IT Security Consultant (Incident Response) IT Security Consultant (Incident Response) IT Security Consultant (Incident Response) Austin, TX Work Experience IT Security Consultant (Incident Response) Maricopa Community College June 2018 to January 2019 Developing Documentation run books for best practices. ? Lead asset in building out incidence response team. ? Leveraging Firesight Sourcefire for indications of events or incidents. ? Tracking down users that have broken Security compliance rules and retraining them on proper search habits. ? Running Virus scans within Kaspersky and triaging results as needed. ? Working with various departments and vendors to Block, unblock, recategorize and troubleshoot various events. ? Working with a variety of Trojans, worms, and botnets. ? Making critical judgement calls as to whether to isolate the host from the network. ? Instrumental in the implementation and buildout on the incident response applications and foundation. ? Analyzing traffic to analyze user search habits and to rule out false positive alerts. ? Experience in administering, and configuring. ? Information security assessment of one or more centralized endpoint information security technologies (device management, malware protection, application whitelisting/blacklisting, patch management, software deployment, ? Running Nmap scans to determine vulnerabilities such as ports open and to scan ip addresses. ? Working to implement policies to block adware as a security precaution. ? Escalating incidents as needed to the appropriate departments IT Security Analyst Incident investigative Response June 2016 to May 2018 Monitored, analyzed, and performed front-line extensive investigations of cyber security risks and compliance ? Identified potential and current cyber threats and actively worked to prevent or eliminate threats. ? Analyzed network and host-based security logs to determine remediation actions and escalation paths. ? Independently followed procedures to contain, analyze, and eradicate malicious activity. ? Owned and managed tickets through to resolution. ? Escalated events to specific groups in a timely matter ? Troubleshooting agents that are not reporting, tagging of servers and enabling real-time monitoring. ? Blocked and unblocked various sites upon conclusive investigations. ? Monitored tickets for security alerts and events from various applications. ? Ability to work with multiple Departments upon confirming an incident. ? Develop and maintain Computer Security Incident Response processes and procedures. ? Experience with

Building and maintaining awareness of the broader context and implications of the various types of risk affecting the business (e.g., financial, legal, reputation, etc.) ? Isolating systems in Carbon Black ? Remove Malicious files via Carbon Black live ? Creating Policies via Carbon Black ? Creating Documentation Run books for Best practices and Troubleshooting tips ? Experience with NIST 800-53, and ISO 27001/27002 security frameworks. ? Working with travel policies and blocked country list. IT Security Specialist Entergy/HCL April 2013 to June 2016 Handles issues such as access requests, password changes, and turning profiles on and off again. ? All support was done remotely using ticketing systems or office communicators. ? Analyze, review, Approve and gather documents pertaining to Access request process Creating tickets as issues arise and elevating if necessary. ? Following CIP demands for removing access in a timely manner such as within 24 hours after firing, or Hiring. ? Resetting passwords, basic troubleshooting and interacting with the business area. ? Perform daily monitoring of Security Incident and Event Management system and fine tuning. ? Coordinating with Managers and coworkers to grant access in a timely manner. ? Previously trained and supported internal and external users one FERC.. ? Verifying that applicant keeps with guidelines of FERC processes and procedures. ? Developing processes and coordinating compliance throughout the enterprise. ? Strong analytical problem solving skills with the ability to make a decision with little to no supervision. ? Adding and removing roles using Active Directory for Authorized and unauthorized users. ? Configured User Accounts and group Policies IT Specialist Tenaris February 2009 to April 2013 Education Smithville High School - Smithville, TX Certification Cybertex Institute Of Technology Austin Texas New Horizons Computer Learning Center Skills Acrobat (Less than 1 year), Active Directory (3 years), Adobe Acrobat (Less than 1 year), DNS (Less than 1 year), Excel. (Less than 1 year), Exchange (Less than 1 year), FERC. (3 years), ITIL. (Less than 1 year), JIRA (Less than 1 year), Mac (Less than 1 year), MAC/OS (Less than 1 year), Microsoft Outlook (Less than 1 year), MICROSOFT SHAREPOINT (Less than 1 year), MICROSOFT WINDOWS (Less than 1 year), MS Exchange (Less than 1 year), MS SQL SERVER (Less than 1 year), Nmap (Less than 1 year), Outlook (Less than 1 year), PowerPoint (Less than 1 year), Printers (Less than 1 year), Information Security, Cissp, PCI, It

Security, Cisa, Siem

Name: Ronald Woods

Email: lguerra@example.com

Phone: 572-993-2171