Curso 2 de 8 - Gerenciamento de riscos

Módulo 1

Os oito domínios de segurança CISSP

Security posture (Postura de segurança): Se refere à capacidade de uma organização gerenciar sua defesa de ativos e dados críticos e reagir às mudanças.

***Domínio 1* - Security and Risk Management (Segurança e gerenciamento de riscos):** Definição de metas e objetivos de segurança, redução de riscos, conformidade, continuidade de negócios e regulações legais.

- **Definição de metas:** Ao definir as metas e objetivos de segurança, as organizações podem reduzir os riscos a ativos e dados críticos como PII.
- **Redução de riscos:** Significa ter os procedimentos e regras corretas em vigor para reduzir rapidamente o impacto de um risco, como uma violação.
- **Conformidade:** Principal método usado para desenvolver as políticas internas de segurança, os requisitos regulatórios e os padrões independentes de uma organização.
- **Continuidade de negócios:** Está relacionado à capacidade de uma organização de manter a sua produtividade diária ao estabelecer planos de recuperação de riscos e desastres.
- **Regulações legais:** Seguir as regras e expectativas de comportamento ético para minimizar a negligência, o abuso ou a fraude.

***Domínio 2* - Asset Security (Segurança de recursos):** Domínio focado na proteção de ativos digitais e físicos. Também relacionado a armazenamento, manutenção, retenção e destruição de dados. Significa que ativos como PII ou SPII devem ser manuseados e protegidos com segurança, armazenados em um computador, transferidos por uma rede ou coletados fisicamente.

As organizações também devem ter políticas sobre como os dados serão armazenados, mantidos e destruídos adequadamente.

Domínio 3 **- Security Architecture and Engineering (Arquiteturas e Engenharia de segurança):** Domínio focado na otimização da segurança de dados, garantindo a implementação de ferramentas, sistemas e processos eficazes para proteger os ativos e os dados de uma organização.

Um dos principais conceitos da arquitetura de design seguro é a responsabilidade compartilhada.

Shared responsibility (Responsabilidade compartilhada): Significa que todos os indivíduos de uma organização possuem um papel na diminuição de riscos e na manutenção da segurança física e virtual.

Domínio 4 **- Communication and Network Security (Comunicação e segurança de rede):** Domínio que se concentra no gerenciamento e na proteção de redes físicas e comunicações sem fio. Redes seguras mantêm os dados e as comunicações de uma organização seguros.

Exemplo: Funcionários que trabalham remotamente em espaços públicos precisam ser protegidos contra vulnerabilidades que podem ocorrer ao utilizar conexões Bluetooth inseguras ou pontos de acesso Wi-Fi públicos.

Domínio 5 **- IAM Identity and Access Management (Gerenciamento de identidade e acesso):** Domínio focado no acesso e na autorização para manter os dados seguros, garantindo que os usuários sigam as políticas estabelecidas para controlar e gerenciar ativos.

Um analista deve garantir que o acesso de um usuário seja limitado ao que os funcionários precisam, reduzindo o risco geral para sistemas e dados.

Componentes do IAM:

- **Identificação:** É quando o usuário se identifica ao fornecer um nome de usuário, um cartão de acesso ou dados biométricos.
- **Autenticação**: É o processo de verificação para provar a identidade de uma pessoa, como inserir uma senha ou pin.
- **Autorização:** Ocorre após a confirmação da identidade do usuário e está relacionada ao seu nível de acesso, que depende da sua função na organização.
- **Accountability (responsabilidade):** Se refere ao monitoramento e registro das ações do usuário, como tentativa de login.

Domínio 6 **- Security Assessment and Testing (Avaliação e teste de segurança):** Domínio que se concentra na realização de testes de controle de segurança, coleta e análise de dados e a realização de auditorias de segurança para monitorar riscos, ameaças e vulnerabilidades.

Envolve examinar as metas e objetivos organizacionais e avaliar se os controles usados realmente atingem essas metas.

***Domínio 7* - Security Operation (Operações de segurança):** Domínio focado na condução de investigações e na implementação de medidas preventivas de proteção. As investigações começam quando um acidente de segurança é identificado, exigindo um alto senso de urgência para minimizar os riscos potenciais para a organização.

Assim que um ataque é neutralizado, a coleta de evidências digitais e físicas começa para a realização de uma investigação forense. A investigação forense é realizada para identificar *quando*, *como* e *por que* a violação ocorreu.

