Curso 1 de 8 - Fundamentos da Segurança Cibernética

Módulo 1

Introdução à segurança cibernética:

O principal objetivo na segurança da informação é proteger organizações e pessoas, permitindo o apoio e a interação com pessoas de todo o mundo.

- **O que profissionais de segurança REALMENTE fazem?**

Os analistas de segurança ajudam a minimizar os riscos para organizações e pessoas, trabalhando para se proteger proativamente contra incidentes enquanto, ao mesmo tempo, monitoram os sistemas e as redes.

Além disso, caso ocorra um incidente, eles investigam e relatam suas descobertas. Estão sempre fazendo perguntas e procurando soluções. O objetivo maior é minimizar os riscos e possíveis danos.

Cybersecurity (Cibersegurança): É a prática de garantir a confidencialidade, a integridade e a disponibilidade da informação protegendo redes, dispositivos, pessoas e dados de acessos não autorizados ou explorações criminosas

Threat actor (Agente de ameaça): Qualquer pessoa ou grupo que apresenta um risco à segurança.

Benefícios da segurança:

- Protege contra ameaças externas (alguém de fora da organização) e internas (funcionários ou ex funcionários)
- Garantir que a organização atenda à conformidade regulatória e as leis e diretrizes que especificam a implementação de padrões de segurança.
- Mantêm e melhoram a produtividade dos negócios
- Reduzir custos (como a perda de dados ou inatividade de serviços)
- Manter a confiança da marca

Cargos de segurança (após finalizar o certificado):

- Analista ou especialista de segurança
- Analista ou especialista de cibersegurança
- Analista de centro de operações (SOC)
- Analista de segurança de informações

- **Responsabilidades de um analista de segurança iniciante:**

Os analistas de segurança são responsáveis por monitorar e proteger as informações e os sistemas.

Responsabilidades de um analista de segurança:

- Proteção de computadores e sistemas de rede
- Instalar softwares de prevenção para identificar riscos e vulnerabilidades
- Realizar auditorias de segurança periódicas

Terminologias importantes:

- **Conformidade:** É o processo de adesão a regulamentações de segurança internas que permite que as organizações evitem muitas violações de segurança

- **Frameworks de segurança:** Diretrizes usadas para criar planos que ajudem a reduzir os riscos e as ameaças aos dados e à privacidade dos dados

- **A postura de segurança:** é a capacidade da organização de gerenciar a defesa de recursos e dados críticos e reagir a mudanças. Uma postura de segurança forte leva a um risco menor para a organização.

- **Segurança de rede:** é a prática de manter a infraestrutura de rede de uma organização protegida contra acesso não autorizado. Isso inclui dados, serviços, sistemas e dispositivos armazenados na rede de computadores de uma organização.

- **Segurança na nuvem:** A Segurança na nuvem é um subcampo crescente da segurança cibernética que se concentra especificamente na proteção de dados, aplicativos e infraestrutura na nuvem.

- **Programação:** É um processamento que permite criar um conjunto de instruções de computador para realizar tarefas de automação, análise de tráfego e alerta de atividades suspeitas.

Habilidades essenciais para profissionais de segurança da informação:

Transferable skills (Habilidades transferíveis): São habilidades de outras áreas que podem ser aplicadas a diferentes carreiras.

Technical Skills (Habilidades técnicas): São habilidades que requerem conhecimento de ferramentas, procedimentos e políticas específicas (podem ser usadas em outras áreas também).

Security analyst transferable skills:

- Comunicação
- Colaboração
- Análise
- Solução de problemas

Security analyst technical skills:

- Programação
- Ferramentas de gerenciamento de eventos e informações de segurança (SIEM)
- Computação forense

Personally identifiable information PII (Informações de identificação pessoal): Qualquer informação usada para inferir a identidade de um indivíduo, incluindo o nome completo, data de nascimento, endereço físico, número de telefone, endereço de e-mail, protocolo de internet ou endereço ip.

Sensitive Personally identifiable information SPII (Informações de identificação pessoal confidenciais): Tipo específico de PII que se enquadra em diretrizes de manuseio mais rígidas, incluindo número de previdência social, informações médicas ou informações financeiras e dados biométricos, como reconhecimento facial e biometria.

