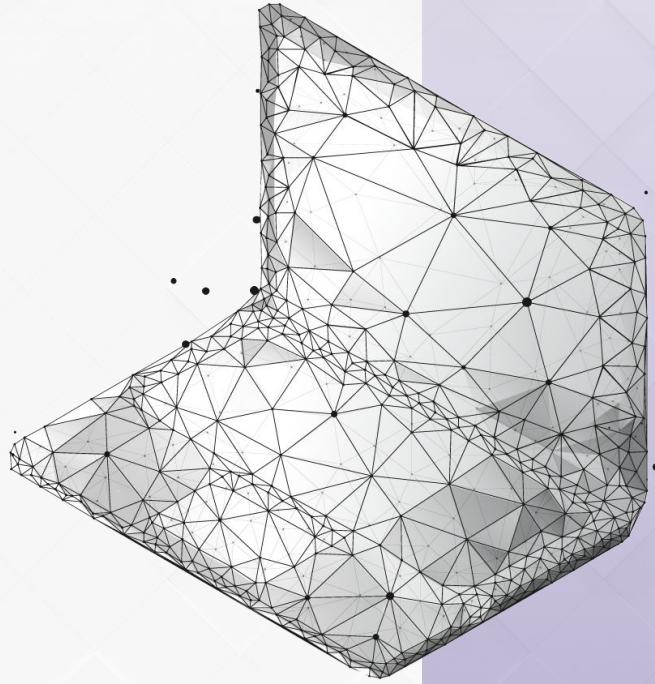


Parte 6



Segurança, Privacidade e Compliance





Overview

Capacitar os analistas a entender como empresas de tecnologia abordam a segurança, a privacidade e a conformidade regulatória. Eles aprenderão a avaliar a eficácia das estratégias de segurança, identificar possíveis vulnerabilidades e reconhecer riscos que podem comprometer o crescimento da startup.





Revisitando a última aula



Colocar a nota e principais feedbacks das últimas aulas



Retificar e esclarecer informações da última aula

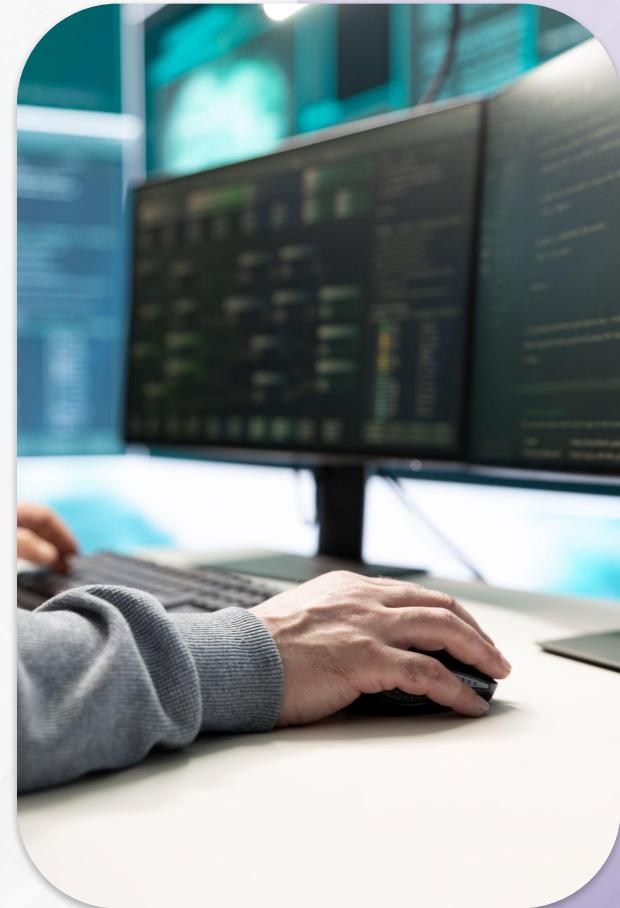
O que é Cybersegurança e tipos de Cyberataques mais comuns

Cybersegurança refere-se ao conjunto de práticas, tecnologias e processos destinados a proteger sistemas, redes e dados contra ataques digitais.

Um cyberataque é uma tentativa maliciosa de comprometer a confidencialidade, integridade ou disponibilidade de sistemas de informação, geralmente executada por hackers ou grupos criminosos.

