**Resumo curso Cyber Security Udemy**

Capítulo 1 e 2 – Introdução e história

**O que é Cyber Security?**

* Cyber Security é a prática de proteger os ativos de uma empresa, tais como: dados, redes, sistemas e equipamentos contra ciberataques como por exemplo, roubo de dados, danos a sistemas, interrupções ou desorientações de serviços através de técnicas de defesa, soluções tecnológicas, processos de prevenção, monitoramento e resposta a incidentes de segurança.
* Empresas progressivamente reconhecendo o tema.
* O mercado está aquecido e é considerado como uma das áreas mais promissoras em TI.

**Cenário atual em Tecnologia da Informação**

* Transformação digital: Empresas e governos prestando serviços na internet. Sociedade interagindo cada vez mais pela internet.
* Mais pessoas acessando a internet.
* Mais dispositivos que pessoas no mundo.
* Alto volume de dados sendo trafegados.

**Principais desafios para manter Cyber Security**

* Acessos advindos do mundo inteiro.
* BYOD (Bring Your Own Device). Pode conter vulnerabilidades.
* Dados armazenados em vários lugares (cloud e on premise).
* Dados se tornam cada vez mais preciosos.
* Novos marcos regulatórios (LGPD – Brasil e AGDPR – Europa).
* Técnicas de ataques cada vez mais avançadas.
* Volume de ciberataques cada vez mais alto.

**Princípios de Segurança da Informação**

* 3 princípios: Confidencialidade, Integridade e Disponibilidade
  + **Confidencialidade**: Assegurar que apenas pessoas autorizadas tenham acesso a informações restritas.
  + **Integridade**: Assegurar a forma original de uma informação, por exemplo através de cópias de segurança (backup) e rastreamento de modificações.
  + **Disponibilidade**: Assegurar que sempre que se fizer necessário as informações estejam disponíveis a pessoas autorizadas.

**Evolução de ciberataques ao longo dos anos:**

* 1977: Códigos maliciosos, trojan, Worms.
* 2004: Roubo de identidade, phishing.
* 2007: Ataques a DNS, Botnets, SQL injection, espionagem industrial.
* 2010: Engenharia Social, DDoS, aumento massivo de Botnets, ransoware.
* 2021...: Malware de Internet Banking, Keylogger, Roubo de bitcoins, sequestro de telefones, guerras cibernéticas.

**Ciberataques famosos:**

* **Stuxnet:** Ataque efetuado em uma usina de enriquecimento de Urânio do Irã, projetado para afetar as centrifugas da usina e específico para o sistema operacional escada. Descoberto em 2010 por uma empresa russa, onde reprogramava as centrifugas para o Irã não conseguir produzir o enriquecimento do Urânio para usar em poder Bélico.
* **WannaCry:** Ransoware criado para atacar sistemas Windows, pedindo resgate em bitcoins.
* **Conficker:** Descoberto em 2008, um worm que afetava computadores com OS Windows e usando técnicas avançadas de ataques, projetado para tornar computadores escravos respondendo comandos remotos, infectando até a marinha francesa.

**Meios usados em ciberataques**

* E-mail (hoje o mais utilizado).
* Pen drives / smart cards.
* Navegação internet.
* Websites internos.
* Aplicativos de celular.
* Acessos físicos a dependências, como data center (checando ar condicionado e etc).
* Pessoas.

Capítulo 3 – Ciberataque e suas características

**Principais objetivos de ciberataques:**

* Roubo de informações financeiras ou sigilosas de pessoas físicas ou instituições privadas ou públicas.
* Ciberativismo (denegrir a imagem de pessoa física ou jurídica, ou apoiar alguma ideologia).
* Sequestro de informações, coletando dados e pedindo algo para o retorno dos mesmos.
* Negação de serviços, tentando derrubar um sistema.
* Espionagem industrial, coletando informações estratégicas para obter benefícios.
* Guerras modernas, nações que tentam obter vantagem sobre nações inimigas.

**Quem está por trás de ciberataques**

* Pessoas buscando recreação.
* Hackers, pessoas com alto conhecimento técnico podendo efetuar ataques para benefícios próprios ou sendo contratado por empresas e/ou governos.
* Malicious insiders, pessoas não autorizadas com acesso a sistemas ou dependências físicas.
* Ativistas políticos, pessoas com ideologias contrárias querendo denegrir seu concorrente.
* Governos estrangeiros, causando as guerras modernas citadas acima.
* Terroristas, pessoas que tentam fazer algo contra a vida humana.

**Impactos de um ciberataque**

* Impactos técnicos, causando indisponibilidade de serviços e lentidão.
* Imagem/reputação.
* Resultados financeiros, perdendo lucratividade e o marketing.
* Perda de parcerias.
* Consequências jurídicas, podendo ser processadas por clientes ou parceiros.
* Multas e sanções regulatórias.

**Dark Web (submundo da internet)**

* Ambiente de privacidade para bem feitores e também mal feitores (em sua maioria).
* Costuma ser paraíso da ilegalidade com diversos MarketPlaces e usa cripto moedas em negociações pois são de difícil rastreabilidade.
* Navegador TOR.
* Sites com terminações diferentes, como por exemplo .onion.
* Difícil de rastrear pois o IP do usuário é criptografado.
* Sites não aparecem em mecanismos de buscas, navegações por diretórios.

**Comércio de dados vazados**

Infrator: paga desenvolvedores para criar malwares e roubar dados, além de vender dados a distribuidores.

Desenvolvedores: criam malwares para roubar dados de usuários como números de cartão de crédito, credenciais e etc...

Distribuidores: Traficar dados roubados, vendendo isso a cibercriminosos.

Cibercriminosos: Usa dados roubados para ganhar dinheiro com atividades online.

Consumidores: Credenciais roubadas, cartões de créditos, contas bancárias e etc...

Capítulo 4 - Tipos de ciberataques (resumo)

**Definindo o que é um ciberataque:** qualquer tentativa de expor, alterar, desativar, destruir, roubar ou fazer uso não autorizado em computador, sistema ou a dados.

**Cross-site Scripting (XSS):**

* O que é: ataque que tenta inserir script com código malicioso em websites.
* Como acontece o ataque: O atacante tenta inserir um script malicioso nos elementos do site que aceitam entrada de dados como campos e a própria URL do site, isso acontece em sites que não validam entrada de dados para detectar scripts maliciosos.

