SOC Analyst - Career

joas antonio

Details

- The objective is to help those who wish to enter the job market and especially security professionals to enter the SOC area;
- This is a list of skills gathered from various job openings, to which I've put everything you'd find in a SOC Analyst job opening I to III;
- These are not requirements for just one place, but for several at each level;
- This document is just a guide to help you forward your studies in the SOC area;

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

Skills SOC Analyst I

- Solid knowledge in Computer Networks;
- Knowledge in Programming Logic;
- Communication and service skills;
- Knowledge in SIEM (Gartners);
- Knowledge in regular expressions;
- Skills and knowledge with Analysis and correlation of Logs and IOCs;
- Python and Shell Script Programming (Extraction and Integration);
- Basic knowledge in Risk and Vulnerability Management;
- Threats and Vulnerability Knowledge;
- Basic knowledge in Security Architecture and Solutions (Firewall, IDS, IPS and etc...);
- Essential knowledge in Linux and Windows System Administration;

Certification that can help: Security+ (CompTIA) or CSA (EC-COUNCIL)

SOC Analyst I

- In addition to these technical skills, it is essential that the professional is aware of information security policies;
- Assist in the improvement and implementation of security solutions;
- Problem solving skills;
- Assist in the administration of security solutions;

Skills SOC Analyst II

- Solid knowledge in Computer Networks;
- Knowledge in Programming Logic;
- Skills and knowledge in Programming Languages (Shell Script, Powershell and Python for automation);
- Knowledge in Operating System Administration (Windows and Linux Servers);
- Knowledge in Information Security Architecture and Solutions;
- Knowledge and Skills in Analysis and Log correlation to identify intrusions;
- Skills with Digital Forensics;
- Knowledge in Incident Response (Implementation, Recovery and Planning;
- Writing and communication skills;
- Knowledge in APTs and Miter Att&ck;
- Knowledge in PenTest and Vulnerability Analysis;
- Knowledge in Security Frameworks (NIST, Cyber Kill Chain, Miter, etc...);
- Intrusion detection and containment skills;
- Knowledge in Threat Intelligence;
- Malware Analysis Skills;

Certifications that can help: CSA (EC-COUNCIL), CHFI (EC-COUNCIL), CEH (EC-COUNCIL), CTIA (EC-COUNCIL), Sec+ (CompTIA), CySA (CompTIA)

SOC Analyst II

- Provides threat analysis and security logs for security devices;
- Analyze and respond to hardware and software weaknesses and vulnerabilities;
- Investigate, document and report security issues and emerging security trends;
- Coordinate with other analysts and departments regarding system and network security when necessary;
- Create, implement and maintain security protocols and controls, including protecting digital files and data from unauthorized access;
- Maintain data and monitor security access;
- Perform risk analysis, vulnerability testing and security assessments;
- Conduct security audits, internal and external;
- Anticipate threats, incidents and alerts to help prevent the likelihood that they will occur;
- Manage network intrusion detection systems;

Skills SOC Analyst III

- Have the skills of a SOC Analyst I and II
- Solid knowledge in Malware Analysis and Reverse Engineering;
- Knowledge and Skills with Threat Hunter;
- Cyber Incident Investigation and Analysis;
- Solid knowledge in PenTest;
- Solid knowledge of Security Frameworks;
- Knowledge of security applications and their implementation such as IDS, IPS, SIEM, Firewall, SOAR and other anomaly detection tools;
- Experience with processes in the functional area (ie problem management, fault management and incident management);
- Good communication and writing;
- Identify SOC capability improvement ideas for continuous improvement together with senior management;
- SOC-related metrics report;

Certifications that can help: DoD 8570 (Certifieds), CHFI, CTIA, CEH, CASP+, CySA+, CISSP

SOC Analyst III

- Provides threat analysis and security logs for security devices;
- Analyze and respond to hardware and software weaknesses and vulnerabilities;
- Investigate, document and report security issues and emerging security trends;
- Coordinate with other analysts and departments regarding system and network security when necessary;
- Create, implement and maintain security protocols and controls, including protecting digital files and data from unauthorized access;
- Maintain data and monitor security access;
- Perform risk analysis, vulnerability testing and security assessments;
- Conduct security audits, internal and external;
- Anticipate threats, incidents and alerts to help prevent the likelihood that they will occur;
- Manage network intrusion detection systems;

SOC Analyst III

- Perform detailed and repeatable execution of all operational tasks as documented in the SOC processes and subordinate procedures.
- Monitor SOC key event tools for security events;
- Close or escalate security events as needed;
- Update all relevant documentation such as shift and ticket records, procedures
  Identify the impact of incidents on systems and, using available tools, determine if data has been exfiltrated;
- Document and maintain a knowledge base of alarms (false positives and false negatives, blacklists, whitelists) that IDS and IPS encounter;
- Ensure that security events and incidents are detected and escalated in a timely manner;
- Provides analysis and investigation to determine whether security alerts or events warrant incident classification;
- Track incidents to final resolution;

Conclusion

- The details described refer to the skill levels that each level I, II, III SOC professional has, analyzing vacancies both inside and outside Brazil;
- It doesn't mean that all the information described is the requirements of just one position, but rather, I just gather what many companies look for from a SOC professional at every professional level, whether small or large companies;
- Many companies have few requirements and others demand a little more, but in the end, with a solid foundation and foundation, it won't be difficult for you to develop your skills as a SOC Analyst;