Glossary

Cybersecurity

Terms and definitions from Course 8

B

Business continuity plan: A document that outlines the procedures to sustain business operations during and after a significant disruption

C

Confidential data: Data that often has limits on the number of people who have access to it

D

Data controller: A person that determines the procedure and purpose for processing data

Data processor: A person that is responsible for processing data on behalf of the data controller

Data protection officer (DPO): An individual that is responsible for monitoring the compliance of an organization's data protection procedures

E

Elevator pitch: A brief summary of your experience, skills, and background

Escalation policy: A set of actions that outlines who should be notified when an incident alert occurs and how that incident should be handled

I

Improper usage: An incident type that occurs when an employee of an organization violates the organization's acceptable use policies

Incident escalation: The process of identifying a potential security incident, triaging it, and handing it off to a more experienced team member

M

Malware infection: An incident type that occurs when malicious software designed to disrupt a system infiltrates an organization's computers or network

O

OWASP Top 10: A globally recognized standard awareness document that lists the top 10 most critical security risks to web applications

P

Private data: Information that should be kept from the public

Public data: Data that is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others

R

Rapport: A friendly relationship in which the people involved understand each other's ideas and communicate well with each other

S

Security mindset: The ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, an application, or data

Sensitive data: A type of data that includes personally identifiable information (PII), sensitive personally identifiable information (SPII), or protected health information (PHI)

Stakeholder: An individual or a group that has an interest in any decision or activity of an organization

STAR method: An interview technique used to answer behavioral and situational questions

U

Unauthorized access: An incident type that occurs when an individual gains digital or physical access to a system or an application without permission

V

Visual dashboard: A way of displaying various types of data quickly in one place

---