Glossary

Cybersecurity

Terms and definitions from Course 8

A

AI bias: Risks involved when bias is present in artificial intelligence (AI) data, potentially leading to inaccurate, unfair, or unreliable outputs

Artificial intelligence (AI): Computer programs designed to perform cognitive tasks typically associated with human intelligence, such as learning, problem-solving, and understanding language

B

Business continuity plan (BCP): 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

Context (in prompting): The necessary details provided to an artificial intelligence (AI) tool to help it understand what you need from 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

Disaster recovery plan: A plan that allows an organization's security team to outline the steps needed to minimize the impact of a security incident

E

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

Evaluate (in prompting): The step in the TCREI framework where you review the output from an artificial intelligence (AI) tool to determine if it meets your needs and expectations

G

Generative AI (Gen AI): A type of artificial intelligence (AI) that is capable of creating new content, such as text, images, code, or other media, in response to prompts

H

Human-in-the-loop approach: A method of using artificial intelligence (AI) responsibly that combines the strengths of machine intelligence with human oversight, involvement, and validation to train, use, verify, and refine AI results

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

Iterate (in prompting): The process in the TCREI framework of refining and improving artificial intelligence (AI) prompts and outputs through repeated cycles of testing and adjustments to achieve desired results

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

Prompt: The input (which can be text, images, or other data) you provide to an artificial intelligence (AI) model to elicit a specific response or generate new content

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

References (in prompting): Examples or specific information provided to an artificial intelligence (AI) tool to use as a guide when creating its output

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: A storytelling framework that helps you communicate your experiences and skills in a clear, concise, and compelling way to help an interviewer understand exactly how you successfully managed certain situations; stands for Situation, Task, Action, and Result; you'll learn more about this method in the last course of the certificate

T

Task (in prompting): The specific instruction or goal you give to an artificial intelligence (AI) model, often including details about the desired persona and format for the output

TCREI framework: A practical framework for writing effective prompts for generative artificial intelligence (AI) tools, which stands for Task, Context, References, Evaluate, and Iterate

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

---