IT Specialist IT Specialist IT Specialist - DoJ Fairfax, VA Experienced IT security professional with diverse experience that spans both commercial and Federal environments. Possess extensive knowledge in Cyber Security, secured systems administration, and SOC operations. Work Experience IT Specialist DoJ - Fairfax, VA August 2008 to Present * Use Splunk and other SIEM tools to perform monitoring of security events. * Manage day-to-day security operational tasks such as security event monitoring, log monitoring, security incident management, and compliance monitoring. * Manage inbound requests via ticketing system, as well as via telephone calls, and provide security notifications. * Review RFC requests for security policy compliance and best practice. Network Security Analyst (DHS/US-CERT) InfoTek Corp - Arlington, VA August 2015 to June 2018 * Analyze alerts using ArcSight. * Traffic analysis using NetFlow. * Packet analysis using Wireshark. * Incident management using Remedy. * Research security information using Open Source Reporting. * Research threat information using Classified Reporting. * Monitor and analyze network traffic, IDS, security events and logs. * Identify and investigate malicious activities or other events which violate security policies. * Prioritize and differentiate between potential intrusion attempts and false alarms. * Create and track security investigations to resolution. Information Security Engineer DoJ August 2014 to August 2015 * Investigate suspicious traffic alerts and recommend preventive, mitigating, and compensating controls. * Assess threats, risks, and vulnerabilities from emerging security issues. * Collect forensic evidence from compromised machines and logs. * Install and maintain security assessment systems: McAfee IPS/IDS and Splunk. * Assist in the development of access-controls, separation of duties, and roles. * Participate in security briefing with management regarding InfoSec incidents and issues. * Review RFC requests for security policy compliance and best practice. * Attend to the security needs of multiple sites both during and after business hours. * Ensure uptime, availability, and integrity of network security systems. SOC Analyst Silver Rhino/CSC - Arlington, VA August 2013 to August 2014 DHS/TSA-ITIP) * Work in 24x7/365 EMOC/SOC environment supporting TSA, where high availability is critical to the end user community. * Support the Transportation Security Administration (TSA) Network infrastructure by proactively monitoring the network and isolate point

of failures to a quick resolution. * Provide technical support in accordance with SLA time frame using BMC Remedy. * Coordinate with Messaging teams to implement Exmerge, Message Tracker, and remote configuration of Blackberry phones. * Implement malicious scans, proxy blocks, and antigen filters as requested by SOC. * Disconnected/disable/configure affected equipment in the network per SOC request. * Updated antivirus software definitions on existing equipment remotely. * Monitor and track scheduled Request for Changes/Break Fixes/Ongoing Maintenances and system anomalies that are logged in daily shift log and daily report to management. * Research and resolve technical/operational questions from end users' community. * Prepare reports for: IDS, Nessus, Symantec, SLAs, and others as requested by managers. * Provide shift reports, and support the security center with incidents tracking. Information Security Tech JSS - Arlington, VA January 2009 to August 2013 Information Security Tech * Monitor and investigate IDS and firewall logs for potential threats and vulnerabilities. * Building and hardening servers and workstations based on NIST recommendations. * Install, configure, and administer Oracle Application Servers. * Responsible for weekly enterprise anti-virus updates. * Integrate Oracle's OID with Microsoft Active Directory. * Respond to emergency and time-sensitive requests both during on and off hours. * Research and recommend equipment purchase appropriate for customers' environment. Sr. System Engineer JSS January 2008 to January 2009 * Participate and assist in the design of a new network domain, based on the implementation of Microsoft Exchange2007 and Microsoft SMS for improved system security, reliability, patching, and software delivery. * Evaluate and recommend appropriate software products for proposed standard environment to assure compliance with proposed architecture and system security. * Planning and configuration of server naming, network naming, network directory services, and network synchronization tools. * Built single and/or multiple users' profiles and migrated desktop settings and networking preferences from Exhange2003 environment to Exchange2007. * Additionally, responsible for stabilization of current network to insure proper operation of existing topology and to ease conversion to new domain. * Work on both unclassified and classified account access troubleshooting. * Perform server OS hardening as required for security policies and industry best practice. Network Administrator IBM - Chicago, IL January 1998

to May 2007 * Building, monitoring, and troubleshooting Windows, Linux, UNIX, Netware, Exchange, Oracle, and SQL servers to optimize network performance. * Planned, scheduled, and coordinated rollouts, upgrades, and patches. * Worked on a potential design of Windows 2003 internal network using Active Directory, DNS, DHCP, System Security, and other services. * Determination and implementation of systems performance tuning for specialized financial software. * Managing users' accounts on Active Directory and Netware. * Monitoring and supporting Telecom/Voice Response System. * Work with and coordinate software support and troubleshooting with outside vendors. Education M.S., Telecom Systems DePaul University - Chicago, IL B.S. in Business Administration. Trinity College Skills Splunk, ArcSight, Information Security, It Specialist, Information Technology Certifications/Licenses CISSP Security+ CNA Additional Information SKILLS: * Security Technologies: Arcsight, Splunk, SiLK, Wireshark, Websense, Tripwire, PGP, VirusTotal, iSight, Looking Glass, Active Trust Dossier, Anti-Virus (Norton, Symantec, Ghost), Avocent, Snort, Citrix, HP OpenView, Insight Manager, McAfee IDS/IPS, Integrity, ISA, Nessus, NetIQ, Sidewinder, VMware. * Networking: LANs, WANs, VPNs, Routers, Firewalls, and TCP/IP. * Operating Systems: Windows, Linux, and UNIX.

Name: Dawn Mills

Email: bennettjasmine@example.org

Phone: (779)738-4423x90269