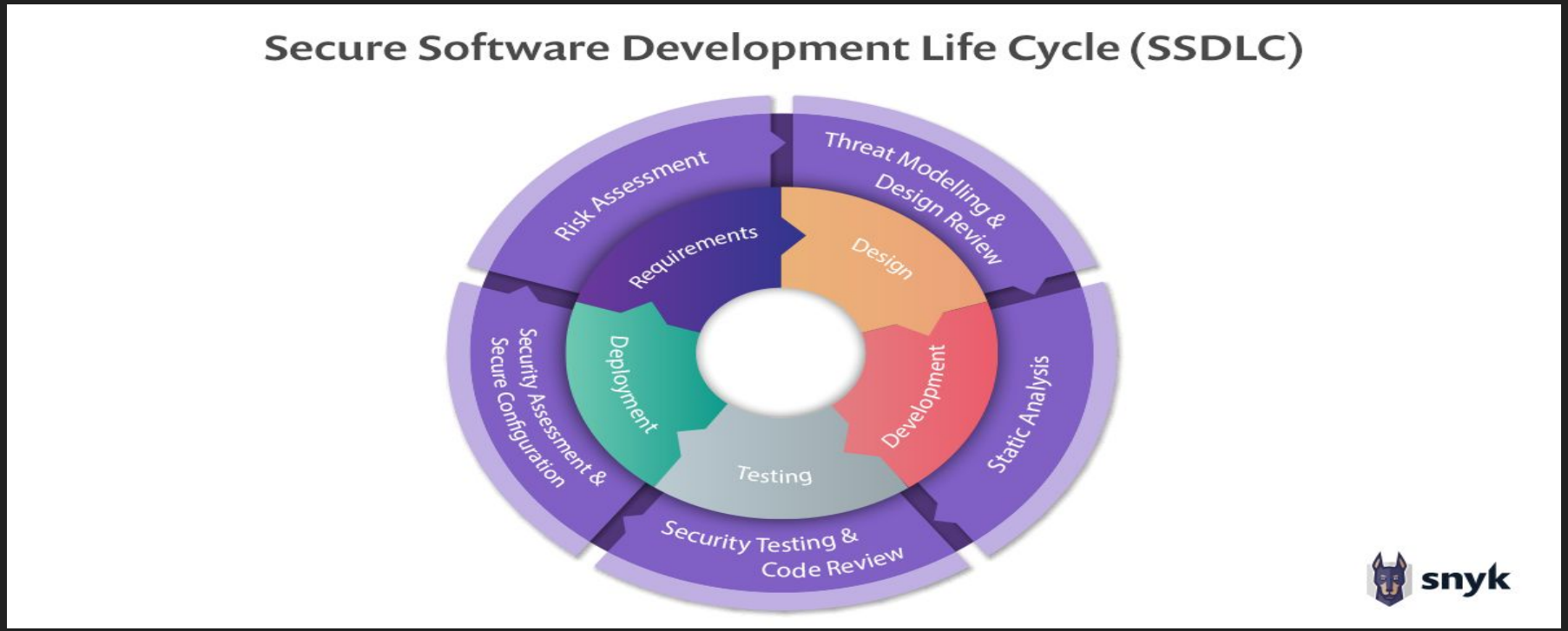
