Jessica Claire

100 Montgomery St. 10th Floor • (555) 432-1000 • resumesample@example.com

Website, Portfolio, Profiles

- http://100miles.yolasite.com/
- https://www.linkedin.com/in/Jessicasha/
- https://twitter.com/inforsecur

Professional Summary

Forward-thinking Senior Manager adept at managing teams of 7 penetration testers with 3 direct reports to accomplish challenging objectives. Imparts clear vision to guide cohesive, high-performing teams. Jessica has over twelve years of information security, control and IT audit experience in a number of industries, including financial institutions, insurance and healthcare. Jessica's experience includes: reviewing system configuration (router/switch/firewall/server settings etc.), conducting Web and Mobile Application security, Source Code Reviews, Social Engineering Assessments as well as performing Black-Box/White-Box Network Penetration Testing on IT infrastructure components deployed and managed by the client infrastructure team. Jessica has assisted with IT general control reviews, PCI-DSS, SOC reviews and database security audits. Jessica holds a Bachelor of Computer Engineering from Mumbai University. Jessica is certified in Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA) and Provisional ISO 27001 Lead Auditor (ISO 27001 LA) & Certified Information Systems Security Professional (CISSP). Jessica regularly attends ISSA, ISC2 and ISACA Chapter meetings and participates InfoSec discussions to identify challenges faced in security industry.

Skills

- External Penetration Testing - Performing technical security testing on client's external (Internet) perimeter security to simulate real world cyber attacks from outside the Organization
- Internal Penetration Testing - Performing technical security testing on client's internal networks to simulate real world cyber attacks from known insiders or compromised systems.
- Web Application Penetration Testing - Performing sophisticated web application security testing that targets client websites that stores, processes or transmits sensitive PII information, healthcare data,credit card information, customer accounts and credentials. These websites are core client applications running their business to generate revenue.
- Mobile Device and Mobile Application Security - Performing security testing on Mobile applications and devices custom developed by Plante Moran's clients. The apps are developed for Android and iOS.
- Application Source Code Reviews- Reviewing the source code for security vulnerbailities within client's custom built application
- Data Leakage Prevention (DLP) Technical Auditing - Conducting simulated test to review client's Data Leak Prevention controls in place
- Social Engineering Assessments - Social engineering involves exploiting human emotions and trust factor to extract sensitive information through art of deception. This may include phishing campaigns, phone solicitation or physical impersonation. These projects are management approved and assist the client in devloping and improving their security awareness training programs.
- Network Device Configuration Reviews - Performing a configuration review for network devices such as routers, switches, firewalls, access points, SIEM and other security devices.
- Wireless Penetration Testing - Conduct review of wireless settings, encryption and security of devices to identify gaps and recommend best practices.
- Cloud Security Assessments - Performing a configuration review of Cloud environemnts such as AWS, Azure and Microsoft 365.
- Internal IT Lab Network monitoring, patch management - Maintaining, monitoring, patching and upgrading Plante Moran Cybersecurity Lab consisting of Servers, workstations, network devices, GPU based password cracking rigs and other penetration testing hardware such as DropBoxes for remote penetration testing, RFID cloner, rubber ducky, bash bunny, bad USB, WiFi Pineapple etc.
- IoT Device Security Research and testing - Research and security testing on IoT components that include medical devices, Automotive ECUs, Temperature control sensors and several other smart devices.
- CyberRange Simulation Training - Conduct and oversee planned red team (Offense) and blue team (defense) training for Plante Moran clients to improve their cyber defense skills, strategies and incident response.

Work History

Senior Manager - Penetration Testing, 04/2009 to Current
Verizon – Warren, NJ

- Developed and implemented Cybersecurity marketing plans to drive sales, profit and brand objectives.
- Supervised and managed all client-related communication to achieve messaging accuracy and service correctness.
- Managed large-scale projects and initiatives including, introducing new systems, tools, and processes to support attainment of challenging objectives.
- Managed team of 7 and practice development and management of $500,000 in revenue and oversaw all client related projects.
- Led teams focused on Penetration Testing and Vulnerability Assessment to accomplish quality report deliverables, surpassing established goals.
- Supervised and directed consultants, senior consultants, managers and technical teams to keep projects on-track and tasks prioritized.
- Developed proposals based on client requirements or RFPs
- Assisted in building 3 password cracking rigs consisting of 6 GPU cards each
- Regularly performed hands on advance penetration testing and vulnerability assessments.

