Sr. Security Analyst Sr.Security Analyst Sr. Security Analyst - VIRTUSTREAM Newtown, PA To obtain an IT Security position utilizing my technical knowledge and solid experience to effectively deliver security solutions. Work Experience Sr. Security Analyst VIRTUSTREAM December 2017 to Present Member of the SIOC team that is responsible for security monitoring and operations of cloud based infrastructure for multiple clients. Primary responsibilities are managing vulnerability management solution for cloud based systems utilizing Nexpose & Nessus software Provide support for Information Security requests: Review security policy clarifications and exception requests; lead Security projects; triage general security questions from other internal teams. Tune, monitor and analyze network traffic and respond to IDS/IPS alerts Analyze network and host-based security logs to identify potential security threats. Participate in incident response and triage Participate in an on call rotation including after hours and weekends to support critical security issues. Drive down mean time to resolution for all Security work. Continuously create and review documentation for Security Operations procedures. Sr. Security Engineer ATOS September 2015 to December 2017 Senior member of Security operations team that is responsible for security operations for multiple clients. ? Provide guidance, support, implementations of multiple IT security solutions to corporate clients ? Manage and support multiple corporate clients current IT security infrastructure ? Provide vulnerability reports and patch management solutions to corporate clients ? Executed scheduled and manual vulnerability scans for the client's infrastructure ? Vulnerability management services for multiple clients using Nessus & Nexpose tools ? Managing cloud based security infrastructure for multiple clients Sr. Information Security Engineer CHUBB INSURANCE March 2015 to September 2015 Senior member of IT Security team that supporting and protecting corporate networks. ? Analyze network traffic to identify anomalous activity and potential threats to network resources using QRadar Siem. ? Implement tuning and auditing of QRadar rules in order to tune down the false positive events ? Perform internal investigations on endpoint systems utilizing FireEye and Carbon Black solutions ? Identify and manage vulnerabilities on the corporate network via IBM VMS SECURITY ENGINEER SYSTEGRA INC January 2014 to February 2015 Senior member of IT Security team that supports and protects City Of Philadelphia Network. ? Managing

and supporting security infrastructure utilizing Checkpoint's Software security implementations. ? Initiated and completed projects to upgrade all security solutions to the latest software release by the vendor. ? Setup and automated configuration backup solution for the security infrastructure. ? Initiated a Firewall rules and IPS policy audit, to optimize performance and security of the current network. ? Responsible for network and server security audit based on latest security policy. ? Responsible for vulnerability and pen-testing local servers via Nexpose and Metasploit PRO SR. SECURITY OPERATIONS ANALYST SRA INTERNATIONAL, INC - Fairfax, VA June 2013 to January 2014 Senior member of Computer Network Defense team that supports and protects Army National Guard's network ? Primary role is to Manage McAfee Network Security Manager servers and IPS sensors ? Investigate all cyber security incidents that are detected on the network ? Utilizing Arcsight as correlating engine during the incident investigations ? Documenting and managing cyber incidents via ITSM Remedy system based on the ITIL model ? Perform vulnerability assessment, threat assessment, utilizing Nessus, NMAP, Retna CYBER ANALYST SRA INTERNATIONAL, INC - Altoona, PA January 2011 to June 2013 Supporting a civilian agency computer emergency response team (CERT) organization protecting the network security of tens of thousands of users as part of the FAA cyber security management center (CSMC). ? Providing real-time security monitoring and incident reporting and analyzing data gathered by the ArcSight. ? Identify, analyze, re-mediate, and report on cyber security incidents. ? Interacted with cyber intelligence analysts conducting threat analysis operations as well as numerous IT professionals performing varying technical roles within the client organization. ? Performed open-source intelligence research for new threats or trends and leveraged us-cert Netflow system and CSCM Arcsight system to review these events. ? Perform daily vulnerability assessment, threat assessment, utilizing Nessus, NMAP & Metasploit SR. HELP DESK ANALYST LOCKHEED MARTIN - Morristown, NJ September 2009 to December 2010 Member of the Classified Help Desk providing IT systems phone support to the company engineers working on classified systems ? Utilizing Remedy 7.0 ticketing system. ? Providing remote computer technical support to end-users on a variety of moderate to complex technical issues ? Managing user accounts on 2003 server

