Aula - 02

Curso BlueTeam - Hacker do Bem

Aula 2 - Ataques e estratégias de defesa

Objetivos

Bem-vindo de volta *Hacker do Bem*! Iniciamos aqui a aula 2 do curso BlueTeam, de segurança defensiva. Neste encontro falaremos sobre "Ataques e estratégias de defesa" onde abordaremos os seguintes tópicos:

- Crescimento dos ciberataques no mundo
- Tipos de Atores de ameaças e Vetores de ataque
- Fontes de inteligência de ameaças
- Comparar e contrastar Tipos de controles e Estruturas de segurança

Conceitos

Aqui, exploraremos conceitos interessantes como:

- Contexto global dos ciberataques
- Atores e ameaças
- Frameworks de segurança

Crescimento dos ciberataques no mundo

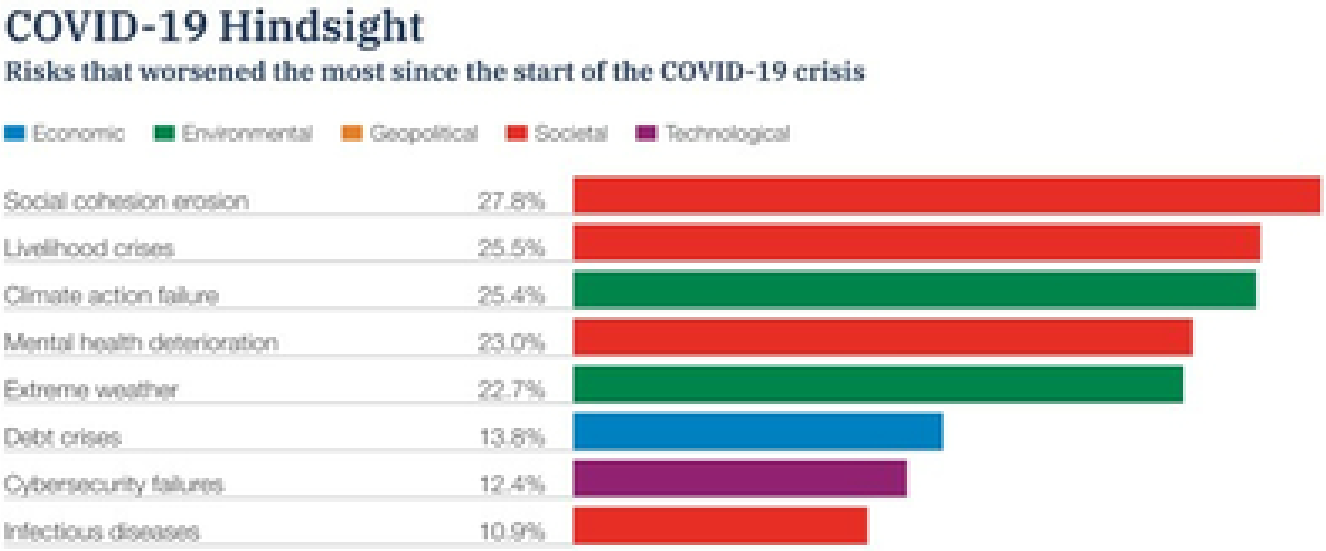
Os ciberataques têm se tornado uma ameaça cada vez mais preocupante em todo o mundo. Organizações de todos os setores enfrentam uma enxurrada de ataques cibernéticos, que podem resultar em danos financeiros, perda de dados e danos à reputação. Vamos examinar os relatórios do Fórum Econômico Mundial para obter uma visão mais ampla dessa tendência preocupante.

Relatórios do Fórum Econômico Mundial

O Relatório de Riscos Globais 2022 do Fórum Econômico Mundial destaca os ciberataques como um dos sete principais riscos globais em termos de probabilidade. Essa classificação ressalta a

crescente importância de implementar medidas eficazes de segurança cibernética. Os ataques cibernéticos estão se tornando mais frequentes e sofisticados, o que exige uma postura defensiva sólida para proteger os ativos de uma organização.

Relatório de Riscos Globais 2022



Cybersecurity report

Relatório de Riscos Globais 2023

No Relatório de Riscos Globais 2023, o Fórum Econômico Mundial continua a destacar a importância dos ciberataques como uma preocupação global. O aumento da complexidade das ameaças e a interconectividade crescente dos sistemas exigem uma abordagem proativa e multifacetada para proteger os ativos digitais. A segurança defensiva desempenha um papel fundamental na mitigação dos riscos associados aos ciberataques.

Acessando o IBRASPD

Uma maneira de entender a realidade dos ciberataques é por meio de exemplos divulgados na mídia. O Instituto Brasileiro de Segurança Proteção e Privacidade de Dados (IBRASPD) mantém uma lista de incidentes de segurança cibernética ocorridos em 2021 e 2022 em seu site IBRASPD.org. Ao explorar essa lista, é possível ter uma visão mais próxima dos tipos de ataques e das organizações afetadas.

Ibraspd 2022

Navegue pelo site do IBRASPD para examinar os incidentes de segurança cibernética ocorridos nos últimos anos. Isso permitirá que você entenda os métodos empregados pelos invasores, as vulnerabilidades exploradas e as consequências enfrentadas pelas organizações atacadas. Essa análise fornecerá uma visão valiosa do mundo real da segurança cibernética e o ajudará a desenvolver habilidades defensivas mais eficazes.

Ibraspd-2021

Os ciberataques continuam a representar uma ameaça significativa para empresas e indivíduos em todo o mundo. Os relatórios do Fórum Econômico Mundial nos anos de 2022 e 2023 destacam a importância de abordar esse problema com seriedade. Através do acesso ao IBRASPD e da análise de incidentes de segurança cibernética, você poderá compreender melhor a gravidade dos ataques e a necessidade de adotar uma postura defensiva eficaz.

Prepare-se para aprofundar seu conhecimento e se tornar um profissional capacitado para enfrentar os desafios da segurança cibernética. Estamos empolgados em tê-lo como parte deste curso emocionante!

Tipos de Atores de ameaças e Vetores de ataque

Nesta seção, vamos explorar com mais detalhes os diferentes tipos de atores de ameaças e os vetores de ataque que eles utilizam para comprometer a segurança dos sistemas. É essencial compreender as características e motivações desses atores, bem como os métodos que empregam, a fim de implementar estratégias de defesa eficazes. Vamos mergulhar neste mundo sombrio da segurança cibernética!

Vulnerabilidade, Ameaça e Risco

Antes de mergulharmos nos tipos de atores de ameaças e vetores de ataque, vamos relembrar alguns conceitos básicos. Vulnerabilidade refere-se a uma fraqueza ou falha em um sistema que pode ser explorada por um ator de ameaça. Ameaça é a intenção de explorar uma vulnerabilidade para realizar atividades maliciosas. Já risco é a probabilidade de uma ameaça explorar uma vulnerabilidade e o impacto resultante.

