Red Team Operations – Concepts #1

Joas A Santos

Whoami

- I just like creating materials and sharing them for free, that's all

My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/

What is Red Team?

- The Red Team aims to study real adversaries and TTPs (Tactics, Techniques and Procedures) and simulate or emulate a real adversary, focusing on attacking mainly a company's people, processes and technologies.
- Unlike PenTester which aims to explore vulnerabilities in the context of understanding the vulnerabilities that the organization has.
- The objective of the Red Team is to evaluate detections, incident response, policies and processes defined by the Blue Team and the entire security operation team. Without Blue Team's consent for any action.

O que é o Red Team?

- O Red Team tem como objetivo estudar adversários reais e TTPs (Táticas, Técnicas e Procedimentos) e simular ou emular um adversário real, focando em atacar principalmente as pessoas, processos e tecnologias de uma empresa.
- Diferente do PenTester que visa explorar vulnerabilidades no contexto de entender as vulnerabilidades que a organização possui.
- O objetivo do Red Team é avaliar as detecções, a resposta a incidente, as políticas e os processos definidos pelo Blue Team e todo time de operação de segurança. Sem o consentimento do Blue Team para qualquer ação.

What is Ethical Hackers?

- Ethical hackers are individuals with advanced skills and knowledge in different types of security tests, mainly with an offensive focus.
- He is not just a PenTester, but he can be a professional with capabilities to perform Red Team actions and simulate an opponent.
- Ethical was defined as a strategy used by some companies to differentiate it from the traditional Hacker, which generally does not have pre-established rules for its tests and ways of acting, creating this definition that covers every individual with the knowledge and technical capacity of a hacker, but uses your knowledge and skills to help companies.

O que são os Ethical Hackers?

- Os hackers éticos são indivíduos com skills e conhecimentos avançados em diferentes tipos de testes de segurança, principalmente com foco ofensivo.
- Ele não é apenas um PenTester, mas pode ser um profissional com capacidades para executar ações de Red Team e simular um adversário.
- O ético ele foi definido como uma estratégia de algumas empresas para diferenciar do Hacker tradicional que geralmente não tem regras pré-estabelecidas para os seus testes e formas de agir, criando essa definição que abrange todo individuo com conhecimento e capacidade técnica de um hacker, mas usa seus conhecimentos e habilidades para ajudar as empresas.

What is Adversary Emulation?

- The objective of adversary emulation is to choose a real threat profile and collect its TTPs to understand the behavior of attacks from an APT (Advanced Persistent Threat) group on your organization's infrastructure, in order to assess whether your company is prepared for an attack sophisticated of an APT group.
- Threat Intelligence is very important in this sense, in order to build and plan an accurate emulation of an adversary.

O que é Adversary Emulation?

- O objetivo da emulação de adversário é escolher um perfil de ameaça real e coletar seus TTPs para entender o comportamentos dos ataques de um grupo APT (Ameaça Persistente Avançada) na infraestrutura da sua organização, afim de avaliar se a sua empresa esta preparada para um ataque sofisticado de um grupo APT.
- O Threat Intelligence é bastante importante nesse sentido, afim de construir e planejar uma emulação precisa de um adversário.

Adversary Emulation vs Adversary Simulation

- Although they are similar concepts, the difference is to emulate and simulate this in their specific approach.
- **Adversary Emulation:** Focuses specifically on imitating the behavior of an APT group and its TTPs specifically.
- **Adversary Simulation:** It already works with more than one set of TTPs with a focus on creating a more personalized scenario for your organization, making it difficult for the Blue Team to detect your actions.
- Both can be used during an exercise, however it is good to remember that for any success, the pattern has to be completely different from the ordinary.

Adversary Emulation vs Adversary Simulation

- Apesar de serem conceitos parecidos a diferença de emular e simular esta na sua abordagem especificamente.
- **Emulação de Adversário:** Foca especificamente em imitar o comportamento de um grupo APT e seus TTPs especificamente.
- Simulação de Adversário: Ela já atua em trabalhar com mais de um conjunto de TTPs com foco em criar um cenário mais personalizado para sua organização, dificultando para que o Blue Team detecte suas ações.
- Ambos podem ser usados durante um exercício, contudo é bom lembrar que para qualquer sucesso, o padrão tem que ser totalmente diferente do comum.

Mitre Att&ck

- attack.mitre.org is a valuable source of information about APT (Advanced Persistent Threats) groups and their operations. The site is maintained by MITER Corporation and features the ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework, which is a globally accessible knowledge base on adversarial behaviors based on real-world observations. This framework is widely used by cyber defense professionals (blue team) to understand and classify threat actions, improving the security posture against sophisticated adversaries.

Mitre Att&ck

- O attack.mitre.org é uma fonte valiosa de informações sobre grupos APT (Advanced Persistent Threats) e suas operações. O site é mantido pelo MITRE Corporation e apresenta o framework ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge), que é uma base de conhecimento globalmente acessível sobre os comportamentos adversários baseados em observações do mundo real. Este framework é amplamente utilizado por profissionais de defesa cibernética(blue team) para entender e classificar as ações de ameaças, melhorando a postura de segurança contra adversários sofisticados

What is TTPs?

