

Sr. Cyber - Cloud, Network & Data Sr. Cyber - Cloud, Network & Data Sr. DevOps, Network & Data
Threat Security Engineer - U.S. Securities and Exchange Commission-OIT-SEC Washington, DC
Available only in Maryland, Washington D.C. or 100% Remote. No other areas will be considered!
I'm looking for Sr Cyber Security, Data Security and Cloud Engineer/Architect or Devop
engagements. Altogether, 40+ years of IT Experience. With 20 years IT Security Advanced Threat
and Vulnerability Engineering/Architecture, 35 years of Database and Enterprise Application
design, development, coding, testing and implementation. 25 years of Cyber Security Threat and
Vulnerability Analysis. Work Experience Sr. Cyber - Cloud, Network & Data U.S. Securities and
Exchange Commission-OIT-SEC August 2016 to Present Aug 2016 - Present. Tasks and projects:
AWS SEC-C3 Cloud Security design, development, testing and implementation of SEC
Micro-Services as well as Red Shift and Neptune binomial security prediction analysis.. Provided
solutions using MS Azure PaaS services such as SQL Server, HDInsight, service bus. Azure SEC
Cloud implementation and security hardening. Coordinating Imperva, Skybox, Varonis and Tenable
Threat/Vulnerability scanning. Skybox Infrastructure Threat and vulnerability analysis and
remediation. As well as providing Python scripts for network workarounds. Imperva SecureSphere
Threat and vulnerability analysis, Security Assessments and remediation via MXs and GWs.
Implement Splunk to the SOC and Analyze AWS Log traffic for Skybox 9.0.5 Build and Configure
SNMP Traps Rules and Polling to the NOC Implemented Imperva, Skybox, Varonis, AWS Services
and CyberArk using Ansible Playbooks Perform Network analysis and remediation using Lua
scripts, configuration and WireShark Analysis Provide DLP-DCF-Filewalks, Insider and Cyber
Threat Analysis via Varonis and DatAdvantage Provide Skybox Network, Firewall, Threat and
Vulnerability remediation with Horizon Network Visualization for Cisco ASA, 3000, 6000, Switches,
Routers, Firewalls and Gateways. As well as Python network interface scripts. Provide constant
discovery, configuration and remediation to CyberArk Vaults/safes and perform security behavior
analysis using PTA Maintain SSLKey Certs and Security analysis tools with upgrades, patches and
diagnostics. And code test and implement Python and Java/Javascript workarounds. Provide
Skybox Threat and Vulnerability Analysis. As well as Network and Firewall, Router, Switch and

Gateway, Threat and Vulnerability analysis. Provide Splunk Cloud Security and Data analysis. Perform Tenable, Tenable.io and Nessus Security Assessment scans throughout the SEC Design, code, test and Implement Security AI and Machine Learning behavior analysis using Anaconda Orange Tools and Python. As well as build symmetric analysis with PERL Provide EDGAR BigInsights support and analysis using Azure Tools and Services Generate MVC Quick Designs using Ruby on Rails as well as script ruby to address network issues. Performed POA&M policy & rule design, remediation and compliance checks against NIST SP 800-53, STIG, CIS recommendations. Designed and developed SOPs and software/hardware baselines which were appended into organization Information Security Controls. Estimated LOE and time/cost projections for current project. Configured, tested and performed SEC threat and vulnerability analysis with a10 Galaxy-Thunder, Panorama-Palo Alto. Configured, tested and implemented Cyberark privileging with PUU and manually connecting endpoints. Designed, coded, tested and implemented Skybox to Splunk tail - f logs using Python 2.7 scripts. As well installed, configured and tested Universal Forwarders with load balancing and compression for multi-syslog servers. And, fleshed out Splunk Enterprise Dashboards with AWS, Azure Activity, Audit and User data. Designed, coded, tested and implemented FINRA AWS Snowball Security Data feeds to SEC Data Science Workstations (DSW).

Performed Fireeye-Helix advanced threat protection analysis as well as detailed Notification-Escalation hierarchies for key decision binding. Programming Languages used to design, develop, code, test and implement: C++ Python, IPython Java and Javascript Lua Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting Spark and R YAML Operating and Cloud Systems: Amazon Commercial and Gov-Cloud, Azure, Google Analytics AWS Linux, RedHat, Centos, Cisco-IOS, NX-OS, Windows10, Mac-OS X, Cisco-IOS MS Azure PaaS Threat and Vulnerability Analysis Tools: Skybox Infrastructure Threat and vulnerability analysis of Router, Switch, Firewall, WAF, and Gateways Nmap and WireShark - Router, Switch, Firewall and Gateway analysis Imperva SecureSphere Threat Radar & Risk Analyzer Tenable, Tenable.io and Nessus Varonis Insider and Cyber Threat Analysis CyberArk PAS, PTA, PSM AWS Inspector, Trusted Advisor, Config-Explorer Splunk Behavior Analysis IBM BigInsights EDGAR behavioristic analysis

