

EXPERIENCE

SECURITY ENGINEER

Dallas, TX

04/2014 – present

- Establishes networking environment by designing system configuration; directing system installation; defining, documenting, and enforcing system standards
- Driving secure coding initiatives across the company by defining training, identifying weaknesses, and educating developers
- Assist with identifying, communicating, researching, evaluating and remediating errors, issues and risks
- Candidate will join a team of security engineers in designing, engineering, planning, implementing, and supporting security solutions globally
- Day to day servicing and maintenance; including Diagnoses, repairing faults, programming and commissioning in security, access control and CCTV systems
- Identifies opportunities to improve risk posture, designing security controls for remediating or mitigating risks and assessing the residual risk
- Working with stakeholders to perform risk management and ongoing assessments, and then selecting mitigating and corrective controls based on Pareto analysis

SECURITY ENGINEER

Dallas, TX

12/2007 – 10/2013

- Identifying, Collecting and Analyzing security relevant logs for reporting and compliance purposes
- Secures network system by establishing and enforcing policies; defining and monitoring access
- Perform root cause analysis for reoccurring or high impacting incidents, assist with proposing and implementing structural solutions
- To support system development by adding security rigor to the design, assessing the security posture and hardening dynamic operating environments
- Assists in ensuring positive event by coordination and direction in development, planning, analysis, training, testing and maintenance
- Engineering, securing, implementing, and managing security solutions
- You will join the patching team and steer our automated patching boat. If you're a scripting guru, you can get involved in making it even more automated

EDUCATION

PORTLAND STATE UNIVERSITY

Bachelor's Degree in Computer Science

SKILLS

- Strong verbal skills and demonstrated ability to produce clear, concise and high quality written deliverables
- Strong knowledge of security management principles and practices, including vulnerability management, event management and application security
- Experience in engineering a detailed design of highly available, high capacity geographically distributed applications
- Detailed knowledge of operating system security as well as knowledge as common software stacks
- Ability to meet aggressive reliability, performance, cost, serviceability, and delivery targets
- Strong knowledge of Federated SSO (SAML, OAuth/OpenID). Working knowledge of Okta Federated SSO and Oracle Access Manager policy management
- Excellent ability to identify threats and vulnerabilities in a system, model exploits, and design mitigations
- Execute remediation process to implement technical solutions to address vulnerability findings in ACAS and other vulnerability assessment tools
- Strong understanding of TCP/IP, basic and advanced routing protocols (OSPF, BGP) and related Internet protocols
- In-depth knowledge and understanding of vulnerability/patch management and malware protection