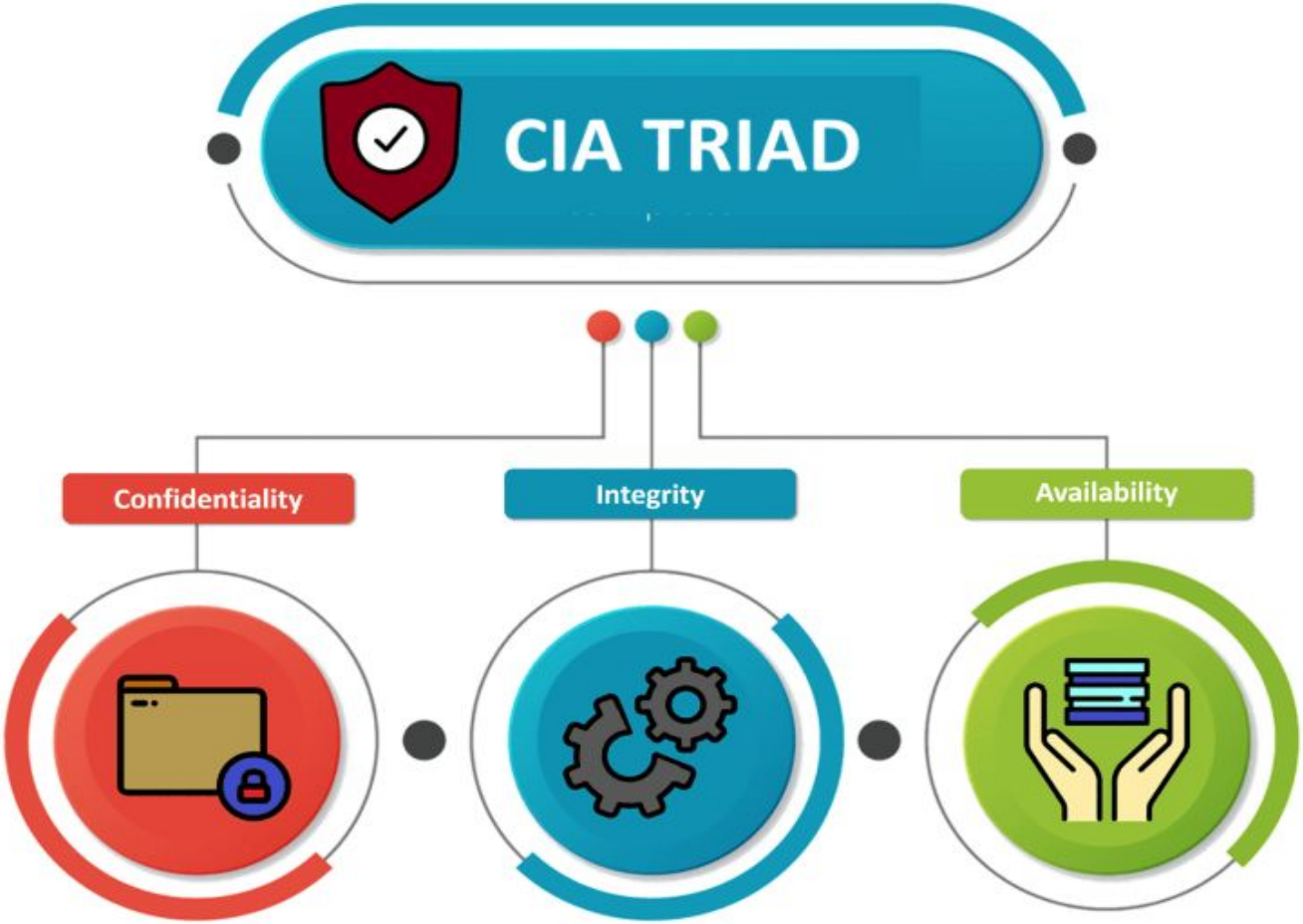
Secure SDLC (SSDLC)



