BLUE e RED TEAM – Mercado de Trabalho

Joas Antonio

Detalhes

- Esse documento foi criado para ajudar aqueles que estão iniciando na área de segurança da informação, tanto aqueles que já atuam no mercado de trabalho;
- Ele apresenta os conhecimentos essenciais que muitas vagas exigem para atuar com Blue Team ou Red Team, foram coletado essas informações nos sites Indeed e LinkedIn;

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

BLUE TEAM

BLUE TEAM – O que o mercado pede?

- Fundamentos em Base computacional;
- Conhecimentos em Redes de Computadores (Ex: As ementas CCNA e N+ dão uma base sólida do que é necessário conhecer);
- Conhecimentos em Lógica e Linguagem de Programação (Ex: Python, C, Ruby, Go, Powershell, Shell Script e etc);
- Conhecimentos em Administração de Sistemas Operacionais (Linux Server e Windows Server);
- Conhecimentos em soluções de segurança da informação (Firewalls, IDS/IPS, Proxys, DLPs, CASB, Password Management, EDR, WAF, SOAR, ANTI-APT, SIEM);
- Conhecer de Frameworks, Normas e Padrões (NIST, PCI, C2M2, LGPD/GDPR, Familia ISO 27000;
- Conhecimentos no Mitre Att&ck;
- Conhecimentos em Resposta a Incidentes de Segurança da Informação;
- Gerenciamento de Risco e Vulnerabilidades;
- Politicas de Segurança da Informação e Gestão de Patchs de segurança;
- Habilidades com elaboração de documentação;
- Conhecimentos em ambientes Clouds e Containers;

BLUE TEAM – Ponto crucial

- A área de Blue Team tem um mercado muito amplo e que falta profissionais para atuar;
- Principal dica é desenvolver as suas habilidades em conhecimentos fundamentais como Redes de computadores, pegue conteúdos da CCNA e Network+ não precisa tirar a certificação;
- Além disso, conheça de Administração de Sistemas Operacionais, seja Windows Server como Linux Server, desde configurações até linha de comando;
- É crucial que um Blue Team conheça de soluções de segurança, por isso a minha recomendação é dar uma olhada nos produtos de mercado, pesquisar por gartners e criar laboratórios com as demos que algumas empresas liberam, o importante é ter conhecimento de como uma solução funciona;
- Além disso, a maioria das vagas colocam alguns pontos chaves que o Blue Team deve trabalhar, Ex: (Diagnosticar e Solucionar problemas de segurança, Implementar os melhores controles de segurança, Auxiliar no Gerenciamento de Riscos, Trabalhar com Red Team para detectar vulnerabilidades e Manter a organização em compliance com os principais padrões de mercado);

BLUE TEAM – Certificações

- Essa são as certificações que diversas vagas de Red Team pedem, claro que não é para tirar todas as certificações, mas com certeza possuindo uma delas você vai ter uma vantagem maior em um processo seletivo:

CSCU (EC-COUNCIL);

CND (EC-COUNCIL);

CEH (EC-COUNCIL);

CSA (EC-COUNCIL);

ECIH (EC-COUNCIL);

Security+ (CompTIA);

CySA+ (CompTIA);

Network+ (CompTIA);

Linux+ (CompTIA);

GSEC, GSIF, GCIA, GCIH (SANS);

LPI1 a LPI3 (LPI)

CCNA and CCNP (CISCO);

MCSA,MCSE ou AZ900 e AZ500(Microsoft);

CISSP, CSSLP, CCSP (ISC2);

RED TEAM – Extra

- Caso queira mais detalhes sobre a carreira de um profissional de Segurança de Redes ou Analista de SOC, segue um guia de carreira que eu fiz

- https://bit.ly/3nShJcE (Cyber Security Career)
- https://bit.ly/3rsgCSO (SOC Career)

RED TEAM

RED TEAM – O que o mercado pede?