Os principais motivadores para cyberataques incluem:

- Ganho financeiro (através de roubo de dados, extorsão ou fraude);
- Espionagem industrial/corporativa para obter vantagem competitiva;
- Hacktivismo por causas políticas/ideológicas;
- Ataques patrocinados por estados visando infraestrutura crítica ou informações sensíveis de outros países.



✿ Tipos de Cyberataques mais comuns

Malware: ou software malicioso — é qualquer programa ou código criado com a intenção de prejudicar um computador, rede ou servidor.

Malware é o tipo mais comum de ciberataque, principalmente porque esse termo abrange muitos subtipos como ransomware, trojans, spyware, vírus, worms, keyloggers, bots, cryptojacking, e qualquer outro tipo de ataque de malware que utilize software de forma maliciosa.



✿ Tipos de Cyberataques mais comuns

DoS / DDoS: Um ataque de Negação de Serviço (DoS) sobrecarrega uma rede com solicitações falsas para interromper operações, impedindo usuários de acessar recursos como e-mail e sites. Embora raramente cause perda de dados, consome recursos da organização para restaurar operações. Já o ataque de Negação de Serviço Distribuído (DDoS) difere por usar múltiplos sistemas em vez de apenas um, tornando-o mais rápido e difícil de bloquear, pois requer a neutralização de várias fontes.



✿ Tipos de Cyberataques mais comuns

Phishing: é um tipo de ataque cibernético que usa e-mail, SMS, telefone, redes sociais e técnicas de engenharia social para induzir uma vítima a compartilhar informações sensíveis — como senhas ou números de conta — ou baixar um arquivo malicioso que instalará vírus em seu computador ou telefone.



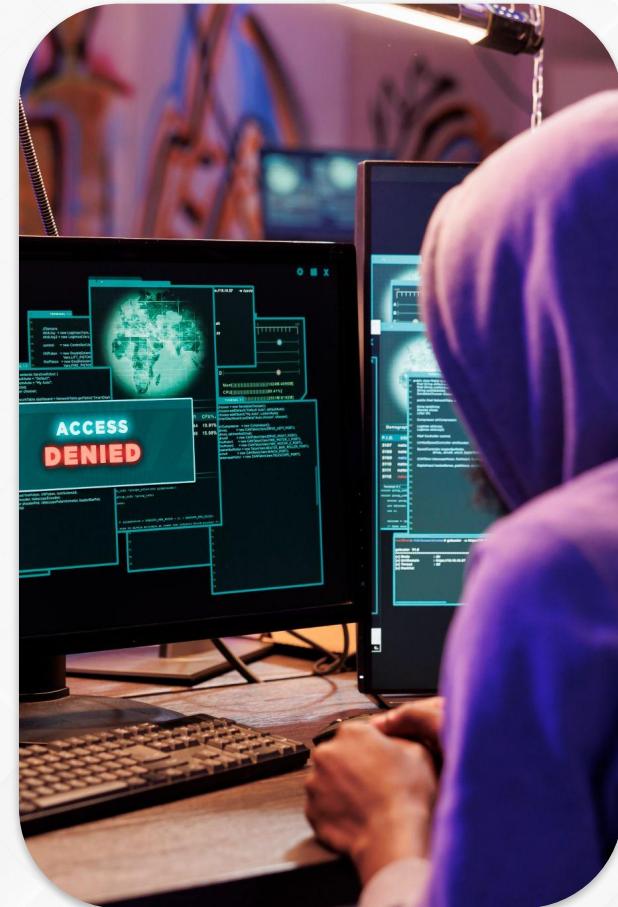
✿ Tipos de Cyberataques mais comuns

Spoofing: é uma técnica pela qual um criminoso cibernético se disfarça como uma fonte conhecida ou confiável. Ao fazer isso, o adversário consegue interagir com o alvo e acessar seus sistemas ou dispositivos com o objetivo final de roubar informações, extorquir dinheiro ou instalar malware ou outros softwares prejudiciais no dispositivo.



✿ Tipos de Cyberataques mais comuns

Ataques baseados em identidade: são extremamente difíceis de detectar. Quando as credenciais de um usuário válido são comprometidas e um adversário se passa por esse usuário, frequentemente é muito difícil diferenciar entre o comportamento típico do usuário e o do hacker usando medidas e ferramentas de segurança tradicionais.