Vulnerabilidade

Características dos atores de ameaças

Os atores de ameaças apresentam características distintas, o que influencia suas motivações e métodos. Vamos examinar com mais detalhes alguns desses tipos de atores:

Hackers, Script Kiddies e Hacktivistas

Os hackers são indivíduos habilidosos e experientes, com conhecimento profundo em sistemas de computadores. Eles possuem habilidades técnicas avançadas e podem explorar vulnerabilidades para obter acesso não autorizado a sistemas. Alguns hackers são movidos por desafios intelectuais e buscam aprimorar suas habilidades.

Já os script kiddies, em contraste, são menos habilidosos e dependem de ferramentas e scripts prontos para realizar ataques. Eles geralmente não têm um profundo entendimento técnico e são motivados pela busca de emoção e notoriedade.

Os hacktivistas são atores de ameaças com motivações políticas, sociais ou ideológicas. Eles usam ataques cibernéticos para expressar suas opiniões ou protestar contra determinadas organizações, governos ou práticas. Seus ataques podem variar de deface de websites a vazamento de informações confidenciais.

Atores estatais e Ameaças Persistentes Avançadas

Os atores estatais são representados por governos ou agências governamentais que conduzem ataques cibernéticos com intenções políticas, estratégicas ou militares. Esses atores possuem recursos consideráveis e são capazes de lançar ataques sofisticados e de longo prazo. Eles podem buscar obter informações confidenciais, interromper infraestruturas críticas ou espionar governos e organizações.

As Ameaças Persistentes Avançadas (APTs) são ataques conduzidos por atores altamente habilidosos e persistentes. Muitas vezes, são patrocinados por governos ou grupos organizados. Esses ataques têm como alvo específico organizações de alto valor, como empresas, instituições governamentais ou de defesa. As APTs são caracterizadas por sua capacidade de evasão e longa duração, visando comprometer sistemas e obter informações valiosas.

APT

O Brasil é um dos paises mais visados por criminosos cibernéticos na América Latina.

Num relatório publicado pela empresa FireEye, sobre ataques cibernéticos na América Latina, o Brasil aparece nas primeiras posições de maiores alvos de criminosos, além de mostrar também os

setores mais afetados pelos invasores.

O Brasil continua sendo o primeiro em número de call-backs, enquanto o chile é o quarto, pois lá há um investimento maior na área de segurança cibernética. Nos anos 90 o foco era prevenção. Na década de 2000, detecção. Agora, é momento da resposta.

> **Curiosidade: callback**
>
> Uma "callback" (ou "call-back") é um termo comumente usado no contexto de uma ameaça persistente avançada (APT). Em uma APT, os atacantes geralmente buscam manter acesso persistente e contínuo a um sistema comprometido, mesmo após a exploração inicial.
>
> Uma callback é uma técnica usada pelos atacantes para estabelecer um canal de comunicação oculto e seguro entre o sistema comprometido e os servidores controlados pelos atacantes. Essa comunicação é geralmente estabelecida por trás de firewalls, detectores de intrusão e outras medidas de segurança, para evitar a detecção pelos sistemas de defesa.
>
> A callback pode ser realizada de diferentes maneiras, dependendo das estratégias e ferramentas usadas pelos atacantes. Uma abordagem comum é o uso de comunicações cifradas, como o uso de protocolos de comunicação seguros (por exemplo, HTTPS) ou o uso de túneis criptografados para encapsular o tráfego de rede. Isso permite que os atacantes enviem comandos, recebam informações e até mesmo atualizem o malware implantado no sistema comprometido.
>
> Uma vez estabelecida a callback, os atacantes podem controlar remotamente o sistema comprometido, realizar atividades maliciosas adicionais, roubar informações confidenciais, implantar outras cargas úteis de malware ou expandir sua presença na rede.
>
> Detectar uma callback é um desafio significativo, pois os atacantes se esforçam para ocultar suas atividades e mascarar a comunicação com técnicas sofisticadas. A detecção eficaz requer monitoramento contínuo, análise de tráfego de rede, identificação de padrões anormais e uso de soluções de segurança avançadas.
>
> No contexto de defesa contra APTs, a detecção e a interrupção das callbacks são fundamentais para mitigar os riscos associados a essas ameaças persistentes. Isso pode envolver a implementação de soluções de detecção de intrusão, sistemas de prevenção de intrusões, firewalls avançados, monitoramento de tráfego de rede e outras medidas de segurança para identificar e bloquear as comunicações callback e interromper o controle remoto do sistema comprometido pelos atacantes..

Sindicatos criminosos e Competidores

Os sindicatos criminosos são organizações criminosas que visam obter lucro financeiro por meio de atividades cibernéticas ilegais. Esses atores estão envolvidos em atividades como roubo de dados, extorsão, fraude e tráfico de informações sensíveis. Eles operam em redes criminosas e geralmente têm acesso a recursos técnicos avançados. Seus ataques podem causar danos significativos a organizações e indivíduos.

Competidores comerciais também podem representar uma ameaça para a segurança cibernética de uma organização. Esses atores buscam obter vantagem competitiva, comprometendo a segurança

de seus concorrentes. Eles podem realizar espionagem industrial, roubo de propriedade intelectual ou sabotagem de sistemas para ganhar uma posição de destaque no mercado.

Atores de ameaça interna

Os atores de ameaça interna são pessoas que têm acesso legítimo aos sistemas de uma organização, como funcionários, ex-funcionários ou prestadores de serviços. Esses atores representam um risco significativo, pois já possuem acesso privilegiado aos sistemas e dados sensíveis. Suas motivações podem variar desde vingança até o desejo de obter informações confidenciais para uso pessoal ou para repassar a terceiros.

Superfície e Vetores de ataque

A superfície de ataque refere-se ao conjunto de pontos de acesso potenciais que um ator de ameaça pode explorar em um sistema. Isso inclui servidores, aplicativos, dispositivos de rede e outros elementos da infraestrutura de TI. Quanto maior a superfície de ataque, maior a probabilidade de encontrar vulnerabilidades exploráveis.

Os vetores de ataque são as técnicas e métodos utilizados pelos atores de ameaça para explorar vulnerabilidades e comprometer a segurança dos sistemas. Alguns exemplos comuns de vetores de ataque incluem:

Os vetores de ataque são as diferentes formas pelas quais os atores de ameaças podem explorar vulnerabilidades e comprometer a segurança dos sistemas. Vamos explorar com mais detalhes os principais vetores de ataque a seguir:

1. Acesso direto

O acesso direto refere-se à exploração de vulnerabilidades em sistemas que estão fisicamente acessíveis aos atacantes. Isso pode envolver tentativas de invadir servidores, computadores ou dispositivos de rede por meio de acesso físico não autorizado, como conexão direta a portas USB, interfaces de rede ou acesso físico aos equipamentos.

2. Mídia removível

O uso de mídia removível, como pendrives USB ou discos externos, representa um vetor de ataque comum. Os atacantes podem infectar essas mídias com malware e distribuí-las de forma maliciosa. Quando os usuários inserem essas mídias em seus sistemas, o malware é executado, comprometendo a segurança e permitindo a exploração de vulnerabilidades.

