Introduction to Cybersecurity

Cybersecurity in E.U. & Romania

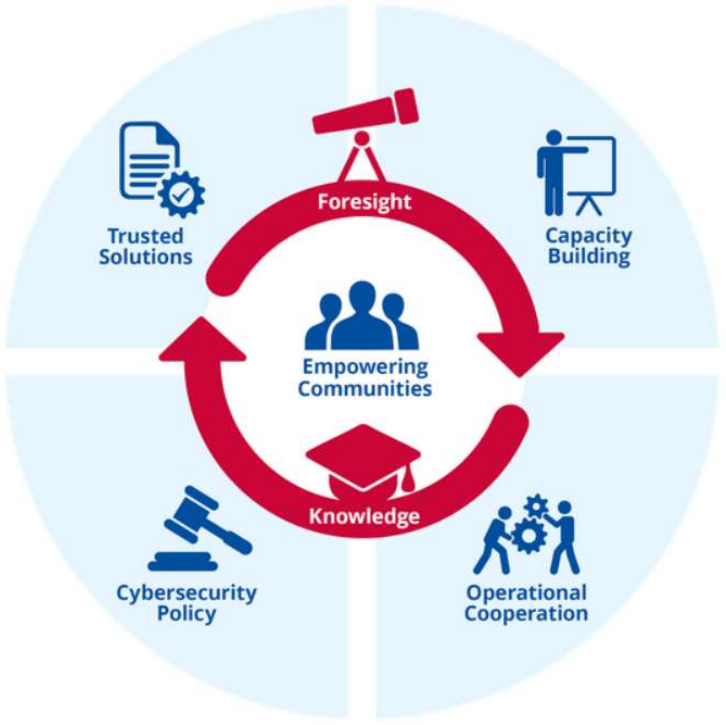
Basic Security concepts & Definitions

Security Roles

Fundamental Principles of Security

Cybersecurity in E.U. & Romania

European Union Agency for Network and Information Security
ENISA



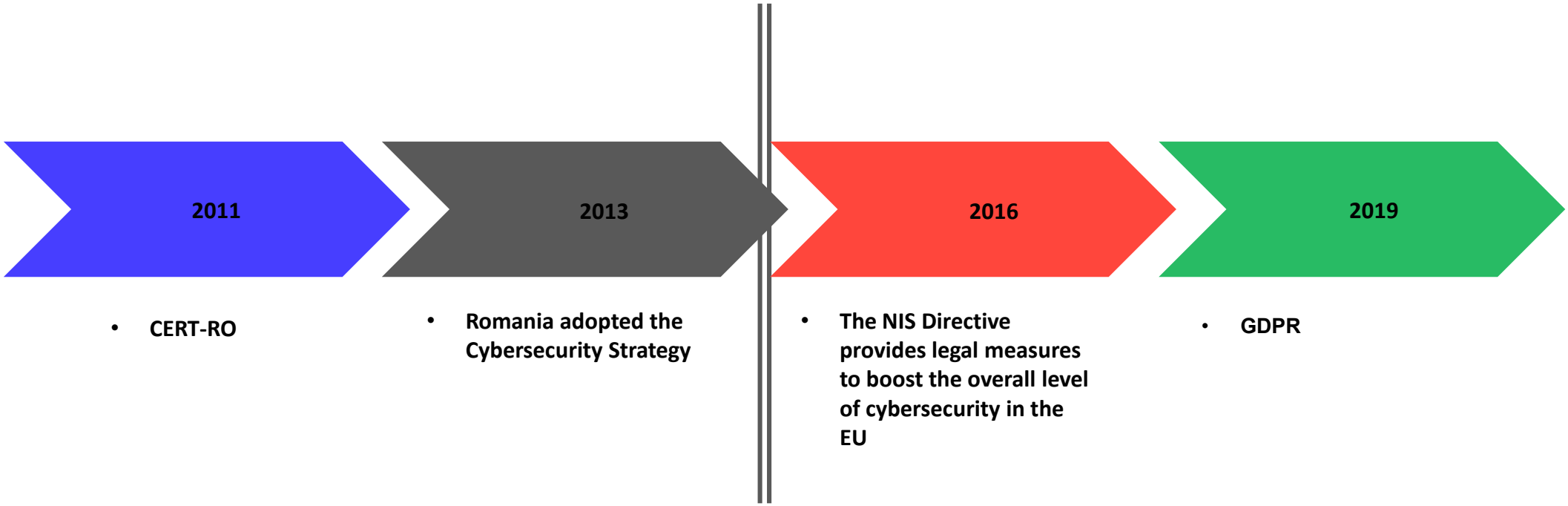
Cybersecurity in E.U. & Romania

Initiatives

EUROPEAN CYBER SECURITY MONTH

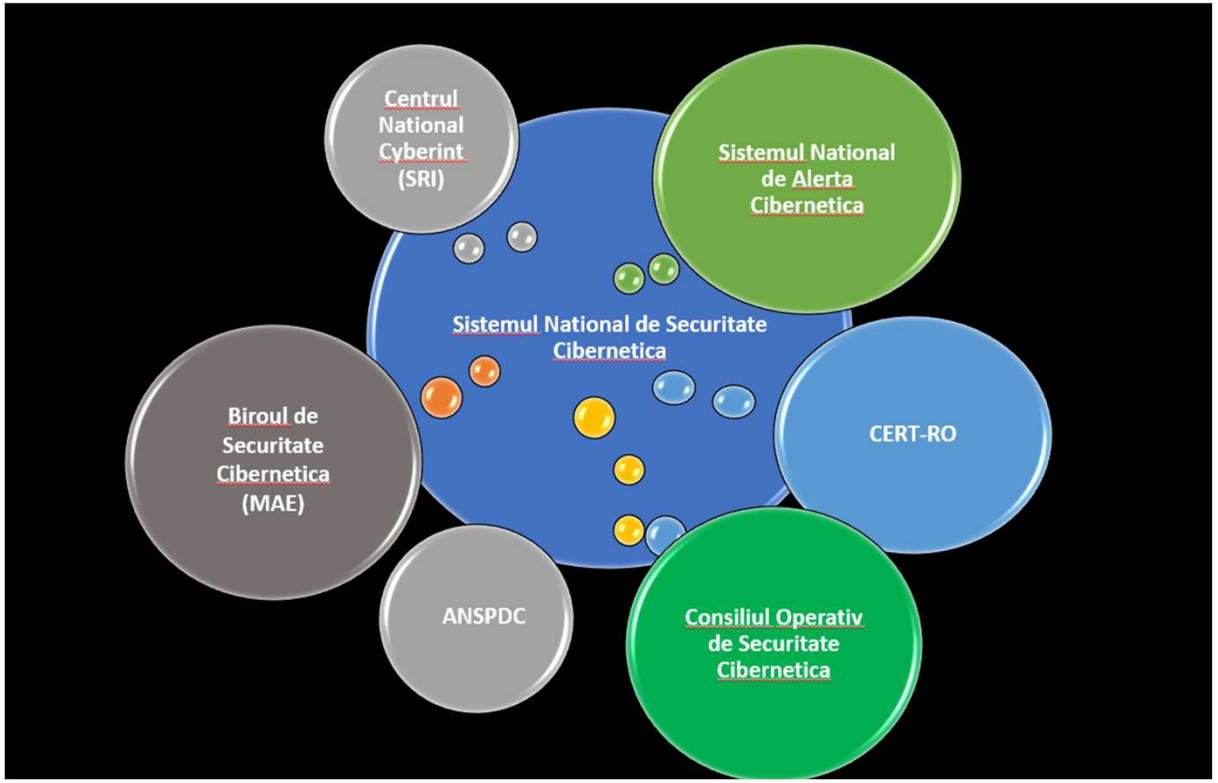