Exemplos de ataques baseados em identidade:

Ataque

Man-in-the-Middle

é um ataque onde um invasor intercepta comunicações entre duas partes para roubar dados sensíveis ou manipular a vítima a realizar ações como transferências financeiras

Credential Harvesting

criminosos cibernéticos coletam credenciais de usuários — como IDs de usuário, endereços de e-mail, senhas e outras informações de login — em massa para então acessar sistemas, coletar dados sensíveis ou vendê-los na dark web

Credential Stuffing

ataques funcionam com base na premissa de que as pessoas frequentemente usam o mesmo ID de usuário e senha em várias contas. Portanto, possuir as credenciais de uma conta pode permitir acesso a outras contas não relacionadas

Exemplos de ataques baseados em identidade:

Password Spraying

ataque envolve um agente de ameaça usando uma única senha comum contra múltiplas contas na mesma aplicação. Isso evita os bloqueios de conta que normalmente ocorrem quando um atacante usa um ataque de força bruta em uma única conta tentando várias senhas

Brute Force

ataque utiliza uma abordagem de tentativa e erro para adivinhar sistematicamente informações de login, credenciais e chaves de criptografia. O atacante submete combinações de nomes de usuário e senhas até finalmente adivinhar corretamente

✿ Tipos de Cyberataques mais comuns

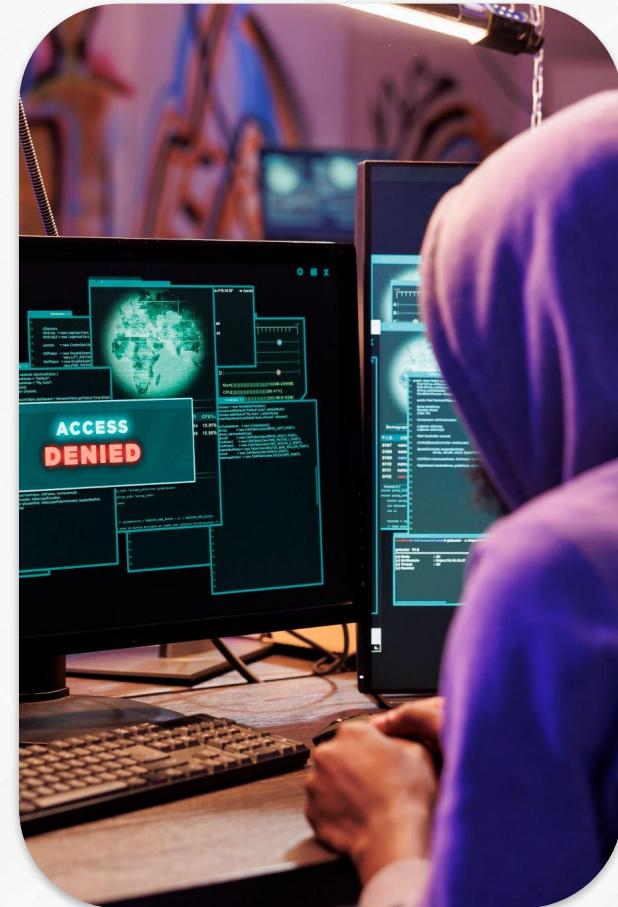
Ataques de injeção de código: consistem em um atacante injetando código malicioso em um computador ou rede vulnerável para alterar seu curso de ação. São exemplos:

1. **SQL Injection:** o ataque injeta comandos SQL maliciosos em aplicações para extrair, modificar ou apagar dados do banco de dados.
2. **Cross Site Scripting (XSS):** é um ataque onde código malicioso é inserido em um site legítimo para ser executado no navegador do usuário, permitindo roubo de dados ou roubo de identidade. Sites que permitem publicação de conteúdo por usuários são os mais vulneráveis.



✿ Tipos de Cyberataques mais comuns

Supply Chain Attack: tem como alvo fornecedores que prestam serviços ou softwares essenciais. Ataques à cadeia de suprimentos de software inserem código malicioso em aplicações para infectar usuários, enquanto ataques à cadeia de suprimentos de hardware têm como alvo componentes físicos. O software é especialmente vulnerável devido à sua dependência de componentes de terceiros como APIs e código open source.



✿ Tipos de Cyberataques mais comuns

Engenharia social: é uma técnica onde atacantes usam táticas psicológicas para manipular pessoas a realizar uma ação desejada. Através do uso de motivadores poderosos como amor, dinheiro, medo e status, os atacantes podem coletar informações sensíveis que posteriormente podem ser usadas para extorquir a organização ou aproveitar essas informações para obter vantagem competitiva.