Durante um ataque ou vazamento, o PII e o SPII são os dados que serão prioritariamente procurados pelos agentes de ameaça com o intuito de realizar o roubo de identidade (ato de roubar informações pessoais para cometer fraude enquanto se faz passar por vítima), tendo como objetivo principal o **ganho financeiro.**

Principais habilidades que um analista de segurança deve ter para ajudar a manter a organização segura:

- **Pensamento Analítico:** Analistas usam do pensamento analítico quando monitoram redes de computador para responder a ataques em potencial, definindo privilégios e determinando maneiras de gerenciar os riscos.
- **Colaboração:** Analistas trabalham com stakeholders e outros membros do time para solucionar problemas e bloquear acessos não autorizados.
- **Prevenção de Malware:** Um analista deve instalar softwares de prevenção, que são sistemas que trabalham proativamente para prevenir ameaças de acontecerem.
- **Comunicação:** Ao encontrar riscos, ameaças ou vulnerabilidades, os analistas devem documentar e reportar os seus achados. O documento deve conter detalhes sobre as tentativas de tornar o sistema seguro, testes de pontos fracos ou oferecer soluções para a melhoria do sistema. Ao reportar achados, uma comunicação assertiva é essencial.
- **Entender linguagens de programação:** Analistas podem trabalhar com times de desenvolvimento de software para melhorar a segurança, instalar softwares e realizar processos. É vantajoso para o analista que ele entenda de programação.
- **Usar ferramentas SIEM:** Quando um analista precisa procurar por vulnerabilidades, ele conduz uma auditoria periódica de segurança, a qual se trata de uma revisão a respeito dos documentos e atividades da organização. As ferramentas SIEM ajudam os analistas a entender ameaças de segurança, riscos e vulnerabilidades nessas ocasiões.

Glossário de revisão:

- **Segurança cibernética (ou segurança):** A prática de garantir a confidencialidade, a integridade e a disponibilidade das informações, protegendo redes, dispositivos, pessoas e dados contra o acesso não autorizado ou a exploração criminosa

- **Segurança na nuvem:** O processamento para garantir que os recursos armazenados na Nuvem sejam configurados adequadamente e que o acesso a esses recursos seja limitado a usuários autorizados
- **Ameaça interna:** Um funcionário ou ex-funcionário, um fornecedor externo ou um parceiro confiável que represente um Risco à segurança
- **Segurança de rede:** A prática de manter a infraestrutura de rede de uma organização protegida contra acesso não autorizado
- **Informações de identificação pessoal (PII):** Qualquer informação usada para inferir a identidade de um indivíduo
- **Postura de segurança:** A capacidade de uma organização de gerenciar sua defesa de recursos e dados críticos e reagir a mudanças
- **Informações sensíveis de identificação pessoal (SPII):** Um tipo específico de PII que se enquadra em diretrizes de manuseio mais rigorosas
- **Habilidades técnicas:** Habilidades que exigem conhecimento de ferramentas, procedimentos e políticas específicas.
- **Ameaça:** Qualquer circunstância ou evento que possa afetar negativamente os recursos
- **Ator da ameaça:** Qualquer pessoa ou grupo que apresente um Risco à segurança
- **Habilidades transferíveis:** Habilidades de outras áreas que podem ser aplicadas a diferentes carreiras

Módulo 2

A evolução da Segurança Cibernética

Uma das razões pelas quais hoje há tantos empregos na área de segurança é por causa dos ataques que aconteceram nos anos 80 e 90. Décadas depois (hoje em dia) os profissionais de segurança trabalham para proteger organizações e pessoas das variantes atuais desses ataques.

