Security Operations Analyst (SOC) Security Operations Analyst (SOC) Security Operations Analyst (SOC) - Agile Defense Largo, MD A position to further develop my proven technical skills in the information technology field. Also to be offered the opportunity for growth based on demonstrated abilities and accomplishments. I have proven my reputation for customer service, with strong interpersonal skills. I am a great communicator and a Team Player with the ability to work in a fast-paced and high pressure environment whether I am working a site alone or with a team. Authorized to work in the US for any employer Work Experience Security Operations Analyst (SOC) Agile Defense - Reston, VA March 2016 to Present Conduct Network Monitoring and Incident Response operations supporting 24x7x365. Perform real-time analysis to provide network and data security using SPLUNK, Content Security Management Appliance, Palo Alto, FireEye and SourceFire. Document all client communications. Work in a team environment and monitor the health and wellness of security devices on our client's networks. Resolve client issues by taking the appropriate corrective action, or following the appropriate escalation procedures. Perform packet and malware analysis. Review Open Source Intelligence for cybercrimes and APTs. Stay current with common intrusion Detection Systems, virus and malware behavior, and intrusion methodologies. Maintain knowledge of the current security threat level by monitoring related internet postings, intelligence reports, and other related documents as necessary. Responsible for determining appropriate response action(s) required mitigation risk and providing threat and damage assessment for security threats which may impact the customer networks. Utilize case management processes to properly document incident, alert message, PCAP and analysis tools. Possession of excellent initiative, analytical, and critical thinking skills. Ability to learn and operate in a dynamic environment. Ability to pay strict attention to detail, logic, and solution orientation and learn and adapt quickly. Agile Defense - Fort Belvoir, VA October 2017 to March 2018 Network Operations Security Center (NOSC) The Network Analyst provides third-tier support to Help Desk Analysts, supports the evaluation of network-based hardware and software, implementation plans for these items, the ability to take the lead or supporting role on special projects as assigned. Conduct administration of NOC network-monitoring systems using Solarwinds and SCOM for both NIPR and

SIPR. Monitors network systems for error conditions, performance issues, and attempted intrusion. Observes computer systems, peripheral equipment, and network monitors to detect error conditions; Conduct periodic and scheduled testing to ensure that network operations are performing to normal standards; Corrects minor problems on network systems and notifies the correct personnel of the problem, and initiates proper recovery procedures. Performs network account administration and system administration of identified DTRA servers. Understanding of ESXi hosts and virtual machines with VServer via the VSphere client. Ability to work effectively independently as well as within a team environment. Excellent Communication and writing skills. Demonstrated a strong work ethic and ability and willingness to take on new challenges. Network Operation Center Analyst Agile Defense - Reston, VA October 2011 to October 2017 The Network Analyst provides third-tier support to Help Desk Analysts, supports the evaluation of network-based hardware and software, implementation plans for these items, the ability to take the lead or supporting role on special projects as assigned. Conduct administration of NOC network-monitoring systems using Solarwinds and SCOM. Monitors network systems for error conditions, performance issues, and attempted intrusion. Observes computer systems, peripheral equipment, and network monitors to detect error conditions; Conduct periodic and scheduled testing to ensure that network operations are performing to normal standards; Corrects minor problems on network systems and notifies the correct personnel of the problem, and initiates proper recovery procedures. Performs network account administration and system administration of identified DARPA servers. Installs pre-configured Servers in the Computer Room. Coordination, distribution, and tracking the use of static IP addresses for the DARPA networks. Monitor and manage email zip quarantine after-hours. Maintains contact with the Networking and Software groups to ensure all systems are operational. Monitor EMS tool for all network support facilities using including Power Distribution Unit; Uninterruptible Power Supply, HVAC, Fire Protection Systems, and Access Control equipment; Correction of minor problems and notification of venders and expert staff when necessary. Performs power shutdown and power-up procedures in cases of network power outages Answers and supports incoming, after-hours, customer help desk issues Senior VIP Support Analyst Agile