- Each APT group profile is linked to a set of TTPs that the group is known to use. These are categorized according to the ATT&CK framework, which includes:
- **Tactics**: Represent the objectives that an adversary may try to achieve, such as "Initial Access", "Execution", "Persistence", among others.
- **Techniques**: These are the specific methods that opponents use to achieve their tactical objectives. For example, under the "Initial Access" tactic, a technique might be "Spearphishing Attachment".
- **Procedures**: These are more detailed or specific variants of techniques, often including information about how a particular group applied that technique in real attacks.

O que são os TTPs?

- Cada perfil de grupo APT é vinculado a um conjunto de TTPs que o grupo é conhecido por usar. Estas são categorizadas de acordo com o framework ATT&CK, que inclui:
- **Táticas**: Representam os objetivos que um adversário pode tentar alcançar, como "Acesso Inicial", "Execução", "Persistência", entre outros.
- **Técnicas**: São os métodos específicos que os adversários usam para alcançar seus objetivos táticos. Por exemplo, sob a tática de "Acesso Inicial", uma técnica pode ser "Spearphishing Attachment".
- **Procedimentos**: São variantes mais detalhadas ou específicas de técnicas, muitas vezes incluindo informações sobre como um grupo particular aplicou essa técnica em ataques reais.

Unified Cyber Kill Chain

The Unified Kill Chain		
1	***Reconnaissance***	*Researching, identifying and selecting targets using active or passive reconnaissance.*
2	***Weaponization***	*Preparatory activities aimed at setting up the infrastructure required for the attack.*
3	***Delivery***	*Techniques resulting in the transmission of a weaponized object to the targeted environment.*
4	***Social Engineering***	*Techniques aimed at the manipulation of people to perform unsafe actions.*
5	***Exploitation***	*Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.*
6	***Persistence***	*Any access, action or change to a system that gives an attacker persistent presence on the system.*
7	***Defense Evasion***	*Techniques an attacker may specifically use for evading detection or avoiding other defenses.*
8	***Command & Control***	*Techniques that allow attackers to communicate with controlled systems within a target network.*
9	***Pivoting***	*Tunneling traffic through a controlled system to other systems that are not directly accessible.*
10	***Discovery***	*Techniques that allow an attacker to gain knowledge about a system and its network environment.*
11	***Privilege Escalation***	*The result of techniques that provide an attacker with higher permissions on a system or network.*
12	***Execution***	*Techniques that result in execution of attacker-controlled code on a local or remote system.*
13	***Credential Access***	*Techniques resulting in the access of, or control over, system, service or domain credentials.*
14	***Lateral Movement***	*Techniques that enable an adversary to horizontally access and control other remote systems.*
15	***Collection***	*Techniques used to identify and gather data from a target network prior to exfiltration.*
16	***Exfiltration***	*Techniques that result or aid in an attacker removing data from a target network.*
17	***Impact***	*Techniques aimed at manipulating, interrupting or destroying the target system or data.*
18	***Objectives***	*Socio-technical objectives of an attack that are intended to achieve a strategic goal.*

https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/

Unified Cyber Kill Chain

- Reconnaissance - Searching, identifying and selecting targets using active or passive reconnaissance.
- Arming (Weaponization) - Preparatory activities aimed at configuring the infrastructure necessary for the attack.
- Delivery - Techniques that result in the transmission of a weaponized object into the target environment.
- Social Engineering - Techniques aimed at manipulating people to carry out unsafe actions.
- Exploitation - Techniques for exploiting vulnerabilities in systems that may, among others, result in code execution.
- Persistence - Any access, action, or change to a system that gives the attacker a persistent presence on the system.
- Defense Evasion - Techniques that an attacker can use specifically to avoid detection or other defenses.
- Command and Control - Techniques that allow attackers to communicate with controlled systems within a target network.
- Pivoting - Tunneling traffic through a controlled system to other systems that are not directly accessible.
- Discovery - Techniques that allow an attacker to gain knowledge about a system and its network environment.
- Privilege Escalation - The result of techniques that provide an attacker with greater permissions on a system or network.
- Execution - Techniques that result in the execution of attacker-controlled code on a local or remote system.
- Credential Access - Techniques that result in the access or control of system, service or domain credentials.
- Lateral Movement - Techniques that enable an adversary to horizontally access and control other remote systems.
- Harvesting - Techniques used to identify and gather data from a target network prior to exfiltration.
- Exfiltration - Techniques that result in or assist an attacker in removing data from a target network.
- Impact - Techniques aimed at manipulating, disrupting or destroying the target system or data.
- Objectives - Socio-technical objectives of an attack that are intended to achieve a strategic objective.

