

Whoami

- Joas Antonio dos Santos
- Head de segurança ofensiva
- Autor de livros ->
- Contribuidor do Mitre





Red Team x Blue Team: Funções



- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



- Defensive Security
- Infrastructure Protection
- Damage Control
- Incident Response
- Operational Security
- Threat Hunting
- Digital Forensics



Red Team x Blue Team: Objetivos

Red Team vs. Blue Team Cybersecurity

Red Team

Launches coordinated penetration attacks to test strength and coverage of overall security systems.

Mimics attacks like phishing, social engineering, and employee impersonation.

Operates from a current, "presentmoment" view of a company's cybersecurity measures.

Team members need a strong background in software development for custom tool and strategy creation.

Blue Team

Responds to attacks launched by the red team.

Has to constantly strengthen the overall cybersecurity posture for a company or clients.

Utilizes tools like log and memory analysis, PCAP, risk intelligence, digital footprint analysis and more.

Has a more holistic, "bird's eye" view of a company's entire security strategy.





Purple Team: Conceito



RED TEAM

Vulnerability Assessment & Penetration Testing

Threat Hunting

Exploit Development

Cyber Threat Intelligence

Malware Analysis

Social Engineering



PURPLE TEAM

Red Team and
Blue Team working
collaboratively to improve
the cybersecurity
posture of the
organisation



BLUE TEAM

Incident Responders
Security Operations
IT Network & Systems

CIO & CISO office

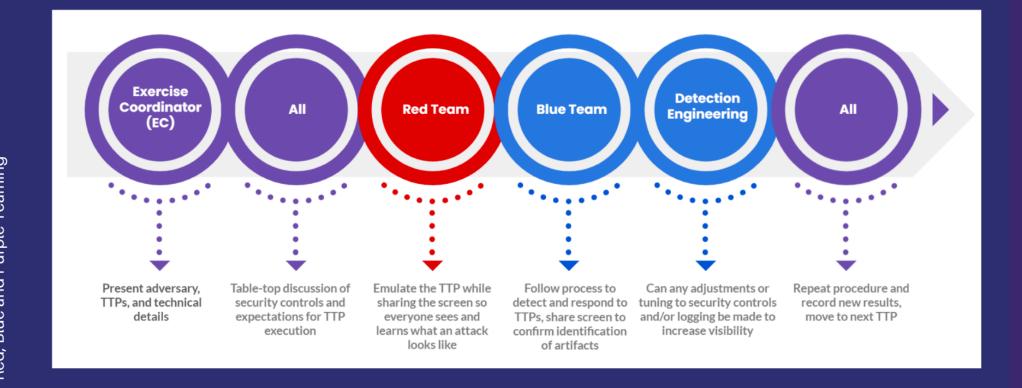




Purple Team: Objetivo

8 Purple Teaming What this exercise covers?





Purple Team: Ciclo de avaliação

THREAT ASSESSMENT

OSINT and threat analysis used to create attack plan to be deployed throughout the assessment, including custom tactics & techniques.

TABLETOP PREVIEW SESSION

Presentation of the Tactics, Techniques & Procedures to be simulated and discussion between Red and Blue Teams of expected outcomes.

TABLETOP REVIEW SESSION

Discussion to review the exercise, understand effective remediation, improvement of existing capabilities and how to address any gaps in detection & response capability.

ASSESSMENT CYCLE

DETECT AND RESPOND ACTIVITY

Blue Team follows existing processes to detect & respond to TTPs.

OBSERVED ATTACK SIMULATION

Blue Team members observe and participate in attack simulations.



Purple Team: Resultados esperados do Exercícios/Avaliação

Before purple teaming			After purple teaming		
Execution	Persistence	Lateral Movement	Execution	Persistence	Lateral Movement
Hardware additions	AppCert DLLs	Logon scripts	Hardware additions	AppCert DLLs	Logon scripts
Valid accounts	Logon Scripts	Pass the ticket	Valid accounts	Logon Scripts	Pass the ticket
Supply chain compromise	Application shimming	Remote file copy	Supply chain compromise	Application shimming	Remote file copy
		Remote services			Remote services



Empregabilidade do Red Team

Social Physical PenTest Mitre Attack Engineering PenTest Cyber Kill Adversary Exploit Threat Hunting Emulation Development Chain Programming Cyber Threat Defense Cloud Attack Expertise (Python, Intelligence Evasion Go or C#) Command and Hardware Threat Risk Identified Modeling Control Hacking



Empregabilidade do Blue Team

Incident Data and Log Network **Vulnerability** Analysis Response Security Management Malware Cyber Kill Risk Threat Hunting Analysis Chain Assessment Programming **Operational** Threat Computer Expertise (Python, Intelligence Security Forensic Go or C#) Security Security Threat Operation OSINT Controls Detection Center



RTFM e BTFM





Na prática

- Wazuh OVA
- Windows Server 2016 Vulnerável
- Kali Linux



OBRIGADO!