Cybersecurity in E.U. & Romania

Cybersecurity in Romania



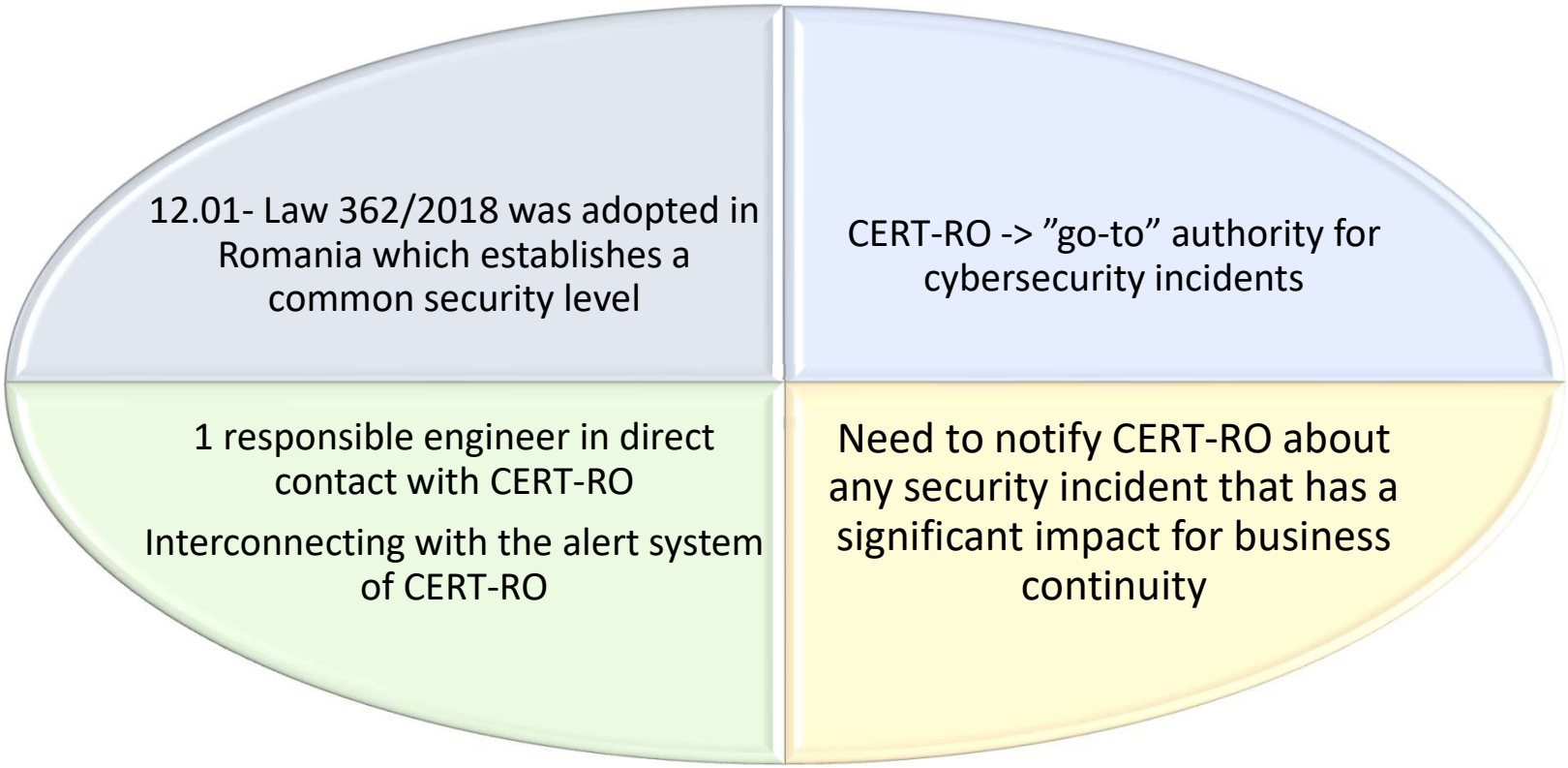
Cybersecurity in E.U. & Romania

Romanian National Structures with roles in Cybersecurity



Cybersecurity in E.U. & Romania

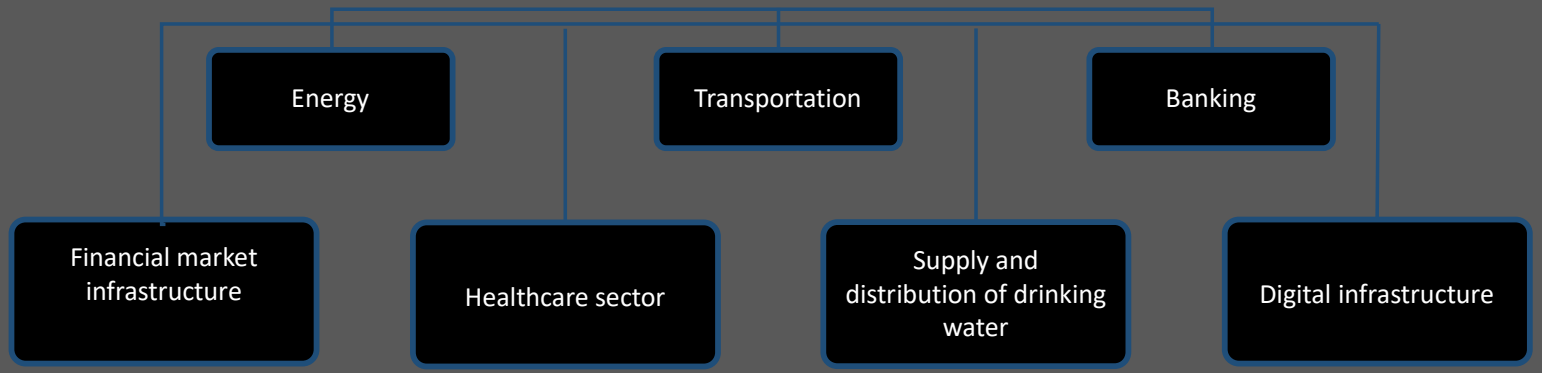
NIS Directive: Law 362/2018



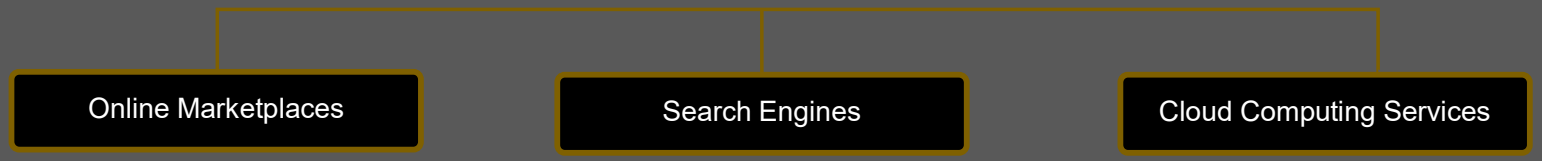
Cybersecurity in E.U. & Romania

NIS Directive: Law 362/2018

Essential Services Providers



Digital Services Providers



Cybersecurity in E.U. & Romania

Regulation (EU) 2016/679 - **GDPR**

- The possibility of obtaining comprehensive information on the purpose and legal basis in the personal data processing
- The data storage period and entailing rights;
- The right to be forgotten, applicable in the online environment
- The obligation of the operator to demonstrate consent for personal data processing
- Portability of data - the possibility to request the transfer of data to another data operator