Unified Cyber Kill Chain

- Reconhecimento - Pesquisando, identificando e selecionando alvos usando reconhecimento ativo ou passivo.
- Armar (Weaponization) - Atividades preparatórias destinadas a configurar a infraestrutura necessária para o ataque.
- Entrega - Técnicas que resultam na transmissão de um objeto armado para o ambiente alvo.
- Engenharia Social - Técnicas direcionadas à manipulação de pessoas para realizar ações inseguras.
- Exploração - Técnicas para explorar vulnerabilidades em sistemas que podem, entre outros, resultar em execução de código.
- Persistência - Qualquer acesso, ação ou mudança em um sistema que dá ao atacante uma presença persistente no sistema.
- Evasão de Defesa - Técnicas que um atacante pode usar especificamente para evitar detecção ou outras defesas.
- Comando e Controle - Técnicas que permitem aos atacantes se comunicar com sistemas controlados dentro de uma rede alvo.
- Pivoteamento - Tráfego de túnel através de um sistema controlado para outros sistemas que não são diretamente acessíveis.
- Descoberta - Técnicas que permitem a um atacante obter conhecimento sobre um sistema e seu ambiente de rede.
- Escalação de Privilégios - O resultado de técnicas que fornecem a um atacante maiores permissões em um sistema ou rede.
- Execução - Técnicas que resultam na execução de código controlado pelo atacante em um sistema local ou remoto.
- Acesso a Credenciais - Técnicas que resultam no acesso ou controle de credenciais de sistema, serviço ou domínio.
- Movimento Lateral - Técnicas que possibilitam a um adversário acessar e controlar horizontalmente outros sistemas remotos.
- Coleta - Técnicas usadas para identificar e reunir dados de uma rede alvo antes da exfiltração.
- Exfiltração - Técnicas que resultam ou auxiliam um atacante na remoção de dados de uma rede alvo.
- Impacto - Técnicas visando manipular, interromper ou destruir o sistema alvo ou dados.
- Objetivos - Objetivos sócio-técnicos de um ataque que são destinados a alcançar um objetivo estratégico.