3. E-mail

O e-mail é um vetor de ataque amplamente utilizado pelos atores de ameaças. Isso inclui técnicas como phishing, em que os atacantes enviam e-mails fraudulentos ou enganosos para induzir os usuários a revelar informações confidenciais, clicar em links maliciosos ou baixar anexos infectados. Os e-mails de phishing podem se passar por entidades confiáveis, como bancos, empresas ou instituições governamentais.

4. Acesso remoto e Sem fio

O acesso remoto e sem fio oferece aos atacantes a oportunidade de explorar vulnerabilidades em conexões de rede sem fio, acesso VPN (Virtual Private Network) ou sistemas de administração remota. Os atacantes podem tentar obter acesso não autorizado a redes corporativas ou dispositivos pessoais por meio de senhas fracas, configurações inadequadas ou exploração de vulnerabilidades de segurança em protocolos de comunicação sem fio.

5. Cadeia de suprimentos

A cadeia de suprimentos representa um vetor de ataque em que os atacantes buscam comprometer os sistemas e aplicativos por meio de fornecedores ou parceiros de confiança. Isso pode incluir a exploração de vulnerabilidades em software ou hardware fornecido, inserção de backdoors ou modificações maliciosas em componentes de software durante o processo de desenvolvimento ou distribuição.

6. Web e Mídias sociais

A web e as mídias sociais oferecem um amplo espaço para vetores de ataque. Isso inclui a exploração de vulnerabilidades em sites, ataques de injeção de código, ataques de cross-site scripting (XSS) e ataques de engenharia social direcionados a usuários de redes sociais. Os atacantes podem distribuir links maliciosos, malware ou phishing por meio de sites comprometidos, anúncios maliciosos ou perfis falsos em redes sociais.

7. Nuvem

A computação em nuvem também representa um vetor de ataque significativo. Os atacantes podem tentar explorar vulnerabilidades nos serviços em nuvem, como armazenamento, servidores virtuais ou serviços de autenticação. Isso pode incluir ataques de injeção de código, acesso não autorizado a recursos em nuvem ou comprometimento de credenciais de acesso.

A compreensão dos diferentes tipos de atores de ameaças e vetores de ataque é essencial para proteger adequadamente os sistemas e dados contra ameaças cibernéticas. Ao conhecer suas características e motivações, você estará mais preparado para implementar medidas de defesa eficazes e responder de forma adequada aos incidentes de segurança.

Esteja preparado para fortalecer suas habilidades na proteção de servidores e enfrentar os desafios apresentados pelos atores de ameaças. Estamos animados para guiá-lo em sua jornada de aprendizado!

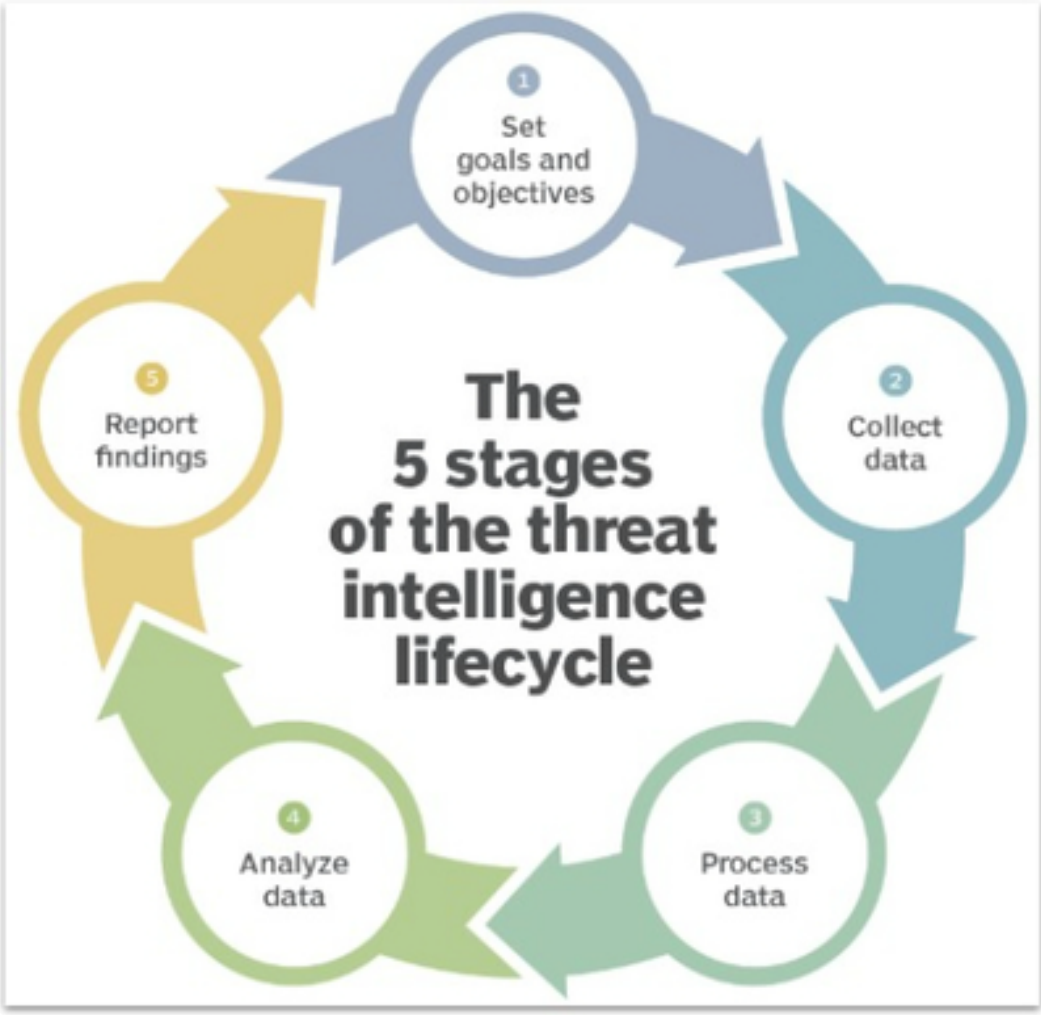
Fontes de inteligência de ameaças

No mundo em constante evolução da segurança cibernética, é essencial ter acesso a informações atualizadas sobre as ameaças existentes. Para isso, contamos com diversas fontes de inteligência de ameaças que nos fornecem insights valiosos sobre os atores de ameaças, suas táticas, técnicas e procedimentos (TTPs) e indicadores de comprometimento (IoCs). Vamos explorar essas fontes a seguir:

Fontes de pesquisa de ameaças

As fontes de pesquisa de ameaças incluem organizações, institutos de pesquisa, universidades e grupos independentes que realizam estudos e análises detalhadas sobre ameaças cibernéticas. Essas fontes fornecem informações cruciais sobre as táticas, técnicas e procedimentos utilizados pelos atores de ameaças. Por exemplo, elas podem analisar e documentar as diferentes fases de um ataque, como reconhecimento, exploração, comprometimento, exfiltração de dados e persistência.

