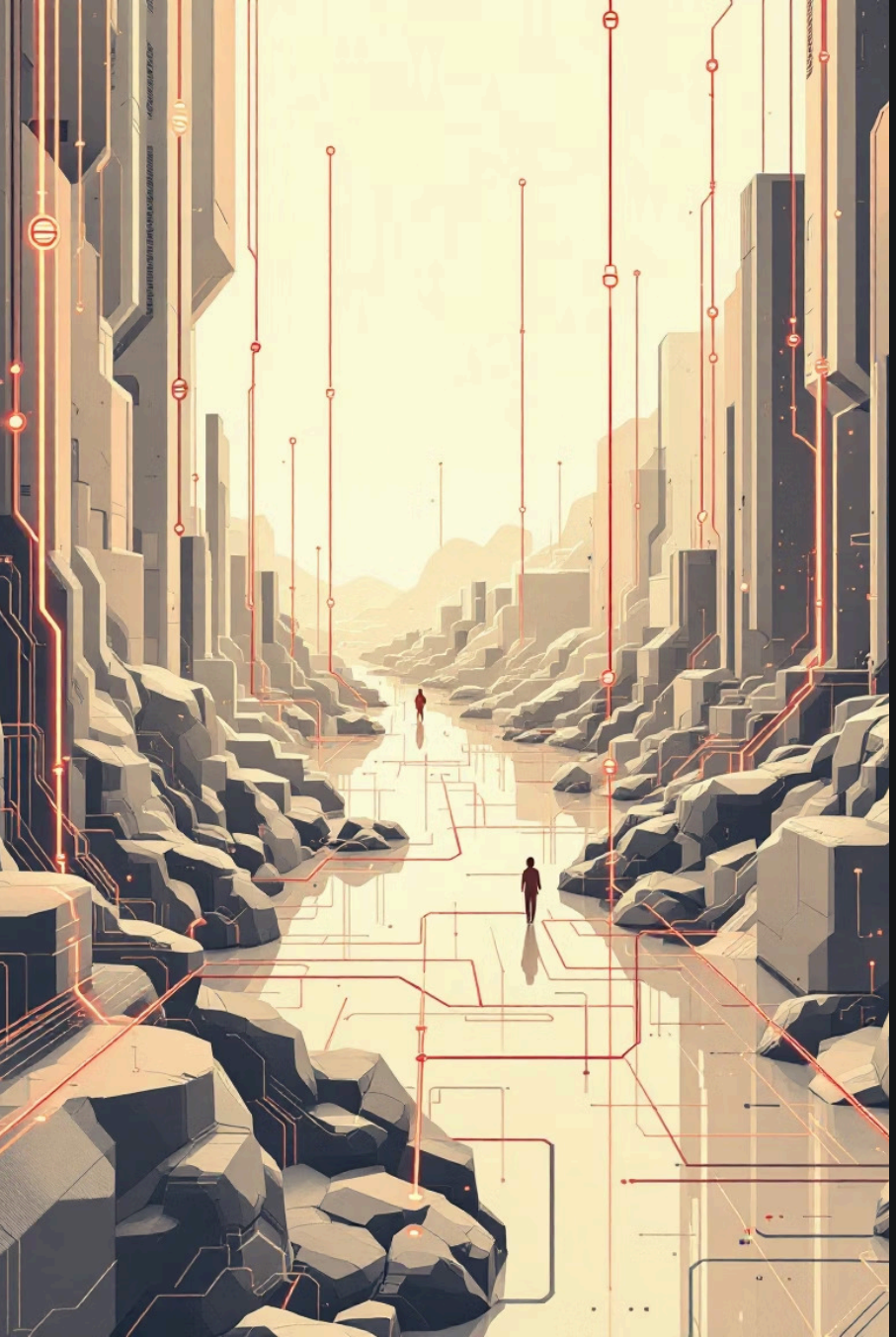


Red Team

Inteligência Ofensiva: Além do Pentest

Apresentado por: **Luan Garcia** & Enzo Teles

O que é Red Team?

Uma equipe de elite que simula os mais sofisticados ataques cibernéticos do mundo real.

Ataques Reais

Simulações avançadas de ameaças persistentes para testar a organização de ponta a ponta.

Avaliação 360°

Testa a eficácia de processos, a conscientização de pessoas e a robustez da tecnologia.

Medir Resiliência

Objetivo primordial é quantificar a capacidade de detecção e resposta da organização, não apenas encontrar falhas.

Pentest: Uma Avaliação Pontual

O Pentest é uma simulação de ataque controlada, focada em vulnerabilidades específicas.

