Cybersecurity Analyst/Instructor Cybersecurity Analyst/Instructor Cybersecurity Analyst/Instructor - DCI Resources LLC Work Experience Cybersecurity Analyst/Instructor DCI Resources LLC - Bridgeport, CT July 2018 to Present   Perform automated and manual security assessments to identify configuration and patch related vulnerabilities using commercial and open-source tools. Gathering all the required information from IDS, and Wireshark to investigate some of the attacks Identifying, triaging, and remediating threats and vulnerabilities as a security operation monitoring (SOC)   Identify network intrusions by aggregating and correlating all reported events from various devices   Execute appropriate mitigation strategies for identified threats.   Perform security incident response & incident handling based on risk categorization & by the established procedure   Perform incident containment and eradication activities as needed, and support post-incident activities, including reporting and lessons learned   Documenting incident results and reporting details through the ticketing system   Automate frequent tasks and produce custom scripts using Powershell and python   Performed real-time proactive security monitoring and reporting on various security enforcement systems, such as Splunk (SIEM), anti-virus, internet content filtering/reporting, malware code prevention, firewalls, IDS & IPS, Web security, and anti-spam.   Knowledgeable and experienced in the installation, configuration, and administration of Windows Servers 2000/2003/2008/2012/2016, SCCM, Active Directory, GPOs, DFS, FTP, DNS, DHCP, TFTP, Ubuntu, Red Hat Linux OS under LAN and WAN environments, implementation of name resolution using WINS and DNS in the TCP/IP environment.   Provide training in the following topics: cybersecurity, ethical hacking, CompTIA Security+, Pentest+, Network+, A+, and MTA Security, cloud, networking and CCNA Cybersecurity Graduate Research Assistant Sacred Heart University - Fairfield, CT January 2018 to June 2018   Published five cybersecurity-related research papers in IEEE and SSIC conferences   Assisted graduate students in-class assignments and provided lectures   Knowledgeable in cyber kill chain framework, OWASP, machine learning, and digital forensics tools (AccessData)   Utilized AWS, GCP and chameleon cloud to deploy virtual instances, Ansible and Terraform for automation, Docker, Kubernetes, deployed a three-tier application in AWS, Nessus, Wireshark, Nmap, OWASP ZAP, and SpiderFoot. IT Security Consultant Population

Services International, Techno Brain IT Solution, Addis Ababa University - Addis Ababa, ET January 2016 to July 2017   Analyzed network traffic captures and network mapping using Wireshark, Nstat, ZenMap, AirCrack, NetStalker, etc.   Designed, installed, and configured secured enterprise standard controller-based Ruckus wireless network with multi-factor authentication and server farm wired network.   Excellent understanding of secure data storage and transport implementations (PGP, SSH, SSL, IPSEC), Windows system administration, and security assessment skills, including Active Directory.   In-depth knowledge of TCP/IP, IEEE 802.11, wireless, and routing protocols.   Utilized Security Information and Event Management (SIEM), Intrusion monitoring, IDS, IPS, Data Leakage Prevention (DLP), and System Center Configuration Manager (SCCM) Knowledge of email and web filtering, TMG, Websense, Cyberoam, and McAfee Site Advisor. Provided training on Windows Server Infrastructure 2008, 2012, Private Cloud training and Core and Advanced Solutions of Exchange Server 2013   Designed, installed, and configured Active Directory Domain Services (ADDS), GPOs, DNS, DHCP, and WSUS.   Maintained IT services: mail, ADDS, DNS, DHCP, file and print servers Information Technology Specialist World Vision - Addis Ababa, ET December 2015 to December 2015 - Dec 2015   Developed a business case for a centralized storage solution, prepared technical specification and implemented Storage Area Network (SAN)   Perform Risk Assessment, gap analysis, and create a Risk Mitigation Plan. Experience configuring and deploying McAfee modules and products like McAfee ePO, McAfee VSE, McAfee HIPS, McAfee Endpoint Encryption, McAfee Network DLP, McAfee DLP Endpoint, McAfee SIEM.   Oversee vulnerability assessment/penetration testing of scoped systems and applications to identify system vulnerabilities.   Hands-on experience with creating regular expressions for any signatures   Prepared ToR for datacenter infrastructure standardization project, evaluated, supported & managed the overall project implementation System Administrator World Vision - Addis Ababa, ET October 2013 to November 2015   Prepared ICT infrastructure security baseline survey, vulnerability scan, and recommended countermeasures   Managed all client systems from endpoint perspective using McAfee ePO tool which includes managing Agent, VSE, pushing client tasks, managing ODS & OAS scans   Administered unified threat management