Terminologias importantes:

- **Computer virus (vírus de computador):** Trata-se de um código malicioso criado para interferir nas operações do computador e causar dano aos dados e ao software.
- **Malware:** Software projetado para danificar dispositivos ou redes.
- **Brain Virus:** Embora tivesse o intuito de rastrear cópias ilegais de softwares médicos e impedir o uso de licenças piratas, o malware infectava o computador e qualquer disco que utilizasse a licença e se espalhava sempre que alguém utilizasse o disco infectado, acabou se espalhando globalmente em alguns meses de forma irrastreável. Não destruia dados ou hardware, mas diminuía a produtividade, impactando significativamente as operações comerciais. Impactou o ramo da segurança ao enfatizar a necessidade de um plano para manter a segurança e a produtividade.
- **Morris Worm:** Em 1988, Robert Morris desenvolveu um software que se espalhava pela rede para avaliar o tamanho da internet. Ele rastreou a web e se instalou em máquinas para contabilizar o número de computadores conectados à internet. No entanto, o vírus falhou em detectar a sua presença em máquinas que já havia infectado, se reinstalando nas mesmas até que ficassem sem memória e travassem. 6.000 computadores foram afetados, representando 10% da internet na época. Depois do Morris Worm, equipes de resposta a emergências de computadores (CERTs) foram estabelecidas para responder a incidentes de segurança.

Ataques na era digital:

Com a expansão e popularização da internet, os agentes de ameaça não precisam mais utilizar discos físicos para injetarem malwares.

- **LoveLetter (ILOVEYOU):** Em 2000, Onel de Guzman criou o malware LoveLetter, que roubava credenciais de login na internet. Os usuários recebiam um email com o assunto “Eu te amo”, contendo um anexo chamado de “Carta de amor”. Quando o anexo foi aberto, o malware escaneou o catálogo de endereços do usuário e enviava o mesmo e-mail para cada uma das pessoas da lista e instalava um programa para coletar informações e senhas de usuários. O LoveLetter infectou 45 milhões de computadores no mundo todo, causando mais de 10 bilhões de dólares em danos. É o primeiro exemplo de engenharia social.
- **Engenharia Social:** É uma técnica de manipulação que explora o erro humano para ganhar acesso a informações privadas, acessos ou objetos de valor.

- **Phishing:** É o uso de comunicações digitais para induzir as pessoas a revelarem dados sensíveis ou instalar softwares maliciosos.
- **Equifax Breach:** Em 2017, hackers conseguiram se infiltrar na agência de relatórios de crédito Equifax, resultando numa das maiores violações de dados conhecida de informações confidenciais. Mais de 143 milhões de registros de clientes foram roubados, afetando cerca de 40% de todos os americanos. Os registros incluíam informações como número de previdência, data de nascimento, carteira de motorista, endereços residenciais e números de cartão de crédito.

Os oito domínios de segurança CISSP

- **Security and Risk Management (Segurança e gerenciamento de riscos):** Se concentra na definição de metas e objetivos de segurança, na redução de riscos, na conformidade, na continuidade dos negócios e na lei. Exemplo: Atualizar as políticas da empresa relacionadas às informações privadas de saúde.
- **Asset Security (Segurança de recursos):** Se concentra na proteção de ativos digitais e físicos, também estando relacionado ao armazenamento, manutenção, retenção e destruição de dados. Exemplo: Garantir que equipamentos antigos sejam descartados e destruídos adequadamente, incluindo qualquer tipo de informação confidencial.
- **Security Architecture and Engineering (Arquitetura e engenharia de segurança):** Se concentra na otimização da segurança de dados, garantindo a implementação de ferramentas, sistemas e processos eficazes. Exemplo: Instalar e configurar um firewall.
- **Communication and Network Security (Comunicação e segurança de rede):** Se concentra no gerenciamento e na proteção de redes físicas e comunicações sem fio. Exemplo: Analisar o comportamento do usuário em sua organização, visando identificar vulnerabilidades ou infrações. Também podendo criar políticas de rede para evitar e reduzir a exposição.
- **Identity and Access Management (Gerenciamento de identidade e acesso):** Se concentra em manter os dados seguros, garantindo que os usuários sigam as políticas estabelecidas para controlar e gerenciar ativos físicos, como espaços de escritório, e ativos lógicos, como aplicativos e redes. Exemplo: Configurar o acesso dos funcionários com cartão-chave aos edifícios.
- **Security Assessment and Testing (Avaliação e teste de segurança):** Se concentra na realização de testes de controle de segurança, coletando e analisando dados e conduzindo auditorias de segurança para monitorar riscos, ameaças e vulnerabilidades. Exemplo: Auditar regularmente as permissões para garantir que nenhuma pessoa não autorizada possa ver o salário dos funcionários.