**DDoS: (ataque de negação de serviço distribuído)**

* O que é: Ataque que tenta gerar instabilidade ou derrubar um serviço.
* Como acontece o ataque: Os atacantes sequestram milhares de computadores para que os membros executem solicitações em massa ao mesmo tempo bombardeando o IP ou serviço da vítima (ex. Website), esses computadores agem como zumbi formando uma rede de ataque conhecida como botnet.

**Phishing:**

* O que é: ataque efetuado por envio de e-mail falso utilizando de engenharia social.
* Como acontece o ataque: Envio de email falso fingindo ser alguém que você conhece para você baixar conteúdo ou clicar em links que são maliciosos.
* Características de um PHISHING: <https://www.phishing.org/what-is-phishing>

**Ransoware:**

* O que é: ataque que tenta criptografar os dados da vítima pedindo resgate.
* Como acontece o ataque: Tenta infectar a máquina da vítima com um malware (vírus de computador) e o código malicioso procura por dados e os criptografa, quando o usuário tenta abrir os documentos recebe uma mensagem pedindo resgate financeiro para enviar a chave e de criptografar os dados.
* Simulador para testar se você estaria protegido de um ransoware: <https://www.knowbe4.com/ransomware-simulator>

**Man in the Middle**

* O que é: tipo de ataque que o atacante se insere de forma oculta no meio de uma comunicação entre duas pessoas ou sistemas se fazendo passar por uma das partes (personificando), parecendo ser uma entidade autentica da comunicação.
* Como acontece: Através da personificação de dados trocados na comunicação. A personificação pode ser por exemplo clonando o endereço IP ou MAC da máquina da vítima. Esse tipo de ataque é mais raro e difícil, pois exige técnicas avançadas de ataque.

**Engenharia social**

* O que é: ataque que tenta manipular psicologicamente a vítima para obter informações preciosas.
* Como acontece: Atacante geralmente investiga a vítima para reunir informações básicas como potenciais pontos de entrada e protocolos de segurança fracos. Após isso, o atacante ganha a confiança da vítima e fornece estímulos para ações subsequentes quebrando as práticas de segurança, como fazer a vítima revelar informações confidenciais ou concessão de acesso a recursos críticos.
* Framework para simular ataque de engenharia social: <https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/>

**Brute Force**

* O que é: ataque que tenta descobrir login e senha de um usuário por meio de técnicas de combinação visando o acesso não autorizado a sistemas.
* Como acontece: O atacante usa uma lista de possíveis senhas testando cada senha da lista até acertar e conseguir o acesso não autorizado ao sistema. Esse dicionário de senhas, contém senhas vazadas ou que são frequentemente utilizadas. As listas são facilmente encontradas na internet.

**APT (Advanced Persistent Thread)**

* O que é: Em português ameaça persistente avançada (APT), é um ataque altamente avançado que utiliza um conjunto de técnicas sofisticadas para se tornar persistente na rede.
* Como acontece o ataque: O atacante infecta um computador e logo após tenta ganhar escala infectando a rede toda, se alojando de forma persistente, duradoura e sem deixar grandes indícios. Geralmente utilizado por motivações de negócio para roubo de propriedade intelectual ou espionagem política.

**SQL Injection**

* O que é: Um ataque utilizado para destruir, manipular e ter acesso não autorizado a banco de dados.
* Como acontece: O atacante insere um comando SQL (query) no campo de uma aplicação ou site que não possui verificações de padrões aceitáveis de entrada de dados, quando deveriam para evitar esses comandos maliciosos. Com isso o atacante pode ter acesso e modificar dados críticos ou danificar o banco de dados.

**Drive By Download**

* O que é: Ataque por contaminação não intencional por download de código malicioso.
* Como acontece: O atacante insere um código malicioso em um website e quanto a vítima acessa o site a mesma faz o download de forma não intencional do código malicioso, sem perceber, ou seja, somente de visitar a página a vítima é infectada, ela não precisa clicar ou abrir algo.

**Cryptojacking**

* O que é: Ataque que sequestra um computador para minerar criptomoedas com objetivo de fomentar a criptomoeda e ter ganhos financeiros.
* Como acontece: O atacante tenta afetar a vítima através de um link malicioso via e-mail (PHISING) ou através de código em websites, com isso, instala um malware oculto que utiliza o poder computacional da máquina da vítima para ficar fazendo mineração de moedas digitais.

Capítulo 5 – Táticas e técnicas usadas em ataque e defesa.

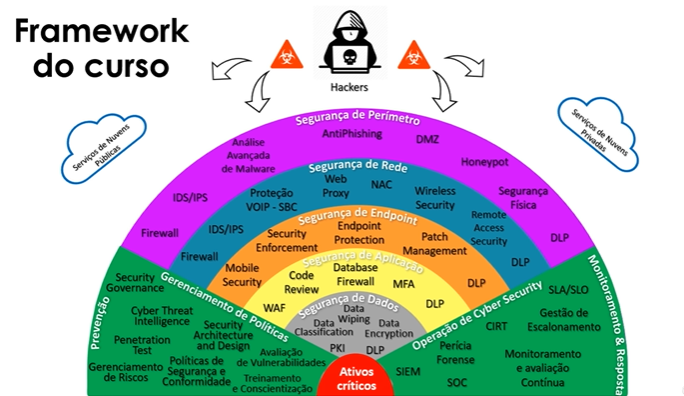
**MITRE 🡪** Poderoso framework que funciona como um base de conhecimento para ações táticas e técnicas tanto para ataques cibernéticos quanto para defesa. <https://attack.mitre.org/> (para ver a matriz de possibilidade de um ataque)

Para a parte de defesa, temos o mitre na versão Shield: <https://engage.mitre.org/matrix/>

**Sinais que podem indicar um ciberataque**

* Aumento considerável na utilização de links de internet.
* Redes, computadores e serviços lentos.
* Antivírus desabilitado em computadores e servidores.
* Programas de fontes desconhecidas instalados ou em execução.
* Logs exibindo número alto de falhas de autenticação.
* Arquivos deletados ou modificados sem interação humana.
* Arquivos criptografados sem interação humana.
* Computadores acessando a internet sozinhos.
* Colaboradores recebendo e-mails de si mesmos.

