IT Security Operations Engineer IT Security Operations Engineer Security Engineer Exton, PA Authorized to work in the US for any employer Work Experience IT Security Operations Engineer Godiva Chocolatier - Reading, PA July 2016 to Present SIEM architect providing advanced analytics on security event logs. Routinely review security logs, respond to security alerts, resolve security events, escalate policy violations, assist with IT forensic investigations and inspect security configurations of IT systems. Completed an entire SIEM upgrade and log management solution with high event throughput for security event logging from an existing end of service life enterprise solution. The upgrade included assessing the current SIEM solution, conducting meetings with key stakeholders in an effort to incorporate multiple log sources for security event monitoring, negotiating quotes from vendors and coordinating with procurement to purchase an efficient long-term storage solution for all security events required for investigations and PCI compliance. Cyber Security Engineer Computer Sciences Corporation - Newark, DE February 2016 to July 2016 Linux Server Administrator working with CentOS/RHEL server and supporting technologies, network protocols, and web related protocols. Evaluating, designing, developing, implementing and/or integrating security solutions, SIEM products, Vulnerability Management, and Enterprise Endpoint Protection products. Key initiatives: Linux Server Administrator for the security architect team within the 24/7 Security Operating Center environment. Knowledge of network and web related protocols (e.g., TCP/IP, UDP, IPSEC, HTTP, HTTPS, routing protocols) and strong Linux administration experience Creating and installing security products for testing environments with integration and configuration with logging systems (i.e., Syslog, Windows Event Log) Experience with evaluating, designing, developing, implementing and/or integrating security solutions may include, but are not limited to: SIEM (QRadar, Splunk, ArcSight) and Vulnerability Management (Nessus) Senior Security Analyst Genesis HealthCare - Kennett Square, PA January 2014 to February 2016 As part of the Information Security Team provide comprehensive management and execution of processes related to Security Event Information Management via Enterprise Logging Platform and related systems. Architect and implement comprehensive alerting and workflow related to security events. Serve as key stakeholder in Incident Management processes. Collaborate with

other team members in providing Vulnerability Management and Assessment (host, network, application). Work with internal and external audit teams to provide support for annual audits and control reviews. Provided support directly to CISO and other key business stakeholders. Key initiatives: Manage implementation of an enterprise SIEM Proof of Concept for Gartner's top right quadrant SIEM products Logging - Security Event Information Management - Program and Technical Incident Management - collaborate in leading Security Incident Management Investigations - participate as needed in supporting investigations through data Vulnerability Management - collaborate with other team members in executing auditing Risk Assessment Support - Support routine and ad hoc audits Reporting, Metrics, Deliverables - Provide concise and professional deliverables for architecting and implementing Enterprise-level logging and security event information management solution. Design alerting, communications, workflows and training of other IT users. Assist in engineering integration to other key security systems (IPS, Ticketing, etc.). Associate Security Analyst ACCUVANT INC - Elkridge, MD September 2013 to January 2014 Served as the primary responder for managed security incidents pertaining to client firewalls and all network infrastructure components. Troubleshoot and researched security incidents using SIEM applications, McAfee Enterprise Security Manager, McAfee Endpoint Protection, IBM Qradar Security Intelligence Platform and HP ArcSight. Responsible for providing remote consulting services to assist with deployment of network infrastructure configurations across multiple product vendors and technologies. Key initiatives: ? Event analysis and correlation using multiple log sources including Windows / Linux / Cisco ASA systems and SIEM solutions ? Investigating logs and payloads for server crashes/core dumps, DDoS attacks, SQL/XSS, SPAM, etc. ? Provide root cause analysis and remediation techniques for clients in regards to security incidents and governance documents. ? Collaborate with team members in tuning SIEM applications in an effort to establish a baseline for network activity and rule out false positive events. Technical Operations Specialist Laureate Education - Baltimore, MD November 2011 to September 2013 Responsibilities Responsible for providing technical support to the employees and authorized users of the Laureate Higher Education Group Inc. Responsibilities included: communicating and documenting issues,