Essas fontes também podem fornecer insights sobre as ferramentas e os métodos utilizados pelos atacantes, como malware, engenharia social, phishing, ransomware e exploração de vulnerabilidades. Com base nessas informações, os profissionais de segurança podem entender melhor as ameaças e desenvolver estratégias de defesa mais eficazes.



5-estagios

Provedores de inteligência de ameaças

Os provedores de inteligência de ameaças são organizações especializadas que coletam e analisam dados de ameaças de várias fontes para fornecer informações acionáveis aos profissionais de segurança. Esses provedores geralmente possuem equipes de pesquisa dedicadas que monitoram ativamente as atividades dos atores de ameaças e rastreiam suas táticas, técnicas e procedimentos em tempo real.

Esses provedores de inteligência de ameaças podem fornecer relatórios detalhados sobre as últimas ameaças e tendências, bem como IoCs associados. Eles podem destacar os métodos de ataque mais recentes, como ataques de dia zero, ataques de força bruta, injeção de SQL, ataques de phishing sofisticados e técnicas avançadas de evasão de detecção.

> **VOCÊ SABIA? Uso de OSINT para Reconhecimento e Monitoramento**
>
> Falaremos sobre uma ferramenta poderosa usada no mundo da segurança cibernética: a OSINT, que significa "Open Source Intelligence" ou "Inteligência de Fontes Abertas". Você sabia que a OSINT é amplamente utilizada para reconhecimento e monitoramento de ameaças?
>
> A OSINT refere-se à coleta e análise de informações provenientes de fontes abertas disponíveis publicamente, como sites, redes sociais, fóruns, blogs e outras fontes online. Essas informações podem fornecer valiosos insights sobre organizações, indivíduos, infraestruturas de rede e até mesmo possíveis ameaças.
>
> Quando se trata de segurança defensiva, o uso da OSINT é essencial para entender o cenário atual de ameaças e identificar possíveis vulnerabilidades. Veja alguns pontos interessantes sobre como a OSINT pode ser aplicada no reconhecimento e monitoramento:
>
> **Identificação de ativos expostos:** Com a OSINT, é possível descobrir quais ativos de uma organização estão expostos na internet, como servidores, dispositivos de rede e informações sensíveis. Isso permite que os profissionais de segurança tenham uma visão clara de sua superfície de ataque e possam tomar medidas para proteger adequadamente esses ativos.
>
> **Perfilagem de ameaças:** Através da OSINT, é possível coletar informações sobre atores de ameaças, suas motivações, métodos e até mesmo seus históricos de ataques. Isso ajuda a criar perfis detalhados das ameaças e entender suas possíveis estratégias. Com esses insights, os profissionais de segurança podem desenvolver contramedidas mais eficazes para se proteger contra ameaças conhecidas.
>
> **Monitoramento de mídias sociais:** As mídias sociais se tornaram um terreno fértil para coleta de informações. Através da OSINT, é possível monitorar as atividades e as postagens nas redes sociais para detectar possíveis ameaças. Por exemplo, postagens suspeitas de usuários podem revelar intenções maliciosas ou fornecer pistas valiosas sobre ataques iminentes.
>
> **Análise de vulnerabilidades:** A OSINT também pode ser usada para identificar possíveis vulnerabilidades em sistemas, aplicativos e infraestruturas. Através da análise de informações públicas, como relatórios de segurança, comunicados de imprensa e fóruns de discussão, é possível obter conhecimento sobre vulnerabilidades conhecidas e seus respectivos patches ou soluções.
>
> **Detecção de vazamentos de dados:** Com a OSINT, é possível monitorar a internet em busca de vazamentos de dados. Esses vazamentos podem conter informações sensíveis de uma organização, como senhas, dados de clientes ou informações confidenciais. Ao detectar esses vazamentos precocemente, as medidas corretivas podem ser tomadas para mitigar danos e proteger a reputação da organização.

> A OSINT é uma poderosa aliada na segurança cibernética, fornecendo informações valiosas para o reconhecimento e monitoramento de ameaças.

Outras fontes de pesquisa de inteligência de ameaças

Além das fontes mencionadas acima, existem outras fontes valiosas de pesquisa de inteligência de ameaças que podem fornecer informações cruciais para a segurança cibernética:

Comunidades de segurança: Fóruns, grupos de discussão e comunidades online de profissionais de segurança cibernética são uma fonte importante de compartilhamento de informações e colaboração na identificação de ameaças e estratégias de defesa. Nessas comunidades, os profissionais podem compartilhar suas experiências, discutir novas ameaças e trocar informações sobre as últimas TTPs observadas.

Relatórios de incidentes: Organizações e agências governamentais podem publicar relatórios de incidentes de segurança cibernética, destacando ataques recentes, tendências e práticas recomendadas. Esses relatórios podem fornecer insights valiosos sobre as

TTPs utilizadas pelos atacantes e os setores ou indústrias mais visados.

Redes de compartilhamento de IoC: Existem redes dedicadas ao compartilhamento de Indicadores de Comprometimento (IoCs) entre organizações de segurança, permitindo uma resposta mais rápida a ameaças conhecidas. Essas redes são fundamentais para identificar IoCs relevantes e aplicar medidas preventivas e de detecção precoce.

Relatórios produzidos pelo The DFIR Report

O The DFIR Report (https://thedfirreport.com/) é uma equipe dedicada à análise e divulgação de informações relacionadas à resposta a incidentes e investigação forense em segurança cibernética. Eles desempenham um papel crucial na comunidade de segurança, fornecendo análises detalhadas de incidentes de alto perfil, estudos de caso e informações relevantes para profissionais de segurança cibernética.

