SOC ANALYST

FUNCTION: A SOC Analyst is dedicated to defending digital realms against the relentless onslaught of cyber threats. Armed with knowledge of cutting-edge technologies, strategic thinking, and a keen eye for anomalies, the SOC Analyst stands as a vigilant guardian of data and systems.

COMMON QUALIFICATIONS

- On-the-job-training
- CompTIA: PenTest+, Networking+, Security+, Cybersecurity Analyst+
- GIAC Certified Incident Handler Certification (GCIH)
- SANS Certification
- MITRE ATT&CK training
- Forensics training
- Blue Team labs and training
- ISC2 membership
- Degree in Forensics and Information Assurance or Network Security

ABILITIES

Threat Perception: Has an innate ability to detect subtle signs of impending cyber threats. This includes recognizing patterns in network traffic, identifying suspicious user behavior, and uncovering anomalies in system logs.

Cyber Defense Tactics: Proficient in the use of defensive technologies such as firewalls, security information and event management (SIEM) tools, and endpoint protection tools, a SOC Analyst excels at fortifying digital fortresses against cyberattacks.

Cyber Intelligence Gathering: Adept at gathering and analyzing cyber threat intelligence from various sources. This includes monitoring underground forums, tracking threat actor activity, and staying updated on the latest cyber threat landscape.

Security Enthusiast: Skilled in using a wide array of query languages, SIEMs, intrusion detection systems, and penetration testing frameworks - with a craving to unearth new tools and exploits.

Continuous Learning: In the ever-evolving field of cybersecurity, a SOC Analyst prioritizes continuous learning and skill development. They stay on top of emerging cyber threats, attend training programs, and obtain industry certifications to enhance their expertise.

Persuasive Translator: Excels in communicating complex information to both technical and non-technical stakeholders. This includes crafting detailed incident reports, presenting findings to management, and conducting cybersecurity awareness training sessions.

"Making the world a safer place."

Incident Response Coordinator: Leads incident response efforts for critical cyber incidents, coordinating with cross-functional teams to contain threats, mitigate impact, and restore operations.

Tool Optimizer: For improved threat detection and response capabilities, a SOC Analyst collaborates with cybersecurity engineers to enhance SIEM rules, develop custom threat detection signatures, and bolster SOC toolsets.

Ardent Mentor: Always ready to share expertise and guidance to other team members on needed technical skills, incident handling procedures, and professional development in the cybersecurity field.

BINARY DEFENSE™

SOC ANALYST

PERSONALITY TRAITS

Detail-Oriented: Pays meticulous attention to detail, ensuring no threat goes unnoticed and no security gap remains unaddressed with a passion to fix things or scour logs sources.

Adaptable: In the fast-paced world of cybersecurity, a SOC Analyst remains flexible to pivot at a moment's notice and quick to respond to challenges where time is of the essence.

Charismatic: Engaging with a wide variety of internal teams and clients is a constant. A great SOC Analyst brings a positive and alluring attitude to each meeting.

Ethical Integrity: Upholding a strong sense of ethics, a SOC Analyst prioritizes the protection of privacy and the responsible use of cybersecurity tools and techniques.

Aptitude: Possesses a deep understanding of cybersecurity concepts, ranging from network protocols to threat detection methodologies. This intelligence allows them to quickly analyze and respond to complex cyber incidents.

Defender-at-Heart: As both a sentry and detective, a SOC Analyst derives meaning from their role by relentlessly safeguarding and protecting clients to the best of their abilities as a strategic partner.

Analytical Mind: A SOC Analyst's analytical prowess shines when reviewing behavioral analysis dashboards where keen observation and data analysis lead to the discovery of hidden threats and vulnerabilities.

A SOC ANALYST'S PROWESS SHINES WHEN REVIEWING BEHAVIORIAL ANALYSIS DASHBOARDS

PAYS METICULOUS ATTENTION TO DETAIL

STANDARD EQUIPMENT

- Laptop with cybersecurity tools and software
- Custom dashboards with dynamic metrics
- CLI coding and tooling
- Excel for scoping and data analysis
- Cyber Threat Intelligence feeds from OSINT
- Endpoint Detection and Response (EDR) tools
- Network Detection and Response tools
- Forensics Toolkit (FTK)
- SIEMs – sift through and query data
- SOAR – task and tool automation
- Secure communication applications and devices
- Notetaking apps

FIERCELY PROTECTING YOUR EVERYTHING

Meet all the Defenders at BinaryDefense.com

BINARY DEFENSE™

The Right Partner is the Best Defense