Capítulo 6 – Framework do curso



Capítulo 7 – Proteções de camada de perímetro

**Camada de perímetro** é a primeira camada em contato com a internet, tendo os primeiros soldados de defesa, ajudando a prevenir, atrasar e detectar ciberataques.

**Firewall:**

* Definição: Solução que monitora tráfego de entrada e saída de rede permitindo ou bloqueando através de políticas de segurança com o objetivo de estabelecer uma barreira de segurança contra tráfegos maliciosos entre a rede de uma empresa e redes externas como a internet.
* Inspeciona: origem, destino, porta e protocolo.
* Gerenciamento padrão: bloqueia tudo e permite progressivamente.
* Tipos: software, appliance físico, appliance virtual ou solução em nuvem.
* Pode agregar funções: IDS/IPS, inspeção de malwares, inspeção de SSL, concentrador de VPN etc.
* Firewall Leste-Oeste: tipo de firewall que implementa a mesma proteção entre servidores geralmente dentro do mesmo Data Center.

**IDS/IPS:**

* Definição: Proteção de segurança que analisa pacotes em um nível de profundidade maior que um firewall, sua existência não elimina a necessidade de um firewall.
* Como trabalha? Inspecionando a assinatura do pacote.
* Geralmente instalado junto com o firewall, mas pode funcionar em dispositivos específicos.
* **Resumo:** Faz uma análise mais comportamental.

**Análise avançada de malware – Sandbox**

* Definição: solução de segurança hospedada em ambiente isolado em uma rede que imita os ambientes operacionais e comportamentos de um usuário utilizado para executar conteúdos desconhecidos ou suspeitos com segurança.
* Pode ser usado como SaaS ou on premise.
* Benefícios:
  + Evita que malwares tragam danos ao dispositivo do usuário ou rede corporativa.
  + Protege contra ataques Zero-day.
  + Utiliza analise avançada (comportamental).
  + Protege contra ataques avançados (APT).
* Podemos testar arquivos, url’s e pesquisas de IP, domínio e etc com o site virustotal: <https://www.virustotal.com/gui/home/upload>

**Antiphishing / Antispam**

* Definição: solução que visa proteger a empresa contra e-mails indesejados (spams) e ataques efetuados por e-mail através de filtros e técnicas de varredura do conteúdo de mensagens.
* Tipos: Software, appliance físico, virtual appliance ou PaaS.
* Pode analisar a reputação do domínio, IP ou assinatura do e-mail para autorizar ou não a entrega de uma mensagem.
* Varredura no corpo e anexo da mensagem detectando malwares.
* Métodos de checagem: estatística, heurística ou preditivo.
* Com o site mxtoolbox podemos verificar se o IP ou domínio está em um black list, marcada como maliciosa: <https://mxtoolbox.com/>

**DLP (Data Leak Prevenge)**

* Definição: solução para prevenir vazamento de informações e movimentações inadequadas de dados sensíveis ao negócio (número de cartões, informações estratégicas) através de monitoramento, detecção e bloqueio.
* Pode ser instalado em outras camadas da rede.
* Protege dados em várias etapas: em armazenamento, em trânsito ou em uso.
* Técnicas para identificar e classificar tipos de dados e advertir.
* Pode educar os colaboradores para manejar dados de forma.
* Protege de dados em diversas mídias: e-mail, pen drives, dispositivos móveis, servidores de arquivos, IM, cloud services, OS clipboards, e até mesmo impressora.

**Segurança física:**

* O departamento de cyber security precisa de preocupar não somente com a segurança lógica, mas também com a segurança física, de nada adianta você ter as melhores soluções e controles lógicos se você não protege seu data center fisicamente, por exemplo. Muitas vezes essa responsabilidade é dividia com a área administrativa ou facilities da empresa.
* Objetivo: proteger e prevenir contra ameaças as dependências físicas de uma organização incluindo espionagem, sabotagem, terrorismo, danos, furtos e roubos.
* Proteger o que? Ameaças como dano e roubo, a bens, como pessoas (ex: o escritório da empresa), equipamentos (nos datacenters e salas técnicas), instalações, materiais e informações.
* Soluções utilizadas: câmeras de vigilância (para verificar quem está acessando ou oque aconteceu, quem cometeu o delito), controles de acesso (restringir acesso com biometria como por exemplo leitura de digital, íris, reconhecimento facial, chachas para identificação e liberação de catracas e etc), extintores de incêndio, detectores de fumaça, ar condicionado, no-breaks, cages, seguranças patrimoniais.
* Boa parte do trabalho do profissional de cyber security é verificar se tem alguma falha nas instalações como por exemplo falta de câmeras ou ponto cego, e auditar se somente pessoas autorizadas estão acessando áreas restritas como por exemplo o data center da empresa.

**Boas práticas:**

* DMZ’s 🡪 segmentação de rede para priorizar as defesas dos sistemas de dados mais críticos pra companhia.
* Honeypot 🡪 estudar atacantes da empresa e customizar as defesas, tornando-as mais efetivas.

**DMZs**

* Definição: é uma prática de segmentar a rede através de firewalls separando servidores que são publicados na internet dos servidores que são acessíveis apenas internamente ou via VPN.
* Protege os ativos / dados da empresa contra tráfegos não confiáveis e/ou desconhecido, geralmente é segmentado por duas ou mais camadas de firewall.

**Honeypot**

* Definição: solução que serve de armadilha para entender as táticas e técnicas utilizadas por um atacante.
* Pode detectar: as técnicas utilizadas, origem dos ataques, frequências e outras importantes características.
* Pode ser usada para desviar a atenção de um atacante.
* Pode simular partes da rede.
* Site para estudar e praticar a técnica do honeypot: <https://www.honeyd.org/>

Capítulo 8 – Proteções de camada de Rede

**A camada de rede** geralmente tem ampla segmentação de rede e hospedando sistemas e dados valiosos, sendo acessíveis internamente ou VPN.

**SBC – Proteção tráfego de voz**

* Definição: proteção de segurança para redes de voz principalmente protegendo protocolo SIP utilizado em plataformas que usam VOIP.
* Protege ligações que podem conter dados sensíveis como por exemplo número de cartão de créditos.
* Principais proteções: ACL, ataques DDoS, gerencia sessões SIP evitando fraudes e taxas com ligações, criptografia de sinalização.
* Também pode servir para interconectar diferentes sistemas com diferentes sinalizações de telefonia de forma segura.