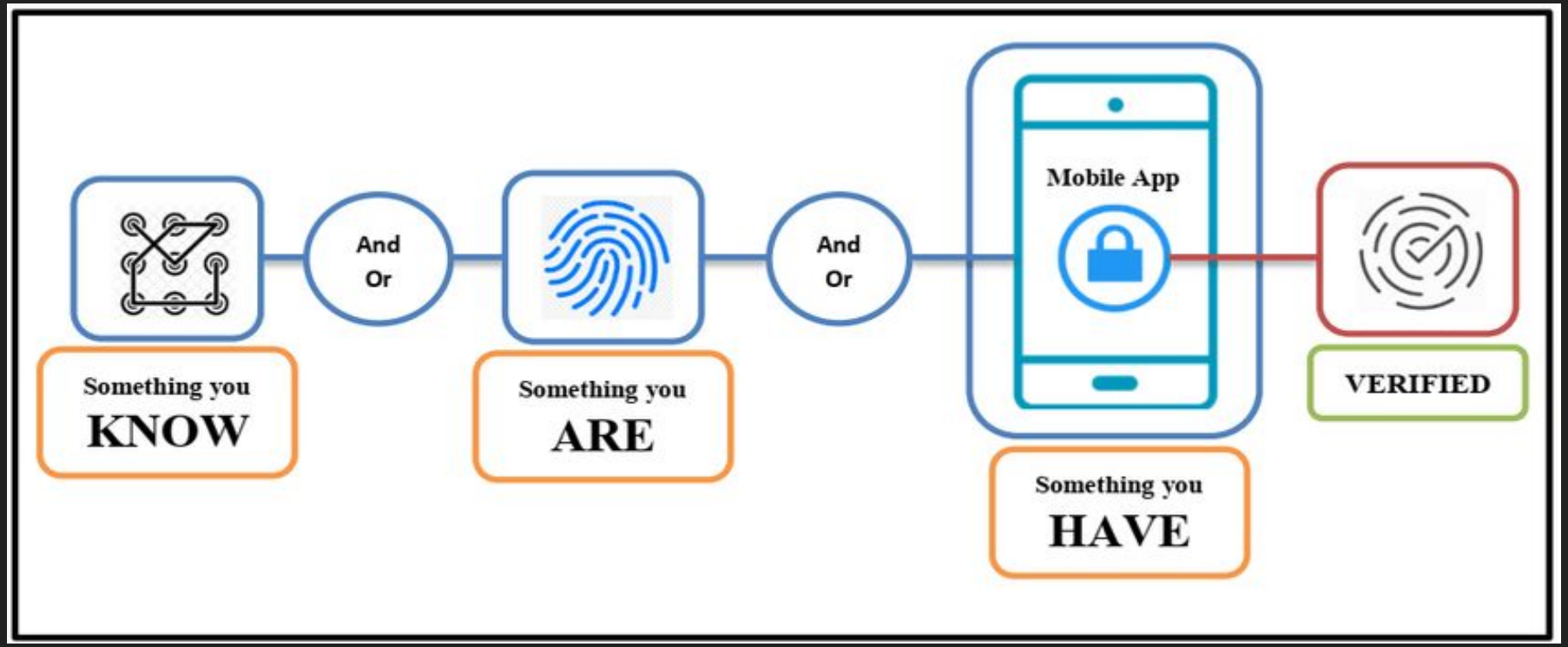

CIA TRIAD
Confidentiality
Integrity
Availability

CIA Triad & AAA

- Confidentiality
- Integrity
- Availability
- Authentication / Identification
- Authorization
- Auditing / Accountability

Authentication

Authentication Factors



Authentication vs. Authorization

Who are you?

Validate the identification of the user

What are you allowed to do?

Check users' permissions to access data

Confidentiality

- Cracking Encrypted Data
- Man In The Middle attacks on plain text
- Data leakage/ Unauthorised copying of sensitive data
- Installing Spyware/Malware on a server

Integrity

- Web Penetration for malware insertion
- Maliciously accessing servers and forging records
- Unauthorised Database scans
- Remotely controlling zombie systems

Availability

- DOS/DDoS attacks
- Ransomware attacks – Forced encryption of Key data
- Deliberately disrupting a server rooms power supply
- Flooding a server with too many requests

Vulnerability

- Vulnerability refers to the weakness of an asset that can be exploited by one or more attacker
- In context of cyber world, vulnerability refers to a bug/ defect in hardware or software which remains to be fixed and is prone to be exploited to cause a damage to one of the elements within CIA triad

Threat

- A threat is any event that has the potential to bring harm to an organisation or individual
- Natural Threats, Intentional Threats, Unintentional threats
- Threat assessment techniques are used for understanding threats.

Risk

- Risk refers to the potential for loss or damage when a threat exploits a vulnerability
- Risk = Threat x Vulnerability
- Risk management is key to cybersecurity

Vulnerability vs Threat vs Risk

An asset is what we're trying to protect.

A threat is what we're trying to protect against.