Cybersecurity in E.U. & Romania

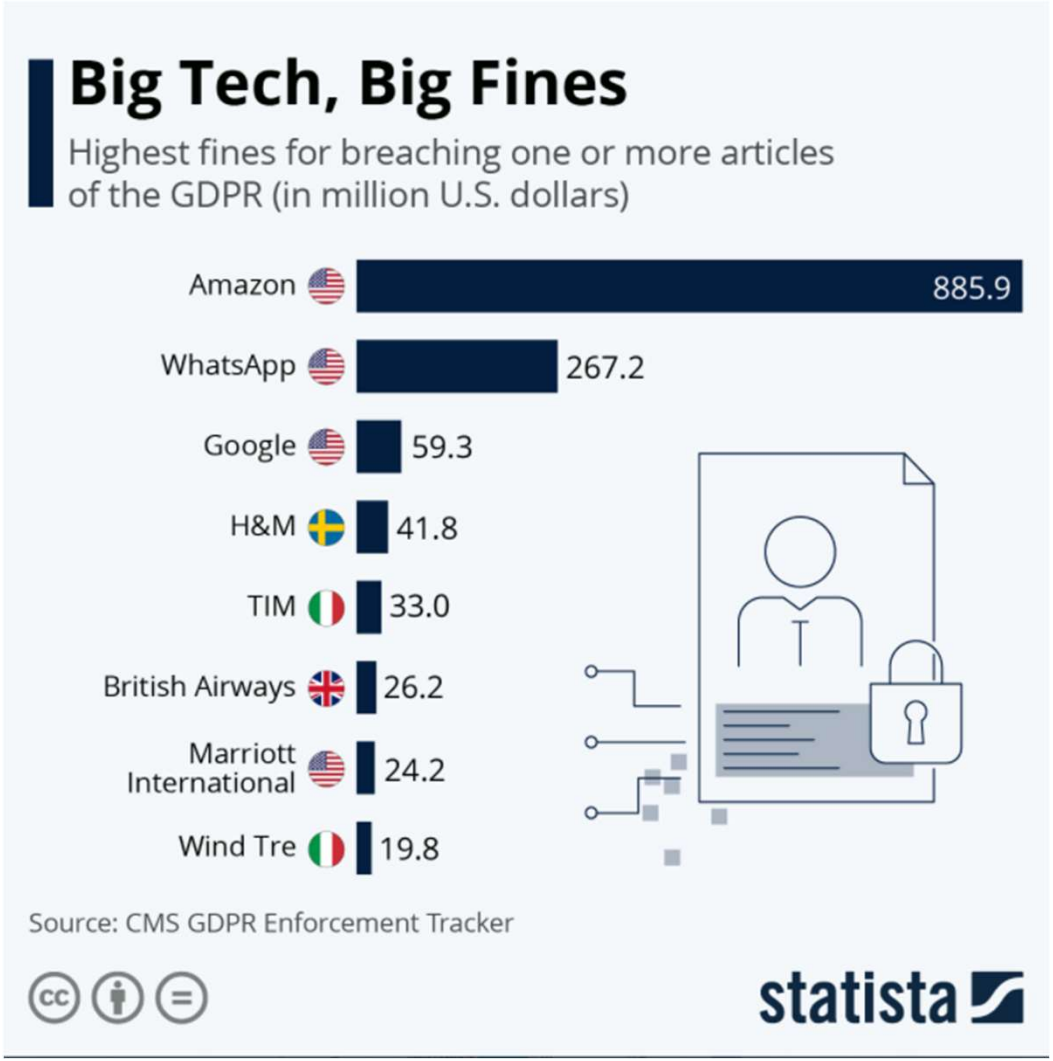
Data security under **GDPR**

- Handle data securely by implementing “appropriate technical and organizational measures.”
- Technical measures: use two-factor authentication/ contracting with cloud providers that use end-to-end encryption etc
- Organizational measures: staff trainings, adding a data privacy policy to your employee handbook, or limiting access to personal data
- If you have a data breach, you have 72 hours to tell the data subjects or face penalties.

Cybersecurity in E.U. & Romania

GDPR fines

- up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher
- up to €20 million or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher



Basic concepts & Definitions

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Threat

Any potential danger that is associated with the exploitation of a vulnerability

Information Security Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

Basic concepts & Definitions

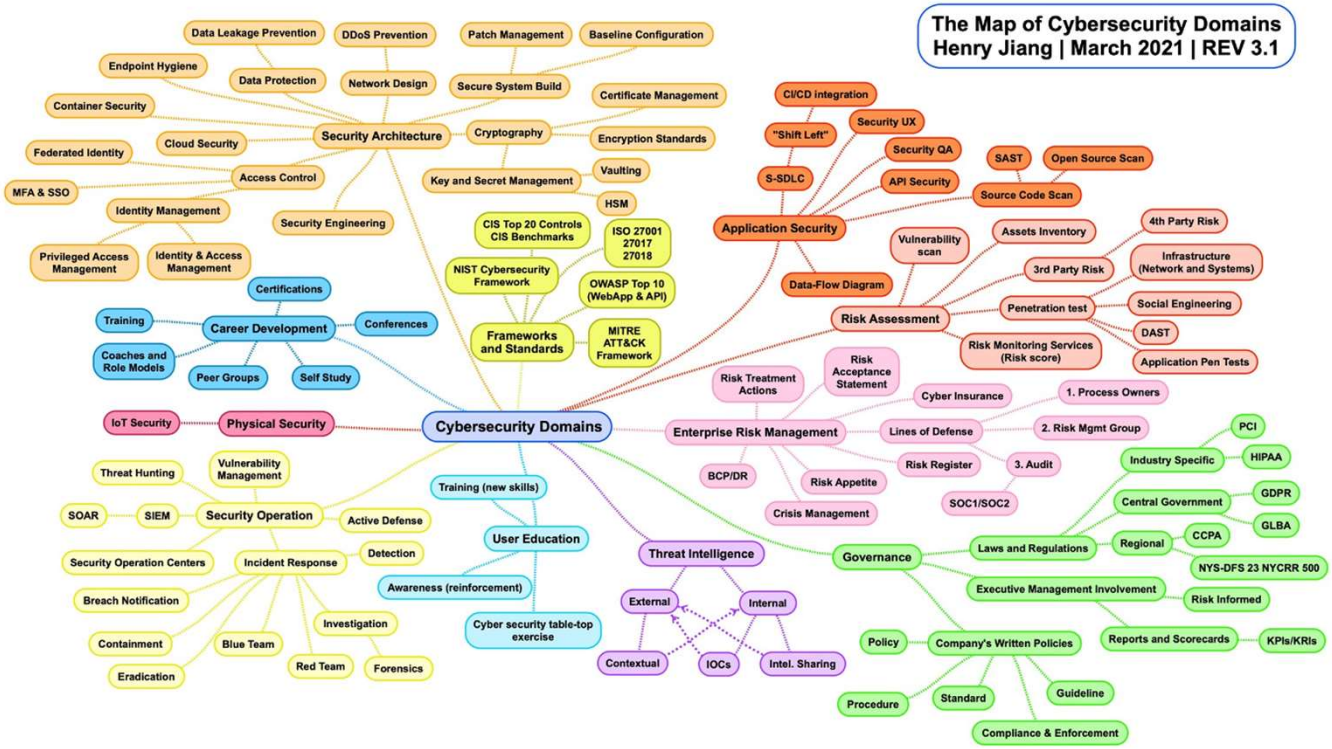
Risk
The likelihood of a threat source exploiting a vulnerability and the corresponding business impact.