gateway (Cyberoam), URL filtering and Cisco firewall   Prepared Service Improvement Plan (SIP) based on ITIL framework for datacenter virtualization & service upgrade   Implemented datacenter virtualization and upgraded all servers operating systems from Window Server 2003 to 2008 R2 without service downtime   Administered Security Information and Event Management (SIEM), IDS / IPS, and Data Loss Prevention (DLP) Acting ICT Infrastructure Unit Coordinator World Vision - Addis Ababa, ET February 2015 to June 2015   Prepared for 15 cluster program (regional offices) standardized network infrastructure project Terms of Reference (ToR), evaluated the technical documents and supervised the implementation   Prepared enterprise standard wireless network ToR for Head Quarter and evaluated the technical document, supported and supervised the overall project implementation   Managed and supported 54 Area Program (branch offices) wireless network implementation project   Developed a Disaster Recovery Plan (DRP) policy and implemented as per the policy document   Prepared and implemented backup and restoration policies and procedures Senior Server and Storage Systems Administration Engineer Ethiopian Revenues and Customs Authority - Addis Ababa, ET December 2011 to October 2013 Successfully implemented and administered System Center Configuration Manager 2012 R2 (SCCM)   Successfully implemented Microsoft Dynamics CRM and Microsoft Lync server for call center project   Successfully implemented and operated Symantec Backup Exec 2012 tape backup system   Installed and configured Net App Storage (SAN) and manage HP EVA 5000 SAN Storage   Successfully upgraded Network infrastructure OS from Windows Server 2003 to 2008 R2, and RHEL 5.5 to 6.0   Successfully installed and configured blade servers and implemented datacenter virtualization   Successfully upgraded Microsoft Exchange Server 2003 to 2010 for around 2000 mail users(mailboxes) Information System Security Engineer Ethiopian Revenues and Customs Authority - Addis Ababa, ET May 2011 to December 2011   Successfully implemented Web-sense Unified Threat Management Gateway   Administered ASA Firewall, IPS, IDS, Web Sense, TMG Servers, ACS, and VPN   Coordinated Security testing initiatives and handled physical security Applied patches /fixes/ to prevent vulnerabilities to all security-related assets /firewall, router, switches, ACS server, certificate server, mail gateway, DMZ servers, antivirus, web security, and

ISA/TMG servers/ Network Administrator Ethiopian Revenues and Customs Authority - Addis Ababa, ET March 2009 to May 2011   Installed and Configured communication devices for new headquarter building access and core switch and routers   Installed, configured Antivirus Server and periodically roll out updates to networked devices   Established seven medium-size datacenters for branch offices   Supported 209 branch offices connectivity problems and resolve issues, administered LAN and WAN Web Developer Ethiopian Revenues and Customs Authority - Addis Ababa, ET August 2008 to March 2009   Plan website related works, web site design, website kit development   News upload to the website, update information and upload FAQs, etc. Network Operation Technician Ethiopian Revenues and Customs Authority - Addis Ababa, ET April 2005 to August 2008   End-user support, network technical support and LAN Administration   Troubleshoot, diagnose and resolve hardware, software problems of Desktop Computers, Laptops, and other IT equipment like printers, scanners, fax machine, etc. Programmer Visions of St. Mary's Information Technology LLC - Addis Ababa, ET September 2004 to April 2005   Gathered system requirements   Analyzed and designed the system, implemented a database of the system & wrote source code for the system   Prepared system and user manual documentation and conducted system usage training Education MS in Cybersecurity in Cybersecurity Sacred Heart University - Fairfield, CT December 2018 Bachelor of Science in Computer Science Addis Ababa University - Addis Ababa, ET July 2009 Associate Degree in Computer Science St. Mary's University - Addis Ababa, ET July 2004

Name: Brad Cruz

Email: banderson@example.org

Phone: 545.661.5875