Senior Cyber Security Engineer Senior Cyber Security Engineer Senior Cyber Security Engineer - Terp Techs LLC Silver Spring, MD Work Experience Senior Cyber Security Engineer Terp Techs LLC - Hyattsville, MD May 2019 to Present Relevant Skills: RMF - DODAF/TOGAF, Categorize Info. Systems, Security Impact Analysis, Select Sec Controls - SSP, Implement Sec Controls, Sec. Control Assessment - SCA, Security Assessment Report - SAR, Authorize Info System - POAM, and Monitor Sec Controls. Analysis/Auditing of Major/Minor Applications', RoB, ETA/ERA, ISA, MOU, MOA, PTA, PIA, SDD, DRP, SORN, BIA, IRP, CMP, ISCP, CIS Report/Worksheet, VSE, Incident Response, Tenable Nessus Security Center Analytics/Audits, FireEye HX, Microsoft Threat Modeling Tool, carbon Black, IBM App Scan Analytics/Audits, Check Point-Smart Endpoint Analytics/Audits, Splunk Analytics/Audits, IT Security System/App Waivers, Software Release Plan, JIRA, ESET Admin, Infoblox Grid Manager, Patch Management Audits, Cylance Admin, SharePoint Admin, IBM BigFix Analytics/Audits, Management of OWASP SAMM, Secure Code Review, Pen Test Results, Nessus Results, Database scan - POA&Ms, HP Fortify scans, CVE, CCE, CVSS, Cloud Security Auditing, Amazon Web Services (AWS) and Azure Cloud Computing Platforms, GRC Tools - NSAT/RV/eMASS, and Archer. STIGS, SRG, CIS benchmarks, Security A&A, NIST SP 800 series', DOD 8500, 8510, VA 6500, DHS 4300A, DOD SRG, DOD STIGS, DOD SCCA, FIPS, IRs', FISMA, FedRAMP, Standards and Guidelines, Laws and Regulatory Compliance (OMB M-04-04, HSPD-7, OMB A-123/130/130 Appendix III/108, 5 USC 552a, 44 USC 31, GLBA, PCI, SOX, HIPAA), Standard Operating Procedures, Policies, Analysis of Alternate Security Solutions (AoA) etc. Description of Role on Project: Lead/Manage SA&A program. Lead/Manage the preparation of a Government Accountability Office (GAO) audit. Manage the closure of POAMs in preparation of the Audit. Manage the ATO process of current systems. Review, Analyze & make recommendations based upon technical and administrative needs to mature the posture of the Cyber Security program. Performing oversight and manage the remediation of architecture design gaps of the Vulnerability Management Program to meet FISMA regulations. Support a client as a Sr. SME for assessment and authorization (A&A), including A&A efforts for various agency systems.

Maintain responsibility for supporting federal clients obtaining the authority to operate (ATO) for

new and modernized systems. Adhere to the NIST Risk Management Framework (RMF) to support the A&A process, including analyzing the development of supporting policies, procedures, and plans, designing and implementing security controls, testing and validating security controls, and analyzing and tracking corrective action plans. Ensure all supporting artifacts and results will be documented in the NIH System Assessment Tool (NSAT). Lead/Manage technical security engineering A&A support and implementation. Government risk and compliance tool (GRC Tool) Analysis. Integrating IT security architecture frameworks (DODAF, TOGAF, and Zachman). Lead FISMA/FedRAMP security control reports development. Identify security risks through the analysis of known information. Assess the Cybersecurity risk of IT systems documenting them in formal risk assessments and supporting artifacts associated with the Assessment and Authorization (A&A) process, including System Security Plans. Organize, develop, and present security briefings, written summaries, and written reports incorporating narrative, tabular and/or graphic elements on A&A activities. Manage the development of IT security solutions and assure successful implementation. Providing analysis of how the client currently employs and embeds Cybersecurity into its tools, design and development methodologies, and Application Programming Interface (API)/service driven architecture. Lead and manage IT security engineering support to cross-functional project teams to ensure that the clients' security policies, processes, procedures, and controls are adhered to, planned for, implemented throughout the project lifecycle Establish standard operating procedures for embedding Cybersecurity driven processes into the Software Development Life Cycle (SDLC). Analyze and recommend an integrated system security engineering process. Lead and Manage risk management framework support. Applying experience in NIST FIPS and SP 800 series to relevant documentations. Lead the assessment of current A&A processes to address both FISMA and FedRAMP control requirements and make recommendations for integration in current A&A process. Providing ongoing guidance regarding security impacts to design and architecture changes. Consult directly with the clients' project teams to provide security engineering expertise and observations and recommendations where appropriate. Provide support for multiple projects requiring ATO approval. Lead security Control

