Sr. Manager Information Security Sr. Manager Information Security Sr. Manager Information Security - Zenimax Media Inc Austin, TX I am a Senior Information Systems Security Manager with 20 years of professional experience. I have provided security solutions for massively multiplayer online games, such as World of Warcraft, Diablo 3, Defiance, Rift, and Elder Scrolls Online as well as security solutions for other intellectual property created by Zenimax Media Inc, Trion Worlds Inc and Blizzard Entertainment. I joined the USAF after graduating from high school and was honorably discharged from the Air Force after serving four years at Lackland AFB in San Antonio, TX. After parting with the military I worked as an intrusion detection/information systems analyst for the Air Force Computer Emergency Response Team (AFCERT) at the Air Intelligence Agency. I have experience meeting and exceeding regulatory government compliance such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI) compliance and EUGDPR. I have provided information security governance through policies and training programs as well as risk management and evaluation for multiple software development companies with hosted cloud and online presence. I am familiar with IT governance programs such as ITIL and COBIT. Work Experience Sr. Manager Information Security Zenimax Media Inc - Austin, TX August 2016 to Present - Lead a team of security professionals and provide them with growth and training opportunities as well as annual evaluations and checkpoint feedback for new hires in 30, 60 and 90 days. - Responsible for creating global risk management strategies for online resources provided to customers from all development studios. - Advises executive leadership on key security initiatives that reduce risk while without impacting business operations. - Create and manage an incident response plan and recovery process. - Provides leadership and governance for managing threats and evaluating solutions to mitigate risk to business operations. - Implement and oversee vulnerability management programs designed to increase the security posture of online systems in both cloud and datacenter providers. - Oversees development of security training requirements enterprise wide for all development engineers. - Responsible for creating corporate strategies for handling regulatory compliance. - Implement security practices and standards for all data center information systems and applications in anticipation of new product releases by Zenimax Media subsidiaries. Sr.

Security Engineer Zenimax Media Inc - Austin, TX September 2013 to August 2016 Create security solutions for monitoring cloud computing access and systems in Amazon Web Services. Cloud Tools: Security Monkey (Netflix OpenSource), Evident.io (Cloud Monitoring Solution), and ThreatStack Cloud Monitoring. - Write and maintain Information Security Policies for live environments and publishing systems. - Implement and maintain F5 security products such as Application Security Manager, which is a Web Application Firewall, the F5 Access Policy Manager, which is an access control system for internal applications. (F5 ASM/APM) - Create and maintain python scripts for automated processes triggered by Splunk alerting and calling JSON endpoints to automate remediation of in-game security issues. - Create Splunk searches and alerts that aggregate into behavioral analysis of in-game account actions to determine account intention and use of in-game mechanisms. - Maintain 2-factor access to data center resources using DUO and resource assigning with LDAP groups/permissions. - Deployed OSSEC and Linux Auditd data center wide, grooming the data for Splunk consumption and enriching the logs to make them human readable. - Implement and maintain Network Security Monitoring using Gigamon, Bro IDS, Security Onion technologies reporting to Splunk via syslog-ng or Splunk forwarding. Senior Security Analyst Trion Worlds Inc - Austin, TX September 2012 to September 2013 Evaluate and implement security system products across the IT Enterprise. Monitor and report IT anomalies resulting in poor security practices. - Engineer and evaluate security posture for all enterprise systems hosting customer services. - Maintain security for released intellectual properties developed by Trion Worlds Inc. and third party associates including Rift and Defiance, as well as IP that is not currently released or public knowledge. IT Security Engineer Blizzard Entertainment - Irvine, CA January 2006 to September 2012 Provide technical security oversight for all information systems and engineer solutions to meet regulatory compliance standards such as Payment Card Industry (PCI) and Sarbanes-Oxley Act (SOX) compliance. - Daily duties include penetration testing internal and external networked systems, monitoring of Intrusion Prevention Systems, correlating log events to determine risk of security incidents and researching the newest security threats and vulnerabilities. - Project work included researching security solution vendor products and evaluating them for use in the environment, engineering custom solutions for known and unknown security gaps and upgrading or re-engineering current security systems to bring them in line with ever persistent threats. Network Security Analyst AFCERT, Lackland AFB - San Antonio, TX February 2001 to January 2006 Worked for multiple government contracting companies including Computer Science Corporation and McAuley-Brown Inc. - Network Security Analyst for the Unites States Air Force. Used Intrusion Detection System(IDS) to monitor network traffic worldwide in near real time. Also creates SQL queries to pull information from the database for correlational analysis. - Computer Forensics and Reverse Engineering of malicious logic using many different tools. - Lead Analyst for the Air Force Computer Emergency Response Team. - Provide policies and directives for the Air Force Computer Emergency Response Team (AFCERT) operations floor. - Isolate, contain, and prevent intrusive activities and or security vulnerabilities on Air Force Automated Information Systems (AIS) and networks. - Conduct network monitoring and intrusion detection analysis using the AF's selected intrusion detection tool and Activities related to AFCERT mission execution. Systems Integration Engineer USAF, Lackland AFB - San Antonio, TX September 1997 to September 2001 - Automated System Intrusion Measurement (ASIM) Project Manager for 67th IOW - Four years network administration and Desktop Support - System Security Plans Accreditation Manager - Information Systems Security Manager, and Computer Security Manager Education Associate of Science in (A.S.) Computer Science ITT Technical Institute - San Antonio, TX 2002 to 2004 Skills DNS, SECURITY, IDS, IPSEC, IPS, METASPLOIT, NESSUS, NEXPOSE, NMAP, SNORT, SPLUNK, SSL, TRIPWIRE, CISCO, AUTHENTICATION, RSA, JAVASCRIPT, PYTHON, SCRIPTING, TCL Links http://www.linkedin.com/pub/scott-harrison/49/1a/5a9 Military Service Branch: United States Air Force Rank: E4 Additional Information SKILLS PROFILE - IPS/IDS (Cisco IPS, Tipping Point, SNORT, Bro IDS) - HIDS/Anti Virus (AIDE, Tripwire, Symantec Endpoint Protection, McAfee Enterprise) - SEIM Experience (Splunk, MARS, RSA Envision, Security Onion) - Security Policy Writing and Security Training Program Management - Network Protocols TCIP/IP, SSL, IPSEC, DNS, HTTP, FTP, SSH, ICMP etc .. - Network Penetration Testing, (Metasploit, NMAP, Nessus, Nexpose, NETCAT) - Web Application Penetration Testing (DirBuster, Acunetix, BURP Suite, OWASP Top 10) - Host/Server Hardening (CIS Benchmarks) - Programming/Scripting (BASH, Python, Javascript, Java, TCL/TK, SQL) - 2 Factor Authentication (RSA SecureID, Vasco Digipass, DUO) - Operating Systems (Linux, HPUX, Sun Solaris, Windows, Cisco IOS, OSX) - Network analysis/packet capture (Ethereal, TCP Dump) - Forensics and recovery, incident analysis (NCase, Recuva) - Database Security Auditing (MySQL, Oracle, MSSQL)

Name: Jennifer Perkins

Email: lrose@example.com

Phone: 450-807-2713