Security Analyst Security Analyst Cyber Seucrity Professional Knoxville, TN Led $30-35K annual penetration tests at Edfinancial, identified and classified cybersecurity issues, and developed mitigation plans to ensure compliance with the company's vulnerability management program. Identified 5K+ cybersecurity issues at Edfinancial by automating vulnerability assessment scans and report generation for 500+ corporate systems - including VoIP servers, network servers and workstations. Trained two junior security analysts at Edfinancial on risk assessments, and provided host-based security for 35K+ systems using Anti-Virus, Host based firewalls, HIPS and HDLP products while at SAIC. Gained Edfinancial executive buy-in for the implementation of Cisco Umbrella services, which acted as the first line defense technology for 500+ systems against internet threats. Established a $240K+ Computer Network Defense (CND) non-production network for the US Navy - its first ever - to participate in joint military Computer Network Defense exercises. Saved $750K+ in contractor and outsourcing costs and served as Project Lead on three IT restructuring projects while in the US Navy, in addition to leading 110 personnel as IT Division Manager. Authorized to work in the US for any employer Work Experience Security Analyst StaffingSolutions - Knoxville, TN August 2019 to Present My partnership with Staffing Solutions, which is one of the largest providers of temporary workforce solutions throughout the Southeast US, helped introduce me to the following company: Covenant Health, Knoxville, TN A healthcare network with nine acute-care hospitals, outpatient and specialty services, and Covenant Medical Group the company's fastest-growing physician practice division. Analyze and investigate security events/threats to determine appropriate action; responded directly to clients needs and claims and follow-up on client incidents; support endpoint protection and vulnerability management activities reporting to the Senior Security Analyst. Create, update, transfer, and close security-related helpdesk tickets using EasyVista IT Service Management (ITSM) software. Audit files for sensitive data; partner with teammates and other business groups to research, assess, and recommend security control to enhance protection of sensitive data. Utilize McAfee ePolicy Orchestrator (ePO) to identify endpoint devices using McAfee Endpoint Encryption, Virus Scan Enterprise (VSE), and Host-Based Intrusion Prevention (HIPS); removed McAfee products for

migration to Trend Micro. Performed security event monitoring of heterogeneous network architecture using Trend Micro OfficeScan Endpoint Encryption, Data Loss Prevention (DLP), Anti-Virus, and Endpoint Firewall. Analyze endpoint application data in real-time to identify potential threats, rogue systems, vulnerabilities, unauthorized devices and/or system changes, and data loss prevention. Conduct assessments and report vulnerabilities of non-complaint systems; create tickets to monitor ongoing management of critical and high vulnerability using Vulnerability Priority Rating (VPR) summaries. Information System Security Analyst Edfinancial Services LLC - Knoxville, TN October 2012 to May 2018 A financial company which provides student loans servicing for 15 of the top 100 lenders in the USA, including regional and national banks, secondary markets, state agencies, and other student loan providers. In charge of maintaining network security appliances, systems and software risk assessments, network vulnerability scanning, and development of Standard Operating Procedures as well as accreditation documentation. Conducted system vulnerability as well as virus and malware security threat reviews, monitored and coordinated the resolution of security incidents, and reviewed and updated IT system security policies. Maintained and configured the Cisco Firepower Management Center (FMC) Access Control Policies (ACP), IPS Policies, malware and file policies, and other configuration settings deployed to FMC managed devices. Used Nipper Studio to conduct configuration audits on various appliances, and executed complete system as well as network vulnerability and compliance scans using Tenable Security Center and Nessus vulnerability scanners. Analyzed network traffic packets captured by the Sourcefire Intrusion Prevention System while leading system and software risk assessments through user-friendly and automated tools, controls and open-source research. IT Security Analyst Science Applications International Corporation - Oak Ridge, TN June 2010 to September 2012 A premier technology integrator solving the nation's most complex modernization and readiness challenges across the defense, space, federal civilian and intelligence markets. Responsible for managing information security infrastructure and the McAfee ePO (ePolicy Orchestrator) infrastructure as well as the deployment of new software, upgrades and security patches. Ensured optimal security for agency systems and infrastructure, directed and

maintained system and network security devices, and also conducted system patching, virus detection and auditing functions. Handled configuration management and vulnerability assessments through effective utilization of commercial and non-commercial software, and administered Remedy tickets in multiple ticketing queues. IT Security Analyst SCI Consulting Services Inc - Oak Ridge, TN November 2007 to June 2010 A company servicing the US Federal Government, Coast Guard, Department of Homeland Security, Department of Energy and the Environmental Protection Agency through partnerships with SI integrators, SAIC, CSRA, and Unisys. Accountable for leading the security operations of multiple departments by monitoring, reviewing and recommending remediation course of actions for threats and vulnerabilities aimed at the IT infrastructure. Coordinated information assurance efforts with federal agencies and the US-CERT, led security analysts and conducted vulnerability and compliance assessment scans on operating systems, websites and databases. Analyzed IDS events to determine the validity of threats, documented false positives and real-world threats through the submission of service desk tickets, and ensured secure final resolution of help desk tickets. Managed incident response and technical investigations, and mentored juniors on information security policies and emerging technologies as well as agile methodologies. Cryptologic Technician United States Navy August 1987 to August 2007 The naval warfare service branch of the United States Armed Forces, and the largest and most capable maritime force in the world. In charge of operating state-of-the-art computer systems to conduct information operations, collecting and analyzing signals of interest to identify global threats, and safeguarding access to classified material and information systems. Conducted Department of the Navy vulnerability assessments and limited penetration tests, planned and managed organizational network architecture, and evaluated network security and mapping software for the Navy. Education Bachelor of Science in Computer Information Systems Florida Institute of Technology - Melbourne, FL Skills Security, FISMA, HIPAA, Information security, NIST, Proxies, Data architecture, Data governance, Middleware, Systems analysis, Cots, Architecture, Strategic planning, Asset management, Scanning, Risk assessments, Operations, Training, Governance, Linux, Siem, Cyber Security, Network Security, Comptia, It Security, Endpoint Security,

Information Assurance, Vulnerability Management Military Service Branch: United States Navy Rank: E7 Certifications/Licenses Certified Ethical Hacker (CEH) October 2015 to November 2021 CompTIA Advanced Security Practitioner ce (CASP+) January 2018 to January 2021 CompTIA CySA+ ce November 2018 to November 2021 CompTIA Security+ ce April 2019 to April 2022 Additional Information AREAS OF EXPERTISE Information Security Security Compliance and Controls Strategic Planning Executive Leadership Training & Development IT Architecture Risk Assessments Data Asset Management Vulnerability Scanning Vulnerability Management IT Systems Analysis Data Architecture Troubleshooting Data Governance Information Operations Middleware Management Technical Writing COTS Software & Hardware Network Proxies NIST, FISMA & HIPAA Regulations

Name: Susan Davis

Email: ebarton@example.com

Phone: 688.586.3943x957