Defense - Reston, VA April 2015 to March 2017 Provide day-to-day technical assistance to high end customers for a Government agency. Support government and contractor personnel for PC\MAC and associated software packages, network services and Internet applications. In-process and out-process personnel which can include requirements analysis, training and assistance as required. Provide troubleshooting and installation of printers, VTC's, desktops, laptops and Cisco VPN client. Review daily or long term requirements and make recommendations for improvement. Create Remedy tickets for customer service requests and thoroughly document work logs. Maintain compliance with Standard Operating Procedures (SOPs). Troubleshoot clients using remote tools like SCCM and Bomgar console. Configure, deploy, troubleshoot and update all types of smartphones. Administer all smartphone using AirWatch and GMC. Restore and backup customer's data thru CommVault. Configure ACAS scans to make sure systems are IAVA compliant. Executive Support Engineer II Northrop Grumman - Fort Belvoir, VA February 2012 to April 2015 Provides tier II-III support to Senior Executives, General Officers, Flag Officers, Military officers and federal civil employees. Troubleshoot all hardware and software issues on ULAN\ CLAN computers, thin clients, thick clients and zero clients. Provide remote assistance thru Configuration Manager Console. Provide account administration thru Active Directory for both ULAN\CLAN network. Configure and administer Smartphone and blackberry devices. Distribute software packages to workstations using SCCM. Position also includes Hardware Engineering and assisting Network Engineering with minor project work such as writing white papers, executing manual desktop installations, researching problems and proactively conducting maintenance for customers as well as contributing to enterprise projects. Lead for Apple device configuration and deployment. Over the course of past 3 years I have deployed over 75 iPhone's and iPad's. I am knowledgeable with using GOOD Technology and AirWatch. Strong experience with mobile devices such as the iPhone, iPad, Android, Windows mobile, and/or Blackberry from an integration, use and deployment perspective (Apple and Android devices of primary interest). Understanding of the unique security issues related to mobile device use and connectivity; especially in federal government environments. Working knowledge of Citrix and related technologies. Senior Computer Support Analyst DARPA - Arlington,

VA 2010 to 2012 Provide day-to-day technical assistance to high end customers for a Government agency. Support government and contractor personnel for PC\MAC and associated software packages, network services and Internet applications. In-process and out-process personnel which can include requirements analysis, training and assistance as required. Provide troubleshooting and installation of Blackberry's, printers, VTC's, PC's, laptops and Nortel/Cisco VPN client. Review daily or long term requirements and make recommendations for improvement. Create Remedy tickets for customer service requests and thoroughly document work logs. Maintain compliance with Standard Operating Procedures (SOPs). Troubleshoot clients thru SCCM console and patching. Configure, deploy, troubleshoot and update iphones and ipads, also configure iDevices with GOOD. Restore customer's data thru Atempo (LiveBackup), make sure systems are IAVA compliant IT Resource Analyst I Institute for Defense Analyses - Alexandria, VA 2006 to 2010 Provide technical support for microcomputers systems, which include Macintoshes and PCs. Responsibilities include coverage for Tier 2 Help Desk tickets in a REMEDY environment. Account administration thru Active Directory and Exchange console. Install new and reconfigure reassigned systems by backing up old system, and installing a current operating system and reinstalling old upgraded or new approved application software. Responsible for researching and resolving system or remote access problems for users. Assist with the network portion of new and reassigned system installations and system disposal. Ensure that workstations are properly configured to receive patches, other critical updates and to provide software and hardware census information to the corporate asset management system. Senior Micro-Computer Technician Institute for Defense Analyses - Alexandria, VA 2003 to 2006 Respond promptly to user questions on hardware and software problems submitted via the Remedy Help Desk System. Updates Remedy database to reflect tasks performed and issue resolutions. Inspects new computer hardware deliveries in the Purchasing Department; ensures conformity with stated requirements and purchase orders. Configure new systems by assembling the required components in accordance with user requests. Maintains installed systems, troubleshoots hardware and software problems, and repairs any inoperable systems or associated equipment. Serve as a Conference Support Technician, setting up computer systems and audio-visual equipment for

meetings. Respond to user issues with Conference equipment. Complete tasks assigned in Remedy Work Orders for equipment movement throughout IDA. Participate in testing new hardware and software and developing implementation plans for new configurations. Maintain technical proficiency as new hardware and software technologies are implemented. Inform the Tech Support Supervisor of any system problems or issues that have not been resolved. PC/LAN Technician L-3/TMA Corporation - Washington, DC 1999 to 2003 Provide daily administration of Windows NT 4.0 and 2000 Servers. Provide technical support to users in person and over the phone. Provide Video Teleconferencing support to Corporate/Navy personnel. Provide daily maintenance of desktops PC's running Windows 95/98/2000 and NT 4.0. Provide maintenance for Netscape Messenger/Microsoft Outlook mail users. Responsible for installing and configuring BrightStor ACRserve Version 6.5/9.0/2000 for tape/library backup in a Windows 2000 Server environment. Installed and configured Oracle software for clients to connect to various databases. Assembled category 5 cabling for LAN connection. Education Computer Networking Strayer University - Washington, DC 1996 to 1999 Skills Active Directory (7 years), application software. (4 years), blackberry (3 years), MAC (3 years), Solarwinds (6 years), Splunk, SOC Certifications/Licenses Security+ October 2014 to October 2020 Certified Ethical Hacker (CEH) September 2018 to September 2022 Additional Information SKILLS: Operating Systems: Windows Server; Windows 8/10; Mac OS Application Software: Symantec Antivirus; McAfee; BrightStor ARCserve 6.5, 9.0 and 2000; Microsoft Office; Adobe DC; Quick View Plus; Internet Explorer; Polycom; Argent, CounterAct, ArcSight, BlackBerry Enterprise Server(BES); Citrix, Active Directory; AirWatch, GMC, SolarWinds

Name: Joseph Dixon

Email: simpsonnicole@example.net

Phone: (233)492-2323x520