**Mobile Security / MDM**

* Definição: solução de segurança e gerenciamento de dispositivos móveis que certifica que os dispositivos que acessam os sistemas de uma empresa seguem a política de segurança.
* Quais requisitos de segurança podem ser checados / aplicados?
  + Aplicativos permitidos.
  + Versão de Sistema Operacional e patchs.
  + Gerenciar atualizações.
  + Wipe de dispositivos.
  + Isolar dados corporativos de dados pessoais.
  + Se possui as políticas aplicadas.
  + Se o dispositivo tem criptografia habilitada.
  + Monitoramento e rastreamento do equipamento.

**Content Filtering (Proxy)**

* Definição: solução de segurança que monitora a navegação e/ou acesso a web bloqueando conteúdos maliciosos ou impróprios.
* Virtual appliance é o tipo mais comum de implementação, mas pode também estar agregado a um firewall UTM (Unified Threat Management 🡪 Gerenciamento Unificado de Ameaças)
* Método: utiliza uma base de dados mantidas por fabricantes classificando a categoria e reputação de websites.
* Faz varreduras por malwares.
* Pode ser usado também para manter a produtividade da força de trabalho de uma empresa.
* Para analisar a categoria de uma url podemos testar no site: <https://sitereview.bluecoat.com/#/>

**NAC**

* Definição: solução de segurança que se propõe a verificar a conformidade do endpoint como antivírus, IPS, análise de vulnerabilidade, autenticação e aplicação de políticas de segurança.
* Analisa se um dispositivo está saudável para por exemplo decidir se permite a conexão à rede.
* Permite rastrear uma conexão, quando aconteceu, que IP usava, que usuário estava logado.
* Uso comum é verificar se o dispositivo está autorizado a conectar em uma rede.
* Faz verificações de pre-admissão e pós-admissão.

**Wireless Security**

* Definição: Segurança em rede wireless pode ser protegida por soluções como WIPS e por práticas de aplicar políticas fortes de seguranças
* Tipos de ameaças cobertos por WIPS:
  + Rogues access points.
  + Access Point mal configurado.
  + Associação não autorizada.
  + Ataque Man In The Middle.
  + MAC spoofing.
  + Ataque de DDoS.
* Práticas de segurança em redes wireless:
  + Ocultar SSID.
  + Filtrar MACs.
  + Autenticação por certificado.
  + Protocolos seguros de criptografia.

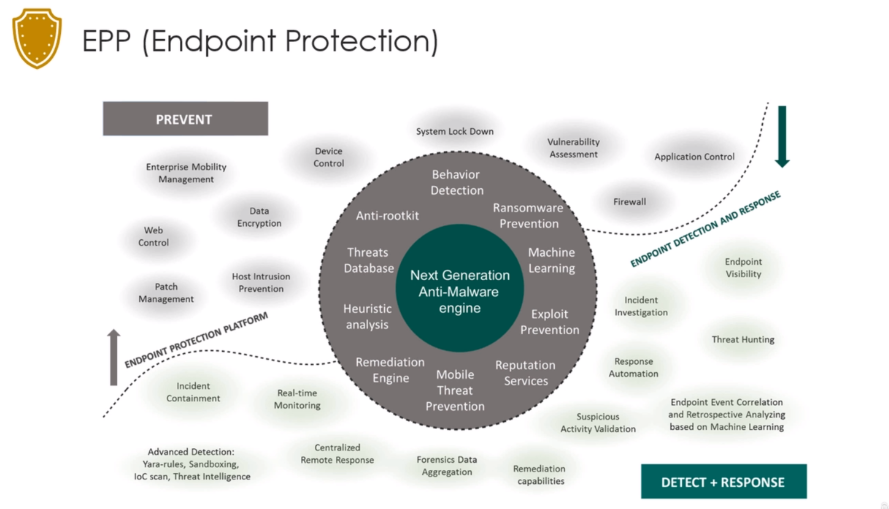
**Remote Access Security**

* VPN client.
* Single sign-on (SSO).
* PAM (Privileged Access Management).
* VDI (Virtual Desktop Infrastructure) ou DaaS (Desktop as a Service).
* Solução Zero Trust.

Capítulo 9 – Proteções de camada de Endpoint

**A camada de endpoint** geralmente são desktops, notebooks, servidores, celulares e tudo aquilo que faz parte da solução da empresa, prevenido e assegurado por antivírus.

**EPP (EndPoint Protection):**



Antivírus está ficando ultrapassado em relação ao EPP, que é muito mais adequado para os desafios de Cyber Security hoje em dia.

Teste de antivírus: <https://www.eicar.org/download-anti-malware-testfile/>

Neste site você pode testar o antivírus a partir de um arquivo malicioso fake criado pelo site.

**Security Enforcement**

* Definição: Security enforcement é a prática de gerenciar, monitorar e manter políticas de segurança aplicadas.
* Exemplo: desabilitar protocolo inseguro de um sistema ou equipamento.
* Soluções de Security Enforcement: Ansible, GPO, etc.
* Passo a passo: cria a política, solução monitora e reforça a aplicação da política periodicamente.
* Soluções de security enforcement podem ser utilizadas para manter o hardening em dia.

**Patch Management**

* Definição: processo de distribuição e aplicação de atualizações em sistemas operacionais e softwares. Os patches são necessários para corrigir erros nos softwares/sistemas que podem ser bugs ou vulnerabilidades.
* Pacotes são fornecidos por fabricantes de: S.Os, aplicativos/sistemas e equipamentos de rede.
* Processo pode ser manual ou por uma solução que automatiza (exemplo: SCCN – Microsoft e Red Hat – Linux)
* Processo deve ser periódico, geralmente acontece em ciclos.
* Rotinas de scans de vulnerabilidades podem verificar a efetividade do processo de patch management.

Capítulo 10 – Proteções de camada de Aplicação

**A camada de aplicação** é onde ficam boas práticas e controles dos domínios da empresa, prevenindo contra acessos não autorizados pela empresa.