***Domínio 8* - Software Development Security (Segurança do desenvolvimento de software):** Se concentra no uso de práticas de programação seguras, que são diretrizes recomendadas usadas para criar aplicativos e serviços seguros.

O ciclo de vida de desenvolvimento de software é um processo eficiente usado pelas equipes para criar rapidamente produtos e recursos de software, onde a segurança se torna uma etapa adicional do processo, garantindo que cada fase do ciclo de vida passe por análises de segurança. A segurança também pode ser totalmente integrada ao produto de software, realizando os testes de segurança durante o desenvolvimento de cada etapa.

Ameaças, riscos e vulnerabilidades

Threat (Ameaça): É qualquer circunstância ou evento que pode impactar negativamente os recursos da empresa. Exemplo: Ataque de engenharia social.

Engenharia social: Técnica de manipulação que explora o erro humano para ganhar informações privadas, acesso ou objetos de valor. Exemplo: Phishing.

Risk (Risco): Qualquer coisa que pode impactar a confidencialidade, integridade ou disponibilidade (CIA) de um recurso. É a probabilidade de uma ameaça ocorrer. Exemplo: Falta de protocolos de backup para garantir a recuperação de informações perdidas em ataques.

Os riscos são classificados em diferentes níveis: baixo, médio e alto, dependendo das possíveis ameaças e do valor de um recurso.

- **Low-risk asset (Recurso de baixo risco):** É uma informação que não prejudicaria a reputação e as operações em andamento da empresa e que não causaria dano financeiro se comprometido. Exemplo: Informações públicas (Como dados de site ou pesquisas publicados).
- **Medium-risk asset (Recurso de médio risco):** Informações que não estão disponíveis para o público e que podem causar danos às

finanças, à reputação ou às operações em andamento da organização. Exemplo: Divulgação antecipada dos lucros trimestrais de uma empresa.

- **High asset (Recurso de alto risco):** Informação protegida por regulamentos ou leis na qual, se comprometida, pode trazer impactos negativos severos para às finanças, à reputação e às operações em andamento da organização. Exemplo: Ativos vazados como SPII, PII ou propriedade intelectual.

Vulnerabilidade: Uma fraqueza que pode ser explorada por uma ameaça. Nota-se que uma vulnerabilidade deve estar em conjunto de uma ameaça para que exista um risco. Exemplo: Firewall, software ou aplicativo desatualizados; senhas fracas; ou dados confidenciais desprotegidos.

Ransomware: Ataque malicioso em que os agentes de ameaça criptografam os dados da organização e demandam pagamento para restaurar o acesso. O ataque pode congelar os sistemas de redes, inutilizar os dispositivos e criptografar ou bloquear dados confidenciais.

Camadas da web:

- **Surface web:** Camada que a maioria das pessoas utiliza, contém conteúdo que pode ser acessado usando um navegador web.
- **Deep web:** Geralmente requer autorização para acessá-la, como a intranet de uma organização, pois só pode ser acessado por funcionários ou outras pessoas que tenham acesso concedido.
- **Dark web:** Só pode ser acessada através de um software especial. Geralmente possui uma conotação negativa, pois é a camada preferida dos criminosos devido ao sigilo que fornece.

Três principais impactos de ameaças, riscos e vulnerabilidades:

- **Financeiro:** Interrupção da produção e dos serviços, custo de correção de problemas e multas caso exista comprometimento de ativos devido à não conformidade com leis e regulamentações.
- **Roubo de identidade:** Roubo e venda de PII
- **Dano à reputação:** A exploração de uma vulnerabilidade pode levar clientes a buscarem novos relacionamentos comerciais com concorrentes ou criar má reputação para a organização.

Estrutura de Gerenciamento de Riscos (RMF) do NIST:

- **Preparar:** Se refere a atividades que são necessárias para gerenciar riscos de segurança e privacidade antes que uma violação ocorra.

Etapa utilizada para monitorar riscos e identificar controles que podem ser usados para reduzir riscos.