Security Patch
Software or operating-system patch that is intended to correct a vulnerability to hacking or viral infection

Malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system

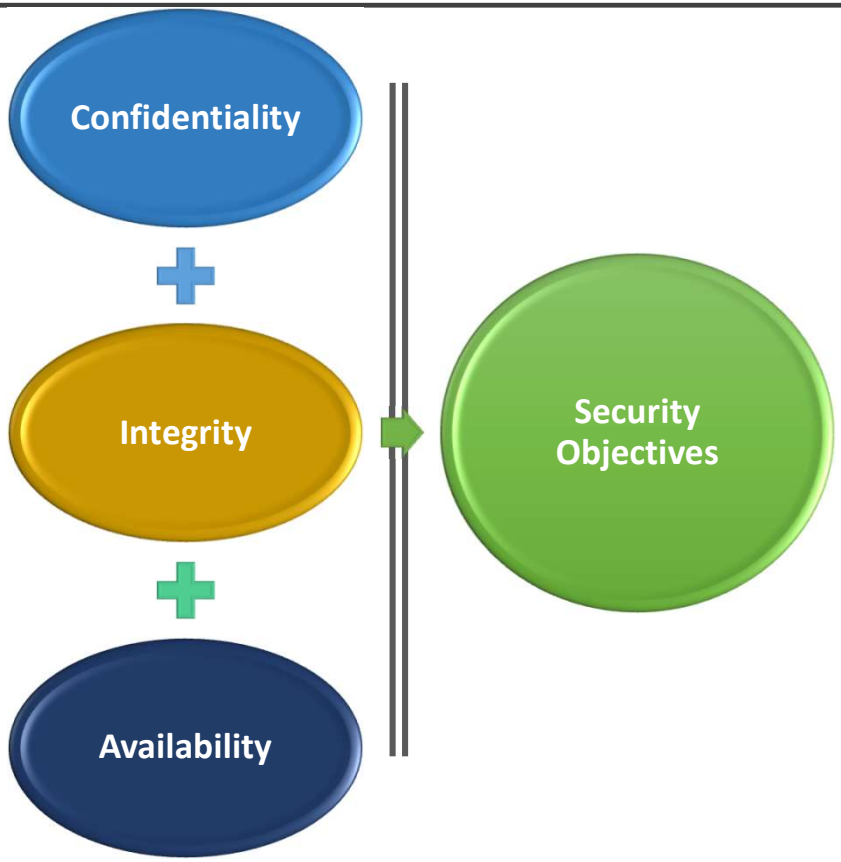
Control (Countermeasure)
Measures put in place to mitigate (reduce) the potential risk

Security Roles



Fundamental Principles of Security

CIA Triad



Fundamental Principles of Security

Confidentiality

Ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess it.

It is implemented through security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption.

The level of secrecy should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination.

Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing password files, breaking encryption schemes, and social engineering.

Fundamental Principles of Security

Cryptography

Is a method of storing and transmitting data in a form that only those it is intended for can read and process

It is considered a science of protecting information by encoding it into an unreadable format

Old cryptographic techniques includes: Scytale cipher, Caesar cypher, ROT13

With enough time, resources, and motivation, hackers can successfully attack most cryptosystems and reveal the encoded information.

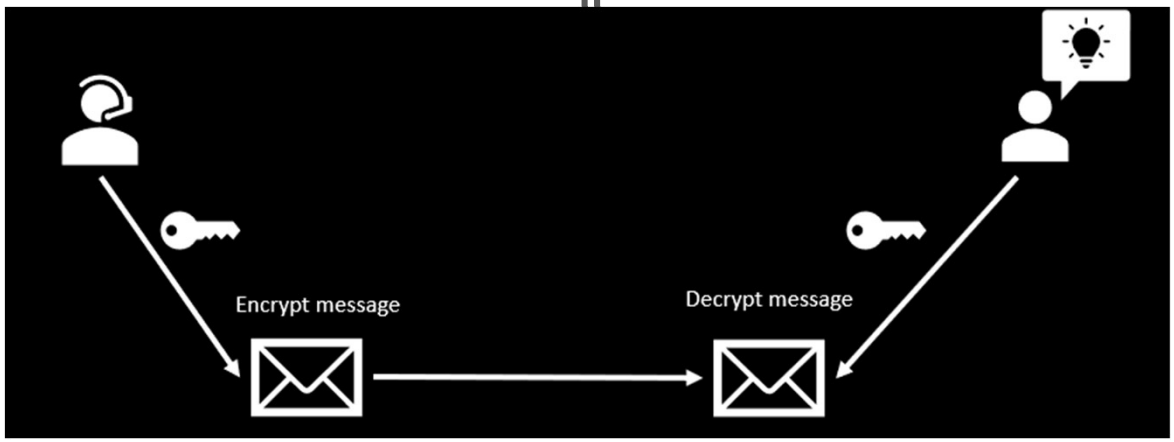
Fundamental Principles of Security

Symmetric Cryptography

The sender and receiver use the same key for encryption and decryption

The security of the symmetric encryption method is completely dependent on how well users protect the key

The key must be shared through an out-of-band method.