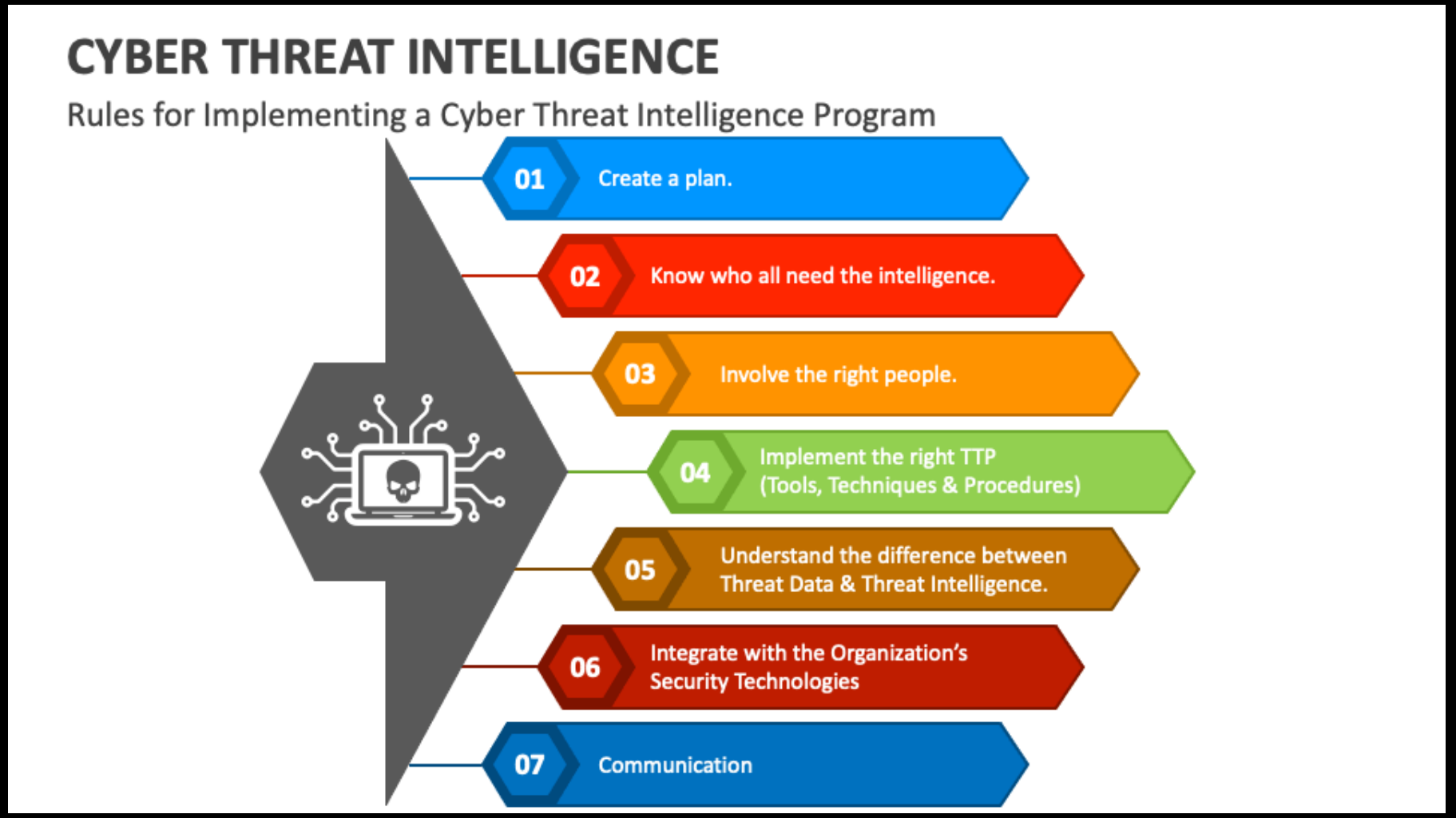
Extras Frameworks

1. **CBEST Intelligence Led Testing (Bank of England):** CBEST is a framework developed by the Bank of England for the UK financial sector, focusing on improving resilience against cyber threats. It uses real threat intelligence to simulate attacks on critical financial infrastructures, helping institutions understand their vulnerabilities and how attackers could exploit them.
2. **Threat Intelligence-Based Ethical Red Teaming (TIBER-EU):** TIBER-EU is the European framework equivalent to CBEST, aimed at testing and improving the cyber resilience of significant financial market entities. It involves tailored red-team testing (simulated cyber-attacks) based on current threat intelligence, providing a realistic assessment of an institution's defenses against sophisticated attackers.
3. **Red Team: Adversarial Attack Simulation Exercises (Association of Banks in Singapore - ABS):** This Singaporean initiative involves conducting red team exercises to simulate sophisticated cyber-attack scenarios specifically tailored for financial institutions. These exercises are designed to test the effectiveness of the institutions' cyber defenses and their ability to respond to and recover from attacks.
4. **A Framework for the Regulatory Use of Penetration Testing and Red Teaming in the Financial Services Industry (Global Financial Markets Association - GFMA):** This framework provides guidelines for the global financial industry, recommending practices for conducting penetration testing and red teaming exercises. It aims to standardize how these cybersecurity assessments are performed across different jurisdictions, promoting a consistent approach to identifying and mitigating cyber risks in the financial sector.

Extras Frameworks

1. **CBEST Intelligence Led Testing (Bank of England):** CBEST é um framework desenvolvido pelo Bank of England para o setor financeiro do Reino Unido, focando em melhorar a resiliência contra ameaças cibernéticas. Ele utiliza inteligência de ameaças reais para simular ataques a infraestruturas financeiras críticas, ajudando as instituições a entenderem suas vulnerabilidades e como os atacantes poderiam explorá-las.
2. **Teste de Equipe Vermelha Baseado em Inteligência de Ameaças (TIBER-EU):** TIBER-EU é o framework europeu equivalente ao CBEST, voltado para testar e melhorar a resiliência cibernética de entidades significativas do mercado financeiro. Envolve testes personalizados de equipe vermelha (ataques cibernéticos simulados) baseados em inteligência de ameaças atual, fornecendo uma avaliação realista das defesas de uma instituição contra atacantes sofisticados.
3. **Red Team: Exercícios de Simulação de Ataques Adversários (Associação de Bancos de Singapura - ABS):** Esta iniciativa singapuriana envolve a condução de exercícios de equipe vermelha para simular cenários de ataques cibernéticos sofisticados especificamente adaptados para instituições financeiras. Estes exercícios são desenhados para testar a eficácia das defesas cibernéticas das instituições e sua capacidade de responder e se recuperar de ataques.
4. **Um Framework para o Uso Regulatório de PenTest e Red Team na Indústria de Serviços Financeiros (Associação Global de Mercados Financeiros - GFMA):** Este framework fornece diretrizes para a indústria financeira global, recomendando práticas para a condução de testes de penetração e exercícios de equipes vermelhas. Ele visa padronizar como essas avaliações de segurança cibernética são realizadas em diferentes jurisdições, promovendo uma abordagem consistente para identificar e mitigar riscos cibernéticos no setor financeiro.