- **Categorizar:** Usada para desenvolver processos e tarefas de gerenciamento de riscos. Profissionais de segurança usam esses processos e desenvolvem tarefas pensando em como a confidencialidade, integridade e a disponibilidade dos sistemas e das informações podem ser afetados pelo risco.
- **Selecionar:** Significa escolher, personalizar e capturar a documentação dos controles que protegem a organização. Exemplo: Manter um manual atualizado ou ajudar a gerenciar outra documentação que ajude a equipe a resolver problemas com mais eficiência.
- **Implementar:** Implementar planos de segurança e privacidade para a organização.
- **Avaliar:** Determina se as estruturas de controle estabelecidas foram implementadas corretamente. O analista identifica possíveis pontos fracos e determina se as ferramentas, procedimentos, controles e protocolos da organização devem ser alterados.
- **Autorizar:** Ser responsável pelos riscos de segurança e privacidade que podem existir na organização. Envolve a geração de relatórios, o desenvolvimento de planos de ação e o estabelecimento de marcos do projeto que esteja alinhado às metas de segurança.
- **Monitorar:** Estar ciente de como os sistemas estão funcionando. Avaliar e manter as operações técnicas.

Glossário de revisão:

- **Avaliar:** A quinta etapa do NIST RMF, que significa determinar se os Controles estabelecidos estão implementados corretamente
- **Autorizar:** A sexta etapa do RMF do NIST refere-se à contabilização dos riscos de segurança e privacidade que podem existir em uma organização
- **Continuidade dos negócios:** A capacidade de uma organização de manter sua produtividade diária por meio do estabelecimento de planos de recuperação de desastres de risco
- **Categorizar:** A segunda etapa do NIST RMF, que é usada para desenvolver processos e tarefas de Gerenciamento de Riscos
- **Ameaça externa:** Qualquer coisa fora da organização que tenha o potencial de prejudicar os recursos organizacionais
- **Implementar:** A quarta etapa do NIST RMF, que significa implementar planos de segurança e privacidade para uma organização
- **Ameaça interna:** Um funcionário ou ex-funcionário, fornecedor externo ou parceiro de confiança que represente um Risco de segurança

- **Monitorar**: A sétima etapa do NIST RMF significa estar ciente de como os sistemas estão operando
- **Preparar-se:** A primeira etapa do NIST RMF relacionada às atividades necessárias para gerenciar os riscos de segurança e privacidade antes que ocorra uma violação
- **Ransomware:** Um ataque malicioso em que os agentes da ameaça criptografam os dados de uma organização e exigem pagamento para restaurar o acesso
- **Risco:** qualquer coisa que possa afetar a confidencialidade, a integridade ou a disponibilidade de um recurso
- **Redução de riscos:** O processamento de ter os procedimentos e as regras corretos em vigor para reduzir rapidamente o impacto de um risco, como uma violação
- **Postura de segurança:** A capacidade de uma organização de gerenciar sua defesa de recursos e dados críticos e reagir a mudanças
- **SELECT**: A terceira etapa do RMF do NIST significa escolher, personalizar e capturar a documentação dos Controles que protegem uma organização
- **Responsabilidade compartilhada:** A ideia de que todos os indivíduos de uma organização desempenham um papel ativo na redução do Risco e na manutenção da segurança física e virtual
- **Engenharia social:** Uma técnica de manipulação que explora o erro humano para obter Informações privadas, acesso ou valores
- **Vulnerabilidade:** Um ponto fraco que pode ser explorado por uma ameaça

Módulo 2

Frameworks e Controles

Security frameworks (Estruturas de segurança): São diretrizes usadas para construir planos para mitigar riscos e ameaças a dados e à privacidade. As empresas utilizam os frameworks como ponto de partida para criar suas próprias políticas e processos de segurança.

Os frameworks também abrangem o espaço físico, como exigir o uso de cartões ou crachás para adentrar em um determinado local. Também podem ser utilizados para criar planos que aumentem a conscientização dos funcionários e os eduquem sobre como eles podem proteger a organização.

Security controls (Controles de segurança): São proteções projetadas para reduzir riscos de segurança específicos. Existem três tipos principais de controles de segurança:

- **Criptografia:** É o processo de conversão de dados de um formato legível para um formato codificado. Normalmente, a criptografia converte dados de texto simples em texto cifrado. Textos criptografados são mensagens brutas e codificadas que são ilegíveis para humanos e computadores. É usada para manter a confidencialidade de dados confidenciais, como informações de contas de clientes ou números de previdência social.