Fundamental Principles of Security

Symmetric Cryptography

Strengths:

- ❑ Much faster (less computationally intensive) than asymmetric systems.
- ❑ Hard to break if using a large key size.

Weaknesses:

- ❑ Requires a secure mechanism to deliver keys properly.
- ❑ Provides confidentiality but not authenticity or nonrepudiation.
- ❑ Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.

Fundamental Principles of Security

Symmetric Cryptography - examples

Data Encryption Standard (DES)

- Has been used since the mid-1970s.
- It was the primary standard used in government and industry until it was replaced by AES.
- It's based on a 56-bit key
- It is now considered insecure because of the small key size.

Triple-DES (3DES)

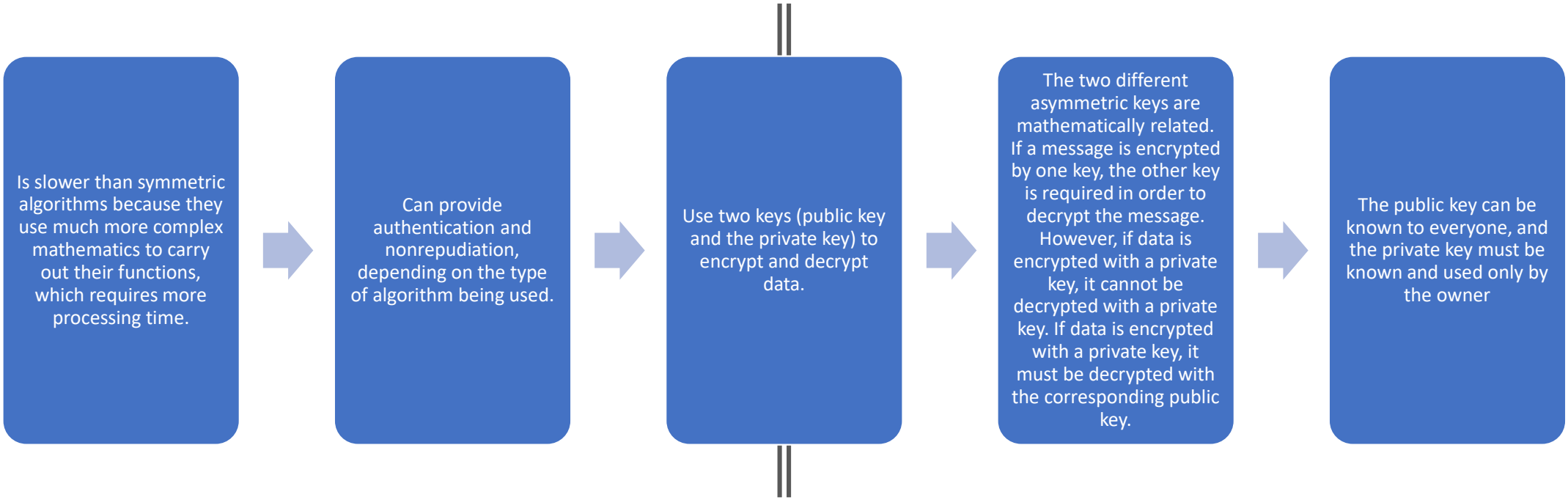
- Is a technological upgrade of DES.
- It increases the key length to 168 bits (using three 56-bit DES keys).

Advanced Encryption Standard (AES)

- Has replaced DES as the current standard.
- Is the current product used by U.S. governmental agencies.
- It supports key sizes of 128, 192, and 256 bits, with 128 bits being the default.

Fundamental Principles of Security

Asymmetric Cryptography



Fundamental Principles of Security

Asymmetric Cryptography

Strengths:

- ❑ Better key distribution than symmetric systems.
- ❑ Better scalability than symmetric systems.
- ❑ Can provide authentication and nonrepudiation.

Weaknesses:

- ❑ Works much more slowly than symmetric systems.
- ❑ Mathematically intensive tasks.

Fundamental Principles of Security

Asymmetric Cryptography - examples

Diffie-Hellman Algorithm

- Is used primarily to send keys across public networks

RSA

- Can be used for digital signatures, key exchange, and encryption.
- Developed in 1978 at MIT.
- The security comes from the difficulty of factoring large numbers into their original prime numbers.

El Gamal

- Can be used for digital signatures, encryption, and key exchange.
- It is based calculating discrete logarithms in a finite field (if b and g are integers, then k is the logarithm in the equation bk= g.
- When compared to other algorithms, this algorithm is usually the slowest.

Elliptic curve cryptosystem (ECC)

- Provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption.
- ECC is more efficient than RSA and any other asymmetric algorithm.

Fundamental Principles of Security

Integrity

- The second principle of the CIA Triad
- Protects the reliability and correctness of data
- Prevents unauthorized alterations of data
- Ensures that data remains correct, unaltered, and preserved.
- It protects against malicious unauthorized activities as well as mistakes made by authorized users
- Alterations should not occur while the object is in storage, in transit, or in process.