Assessment working group. Developed and Built Security Control Implementation and Inheritance Matrix tool (SCIM). Cyber Security Engineer Terp Techs LLC - Chantilly, VA January 2018 to May 2019 Relevant Skills: Cloud Security Auditing, Amazon Web Services (AWS) and Azure Cloud Computing Platforms, GRC Tools - NSAT/RV/eMASS, and Archer. STIGS, SRG, CIS benchmarks, Security A&A, NIST SP 800 series', DOD 8500, 8510, VA 6500, DHS 4300A, DOD SRG, DOD STIGS, DOD SCCA, FIPS, IRs', FISMA, FedRAMP, Standards and Guidelines, Laws and Regulatory Compliance (OMB M-04-04, HSPD-7, OMB A-123/130/130 Appendix III/108, 5 USC 552a, 44 USC 31, GLBA, PCI, SOX, HIPAA), Standard Operating Procedures, Policies, Analysis of Alternate Security Solutions (AoA), RMF - DODAF/TOGAF, Categorize Info. Systems, Security Impact Analysis, Select Sec Controls - SSP, Implement Sec Controls, Sec. Control Assessment - SCA, Security Assessment Report - SAR, Authorize Info System - POAM, and Monitor Sec Controls. Analysis/Auditing of Major/Minor Applications', RoB, ETA/ERA, ISA, MOU, MOA, PTA, PIA, SDD, DRP, SORN, BIA, IRP, CMP, ISCP, CIS Report/Worksheet, VSE, Incident Response, Tenable Nessus Security Center Analytics/Audits, FireEye HX, Microsoft Threat Modeling Tool, carbon Black, IBM App Scan Analytics/Audits, Check Point-Smart Endpoint Analytics/Audits, Splunk Analytics/Audits, IT Security System/App Waivers, Software Release Plan, JIRA, ESET Admin, Infoblox Grid Manager, Patch Management Audits, Cylance Admin, SharePoint Admin, IBM BigFix Analytics/Audits, Management of OWASP SAMM, Secure Code Review, Pen Test Results, Nessus Results, Database scan - POA&Ms, HP Fortify SCA, CVE, CCE, CVSS, etc. Description of Role on Project: Lead/Manage technical security engineering A&A support and implementation. Government risk and compliance tool (GRC Tool) Analysis. Integrating IT security architecture frameworks (DODAF, TOGAF, and Zachman). Lead FISMA/FedRAMP security control reports development. Identify security risks through the analysis of known information. Assess the Cybersecurity risk of IT systems documenting them in formal risk assessments and supporting artifacts associated with the Assessment and Authorization (A&A) process, including System Security Plans. Organize, develop, and present security briefings, written summaries, and written reports incorporating narrative, tabular and/or graphic elements on A&A activities. Manage the

development of IT security solutions and assure successful implementation. Providing analysis of how the client currently employs and embeds Cybersecurity into its tools, design and development methodologies, and Application Programming Interface (API)/service driven architecture. Lead and manage IT security engineering support to cross-functional project teams to ensure that the clients' security policies, processes, procedures, and controls are adhered to, planned for, implemented throughout the project lifecycle Establish standard operating procedures for embedding Cybersecurity driven processes into the Software Development Life Cycle (SDLC). Analyze and recommend an integrated system security engineering process. Risk management framework support. Applying experience in NIST FIPS and SP 800 series Assist in assessing current A&A process to address both FISMA and FedRAMP control requirements and make recommendations for integration in current A&A process. Providing ongoing guidance regarding security impacts to design and architecture changes. Work directly with the clients' project teams to provide security engineering expertise and observations and recommendations where appropriate. Provide support for multiple projects requiring ATO approval. Security Control Assessment working group. Security Control Implementation and Inheritance Matrix tool. IT Security Analyst (ISSO/A&A Cyber Security Expert) Fusion PPT - Vienna, VA November 2015 to November 2017 Relevant Skills: Vulnerability Remediation, Malware Analysis, Phishing & Ransomware Analytics (PhishMe Reporter), IDS/IPS Analysis, Enterprise Cyber Security and Information Assurance Analytics, Technical Writing, Configuration Management, Network & System Security, Agile, Scrum, USGCB, FDCC, Risk Management Framework, Vulnerability Assessments, Enterprise Network Access Control (NAC) ForeScout CounterACT, Security System Analytics, Regulatory Compliance, Work Instruction, Standard Operations Procedure, Policies, Analysis Of Alternate Security Solutions (AoA), System Integration Planning, Multitier Network Architectures, Cloud Security/Auditing, Amazon Web Services (AWS), Azure Cloud Computing Platform, Active Directory, Incident Response, Tenable Security Center Analytics/Audits, FireEye HX, carbon Black, IBM App Scan Analytics/Audits, Check Point-Smart Endpoint Analytics/Audits, Splunk Analytics/Audits, IT Security System/App Waivers, Software Release Plan, JIRA, ESET Admin, Infoblox Grid Manager, Patch