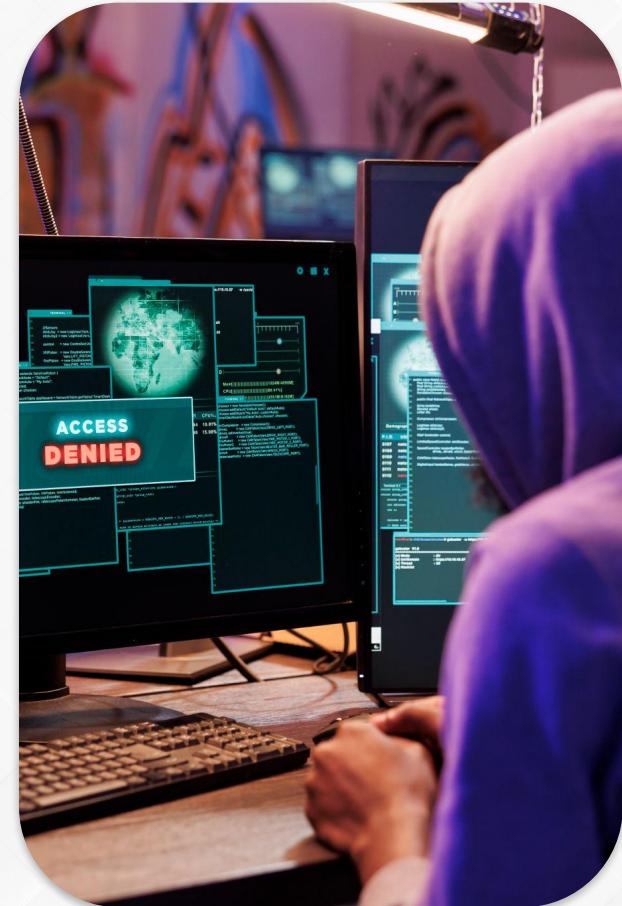
✿ Tipos de Cyberataques mais comuns

Insider threats: Focar apenas em ameaças externas deixa as organizações vulneráveis. As ameaças internas vêm de funcionários atuais ou ex-funcionários que têm acesso a redes, dados e conhecimento da empresa que poderiam possibilitar ataques. Essas ameaças podem ser maliciosas (como vender dados na dark web) ou não intencionais por negligência. As organizações devem abordar isso através de treinamento abrangente em cibersegurança que cubra a conscientização sobre ameaças tanto externas quanto internas.



💡 Tipos de Cyberataques mais comuns

Ataque IoT (Internet das Coisas): visa dispositivos ou redes IoT conectados. Após comprometer um dispositivo, o hacker pode controlá-lo, roubar dados ou criar botnets para ataques Dos/DDoS. Com o crescimento esperado de dispositivos conectados e redes 5G, especialistas preveem aumento nesses ataques.



✿ Tipos de Cyberataques mais comuns

Ataques potencializados por IA: conforme a tecnologia de IA e ML evolui, o número de casos de uso também aumentou. Assim como os profissionais de cibersegurança utilizam IA e ML para proteger seus ambientes online, os atacantes também aproveitam essas ferramentas para obter acesso a redes ou roubar informações sensíveis.



Por que Cybersegurança é importante para empresas escaláveis

As organizações não devem focar apenas em ameaças externas. Ameaças internas de funcionários atuais ou ex-funcionários com acesso privilegiado representam riscos significativos, seja por ações maliciosas ou negligência.

Um programa de treinamento em cibersegurança é essencial para mitigar ameaças internas e externas.



 Case

Netshoes



- Em 2018, a Netshoes sofreu um vazamento que expôs dados pessoais de cerca de 2 milhões de clientes, incluindo nome, CPF, e-mail, data de nascimento e histórico de compras.
- A empresa foi multada em R\$ 500 mil por danos morais. Apesar de dados sensíveis como cartões de crédito e senhas não terem sido expostos, o incidente deixou clientes vulneráveis a fraudes.

Case

Lojas Marisa



- Em novembro de 2024, a Lojas Marisa sofreu um ataque de ransomware pelo grupo Medusa, que comprometeu dados sensíveis da empresa, incluindo documentos financeiros e relatórios internos.
- Os hackers exigiram US\$300 mil como resgate, dando um prazo de 10 dias para a empresa decidir entre pagar e evitar o vazamento público dos dados ou enfrentar possíveis prejuízos reputacionais e financeiros.

