Example of Cyber Threat & Intelligence Job Description

Powered by www.VelvetJobs.com

Our company is growing rapidly and is hiring for a cyber threat & intelligence. To join our growing team, please review the list of responsibilities and qualifications.

Responsibilities for cyber threat & intelligence

- You will establish and operate processes necessary to collect, analyses, prioritize and disseminate current all-source intelligence product in support of JSOC priorities
- Your team will provide timely and prioritized intelligence support into the JSOC detection lifecycle and incident response processes
- Use your interpersonal skills to develop and maintain key cross-functional relationships with Security Research, Physical Security, Product Security, IT, Legal, and other critical business unit areas
- You and your team will ensure the JSOC is able to respond appropriately to both commonly used and specific adversary TTPs through the development and participation in table-top and adversary simulation exercises
- You will collaborate with stakeholders to drive a deep understanding of significant threats
- You will work with Risk Management teams to escalate risk and create mitigation plans
- You will develop and maintain key multi-functional relationships with Security Research, Physical Security, Product Security, IT, Legal, and other critical business unit areas
- You will document analytic tradecraft and methodology
- You will collaborate on workflow to foster lessons learned into SOC and DFIR Intel teams to enhance detection capability
- You will take new indicators from SOC and DFIR teams and create feedback loop to educate SOC/DFIR analysts

- Tracking cyber threat actors and their infrastructure, targeted attack techniques, tactics, and procedures
- Lead and take action on a diverse range of technical and threat information, conduct deep-dive analysis to draw out trend analysis and context, drawing relevant conclusions and assessment
- A detailed understanding of the current developing crime-ware and security landscape Espionage, Crime and Hacktivism
- Scripting in languages such as Python, Perl, Powershell and a deep understanding of command line across Linux, Unix, OSX, Windows
- A motivated, self-managed, individual who can demonstrate above average analytical skills and work with peers and customers
- Initiate, organize and conduct data collection and research using all the tools and applications proactive open source information