Cyber Threat Intelligence



https://www.collidu.com/presentation-cyber-threat-intelligence

Cyber Threat Intelligence

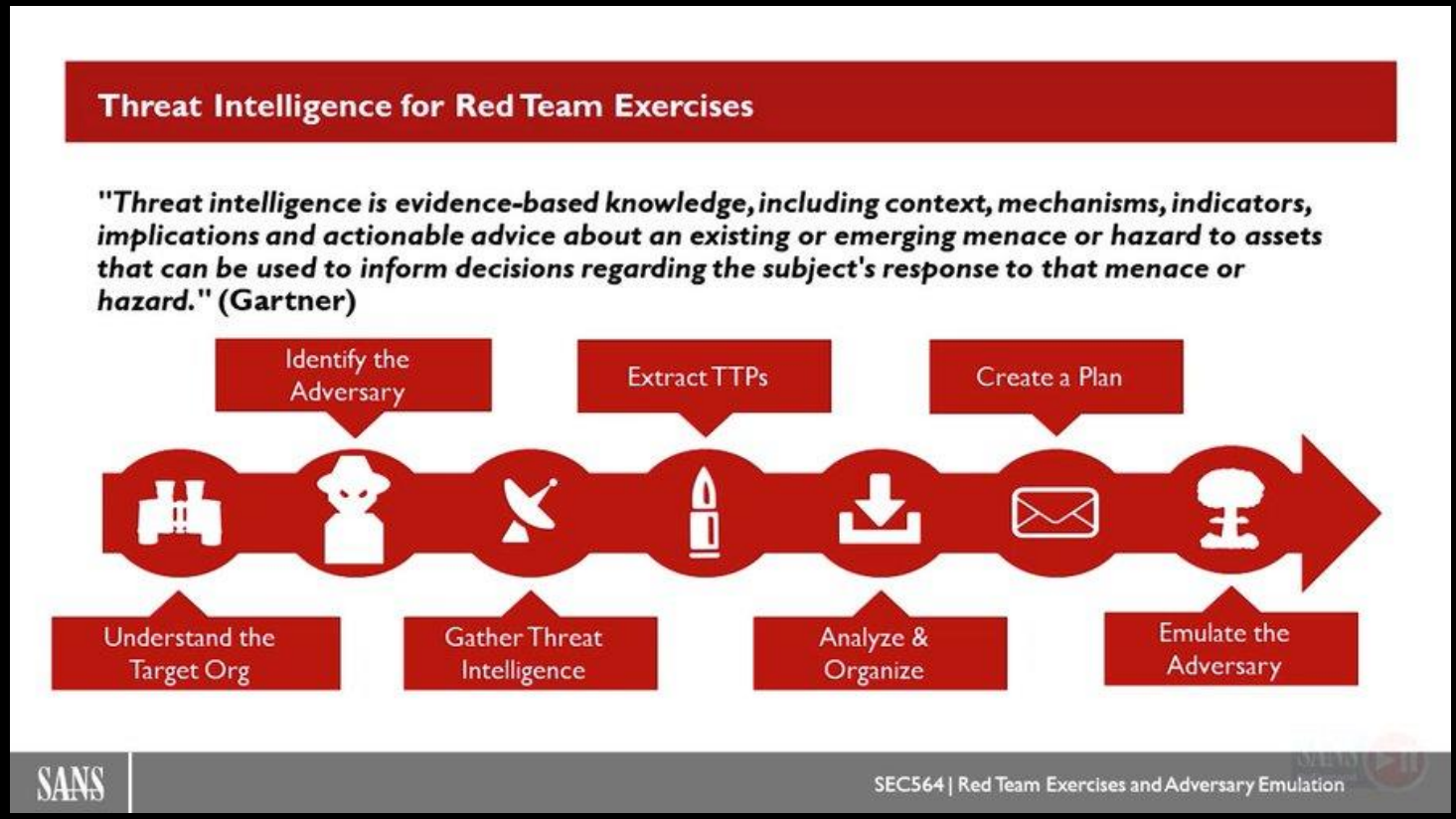
1. **Create a Plan:** Outline the objectives, scope, and timeline of your threat intelligence program. Clearly define what you aim to achieve and how you plan to go about it.
2. **Know Who Needs the Intelligence:** Identify the stakeholders within your organization who will benefit from threat intelligence. Understand their specific needs and how intelligence can support their roles.
3. **Engage the Right People:** Assemble a team with the right mix of skills and expertise. This should include cybersecurity professionals, analysts, and members from relevant departments who can provide insights and support.
4. **Implement the Correct TTPs (Tools, Techniques, and Procedures):** Choose the appropriate tools, techniques, and procedures that align with your threat intelligence goals.
5. **Understand the Difference Between Threat Data and Threat Intelligence:** Recognize that threat data consists of raw information about potential threats, while threat intelligence involves analyzed data that provides context and actionable insights. Knowing the difference is crucial for effective decision-making.
6. **Integrate with the Organization's Security Technologies:** Ensure that your threat intelligence program works in tandem with existing security technologies within your organization. This includes integrating intelligence feeds into security information and event management (SIEM) systems, firewalls, and endpoint protection platforms to enhance overall security posture.
7. **Communication:** Establish robust communication channels to share intelligence within the organization. Effective communication ensures that relevant stakeholders are informed about the latest threats and intelligence findings, enabling timely and informed decisions.