- **Autenticação:** É o processo de verificar quem é alguém ou alguma coisa. Exemplo: registro em um site com um nome de usuário e senha. Além disso, podem ser usadas formas de autenticação mais avançadas, como a autenticação multifatorial, que pede, além da senha, mais um método de autenticação, como a biometria.

    - **Biometria:** É uma característica física única que pode ser usada para verificar a identidade de uma pessoa. Exemplo: Impressão digital.
    - **Vishing:** É a exploração da comunicação de voz para se obter informações confidenciais ou se passar por uma fonte conhecida.

- **Autorização:** Se refere ao conceito de conceder acesso a recursos específicos dentro de um sistema. É utilizada para verificar se uma pessoa tem permissão para acessar um recurso.

Tríade CIA: Confiança, Integridade e Disponibilidade

Tríade CIA: É um modelo que ajuda a informar como as organizações consideram o risco quando configuram sistemas e políticas de segurança.

- **Confidencialidade:** Apenas usuários autorizados podem acessar ativos ou dados específicos.
- **Integridade:** Os dados devem estar corretos, autênticos e confiáveis.
- **Disponibilidade:** Os dados são acessíveis para aqueles que estão autorizados a acessá-los.

Frameworks do NIST

NIST Cybersecurity Framework (CSF): É um framework voluntário que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos de segurança cibernética. O CSF consiste em cinco funções principais importantes: identificar, proteger, detectar, responder e recuperar.

NIST S.P. 800-53: Um framework NIST unificado para proteger a segurança da informação dos sistemas dentro do governo federal, incluindo os sistemas fornecidas por empresas para o governo.

As 5 funções do NIST CSF:

- **Identificar:** Gerenciamento do risco de segurança cibernética e seu efeito nas pessoas e ativos da organização. Exemplo: monitorar sistemas e dispositivos na rede interna da organização para identificar possíveis problemas de segurança.
- **Proteger:** É a estratégia usada para proteger uma organização através da implementação de políticas, procedimentos, treinamentos e ferramentas que ajudam a mitigar ameaças de segurança cibernética.
- **Detectar:** Identificar potenciais incidentes de segurança e melhorar o monitoramento para aumentar a velocidade e a eficiência das detecções. Exemplo: Analisar a configuração de uma nova ferramenta para verificar se ela está sinalizando risco baixo, médio ou alto e, em seguida, alertar a equipe de segurança.
- **Responder:** Ter certeza de que os procedimentos adequados estão sendo usados para conter, neutralizar e analisar os incidentes de segurança, e implementar melhorias no processo de segurança.
- **Recuperar:** O processo de retornar sistemas afetados de volta às operações normais. Exemplo: restaurar sistemas, dados e ativos, como arquivos financeiros ou legais que foram afetados por um incidente de segurança.

Princípios da OWASP e auditorias de segurança

Open Web Applications Security Project (OWASP) security principles:

- **Minimizar a área da superfície de ataque** (todas as vulnerabilidades potenciais que podem ser exploradas, como vetores de ataque, tais como e-mails de phishing e senhas fracas).
- **O princípio de privilégio mínimo** (Significa garantir que os usuários tenham a menor quantidade de acesso necessária para realizar suas tarefas diárias)
- **Defesa em profundidade** (Significa que a organização deve ter vários controles de segurança que abordem riscos e ameaças de maneiras diferentes, como MFA, firewall e sistemas de detecção de intrusão).
- **Separação de funções** (Significa que ninguém deve ter tantos privilégios que possa usar o sistema de forma indevida)
- **Manter a segurança simples** (Significa evitar soluções de segurança extremamente complicadas, pois podem se tornar incontroláveis)
- **Corrigir os problemas de segurança corretamente** (É importante encontrar a causa raiz rapidamente, corrigir todas as vulnerabilidades e realizar testes para garantir que os reparos foram bem-sucedidos.

Auditoria de segurança: É uma revisão dos controles, das políticas e dos procedimentos de segurança da organização em relação a um conjunto de expectativas.

Auditoria interna: Geralmente conduzida por uma equipe de pessoas que pode incluir o oficial de conformidade da organização, o gerente de segurança e outros membros da equipe.

São usadas para ajudar e melhorar a postura de segurança de uma organização e ajudar as organizações a evitar multas devido à falta de conformidade.