Management Audits, Cylance Admin, SharePoint Admin, IBM BigFix Analytics/Audits, Casper Admin, Absolute Computrace Admin, ServiceNow Admin, SA&A, NIST SPs', FIPS, IRs', FISMA, FEDRAMP, GLBA, PCI, SOX, HIPPA, 3FA Audits, RSA Token Audits, Zero Day and Advance Persistent Threat Analysis, Critical Information & Critical Information Infrastructure Analytics. Description of Role on Project: Security Analyst for the National Institutes of Health (NIH). Responsible for performing independent assessments of the information security posture of systems using applicable tools and procedures. Differentiate cyber threats and security operations. Analyze/Audit existing SA&A, AppScan, Tenable, and EOL/HRV Vulnerability Remediation's. Assist with compliance reviews and documentation for new and/or noncompliant systems, including FIPS-199 system categorizations, E-Authentication, Risk assessments for eligible systems, and records management requirements. Review vulnerability scans and develop a plan of action to assist in executing the vulnerabilities. Perform application and systems patching process related to App Scan and vulnerability scans. Assist with the audit plan, test, revise, and maintain monitoring and audit plan. Provide support for software developers, assist with Security Control integration and incorporation into the SDLC. Monitor and resolve Helpdesk tickets for all security-related incidents; coordinate and maintain incident response, coordinate to remediate vulnerabilities, misconfigurations, or other technical security controls within the organization. Assist with security authorizations for all systems in the portfolio. Assist with the assessment and selection of Security automation toolsets. Review security training and awareness. Developed Security Impact Analysis Advanced Repair Agent, Geek Squad/Best Buy Best Buy - Hanover, MD June 2014 to November 2015 Relevant Skills: Advance malware research/analysis, and removal from a broad spectrum of computer devices, system backup procedures, installation/remediation of software's and hardware's, to ensure nodes run at full specs. Remediate customer's denial of service (DOS) attacks, XSS, hacking/hijacking (Variety), ransomware, extortionware, clickjacking etc. As well as communicating software/hardware resolutions/best practices to customers. Description of Project: Advanced Repair Agent quickly and accurately diagnose technology issues and create robust solutions as needed at Precincts in Best Buy stores across the country. Identify and take

advantage of opportunities to improve the process of assessing, testing and repairing client electronics. They also help other employees understand how to successfully use the range of Geek Squad resources to meet client tech needs. Description of Role on Project: Demonstrating consistent team leadership skills while quickly and accurately diagnosing technological issues and creating robust solutions as needed. Identifying and taking advantage of opportunities to improve the process of assessing, testing and repairing client devices. Evaluating an array of new software tools for approval and usage within Geek Squad. Help Desk (Tier III) / IT Security Support University of Maryland University College September 2012 to June 2013 Relevant Skills: Provides incident resolution to customers with H/W, S/W and application problems via electronically submitted requests. Manages and monitors the agency's email domains for data loss prevention (DLP) policy enforcement; Manages the agency's Secure File sharing and collaboration systems; Manages and monitors the Enterprise Anti-Virus and Anti-Malware systems which include providing updates and monitoring activity; Works with G-Suite administration on mitigating cyber-attacks and SPAM; Documents incident status and solutions in incident database tools. Possesses current working knowledge of computers, printers, laptops and common windows applications. Works through various types Tier II troubleshooting. Provides answers to Frequently Asked Questions or solutions to common problems as part of a customer self-help capability. Description of Project: Configure and install hardware, software and drivers. Manages and monitors the agency's email domains for data loss prevention (DLP) policy enforcement; Manages the agency's Secure File sharing and collaboration systems; Manages and monitors the Enterprise Anti-Virus and Anti-Malware systems which include providing updates and monitoring activity; Works with G-Suite administration on mitigating cyber-attacks and SPAM; Monitor LAN/WAN and other networks for connectivity, managing components (managed gateways, cellular modems, switches, routers, etc.). Perform software upgrades as requested, managing both business standard and proprietary software. Address/resolve basic and complex incidents and requests; enter quality information into tickets and appropriately capture data; Complete follow-up and follow-through on all tickets. Manages all "Tier 2" escalation incidents and requests to ensure that work is completed to the

