Example of Cyber Intelligence Analyst Job Description

Powered by www.VelvetJobs.com

Our growing company is hiring for a cyber intelligence analyst. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for cyber intelligence analyst

- Maintain and correlate detailed threat actor profiles/groups on adversaries of interest/relevance to the firm, covering tactics, techniques and procedures (TTPs), intent, goals and strategic objectives that could support defensive mitigation and hardening efforts
- Identify, document and share related tactics, techniques and procedures (TTPs) and Indicators of Compromise (IOCs) across all internal/external repositories
- Fuse and analyze all-source information and intelligence to produce quality intelligence products, papers, presentations, recommendations, and findings in support of US government operations
- Leverages advanced investigative skills to initiate pivoting analysis on Threat Intelligence to identify current impact or proactively process mitigations for defense through security technologies and proactive mitigations including zero-day patching identification and anomalous behavior
- Supports junior team members in methods to process tactical mitigations based on results of analysis and determination of threat validity
- Provide remediation support to compromised users, computers or other IT systems
- Contribute to the documentation and development of CIRT processes
- Perform real-time security log and event analysis and takes action within defined parameters to contain and mitigate information security threats and

- Assists 1st level SOC Analysts in performing real-time security log and event analysis and incident response duties when needed
- Build and develop a team of cyber intelligence analysts to identify, track and investigate high priority threat campaigns and malicious actors

Qualifications for cyber intelligence analyst

- Security Tools experience (Firewalls, Intrusion Detection/Prevention Systems, AntiVirus, URL filter)
- 3+ years of experience as a SOC analyst performing threat monitoring and incident response in an enterprise SOC preferred
- Experience with collecting, analyzing, and interpreting qualitative and quantitative data from multiple sources for the purposes of documenting results and analyzing findings to provide meaningful products preferred
- Ability to write high-quality intelligence assessments and briefings for a senior-level audience and technical audiences
- Ability towork in a fast-paced work environment, multi-task, and be comfortable with truncated delivery deadlines
- Must be capable of utilizing information security and monitoring tools