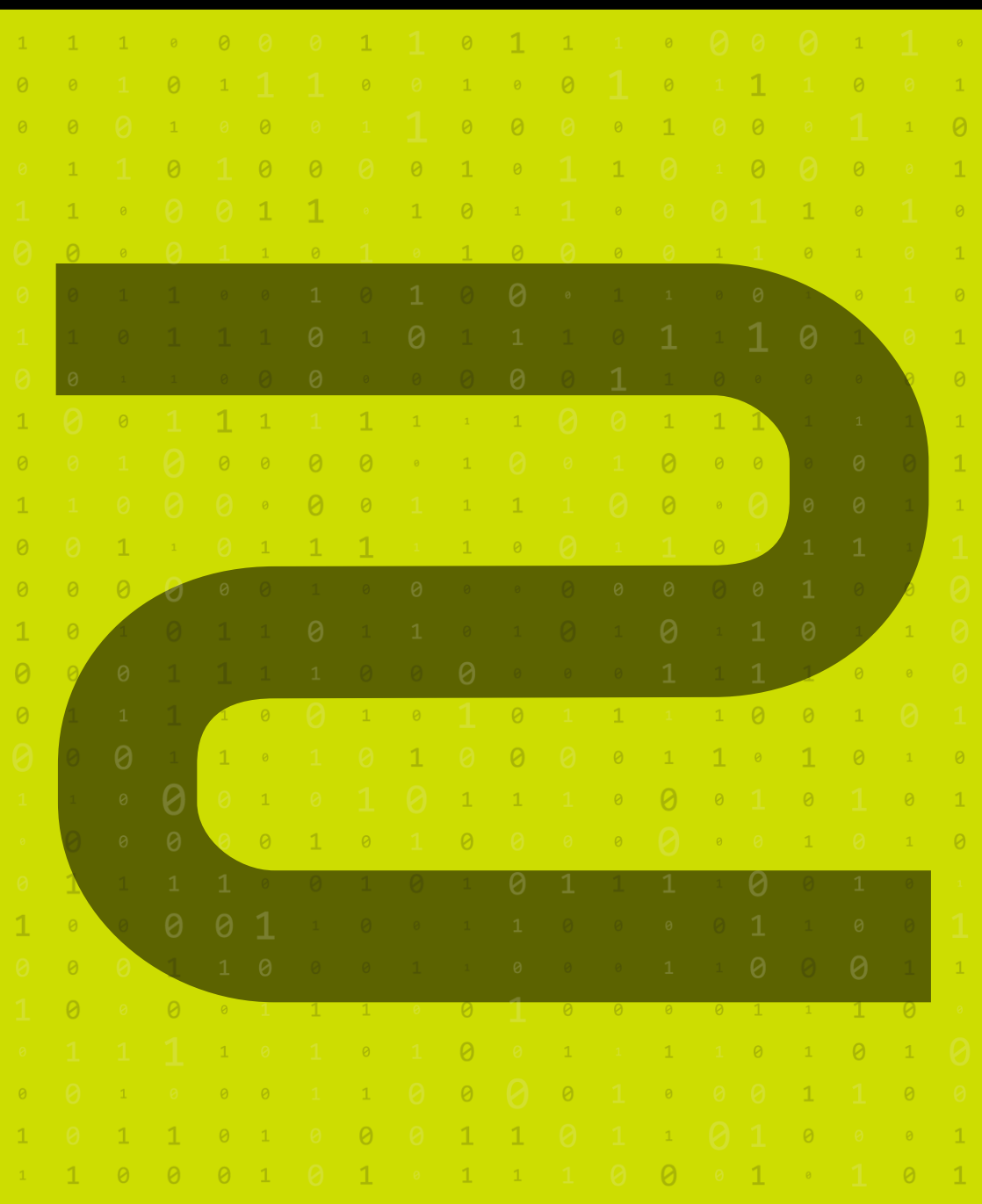





YARA - A tool used to identify and classify malware by creating descriptions (rules) of malicious file patterns. It is widely used in threat hunting and malware research.

YubiKey - A hardware authentication device that supports two-factor authentication (2FA), providing strong security by generating one-time passwords or cryptographic keys for login purposes.

Yellow Team - In the context of cybersecurity, a group that focuses on collaboration between offensive (Red Team) and defensive (Blue Team) security efforts, often helping improve coordination and knowledge sharing between the two.





Zero-day Attack - A cyberattack that exploits a previously unknown vulnerability in software or hardware, which has not yet been patched by the vendor, making it highly dangerous.

Zero Trust Architecture - A security model that assumes no network, device, or user is trusted by default, and access is only granted after verifying identity and security posture continuously.

Zero Trust Network Access (ZTNA) - A security approach that ensures secure, segmented access to network resources based on identity verification, assuming no implicit trust for any device or user inside or outside the network.

Zombie - A computer that has been compromised and is controlled remotely by an attacker, often used as part of a botnet to launch coordinated cyberattacks like Distributed Denial of Service (DDoS).

Zscaler - A cloud-based security company that provides internet security, web filtering, and zero trust network access (ZTNA) solutions for enterprises to secure their data and users.