A vulnerability is a weakness or gap in our protection efforts.

Risk is the intersection of assets, threats, and vulnerabilities.

A + T + V = R

CVSS SCORE METRICS

A CVSS score is composed of three sets of metrics (**Base**, **Temporal**, **Environmental**), each of which have an underlying scoring component.

BASIC METRIC GROUP

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact Metrics

- Compatibility Impact
- Integrity Impact
- Availability Impact
- Scope

TEMPORAL METRIC GROUP

- Exploit Code Maturity
- Remediation Level
- Report Confidence

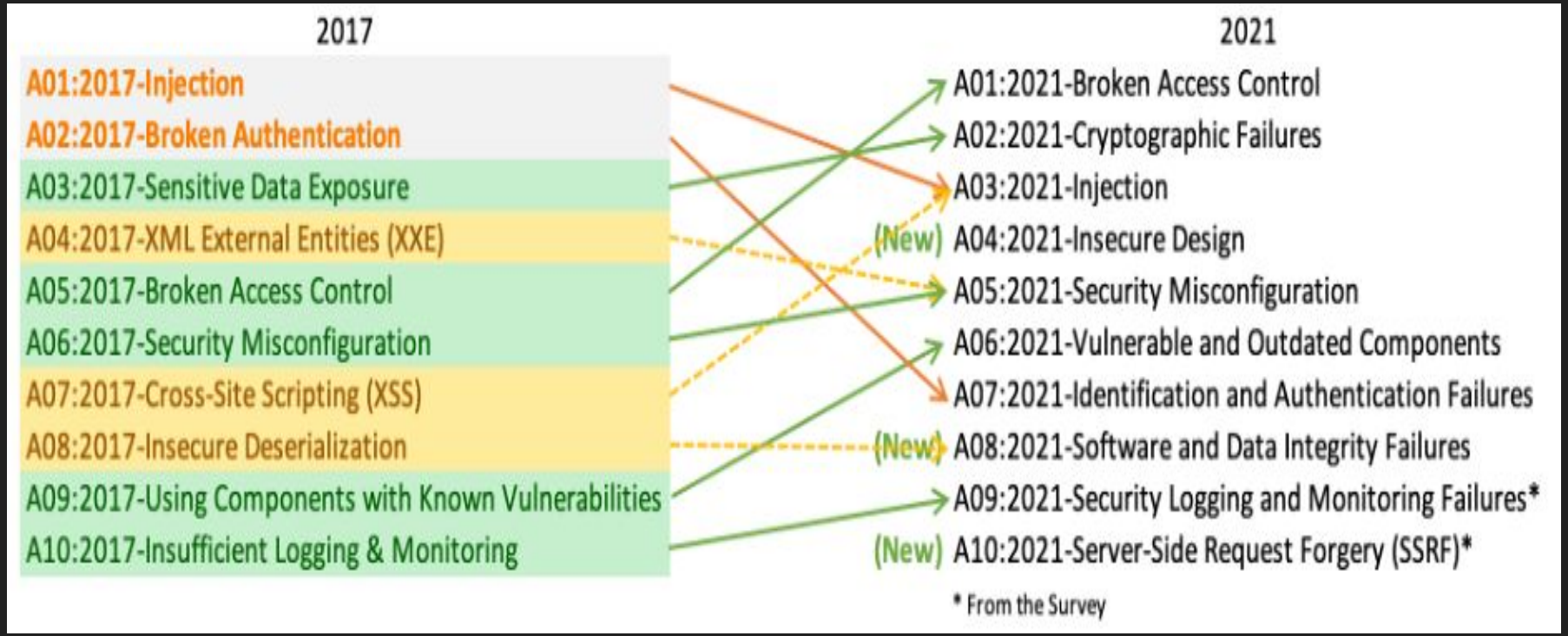