- **Security Operations (Operações de segurança):** Se concentra na condução de investigações e na implementação de medidas preventivas de segurança. Exemplo: Seguir as diretrizes e os procedimentos da organização para deter um alerta de intrusão na rede.
- **Software Development Security (Segurança do desenvolvimento de software):** Se concentra no uso de práticas de programação seguras, que são um conjunto de diretrizes recomendadas usadas para criar aplicativos e serviços seguros. Exemplo: Aconselhar uma equipe de desenvolvimento de software mobile sobre as políticas de senha ou garantir que todos os dados do usuário sejam protegidos e gerenciados adequadamente.

Tipos de ataque de segurança mais comuns:

- **Quebra de senha:** É uma tentativa de acessar dispositivos, sistemas, redes ou dados protegidos por senha. Algumas formas de fazê-lo são: Força bruta e Tabela arco-íris. Se enquadram no domínio de **comunicação e segurança de rede**.
- **Ataque de engenharia social:** É uma técnica de manipulação que explora o erro humano para obter informações privadas. Algumas formas de ataque são: Phishing, Smishing, Spear phishing, Whaling, Phishing de mídia social, Comprometimento de e-mail comercial, Ataque de watering hole, USB baiting, Engenharia social física. Os ataques estão relacionados ao domínio de **Segurança e Gerenciamento de riscos**.
- **Ataque físico:** É um ataque de segurança que afeta, além dos ambientes digitais, os físicos onde o incidente é implantado. Algumas formas de ataque são: Cabo USB malicioso, Unidade flash maliciosa, Clonagem e desnatação de cartões. Estão relacionados ao domínio de **Segurança de Recursos**.
- **Inteligência Artificial Adversária:** É uma técnica que manipula a inteligência artificial e a tecnologia de machine learning para realizar ataques com mais eficiência. Se enquadra nos domínios de **Comunicação e Segurança de Redes** e **Gerenciamento de Identidade e Acesso**.
- **Ataque à cadeia de suprimentos:** Visa sistemas, aplicativos, hardware e ou software para localizar uma vulnerabilidade em que o malware possa ser implantado. Pode focar no processamento envolvendo terceiros, ou seja, pode acontecer em qualquer ponto da cadeia de suprimentos. Se enquadra em vários domínios, tais como: **Segurança e Gerenciamento de Riscos**, **Arquitetura e Engenharia de Segurança** e **Operações de Segurança**.
- **Ataque Criptográfico:** Afeta formas seguras de comunicação entre um remetente e o destinatário pretendido. Algumas formas de ataque

são: Aniversario, Colisão, Downgrade. Se enquadram no domínio da **Comunicação** e da **Segurança de Rede.**

Tipos de agentes de ameaça:

- **Ameaças persistentes avançadas: APTs** são ameaças que têm experiência significativa no acesso à rede de computadores de uma determinada organização. Tendem a pesquisar seus alvos com antecedência e podem permanecer indetectáveis por um longo período de tempo. Suas intenções ou motivações podem ser: Danificar a infraestrutura essencial, como a rede de poder e os recursos naturais, e obter acesso a propriedade intelectual, como segredos ou patentes.
- **Ameaças internas:** São pessoas que abusam de seu acesso autorizado para obter dados que podem prejudicar uma organização. Suas intenções ou motivações podem ser: Sabotagem, corrupção, espionagem e acesso ou vazamento de dados não autorizados.
- **Hacktivistas:** São agentes de ameaça movidos por uma agenda política. Suas intenções ou motivações podem ser: Manifestações, propaganda, campanhas de mudança social e fama

Tipos de hackers:

Um hacker é qualquer pessoa que usa computadores para obter acesso a sistemas, redes de computadores ou dados.

- **Hackers autorizados:** Também chamados de Hackers Éticos, seguem um código de ética e cumprem a lei para realizar testes para realizar testes de avaliação de risco para empresas.
- **Hackers semi autorizados:** Procuram vulnerabilidades, mas não tiram proveito delas. São considerados pesquisadores.
- **Hackers não autorizados:** Também chamados de crackers ou hackers antiéticos, são agentes de ameaça mal intencionados que não seguem a lei. Tem como objetivo coletar e vender dados para ganho financeiro.