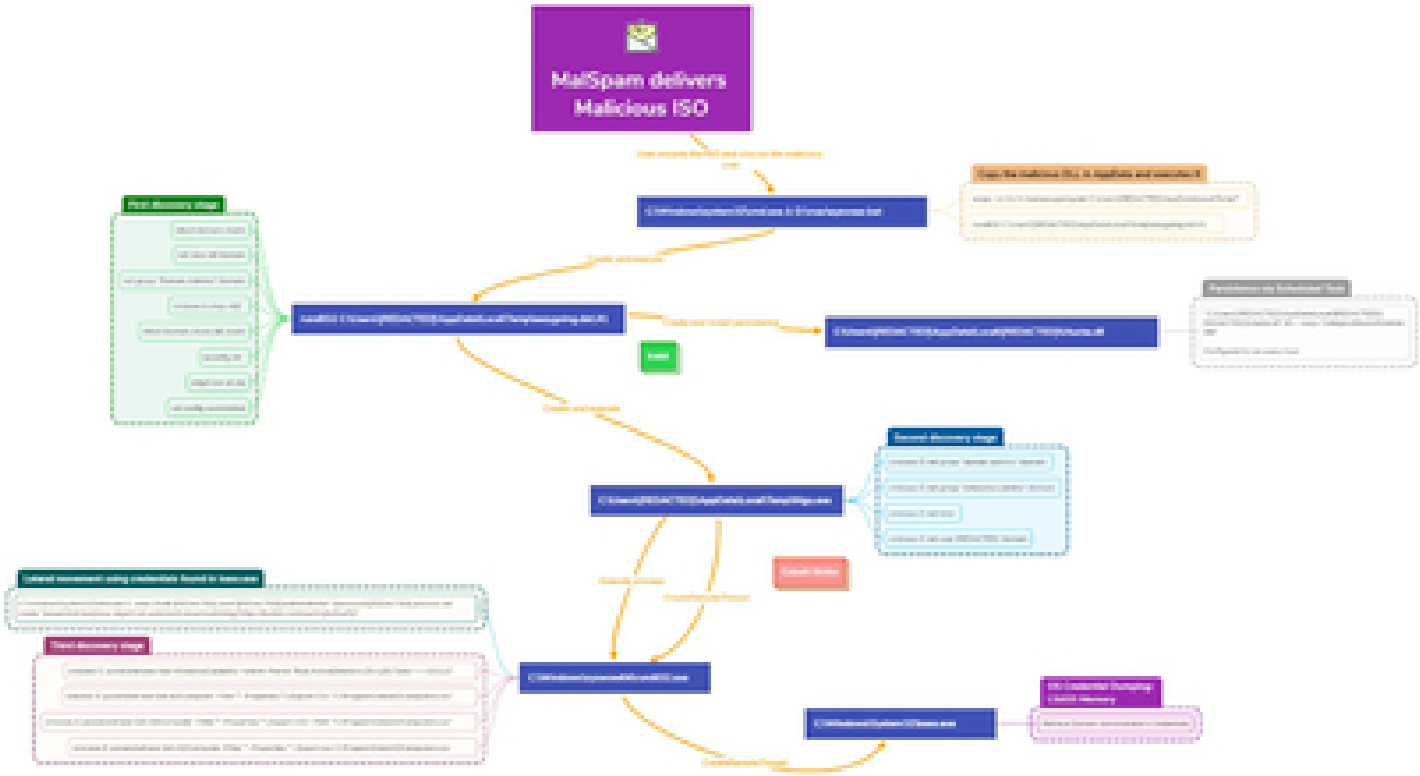
A equipe do The DFIR Report realiza um trabalho minucioso de coleta de dados e evidências em relação a incidentes de segurança cibernética. Eles examinam e analisam as informações disponíveis, como logs de eventos, registros forenses, malware, tráfego de rede e outros artefatos digitais relacionados ao incidente em questão.

Com base nessa análise detalhada, eles desenvolvem relatórios completos e detalhados, nos quais descrevem o cenário do incidente, as táticas, técnicas e procedimentos (TTPs) utilizados pelos invasores, bem como as medidas de mitigação recomendadas. Esses relatórios são compartilhados com a comunidade de segurança cibernética, com o objetivo de aumentar a conscientização sobre ameaças e ajudar outras organizações a se protegerem contra ataques similares.

Além disso, a equipe do The DFIR Report também se dedica a estudar tendências, padrões e evolução das ameaças cibernéticas. Eles acompanham o cenário de segurança, analisam novas

técnicas de ataque e compartilham essas informações por meio de artigos, whitepapers e apresentações em conferências.

O trabalho realizado pela equipe do The DFIR Report é altamente valorizado na comunidade de segurança cibernética, pois fornece informações valiosas que auxiliam na detecção, resposta e prevenção de incidentes. Sua abordagem detalhada e análise profunda contribuem para o avanço da segurança cibernética como um todo, capacitando profissionais e organizações a protegerem melhor seus sistemas e dados contra ameaças cada vez mais sofisticadas.



the-dfir

Táticas, Técnicas e Procedimentos (TTPs) e Indicadores de Comprometimento (IoCs)

As Táticas, Técnicas e Procedimentos (TTPs) referem-se aos métodos, abordagens e processos usados pelos atores de ameaças para realizar ataques. Essas informações são vitais para entender como os atacantes operam, quais são suas motivações e como eles podem explorar as vulnerabilidades de sistemas e redes.

As fontes de inteligência de ameaças coletam e analisam dados sobre as TTPs utilizadas pelos atores de ameaças. Isso inclui informações sobre as ferramentas, técnicas de evasão, estratégias de infiltração, exploração de vulnerabilidades, movimentos laterais e exfiltração de dados. O conhecimento dessas TTPs permite que as organizações se protejam melhor, desenvolvendo estratégias de defesa adequadas, fortalecendo suas posturas de segurança e implementando medidas preventivas e de detecção.

Os Indicadores de Comprometimento (IoCs) são sinais ou evidências que podem indicar a presença ou atividade de um ataque. Isso inclui endereços IP, URLs, hashes de arquivos, padrões de tráfego, assinaturas de malware e outras características que podem ser associadas a atividades maliciosas. Os IoCs são coletados, analisados e compartilhados pelas fontes de inteligência de ameaças, permitindo que as organizações os utilizem para detectar e responder a ataques em tempo real.

Alimentação de dados de ameaças

Uma parte crítica da inteligência de ameaças é a alimentação contínua de dados relevantes. Isso envolve a coleta e a agregação de informações provenientes de diversas fontes, como feeds de vulnerabilidades, feeds de inteligência de ameaças, feeds de eventos de segurança e logs de sistemas.

As ferramentas de gerenciamento de informações e eventos de segurança (SIEM) desempenham um papel importante na coleta, correlação e análise desses dados. Elas permitem que as organizações obtenham uma visão abrangente das atividades de ameaças em sua infraestrutura, identificando padrões, correlações e comportamentos suspeitos.

A alimentação adequada de dados de ameaças permite a detecção precoce de ameaças emergentes, a análise de tendências e a implementação de contramedidas eficazes. Além disso, ajuda as organizações a ajustarem suas estratégias de segurança com base nas informações mais recentes e relevantes.

Inteligência artificial e Análise preditiva

Com o avanço da tecnologia, a inteligência artificial (IA) e a análise preditiva estão desempen

hando um papel cada vez mais importante na área de inteligência de ameaças. Algoritmos de IA podem analisar grandes volumes de dados de ameaças em tempo real, identificar padrões, anomalias e comportamentos maliciosos, e fornecer insights valiosos para a detecção proativa e prevenção de ataques.

A análise preditiva, por sua vez, utiliza técnicas estatísticas e modelos matemáticos para prever e antecipar tendências e ameaças futuras com base em padrões históricos, informações contextuais e dados de inteligência de ameaças. Essa capacidade permite que as organizações estejam um passo à frente dos atacantes, implementando medidas de segurança mais eficazes e antecipando possíveis cenários de ataque.