ENVIRONMENTAL METRIC GROUP

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

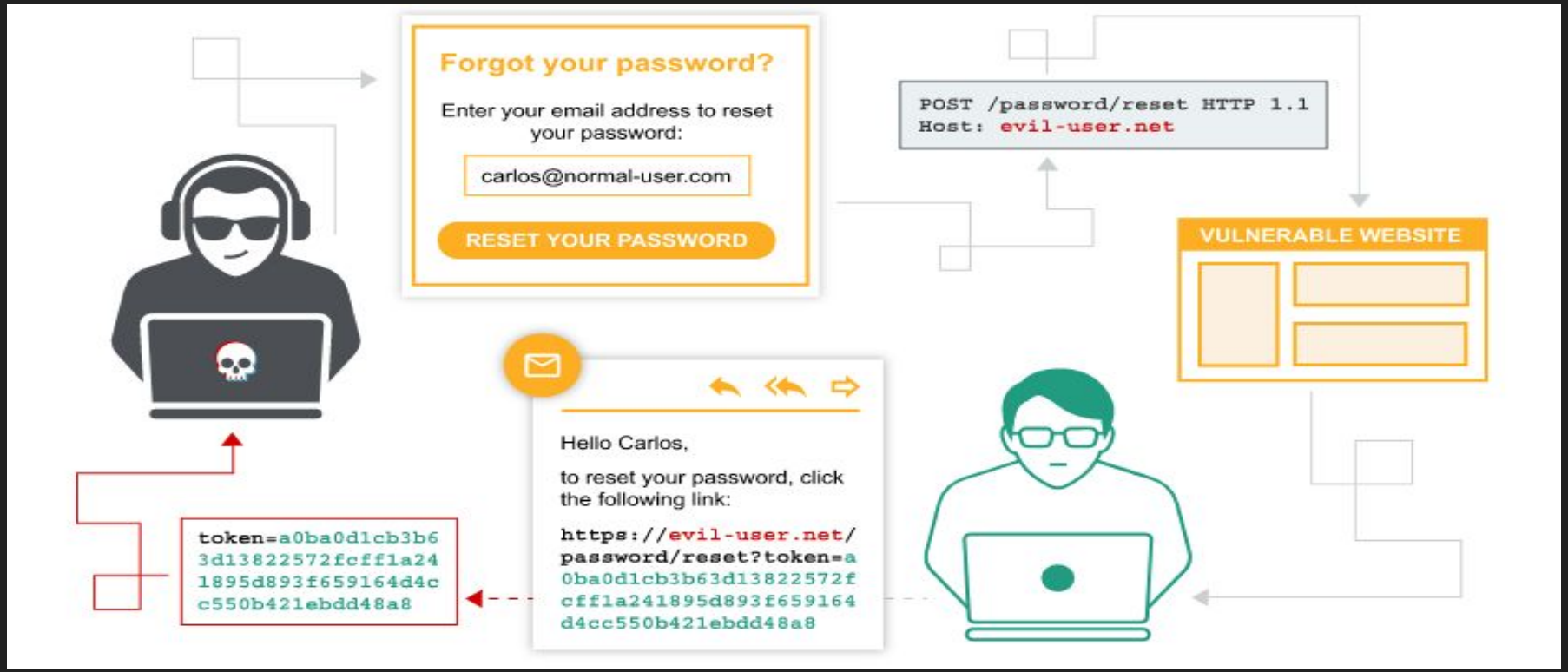
OWASP

Open Web Application Security Project

OWASP Top 10


2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

A07-2021: Identification and Authentication Failures