platform ? Processing and managing users escalations to provide fast and accurate resolutions to their application issues SERVICE DESK ANALYST BRITISH TELECOM AMERICAS - Princeton, NJ June 2008 to September 2009 Member of a service desk providing service delivery assurance of LAN/WAN/ Security services for a large pharmaceutical company utilizing the ITIL v3.0 model. ? Utilizing ITSM Remedy 7.0 ticketing system to document incidents, problems, and changes that occur on the customers global infrastructure ? Troubleshooting LAN/WAN outages using CISCO IOS ? Managing DHCP/DNS changes and requests using Lucent QIP management tool ? Monitoring LAN/WAN using network management tools such as SMARTS and Netcool ? Firewall rule management ? IDS investigations and report assessments IT SUPPORT/JR. SECURITY ANALYST SKYLINE SECURITY CONSULTING - Trenton, NJ May 2008 to May 2009 Configuring, deploying, managing and monitoring intrusion detection and prevention systems such as ISS REALSECURE for local banks. ? Provided vulnerability reports to banks that were produced by NESSUS assessment tool ? Proactively monitored network traffic, watching for suspicious activity and notifying customers when security events require additional analysis or investigation. ? Analyzed network transactions by utilizing WIRESHARK network protocol analyzer ? Daily reporting on IDS alerts to customers with preventive suggestions and actions ? Managing email and user accounts on Microsoft Server 2003 based environment ? Conduct remote administration to include managing accounts, passwords, server updates, patching, and backups of Win 2000 servers. NOC ANALYST SYNERFAC/HOTWIRE COMMUNICATIONS - Wynnewood, PA March 2008 to June 2008 Monitored WAN, using network management tools such as Nagios, Solarwinds Documented network and server issues using RT: Request Tracker ticketing system ? Supported DHCP servers that provided IP addresses for cable modems and VoIP phones ? Provisioned and supported optical network units to provide customers data, phone, IPTV service ? Troubleshot broadband network outages using CISCO IOS ? Enabled switch ports to allow data, IP phone and IPTV traffic SR. NOC ANALYST COMCAST - Mount Laurel, NJ July 2001 to January 2008 Member of Network Operations Center team that supported over 12 million broadband customers. ? Provided system and application support to maintain 100% service availability. ? Supported DHCP/DNS servers that

used Linux operating system ? Managed broadband customers via CISCO BACC/CNR application ? Maintained and monitored web servers that would provide network management data that were running Apache web server, BEA Weblogic, and Linux OS ? Determined and escalated server hardware issues to vendors like Sun Microsystems, HP & CISCO ? Used Remedy ticketing system to troubleshoot and resolve tickets in a timely fashion. ? Monitored WAN, using network management tools, such as Spectrum, Netcool to make sure all the equipment is operating at its optimal level. ? Supported all active servers running various Operating Systems on the nationwide network. Addressed all the OS and hardware issues in a quick and assertive matter. ? Troubleshot broadband customers running on the universal broadband routers from leading manufacturers (Cisco, Motorola, Arris). Resulting resolving the outages in a prompt and decisive manner. TIER 2 DESKTOP SUPPORT TECHNICIAN OAOT / PECO - Philadelphia, PA April 2001 to July 2001 Assigned a special project to complete an operating system upgrade from windows 98 to windows2000. ? Provided system and software support to over 300 PECO employees. ? Troubleshot software functional and operational issues as required. ? Rebuilt and configured PCs using Ghost software tool. ? Documented and escalated trouble calls using MacAfee Help Desk ticketing software. Delivered prompt response. Helpdesk Team Lead McGraw-Hill - Lawrenceville, NJ January 2000 to January 2001 Provided website support using Linux/UNIX, Oracle and in-house software for company's clients (McGraw-Hill, Visa, Frontline Capital, iFinance Partners). ? Tested in-house software and actively participated in process to create solutions to software testing problems. ? Provided training and supervision to technical support personnel (7 people). ? Created and maintained weekly work schedules. ? Managed hardware maintenance and installation tasks. ? Developed a call tracking system using Microsoft Excel Desktop Support Technician SOURCEONEINC/CONGOLEUM CORPORATION - Mercerville, NJ June 1999 to October 1999 Supported over 300 users on Windows 95, 98 and Windows NT workstations on Microsoft based network. ? Handled desktop and software issues escalated by users with urgency and solvability. ? Configured and tested network connections in terms of hardware adapters, software device drivers, network interface cards and network information and addresses. Education Certificate Bucks County

Community College 1998 to 1999 Operation Systems, Intro to WinNT DPT Business School 1996 to 1997 Skills training, Excel, database Certifications/Licenses ITIL v3 Present Security+ March 2012 A+ Certified Present

Name: Damon Summers

Email: ubecker@example.org

Phone: (776)373-9410x1548