Glossário de revisão:

- **Inteligência Artificial (IA):** Uma técnica que manipula a inteligência artificial (IA) e a tecnologia de aprendizado de máquina (ML) para realizar ataques com mais eficiência

- **Business-to-business Compromise (BEC):** Um tipo de ataque de phishing em que um agente de ameaça se faz passar por uma fonte conhecida para obter vantagem financeira
- **CISSP:** Certified Informações Systems Security Professional é uma certificação de segurança da informação reconhecida mundialmente e muito procurada, concedida pelo International Informações Systems Security Certification Consortium
- **Vírus de computador:** Código malicioso escrito para interferir nas operações do computador e causar danos aos dados e ao software
- **Ataque criptográfico:** Um ataque que afeta formas seguras de comunicação entre um remetente e o destinatário pretendido
- **Hacker:** Qualquer pessoa que usa computadores para obter acesso a sistemas, redes de computadores ou dados
- **Malware:** Software projetado para danificar dispositivos ou redes de computadores
- **Quebra de senha:** Uma tentativa de acessar dispositivos, sistemas, redes ou dados protegidos por senha
- **Phishing:** o uso de comunicações digitais para enganar as pessoas e fazê-las revelar dados confidenciais ou implantar software malicioso
- **Ataque físico:** Um incidente de segurança que afeta não apenas os ambientes digitais, mas também os ambientes físicos onde o incidente é implantado
- **Engenharia social física:** Ataque em que um agente de ameaça se faz passar por funcionário, cliente ou fornecedor para obter acesso não autorizado a um local físico
- **Engenharia social:** Uma técnica de manipulação que explora o erro humano para obter informações privadas, acesso ou valores
- **Phishing de mídia social:** um tipo de ataque em que um agente de ameaças coleta informações detalhadas sobre o alvo em sites de mídia social antes de iniciar o ataque
- **Spear phishing:** ataque de e-mail mal-intencionado direcionado a um usuário específico ou a um grupo de usuários, que parece ter sido originado de uma fonte confiável
- **Ataque à Cadeia de Suprimentos:** Um ataque que visa sistemas, aplicativos, hardware e/ou software para localizar uma vulnerabilidade na qual o malware pode ser implantado
- **USB baiting:** Um ataque em que um agente de ameaças deixa estrategicamente um pendrive com malware para que um funcionário o encontre e instale para infectar uma rede sem saber
- **Vírus:** refere-se a "vírus de computador"
- **Vishing:** exploit de comunicação eletrônica de voz para obter informações confidenciais ou para se passar por uma fonte conhecida

- **Ataque watering hole**: Um tipo de ataque em que um agente de ameaça compromete um site frequentemente visitado por um grupo específico de usuários

Módulo 3

Frameworks e controles

Ao identificar alertas de ameaça, um analista deve começar identificando os ativos e riscos críticos da organização. Após isso, ele deve implementar os frameworks (estruturas) e os controles necessários. Mas como fazer isso?

Security frameworks (Estruturas de segurança): São diretrizes usadas para criar planos para ajudar a mitigar riscos e ameaças aos dados e à privacidade. Fornecem uma abordagem estruturada para implementar um ciclo de vida de segurança.

Ciclo de vida de segurança: É um conjunto de políticas e padrões em constante evolução que define como uma organização gerencia riscos, segue as diretrizes estabelecidas e atende à conformidade regulatória ou às leis.

Propósito das estruturas de segurança:

- Proteger PIIs
- Proteger as informações financeiras
- Identificar falhas de segurança
- Gerenciar riscos organizacionais
- Alinha a segurança às metas do negócio

Componentes principais das estruturas de segurança:

- **Identificar e documentar as metas de segurança.** Exemplo: identificar e documentar áreas em que uma organização não está em conformidade com o GDPR.
- **Definir diretrizes para atingir as metas de segurança.** Exemplo: Desenvolver novas políticas sobre como lidar com solicitações de dados de usuários individuais.
- **Implementação de processos de segurança robustos.** Exemplo: Ajudar a criar procedimentos para garantir que a organização cumpra

as solicitações verificadas de dados do usuário (como excluir os próprios dados ou perfil)

- **Monitorar e comunicar os resultados.** Exemplo: Monitorar a rede interna da organização e relatar um possível problema de segurança que afeta o GDPR ao seu gerente.