Security Consultants (System Auditors), 03/2008 to 04/2009
Paramount Equity Mortgage – Dallas, TX

- Review and assess the adequacy of Information security provisions of IT infrastructure components deployed by client such as LAN/WAN architecture, Switching and routing components, perimeter security components and other support systems such as messaging systems managed by the client Infrastructure team. Identify Information Systems control weakness if any and propose a suitable remedy through application of appropriate technology component/compensating controls
  Continuously update the controls on new developments in Information Security space to ensure adequate upgrades are planned and executed

  OTHER ROLES & RESPONSIBILITIES AS FOLLOWING:

  Intrusion Detection, Incident Handling, Managing Firewall / VPN / IDS / IPS Infrastructure
- Security Event Correlation, Auditing & Log Monitoring Of Critical Information Assets like Servers Event Log, Firewall Log, Physical Access Card Reader.
- Information Security Auditing & testing Of Organization's Disaster Recovery Plans For Information Systems
- Providing Direct Information Security Training To All Employees, Contractors, Alliances, And Other Third Parties
- Establish And Maintain Best Practice Operating Policies, Write And Maintain Documentation For All Procedures And Processes.
- Working Knowledge Of Information Security Principles, Techniques And Technologies
- Hand On Experience In Vulnerability Assessment Tools Like MBSA, Nessus, WebInspect, Qualys
- Knowledge Of LAN And Microsoft Windows Network Technology
- Experience Configuration and Management Firewalls.
- Extensive Knowledge Of Hacking Tools
- Experience In Security Hardening Practices For Operating System
- Expertise With Application Security Testing I.E. Cross Site Scripting, SQL Injection, Buffer Overflow

Corporate Trainer, 10/2006 to 02/2008
KarROX Technologies – City, STATE
Providing IT Training In High End Technologies Like CCNA, CCNP, CCSP, LINUX L1 To Corporate Companies.
TRAINED PROFESSIONALS ON VARIOUS IT SKILLS AND TECHNOLOGY SUCH AS FOLLOWING:

- IP Addressing, IPv6, Routing, Routing protocols, Switching, Wireless, MPLS
- Ethical hacking, Linux, Configuring various Cisco Routers and switch series
- Troubleshoot client's network infrastructure, Basic configured and Managed Windows 2003 Domain Controllers for centralized user account management & DNS/WINS/DHCP server setup
- Handling queries and problem related to LAN connectivity
- Troubleshooting and Analyzing LAN problems
- Installation, Administration & Configuring Windows 98, Windows 2K Server & Professional
- Installations & Implementation virtual machine
- Implementing proper virus protection and security to secure LAN & systems

Education

Bachelor of Computer Engineering: Computer Engineering, 04/2006
University of Mumbai - Mumbai

Diploma in Computer Engineering: Computer Engineering, 06/2003
Maharashtra State Board of Technical Education - Mumbai

Affiliations

- Member of National Sports Club of India (NSCI)
- Member of Information Systems Audit & Control Association (ISACA) Chicago Chapter
- Member of ISC2 Chicago Chapter

Certifications

- Provisional ISO 27001 Lead Auditor (ISO 270001 LA) – Dec 2014
- Certified Information Systems Auditor (CISA) – Feb 2014
- Certified Information Systems Security professional (CISSP) - 2018
- Cisco Certified Network Associate – Security (CCNA Security) – June 2013 – NOW EXPIRED
- Certified on Fire Safety and Emergency Preparedness – Feb 2013
- EC-Council Certified Security Analyst (ECSA) – Mar 2010
- Certified Ethical Hacker (CEH) – Aug 2008
- Farhad Daudani Best Report Award for Internal Audit of Information Technology, 2008
- Cisco Certified Security Professional (CCSP) – Cleared SND, SNRS and SNAF – NOW EXPIRED

Languages

English:
Negotiated:

Hindi:
Negotiated:

Gujarati:
Negotiated:

Marathi:
Negotiated:

French:
Negotiated: