SOC Analyst - Career

Joas Antonio

Details

- O objetivo é auxiliar aqueles que desejam entrar no mercado de trabalho e principalmente os profissionais de segurança a ingressar na área de SOC;
- Essa é uma lista de habilidades reunidas de diversas vagas, ao qual eu coloquei tudo que você encontraria em uma vaga de SOC Analyst do I a III;
- Essa não são exigências de apenas uma vaga, mas sim de várias em cada nível;
- Esse documento é apenas um guia para auxiliar você a encaminhar seus estudos na área de SOC;

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

Skills SOC Analyst I

- Conhecimentos sólidos em Redes de Computadores;
- Conhecimentos em Lógica da Programação;
- Habilidades em comunicação e atendimento;
- Conhecimentos em SIEM (Gartners);
- Conhecimentos em expressões regulares;
- Habilidades e conhecimentos com Analises e correlação de Logs e IOCs;
- Programação em Python e Shell Script (Extração e Integração);
- Conhecimentos básicos em Gestão de Riscos e Vulnerabilidades;
- Conhecimentos Threats and Vulnerability;
- Conhecimentos básicos em Arquitetura e Soluções de Segurança (Firewall, IDS, IPS e etc...);
- Conhecimentos essências em Administração de Sistemas Linux e Windows;

Certificação que podem ajudar: Security+ (CompTIA) ou CSA (EC-COUNCIL)

SOC Analyst I

- Além dessas habilidades técnicas, é essencial que o profissional fique por dentro das politicas de segurança da informação;
- Auxiliar na melhoria e implantação de soluções de segurança;
- Habilidades para resolver problemas;
- Auxiliar na Administração de soluções de segurança;

Skills SOC Analyst II

- Conhecimentos sólidos em Redes de Computadores;
- Conhecimentos em Lógica da Programação;
- Habilidades e conhecimentos em Linguagens de Programação (Shell Script, Powershell e Python para automatização);
- Conhecimentos em Administração de Sistemas Operacionais (Windows e Linux Servers);
- Conhecimentos em Arquitetura e Soluções de Segurança da Informação;
- Conhecimentos e Habilidades em Analise e correlação de Logs para identificar intrusões;
- Habilidades com Forense Digital;
- Conhecimentos em Resposta a Incidentes (Implementação, Recuperação e Planejamento;
- Habilidades com escrita e comunicação;
- Conhecimentos em APTs e Mitre Att&ck;
- Conhecimentos em PenTest e Analise de Vulnerabilidade;
- Conhecimentos em Frameworks de Segurança (NIST, Cyber Kill Chain, Mitre e etc...);
- Habilidades em detecção e contenção de intrusão;
- Conhecimentos em Threat Intelligence;
- Habilidades com Analise de Malware;

Certificações que podem ajudar: CSA (EC-COUNCIL), CHFI (EC-COUNCIL), CEH (EC-COUNCIL), CTIA (EC-COUNCIL), Sec+ (CompTIA), CySA (CompTIA)

SOC Analyst II

- Fornece análise de ameaças e registros de segurança para dispositivos de segurança;
- Analisar e responder a fraquezas e vulnerabilidades de hardware e software;
- Investigar, documentar e relatar problemas de segurança e tendências de segurança emergentes;
- Coordenar com outros analistas e departamentos em relação à segurança do sistema e da rede quando necessário;
- Crie, implemente e mantenha protocolos e controles de segurança, incluindo a proteção de arquivos digitais e dados contra acesso não autorizado;
- Manter os dados e monitorar o acesso de segurança;
- Realize análises de risco, testes de vulnerabilidade e avaliações de segurança;
- Realizar auditorias de segurança, internas e externas;
- Antecipe ameaças, incidentes e alertas para ajudar a prevenir a probabilidade de que ocorram;
- Gerenciar sistemas de detecção de intrusão de rede;

Skills SOC Analyst III

- Ter habilidades de um SOC Analyst I e II
- Conhecimentos sólidos em Analise de Malware e Engenharia Reversa;
- Conhecimentos e Habilidades com Threat Hunter;
- Investigação e Analise de Incidentes Cibernéticos;
- Conhecimentos sólidos em PenTest;
- Conhecimentos sólidos de Frameworks de Segurança;
- Conhecimento de aplicações de segurança e implementação das mesmas como IDS, IPS, SIEM, Firewall, SOAR e outras ferramentas de detecção de anomalias;
- Experiência com processos na área funcional (ou seja, gerenciamento de problemas, gerenciamento de falhas e gerenciamento de incidentes);
- Boa comunicação e escrita;
- Identifique ideias de aprimoramento de capacidade SOC para melhoria contínua, juntamente com a alta gerência;
- Relatório de métricas relacionadas ao SOC;

Certificações que podem ajudar: DoD 8570 (Certifieds), CHFI, CTIA, CEH, CASP+, CySA+, CISSP

SOC Analyst III

- Fornece análise de ameaças e registros de segurança para dispositivos de segurança;
- Analisar e responder a fraquezas e vulnerabilidades de hardware e software;
- Investigar, documentar e relatar problemas de segurança e tendências de segurança emergentes;
- Coordenar com outros analistas e departamentos em relação à segurança do sistema e da rede quando necessário;
- Crie, implemente e mantenha protocolos e controles de segurança, incluindo a proteção de arquivos digitais e dados contra acesso não autorizado;
- Manter os dados e monitorar o acesso de segurança;
- Realize análises de risco, testes de vulnerabilidade e avaliações de segurança;
- Realizar auditorias de segurança, internas e externas;
- Antecipe ameaças, incidentes e alertas para ajudar a prevenir a probabilidade de que ocorram;
- Gerenciar sistemas de detecção de intrusão de rede;

SOC Analyst III

- Executar a execução detalhada e repetível de todas as tarefas operacionais, conforme documentado nos processos SOC e procedimentos subordinados.
- Monitore as ferramentas de eventos principais do SOC para eventos de segurança;
- Fechar ou escalar eventos de segurança conforme necessário;
- Atualizar toda a documentação relevante, como registros de turnos e tickets, procedimentos
  Identifique o impacto dos incidentes nos sistemas e, usando as ferramentas disponíveis, determine se os dados foram exfiltrados;
- Documente e mantenha uma base de conhecimento de alarmes (falsos positivos e falsos negativos, listas negras, listas brancas) que IDS e IPS encontram;
- Garanta que os eventos e incidentes de segurança sejam detectados e escalados em tempo hábil;
- Fornece análise e investigação para determinar se os alertas ou eventos de segurança garantem a classificação do incidente;
- Rastreie incidentes até a resolução final;

Courses SOC Analyst

- ACADI-TI
- EC-COUNCIL
- Cybrary
- CompTIA
- SANS
- Udemy
- Gohacking
- Sec4us
- ISC2

Conclusion

- Os detalhes descritos é referentes aos níveis de habilidades que cada profissional de SOC de nível I, II, III possui, analisando vagas tanto dentro como fora do Brasil;
- Não significa que todas informações descritas são as exigências de apenas uma vaga, mas ao contrário, eu apenas reunir o que muitas empresas procuram de um profissional de SOC em cada nível profissional, seja empresas pequenas ou grandes;
- Muitas empresas possuem poucas exigências e outras exigem um pouco mais, porém no fim, com fundamentos e base sólidas, não será difícil você desenvolver suas habilidades como um Analista SOC;