Security controls (Controles de segurança): Proteções projetadas para reduzir riscos de segurança específicos. Exemplo: Utilizar uma ferramenta para identificar se os funcionários concluíram os cursos obrigatórios de segurança da empresa ou não.

Frameworks e controles específicos:

- **CIA triad (Tríade CIA):** É um modelo fundamental que ajuda a informar como as organizações consideram os riscos ao configurar sistemas e políticas de segurança. CIA significa **Confidencialidade**, **Integridade** e **Disponibilidade**.

    - **Confidencialidade:** Somente usuários autorizados podem acessar ativos ou dados específicos. Exemplo: Implementação de controles de acesso rígidos que controlam quem tem acesso a o que.
    - **Integridade:** Dados corretos, autênticos e confiáveis. Exemplo: Utilização de criptografia para manter os dados seguros.
    - **Disponibilidade:** Os dados são acessíveis para aqueles que estão autorizados a acessá-los.
    - **Asset (Recurso):** É um item percebido como tendo valor para uma organização.

- **NIST Cybersecurity Framework (CSF):** É um framework voluntário que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos de cibersegurança.

Ética na segurança cibernética

Eticamente, um bom profissional de segurança deve permanecer imparcial e manter a segurança e a confidencialidade. Independente de quem seja o autor da ameaça, é responsabilidade e obrigação do profissional aderir às políticas e protocolos que foi treinado para seguir.

Security ethics (Ética de segurança:): São diretrizes para tomar decisões apropriadas como profissionais de segurança.

Princípios éticos de segurança:

- Confidencialidade
- Proteção de privacidade
- Leis

Questões éticas e legais envolvendo contra-ataques:

- **Estados Unidos:** Nos Estados Unidos é proibido contra-atacar investidas de agentes de ameaças, visto que isso seria considerado vigilantismo, além de ser proibido pela lei de fraude e abuso de computadores de 1986. Presume-se que o contra-ataque pode levar a um maior encaminhamento do ataque, causando mais danos e prejuízos. os únicos indivíduos nos EUA que têm permissão para contra-atacar são funcionários aprovados do governo federal ou militares.
- **Internacional:** A corte internacional de justiça afirma que uma pessoa ou grupo pode contra-atacar se:

    - O contra-ataque afetar apenas a parte que atacou primeiro.
    - O contra-ataque for uma comunicação direta para que o atacante pare.
    - O contra-ataque não aumentar a situação.
    - Os efeitos do contra-ataque puderem ser revertidos.

Glossário de revisão:

- **Recurso:** um item percebido como tendo valor para uma organização
- **Disponibilidade:** A ideia de que os dados são acessíveis àqueles que estão autorizados a acessá-los
- **Conformidade:** O processamento de adesão a padrões internos e reguladores externos
- **Confidencialidade:** A ideia de que somente usuários autorizados podem acessar recursos ou dados específicos
- **Tríade Confiança, integridade e disponibilidade (CIA):** Um modelo que ajuda a informar como as organizações consideram o Risco ao configurar sistemas e políticas de segurança
- **Hacktivista:** Uma pessoa que usa hacking para atingir um objetivo político
- **Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA):** Uma lei federal dos EUA estabelecida para proteger as informações de saúde dos pacientes
- **Integridade:** A ideia de que os dados são corretos, autênticos e confiáveis