A01-2021: Broken Access Control

A06-2021: Vulnerable and Outdated components

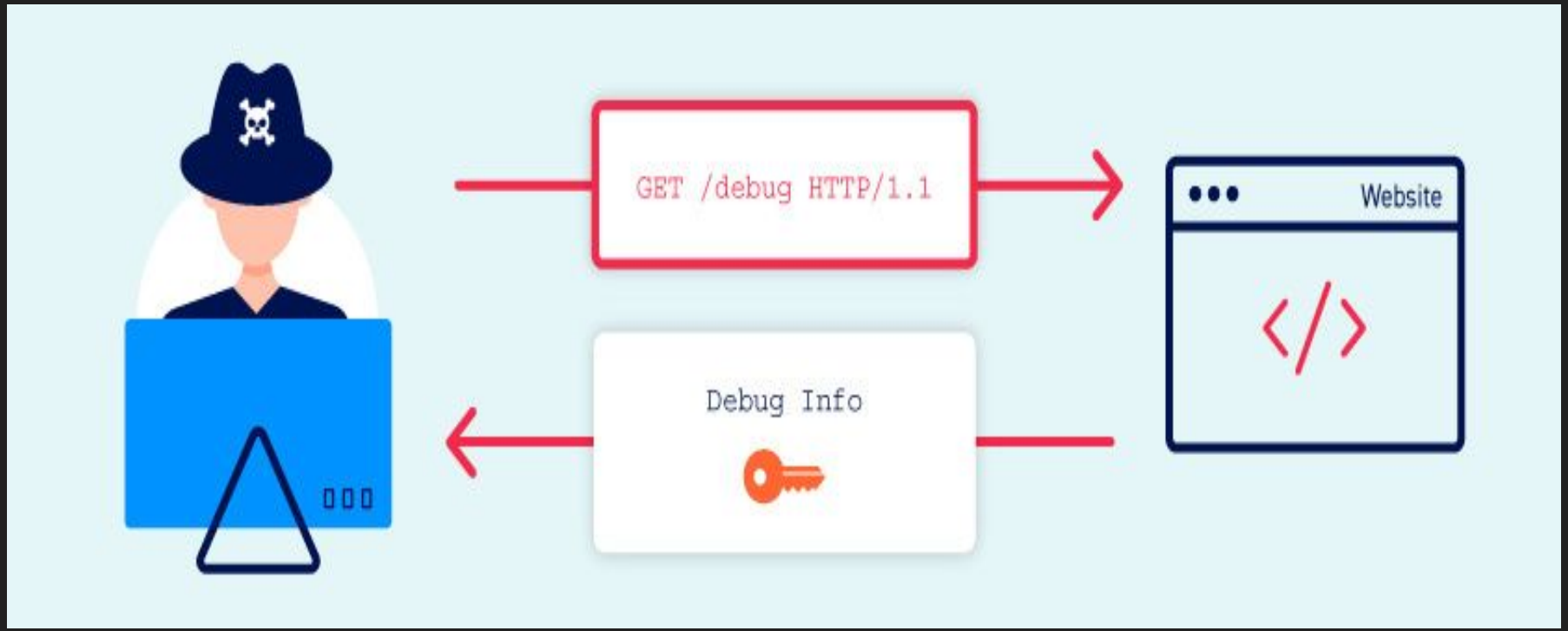
Zero Day Vulnerability Timeline


Apache
LOG4J
TM

Common Vulnerabilities and Exposures

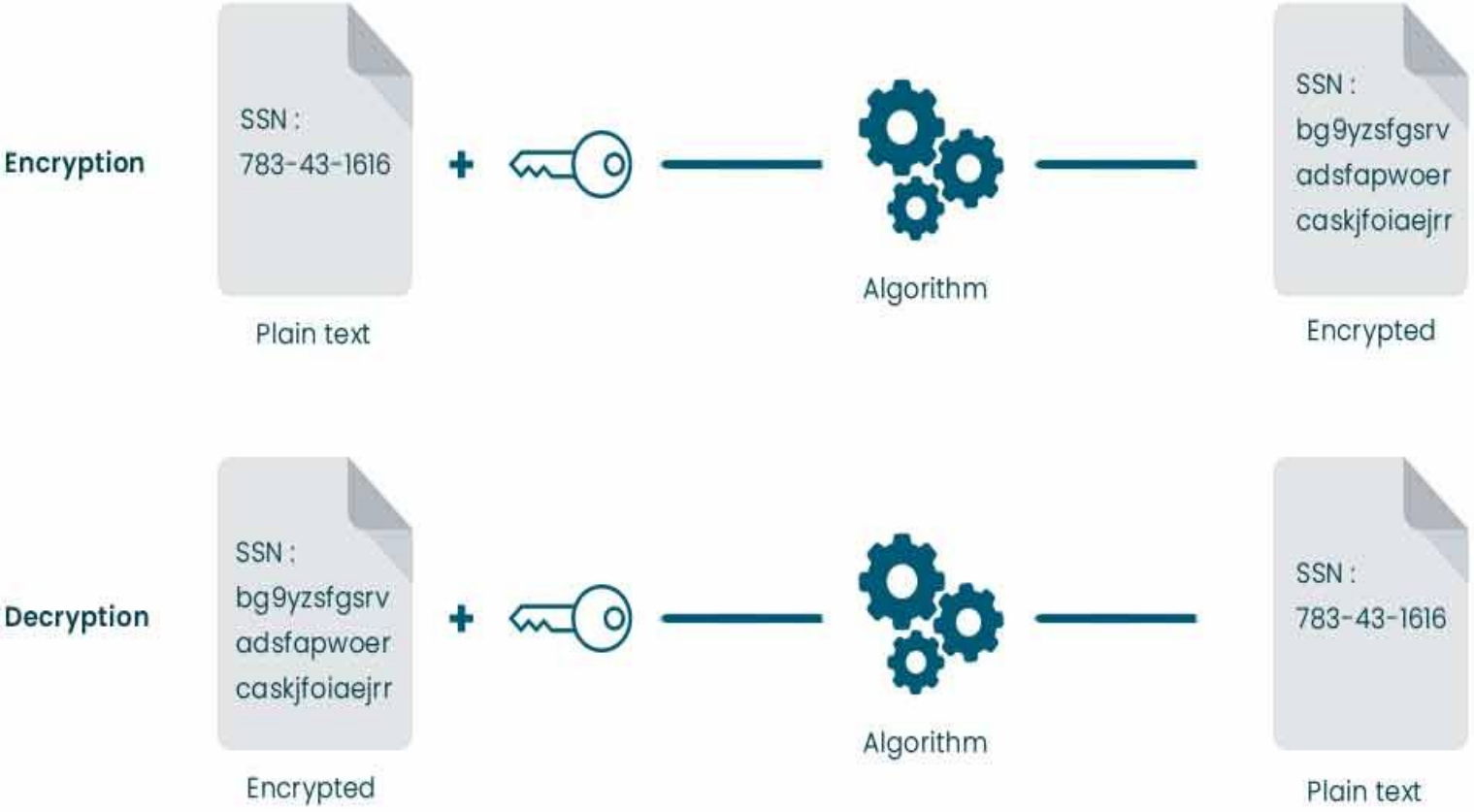
A09-2021: Security Logging and Monitoring Failures