- Fundamentos em Base computacional;
- Conhecimentos em Redes de Computadores (Ex: As ementas CCNA e N+ dão uma base sólida do que é necessário conhecer);
- Conhecimentos em Lógica e Linguagem de Programação (Ex: Python, C/C++, PHP, JavaScript, Ruby, Go, Shell Script, Powershell e etc);
- Conhecimentos em Administração de Sistemas Operacionais (Linux Server e Windows Server);
- Conhecer de Frameworks, Normas e Padrões (NIST, PCI, C2M2, LGPD/GDPR, Familia ISO 27000;
- Conhecimentos no Mitre Att&ck e familiaridade com TTPs;
- Gerenciamento de Risco e Vulnerabilidades;
- Conhecer ferramentas de analise e avaliação de vulnerabilidade (SAST, DAST, IAST E ETC);
- Habilidades com elaboração de documentação e relatórios de PenTest;
- Habilidades com PenTest em aplicações web, mobile, Redes/Infraestrutura;
- Conhecimentos em ambientes Clouds e Containers;
- Experiência com as principais ferramentas de PenTest (Nmap, Burp, Metasploit e etc);
- Conhecimentos em metodologias de PenTest (OSSTMM, PTES, OWASP, NIST e etc);

RED TEAM – Ponto crucial

- A área de Red Team tem um mercado muito amplo e que falta profissionais com muitas qualidades;
- Minha principal dica é desenvolver bastante seus fundamentos e ter conhecimentos sólidos em Redes de Computadores;
- É crucial que um Red Team saiba conduzir um PenTest, desde a coleta de informação até conseguir apagar seus rastros, além de contribuir com as orientações para correção das vulnerabilidades ao lado do Blue Team;
- Além de ser um pesquisador e sempre estar por dentro das ameaças e riscos de segurança, além de validar e testar os principais serviços da organização;
- Muitas vagas colocam alguns pontos chaves para um bom Red Team, Ex: (Capacidade de executar um bom PenTest e elaborar relatórios bem detalhados tanto técnicos como executivos, Revisar e validar descobertas de segurança, Analisar os riscos e impactos das ações realizadas durante os testes, conduzir e realizar pesquisas de vulnerabilidades, boa comunicação entre equipe, capacidade de criar os próprios scripts e garantir a conformidade com os principais padrões de mercado);

RED TEAM – Certificações

- Essa são as certificações que diversas vagas de Red Team pedem, claro que não é para tirar todas as certificações, mas com certeza possuindo uma delas você vai ter uma vantagem maior em um processo seletivo:

CND (EC-COUNCIL);

CEH (EC-COUNCIL);

CPENT (EC-COUNCIL);

LPT (EC-COUNCIL);

GPEN (SANS);

GXPN, GMOB, GWAPT (SANS);

OSCP (Offensive Security);

OSCE ou OSEP (Offensive Security);

OSWP (Offensive Security);

PenTest+ (CompTIA);

eJPT, eCPPT e eCPTX (eLearnsecurity);

eWPT e eWPTX (eLearnsecurity);

CISSP, CSSLP, CCSP (ISC2);

Security+ (CompTIA);

Linux+ (CompTIA);

LPI1 a LPI3 (LPI);

CCNA (CISCO);

AZ900 e AZ500(Microsoft);

Certificações AWS (Amazon);

RED TEAM – Extra

- Caso queira mais detalhes sobre a carreira de um PenTester, segue um guia de carreira que eu fiz

- https://bit.ly/37LytN6

CONCLUSÃO

- Esse é um PDF complementar dos guias de carreira que eu desenvolvi, espero que ajude você a ter uma noção do que o mercado exige dos profissionais de segurança da informação;
- Mas claro, não significa que você precisa saber de tudo, porém noto que muitas vagas exige que você conheça de como funciona o processo, ou seja, pelo menos o básico para conseguir se desenvolver na área;
- Além disso, as certificações são essenciais, eu recomendo que você monte um cronograma e faça um investimento para tira-las, claro, não precisa tirar todas aquelas;

Estou preparando uma documentação em relação ao cronograma de certificações na área de segurança da informação