Senior Security Analyst - Security Operations Center Senior Security Analyst - Security Operations Center Senior Security Analyst - Security Operations Center - Deloitte Sevices LP Work Experience Senior Security Analyst - Security Operations Center Deloitte Sevices LP - Nashville, TN October 2017 to Present Threat hunting, Senior Security Analysis, Architecture, Leadership. Assisted with the dramatic improvement of the overall security posture of a Major, Multinational Accounting Firm *following* two major breaches. Spearheaded efforts to Stabilize, and Configure, firm's EDR platform (157,000 End Points). Authored several (EDR) signals responsible for assisting with improvements in the overall security posture of the firm. Participated in and contributed to Several, Critical War Room Incidents. Assisted with efforts to identify Architectural Gaps and assist with identifying mitigating and detective controls designed to close those gaps. Assisted with efforts to implement (and stabilize) the ingestion of Threat Intel across Firm's Architecture. Directed and Assisted with Purple Team exercises designed to improve detection capabilities for the US Firm. Assisted with documentation of Firm's Network. Assisted with designing templates designed to provide improved metrics for incidents to leadership. Authored, Published, and Socialized several SEIM Dashboards. Information Security Analyst Security Operations Center - Memphis, TN January 2017 to September 2017 Contractor - Memphis, TN January 2017 - September 2017 Assisted with Vulnerability Scanning using both Open Source and Commercial Scanning Platforms. Assisted with Penetration Testing exercises directed against Organizational Computing and Network Resources using Kali Linux, MetaSploit, and other exploit toolsets. Assisted the Director of Information Security with conducting compiling and documentation for PCI Audits. Assisted with Proof of Concept for two PAM products. Assisted with rollout of new PAM platform across the Enterprise. Assisted with Proof of Concept for new AV/EDR platforms. Assisted with Daily Montioring of EndPoint Security, Desktop Hardening, Email, SIEM, FIM, SecureWorks IPS, Policy Writing and Maintenance. Blue Team Exercises. Performed Liasion Responsibilities with Several Agile, DevOps teams to improve overall security of our organizational web prescence. Assisted with management and monitoring of WAF. Information Security and Systems Analyst International Paper - Memphis, TN October 2013 to October 2016 Defined and maintained security posture for over 300 Solaris and Linux Servers.

Performed Risk Assessments, defined standards and procedures, performed vulnerability assessments and assisted with mitigation and remediation for all associated systems. Also responsible for assisting with the IT Operations for over 300 Solaris and Linux Servers. UNIX IT Operations Manager/ Security Enforcement Officer United States Army - Fort Knox, KY May 2011 to October 2013 Responsible for 200+ Mission Critical, Solaris Servers, and Twelve Supporting Direct Reports. Designed, Implemented, and Tested Disaster Recovery and Business Continuity Plans. Scanning and Enumeration of Operating Systems using (Nessus/Retina/nMAP), and code for Web Applications using fortify. Served as Web Application Security Subject Matter Expert. Served as Solaris, Linux, UNIX Security Subject Matter Expert. Manage Deployment, Maintenance, Development and Upgrade of all IT Systems. Managed and Monitored Deployment and Upgrade of all IT Application/Web Platforms. Technical Lead/Solaris/Web/Application Administrator/ Security Engineer Lockheed Martin - Fort Knox, KY June 2006 to April 2011 Fort Knox, KY June 2006 to April 2011 Team Lead for Group of Solaris, Web, and Application Administrators. Primary Solaris Administrator responsible for over 200 Mission Critical Servers. Used vulnerability assessment tools (Nessus/Retina/nMAP) to identify critical OS vulnerabilities. Primary Application/Web Administrator responsible for Over a Dozen Mission Critical Apps. DirectedSecurity Risk Assessments for Operating Systems, and Web Applications. Identified, Reported, and Responded to Security Attacks and Intrusions. Served as Web Application Security Subject Matter Expert. Served as Solaris, Linux, UNIX Security Subject Matter Expert. Liaised and Coordinated with Development Teams. Tested Disaster Recovery and Business Continuity Plans. Security Remediation. Consulted and worked with Information Assurance on all Solaris and Web Security Matters. SOLARIS Engineer EDS - Tulsa, OK August 2004 to June 2006 Primary SOLARIS Administrator for over 60 Mission Critical Servers. Solaris, Linux, UNIX Security Subject Matter Expert. Used nessus, tcpdump, and netcat to assist with vulnerability assessments. Application and Web Administrator for Mission Critical Apps. Patch Maintenance and Server Maintenance. Technical Lead/UNIX Admin/ Security Engineer EDS - Pearl Harbor, HI March 2002 to August 2004 Technical Lead for a group of 5 SOLARIS and Tivoli Administrators. Served as Solaris, Linux, UNIX Security Subject Matter Expert. Assisted With

Periodic Security Audits for all UNIX Platforms. Identified, Reported, and Responded to Security Attacks and Intrusion. Identified, Documented, Verified, and Communicated Key Operations Tasks. Responsible for Development and Training of SOLARIS Team. Vulnerability Scans, Security Audits, and Patch Maintenance. Kernel Engineer Customer Call Center - Broomfield, CO September 1997 to May 2001 Kernel Engineer responsible for providing SUN's most critical customers with Engineering support to help resolve the following issues: System Panics, Performance Tuning, Capacity Planning, Patch Management, Hardware Troubleshooting, and Device Driver Troubleshooting. Education Bachelor of Science degree in Computer Science Engineering University of Colorado - Denver, CO

Name: Samuel Cross

Email: christine52@example.net

Phone: (550)863-2364x562