A02-2021: Cryptographic Failures



Cryptography Terms

Encryption & Decryption



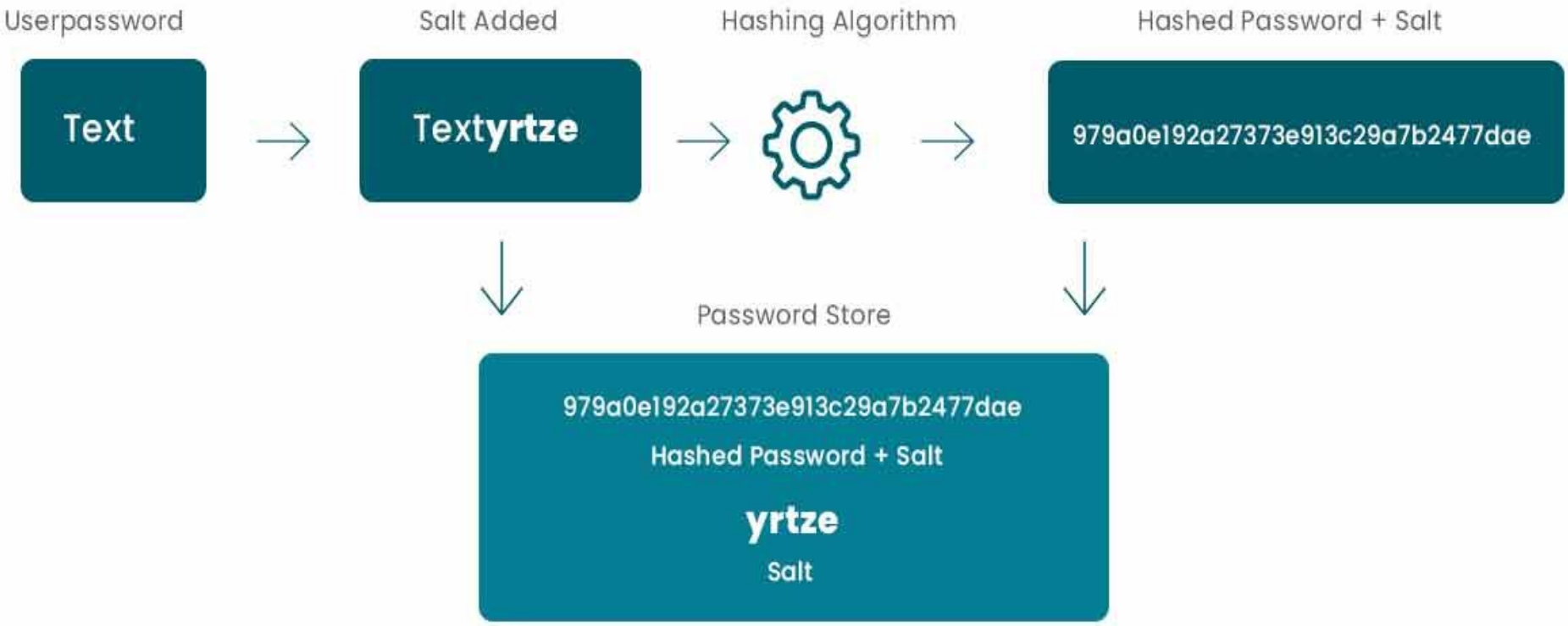
Hashing

Plain Text

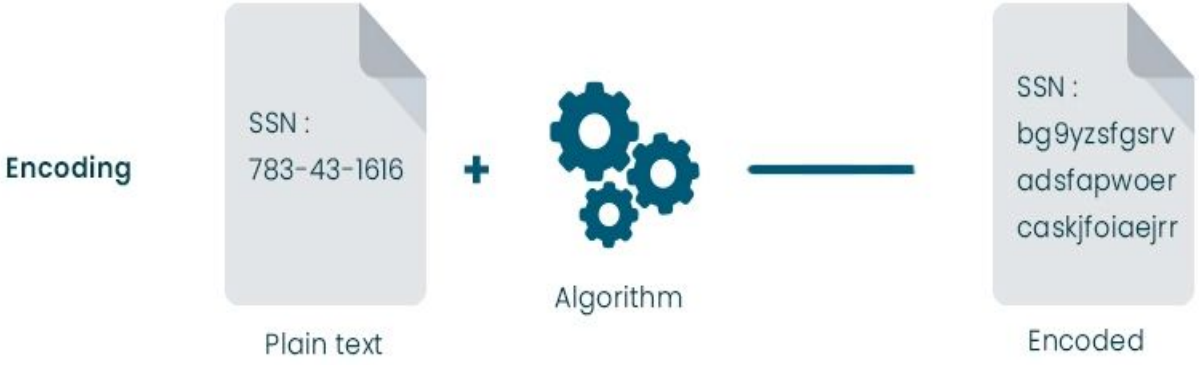
Hash Function

Hashed Text

Salting


Userpassword
Text
Salt Added
Textyrtze
Hashing Algorithm
Hashed Password + Salt
979a0e192a27373e913c29a7b2477dae
Password Store
979a0e192a27373e913c29a7b2477dae
Hashed Password + Salt
yrtze
Salt

Encoding


Encoding
SSN :
783-43-1616
Plain text
Algorithm
SSN :
bg9yzsfgsrv
adsfapwoer
caskjfoiaejrr
Encoded
Decoding
SSN :
bg9yzsfgsrv
adsfapwoer
caskjfoiaejrr
Encoded
Same Algorithm
SSN :
783-43-1616
Plain text