

Information Technology (IT) RESUME

1010 South Street, New York, NY 10002

(212) 304-5645

john.doe@gmail.com

IT Specialist with over 4+ years of experience in information security and digital forensics. Expert and highly familiar with a wide variety of security, engineering, networking, and operating system software. Possess an Associate Degree in Information Security and Digital Forensics.

TECHNICAL SKILLS

- **SECURITY:** McAfee SIEM/EPO/NSM, FireEye CMS/ETP, SecureWorks, IDS/IPS, Sumo Logic cloud-based log management, SSL certificate configuration and management, Juniper NetScreen Palo Alto Networks firewall
- **REVERSE ENGINEERING:** Ollydbg, WinBdg, GDB, IDA Pro, PEiD, malware sandbox
- **NETWORKING:** Wireshark TCPView packet analysis, DNS servers, mail server
- **OPERATING SYSTEMS:** Windows XP, Vista, 7, 8; Windows Server 2003, 2008, 2012; Linux including CentOS, Ubuntu, Arch, Debian, BackTrack, and Kali

PROFESSIONAL EXPERIENCE

SECURITY PROFESSIONALS INC.

Security Operations Center Security Analyst

Columbia, SC

January 2014 – Present

- Monitor multiple security systems for a Fortune 500 company
- Investigate arising incidents caused by malicious activities, and identified false positives
- Documented security events daily to create a baseline of activity for the client network

TECHNOLOGY SMARTS

Network Operations Center Monitoring Technician

Charleston, SC

January 2012 – December 2014

- Refined and improved existing documentation system, resulting in reduced labor costs totaling \$15,000 annually via increased workplace efficiency
- Consolidated multiple ticketing systems, improving communication and ticket turnover rate by 7%
- Investigated alerts created by IDS/IPS including malicious file uploads, compromised servers, SQL injections, and port scanning

CHICAGO GOVERNMENT

Information Security Intern

Chicago, IL

May 2011 – December 2012

- Monitored and managed email spam filters, firewalls, anti-virus systems, and vulnerability scanners
- Deployed and observed IDS sensors and their resulting alerts
- Performed in-depth forensics on workstation hard drives

EDUCATION

TRIDENT COMMUNITY COLLEGE

Associate Degree in Information Security and Digital Forensics, May 2011

Chicago, IL

- GPA 3.7/4.0