Analyst Analyst Analyst - U.S. National Institutes of Health - Incident Response & Cyber Intel Arlington, VA To find an opportunity in Security Analysis, Incident Response, Security Consulting, Security Engineering/Architecture, or Security management that provides a challenging, growth-oriented, and teamwork-oriented environment. Work Experience Analyst U.S. National Institutes of Health - Incident Response & Cyber Intel January 2018 to Present Responding to attempts and successful breaches of the U.S NIH network by taking immediate and appropriate steps to thwart, mitigate, investigate, and proactively prevent cyber-attacks. Time to detection to final decision faster than any analyst in 85-50 % of events Improved incident response time across the team significantly; often by multiples of time Improved average time for response and mitigation of phishing campaigns by at least ten-fold by increasing coordination with email team, introducing new processes and procedures, suggesting and implementing new detection methods, and writing documentation for analysts to reference. Wrote java application to automate the process of syntax encapsulation for large amounts of threat indicators gathered from intelligence sources, leading to significant increase in investigative speed, and a decrease in work load for analysis. Suggested, created, and tested Linux virtual machine used by analysts to handle and sandbox-analyze malware. Assisted engineers in finding errors and misconfigurations in IDS tools, as well as investigating the sources for "noisy" alerting across the NIH network. Helped to train six new analysts in full scope of work duties and general incident response practices. Suggested and helped design new Splunk dashboards that improved organization and accounting of incidents, detection of incidents, and ease of investigation. Participated in evaluating new security tools in meetings with sales reps from various vendors Using various tools to analyze malware, such as, FireEye AX, Virus Total, Wildfire, Joe's Sandbox, and Hybrid Analysis Using host based and network-based IDS systems (FireEye HX & NX and Carbon Black) to analyze and contain malicious activity on the network. Also wrote host-based IDS rules for malicious activity detection. Using PhishMe Triage, Cisco IronPorts, IDS Tools, Splunk, and Netwitness to analyze, investigate and take appropriate actions on malicious emails and campaigns. Using Grafana to graphically analyze firewall and router log data to determine DDOS activity Using Splunk to research and

correlate log data from hosts and various types of servers for detection and investigation of incidents Using Redline to analyze system triages to determine stages of infections, delivery methods, and network abuse Using RSA Netwitness and Wireshark to capture and analyze packet data for malicious activity Generating and submitting daily threat activity reports to the U.S Dept. of Health and Human Services Attending and participating in meetings with CISOs/ISSOs of all 31 NIH Institutional Centers in order to provide and gain intelligence on security posture, threat trends, strategy, etc. Advisor & Investor Samurai Security June 2016 to Present Assisting a team of technical and non-technical individuals in building a total cyber security system and infrastructure ? Further details cannot be disclosed at this time due to intellectual property and copyright considerations. Cyber Security Analyst World Learning & SIT Graduate Institute December 2016 to January 2017 Security incident response, incident handling, and remediation Using PDQ deploy to send out domain-wide updates and patches for antiviruses, browsers, and other software applications Managed large-scale DoD standard drive wiping operation with personally created DBaN bootable drives, and coordinated the donation of the computers to people in need in Uganda, Namibia, Mongolia, and the U.S. Malware sandboxing on Linux and Windows VMs Responding to and managing network access control with 802.1x and ForeScout CounterAct Conducted vulnerability scans with Tenable Nessus Scanner and Tenable Security Center SIEM Using Splunk for machine log collection and analysis Used Tenable Security Center to analyze amalgamation of security events, set policies, and create reports Active Directory administration via GUI and PowerShell scripting. Actions including but not limited to: user account creation and administration, security group management, OU organization, BitLocker key management, Device management, distribution group management Symantec Endpoint Protection Management and Server configuration Conducting employee cyber security training and enforced adherence to security policies Effectively instituted pre-travel hardware hardening and preparation for employees traveling internationally, as well as post-trip malware scanning and OS reconfiguration Performing machine baseline analysis and vulnerability checking with Microsoft Security Baseline Analyzer Conducting analysis on SSL/TLS certificates Conducting log analysis on systems for

security alerts, anomalies, and to generate reports Performing file integrity checking for new software and updates prior to global domain-wide deployment Linux client administration and troubleshooting Remotely supporting users in field offices around the world whilst using security and privacy skills to circumvent content policy filters in foreign nations, i.e., China Performed major lost data retrieval for professors and NGO program officers and associates that helped to recover entire course packages and USAID grant programs respectively Using Excel to create pivot tables, graphs, and spreadsheets for data reporting and project planning Partner, CCO GreenLED November 2015 to December 2016 Helped company to secure investment capital and a partnership with Transit Labs Integral in creation of the company's overall market strategy and business plan Oversaw design of company website Performing OS fingerprinting and web analytics in order to gather and use data on web site visitors Assisted in search engine optimization for www.greenled.world Made connections with complementary and supplementary businesses, thought leaders, and policy makers Managed various personnel including web developers, graphic artists, sound technicians, social media managers, and professional actors Produced, directed, casted, and helped to write script, for crowd-funding infomercial Helped to design crowd-funding campaign and marketing strategy IT Support Specialist Tier II Samurai Security June 2016 to October 2016 Remote troubleshooting of technical issues for students and staff on various computers and mobile devices via phone and remote desktop support with GoTo Assist and Citrix Security incident response with malware identification and removal Conducted analysis on SSL/TLS certificates Analyzing emails and web traffic to alert students and staffs of malicious emails and sites Used CRM analysis and identity verification to detect social engineering attempts Remote LAN troubleshooting Advising students on the best course of action for dealing with technical and administrative issues Supporting and troubleshooting web applications such as ICampus, BlackBoard, Canvas, and Pearson Ilabs Troubleshooting internet browser issues (Chrome, IE, Firefox, & Safari) IT Support Specialist L3 Communications April 2015 to November 2015 Conducted incident response and incident handling for malware, phishing, and certificate related incidents Primary virus detection and removal technician Employed identification

