Cyber Intelligence Analyst Cyber Intelligence Analyst Cyber Intelligence Analyst - Prudential Financial Livingston, NJ Cyber security analyst and system administrator with a background in security incident reporting and management. Hands on knowledge including backup and retrieval, system hardening, security management, email systems, applications support and endpoint security response. Extensive experience monitoring, tracking, and evaluating global IT infrastructure incidents through penetration testing as well as organizing data reports and logs for enhanced security protection. Professional, detail-oriented administrator motivated to drive projects from start to finish as part of a dynamic fast paced team. Understanding of business relations and security impact from a risk analysis and cost perspective from an overarching concern. CompTIA Security+ Certification | CEH Certification | Training in CISSP Work Experience Cyber Intelligence Analyst Prudential Financial - Roseland, NJ March 2018 to Present Monitor, manage and fortify user integrity on a global scale using latest cyber security tools and practices, while building layers of defense and creating best practices and reports to streamline services, and technology. Maintained situational awareness of cyber activity by reviewing open source reporting for new vulnerabilities, malware, or other threats that have the potential to impact the organization. Deployment of AWS Guardduty, Cloud Formation Templates, CloudTrail development and CloudWatch monitoring Performed cyber threat intelligence analysis, correlate actionable security events, perform network traffic analysis using raw packet data, net flow, IDS, IPS, and custom sensor output with McAfee as it pertains to the cyber security of communication networks, and participate in the coordination of resources during incident response efforts. Coordinated resources during enterprise incident response efforts, driving incidents to timely and complete resolution. Employ advanced forensic tools and techniques for attack reconstruction, including forensic analysis and volatile data collection and analysis and Recommend sound remediation and recovery strategies, suggest defensive policy enhancements and information technology procedures. Conducted malware analysis of attacker tools providing indicators for enterprise defensive measures, such as Fireye utilizations Interface with external entities including law enforcement organizations, intelligence community organizations and other government agencies as

required. Delivered and analyzed status reports, briefings, recommendations, and findings to management and executives as required including but not limited to threat campaign (s) techniques, and extract indicators of compromise (IOCs). Assists in phishing test deployment, and training Understanding and involvement in threating hunting and analysis Monitoring and usage of Recorded Future for threat analysis Splunk development and including but not limited to reporting, alert creation, and SPL coding IT Security Analyst Realogy Holding Corp - Madison, NJ September 2016 to November 2017 Manages and system administrator of operations & configuration of all website technologies & data feeds including incident management, performance monitoring, and security platform, monitoring, configuration and deployment. System intrusion & detection using Carbon Black as well as ensured network, system and data availability and integrity through preventative, user endpoint security and monitoring. NMAP, Malware protection and management maintenance and upgrades. DNScrypt setup and deployment for wired and wireless devices Security monitored network performance and provided network performance statistical reports for both real-time and historical measurements, and recording using Splunk Established compatibility with third party software products by developing program for modification and integration. Coordinated with systems partners to finalize designs and confirm requirements, for security development and planning. Incident Response Management including assessing risk and external threats Firewall network vulnerability security monitoring, patching for clients, servers, and applications, with Qualysguard, Wireshark and Glasswire Incident Response Management, logging, reporting and resolution of known threats, including motioning and threat detection. Built application platform foundation to support migration from client to server with security concepts Secure based backup and management of data using NAS devices and software Forensics experience with Encase, reporting and detection Created Qualisys Guard and Nessus policy for reporting and monitoring Security Analyst Bayer Pharmaceuticals - Whippany, NJ November 2013 to September 2016 Security support for end-users utilizing Carbon Black to perform testing and problem analysis for server, desktop and IT infrastructure work, including penetration testing, Kali Linux Security system and device hardening and deployment Understanding of All Phases of The

Incident Response Life Cycle and Lockheed Martin "kill chain" methodology Provided security maintenance and development of bug fixes and patch sets for existing web applications. Deterrent management and control, PRTG network monitoring/troubleshooting Designed strategic plan for component development practices to support future projects, and introduction to disaster recovery options and proposals. Diagnosed and troubleshooted UNIX and Windows processing problems and applied solutions to increase company efficiency. Built application platform foundation to support migration from client to server with security concepts Secure based backup and management of data using NAS devices and software Forensics experience with Encase, reporting and detection Security Specialist Novartis Pharmaceuticals - East Hanover, NJ March 2011 to September 2013 Managed firewall, LAN/WLAN hardware and network monitoring and server monitoring both on and off and on site. Security configuration for routers, switches, and load balancers Implemented company policies, technical procedures and standards for preserving the integrity and security of data, reports and access. Tasked with implementing process & procedures for monitoring and analyzing performance of websites. Mcafee and Systematic integration, management, and support Managed PC migration across distinctive ecosystems including, Microsoft, Linux and MAC, including PC software/hardware migration. Wired and Wireless snorting and logging Managed internal Active Directory Group Policies and enforced user security Managed and setup implementation of Microsoft Exchange Server and user configuration VNC and OpenVPN configuration and management Education Master in Cyber Security in Cyber Security The University of Maryland College Park - College Park, MD Bachelors of Science in design The University of Maryland College Park - College Park, MD Associate of Applied Science in depth programming County College of Morris Randolph Skills Encase (4 years), LAN (2 years), Linux (5 years), MAC (2 years), UNIX (2 years) Links https://www.linkedin.com/in/michael-czarnecki-421849ab Additional Information Technical Abilities Platforms: Windows 7/8/8.1/10, Windows Server 2012 R2, UNIX, Linux (Red Hat, Ubuntu, Mint), Mac OS, Android, iOS, Blackberry, Windows Mobile OS, Virtual Machines Networking: LAN / WAN Administration, VPN, TCP/IP, SMS/SQL,Cisco Routers & Switches (Configuration), VoIP

Languages: HTML/HTML 5, Java, JavaScript, PHP, CSS, Python Tools: PRTG, Glasswire, Wireshark, Metasploit, Back Track, and Nessus, HEAT, JIRA, HP, ZEN Desk, Cisco, AVAST, Mcafee (IPS), Carbon Black, Teamviewer, VNC Windows Server 2012, qTest, TestFLO, QualysGuard, OpenVPN, DNSCrypt, Filezilla (Client and Server) VMware, Kali Linux, NMAP, SolarWinds, Malwarebytes, Fireye, EnCase, Hyper-V, Snort, Splunk, Frotifty, Burp Suit, Redline, MSS Blue Coat, IBM Resilient, and Remedy, Checkpoint, Fireeye, Trustwave, AWS Cloudwatch/CloudTrail, Recorded Future, Trustar, Dome9, Maice, Trustar, Risk Fabric

Name: Andrew Thompson

Email: bmunoz@example.com

Phone: (286)831-5150x407