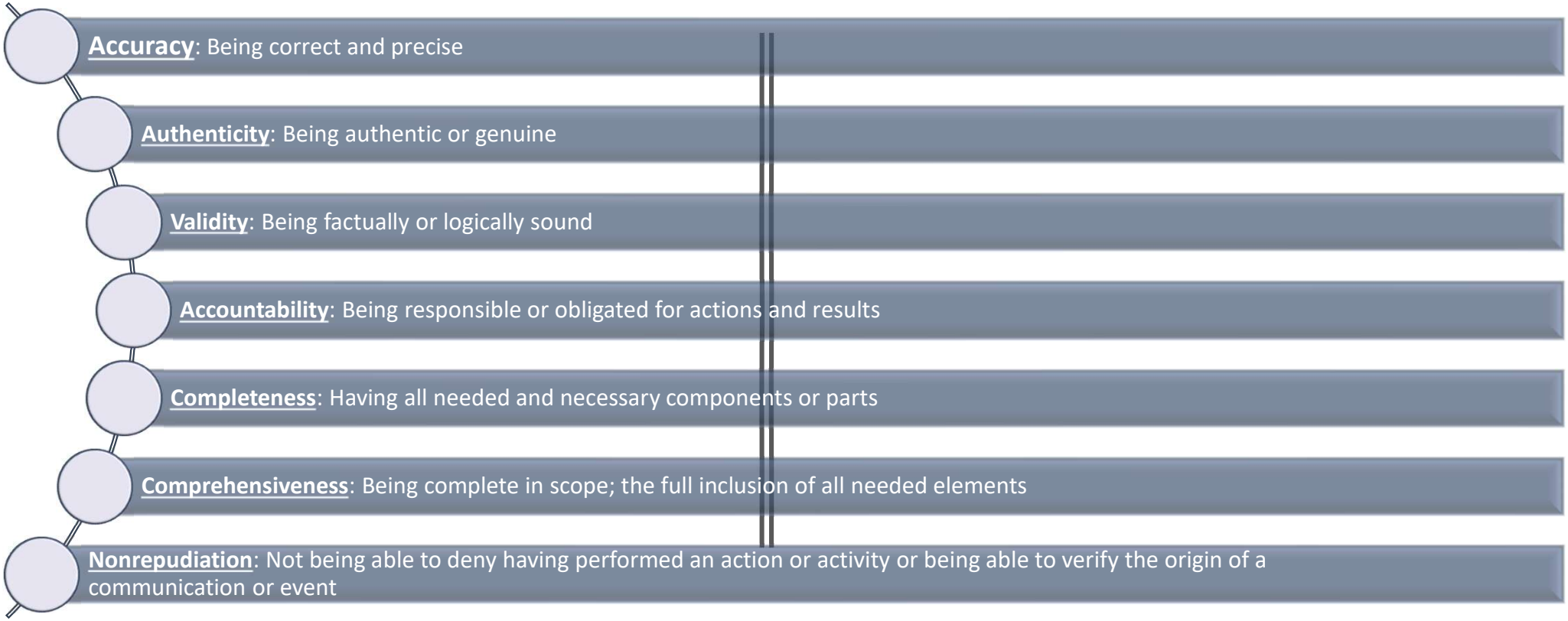
Fundamental Principles of Security

Integrity

- Prevents unauthorized subjects from making modifications
- Prevents authorized subjects from making unauthorized modifications, such as mistakes
- Maintains the internal and external consistency of objects so that the data is a correct and a true reflection of the real world (protecting the reliability and correctness of data)
- In order to maintain integrity on a system, we must use controls that restrict access to data, objects, and resources.
- Modifying or deleting files, entering invalid data, altering configurations (including errors in commands), introducing a virus, executing malicious code such as a Trojan horse are some examples of integrity breaches