**Code Review**

* Definição: code review ou revisão de código é o processo pelo qual visa garantir que uma aplicação é desenvolvida sem bugs ou vulnerabilidades de segurança.
* Principais checagens:
  + Melhor prática de desenvolvimento.
  + Detecção de erros.
  + Vulnerabilidades.
* Objetivo de segurança: Verificar o nível de segurança antes de ser publicado.
* Existem diversas soluções que automatizam o processo para citar uma das principais podemos mencionar o Sonarqube.
* Geralmente é verificado em todos os passos da esteira (pipeline).

**Web Application Firewall (WAF)**

* Definição: firewall de aplicação que filtra e monitora tráfegos de camada 7 como por exemplo HTTP e HTTPs.
* Função principal é proteger uma aplicação com bugs e/o vulnerabilidades.
* Protege principalmente contra ataques do tipo: XSS (Cross Site Scripting), injeção SQL etc.
* Tipos: Serviço SaaS (Software as a Service) e virtual/físicos appliances.
* Serve como proxy reverso.

**Múltiplo Fator de Autenticação (MFA)**

* Definição: MFA é um mecanismo de autenticação que exige a apresentação de duas ou mais evidências para permitir o acesso a um sistema.
* Exemplo: além de prover seu usuário e senha você precisa prover um token (código randômico que expira geralmente de 4 a 6 dígitos) para acessar um sistema.
* Protege o vazamento de credenciais.
* Meios usados: aplicativo de celular (mais usado), SMS, ligação telefônica, e-mail, token físico, Smartcard, ou biometria como por exemplo impressão digital.
* Provedores de serviços em nuvem já possuem soluções gratuitas de MFA.

**Boas práticas da camada de aplicação**

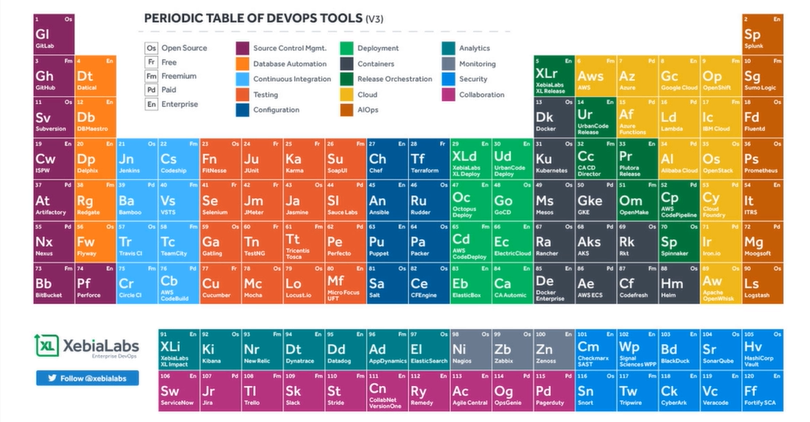
* Aplicação em camadas 🡪 melhor arquitetura voltada para segurança.
* DevSecOps 🡪 soluções que automatizam inspeções de segurança logo no começo do desenvolvimento.

**Desenvolvimento em camadas**

* Definição: o desenvolvimento em camadas é uma prática que propõe segmentar um sistema em 3 ou mais camadas.
* As 3 camadas: Apresentação, aplicação e dados.
* Apresentação: é a interface gráfica, onde o usuário interage com o sistema.
* Negócio: é onde ficam as regras de negócio do sistema.
* Dados: é onde fica o repositório de informações de um sistema, geralmente um SGBD.
* Benefícios:
  + Proteger as regras de negócio e os dados, se tiver uma invasão o atacante só acessa a camada de apresentação da qual não possui valor.
  + A mudança em uma camada não afeta outras camadas, ajudando a manter a continuidade do negócio.

**DevSecOps**

* Definição: DevOps é uma cultura em engenharia de software que integra equipes que desenvolvem o código (Dev) e equipes que administram sistemas e servidores (Ops) com objetivo de agilizar correções e melhorias de código através de soluções de automação e monitoramento constituindo uma esteira (pipeline) de desenvolvimento. O termo DevSecOps inclui a disciplina de Segurança da Informação no ciclo de vida e desenvolvimento dos sistemas.
* DevSecOps permite automatizar grande parte da inspeção de segurança e mitigar vulnerabilidade de forma rápida, antes que o código seja publicado.
* Empresas com DevOps possuem grande maturidade de TI. Desafio: Converter o processo de DevOps para DevSecOps.
* Vamos ver exemplos de soluções de segurança que podem compor o pipeline:

****

Capítulo 11 – Proteções de camada de Dados

**A camada de dados** é onde aplicamos as soluções e práticas para proteger o material mais valiosos para empresa: os dados.

**PKI – Infraestrutura de chaves públicas**

* Definição: PKI é um mecanismo de segurança utilizado para gerenciar chaves de criptografia de dados e garantir a autenticidade das entidades participantes em uma comunicação digital.
* Permite criptografar uma comunicação garantindo a autenticidade das entidades participantes.
* A autoridade que gerencia e emite as chaves pode ser interna (quando a estrutura é provida pela própria empresa) ou externa.
* Chaves são usadas para criptografar e de criptografar dados.
* A PKI protege principalmente contra ataques Man In The Middle.
* Com o site ssllabs.com podemos ver o nível de segurança de um site com base em um endereço certificado: <https://www.ssllabs.com/ssltest>

**Data Wiping**

* Definição: data wiping é um processo lógico utilizado para tornar um dado permanente ilegível geralmente por um processo que sobrescreve dados.
* Objetivo: ser utilizado quando há roubo ou furto de equipamentos ou quando o equipamento precisa ser descartado.
* Deve ser sempre utilizado no processo de descarte em substituição a formatação convencional.
* Tipos de data wiping: single pass overwrite, a three pass overwrite, a seven pass overwrite, and a secure erase.
* Lista de ferramentas para data wiping: <https://en.wikipedia.org/wiki/List_of_data-erasing_software>

**Data classification**

* Definição: processo que organiza dados atribuindo categorias a informação apoiando assim a aplicação de políticas de segurança visando o correto uso das informações.
* Classificando é possível instruir e/ou advertir quanto as políticas adotadas no uso e tratamento da informação.
* Exemplo de categorias: uso interno, uso restrito e uso público.
* O processo pode ser feito de forma manual e cooperativa onde os colaboradores assinalam a categoria, mas geralmente é apoiado por uma solução de automação.
* Objetivo principal: evitar vazamento de dados.