1

Escopo Limitado

Focado em um ativo ou sistema específico, com limites bem definidos.

2

Tempo Definido

Executado em um período pré-determinado, otimizado para eficiência.

3

Busca por Falhas

Principal objetivo é identificar vulnerabilidades e fragilidades conhecidas.

4

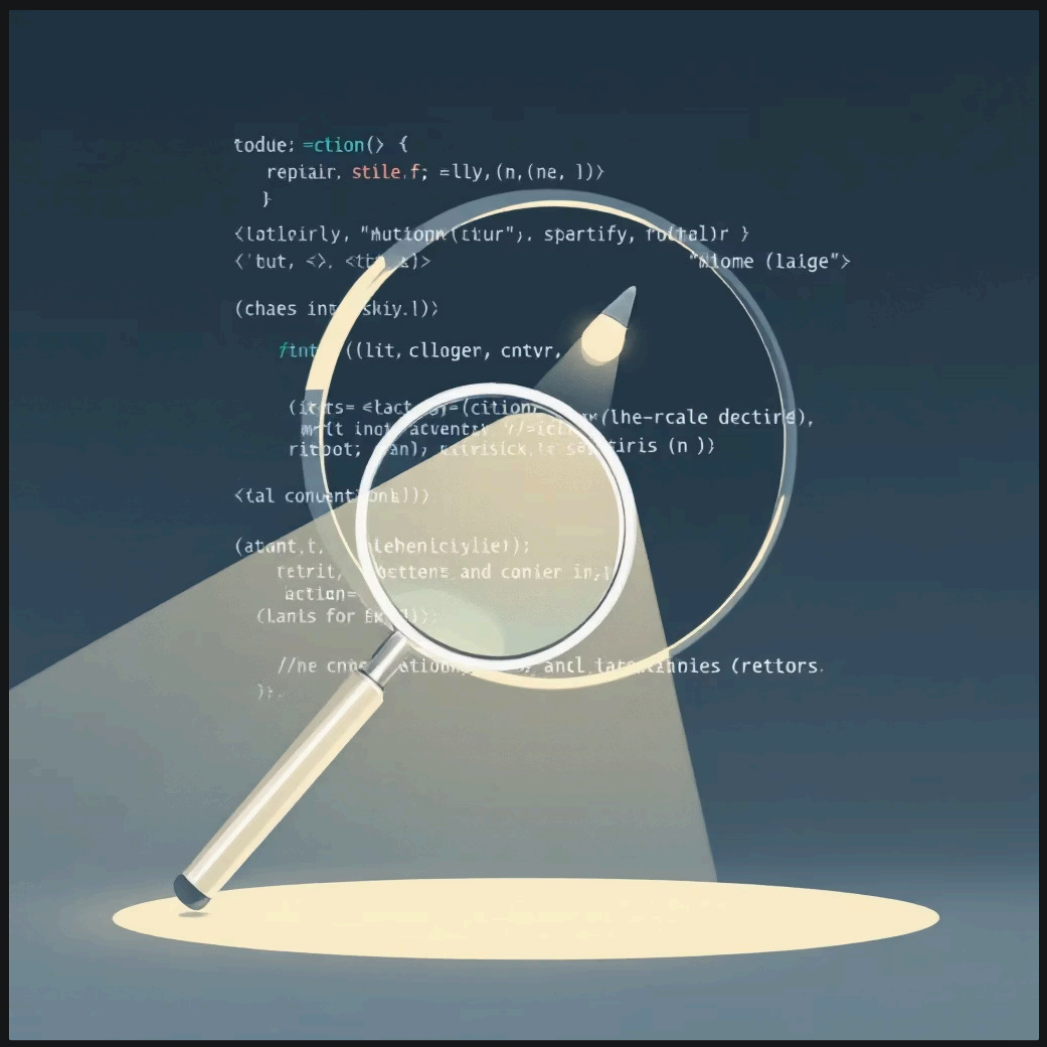
Lista de Recomendações

Entrega um relatório detalhado com as falhas encontradas e sugestões de correção.

Red Team vs. Pentest: As Diferenças Cruciais

Embora complementares, Red Team e Pentest possuem abordagens e objetivos distintos.

Pentest



- Foca na **caça a bugs** dentro de um escopo predefinido.
- Avaliação técnica de **vulnerabilidades conhecidas**.
- Resulta em uma **lista de falhas** para correção.

Red Team

- Atua como um **adversário simulado** com objetivos de negócio reais.
- Avalia a **capacidade de detecção e resposta** da organização.
- Busca por **caminhos de ataque completos**, explorando múltiplas vulnerabilidades e táticas.