A inteligência de ameaças impulsionada por IA e análise preditiva é especialmente útil para lidar com ameaças sofisticadas e em constante evolução. Essas tecnologias permitem uma resposta mais rápida, precisa e automatizada, ajudando as organizações a se protegerem contra ameaças avançadas e desconhecidas.

Em resumo, a inteligência de ameaças é fundamental para uma estratégia eficaz de segurança cibernética. Ao aproveitar fontes de pesquisa de ameaças, provedores de inteligência de ameaças, TTPs e IoCs, alimentação contínua de dados e tecnologias avançadas como IA e análise preditiva, as organizações podem fortalecer sua postura de segurança e proteger-se de maneira mais efetiva contra as ameaças cibernéticas em constante evolução.

Tipos de controles e Estruturas de segurança: Um mundo de proteção cibernética

E aí, galera! Vamos falar agora sobre os diferentes tipos de controles de segurança e as estruturas que os cercam. Quando se trata de garantir a segurança cibernética, é importante entender as categorias de controle, suas funções e como eles se encaixam em diferentes estruturas de segurança. Vamos lá!

Categorias de Controle de Segurança

Os controles de segurança podem ser agrupados em categorias principais para melhor organização e abordagem. Essas categorias incluem controles administrativos, controles técnicos e controles físicos.

Os controles administrativos estão relacionados a políticas, procedimentos e práticas organizacionais.

Os controles técnicos referem-se a tecnologias e mecanismos implementados para proteger os sistemas.

Já os controles físicos estão relacionados à segurança física de instalações e equipamentos.

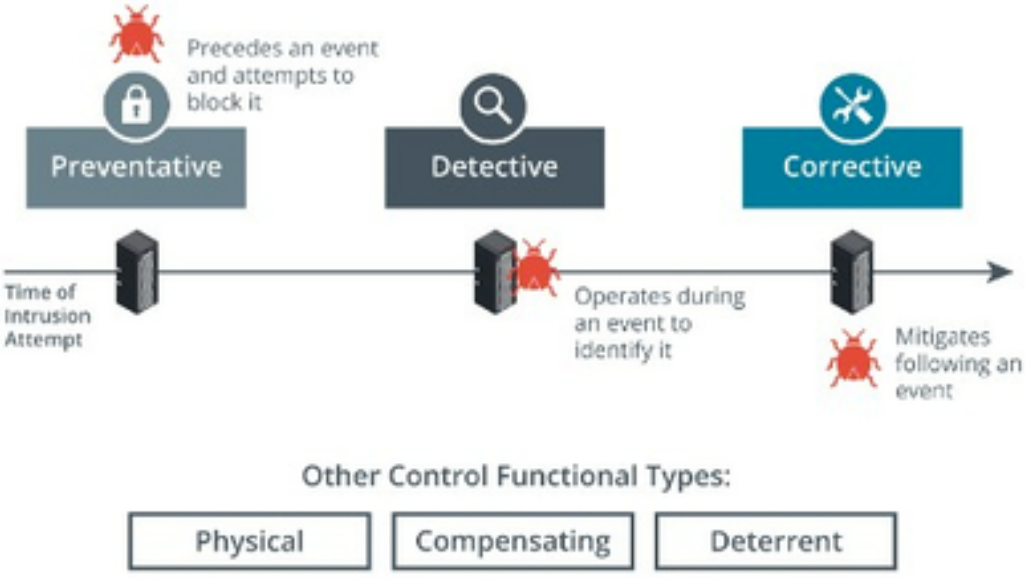
Tipos Funcionais de Controle de Segurança

Os controles de segurança podem ser classificados em três tipos funcionais: preventivos, detectivos e corretivos.

Controles preventivos são projetados para evitar a ocorrência de incidentes de segurança. Eles incluem firewalls, sistemas de autenticação forte e políticas de segurança.

Controles detectivos são usados para identificar e alertar sobre incidentes em andamento. Isso inclui sistemas de detecção de intrusões e monitoramento de rede.

Controles corretivos são acionados após um incidente ocorrer e têm como objetivo mitigar os danos e restaurar a normalidade. Isso inclui backups de dados, processos de resposta a incidentes e planos de continuidade de negócios.



Tipos Funcionais de Controle de Segurança (Continuação)

Além dos tipos funcionais mencionados anteriormente, existem outros que desempenham papéis importantes na segurança cibernética.

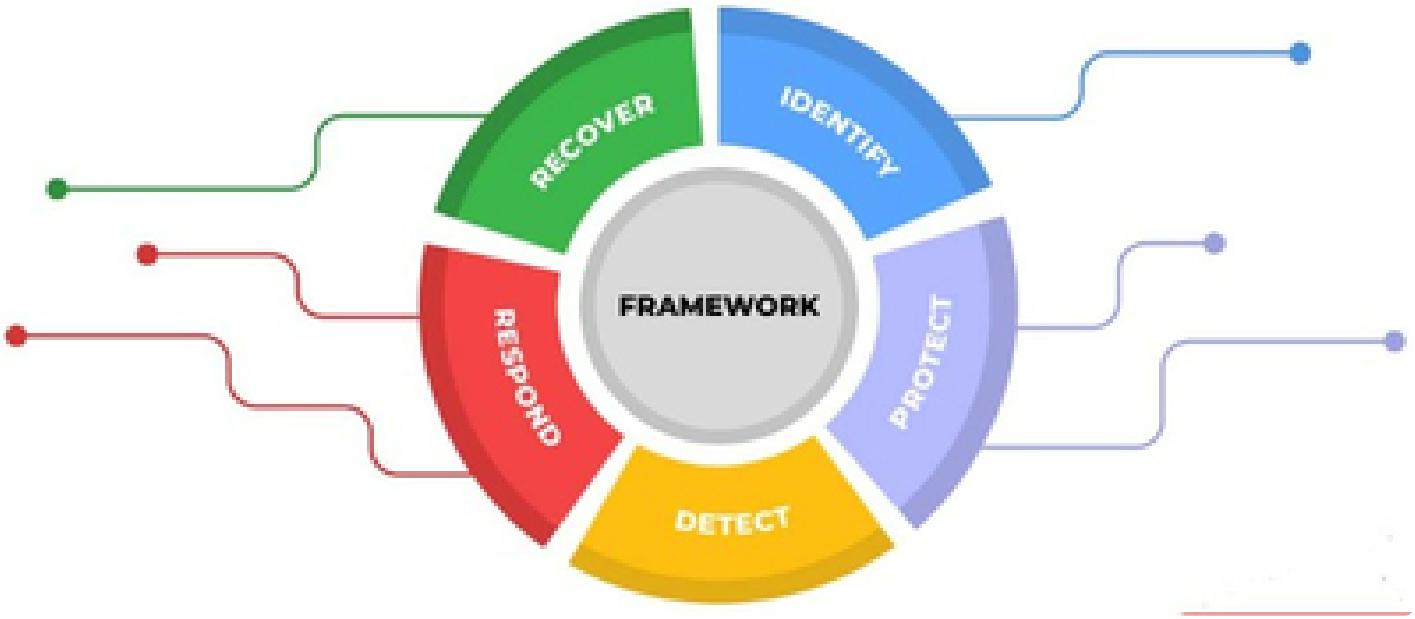
Os controles físicos são voltados para a proteção física de ativos, como servidores e data centers, e podem incluir câmeras de vigilância, sistemas de controle de acesso e proteção contra incêndio.