Cyber Threat Intelligence

1. **Criar um Plano:** Defina os objetivos, o escopo e o cronograma do seu programa de inteligência de ameaças. Especifique claramente o que você pretende alcançar e como planeja fazê-lo.
2. **Saiba Quem Precisa da Inteligência:** Identifique os stakeholders dentro da sua organização que se beneficiarão da inteligência de ameaças. Compreenda as necessidades específicas deles e como a inteligência pode apoiar seus papéis.
3. **Envolver as Pessoas Certas:** Monte uma equipe com a combinação certa de habilidades e expertise. Isso deve incluir profissionais de cibersegurança, analistas e membros de departamentos relevantes que possam fornecer insights e suporte.
4. **Implementar os TTPs Corretos (Ferramentas, Técnicas e Procedimentos):** Escolha as ferramentas, técnicas e procedimentos apropriados que estejam alinhados com os objetivos da sua inteligência de ameaças.
5. **Entender a Diferença Entre Dados de Ameaças e Inteligência de Ameaças:** Reconheça que dados de ameaças consistem em informações brutas sobre ameaças potenciais, enquanto a inteligência de ameaças envolve dados analisados que fornecem contexto e insights acionáveis. Conhecer a diferença é crucial para a tomada de decisão eficaz.
6. **Integrar com as Tecnologias de Segurança da Organização:** Garanta que seu programa de inteligência de ameaças trabalhe em conjunto com as tecnologias de segurança existentes dentro da sua organização. Isso inclui integrar feeds de inteligência a sistemas de gestão de informações e eventos de segurança (SIEM), firewalls e plataformas de proteção de endpoints para melhorar a postura de segurança geral.
7. **Comunicação:** Estabeleça canais de comunicação robustos para compartilhar a inteligência dentro da organização. Uma comunicação eficaz garante que os stakeholders relevantes sejam informados sobre as últimas ameaças e descobertas de inteligência, possibilitando decisões informadas e oportunas.

Threat Intelligence no Exercício Red Team

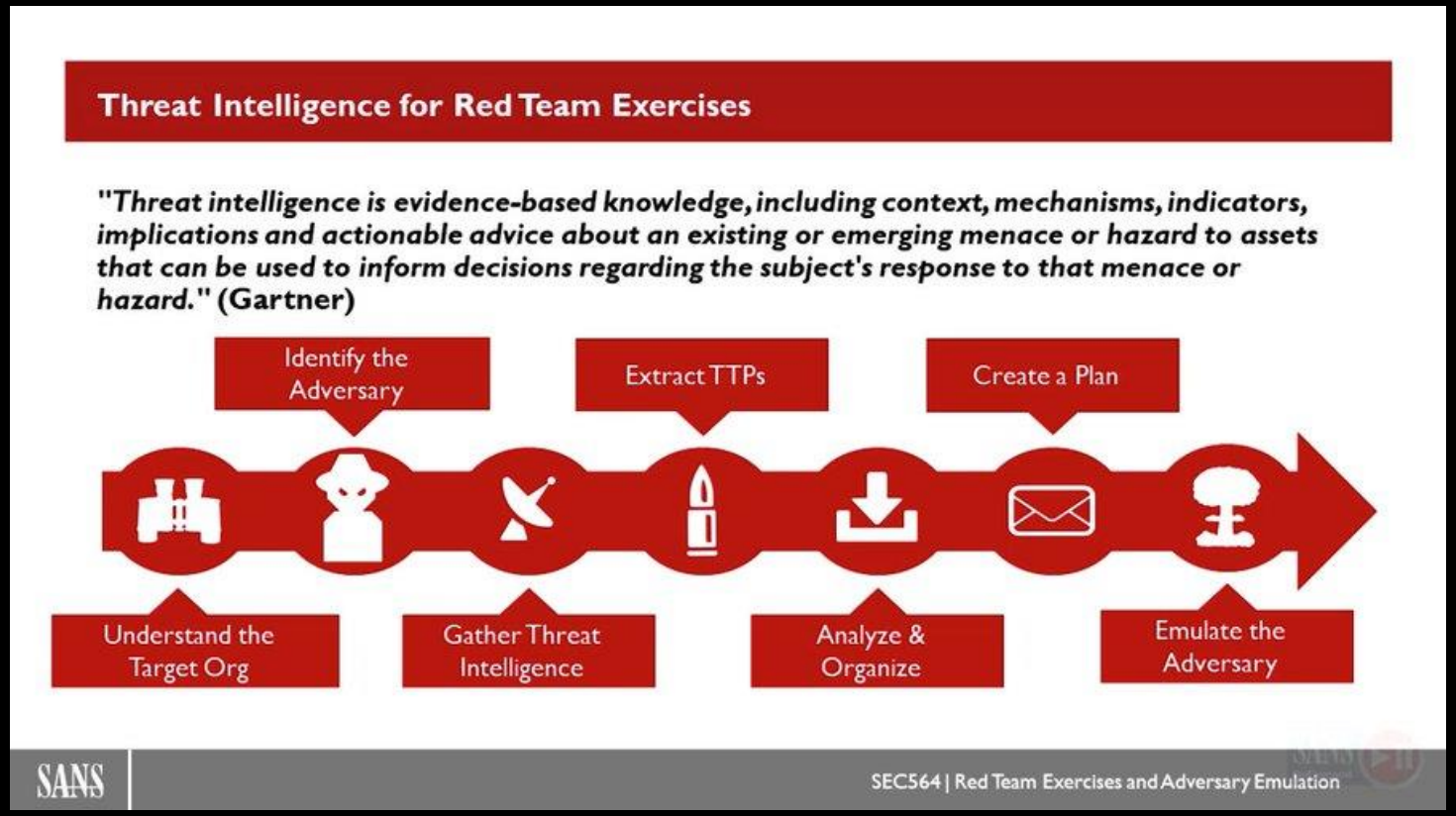
- A inteligência de ameaças é um conhecimento baseado em evidências, incluindo contexto, mecanismos, indicadores, implicações e conselhos acionáveis sobre uma ameaça ou perigo existente ou emergente para ativos que pode ser usado para informar decisões a respeito da resposta do sujeito a essa ameaça ou perigo.