customers' satisfaction. Contributes to ensuring client self-help knowledge; documenting typical requests and incidents, resolutions, and work-around procedures. Identifies, evaluates, promotes, and implements customer support best practices. Mentors, supports, and cross-trains other service desk analysts. Uses creativity and innovation to automate and streamline processes and procedure. Description of Role on Project: Assists in the development and implementation of data access security measures by identifying, analyzing and resolving security and system problems relating to data access security, applications, programs and functions; Maintains the agency firewall which includes rule modification, updates and event log monitoring; Manages and monitors the agency's email domains for data loss prevention (DLP) policy enforcement; Manages the agency's Secure File sharing and collaboration systems; Manages and monitors the Enterprise Anti-Virus and Anti-Malware systems which include providing updates and monitoring activity; Works with G-Suite administration on mitigating cyber-attacks and SPAM; Analyzes security risks and develops an Incident Response Plan in the event of a data compromise; Identifies compromised machines and reports on security measures taken to address threats; Monitors the computer data network system for security threats and unauthorized users; Works with the Active Directory (AD) administration on AD policies related to security; Oversees and participates in phishing testing and training for staff; Provides periodic email and presentations to staff and districts on Cyber security trends; Runs and/or coordinates periodic vulnerability and penetration tests on the agency network; Prepares security status reports; may conduct periodic audits of various system users to determine user removal, transfer or limitation of access. Network Security Technician Integrated Design & Electronics Academy - Washington, DC September 2010 to December 2011 Relevant Skills: Monitoring of IT security devices to include firewalls, intrusion detection / prevention (IDS/IPS), data loss prevention (DLP), network access control (NAC), etc. Planning, deploying, and supporting network security devices Develop Change Management process Creation of technically detailed reports on firewall block lists, device status, change management, hardware/software upgrades, and other areas Assist in the analytics and evaluation of network and systems activity Assist in troubleshooting and problem solving a wide variety of

client issues Consult with internal and external partners on execution of firewall and security best practices Recommend and implement improvements for preventive maintenance on an on-going basis Maintain and update relevant system and process documentation and develop ad-hoc reporting as needed Enforce and follow firewall standards and policies Configure, deploy, and maintain firewall infrastructure (ASA, Palo Alto, etc.) Respond to Tier 2 customer support issues via ticket, chat, or phone Liaise with Customer Support Technicians (CSTs) and Engineering to provide support for projects and customers as needed Description of Project: Experience working with information technology infrastructure. Knowledge in the following technologies: Firewalls, Data Loss Prevention, VPN, Intrusion Detection/Prevention, Network Scanning and Compliance, Network Access control, and Advanced Persistent Threat Prevention. Experience in performing infrastructure support at an enterprise level. Ability to demonstrate knowledge of computer security concepts. Overall IT work experience is required. Must have the ability to communicate, analyze and troubleshoot issues. Oral and written communication skills, including the ability to interact with engineers, vendors, peers, customer support technicians, and customers. Experience in Internet networking subject matter TCP/IP, Layer 2, Layer 3, Firewalls, etc. Description of Role on Project: Experience working with information technology infrastructure. Knowledge in the following technologies: Firewalls, Data Loss Prevention, VPN, Intrusion Detection/Prevention, Network Scanning and Compliance, Network Access control, and Advanced Persistent Threat Prevention. Experience in performing infrastructure support at an enterprise level. Ability to demonstrate knowledge of computer security concepts. Assist in the analytics and evaluation of network and systems activity Assist in troubleshooting and problem solving a wide variety of client issues Consult with internal and external partners on execution of firewall and security best practices Recommend and implement improvements for preventive maintenance on an on-going basis Maintain and update relevant system and process documentation and develop ad-hoc reporting as needed Enforce and follow firewall standards and policies Configure, deploy, and maintain firewall infrastructure (ASA, Palo Alto, etc.) Respond to Tier 2 customer support issues via ticket, chat, or phone Liaise with Customer Support Technicians (CSTs) and

Engineering to provide support for projects and customers as needed Education Bachelor of Science in Cyber Security/Information Assurance University of Maryland University College 2014 Skills Cyber Security, Cissp, Nist, Information Security, Siem, It Security, Information Assurance, Comptia, Cybersecurity, Network Security

Name: Dana Thompson

Email: alewis@example.org

Phone: 374-482-4207