Propósitos das auditorias internas de segurança:

- **Identificar riscos organizacionais**
- **Avaliar controles**
- **Corrigir problemas de conformidade**

Elementos comuns das auditorias internas:

- **Estabelecer o escopo e as metas da auditoria**
  - O escopo se refere aos critérios específicos de uma auditoria interna de segurança, definindo **o que** será avaliado. Exige que

as organizações identifiquem pessoas, ativos, políticas, procedimentos e tecnologias que possam afetar a postura de segurança da organização.
    - As metas são um esboço dos objetivos de segurança da organização, definindo o **porquê** da auditoria e o que se espera alcançar.
- **Conduzir uma avaliação de risco dos ativos da organização**
    - Focada na identificação de possíveis ameaças, riscos e vulnerabilidades. Ajuda as organizações a decidir quais medidas de segurança devem ser implementadas e monitoradas para garantir a segurança dos ativos.
    - Geralmente concluída por gerentes ou outras partes interessadas.
- **Concluir uma avaliação dos controles**
    - Se trata da análise dos ativos de uma organização e, em seguida, avaliar os riscos potenciais para esses ativos para garantir que os controles e processos internos sejam eficazes.
    - Para executar essa tarefa, os analistas podem ser instruídos a classificar os controles nas seguintes categorias: **controles administrativos** (componente humano da cibersegurança, como políticas e procedimentos internos), **controles técnicos** (soluções de hardware e software como sistemas de detecção de instrusão ou criptografia) e **controles físicos** (medidas para impedir o acesso físico a ativos protegidos, como câmeras de vigilância e fechaduras)
- **Avaliar a conformidade**
    - Se trata de determinar se a organização está aderindo ou não aos regulamentos de conformidade necessários (leis que organizações devem seguir para garantir que os dados privados permaneçam seguros).
- **Comunicar os resultados às partes interessadas**
    - Quando a auditoria for finalizada, os resultados e as recomendações precisam ser comunicadas às partes interessadas (stakeholders).
    - **Stakeholder communication:** resume o escopo e as metas da auditorias, lista os riscos existentes e observa a urgência de solução, identifica os regulamentos de conformidade que a organização precisa seguir e fornece recomendações para melhorar a postura de segurança.

Glossário de revisão:

Recurso: um item percebido como tendo valor para uma organização
Vetores de ataque: Os caminhos que os atacantes usam para penetrar nas defesas de segurança
Autenticação: O processamento de verificação de quem é alguém
Autoridade: O conceito de concessão de acesso a recursos específicos em um sistema
Disponibilidade: A ideia de que os dados são acessíveis àqueles que estão autorizados a acessá-los
Biometria: As características físicas únicas que podem ser usadas para verificar a identidade de uma pessoa
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
Detectar: Função essencial do NIST relacionada à identificação de possíveis incidentes de segurança e à melhoria dos recursos de monitoramento para aumentar a velocidade e a eficiência das detecções
Criptografia: O processo de conversão de dados de um formato legível em um formato codificado
Identificar: Uma função essencial do NIST relacionada ao Gerenciamento de riscos de segurança cibernética e seu efeito sobre as pessoas e os recursos de uma organização.
Integridade: A ideia de que os dados são corretos, autênticos e confiáveis
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): Um framework voluntário que consiste em padrões, diretrizes e práticas recomendadas para gerenciar o risco de segurança cibernética
Publicação Especial (S.P.) 800-53 do National Institute of Standards and Technology (NIST): um framework unificado para proteger a segurança dos sistemas de informação dentro do governo federal dos EUA
Open Web Application Security Projeto/Open Worldwide Application Security Projeto (OWASP): Uma organização sem fins lucrativos voltada para a melhoria da segurança de software
Protect (Proteger): Uma função essencial do NIST usada para proteger uma organização por meio da implementação de políticas, procedimentos, Treinamento e Ferramentas que ajudam a mitigar as ameaças à segurança cibernética
Recuperar: Uma função essencial do NIST relacionada ao retorno dos sistemas afetados à operação normal
Responder: Uma função essencial do NIST relacionada à garantia de que os procedimentos adequados sejam usados para contenção, neutralização e análise de

incidentes de segurança e implementação de melhorias no processamento de segurança
Risco: qualquer coisa que possa afetar a confidencialidade, a integridade ou a disponibilidade de um recurso
Auditoria de segurança: Uma revisão dos controles, políticas e procedimentos de segurança de uma organização em relação a um conjunto de expectativas
Controles de segurança: Salvaguardas projetadas para reduzir Riscos de segurança específicos
Frameworks de segurança: Diretrizes usadas para criar planos que ajudem a reduzir riscos e ameaças aos dados e à privacidade dos dados
Postura de segurança: A capacidade de uma organização de gerenciar sua defesa de recursos e dados críticos e reagir a mudanças
Ameaça: Qualquer circunstância ou evento que possa afetar negativamente os recursos

Módulo 3

Painéis de gerenciamento de eventos e informações de segurança (SIEM)

Log: É um registro de eventos que ocorrem nos sistemas e redes de uma organização.