monitoring assigned tickets and prioritizing to seek fast resolutions and resolving the customer's issues based upon current service response and resolution times. Key initiatives: ? Analyzing, examining, scanning and remediating hard drives and images for malware, viruses and Trojan infections with Microsoft Forefront, Windows Firewall and Malwarebytes ? Compiling documentation of current and ongoing viruses and threats within the LAN infrastructure ? Performing workstation support functions related to business applications for authorized users of the network including workstation configuration, installation and system update maintenance ? Manage Group Policy in Active Directory based on the organizational information security policies ? Work closely with next level network engineers to provide firewall, switch and server hardware/routing support Business Analyst CareFirst BlueCross BlueShield - Owings Mills, MD November 2010 to November 2011 Responsibilities Responsible for providing and administering tier II technical/helpdesk support for all CareFirst members within the Member Online Services portal. Provided feedback of web services and member portal support to web development team on behalf of the implementation of the CareFirst website. Responsible for ensuring members of CareFirst practiced safe browsing techniques and virus/malware prevention while navigating through the CareFirst web portal. Key initiatives: ? Developing business processes and standard operating procedures for helpdesk support ? Performing testing with Microsoft Quality Center 10.0 software to validate business requirements and create existing defects for web service applications IT Specialist US ARMY - Fort Meade, MD September 2009 to September 2010 Responsibilities Served as the system administrator and Information Security Awareness Officer for the 1st Recruiting Brigade Information Management Organization. Provided guidance, technical assistance and training in all areas of help desk support and telecommunications. Responsible for responding to CA Unicenter Service Desk alerts identifying vulnerabilities. Key initiatives: ? Installing and maintaining GOTS workstation operating systems including Microsoft XP, Vista, Active Directory, McAfee and Microsoft Office Suite 2007 ? Imaging workstations for all users in accordance with DOD Army regulations and IAVA reporting ? Facilitating educational seminars Education Bachelor of Science in Computer Information Systems- Computer Forensics Stevenson University 2007 to 2013 Military Service

Branch: Maryland Air National Guard Service Country: United States Rank: Staff Sergeant June 2001 to April 2012 Weapons Armament Specialist (7- level) June 2001 to April 2012 Awarded Iraqi Campaign Medal for serving one tour of duty in Al Assad Iraq, 2007 Additional Information HP ArcSight ESM 6.9 Full life cycle of ArcSight SIEM systems to include ArcSight ESM, Connector Appliances, SmartConnectors, Logger appliances, Windows, Linux servers, and security devices. Design and implementation of ArcSight architecture upgrades and changes. Developing and directing the development of content for a complex and growing ArcSight infrastructure, including use cases for Dashboards, Active Channels, Reports, Rules, Filters, Trends, and Active Lists Providing optimization of data flow using aggregation, filters, etc., develop custom Flex Connector as required to meet use case objectives. Supporting the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses Coordinating and conducting event collection, log management, event management, compliance automation, and identity monitoring activities for our customer's systems Applying Configuration Management disciplines to maintain hardware/software revisions, ArcSight content, security patches, hardening, and documentation Performing firewall rule modification, reviewing network traffic flows to filter required firewall rules to lock down application, and troubleshoot firewall problems over the enterprise environment Real-time traffic analysis, network IDS and packet dissection using WireShark ArcSight courses taken: ArcSight ESM 6.5 Advanced Analyst ASE, Creating Advanced ESM Content for Security Use Cases, ArcSight FlexConnector Configuration Additional SIEM applications used for forensic network investigations: McAfee Nitro (SIEM administration certificate received from McAfee University) Qradar (IBM Qradar certification training for IBM Certified Associate - Security QRadar V7.0 MR4) RSA Security Analytics LogRhythm Windows Network Forensics and Investigation Identifying, collecting, analyzing Windows Event Security logs from AD, DHCP and local endpoints Windows password storage and authentication Windows Kerberos authentication Acquiring and analyzing volatile and non-volatile memory and data Windows Server 2008, 2012, R2, Server Core Securing File Sharing Services, DNS, DHCP, NTFS File and Folder permissions through Group Policy and Active Directory Users and Computers

Endpoint Security and Patch Management McAfee ePO, Host Intrusion Prevention, SolidCore Microsoft Forefront, Microsoft Endpoint Security Essentials, AVG and Sophos Configuring SCCM for log collection and database retrieval Firewalls Cisco - ASA Firewalls, AnyConnect VPN client/IP Sec VPN client and Packet Tracer Fortinet Fortigate, Fortiweb, Fortianalyzer Aruba Mobility Controller, Airwave, ClearPass Computer Forensic Tools Pro Discover Basic, FTK Imager, Wireshark, WinHex, Steganography ITIL and compositions written Technology Law Cyber Security: The legal responsibilities and liabilities Incident Response and Investigation Methods Advanced Persistent Threat: What APT Means to your Enterprise Information Security for the Organization Risk Assessment: Contingency Planning Guide

Name: Brian Hansen

Email: watsontonya@example.com

Phone: (644)408-8389x605