Randy Parrow

Email: parrowrd@gmail.com

Phone: 1-773-648-1880

http://www.linkedin.com/in/parrowrd

Profile

Certified Information Systems Security Professional (CISSP) and accomplished cybersecurity leader. Over 15 years of experience in architectural strategy, technical design, and operational deployments. Innovative and profound technical insight delivers unique value across planning, design, implementation, delivery and operations processes.

A strategic thinker capable of envisioning security solutions which provide scalable, efficient and practical techniques for mitigating risk. A trusted advisor with exceptional commutative skills and strong business acumen capable of articulating the value proposition to executives. A trusted advisor provided consultative security services to well over 50 of Fortune 500 clients on the development of security solutions and capabilities to address complex and emerging security threats: data privacy, cybersecurity, threat remediation and security operations.

Eligible to work for any company in the U.S.

Skills

- **Network Security Infrastructure**: CASB, DLP,SIEM, WAF, Firewalls, Anti-DDOS and IPS
- **Cloud Security and Technologies**: AWS, Azure
- **Threat and Vulnerability Management**
- **Malware and Endpoint Detection and Prevention**
- **Technology Integration and Deployments**
- **NIST SP's, IETF, IEEE, PCI, GDPR frameworks**

Work History

Cybersecurity Architect, Dec 2017– Present

- Deployed next-gen firewalls, web access firewalls & proxies, and end-point monitoring solutions in the Software-Defined (SD) Wide Area Network (WAN) from 400% (50 to 250), across SD-Branch locations.
- Conducted Incident Response Planning and Testing by designing table top exercises, Cyber ranges (including simulation) and evaluating performance based on defined playbooks.
- Served as Cybersecurity Architect leading multiple architectural teams and implementation for organizations seeking to optimize their current security infrastructure. Responsible for securing endpoint, infrastructure, database, web, amd multi-cloud environments, by developing baseline secure configurations including access management to solutions, policy management, onboarding, life-cycle management, for all critical security infrastructure components.
- Developed Incident Response Management Programs including security event systems to identify incidents, and provide actionable intelligent response plans and playbooks, using automaton in security operations.
- Assessed the security infrastructure and design for a newly designed Aryaka Software-Defined (SD) Wide Area Network (WAN) network addressing security and privacy requirements. Assessed the Service Providers' completeness of design and connectivity between Regional Points of

Presence (POP) Point and Global enters. Provided guidance that improved security operational processes, device resiliency, incident & monitoring, and alerting capabilities. The assessment facilitated an optimized deployment reducing execution and implementation risk.

Deloitte, Manager (Specialist Master), Jun 2010 to Dec 2017

- Created a well-defined Cybersecurity Data Architecture expanding monitoring visibility by 1100% (50 to 600 endpoints), enhanced vulnerability identification and remediation by 650% across the enterprise.
- Led a Global Security Operations Center (CSOC) team of 20 through a cognitive intellect transformation that maximized existing security solutions. Leveraged IBM's QRadar Security Intelligence and Event Management (SIEM) with Watson Advisor, Splunk Dashboards, Windows Event Collectors, and Sysmon. The cognitive intelligence solution improved detection rates while reducing false-positives, and false-negatives speeding time-to-threat closure.
- Designed 35 National Institute of Standards and Technology (NIST) Cyber which playbooks and processes to allow cyber analyst to create, classify, prioritize and escalate risk. Improved Level 1 and 2 (L1 / L2) Cyber Analyst's operational capabilities investigative tasks by 97%, from 6 hours to 15 mins.
- Advised 20 State and Local government enterprises on security hygiene and developed actionable strategies which optimized the use of current infrastructure for successful security transformation.

Vail Systems, Information Security Manager Dec 2009 to Jun 2010

- Developed an enterprise security framework used by application teams throughout the software development cycle for customized Voice over Internet Protocol (VoIP) applications to clients.

US Bank, Business Technology Analyst III Jan 2007 to Dec 2009

- Provided tier 3 and 4 developer support for the Bank’s e-payment and ACH application servicing over a 100 business-to-business (b2b) enterprise clients.
- Led application rollout and delivery of the e-payments system including go-live testing.

United States Army and Reserve, Information Systems Operator, Dec 1997 to Dec 2005

- Provided technical and IT infrastructure support for the Battalion (300 to 800 soldiers).

Education

- Master’s Degree, University of Illinois at Springfield, Anticipated Graduation 2023, Computer Science
- Bachelor’s Degree, SUNY Polytechnic Institute, B.S. Computer Science, 2006
- Certified Information Systems Security Professional (CISSP), (ISC)2

Publications/Presentations/Professional

- IBM Interconnect Conference, Presenter February 2016 - "SIA-4113 | Designing a Security Operations Center: Best Practices from [..], Deloitte”
- Deloitte Development, LLC. Publication, Author July 2016 - "Security Intelligence Framework - The comprehensive approach to security foresight” link here.
- Security Intelligence, Author Aug 2016 - " Cybersecurity: This Is Not a Drill" link here
- IBM Interconnect Conference, Presenter March 2017 - “Protecting the Crown Joules: Integrated Cyber Operations at New York Power Authority”