https://twitter.com/SANSInstitute/status/1258480484822257669

Threat Intelligence for Red Team Exercises

- Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.



https://twitter.com/SANSInstitute/status/1258480484822257669

Adversary Emulation Plan - Example

- Adversary Emulation, also known as Red Team Operations Informally, is a proactive cybersecurity approach where an organization simulates real-world attack scenarios to identify vulnerabilities in their systems, processes, and defenses. The goal of adversary emulation is to assess an organization's security posture by adopting the mindset and tactics of a potential attacker.
  - Scope Definition: Define the objectives, constraints, and boundaries of the emulation exercise. Determine the systems, networks, or specific assets to be targeted and identify the rules of engagement.
  - Reconnaissance: Conduct preliminary information gathering to understand the target environment. This may involve gathering publicly available data, analyzing open-source intelligence, or performing network scanning to identify potential entry points.
  - Threat Modeling: Analyze the target infrastructure and applications to identify potential vulnerabilities and attack vectors. This involves mapping out the architecture, identifying weaknesses, and prioritizing potential attack paths.
  - Tactic Selection: Based on the threat modeling exercise, determine the specific attack techniques, tactics, and procedures (TTPs) that will be employed during the emulation. This may include social engineering, network exploitation, privilege escalation, or other tactics commonly used by adversaries.
  - Planning: Develop a detailed plan that outlines the sequence of attack steps, timelines, and required resources. This plan should consider potential contingencies and include any necessary approvals from stakeholders.
  - Execution: Implement the planned attack scenarios, following the predefined TTPs. This may involve deploying specialized tools, exploiting vulnerabilities, attempting to gain unauthorized access, or exfiltrating sensitive information.
  - Detection Evasion: Emulate advanced persistent threats (APTs) by employing techniques to evade detection by security controls and monitoring systems. This may involve bypassing intrusion detection systems, avoiding antivirus detection, or leveraging zero-day vulnerabilities.
  - Post-Exploitation and Persistence: Once access is gained, attempt to establish persistence within the target environment, such as creating backdoors, installing persistent malware, or creating privileged accounts. This step aims to simulate the actions an attacker might take to maintain long-term access.
  - Reporting: Document the findings, observations, and recommendations from the emulation exercise. A comprehensive report should detail the identified vulnerabilities, successful attack paths, and recommendations for improving security controls and mitigating risks.
  - Remediation: Work with the organization's security team to address the identified vulnerabilities and implement appropriate countermeasures. This may involve patching systems, updating configurations, improving network segmentation, or enhancing employee training and awareness.
  - Follow-Up Testing: Conduct additional testing to validate the effectiveness of the implemented remediation measures and ensure that the identified vulnerabilities have been adequately addressed.

Adversary Emulation Plan - Exemplo

- Adversary Emulation, também conhecida como Red Team Operations informalmente, é uma abordagem proativa de segurança cibernética em que uma organização simula cenários de ataque do mundo real para identificar vulnerabilidades em seus sistemas, processos e defesas. O objetivo da emulação do adversário é avaliar a postura de segurança de uma organização, adotando a mentalidade e as táticas de um invasor em potencial.
  - Definição do escopo: Defina os objetivos, restrições e limites do exercício de emulação. Determine os sistemas, redes ou ativos específicos a serem visados e identifique as regras de engajamento.
  - Reconhecimento: Conduza a coleta preliminar de informações para compreender o ambiente alvo. Isso pode envolver a coleta de dados disponíveis publicamente, a análise de inteligência de código aberto ou a realização de varredura de rede para identificar possíveis pontos de entrada.
  - Modelagem de ameaças: analise a infraestrutura e os aplicativos alvo para identificar possíveis vulnerabilidades e vetores de ataque. Isso envolve mapear a arquitetura, identificar pontos fracos e priorizar possíveis caminhos de ataque.
  - Seleção de táticas: com base no exercício de modelagem de ameaças, determine as técnicas, táticas e procedimentos de ataque (TTPs) específicos que serão empregados durante a emulação. Isto pode incluir engenharia social, exploração de redes, escalada de privilégios ou outras táticas comumente usadas pelos adversários.
  - Planejamento: Desenvolva um plano detalhado que descreva a sequência de etapas do ataque, cronogramas e recursos necessários. Este plano deve considerar possíveis contingências e incluir quaisquer aprovações necessárias das partes interessadas.
  - Execução: Implementar os cenários de ataque planejados, seguindo os TTPs predefinidos. Isso pode envolver a implantação de ferramentas especializadas, a exploração de vulnerabilidades, a tentativa de obter acesso não autorizado ou a exfiltração de informações confidenciais.
  - Evasão de detecção: Emule ameaças persistentes avançadas (APTs) empregando técnicas para evitar a detecção por controles de segurança e sistemas de monitoramento. Isso pode envolver contornar os sistemas de detecção de intrusões, evitar a detecção de antivírus ou aproveitar vulnerabilidades de dia zero.
  - Pós-exploração e persistência: Depois que o acesso for obtido, tente estabelecer persistência no ambiente de destino, como criar backdoors, instalar malware persistente ou criar contas privilegiadas. Esta etapa visa simular as ações que um invasor pode realizar para manter o acesso a longo prazo.
  - Relatórios: Documente as conclusões, observações e recomendações do exercício de emulação. Um relatório abrangente deve detalhar as vulnerabilidades identificadas, os caminhos de ataque bem-sucedidos e as recomendações para melhorar os controles de segurança e mitigar os riscos.
  - Correção: Trabalhe com a equipe de segurança da organização para resolver as vulnerabilidades identificadas e implementar contramedidas apropriadas. Isso pode envolver a aplicação de patches em sistemas, a atualização de configurações, a melhoria da segmentação da rede ou o aprimoramento do treinamento e da conscientização dos funcionários.
  - Testes de Acompanhamento: Realize testes adicionais para validar a eficácia das medidas de remediação implementadas e garantir que as vulnerabilidades identificadas foram abordadas de forma adequada.

