CARREIRA COMO SOC ANALYST I

JOAS ANTONIO

DETALHES

- Um PDF sobre carreira na área de SOC para aqueles que desejam começar e estão entrando agora na área;
- https://www.linkedin.com/in/joas-antonio-dos-santos

CONHECIMENTOS ESSÊNCIAS – SOC I

- Conhecimentos em Redes de Computadores é fundamental;
- Habilidades em comunicação e atendimento;
- Conhecimentos em SIEM, seu funcionamento, arquitetura e os principais (Gartners);
- Conhecimentos básicos em expressões regulares;
- Habilidades e conhecimentos com Analises e correlação de Logs;
- Conhecimentos de IOCs e TTPs;
- Conhecimentos básicos em Gestão de Riscos e Vulnerabilidades;
- Conhecimentos básicos em Arquitetura e Soluções de Segurança (Firewall, IDS, IPS e etc...);
- Conhecimentos essências em Administração de Sistemas Linux e Windows;
- Fundamentos de Threat Intell and Hunting é diferencial;

Inglês é fundamental

AONDE ESTUDAR?

- https://cybrary.it/
- https://pluralsight.com/
- https://www.youtube.com/playlist?list=PLkpBBXRDsRPV9Sx4TZs4rAuoEmW6b71TV
- https://www.udemy.com/
- https://www.comptia.org/pt/certificacoes/security (Procure um ATC)
- https://www.eccouncil.org/programs/certified-soc-analyst-csa/ (Procure um ATC)
- https://elearnsecurity.com/
- https://sans.org/
- https://www.impacta.com.br/cursos/fundamentos-de-soc-security-operations-center-online
- https://www.fortinet.com/br/training/cybersecurity-professionals
- Cursos de fornecedores e parceiros de soluções
- https://www.comptia.org/pt/certificacoes/cybersecurity-analyst (Procure um ATC)

AONDE ESTUDAR?

- https://blueteamlabs.online/
- https://securityblue.team/blue-team-labs-online/
- https://cyberdefenders.org/labs/
- https://tryhackme.com/