Fontes de log:

- **Registros do firewall:** É um registro de conexões tentadas ou estabelecidas para o tráfego de entrada da internet. Também inclui solicitações de saída para a internet de dentro da rede.
- **Registros de rede:** É um registro de todos os computadores e dispositivos que entram e saem da rede. Também registra conexões entre dispositivos e serviços na rede
- **Registros do servidor:** É um registro de eventos relacionados a serviços como sites, e-mails ou arquivos compartilhados. Também inclui ações como solicitações de login, senha e nome de usuário.

Ferramenta de gerenciamento de eventos e informações de segurança (SIEM): É um aplicativo que coleta e analisa dados de log (registro) para monitorar atividades críticas em uma organização. Fornece visibilidade em tempo real, monitoramento e análise de eventos e alertas automatizados. Também armazena todos os dados de log em um local centralizado.

Métricas: São atributos técnicos fundamentais, como tempo de resposta, disponibilidade e taxa de falhas, que são usados para avaliar o desempenho de um aplicativo de software. Os painéis SIEM podem ser personalizados para exibir métricas específicas ou outros dados relevantes para diferentes membros de uma organização.

Exemplo: Um analista de segurança pode criar um painel que exibe métricas para monitorar as operações comerciais diárias, como o volume de tráfego de entrada e saída da rede.

Ferramentas de gerenciamento de eventos e informações de segurança (SIEM)

Tipos de ferramentas SIEM:

- **Auto-hospedadas:** Exigem que as organizações instalem, operem e mantenham a ferramenta usando sua própria infraestrutura física, como a capacidade do servidor. São ideais para organizações que precisam manter o controle físico sobre dados confidenciais.
- **Hospedadas em nuvem:** São mantidas e gerenciadas pelos pelos provedores do SIEM, tornando-as acessíveis pela internet. Ideais para organizações que não querem investir na criação e manutenção de sua própria infraestrutura.
- **Híbrida:** Mistura entre ferramentas auto-hospedadas e em nuvem, as organizações podem escolher essa solução para aproveitar os benefícios da nuvem e, ao mesmo tempo, manter o controle físico sobre os dados confidenciais.

Ferramentas:

- **Splunk:** Splunk é uma plataforma de análise de dados.
- **Splunk Enterprise:** É uma ferramenta auto-hospedada usada para reter, analisar e pesquisar os dados de logs de uma organização para providenciar informações e alertas de segurança em tempo real.
- **Splunk Cloud:** É uma ferramenta hospedada em nuvem usada para coletar, pesquisar e monitorar dados de registro. Útil para organizações que executam ambientes híbridos ou somente em nuvem, onde alguns ou todos os serviços da organização estão na nuvem.
- **Google Chronicle:** Ferramenta nativa da nuvem projetada para reter, analisar e pesquisar dados. Fornece monitoramento de logs, análise de dados e coleta de dados.

Glossário de revisão:

Crônica: Uma ferramenta nativa da nuvem projetada para reter, analisar e pesquisar dados
Resposta a incidentes: A tentativa rápida de uma organização de identificar um ataque, contenção dos danos e correção dos efeitos de uma violação de segurança
Geração de registros: Um registro A de eventos que ocorrem nos sistemas de uma organização
Métricas: Atributos técnicos chave, como tempo de resposta, disponibilidade e taxa de falha, que são usados para avaliar o desempenho de um software de aplicativo
Sistema operacional (SO): A interface entre o hardware do computador e o usuário
Playbook: Um manual que fornece detalhes sobre qualquer ação operacional
Gerenciamento de eventos e informações de segurança (SIEM): Um aplicativo que coleta e analisa dados de registros para monitorar atividades críticas em uma organização
Security orchestration, automation, and response (SOAR) (Orquestração, automação e resposta de segurança): Um conjunto de aplicativos, ferramentas e fluxos de trabalho que usam a automação para responder a eventos de segurança
Ferramentas SIEM: Uma plataforma de software que coleta, analisa e correlaciona dados de segurança de várias fontes em toda a infraestrutura de TI, o que ajuda a identificar e responder a ameaças à segurança em tempo real, investigar incidentes de segurança e cumprir os Reguladores de segurança
Nuvem Splunk: Uma ferramenta hospedada na Nuvem usada para coletar, pesquisar e monitorar dados de registro
Splunk Enterprise: Uma ferramenta auto-hospedada usada para reter, analisar e pesquisar os dados de registro de uma organização para fornecer informações e alertas de segurança em tempo real