Case

Renner



- Em agosto de 2021, a Lojas Renner sofreu um ataque de ransomware pelo grupo RansomEXX, que afetou seus sistemas de e-commerce e pagamentos em lojas físicas.
- A empresa conseguiu restaurar suas operações em tempo recorde (48h), embora com lentidão nos sistemas. Apesar de rumores sobre um possível pagamento de US\$ 20 milhões em criptomoedas como resgate, a Renner negou ter negociado com os criminosos e afirmou não ter identificado vazamentos de dados.

Case

Polyfill.io

```
77 function loadScript(args) {
78   var min = args.minify ? '.min' : '';
79   var features = args.fill ? "features=".concat(args.neededPolyfills.join(',')) : '';
80   var flags = args.options ? "&flags=".concat(args.options.join(',')) : '';
81   var monitor = args.rum ? '&rum=1' : ''; // not set to rum=0 since it loads RUM scripts anyway
82
83   var agent = args.agent ? "&ua=".concat(args.agent) : '';
84   var fallback = args.agentFallback ? "&unknown=".concat(args.agentFallback) : '';
85   var js = document.createElement('script');
86   js.src = "https://cdn.polyfill.io/v2/polyfill".concat(min, ".js?").concat(features + flags + mon
87   js.async = true;
88   document.body.appendChild(js);
89
90   js.onload = function () {
91     return args.afterFill();
92   };
}
```

- Em um ataque à cadeia de suprimentos em 2024, a empresa chinesa Funnell adquiriu o domínio Polyfill.io e sua biblioteca JavaScript popular, usada para adicionar compatibilidade com navegadores antigos.
- O código foi adulterado para redirecionar usuários para sites maliciosos, afetando 380.000 hosts, incluindo grandes empresas como Warner Bros e Mercedes-Benz. O ataque foi particularmente sofisticado por usar payloads condicionais baseados em cabeçalhos HTTP, dificultando sua detecção.

Case

Snowflake



- Em junho de 2024, um ataque à Snowflake, plataforma de data warehousing multicloud, resultou no roubo massivo de dados de clientes. O grupo malicioso UNC5537, identificado pela Mandiant, comprometeu sistematicamente 165 organizações usando credenciais roubadas.
- O ataque afetou grandes empresas como Live Nation (impactando 560 milhões de clientes da Ticketmaster), Santander e AT&T, com os dados sendo posteriormente anunciados em fóruns de cibercrime e usados para tentativas de extorsão.

💥 Impactos de Falhas em Segurança

Financeiro: Violação de dados pode levar a multas regulatórias, perdas de clientes e ações judiciais.

Operacional: Interrupções nos sistemas podem paralisar operações críticas e afetar a entrega de valor aos clientes.

Reputacional: Startups dependem de confiança. Uma falha de segurança pode prejudicar a percepção de marca.

Escalabilidade: Sistemas não seguros podem se tornar alvos de ataques conforme a empresa cresce.

Competitivo: Concorrentes com melhor segurança podem ganhar vantagem no mercado, especialmente em setores sensíveis como fintech e saúde.



💥 A Importância de Prevenção Proativa

- Custos de prevenção são menores que os de remediação após uma violação.
- A segurança integrada desde o início é mais eficaz do que corrigir falhas em estágios avançados.
- A cultura de segurança deve ser estabelecida desde cedo para criar consciência em toda a equipe.
- Investimentos em segurança desde o início permitem maior agilidade na expansão internacional e entrada em mercados regulados.
- A prevenção proativa permite construir uma infraestrutura de segurança que escala junto com o crescimento da empresa, evitando gargalos técnicos e retrabalho.



Áreas-Chave para Escrutínio **Proteção de Dados**

Implementação de controles robustos para proteger dados sensíveis, incluindo criptografia, tokenização e mascaramento de dados.

Pergunta-chave: Quais medidas estão em vigor para evitar vazamentos de dados?



Áreas-Chave para Escrutínio **Encriptação**

Utilização de encriptação para proteger dados em trânsito e em repouso.

Práticas Padrão:

- Encriptação ponta a ponta (E2EE) para comunicações.
- Armazenamento seguro usando protocolos como AES-256.

Pergunta-chave: Como a empresa gerencia e atualiza suas chaves de criptografia? Qual é o processo para rotação de chaves?



