Cyber Threat Analyst Cyber Threat Analyst Cyber Threat Analyst - Accenture Federal Services

Work Experience Cyber Threat Analyst Accenture Federal Services - Germantown, MD August 2019 to Present Conduct analysis on NetFlow, Bro, and Palo Alto data using tools like Splunk, Kibana, and other in-house developed tools to identify suspicious traffic. ? Develop new techniques to find threats, attacks, and campaigns against the organization. ? Handle APT tracking using proprietary tools to support other SOC team members. ? Conduct OSINT analysis on current threats to obtain information and IOCs on threats to the DOE using tools such as VirusTotal enterprise account. ? Generate technical reports about important incidents such as spear-phishing or campaigns targeting the energy sector. Cyber Security Analyst Accenture Federal Services - Germantown, MD August 2018 to June 2019 Conduct analysis on NetFlow and Bro data using tools like Splunk, Kibana, and other in-house developed tools to identify suspicious traffic. ? Develop several weekly reports on recurring threats specific to the customer. ? Conduct OSINT analysis on current threats to obtain information and IOCs on threats to the DOE. ? Generate technical reports about important incidents such as spear-phishing or campaigns targeting the energy sector. Website Manager Spamcion - Germantown, MD January 2017 to June 2019 Develop the website Spamcion.com using tools such as AWS, WordPress.org, Mailgun, and CloudFlare. ? Continuously update and patch the CMS versions and other aspect of the website. ? Conduct security assessments using tools such as OpenVAS, WPscan, and other tools in Kali Linux. ? Maintain a well curated RSS feed to write and post technical reports on trending cyber related campaigns, threats and vulnerabilities. Cyber Security Analyst General Dynamics Information Technology - Germantown, MD November 2016 to August 2018 Process cyber security incidents and generate executive reports to be shared with federal leadership. ? Research and vet IOCs using tools such as Ipvoid.com, Domaintools.com, RiskIQ, VirusTotal and Otxalienvault.com ? Generate technical reports about current cyber threats to be shared in an official news bulletin. Temporary IT Intern/ Help Desk Tier George Washington University - Arlington, VA September 2016 to November 2016 Provide technical support for 50+ users and ensure proper maintenance of workstations, printers, and peripherals. ? Deploy new workstations and printers, installing operating systems, applications,

and drivers, and configuring networks. Education A.A.S in Cybersecurity Montgomery College - Germantown, MD May 2016

Name: Kristen Turner

Email: hudsonjerry@example.net

Phone: 502-429-1803x64957