Módulo 4

Fases dos manuais de resposta a incidentes

Playbook (Manual): É um manual que fornece detalhes sobre ação operacional. Também esclarece quais ferramentas devem ser usadas em resposta a um incidente de segurança.

Os manuais garantem que as pessoas sigam uma lista consistente de ações de uma forma prescritiva, independente de quem esteja trabalhando no caso.

Resposta a incidentes: É a tentativa rápida de uma organização de identificar um ataque, conter os danos e corrigir os efeitos da quebra de segurança.

Fases do manual de resposta a incidentes:

- **Preparação:** As organizações devem se preparar para incidentes de segurança ao documentar procedimentos, estabelecer planos de pessoal e educar os usuários. Estabelece a base para uma resposta bem-sucedida a incidentes. Exemplo: A organização pode criar planos e procedimentos de resposta a incidentes que descrevem as funções e responsabilidades de cada membro da equipe de segurança.
- **Detecção e análise:** O objetivo é detectar e analisar eventos usando processos e tecnologias definidos. A utilização de ferramentas e estratégias ajuda os analistas de segurança a determinar se uma violação ocorreu e a analisar sua possível magnitude.
- **Contenção:** O objetivo é evitar maiores danos e reduzir o impacto imediato de um incidente de segurança. Durante essa fase, os profissionais de segurança tomam medidas para conter um incidente e minimizar os danos.
- **Erradicação e recuperação:** Envolve a remoção completa dos artefatos de um incidente para que a organização possa retornar às operações normais. Durante essa fase, os profissionais de segurança eliminam os artefatos do incidente removendo códigos maliciosos e mitigando vulnerabilidades. Após isso, podem começar as operações de retorno dos serviços, fase conhecida como restauração de TI.
- **Atividade pós-incidente:** Inclui documentar o incidente, informar a liderança organizacional e aplicar as lições aprendidas para garantir que a organização esteja melhor preparada para lidar com futuros incidentes.
- **Coordenação:** Envolve relatar incidentes e compartilhar informações em todo o processo de resposta a incidentes, com base nos padrões estabelecidos pela organização. Garante que as organizações atendam aos requisitos de conformidade e permite uma resposta e resolução coordenadas.

Explorar a resposta a incidentes

Um manual de resposta a incidentes é um guia que ajuda os profissionais de segurança a mitigar problemas com um maior senso de urgência, mantendo a precisão.

Os manuais criam estrutura, garantem a conformidade e descrevem o processo de comunicação e documentação. Como utilizar o manual a partir de um alerta de uma ferramenta SIEM?

Avaliar o alerta: Significa determinar se o alerta é realmente válido, identificando por que o alerta foi gerado pelo SIEM. Pode ser feito analisando os dados de log e métricas relacionadas.

Ações e ferramentas: O manual instrui o analista sobre quais ações e ferramentas deve utilizar em determinadas situações.

Como eliminar os vestígios: Após solucionar o problema, o manual fornece maneiras de eliminar os vestígios do incidente e restaurar as operações normais dos sistemas afetados.

Realizar atividades pós-incidente: Após solucionar o problema e eliminar os vestígios, o manual sugere que o analista realize várias atividades pós-incidente e esforços de coordenação com a equipe de segurança. Algumas atividades incluem: criação de um relatório final para comunicar o incidente de segurança às partes interessadas ou relatar o incidente às autoridades competentes.

Glossário de revisão

Resposta a incidentes: A tentativa rápida de uma organização de identificar um ataque, contenção dos danos e correção dos efeitos de uma violação de segurança
Playbook: Um manual que fornece detalhes sobre qualquer ação operacional

FINALIZADO!