Os controles dissuasivos são projetados para desencorajar ataques e incluem avisos de segurança, identificação de ameaças e sistemas de alarme visíveis.

Já os controles compensatórios são implementados como contramedidas adicionais para compensar a falta de eficácia de outros controles e mitigar riscos.

Estrutura de Cibersegurança do NIST

O National Institute of Standards and Technology (NIST) desenvolveu uma estrutura abrangente de cibersegurança amplamente utilizada. Essa estrutura fornece orientações e melhores práticas para ajudar as organizações a gerenciar e mitigar riscos de segurança cibernética. Ela inclui uma abordagem de gerenciamento de riscos, identificação de ativos, proteção contra ameaças, detecção de incidentes e resposta a eles, recuperação e melhoria contínua.



NIST

ISO e Estruturas de Nuvem

A International Organization for Standardization (ISO) desenvolveu uma série de normas relacionadas à segurança da informação, como a ISO/IEC 27001 e a ISO/IEC 27002. Essas normas fornecem diretrizes e controles para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação. Além disso, existem estruturas específicas para segurança em

ambientes de nuvem, como o Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) e o Conselho Nacional de Segurança em Nuvem (National Cloud Security Center - NCSC).

Benchmarks e Guias de Configuração Segura

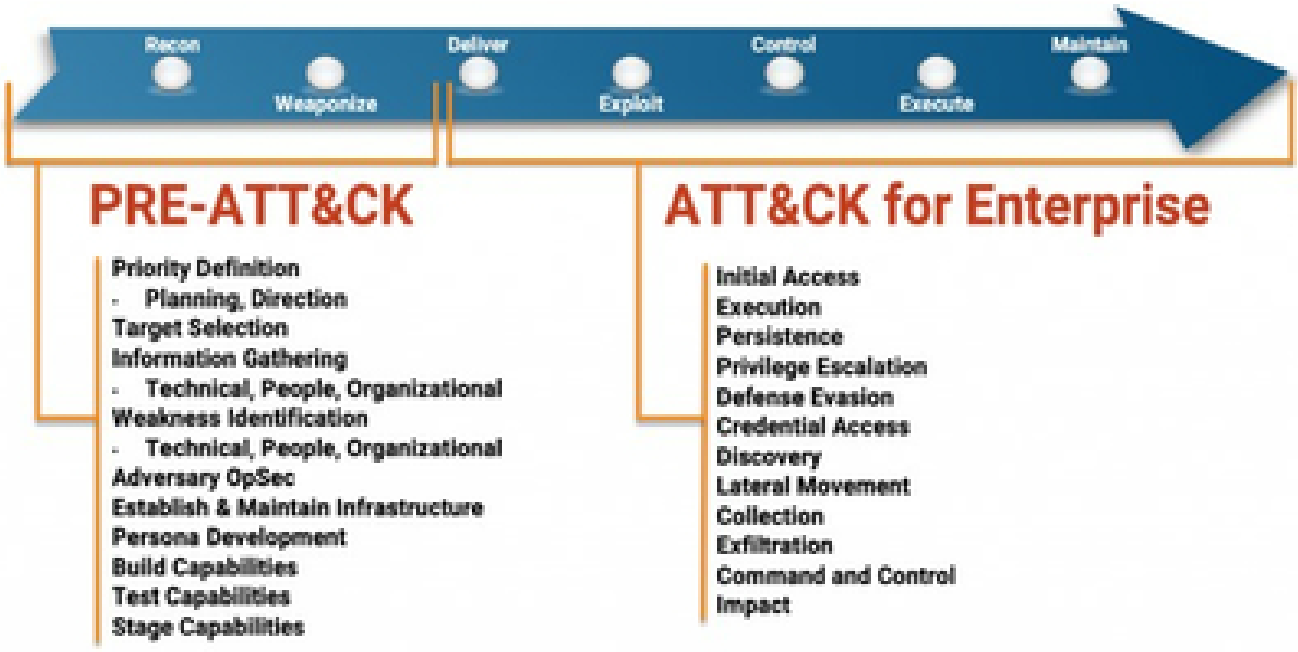
Para ajudar na configuração adequada de sistemas e aplicativos, existem benchmarks e guias de configuração segura, como os fornecidos pelo Center for Internet Security (CIS). Esses benchmarks fornecem orientações detalhadas sobre como configurar corretamente sistemas operacionais, bancos de dados, navegadores e outros componentes para aumentar sua segurança.

Regulações, Normas e Legislação

Regulações e leis relacionadas à segurança cibernética desempenham um papel fundamental na proteção de dados e na conformidade das organizações. Exemplos incluem o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil. Essas regulamentações estabelecem requisitos para a coleta, armazenamento e processamento de informações pessoais, visando proteger a privacidade e a segurança dos dados.