OpSec

- Operational Security (OpSec) in Red Team contexts refers to the practices and procedures adopted to protect sensitive information about the team's operations. The goal is to minimize the chances that adversaries, whether internal or external to the organization, detect, understand, or interfere with penetration testing and attack simulation activities.

OpSec Red Team

- Implement strict access controls to ensure that only authorized team members can interact with critical systems.
- Establish security mechanisms to ensure that scripts and executables can only operate within the confines of the designated environment, preventing unintended impacts.
- Maintain the anonymity of the company's digital properties to prevent direct association with specific vulnerabilities or internal security strategies.
- Utilize advanced encryption techniques to protect sensitive information stored or transmitted by externally accessible systems.
- Conduct detailed analyses of tools and approaches used during attack simulations to identify signs of potential security breaches, aiding the defensive team in enhancing their incident responses.
- Establish protocols for creating isolated environments (sandboxes) where malicious payloads can be tested without risk to the main infrastructure.
- Develop security policies that ensure the continuous updating and maintenance of all tools and systems used by the red team, avoiding vulnerabilities from outdated software.
- Promote debriefing sessions between the red and blue teams after each exercise, to share findings, strategies, and improve interdepartmental collaboration.
- Ensure that all data collected during testing are anonymized or de-identified to protect privacy and comply with data protection regulations.
- Implement a knowledge management system that allows for the secure documentation and sharing of lessons learned and best practices among red team members and other relevant stakeholders.

OpSec

- Operational Security (OpSec) em contextos de Red Team refere-se às práticas e procedimentos adotados para proteger informações sensíveis sobre as operações da equipe. O objetivo é minimizar as chances de que adversários, sejam eles internos ou externos à organização, detectem, compreendam ou interfiram nas atividades de pentest e simulação de ataques.

OpSec Red Team

• Implementar controles de acesso rigorosos para garantir que apenas membros autorizados da equipe de teste possam interagir com sistemas críticos.

• Estabelecer mecanismos de segurança para que scripts e executáveis só possam operar dentro dos limites do ambiente designado, evitando impactos não intencionais.

• Manter o anonimato das propriedades digitais da empresa para prevenir a associação direta a vulnerabilidades específicas ou a estratégias de segurança interna.

• Utilizar técnicas de encriptação avançadas para proteger informações sensíveis armazenadas ou transmitidas por sistemas acessíveis externamente.

• Conduzir análises detalhadas de ferramentas e abordagens usadas durante simulações de ataque para identificar sinais de possíveis brechas de segurança, auxiliando a equipe defensiva a aprimorar suas respostas a incidentes reais.

• Estabelecer protocolos para a criação de ambientes isolados (sandboxes) onde possam ser testadas cargas maliciosas sem risco para a infraestrutura principal.

• Desenvolver políticas de segurança que garantam a atualização e manutenção contínua de todas as ferramentas e sistemas utilizados pela equipe vermelha, evitando vulnerabilidades decorrentes de software desatualizado.

• Promover sessões de debriefing entre as equipes vermelha e azul após cada exercício, para compartilhar descobertas, estratégias e melhorar a colaboração interdepartamental.

• Assegurar que todos os dados coletados durante os testes sejam anonimizados ou despersonalizados para proteger a privacidade e cumprir com regulamentos de proteção de dados.

• Implementar um sistema de gestão de conhecimento que permita documentar e compartilhar de forma segura as lições aprendidas e melhores práticas entre membros da equipe vermelha e outros stakeholders relevantes.

References

- https://redteam.guide/
- https://github.com/CyberSecurityUP/Adversary-Emulation-Guide
- https://medium.com/@zycc2727/red-team-threat-intel-a95dd5501a3d
- https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
- https://www.breachlock.com/resources/blog/top-3-red-teaming-frameworks-tiberaasecbest/
- https://bob-19.gitbook.io/sans-sec565-red-team-operations-review/
- https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-soc/what-is-operational-security-opsec/
- https://medium.com/techiepedia/tryhackme-red-team-opsec-f3721a2e22ff