Áreas-Chave para Escrutínio

Gestão de Acessos e Autenticação

Implementação de controles de acesso baseados em função (RBAC) para garantir que usuários tenham apenas as permissões necessárias para suas atividades.

Exemplos:

- Uso de autenticação multifator (MFA) para sistemas críticos.
- Monitoramento e restrição de acessos privilegiados.

Pergunta-chave: Como a empresa implementa e monitora controles de acesso? Qual é o processo para revisão periódica de permissões de usuários?



Áreas-Chave para Escrutínio

Compliance e Frameworks de Privacidade

Conformidade com regulamentações de privacidade e proteção de dados é crucial para empresas escaláveis, especialmente aquelas que operam globalmente.

Pergunta-chave: Como a empresa garante conformidade com diferentes regulamentações de privacidade em múltiplas jurisdições? Quais certificações e auditorias são realizadas regularmente?





Exemplos de Compliance e Frameworks de Privacidade:

LGPD (Lei Geral de Proteção de Dados do Brasil):

- Estabelece diretrizes para tratamento de dados pessoais no Brasil.
- Exige transparência e consentimento expresso dos titulares dos dados.

GDPR (Regulamento Geral de Proteção de Dados da União Europeia):

- Implica medidas rigorosas de proteção de dados pessoais.
- Exige consentimento claro para coleta e uso de dados.



Exemplos de Compliance e Frameworks de Privacidade:

CCPA (California Consumer Privacy Act):

- Similar ao GDPR, focado em transparência e direitos do consumidor.

Outros Frameworks:

- HIPAA (para dados de saúde nos EUA)
- PCI DSS (para pagamentos com cartão)

Áreas-Chave para Escrutínio

Monitoramento e resposta a ameaças

- Sistemas de detecção e prevenção de intrusão (IDS/IPS) para identificar e bloquear atividades suspeitas em tempo real.
- SOC (Security Operations Center) dedicado ao monitoramento 24/7 de eventos de segurança e resposta a incidentes.
- Uso de ferramentas de SIEM (Security Information and Event Management) para correlacionar eventos e identificar ameaças complexas.

Pergunta-chave: Como a empresa monitora, detecta e responde a incidentes de segurança? Qual é o tempo médio de resposta a incidentes críticos?



Áreas-Chave para Escrutínio

Segurança de infraestrutura e rede

- Implementação de firewalls de próxima geração (NGFW) e segmentação de rede para isolar sistemas críticos.
- Uso de VPNs e conexões seguras para acesso remoto à infraestrutura.
- Proteção contra ataques DDoS através de soluções de mitigação em camada de aplicação e rede.
- Monitoramento contínuo de tráfego de rede para identificar anomalias e comportamentos suspeitos.

Pergunta-chave: Como a empresa protege sua infraestrutura contra ataques externos e garante a segurança do acesso remoto?



Áreas-Chave para Escrutínio

Políticas e treinamentos de segurança

- Desenvolvimento e implementação de políticas claras de segurança que cobrem todos os aspectos críticos, desde senhas até uso de dispositivos pessoais.
- Treinamentos regulares para conscientização sobre segurança, incluindo simulações de phishing e workshops sobre melhores práticas.
- Documentação atualizada de procedimentos de segurança e protocolos de resposta a incidentes.

Pergunta-chave: Como a empresa garante que todos os funcionários estão atualizados e seguindo as políticas de segurança?



Áreas-Chave para Escrutínio **Estratégias de segurança e gestão de vulnerabilidades**

- Desenvolvimento e implementação de estratégias abrangentes para identificar, avaliar e mitigar vulnerabilidades de segurança em sistemas e infraestrutura.
- Utilização de ferramentas automatizadas de varredura e análise de vulnerabilidades para detecção proativa de pontos fracos.
- Processo estruturado de priorização e correção de vulnerabilidades baseado em criticidade e impacto potencial no negócio.

Pergunta-chave: Como a empresa avalia e prioriza a correção de vulnerabilidades? Qual é o processo de gestão do ciclo de vida das vulnerabilidades, desde a identificação até a remediação?





🚩 Identificando Red Flags em empresas que investem pouco em segurança

- **Ausência de Políticas de Segurança**
 - Empresas sem políticas documentadas para gerenciamento de segurança.
- **Falta de Treinamento em Segurança**
 - Ausência de programas regulares de conscientização e treinamento em segurança para funcionários.
- **Falta de Investimentos Visíveis**
 - Orçamento limitado para segurança em relação ao tamanho e complexidade da operação.



