**Termos e definições do Curso 1**

**A**

**Adversarial artificial intelligence (AI): Técnica que manipula inteligência artificial (IA) e tecnologia de aprendizado de máquina (ML) para realizar ataques de forma mais eficiente.**

**Antivirus software: Programa de software usado para prevenir, detectar e eliminar malware e vírus.**

**Asset: Item percebido como tendo valor para uma organização.**

**Authentication: Processo de verificar quem é alguém.**

**Availability: A ideia de que os dados estão acessíveis para aqueles autorizados a acessá-los.**

**B**

**Business Email Compromise (BEC): Tipo de ataque de phishing onde um invasor se passa por uma fonte conhecida para obter vantagem financeira.**

**C**

**Computer virus: Código malicioso criado para interferir em operações de computador e causar danos a dados e software.**

**Confidentiality: Apenas usuários autorizados podem acessar ativos ou dados específicos.**

**Confidentiality, integrity, availability (CIA) triad: Modelo que ajuda organizações a considerar riscos ao configurar sistemas e políticas de segurança.**

**Cryptographic attack: Ataque que afeta formas seguras de comunicação entre um remetente e o destinatário pretendido.**

**Cybersecurity (ou security): Prática de garantir a confidencialidade, integridade e disponibilidade da informação, protegendo redes, dispositivos, pessoas e dados contra acessos não autorizados ou exploração criminosa.**

**D**

**Database: Coleção organizada de informações ou dados.**

**Data point: Um pedaço específico de informação.**

**H**

**Hacker: Qualquer pessoa ou grupo que usa computadores para obter acesso não autorizado a dados.**

**Hacktivist: Pessoa que utiliza hacking para alcançar um objetivo político.**

**Health Insurance Portability and Accountability Act (HIPAA): Lei federal dos EUA criada para proteger informações de saúde dos pacientes.**

**I**

**Integrity: Ideia de que os dados são corretos, autênticos e confiáveis.**

**Internal threat: Funcionário atual ou antigo, fornecedor externo ou parceiro confiável que representa um risco de segurança.**

**Intrusion detection system (IDS): Aplicativo que monitora atividades do sistema e alerta sobre possíveis intrusões.**

**L**

**Linux: Sistema operacional de código aberto.**

**Log: Registro de eventos que ocorrem nos sistemas de uma organização.**

**M**

**Malware: Software projetado para prejudicar dispositivos ou redes.**

**N**

**National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF): Estrutura voluntária composta por padrões, diretrizes e melhores práticas para gerenciar riscos de segurança cibernética.**

**Network protocol analyzer (packet sniffer): Ferramenta projetada para capturar e analisar o tráfego de dados em uma rede.**

**Network security: Prática de manter a infraestrutura de rede de uma organização segura contra acessos não autorizados.**

**O**

**Open Web Application Security Project (OWASP): Organização sem fins lucrativos focada em melhorar a segurança de software.**

**Order of volatility: Sequência que define a ordem dos dados que devem ser preservados do primeiro ao último.**

**P**

**Password attack: Tentativa de acessar dispositivos, sistemas, redes ou dados protegidos por senha.**

**Personally identifiable information (PII): Qualquer informação usada para inferir a identidade de um indivíduo.**

**Phishing: Uso de comunicações digitais para enganar pessoas e obter dados sensíveis ou implantar software malicioso.**

**Physical attack: Incidente de segurança que afeta não apenas ambientes digitais, mas também físicos.**

**Physical social engineering: Ataque em que um invasor se passa por funcionário, cliente ou fornecedor para obter acesso não autorizado a um local físico.**

**Privacy protection: Ato de proteger informações pessoais contra uso não autorizado.**

**Programming: Processo usado para criar um conjunto específico de instruções para um computador executar tarefas.**

**Protected health information (PHI): Informações relacionadas à saúde física ou mental de um indivíduo no passado, presente ou futuro.**

**Protecting and preserving evidence: Processo de lidar adequadamente com evidências digitais frágeis e voláteis.**

**S**

**Security architecture: Design de segurança composto por múltiplos componentes, como ferramentas e processos, para proteger uma organização contra riscos e ameaças externas.**

**Security controls: Medidas de proteção projetadas para reduzir riscos específicos de segurança.**

**Security ethics: Diretrizes para tomar decisões adequadas como profissional de segurança.**

**Security frameworks: Diretrizes usadas para criar planos que ajudem a mitigar riscos e ameaças a dados e privacidade.**

**Security governance: Práticas que ajudam a apoiar, definir e direcionar os esforços de segurança de uma organização.**

**Security information and event management (SIEM): Aplicação que coleta e analisa dados de logs para monitorar atividades críticas em uma organização.**

**Sensitive personally identifiable information (SPII): Tipo específico de PII sujeito a diretrizes de manuseio mais rigorosas.**

**Social engineering: Técnica de manipulação que explora erros humanos para obter informações privadas, acesso ou valores.**

**Social media phishing: Ataque em que o invasor coleta informações detalhadas sobre o alvo em redes sociais antes de iniciar o ataque.**

**Spear phishing: Ataque de e-mail malicioso direcionado a um usuário ou grupo específico, parecendo originar-se de uma fonte confiável.**

**SQL (Structured Query Language): Linguagem de programação usada para criar, interagir e solicitar informações de um banco de dados.**

**Supply-chain attack: Ataque que visa sistemas, aplicações, hardware e/ou software para localizar vulnerabilidades onde malware pode ser implantado.**

**T**

**Technical skills: Habilidades que exigem conhecimento de ferramentas, procedimentos e políticas específicos.**

**Threat: Qualquer circunstância ou evento que possa impactar negativamente os ativos.**

**Threat actor: Qualquer pessoa ou grupo que apresenta um risco de segurança.**

**Transferable skills: Habilidades de outras áreas que podem ser aplicadas a diferentes carreiras.**

**U**

**USB baiting: Ataque em que um invasor estrategicamente deixa um pendrive com malware para que um funcionário o encontre e o insira, infectando uma rede.**

**V**

**Virus: Ver "computer virus".**

**Vishing: Exploração de comunicação por voz eletrônica para obter informações sensíveis ou se passar por uma fonte conhecida.**

**W**

**Watering hole attack: Ataque em que um invasor compromete um site frequentemente visitado por um grupo específico de usuários.**