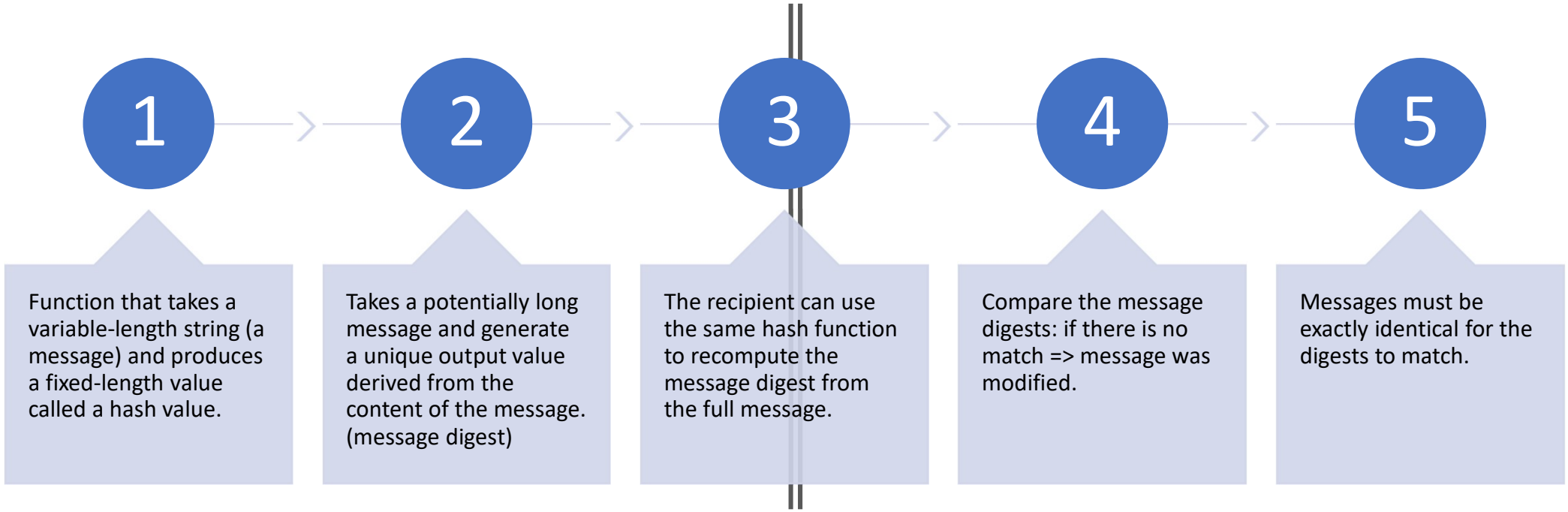
Fundamental Principles of Security

Integrity - Related Concepts



Fundamental Principles of Security

Hashing



Fundamental Principles of Security

Hashing Algorithms

MD2

- ❑ No longer accepted as suitable hashing functions.
- ❑ Pads the message so that its length is a multiple of 16 bytes. It then computes a 16-byte checksum and appends it to the end of the message.
- ❑ A 128-bit message digest is then generated by using the entire original message along with the appended checksum.

MD4

- ❑Pads the message to ensure that the message length is 64 bits smaller than a multiple of 512 bits.
- ❑The MD4 algorithm then processes 512-bit blocks of the message in three rounds of computation. The final output is a 128-bit message digest.

MD5

- ❑It also processes 512-bit blocks of the message
- ❑It uses four distinct rounds of computation to produce a digest of the
- ❑Same length as the MD2 and MD4 algorithms (128 bits).
- ❑-Has the same padding requirements as MD4--the message length must be 64 bits less than a multiple of 512 bits.

Secure Hash Algorithm (SHA)

- ❑Produces a 160-bit message digest. It is used with Digital Signature Algorithm (DSA)
- ❑SHA-1 -Takes an input of virtually any length and produces a 160-bit message digest.
- ❑SHA-256: 256-bit message digest using a 512-bit block size.
- ❑SHA-224: 224-bit message digest using a 512-bit block size.
- ❑SHA-512: 512-bit message digest using a 1,024-bit block size
- ❑SHA-384: 384-bit message digest using a 1,024-bit block size.

Fundamental Principles of Security

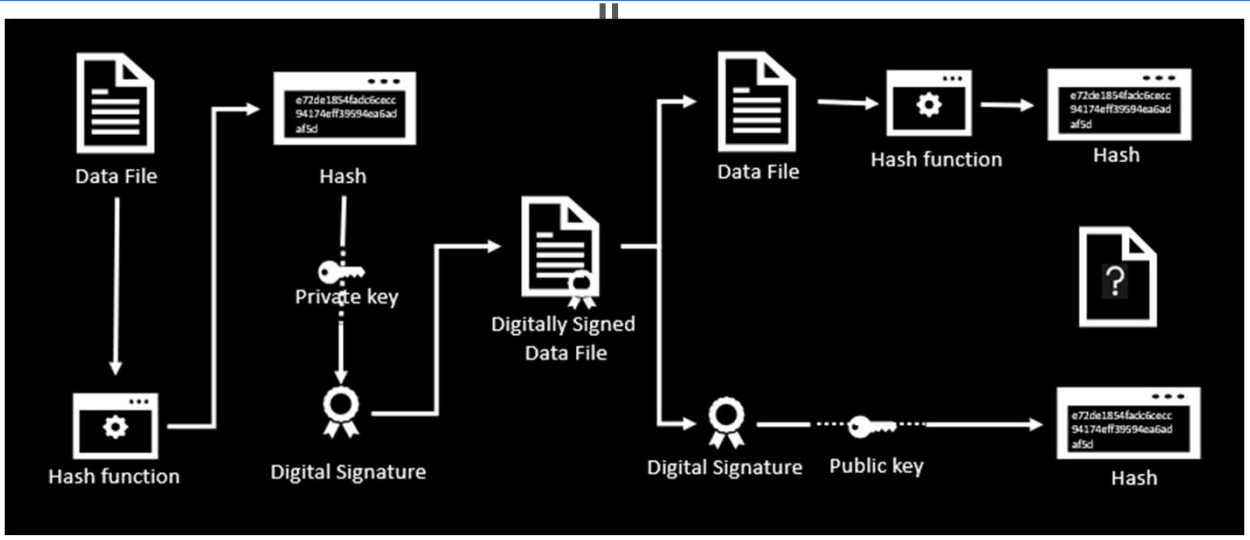
Digital Signatures

Prevents unauthorized subjects from making modifications

=

Prevents authorized subjects from making unauthorized modifications, such as mistakes

=



Fundamental Principles of Security

Availability

- Third principle of the CIA Triad
- Authorized subjects are granted timely and uninterrupted access to specific objects
- Supporting infrastructure: functional and allows authorized users to gain authorized access.
- Prevention of DoS & DDoS attacks

Fundamental Principles of Security

Availability - Related Concepts

- **Usability**: being easy to use or learn or being able to be understood and controlled by a subject
- **Accessibility**: The assurance that the widest range of subjects can interact with a resource regardless of their capabilities or limitations
- **Timeliness**: Being prompt, on time, within a reasonable time frame, or providing low-latency response
- **Redundancy**: duplication of critical components or functions of a system
- **Data backup :** a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.
- **Backup site**: disaster recovery center, is used to store data that can enable computer systems and networks to be restored and properly configure in the event of a disaster.

Fundamental Principles of Security

Availability – Threats