🚩 Identificando Red Flags em empresas que investem pouco em segurança

- **Ausência de Liderança de Segurança**
 - Nenhum CISO (Chief Information Security Officer) ou equivalente em uma empresa com grande dependência de dados.
- **Dependência Excessiva de Soluções Prontas**
 - Uso de ferramentas de terceiros sem integração adequada com medidas de segurança interna.
- **Histórico de Incidentes Recorrentes**
 - Múltiplos incidentes de segurança sem melhorias significativas nos processos e controles.



🚩 Identificando Red Flags em empresas que investem pouco em segurança

- **Resposta Inadequada a Incidentes**
 - Ausência de um plano formal de resposta a incidentes ou procedimentos documentados para lidar com violações de segurança.
- **Falta de Monitoramento Contínuo**
 - Ausência de sistemas de monitoramento em tempo real e alertas automáticos para detecção de ameaças.
- **Negligência com Atualizações de Segurança**
 - Patches e atualizações críticas de segurança não são aplicados regularmente nos sistemas.



🚩 Identificando Red Flags em empresas que investem pouco em segurança

- **Falta de Controles de Acesso Adequados**
 - Ausência de políticas robustas de gerenciamento de identidade e controle de acesso baseado em função (RBAC).

❓ Perguntas estratégicas para detectar Red Flags

Quem é responsável pela segurança na empresa?
Há uma liderança clara?

Quais foram os últimos incidentes de segurança, e como foram tratados?

Que porcentagem do orçamento de TI é alocada para segurança?

Como a empresa gerencia e monitora o acesso de terceiros aos sistemas e dados?

Qual é a frequência de auditorias de segurança e testes de penetração?

Existe um processo documentado para avaliação de riscos de segurança em novas tecnologias ou integrações?

?

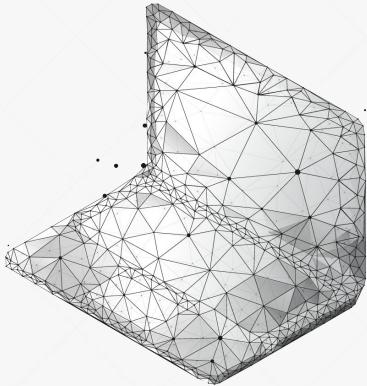
Perguntas estratégicas para detectar Red Flags

Como a empresa lida com a gestão de vulnerabilidades em dispositivos móveis e endpoints remotos?

Como são gerenciados os riscos de segurança relacionados a fornecedores, dependências e parceiros terceirizados?

Como a empresa gerencia backups e recuperação de dados em caso de incidentes de segurança?

Como são conduzidos os testes de segurança em novas integrações ou atualizações de sistema?



 SBC School

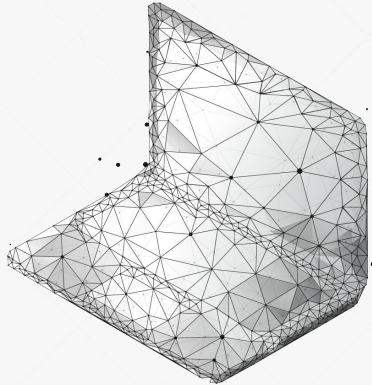


Resultados

**Ao final desta seção, vocês
deverão ser capazes de:**

- Identificar os pilares de uma estratégia de segurança bem estruturada.
- Questionar práticas de segurança para detectar negligências.
- Reconhecer potenciais riscos relacionados à segurança, privacidade e compliance.

Essas habilidades ajudarão os analistas a prever problemas futuros, avaliar o nível de preparação das startups para escalar de forma segura e identificar riscos que possam comprometer o crescimento sustentável do negócio.



 SBC School



Bibliografia

- [Crowdstrike Threat Landscape: APTs & Adversary Groups](#)
- [Cisco - What Is a Cyberattack? - Most Common Types](#)
- [CrowdStrike.com - 12 Most Common Types of Cyberattacks](#)
- [Fortinet - Top 20 Most Common Types Of Cyber Attacks](#)
- [CSIS - Significant Cyber Incidents](#)
- [Yana Storchak - Top 10 Best-Known Cybersecurity Incidents and What to Learn ...](#)