Inteligência Ofensiva: O Coração do Red Team

Não se trata apenas de atacar, mas de entender a mente do adversário e suas táticas.

Estratégia Guiada

Uso de informações estratégicas para planejar ataques simulados altamente realistas e eficazes.

Fontes Diversificadas

Coleta de dados via OSINT, dark web, frameworks como MITRE ATT&CK e perfis de ameaças.

Visão do Atacante

Compreender como um adversário real agiria especificamente contra a organização-alvo.

O Ciclo de Operações do Red Team

Uma metodologia estruturada para simular ameaças complexas e contínuas.

1. Planejamento

Baseado em inteligência e objetivos claros.

2. Reconhecimento

Coleta de informações, OSINT e engenharia social.

3. Execução

Movimento lateral, persistência e exfiltração de dados.

4. Impacto & Relatório

Documentação do ataque e tradução para o contexto de negócio.

5. Lições Aprendidas

Colaboração com Blue/Purple Team para aprimoramento contínuo.

Relatório e Feedback: Valor para o Negócio

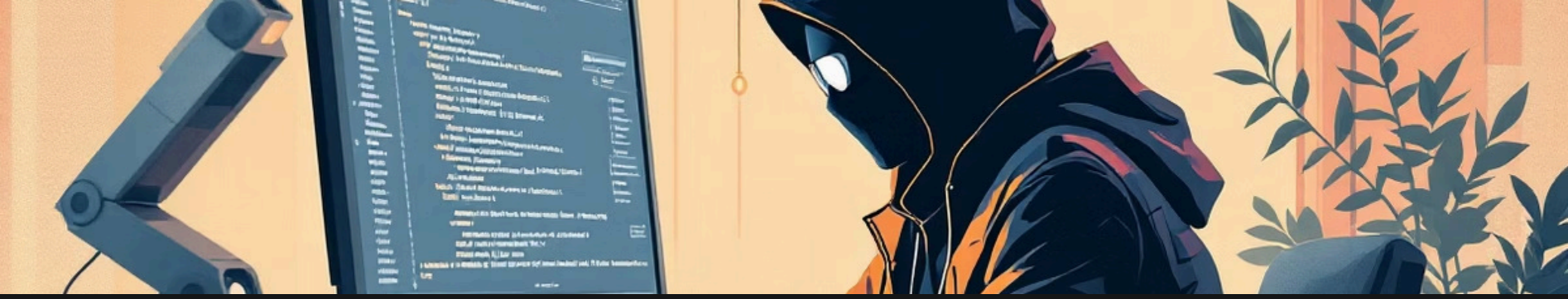
O resultado de uma operação de Red Team vai muito além de um simples checklist técnico.

Relatório Estratégico

O relatório final é traduzido para a linguagem de negócio, detalhando o **impacto real** das vulnerabilidades na organização. Ele apresenta riscos em termos financeiros, operacionais e de reputação, permitindo que a liderança tome decisões informadas.

Feedback Constante

As lições aprendidas são compartilhadas com as equipes **Blue Team (Defesa)** e **Purple Team (Colaboração)**. Essa troca de conhecimento é vital para aprimorar as defesas, refinar playbooks e fortalecer a postura de segurança da empresa proativamente.



Inteligência Ofensiva em Ação: Exemplos Práticos

Veja como a inteligência ofensiva se manifesta em cenários de simulação reais:

Phishing Direcionado

Criação de e-mails de phishing altamente realistas usando dados de **LinkedIn** para testar a conscientização dos funcionários.

Domínios Similares (Typosquatting)

Registro de domínios com grafia similar aos da empresa para simular ataques e treinar o **SOC** na detecção de fraudes.

Simulação de Ransomware

Execução controlada de simulação de ransomware para testar a eficácia de rotinas de **backup** e planos de **resposta a incidentes**.

Validação do SOC

Verificar se o **Security Operations Center** (SOC) gera alertas para as ações do Red Team e se esses alertas resultam em uma resposta adequada.

Carreiras em Segurança Ofensiva

Um campo em constante crescimento, com diversas oportunidades para profissionais especializados.

Pentester

Especialista em testes de invasão e descoberta de vulnerabilidades.

Especialista em Segurança Ofensiva

Profissional com visão estratégica para simulações de ataques complexos.

Engenheiro de Segurança

Desenvolve e implementa soluções de segurança robustas e resilientes.

Consultor de Segurança

Oferece expertise e orientação estratégica para clientes e projetos.

Analista de Threat Intelligence

Coleta e analisa informações sobre ameaças para antecipar ataques.

Obrigado pela atenção!

https://www.linkedin.com/in/luan-garcia-rc

https://www.linkedin.com/in/enzo-teles