Information Security Analyst DLP Analyst Information Security Analyst DLP Analyst IT Security Analyst III Atlanta, GA As a Security Analyst I'm knowledgeable in conducting cyber-risk assessment, security awareness, and serve as a focal point as relates to information security metrics and key performance indicator that's monitored within the organization as it relates to compliance with industry standards and regulations. Authorized to work in the US for any employer Work Experience Information Security Analyst DLP Analyst First Data - Atlanta, GA November 2018 to March 2019 Knowledgeable of hacker methodologies and tactics, system vulnerabilities and key indicators of attacks Knowledgeable of Dynamic Application Security Testing tools Able to investigate ethics and security-related incidents. Able to define events vs. alerts vs. incidents for the organization, and create incident classification, severity, and priority tables in line with all threats, risks and vulnerabilities. Able to identify and document incident trends and compromise patterns. Provide Tier 2 & Tier 3 support to SOC analysts Eight years of technical experience in the information security field Eight years of incident response, analysis and escalation Experience with forensics, chain of custody, and EnCase Identify and isolate malware and provide guidance on remediation and prevention. Perform daily system administration tasks (e.g., backups, patching, log review). Support the vulnerability assessment process. Participate in forensic investigations. Assist in producing and maintaining security metrics. Support internal compliance functions. Stay current on IT Security news, trends and best practices. Security tools utilize are RSA Archer, FireEye HX, NX, AX, McAfee AV, Bit9/Carbon Black, Splunk, Microsoft defender ATP, IBM Q-radar SIEM, LogRhythm SIEM, Juniper Sky ATP, IBM Proventia IPS devices, and Bluecoat proxy. Performs other duties as assigned. IT Security Analyst III Fidelity National Services, Inc April 2018 to November 2018 In depth understanding of Information Security domains, this include governance & compliance. Perform all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. Executes security controls to prevent hackers from infiltrating company information or jeopardizing programs. Maintain security systems and administers security policies to control access to systems. Maintains company firewall and utilizes applicable encryption methods. Implements and administers information security controls using software and vendor security systems. Security tools utilize are RSA Archer, FireEye HX, NX, AX, McAfee AV, Bit9/Carbon Black, Microsoft defender ATP, IBM Q-radar SIEM, LogRhythm SIEM, Juniper Sky ATP, IBM Proventia IPS devices, and Bluecoat proxy. Cyber Security Analyst Comprehensive Health Services - Cape Canaveral, FL June 2015 to October 2017 In depth understanding of networking systems, firewalls, simple DNS & DHCP, security vulnerabilities, exploits, attacks and malware. Monitor use of data files and regulate access to safeguard information in computer files knowledge of NIST 800-53, ISO 27001, PCI DSS and SOC standards Review security events that are populated in a Security Information and Event Management (SIEM) system. Watch active dashboards and replay and interpret events. Investigate using alerts, event graphs, annotations, cases and reports. Recognize patterns or inconsistencies that could indicate complex cyber-attacks. Owasp, Symantec, LogRhythm, Patch management, Privileged identity management, FireEye Quickly and accurately classify, prioritize and escalate events to incidents when necessary. Recommend improvements to service, efficiency and quality of work. Detect security issues, create customer tickets and manage problems until closure. Coordinate escalations and collaborate with external technology teams to ensure timely resolution of issues. Experience identifying threats, vulnerabilities, exploitations and applying security controls, tools and techniques to detect or gather information on domains or subjects. Report common and repeat problems (trend analysis) and propose process and technical improvements. Stay up to date with current vulnerabilities, attacks, and countermeasures. Demonstrate excellent communication and customer care skills. Solid Generate end-of-shift reports for documentation and knowledge transfer to subsequent analysts on duty. Office Assistant True Digital Security April 2008 to October 2011 Monitor use of data files and regulate access to safeguard information in computer files Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures Modify computer security files to incorporate new software, correct errors, or change individual access status Monitor current reports of computer viruses to determine when to update virus protection systems Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs Document computer security and emergency measures policies, procedures, and tests Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated Prepare weekly information security reports   2008-2011 Education Master's in Information Systems Security Dakota State University - Madison, SD August 2016 to Present Bachelor's in Information Assurance South University - Tampa, FL August 2012 to June 2014 Associate in Information Assurance and Digital Forensics Oklahoma State University - Okmulgee, OK September 2005 to April 2009 Skills security, Microsoft Office, Sharepoint, Active Directory, testing, HTML, training Military Service Branch: USAF Service Country: United States Rank: E4 Airforce Aircraft Repair Airman, Designs, repairs, modifies and fabricates aircraft, metal, plastic, composite, advanced composite, low observable, and bonded structural parts and components. Applies preservative treatments to aircraft, missiles, and support equipment. Earned various awards for excellent service. Also, experience supervising functions dealing with corrosion identification, prevention, and repair; applying protective coatings and markings; or fabricating, assembling, and repairing metal, fiberglass, composites, honeycomb, and plastics. Certifications/Licenses Senior Systems Managers CNSS 4012 April 2008 to Present The 4012 certificate program provides the standards for the development and implementation of Information Assurance (IA) training for Senior Systems Managers (SSM) of national security systems and unclassified systems. Information Systems Security (INFOSEC) Professionals NSTISSI 4011 April 2008 to Present The 4011 certificate program is available to undergraduates and non-traditional students. The aim of this program is to provide the minimum course content for the training of information systems security professionals in the disciplines of telecommunications security and automated information systems (AIS) security Senior Systems Administrators CNSS 4013A April 2008 to Present The National Security Agency (NSA) and the Committee on National Security Systems (CNSS) recognized that Cisco security courseware meets the CNSS 4013 training standard. By being compliant, the Cisco CCNP Security certification program provides the required training for network security professionals who assist federal agencies and private sector entities to protect their information and aid in the defense of the nation's vital information resources. This advanced standard is intended for System Administrators responsible for the security oversight or management of critical networks.

Name: Mark Gonzales

Email: brandon38@example.net

Phone: 4023928704