Mitre Att&ck

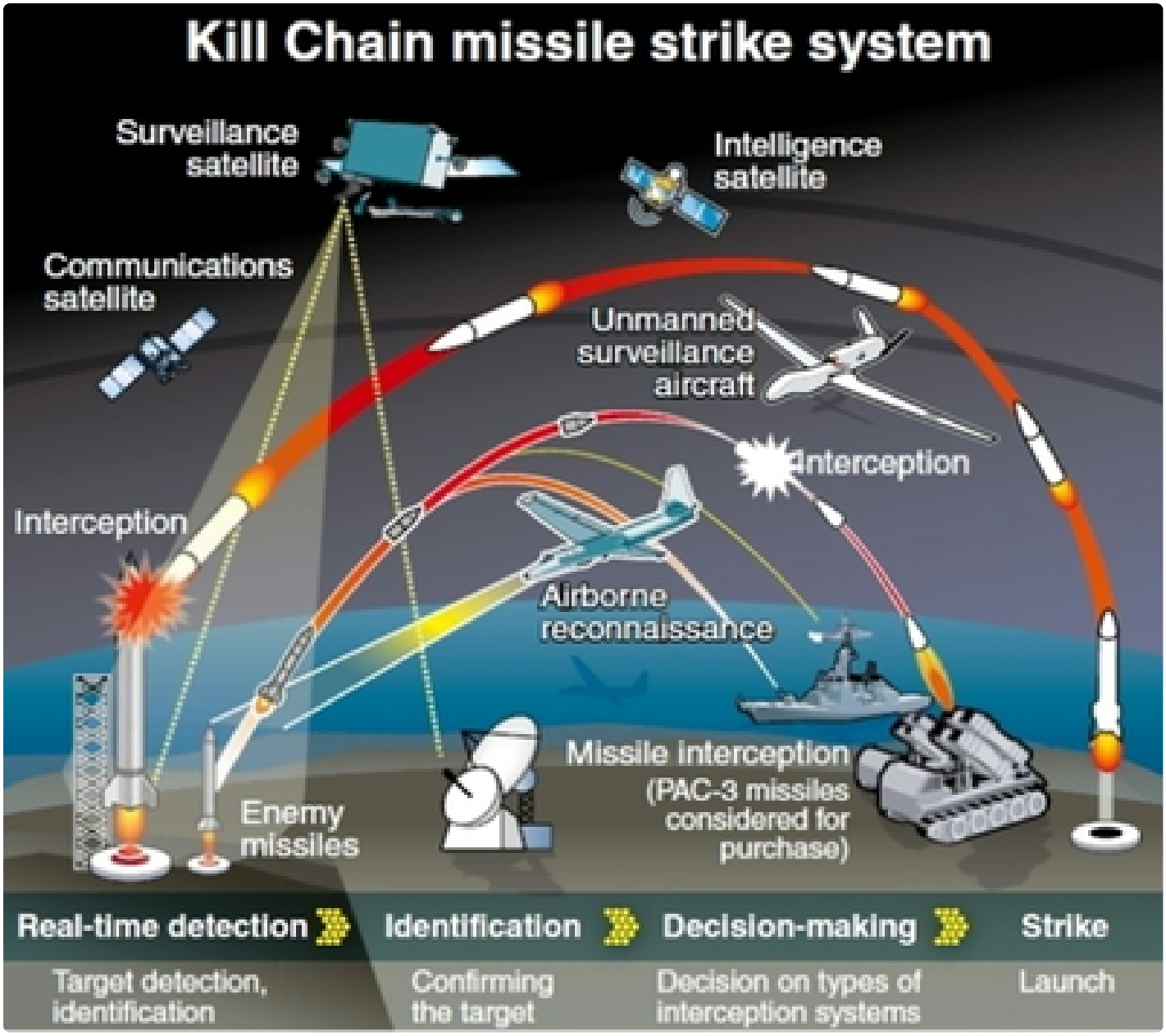
O MITRE ATT&CK é um framework de conhecimento de adversários que descreve táticas, técnicas e procedimentos (TTPs) usados por adversários cibernéticos. Ele fornece uma estrutura para entender as diferentes etapas de um ataque e como os atores mal-intencionados operam em diferentes fases, desde a exploração inicial até a exfiltração de dados.



MITRE

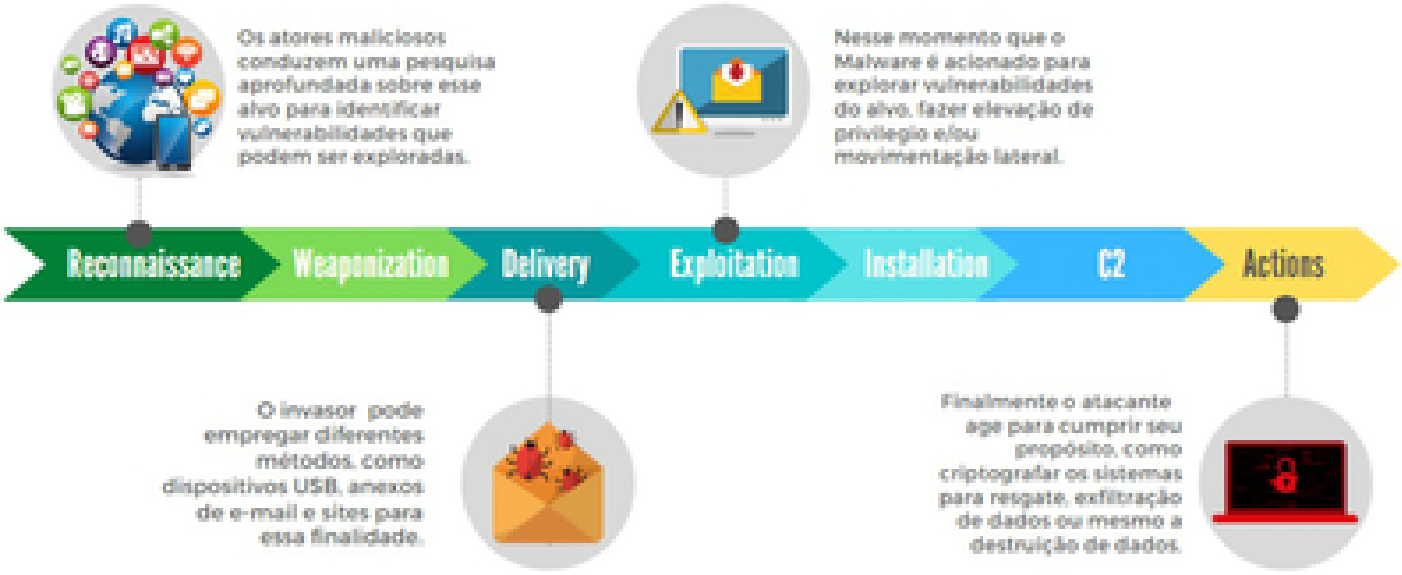
Cyber Kill Chain

> **VOCÊ SABIA? Kill Chain tem origem no mundo militar**
>
> Compreender como os ataques funcionam é fundamental para a defesa e aumentar a resiliência contra ataques cibernéticos avançados por meio da modelagem de ameaças é um enorme desafio.
>
> Kill Chain em português cadeia de destruição é um conceito militar relacionado à estrutura de um ataque definida por estágios. Um modelo de Kill Chain militar é o "F2T2EA", que inclui as seguintes fases:
>
> **Find** – Identifique um alvo. Encontre um alvo dentro de dados de vigilância ou reconhecimento ou através de meios de inteligência.
>
> **FIX** – Corrigir a localização do alvo. Obtenha coordenadas específicas para o alvo a partir de dados existentes ou coletando dados adicionais.
>
> **Track** – Monitorar o movimento do alvo. Mantenha o controle do alvo até que seja tomada uma decisão de não engajar o alvo ou o alvo seja engajado com sucesso.
>
> **Target** - Selecione uma arma ou recurso apropriado para usar no alvo para criar os efeitos desejados.
>
> **Engage** – Aplique a arma no alvo.
>
> **Assess** – Avalie os efeitos do ataque, incluindo qualquer inteligência coletada no local.



Kill-chain

A Cyber Kill Chain é um modelo que descreve as diferentes etapas de um ataque cibernético, desde a identificação e seleção de um alvo até a ação final do adversário. Ela inclui as etapas de reconhecimento, invasão, expansão, exfiltração e manutenção persistente. Compreender a Cyber Kill Chain ajuda as organizações a desenvolverem estratégias de defesa em camadas e a interromper os ataques em estágios iniciais.



Kill-chain

Ufa! Essa aula foi longa hein. Falamos sobre diversos assuntos. Essa é uma visão geral para que você possa começar a compreender a complexidade da segurança cibernética. Continue estudando e mergulhando nesse mundo fascinante da proteção digital!

Até a próxima, pessoal!