Lead Consultant - TCS contracted to Moneymart Lead Consultant - TCS contracted to Moneymart Lead Consultant - TCS contracted to Moneymart West Chester, PA Work Experience Lead Consultant - TCS contracted to Moneymart March 2019 to June 2019 Successfully completed my assignment in leading the migration to the TCS managed security services for the following security tools. ? Vulnerability Management * Managed the migration from Qualys to Rapid7 ? Application Security * ASOC * Veracode * Lookout Appdefense ? Siem * QRadar ? WAF * Radware ? Social Media Security * ZeroFox Incident Response ? Integration of the security toolsets into the Manage Engine Service Desk Plus ticketing system ? Automated workflow White Hat Pen Testing ? Metasploit Managed a team of offshore analysts during the migration Security Engineer Radiant Systems August 2018 to February 2019 contracted to Sungard, Phila. Pa Managing the engineering side of the McAfee Enterprise Security Manager SIEMS for Sungards Managed Security Services and the Sungard internal SIEM ? Responsible for the overall health of the SIEMS' environment and troubleshooting all SIEM health related issues for both client and customers ER's, ESM's, ACES and ELMS ? Diagnosing issues derived from monitoring appliance device logs. Utilizing TCPDUMP and or Wireshark as diagnostic tools for packet capture and analysis Utilizing Linux OS knowledge along with McAfee CLI to assist with diagnosis and repair of all SIEM appliances ? SIEM implementation project management for new customers ? Led client facing meetings to answer all SIEM engineering related technical questions during the SIEM buildout in the client environment. ? Lead engineer for all new client installations, upgrades and the provisioning of new client's ER's and data sources into the SIEM. ? Performance monitoring of all SIEM related appliances and VM's Cloud Security April 2018 to July 2018 04/2018 - 07/2018 - Utilized down time to Acquired AWS Certified Cloud Practitioner certification Focused on strengthening skills in ? Cloud Security, architecture and administration ? Application Security and DevOps ? Audit and Compliance Utilized the AWS free tier for AWS hands on training Completed online training/labs offered by A Cloud Guru and Pluralsight ? Completed the below courses * AWS Certified Cloud Practitioner * Foundations for Cloud Architecture * AWS Fundamentals and Administration * AWS Security Fundamentals * Securing DevOps * Docker fundamentals * SSCP: Risk Identification,

Monitoring and Analysis * SSCP Incident Response and Recovery * Payment Card Security, Processing and the PCI Standards 08/2017 - 03/2018 Recovered from injuries sustained in a car accident. Security Engineer, Pinnacle DuPont - Wilmington, DE May 2017 to August 2017 Supporting the DuPont and Dow merger ? Firewall change management of Juniper firewalls * Utilization of networking knowledge and FireMon toolset to assist with the re-ip of the DuPont firewall rulesets that would affect assets being re-ip'd sitting behind Juniper firewalls in DuPont data centers, corporate and manufacturing sites * Applying security policy to requests for initial approval of requests * Creating change management tickets utilizing FireMon Security Manager and Policy Planner. * Troubleshooting firewall related access issues due to the ongoing merger * Contributing team member for network security design and review of changes necessitated by the merger. ? Firewall cleanup * Heavy utilization of FireMon Security Managers reporting capabilities and functionality to determine policy, rule and object usage * Creating change management tickets with policy planner to facilitate cleanup in regards to unused, shadowed and hidden rules. Sr. IT Security Analyst contracted to CITI Newcastle TSR Consulting October 2016 to February 2017 De Member of the CATE (citi architecture and technology engineering team) Completed the security validation of the BTrade TDCM EDI (electronic data interchange) application prior to being promoted to production * Completed all CITI procedural documentation that was required for application approval thru application acceptance, prior to the applications promotion to Production. * Managed the remediation of application vulnerability failures with the application vendor * Documented and ensured all CITI security policy, relating to application security configuration was in place * Functional application testing. Network Solutions Security Architect contracted DuPont - Wilmington, DE November 2013 to March 2016 Design and implementation of security initiatives and managing those initiatives thru the project lifecycle Lead security architect for the FireMon initiative ? Implemented FireMon Policy Planner and Security Manager to remediate policy violations, change management and logging audit failures on both the global PCN and corporate networks. * Refined and simplified the DuPont firewall change management processes by combining 2 disparate change management systems into 1 * Gathered workflow requirements from stakeholders, firewall owners