Capítulo 12 – Proteções de camada de Nuvem

**A camada de nuvem** é onde ficam os serviços em nuvens, geralmente públicos. Trazendo continuidade de negócios e acessibilidades, porém também criam novos desafios para a cyber security.

**Conceito Zero Trust**

* Definição: Zero Trust (ou ZTN ou ZTNA) vem do inglês zero confiança. Esse conceito é uma proposição de arquitetura de rede em que nenhuma tentativa de acesso é confiável, e todas devem ser inspecionadas continuamente.
* O modelo reconhece que confiar pode ser uma vulnerabilidade na arquitetura de acesso.
* Como é o passo a passo da implementação de uma rede Zero Trust?
  + Identifica a superfície que se deseja proteger.
  + Faz o mapeamento de acessos.
  + Constrói a arquitetura Zero Trust.
  + Monitora e mantem a política determinada pela arquitetura Zero Trust.
* Geralmente as tecnologias que suportam o conceito são chamadas de tecnologias de próxima geração.

**CASB (Cloud Access Security Broker)**

* Definição: CASB é uma espécie de gateway de segurança para acesso a serviços em nuvem que fica entre o usuário ou sistema que acessa o workload na nuvem.
* 4 pilares: visibilidade, conformidade, segurança de dados e proteção contra ameaças.
* Critérios usados pelo CASB:
  + Geolocalização na tentativa de acesso.
  + Tipo de dispositivos que está tentando acessar.
  + Versão do Sistema Operacional que está tentando acessar.
  + Nível de patch de segurança do dispositivo que está tentando acessar.
  + Quais sistemas e aplicativos estão tentando acessar a nuvem.
  + Pode verificar se o dispositivo está de acordo com a PSI da empresa.
  + Pode usar ranqueamento de risco da tentativa de acesso.
* CASB é importante principalmente quando você sabe que sua rede deverá ser acessada por dispositivos pessoais (BYOD) onde você não tem controle e/ou visibilidade do mesmo.

Capítulo 13 – Prevenção e Gerenciamento de Políticas

**A prevenção e o gerenciamento de políticas é a parte verde na lateral esquerda do framework do curso.**

**Política de segurança e conformidade**

* Definição: Política de segurança da Informação ou PSI, são os documentos que definem regras e padrões para proteger a informação e os negócios de uma empresa. Conformidade são as práticas que devem ser seguidas para assegurar padrões requeridos pelo mercado ao qual uma empresa atua.
* Alguns exemplos de PSI:
  + A empresa pode ter uma politica voltada ao desenvolvimento seguro do sistema, como o acesso a dados sensíveis sem criptografia.
  + Outro exemplo é uma política voltada para a proteção de senhas, revogando o compartilhamento de senhas da empresa.
  + Outra é voltada a rotina de backup e cópias de segurança.
* A PSI geralmente é direcionada também a atender as certificações que uma empresa possui como ISO27001, PCI e também as regulamentações de mercado que ela participa.
* Uma PSI pode ser endereçada a evitar negligência no comportamento de uso de sistemas computacionais.
* A PSI pode ser usada para direcionar auditorias internas em cada área de uma empresa.

**Dicas para segurança pessoal**

* Não usar a mesma senha em mais de um site.
* Verificar o indicativo de cadeado do navegador.
* Cartão virtual.
* Gerenciador de senhas. (O mais famoso é o LAST PASS: <https://www.lastpass.com/pt>).
* Criptografar arquivos sensíveis.
* HTTPS Everywhere. (Força a usar a comunicação HTTPS)
* 4Devs (site usado para gerar número de documentos).
* VPN (criptografa dados em trânsito, o mais famoso é o Express VPN: <https://www.expressvpn.com/pt>).
* Ghostery (extensão bloqueadora de rastreador e anúncios).
* Foxyproxy (mascarar IP de navegação e usar proxys gratuitos).
* Site que verifica se seu e-mail já foi vazado em algum lugar.

**Como fazer inspeção de segurança em Cloud**

* AWS weel-architected program (analisa arquitetura de segurança da nuvem).
* Serviços como: AWS Audit Manager para regulamentações, AWS Inspector para scan de vulnerabilidades e serviços externos para checar LGPD: <https://cleancloud.io/>
* Cloud Security Alliance – framework para computação em nuvem, com 17 domínios e 197 controles onde mostra de quem é a responsabilidade por cada controle do CSP ou do consumidor.

**Treinamento e Conscientização – (educando seu usuário)**

* Treinamento e campanhas periódicas previnem ameaças associadas ao mal comportamento do usuário. Você precisa passar noções básicas de melhores condutas.
* Varias empresas possuem plataformas que sua companhia pode usar.
* Itens que podem estar inclusos nesses treinamentos e campanhas: forma segura de navegar na internet e efetuar compras, como cadastrar uma senha segura e como protege-la, como utilizar dispositivos móveis.
* Você pode testar como está o nível de conscientização produzindo campanhas fakes de phishing. Site para testá-los: <https://cybersecurity.centigrade.de/>

**Penetration Test: Testando a segurança de sua empresa**

* O que é? Processo utilizado para simular um ataque e testar o nível de proteção da empresa.
* É recomendável que se faça periodicamente.
* Avalia se os controles e soluções implementadas estão efetivas.
* Pode ser feito por times internos (Red Team) ou se contrata uma empresa independente para fazer o teste.
* Geralmente utiliza as táticas e técnicas do Mitre Attack.
* Tipos de pentest: BlackBox (atacante não recebe informações como credenciais e IP), WitheBox (atacante recebe credenciais e endereços de sistemas) e GreyBox (atacante tem um pouco de informação).

**Avaliação de Vulnerabilidades**

* Definição: Avaliação ou gestão de vulnerabilidades é uma prática cíclica de descobrir, classificar, priorizar e mitigar vulnerabilidades de softwares.
* Vulnerabilidades podem ser encontradas em sistemas operacionais, softwares e equipamentos.
* O processo é efetuado com a ajuda de um software que escanei a rede ou através de boletins ou bases de dados públicas.
* Resoluções feitas com aplicação de patches de correção, ajuste na configuração, atualização da versão ajuste na PSI ou através da reeducação ao usuário.
* O processo de pentest geralmente explora as vulnerabilidades encontradas em um ambiente.
* O processo de gerenciamento de patches ajuda a identificar e tratas as vulnerabilidades encontradas.

