Cyber Defense Security Analyst Cyber Defense Security Analyst Cyber Defense Analyst - Defense Point Security San Antonio, TX Cyber professional proficient in online security research, planning, execution, and preventive measures. Possessing a solid background in network configuration and monitoring, a strong ability to install security software, and operational to counteract cyber threats, either in small businesses or in corporate settings. Work Experience Cyber Defense Security Analyst Defense Point Security - San Antonio, TX October 2017 to Present Supports Cyber security functions for 5 enterprise clients operating in various industries. Duties help build and preserve confidentiality, integrity, and availability of information technology resources. ? Leverages various toolsets to monitor and analyze network traffic, IDS/IPS, and event logs from multiple sources. ? Supports a team of engineers on ongoing security operations, including the analysis, creation, and tuning of alerts (to avoid false positives/negatives) generated by security appliances, such as SIEM and IDS/IPS. ? Performs initial investigations, provides reporting to customers daily on network and system level attack vectors; and recommends mitigation techniques. ? Works with the engineering team to ensure endpoints and devices security through defense in-depth. ? Explores OSINT such as HSIN, Fortinet, nvd.nist.gov, US-CERT, iDefense; and malware scanning portals to maintain a deep understanding of current threats, vulnerabilities, attacks and countermeasures and proactively suggests recommendations. ? Determines threats to the environment and creates tickets (JIRA, Remedy, ServiceNow) to track resolution. ? Participates in updating the internal KB system (SharePoint) and Standard Operating Procedures ? Documents security events, investigates and writes comprehensive reports of incident investigations to appropriate management personnel. ? Collaborates to effectively ensure the on-boarding of new hires through training and guidance. IT Specialist e-Global Technologies - Houston, TX October 2015 to October 2017 Performed network vulnerability assessments using security tools to evaluate attack vectors, detect system vulnerabilities and implement remediation procedures and security measures. Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools. Investigated possible security violations in order to identify threats and provides countermeasures and policy updates.

Configured, managed, and ensured the continuous monitoring of network defense systems such ASA firewalls and routers Configured and troubleshot network devices and servers, Web application firewalls and proxies to harden network security. Monitored the system backup/recovery procedures and incidence response to minimize losses in case of outages/breaches, Supported a team of Engineers with hardware and software issues (OS, security patches, application upgrades, and etc.) Resolved and reviewed a database of problems/requests or incident management using a tracking application such as BMC. Constantly raised user awareness and educates management about threats trough technical documentation. Education Bachelor of Science in Computer Networks and Security University of Maryland - Adelphi, MD Skills Ids (3 years), Ips (3 years), malware (3 years), Security (3 years), Siem (3 years), Cyber Security, Nist, Cybersecurity, Linux, Information Security, Comptia, It Security, Network Security, Malware Analysis (2 years) Certifications/Licenses Splunk Certified Power User Present CompTIA Security+ April 2017 to April 2020 CCNA Security February 2017 to February 2020 CCNA Routing and Switching December 2015 to December 2020 TestOut PC PRO December 2012 to Present CompTIA CySA - In Progress Assessments Technical Support Highly Proficient March 2019 Measures a candidate's ability to apply protocols to identify errors and solutions in order to maintain system function. Full results: https://share.indeedassessments.com/share_assignment/h2hb-yyvnoeguaap Indeed Assessments provides skills tests that are not indicative of a license or certification, or continued development in any professional field. Additional Information TECHNICAL SUMMARY IDS/IPS: Signatures Writing, Bro, Snort, OSSEC, Suricata Intrusion / Security: Snort/Firepower, ASA/ Zone-based firewall, Proxies, Web Application Security Vuln. Scan: Nessus, Retina, MBSA, OpenVAS, Qualys.

Threat/Malware Analysis and Detection: IDA Pro, WinDbg, Remnux, SIFT, Splunk, IDS/IPS, System Log Forensics, Wireshark, TcpDump, TShark, SIEM, FireEye, RSA Netwitness, Web App. Vulnerability: BURP Suite, HP's WebInspect, IBM AppScan, Acunetix WVS. Monitoring: SolarWinds Orion, Zenoss, PRTG Network Monitor, Nagios, Windows Event Log. Cloud Security: McAfee ePO, Zscaler, Blue Coat Incident Response (collection, investigation, unequivocal

validation, escalation and Lessons Learned). Cyber Forensics: AccessData FTK, Encase Guidance Software. Data Loss Prevention & Security: Tripwire, Zix, HIPS, HBF Net. Access: Firewall (Imperva, ASA, Palo Alto, Barracuda, Check Point), 802.1x, ISE, Radius, Tacacs+ Scripting & Others: Python, PowerShell, C/C++, Visual Studio, Visual Basic, and MS Access Operations: LanDesk, IPScan, Endpoints and Mobile Device security: OS: Microsoft Windows, Linux Ubuntu, and Mac. TCP/IP & Routing: OSPF, EIGRP, RIP, IS-IS, eBGP, Frame-Relay, MPLS, etc. Protocols: SSH, HTTP/S, SMTP, RDP, DNS, S/FTP, DHCP, CIFS/NetBIOS, LDAP, SNMP, and more. OSI and DoD reference models. IAM: AD, LDAP, SSO, Federation.

Name: Colin Brown

Email: williamsdavid@example.com

Phone: (863)403-6148x448