and current workflow from existing tools to be integrated into a customized Policy Planner workflow * Reviewed and approved or denied firewall rule change requests by applying AP&C (Automation and Process Control) security policy against requested rule changes * Interpretation of firewall change requests into actionable firewall rules and determining what firewall change requests would need to be applied * Approver for firewall change requests on PCN (Process control network) and IT firewalls. * Designed and integrated the approval process for access and authentication to the toolset ? Implemented FireMon Security Manager core module for approximately 500 Juniper and Checkpoint firewalls to report into FireMon * Dissemination of product functionality to security, audit, firewall owners, approvers and admin groups * Creation of custom searches utilizing FMQL * Implementing reports and recommending changes on shadowed and hidden rules, least and most used rules, unused rules etc. to increase performance and throughput of enterprise firewalls * Path and traffic flow analysis * Managed the tool prior to being handed off to OPS Contributing security architect for the Chemours spinoff ? Lead architect for the Chemours FireMon initiative ? Member of the review board to ensure that adequate security controls were being migrated from the DuPont to Chemours network Contributing security architect for the secure design of the DuPont Extranet ? Threat modeling. ? Determining use cases Contributing security architect for the review of Network Security Solutions and Security Technology Refresh Hosted meetings for stakeholders from the Global enterprise Interaction with cross functional teams included telecom, audit, legal, infrastructure, security and change management CVI certified - Chemical-terrorism Vulnerability Information Researching security technologies and threats to determine if current controls are adequate Review of existing network design and the Juniper UAC architecture to ensure that the network is being vigorously defended against the current threat landscape Network Security Documentation ? Visio Sr. Security Analyst Automated Financial Systems - Exton, PA May 2012 to July 2013 Management and administration of a QRadar SIEM ? Incident response to events identified as deemed to be possible incidents ? Analysis of offenses and events * Behavioral analysis of network flows ? Pruning false positives ? Flow analysis ? Custom rule and Building block design to trigger offenses and events ? Creation of searches in support of security incidents

and investigations ? Generated reports for baselines and metrics ? Customization of dashboards and reports White Hat Pen Testing Active Directory ? Management of ADmanager Plus across 4 domains * Bulk user creations, deletions, group modifications * Report creation in support of audit Analysis of DLP (Proofpoint) logs Analysis of Checkpoint (Smartcenter) rules and logs Application security scans SSL certificate management Nessus and Rapid7 vulnerability scans Virus definition update audit Physical security Consulting Senior IT Security Engineer HCL America - Chesterbrook, PA October 2011 to April 2012 Successfully completed a short-term contract in the role of a consultant with HCL America as a member of the governance risk and compliance team to complete a security gap analysis and vulnerability assessment Member of the Security Gap Assessment team ? Currently in the Plan stage of the ISO 4 phase model. ? Discovery of security gaps based on interviews and responses to questionnaires based on the ISO 27001:2005 framework ? Analysis of the client responses leading to a formal document which outlined the clients' current security posture and the risks that would be assumed for non-compliancy Made the appropriate recommendations for the controls that would need to be put in place to reduce risk and be compliant Managing the vulnerability and network audit scanning project which culminated in scans of targeted servers in the global enterprise data centers ? Utilizing Nessus and Rapid7for the vulnerability scans and Nipper Studio for the network infrastructure audit ? Configuration of multiple scans on targeted servers across the enterprise ? Managing the scan from the perspective of asset identification, identifying the platform and application owners as well as giving guidance to the stakeholders on the results of the scan ? Creating the high level reports from the results for upper management Management and scheduling of resources across the global enterprise to bring the project to a successful conclusion. Senior IT Security Engineer MISI - Philadelphia, PA February 2010 to May 2010 Completed short term contract with MISI in which I was contracted to SunGard while a SunGard employee was on medical leave. Worked within the governance, risk and compliance sector of SunGard ITIL security model. Administration and log analysis for Websense data loss prevention Manage and administer the Rapid 7 Nexpose scanning ? Configure and initiate network scanning. ? Generate

