IT Security Analyst IT Security Analyst IT Security Analyst - FirstCare Health Plans Austin, TX Cybersecurity analyst with 4 years of experience in enterprise IT security and incident response. Aiming to use my current skills in SIEM management, DLP, mail protections, identity management and incident response to further your organizational goals and security posture. Work Experience IT Security Analyst FirstCare Health Plans - Austin, TX March 2018 to Present Data Loss Prevention (DLP) Developed policies using regular expression to search for outbound sensitive material within the Mimecast mail gateway. Resulted in the prevention of over 200 potential HIPAA breaches in first month of implementation. Mail protections Architected attachment and URL protections for inbound email. Attachments were scanned in a sandbox before delivery and URL s were rewritten to be scanned in a sandbox before allowing recipient to access. Resulted in the prevention of multiple ransomware and phishing attempts originating from inbound email. Security policies Wrote policies quarterly to standardize corporate compliance with security best practices. Revised policies to keep pace with changing security landscape. SIEM Aggregated logs in Splunk to then create reports and dashboards to improve and expedite security monitoring. Vulnerability management Utilized vulnerability scans in Rapid7 s Nexpose to compile lists of necessary patching and hardening. Designed sites to pinpoint configuration vulnerabilities within architecture and software. Patched systems using Kaseya. Identity management Configured SSO and MFA for multiple products using Centrify IDM. Resulted in streamlined experience for users while protecting against credential theft. Security awareness training Simulated an Incident Response tabletop for IT management. Performed multiple phishing exercises against user base and then provided training to the users that failed. Incident Response Analyst - Department of Homeland Security (DHS) HQ Knight Point Systems January 2017 to March 2018 Worked as a direct contractor for Department of Homeland Security HQ Enterprise Security Operations Center (SOC). Incident Response Investigated and triaged potential incidents found in security tools and monitored environments. Coordinated response to confirmed incidents. Utilized open source tools to analyze malware and obtain information about threats. Security Policies Wrote multiple Standard Operating Procedures (SOP) and workflows that were submitted for government approval. Created and maintained security policies for the SOC. This allowed for standardization of practices and clear documentation of SOC activity. Training Trained Tier 1 and Tier 2 analysts in basic triaging and monitoring techniques. SIEM Designed, implemented and maintained entire collection of monitoring dashboards in Splunk. Incident Response Analyst United States Citizenship and Immigration Services November 2015 to January 2017 Worked as a direct contractor for Department of Homeland Security Enterprise USCIS SOC. Incident Response Monitored security tools for indications of malicious activity, unauthorized or anomalous behavior on the USCIS Enterprise. Triaged and mitigated incidents. Hunting Defined Enterprise searches for IOC s in FireEye. Determined IOC s by analyzing malware and suspicious activity. PCAP Analysis Retrieved PCAP in NetWitness to then analyze in Wireshark. Used results to identify malicious activity as well as IOC s for hunting purposes. Documentation Authored internal processes and policies. Created wiki for to assist entire team in standard incident response techniques. IT Support CrochetKnitStitch - Waldorf, MD May 2014 to February 2015 Responsible for day-to-day IT operations for this small business. Created and maintained business website and online payments. Managed marketing through various online media. Published weekly and monthly newsletters. Handled all IT related issues for the business. Provided direct support to customers for IT related issues. Education BS in Cybersecurity Western Governors University 2019 AA in General Studies College of Southern Maryland May 2014 Skills It Security, Information Security, Cyber Security, Remedy (1 year), ServiceNow (1 year), McAfee ePO (3 years), McAfee NSM (1 year), Splunk (3 years), FireEye HX (1 year), Mandiant MIR (2 years), Redline (2 years), Tanium (1 year), Mimecast (Less than 1 year), Centrify (Less than 1 year), Rapid7 IDR and Nexpose (Less than 1 year), Cisco Umbrella (Less than 1 year), Palo Alto (Less than 1 year), Policy Development (4 years), Comptia, Documentation (4 years), Carbon Black (1 year), Active Directory Certifications/Licenses GIAC Certified Incident Handler (GCIH) October 2017 to October 2021 CIW Site Development Associate April 2018 to Present ITIL v3 Foundations October 2017 to Present CompTIA A+ March 2017 to March 2020 CompTIA Security+ June 2016 to June 2019 CIW Web Security Associate May 2018 to Present Additional Information Incident Types Handled Malware Ransomware Phishing emails

Improper Usage   Unauthorized Software   Brute Force   ICMP Sweeps   Classified Data Spills

Tor Attempts   Unauthorized Access   Blue team for penetration tests   Spoofed emails

Name: Jessica Butler

Email: nicholas66@example.net

Phone: 733-773-1003