**Governança em Segurança da Informação**

* Área que controla, organiza e direciona como será feita a abordagem da Segurança da Informação dentro de uma empresa/instituição.
* Demonstra quais são os riscos atuais que a empresa possui proteção e quais ainda não possui.
* Dentro dessa área é tomada decisões de alto nível.
* A área mantem um comitê periódico para apresentar os KPIs, acontecimentos relevantes e gaps identificados.
* Garante que as estratégias de Segurança da Informação estão alinhadas com os objetivos de negócios e normas regulatórias.

**Desenho e arquitetura em Cyber Security**

* Área ou disciplina que determina como os controles e soluções em Cyber Security devem ser implementadas.
* Define quais soluções devem ser implementadas, quais pessoas e áreas são envolvidas em cada etapa.
* Avalia aspectos como: protocolos, segmentação de rede e como deve ser distribuídas as soluções de Segurança da Informação.
* Aspectos para a tomada de decisão: avaliação e mapeamento de riscos, desenho da solução, operação e complexidade de implementação da solução.

**Gerenciamento de riscos**

* Objetivo: disciplina que analisa a possibilidade de riscos aos ativos de uma empresa e apoia na tomada de decisões preventivas e reativas.
* Como deve ser conduzido?
  + Identificar os ativos.
  + Identificar ameaças relacionadas a ativos.
  + Identificar as vulnerabilidades dos ativos.
  + Fazer a análise de riscos.
  + Determinar as opções de contramedidas.
  + Tomar decisões associadas a riscos.

**Cyber Insurance – Seguros contra ataques cibernéticos**

* Apólices de seguro que protegem contra danos causadas por ataques cibernéticos.
* Cobertura:
  + Custos associados aos ataques.
  + Recuperação de dados.
  + Analise forense.
  + Custos advocatícios para reparar danos a clientes e parceiros de negócios.
  + Gerenciamento de crise.
* Seguradoras no Brasil: Allianz, Zurich, Cyber Insurance (corretora) etc.

**Regulamentações de privacidade (LGPD)**

* Privacidade individual: Conforme os anos passam os indivíduos estão ganhando mais importância na relação com as instituições, esse é um movimento mundial.
* LGPD (Lei Geral de Proteção de Dados): Lei brasileira que regula a privacidade de dados pessoais, há uma versão europeia equivalente chamada GDPR e nos EUA a CCPA.
* Direitos: Ela assegura o dever de as instituições proteger os dados de clientes assim como rastrear e dar direito ao esquecimento.
* Penalidade: Se houver afetações de privacidade a lei prevê multas aplicadas as empresas responsáveis.

Capítulo 14 – Operação, Monitoramento e Resposta a Incidentes

**A operação, monitoramento e resposta à incidentes é a parte verde na lateral direita do framework do curso. É onde se aplicam parte dos atiradores de elite, com monitoramento a tempo real 24/7, executando ações de controle e recuperação de danos.**

**SIEM**

* Definição: solução que correlaciona eventos de vários dispositivos como firewalls, proxies, antivírus, sistemas de autenticação e etc., provendo uma análise em tempo real de possíveis ataques a uma empresa.
* Consolida a visão de toda a rede.
* Composto de regras avaliando aspectos que podem indicar uma tentativa de ataque.
* Geralmente divide eventos por categorias.
* Quando identifica uma ameaça a solução gera um alerta e atribui uma severidade para o mesmo.
* Utilizam amplamente de Inteligência Artificial.
* É o cockpit de um SOC.

**SOC (Security Operation Center)**

* Definição: SOC é uma central composta por profissionais que monitoram eventos que podem indicar um incidente de segurança da informação. Onde ficam os guardiões dos ativos de uma empresa.
* É responsável por prevenir, detectar, analisar, e prover respostas a tentativas de ataques.
* Geralmente opera 24 horas 7 dias por semana, monitorando ambientes em salas com diversos monitores.
* Geralmente utiliza soluções de SIEM para monitorar o ambiente, SIEM é o cockpit do carro, indica onde possui possíveis problemas e o SOC é o piloto.

**Perícia Forense (Digital Forensics) – Investigação Criminal**

* Área que tem como abrangência a recuperação e investigação de dados e indícios encontrados em equipamentos geralmente voltadas a crimes cibernéticos.
* Essas equipes geralmente contribui com empresas apoiando ou refutando hipóteses perante a ações judiciais.
* Os eventos criminais buscam a defesa ou elucidação de violações de leis definidas pela legislação como por exemplo homicídio, furto e agressão contra a pessoa.
* Os processos cíveis tratam da proteção dos direitos e propriedade de indivíduos e instituições.
* Poucas empresas possuem um departamento próprio de perícia forense, geralmente a atividade é conduzida por uma empresa terceira.

**Gestão de escalonamento**

* Definição: são políticas e procedimentos aprovados para nortear a resposta a eventos e seus escalonamentos quando necessário.
* As políticas e procedimentos devem endereçar os seguintes aspectos:
  + Quando um evento acontecer, quem deve ser comunicado.
  + Quem deve ser envolvido para resolução.
  + Os documentos devem conter entre outras coisas o contato das áreas responsáveis e como as mesmas devem ser acionadas.
  + Se um dado período ou situação acontecer e o processo não for resolvido por vias normais quem deve ser escalado?
* Elas devem estar organizadas de uma forma que se um evento acontecer a empresa perde o menor tempo possível fazendo análise de como proceder.

**Security SLA (Service Level Agreement) / SLO (Service Level Objective) reporting**

* SLA faz a medição da qualidade do serviço, SLO faz a medição de um serviço que você depende.
* Aqui é onde é feito o acompanhamento mostrando como esta a eficiência operacional do time de Cyber Security dentro de uma empresa.
* Há diversos indicadores que podem ser aferidos, como por exemplo: a quantidade de incidentes resolvidos dentro de um prazo estabelecido, a quantidade que não foi resolvida dentro do prazo, tamanho dos impactos causados por incidentes e etc...
* Geralmente é utilizado o framework da ITIL.
* Pode apontar necessidades de treinamento, de uma gestão melhor ou até mesmo necessidade de aumentar o time.