reports to track metrics of the scanning. ? Write procedural documents in support of the scanning process. Application security scans Advise asset owners on security best practices and risk so as to comply with policy. Advise and work with auditors to ensure compliance. Advise and give guidance on how to implement best practices and meet control objectives. Member of the Archer Framework implementation team Network Security Analyst contracted Department of Defense - Aberdeen, MD January 2009 to June 2009 Primarily focused on the analysis of traffic crossing between military and non-military networks bound for military assets as well as military sourced traffic bound for non-military destinations. ? Identify non-compliant, malicious network traffic ? Identify real time external and internal attempts to exploit network and host based assets and applications via HTTP, SNMP, TCP/IP, FTP, IM etc. ? Relay appropriate information to mitigate threats to the firewall team Snort, TCPDUMP and a number of other proprietary tools are used in the analysis of both behavioral and Signature based rules. ? Write and recommend rules for implementation into the toolset Identify and report on assets containing malicious threat capability Contact with all levels of management for the remediation and knowledge sharing of events. Report tracking and management of remediation efforts. Provide technical support to national account director TEKsystems - Philadelphia, PA June 2008 to July 2008 Philadelphia, Pa. Engaged in a short term contract to design a solution for the remediation of network access vulnerabilities discovered during an audit Provide technical support to national account director during client meetings and follow up on any security centric issues the client requires to be addressed Coauthor the following statements of work with the account director ? Scope ? Project lifecycle details ? deliverables Designed a Tacacs+ solution for Network Access Compliance Engage with client technical staff for all pre solution implementation discovery Security Vulnerability Manager for the Cingular Wireless NE Cingular Wireless / AT&T Mobile - Norristown, PA August 2005 to December 2007 As an original member of the vulnerability management security initiative for the NE region I implemented processes and procedures to get the initiative off the ground and continued to review, refine and implement these procedures and processes when applicable Introduced Preventsys as a remediation and automated work flow management tool along with

managing the project lifecycle. Conducted product evaluations of security tools in support of the following security initiatives ? Vulnerability scanners ? IPS and IDS ? Security management toolsets ? Workflow management ? SIEM Generated risk assessment documentation for variances Managed the remediation and mitigation of vulnerabilities for all core network platforms (OSS, SGSN, BSC, RNC, MSC, HLR, and VLR) in all markets of the Cingular Wireless Northeast region for Windows, UNIX and Solaris platforms. Vulnerability Scanning ? Nessus, nCircle, Retina ? Correlation and workflow tools (Preventsys) OS Hardening ? Worked with platform owners of Windows and Unix based systems to standardize new production builds to SANS top 20 * Initiated policy and procedures for hardening of UNIX and Windows based servers * Remediate existing production servers Team member for SOX compliance and audit remediation Team member to assess ISO 17799 controls. Administer the archiving of all security related requests and correspondence in support of due diligence. Represented the NE region on security panels for a variety of security initiatives. Access Management ? AD and Unix ? Account builds ? Account scrubs ? Audit of role based permissions and management of access control matrix Wrote policy and the associated procedures in support of vulnerability management. Worked with all the market operations managers to disseminate security policy, procedures and processes. Working with the platform owners I resolved any issues that arose due to remediation requests on the respective platforms that they own. Acted as a security ambassador to instill the need for security and the timely remediation of vulnerabilities. IT Security Engineer Tek Systems - Pennington, NJ July 2004 to January 2005 Project manager and Team Lead for the Bristol-Myers Squibb Desktop Firewall Initiative Managed the project from inception thru test pilot. Authored all project documentation. ? MS Project document ? Firewall summary and recommendation documents ? Firewall criteria ? Project charter, scope, stakeholder, test plans etc. Conducted the assessment of the current firewall technology and based upon those findings made recommendations for the initial vendor selection. Developed criteria for 2'nd round of vendor selection. Developed test strategy for test phase and conducted the actual testing. Developed the strategy for firewall components that would be implemented. Developed strategy, scope and objectives for pilot phase. Set up and

evaluated McAfee, ISS, Sygate and Zone Labs firewalls along with the enterprise management components. Created line item criteria to be used in the vendor reverse auctions ? This resulted in significant price reductions from initial vendor quotes. Created objectives that vendors would be tasked with. Reviewed Vendor Statements of Work for accuracy. Actively participated in and contributed to the BMS security focus group. Headed project team meetings and created applicable PowerPoint presentations. Gave presentations focused on various aspects of security to the global BMS security group. IT Security Engineer Wyeth - Frazer, PA March 2003 to March 2004 Security analysis for a 50,000 node network Administered an ISS Black ICE firewall implemented a ISS Black ICE Pilot Vulnerability scanning - Nessus and Retina. Cisco June 1981 to March 2003 Desktop and Network Infrastructure design, service and support ? 6 years Cisco infrastructure design and support ? 5 years Server builds and support ? 7 years LAN and WAN NOC support ? 5 years Desktop support Education Liberal Arts Penn State University - Lima, PA September 1974 to June 1975

Name: Valerie Harrell

Email: thomasdarren@example.com

Phone: +1-919-889-7908x18342