- **Framework de segurança cibernética (CSF) do National Institute of Standards and Technology (NIST):** Um framework voluntário que consiste em padrões, diretrizes e práticas recomendadas para gerenciar o risco de segurança cibernética
- **Proteção da privacidade:** O ato de proteger informações pessoais contra o uso não autorizado
- **Informações de saúde protegidas (PHI):** Informações relacionadas à saúde ou condição física ou mental passada, presente ou futura de um indivíduo
- **Arquitetura de segurança:** Um tipo de projeto de segurança composto de vários componentes, como ferramentas e processos, que são usados para proteger uma organização contra riscos e ameaças externas
- **Controles de segurança:** Salvaguardas projetadas para reduzir Riscos de segurança específicos
- **Ética de segurança:** Diretrizes para tomar decisões apropriadas como profissional de segurança
- **Frameworks de segurança:** Diretrizes usadas para criar planos que ajudem a reduzir riscos e ameaças aos dados e à privacidade dos dados
- **Governança da segurança:** Práticas que ajudam a apoiar, definir e direcionar os esforços de segurança de uma organização
- **Informações sensíveis de identificação pessoal (SPII):** Um tipo específico de PII que se enquadra em diretrizes de manuseio mais rigorosas

Módulo 4

Ferramentas importantes de segurança cibernética

Log: É um registro de eventos que ocorrem nos sistemas de uma organização. Exemplo: Registro de funcionários fazendo login em seus computadores ou acessando serviços baseados na web.

Security Information and Event Management (SIEM) tool: É um aplicativo que coleta e analisa dados de log para monitorar atividades críticas em uma organização. Coletam informações em tempo real ou instantâneas e permitem que os analistas de segurança identifiquem possíveis violações à medida que elas acontecem.

Ferramentas SIEM comumente usadas:

- **Splunk:** A Splunk é uma plataforma de análise de dados e a Splunk Enterprise fornece soluções de SIEM. É uma ferramenta

auto-hospedada usada para reter, analisar e pesquisar os dados de log de uma organização.

- **Google Chronicle:** É uma ferramenta SIEM nativa da nuvem que armazena dados de segurança para pesquisa e análise.

Outras ferramentas:

- **Playbooks (manuais):** É um manual que fornece detalhes sobre qualquer ação operacional, por exemplo, como responder a um incidente.
- **Network protocol analysers ou Packet Sniffer (Analisadores de protocolo de rede):** É uma ferramenta projetada para capturar e analisar o tráfego de dados em uma rede. Analisadores de rede comuns incluem o tcpdump e o Wireshark.

Conhecimentos e habilidades essenciais de segurança cibernética

Programming (Programação): Utilizada para criar um conjunto específico de instruções para um computador executar tarefas. Permite que os analistas concluam tarefas e processos repetitivos com um alto grau de precisão e eficiência.

Linux: É um sistema operacional de código aberto ou disponível publicamente. Permite o uso de comandos baseados em texto entre o usuário e o sistema operacional.

SQL ou Structured Query Language (Linguagem de consulta estruturada): É uma linguagem de programação usada para criar, interagir e solicitar informações de um banco de dados.

Database (Banco de dados): É uma coleção organizada de informações ou dados.

Python: Usada para realizar tarefas repetitivas e demoradas que exigem um alto nível de detalhes e precisão.

Glossário de revisão:

- **Software antivírus:** Um software usado para prevenir, detectar e eliminar malware e vírus

- **Banco de dados:** Uma coleção organizada de informações ou dados
- **Dados:** Um pedaço específico de informações
- **Sistema de detecção de intrusão (IDS):** um aplicativo que monitora a atividade do sistema e alerta sobre possíveis intrusões
- **Linux:** Um sistema operacional de código aberto
- **Geração de registros:** Um registro A de eventos que ocorrem nos sistemas de uma organização.
- **Analisador de protocolo de rede (packet sniffer):** Uma ferramenta projetada para capturar e analisar o Tráfego de dados em uma rede
- **Ordem de volatilidade:** Uma sequência que descreve a ordem dos dados que devem ser preservados, do primeiro ao último
- **Programação:** Um processamento que pode ser usado para criar um conjunto específico de instruções para um computador executar tarefas
- **Proteção e preservação de evidências:** O processo de trabalhar adequadamente com evidências digitais frágeis e voláteis
- **Gerenciamento de eventos e informações de segurança (SIEM)**: Um aplicativo que coleta e analisa dados de registros para monitorar atividades críticas em uma organização
- **SQL (Linguagem de consulta estruturada):** Linguagem de consulta usada para criar, interagir e solicitar informações de um banco de dados

FINALIZADO!