**CIRT (Computer Incident Response Team) – Como agir quando estiver sob ataque?**

* Definição: time responsável por controlar os danos causados por tentativas de ataques e pelo plano de recuperação em caso de afetação.
* São responsáveis por:
  + Registrar e comunicar os incidentes para a companhia.
  + Fazer a investigação e executar e/ou propor para eliminar ou conter o ataque.
* Outras ações de mitigação:
  + Isolamento de equipamento e sistemas comprometidos.
  + Preservação da evidência do ataque para posterior análise.
  + Limpeza e restauração dos sistemas afetados.
* Incidentes podem ser notificados por sistemas de monitoramento ou por qualquer individuo dentro de uma empresa.
* Geralmente utiliza um sistema como ITsM para registrar e manter histórico e indicadores de incidentes de segurança.

**Shadow IT e seus riscos**

* Sistemas, equipamentos e principalmente dados gerenciados e hospedados sem o conhecimento de TI.
* Riscos:
  + Segurança da Informação.
  + Software compliance.
  + Normas regulatórias.
  + Gestão de configuração/inventário.
  + Falta de governança (falta de padrão).
* Como prevenir os riscos?
  + Estabelecer normas para utilização e comunicar frequentemente.
  + Ter soluções que mapeiam os workloads como por exemplo CASB.

**Como o profissional pode se manter alerta/atualizado?**

* Participando de fóruns, grupos, usando redes sociais, se inscrevendo em boletins referência do mercado.
* Exemplos de boletins: Sans Institute, NIST, Zero Day Indicative e etc.
* Siga profissionais de Cyber Security e influenciadores nas redes.
* Leia portais de Cyber Security, alguns exemplos:
  + The hacker News
  + It security guru
  + Naked security
* Acompanhar convenções como a DEFCON.

Capítulo 15 – Cyber Security – Mercado e Carreira

**Principais cargos:**

* Analista de segurança da Informação.
* Arquiteto de Segurança da Informação.
* Pentester (encontrar vulnerabilidades).
* Auditor de Segurança.
* Diretor de Segurança da Informação (CISO).

**Certificações do profissional de Cyber Security**

* OSCP – Offensive Security Certified Professional.
* CEH – Certified Ethical Hacker.
* CISSP – Certified Information System Security Professional.
* CompTia Security+.
* CISM – Certified Information Security Manager.

**Modelo operacional de times em Cyber Security**

* Dois times: Red e Blue Team. Geralmente modelo utilizado por empresas com alta maturidade de Cyber Security.
* Red Team:
  + Time responsável por elaborar e executar simulações de ataques Cibernéticos, geralmente são os colaboradores com maior nível de proficiência na área e com profundo conhecimento de técnicas de ataque. Uma empresa terceirizada pode fazer esse papel.
* Blue Team:
  + Time responsável por fazer a defesa das simulações de ataque, podem configurar equipamentos, ajustar processos ou modificar a arquitetura de segurança.

**O mindset do profissional de Cyber Security**

* Como deve ser o mindset? A prática de Cyber Security deve proteger ou até mesmo gerar diferencial ao negócio de uma empresa, mas não deve impedir o sucesso de seus objetivos.
* O profissional deve buscar constates atualizações:
  + Novas tecnologias e os riscos associados.
  + Participar de grupos que proveem informações sobre novas vulnerabilidades/ataques.
* Ter bom senso.
* Apoiar na reavaliação contínua das práticas de Cyber Security.

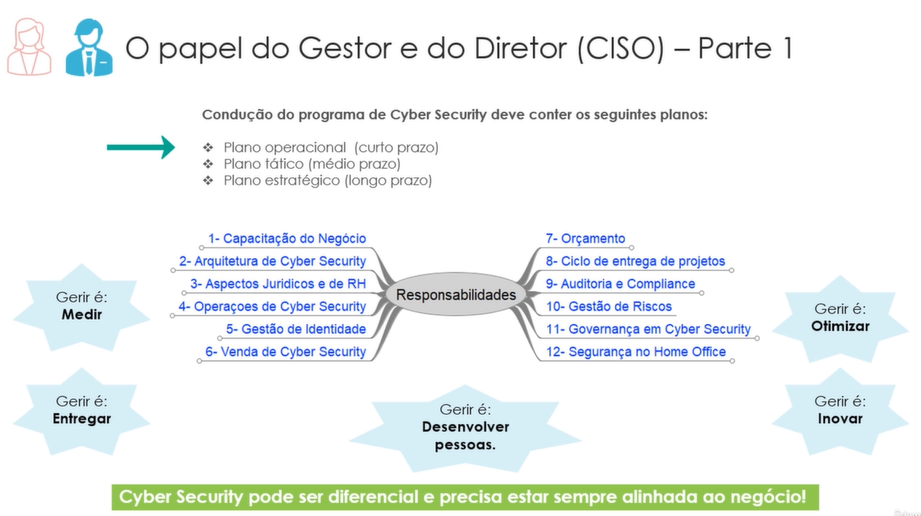
**O mercado de Cyber Security**

* Vamos ver o guia salarial de TI.
* Investimentos de empresas na área.
* Guia de carreira com as características dos cursos de Segurança da Informação.
* Quantidade de vagas não preenchidas.
* Abaixo segue as imagens da tabela salarial.

****

****

**O papel do Gestor e do Diretor (CISO) – parte 1**

****

Capítulo 16 – Aulas Adicionais

**Como avaliar uma solução de Cyber Security?**

* Utilize sites de referência na área como por exemplo Gartner e Forrester.
* Peça uma apresentação técnica ao fornecedor para verificar as características, benefícios e diferenciais da solução.
* Peça para fazer uma PoC em sua estrutura ou uma live demo.
* Utilize sites que fazem benchmark, comparam a efetividade das soluções.
* Considere aspectos importantes na análise: modalidade de suporte, língua do time de suporte e SLA.
* Na comparação, tenha ao menos 3 concorrentes.
* Pela um Battle Card e faça seu próprio em um formato de grid por exemplo.

**Soluções gratuitas usadas em Cyber Security**

* Kali Linux
* OSINT framework
* Nmap
* OpenVAS
* Google Dorks ou Google Hacking
* AirCrack-NG
* HashCat
* Burp Suite
* Metasploit