Security Engineering Consultant Security Engineering Consultant Security Engineering Consultant - Samur.ai Security Arlington, VA To find an opportunity in cyber security analysis, security engineering, threat intelligence, consulting, or project management that provides great challenge and opportunity for growth. My future objective is to transition into penetration testing. Authorized to work in the US for any employer Work Experience Security Engineering Consultant Samur.ai Security - Arlington, VA June 2016 to Present Arlington, VA Assisting a team of technical and non-technical individuals in building a total cyber security system and infrastructure. Researching, testing, and advising on implementation of security tools and controls on the AWS backbone Design and implementation of containerization and segmentation technologies for separation of platform sections. ? Further details cannot be disclosed at this time due to intellectual property and copyright considerations. Cyber Security Analyst/Engineer Bon Secours Mercy Health Systems - Richmond, VA August 2018 to April 2019 Working as a cyber security engineer in Bon Secours' Enterprise Security Assurance and Monitoring team. My role generally consists of studying and monitoring the network and security posture, and devising or advising solutions to increase cyber security. Helped to create a method for prevention of execution of malicious documents and excel files brought in via malicious emails. Success rate of for preventing infection with this method when applied to any Windows system has been 90+% effective. Introduced multiple tools to the security team for use in investigations including sandboxing tools, domain analysis tools, IP analysis tools, packet analysis tools, email header analysis tools, and more. Wrote Java application to increase speed of searching network traffic for known malicious indicators with Qradar's AQL language and Carbon Black Response's syntax. Directly provided the CISO with more than 10 suggestions on infrastructure, processes, and tools to increase the organization's security posture. Uncovered various weaknesses in IPS posture and network architecture, some of which have led to subsequent attacks being thwarted or mitigated. Assisted in evaluating new software for detection of vulnerabilities and risky security postures in medical devices. Created a method for detecting bitcoin addresses in email bodies to prevent bitcoin extortion scams. Conducting research on Snort rules for addition to, and verification of, NIPS Snort rules set. Using DLP tools to analyze data loss after incidents, especially pertaining to possible HIPA related breaches Conducting daily threat hunting, incident response, and security control quality assurance Expanded the team's utilization of RegEx by introducing regex builder software, and applying regex in use cases. Introduced a new standard for security incident documentation Cyber Security Consultant Transit Labs - Washington, DC October 2018 to February 2019 Working as a security advisor in order to assist Transit Labs for their internal organizational privacy and security concerns, as well as those of their clients whom they deploy systems for Advised the company on strategic partnerships for fulfilling physical and cyber security needs of their overseas analytics command centers. Providing advice and suggestions for security aspects of the software development life cycle for their customers' systems. Advising and helping to develop the security controls, tools and policies of the Azure cloud infrastructure, including helping to develop custom rules for access control. Cyber Security & IR Analyst National Institutes of Health- Office - Bethesda, MD January 2018 to August 2018 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 other analyst in 85-90 % 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 in O365 and Cisco Iron Ports, 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 analysts. 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 with the creation of new Splunk applications and dashboards that improved organization and accounting of incidents, detection of incidents, ease of investigation, and key data correlation. 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 Used 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. Used PhishMe Triage, Cisco IronPorts, IDS Tools, Splunk, and Netwitness to analyze, investigate and take appropriate actions on malicious emails and campaigns. Used RSA Netwitness and Wireshark to capture and analyze packet data Used Grafana to graphically analyze firewall and router log data to determine DDOS activity Used Splunk to research and correlate log data from hosts and various types of servers for detection and investigation of incidents Used Redline to analyze system triages to determine stages of infections, delivery methods, and network abuse 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 28 NIH Institutional Centers in order to provide and gain intelligence on security posture, threat trends, strategy, etc. Domain Admin. & Cyber Security Analyst World Learning & SIT Graduate Institute - Washington, DC December 2016 to January 2018 Security incident response, incident handling, system remediation, and forensics collection Used 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 less fortunate in the U.S. Malware sandboxing and memory dumping Responding to and managing network access control with 802.1x 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, and O365 account provision and security policy control implementation and monitoring. 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 Conducted analysis on SSL/TLS certificates Conducted log analysis on systems for security alerts, anomalies, and to generate reports Performed 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 Used Excel to create pivot tables, graphs, and spreadsheets for data reporting and project planning Partner, CCO Rockville, MD 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 Samur.ai Security - Herndon, VA 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 Analyzed 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 Advised students on the best course of action for dealing with technical and administrative issues Supported and troubleshooting web applications such as ICampus, BlackBoard, Canvas, and

Pearson Ilabs Troubleshot internet browser issues (Chrome, IE, Firefox, & Safari) for corporate applications and O365 MD L3 Communications - Rockville, MD 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 Installed and troubleshot Excel macros Configured and supported VPN and remote desktop software Troubleshot BitLocker Drive Encryption issues 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) Education Security + Certification The Ohio State University June 2014 Associate of Arts in General Studies Montgomery College

Name: Francis Archer

Email: jpayne@example.net

Phone: (756)476-6484