Security Analyst Security Analyst Jessup, PA Work Experience Security Analyst Cognizant Technology Solutions 2018 to Present Coordinated development of custom ISIM adapters. Configured provisioning policies and roles per requirements. Perform DAST and SAST scanning for web applications using Blackduck, Fortify, and Qualys WAS. Report metrics to leadership and helped prioritize remediation activities. Installed ForcePoint DLP infrastructure and configured protection policies. Facilitated testing and deployment of agents in enterprise. Coordinated testing, deployment, and tuning activities for Cisco Amp initiative. Provide guidance for new projects from a security architecture perspective. Answer security questionnaires received as part of RFP process. Gather evidence to support internal and external audit activities. Perform incident response activities for alerts triggered by QRadar and other security tools. Cybersecurity Analyst Geisinger 2016 to 2018 Lead implementation of CrowdStrike Falcon NGAV solution across multiple domains and networks spanning 35,000 nodes. Primary resource responsible for management of CrowdStrike Falcon Platform. Coordinating sensor updates, tuning false positive detections, remediating virus-related alerts, and performing threat hunting activities using Splunk query language. Managed information security incidents generated by MssP from triage through resolution. Coordinated with internal and external teams to remediate incidents. Facilitated onboarding of new log sources to MssP. Investigate and remediate log delay alarms. Provided tuning guidance to reduce false positives. Created procedures for incident handling and provide guidance to junior team members. Analyzed threat intelligence data and search environment for exposure to current threat vectors. IT Security Analyst II TMG Health Inc 2015 to 2016 Primary resource responsible for monitoring offenses, creating offense rules, and tuning false positives in QRadar. Worked with IT team to onboard more log sources into the tool for analysis. Configured and maintained active directory change alerts and reports using change auditor. Developed PowerShell scripts for automating manual tasks. Created and maintained roles in IBM Security Identity Manager. Performed security assessment of products prior to use in the enterprise. Primary resource responsible for internal and external audit responses for the security team. Performed vulnerability assessments using Nexpose. Installed and configured CyberArk.

Promoted the use of the tool across the enterprise. IT Compliance Analyst Geisinger Health Plan 2013 to 2015 Performed vendor security risk assessments on applications. Worked with application owners to remediate vulnerabilities identified in Qaulys scan reports and documented exceptions for risks that could not be remediated. Conducted audits on application access, terminations, and change management processes. IT Security Analyst TMG Health Inc 2011 to 2013 Monitored active directory change logs for suspicious activity. Performed vulnerability assessments using Nexpose and worked with operational areas to remediate identified risks. Performed identity and access management for all organizational applications. Performed requirements analysis, end to end testing, and assisted in the development of business roles for the implementation of IBM Security Identity Manager. Developed custom access reports for in-house applications using SQL. Gathered evidence for internal and external auditing requests. Education B.S. in Information Sciences and Technology Pennsylvania State University Skills SECURITY, WEBSENSE, DATA LOSS PREVENTION, DLP, INFORMATION SECURITY Certifications/Licenses Certified Information Systems Security Professional (CISSP) 2016 to Present https://www.youracclaim.com/badges/d9c99999-7883-4954-a6d6-da26ebf9f0cc/public_url Certified Ethical Hacker (CEH) 2015 to Present ITIL v3 2014 to Present GIAC Continuous Monitoring Certification (GMON) 2018 to Present https://www.youracclaim.com/badges/e64fe292-f90d-48b1-a5a1-c79be538332c/public_url Certified Cloud Security Professional (CCSP) 2018 to Present https://www.youracclaim.com/badges/449a9b82-94dc-41d9-9c3b-5ce0204d3717/public_url Information Systems Security Architecture Professional (CISSP-ISSAP) 2019 to Present https://www.youracclaim.com/badges/716e9bec-7f77-4448-98d1-72746da51432/public_url CompTIA Security+ 2014 to Present https://www.youracclaim.com/badges/eafb62e1-83a5-4e9b-b997-fb743382ba81/public_url Additional Information Skills: Strong knowledge of active directory, system architecture, network security, log analysis, and system administration. Over 8+ years of experience in the field of Information Security. Strong understanding of current threat vectors and attacker methodologies.

Experience scripting and automating using PowerShell. Excellent communication, troubleshooting, customer service, and analytical skills. Experience managing security tools and driving security initiatives. Specialties Vulnerability Management Malware Analysis Incident Response Log Analysis Security Monitoring and Threat Analytics Tools Proficiency: Identity Management: IBM Security Identity Management (ISIM), CyberArk Vulnerability Management: Nexpose, Qualys VM Antivirus: CrowdStrike Falcon Platform, Symantec Endpoint Protection, Cisco AMP Security Monitoring: QRadar, Symantec MssP, Dell Change Auditor, NetWrix, ArcSight Logger Proxy: Websense Triton IPS: FireSight, TippingPoint Application Security: BlackDuck Hub, Fortify, Qualys WAS Data Loss Prevention: ForcePoint DLP

Name: Tina Brown

Email: terriwatson@example.org

Phone: 672-938-8532x64199