Intrusion Detection Analyst - Security Operations Center Intrusion Detection Analyst - Security Operations Center Intrusion Detection Analyst - Security Operations Center - CitiCorp Plano, TX Intrusion Detection / Network Security Analyst with about 7 years of experience and expertise in monitoring network-based IDS/IPS technologies for Fortune 500 companies. Proven record of evaluating system vulnerability, compiling actionable analysis, reporting threats, and recommending security improvements. Work Experience Intrusion Detection Analyst - Security Operations Center CitiCorp - Irving, TX September 2012 to Present Member of security operations center and responsible to perform real time security monitoring, incident detection and response services to reduce the risk Citi or Citi's business partners may be exposed to. ? Monitor and analyze network traffic and various log data to detect threats against the network ? Monitor Citi web applications logs to detect brute force attacks and other banking related fraudulent activity like MiTM attacks and account takeovers and escalate to Fraud teams. ? Ensure all pertinent information is obtained to allow the identification, categorization, incident handling and triage actions to occur in a time sensitive environment. ? Facilitate and expedite the tracking, handling, and reporting of all security events and computer incidents in accordance with organizational procedures ? Evaluate and perform incident escalation in accordance with organizational guidelines ? Provide support to the Vulnerability Assessment team for incident validation and manual in-depth analysis, escalation of high severity incidents and co-ordinated in documentation and evidence collection to assist them in remediation. ? Collaborate with various teams that provide the SOC with actionable intelligence on risks and vulnerabilities. ? Develop custom content for the intelligence provided by other teams to ensure detection of new threats and vulnerabilities. ? Content review and tuning the existing content to reduce false positive volume and increase efficiency of analysis and improve device performance. ? Responsible for metrics and oversight to measure and report the operation results and business value of and productivity of the team. ? Recipient of Employee Recognition Award for the contributions to team for effectively mentoring junior level personnel and knowledge transfer among peers Information Security Analyst GAVS Information Services February 2004 to January 2006 Member of network operations center and responsible to administer and monitor logs and events generated by enterprise network and system infrastructure with HP Openview Network Node Manager (NNM). ? Provided support as an escalation engineer in configuration and troubleshooting remote access VPN, Cisco VPN concentrators, Microsoft 2003 and exchange server issues in 24/7 operational environment. ? Communicated and interacted effectively with the customer and internal members of the organization to ensure optimal individual and group performance. ? Perform quarterly audits to ensure continuous monitoring of perimeter architecture to include examination of network security device configuration, validation against security controls and compliance requirements. ? Review web application vulnerability reports generated by scan tools like HP WebInspect and perform analysis of the http requests and responses sent to and from the target servers against the OWASP listed top 10 vulnerabilities like Cross site scripting, SQL Injection, Buffer Overflow etc. ? Conduct internal network and system assessment using commercial and open source scanning tools ? Coordinate and participate in penetration testing of web applications and network infrastructure including routers, firewalls and IDS and databases using open source tools such as nMap, Nessus and Snort to analyze and exploit critical security vulnerabilities. ? Tasked to conduct interviews with application and system owners to review the findings and security posture of the systems after the testing is completed. ? As a member of internal Information Security council, participated and contributed in the design and implementation of Business Continuity and Disaster Recovery Plans. IT Security Analyst GE Capital International Services September 2001 to January 2004 As a member of customer support center responsible to perform IT security analysis and vulnerability assessment solutions for GE international clients and business partners in a 24/7 environment. ? Configured translation and access control Microsoft ISA proxy servers at the perimeter level to ensure security and compliance with organizational policies and procedures. ? Review packet information generated by network sniffers like ethereal and plug-ins which define the actual scripts crafted to run the checks in Nessus. ? Responsible to complete projects and assigned tasks and ensure on time deliverables to meet the service level agreement and communicate directly with GE international clients and customers across the globe. ? Awarded "Voice of the customer" for excellent communication and customer service skills. Education Master of Science (E-Business) , Master of Commer and Business Management in E-Business Sikkim Manipal University - India Skills Security Applications: Palo Alto IDS/IPS, Sourcefire IDS/IPS, McAfee e-Policy Orchestrator, ArcSight SEIM, Arcsight Loggers, Arbor Peakflow,Wireshark ,Fiddler,Burp Suite,SilverTail Systems, BlueCoat Proxy,Netwitness , Forescout CounterAct. Operating Systems: Windows XP/Vista/7/8, Windows Server 2003/2008/2012, Linux, Unix, Cisco IOS Networking: LAN/WAN, TCP/IP, DNS Certifications/Licenses CEH May 2012 ECSA July 2012 GCIH February 2014 Additional Information TECHNICAL QUALIFICATIONS Security Applications: Palo Alto IDS/IPS, Sourcefire IDS/IPS, McAfee e-Policy Orchestrator, ArcSight SEIM, Arcsight Loggers, Arbor Peakflow, Wireshark, Fiddler, Burp Suite, SilverTail Systems, BlueCoat Proxy, Netwitness, Forescout CounterAct. Operating Systems: Windows XP/Vista/7/8, Windows Server 2003/2008/2012, Linux, Unix, Cisco IOS Networking: LAN/WAN, TCP/IP, DNS

Name: Megan Johnson

Email: kramerbrian@example.com

Phone: (492)988-0424