

Network Security Analyst Network Security Analyst Network Security Analyst Work Experience

Network Security Analyst Carnegie Mellon - Information Networking Institute September 2017 to December 2017 Collaborated with a four-man team to perform technical network security assessment and vulnerability mitigation services for Carnegie Mellon University. Configured a honeypot network with Docker and monitoring tools like Kibana and TcpDump, and connected it Microsoft Azure to monitor and troubleshoot network systems. Researched and analyzed Indicators of Compromise using Wireshark, Scapy and Netflow Analyzer to perform intrusion detection. Visualized cyberthreat statistics and created threat documentation using Python data visualization tools to effectively communicate cybersecurity risks to clients. Recommended suitable vulnerability mitigation solutions to executive clients.

Security Risk & Compliance Intern Salesforce - San Francisco, CA May 2017 to August 2017 Created and visualized an enterprise wide risk control matrix for real time and automated technology risk monitoring that enables strategic risk decision making. Led a department wide project to benchmark Salesforce's technology risk and compliance efforts against widely applicable industry practices. This resulted in a matured risk and compliance process as required by organizational objectives. Interfaced with customers to managed customer security requirements by testing and validating product security controls and practices. This maintained customer trust in Salesforce cloud products. Performed ISO 27018, ISO 27001and PCI-DSS assessments to verify high quality cloud security for Salesforce products.

IT Consultant YWCA Greater Pittsburgh January 2017 to May 2017 Identified and planned technology requirements by collecting and analyzing customer data using Python and Excel scripting skills to produce business intelligence and align IT needs with organizational goals while engaging employees at all levels of the organization. Managed deployment of Spiceworks helpdesk ticketing system to optimize the system administration and helpdesk management process. Led the implementation of IT Security capabilities by planning & assessing cybersecurity requirements, performing enterprise wide cyber risk assessments, configuring network security capabilities and continuous security monitoring through Spice Works. Improved system and security operations by 60%.

Network Security/Threat Intelligence Analyst Carnegie Mellon - City of

Pittsburgh September 2016 to December 2016 Sep 2016-Dec 2016 Network Profiling for the City of Pittsburgh using Silk Network Security/Threat Intelligence Analyst Worked with a four-man team to perform a comprehensive network security assessment for the City of Pittsburgh. Performed network monitoring and netflow analysis to identify and analyze Indicators of Compromise using the following tools and skills: SILK, Wireshark, Snort, Bash Scripting. Documented executive cyberthreat reports and visualized findings in a clearly understandable format. Made cost effective recommendations that enabled the city to achieve 70% drop in cyber vulnerabilities without exceeding their budget Information Security Consultant Rhythex Consulting - Lagos, NG June 2015 to July 2016 Collaborated with diverse teams of consultants to successfully deliver high quality security services for multinational banks in Nigeria using the following standards: PCI-DSS, ISO 27001 & COBIT5. Performed technical security compliance assessments through penetration testing and vulnerability scanning using tools like Nmap, Nessus and OpenVas to verify compliance with PCI-DSS. Implemented security solutions like Cisco ASA Firewalls, Symantec DLP, Microsoft Azure IAM. Improved system and security operations by 70%. Education Master of Science in Information Security Policy & Management Carnegie Mellon University - Pittsburgh, PA May 2018 Skills ISO (1 year), PAYMENT CARD INDUSTRY (1 year), PCI (1 year), CISCO (1 year), FIREWALLS (1 year) Additional Information SKILLS Aug 2016 - May 2018 Tools: Nmap, Nessus, Splunk SIEM; Snort & Suricata IDS/IPS; TcpDump; Metasploit; SQLMap; OpenVas; Cisco and Endian Firewalls, Wireshark, Argus, SiLK, Hex Editor Languages: Python, Bash, SQL Platforms: Windows, Linux, VMWare, AWS Frameworks: TCP/IP, SOC, SOX, ISO 27001, ISO 27018, COBIT5, PCI-DSS, HITRUST, Secure Software Development Lifecycle, NIST, FISMA, HIPAA, ISO 2000, EU GDPR

Name: Thomas Thomas

Email: iandrews@example.com

Phone: +1-937-470-9574x37032