methods to thwart social engineering attempts Troubleshot and installed police department devices and software Managed user Active Directory accounts: enabling/disabling accounts, password management, group lists, administrative rights, resource access, resource enabling/disabling, and unlocking accounts Installing and troubleshooting Excel macros and using VLOOKUP Configured and supported VPN and remote desktop software Troubleshooting BitLocker Drive Encryption Primary PC speed optimization technician Solved and administered help desk support tickets for hardware, software, mobile, operating system, and network issues within an ITIL framework via phone and remote desktop support in a virtual desktop environment High volume ticket management and administration (25-30 tickets per day) IT Support Specialist University Research Co. & Center for Human Services March 2015 to April 2015 Created secure physical backups and organized digital data management for company email archives Conducted incident response for malware relate incidents Deployed system images onto various machines Performed user profile back-ups and migrations Configured and supported VPN and remote desktop software to protect medical records for HIPPA compliance Solved help desk support tickets on hardware, software, operating system, mobile phone, Cisco phone, and network issues via both phone support and desk-side support. Set up and installed hardware, software, and networking components for employee work stations Created documentation for Cisco WebEx Conducted a training session on Microsoft Office 365 including One Drive & SharePoint Troubleshot LAN and WAN connection issues Installed custom modules for Microsoft Outlook Education Certification in AP Computer Science Code Academy June 2014 HCI The Ohio State University Associate of Arts in General Studies Montgomery College Skills SECURITY (3 years), INCIDENT RESPONSE (1 year), MALWARE (1 year), CISCO (Less than 1 year), JAVA (Less than 1 year) Additional Information TECHNICAL SKILLS Key Skills: Malware Analysis and Containment, Data Exfiltration detection, Code Analysis, Packet Capture and Analysis, Traffic analysis, Linux Scripting and Engineering, Java Programming, SQL Querying, Vulnerability Assessment, System Hardening, ACL Configuration, System Monitoring, Network & System Security Design Conceptualization, Cryptography writing, Windows / Linux Systems, System Administration, DoD

standard drive wiping, MAC & IP spoofing, File Integrity Checking Tools Used: Palo Alto Firewalls, FireEye HX, FireEye NX, Redline, Splunk, Splunk ES, Wireshark, Tenable Security Center, Tenable Nessus Vulnerability Scanner, RSA Netwitness, Carbon Black, ForeScout CounterAct, Bro, Cisco IronPorts, PhishMe Triage, InfoBlox, Microsoft Security Baseline Analyzer, Websense, Blue Coat, Sodium, Linux IP Tables, Windows Firewall, Comodo Firewall, urlscan.io, Symantec Endpoint Protection Manager, Suricata, Snort, Linux Security Onion, Blue Coat Proxy, Incident Response Database and Tools, Grafana, Active Directory, DBAN, TOR Browser, Jupyter Notebooks, Random User Agent SUMMARY OF QUALIFICATIONS Created malware handling and analysis machine w/ IPS agent Developed custom symmetric text encryption software written in Java for use on Linux Experience configuring Suricata and Snort IPS systems on Linux Experience using Linux to load IPS systems with virus definitions Programming languages in order of strength/experience: Java, SQL, C++, C+, HTML, Python Experience using RegEX for finding text patterns in large data sets Setting up and working in virtual environments for sandboxing with both Windows and Linux Expert in client, router, and server hardening Experience in configuring ACLs for Comodo and Windows firewalls Experienced in using fuzzing techniques to test software for exception handling and errors Experienced in using Wireshark for packet capture and analysis Conducing security incident investigations on clients, servers, and networks Experience using, troubleshooting, and configuring VPNs on Linux, Windows, Mac, and Android Experience with basic to intermediate level Linux scripting in Ubuntu, Fedora, Debian, & CentOS Drive and file encryption in Linux and Windows Experience using PGP to encrypt messages and files Experience creating and deploying group policies Experience with reconfiguration of router settings for security Expert in browser hardening using privacy and security settings in about:config in Firefox Experienced in using web privacy controls such as plug in control, privacy and spoofing add-ons, pop up blockers, proxy configuration, and privacy add-ons Familiarity with domain administration systems: LanDesk, PDQ Inventory, and PDQ Deploy Experienced in employing and checking for secure coding techniques as well as using Fuzzing to test code Managing physical security controls such as entry tokens Proficient in Windows Active Directory administration via GUI & PowerShell

scripting Experience with web design languages: HTML, XML, and JavaScript Experience working within an ITILv3 framework Understanding of DNS, DHCP, TCP/IP, LAN, WAN, and VPN Experienced using TOR and editing system/browser configuration to safely gain access to and do research on the Dark Web Proficient in using Windows Regedit for confirming virus removal, OS optimization, and software troubleshooting Experience with using various ticketing software such as SysAid, Remedy Force, Dell Kbox, and Manage Engine, Service Now Advanced experience using Microsoft Excel for data organization/handling Experience designing technical solutions and procedural documentation for various business scenarios Intermediate Spanish, novice French, novice Arabic

Name: Lisa Sanchez

Email: elizabeth86@example.org

Phone: 447.245.8508x6577