FireEye HX-Mail, Endpoints and Analysis Security AI & Machine Learning Tools: Anaconda Orange Python Feature isolation and analysis Security PCA, Kmean, Monte-Carlo and Markov-Chaining Analysis Privilege and Access Management Tools: Varonis, CyberArk, IAM Data Security and Data Tools: Imperva SecureSphere V13.5 Red-Shift Big Data Parquet Big Data BigInsights Oracle 12c, MSSQL, MySQL, MariaDB, Postgress, Netezza, MongoDB ERwin, RapidSQL, MySQL WorkBench, Toad Tableau Data Analyzer Baseline and Compliance Management: Archer-POA&M AWS-Baselines, Oracle-Baselines, MSSQL-Baselines, Sybase-ASE & IQ Baselines, MariaDB-Baselines, Postgress-Baselines, Netezza-Baselines, MongoDB-Baselines AaaS, IaaS, PaaS, SaaS: EDGAR-AaaS, SRO-AaaS & IaaS, SRO-PaaS, SEC-OIT-SaaS Sr DevOps, Network and Data Threat Detection Security Engineer U.S. Dept of Labor January 2015 to August 2016 Employment and Training Administration (DOLETA) - Jan 2015 to Aug 2016. Tasks and projects: AWS-DOL Cloud Security design, development, testing and implementation. Provided solutions using MS Azure PaaS services such as SQL Server, HDInsight, service bus. Skybox Infrastructure Threat and vulnerability analysis and remediation. Imperva SecureSphere Threat and vulnerability analysis, Security Assessments and remediation via MXs and GWs. Implement Splunk to Analyze AWS Log traffic Implement Elastic-Search, Logstash and Kibana Security Cloud Console Perform Network analysis and remediation using scripts, configuration and WireShark Analysis Maintain SSLKey Certs and Security analysis tools with upgrades, patches and diagnostics. And code test and implement Python and Java/Javascript workarounds. Perform Tenable, Tenable.io and Nessus Security Assessment scans throughout the DOL and its subagencies Design, code, test and Implement Security AI and Machine Learning behavior analysis using Anaconda Orange Tools and Python. As well as build symmetric analysis with PERL Provide BigInsights support and MasterDB analysis using Azure Tools and Services Provide Cloud Cost Models and Budgeting for Cloud Implementations through DOL and its subagencies. Generate MVC Quick Designs using Ruby on Rails as well as script ruby to address network issues. Performed POA&M policy & rule design, remediation and compliance checks against NIST SP 800-53, STIG, CIS recommendations. Designed and developed SOPs and software/hardware

baselines which were appended into organization Information Security Controls. Estimated LOE and time/cost projections for current project. Programming Languages used to design, develop, code, test and implement: C++ Python, IPython Java and Javascript Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting Spark & R Operating and Cloud Systems: Amazon Commercial and Gov-Cloud, Azure, Google Analytics AWS Linux, RedHat, Centos, Cisco-IOS, NX-OS, Windows8, Mac-OS X MS Azure PaaS Threat and Vulnerability Analysis Tools: Nmap and WireShark - Router, Switch, Firewall and Gateway analysis Tenable, Tenable.io and Nessus AWS Inspector, Trusted Advisor, Config-Explorer Splunk Behavior Analysis IBM BigInsights & Tableau Trade data behavioristic analysis Security AI & Machine Learning Tools: Anaconda Orange Python Feature isolation and analysis Security PCA, Kmean, Monte-Carlo and Markov-Chaining Analysis Privilege and Access Management Tools: IAM Data Security and Data Tools: Imperva SecureSphere V5 Red-Shift Big Data Parquet Big Data BigInsights Oracle 12c, MSSQL, MySQL, MariaDB, Postgress, Netezza, MongoDB ERwin, RapidSQL, MySQL WorkBench, Toad Tableau Baseline and Compliance Management: Archer-POA&M AWS-Baselines, Oracle-Baselines, MSSQL-Baselines, Postgress-Baselines, Netezza-Baselines, MongoDB-Baselines AaaS, IaaS, PaaS, SaaS: Trade-AaaS, OSHA-AaaS & IaaS, SRO-PaaS, SEC-OIT-SaaS Sr. Python IaaS-PaaS-SaaS - Cloud Cyber Security and Big Data Architect AT&T Research & Development Center - Annapolis, MD February 2013 to December 2014 02/15/2013 - 12/14/2014. Tasks and projects: AT&T Cloud Security design, development, testing and implementation. Skybox Infrastructure Threat and vulnerability analysis and remediation. Guardium Threat and vulnerability analysis, Security Assessments and remediation via MXs and GWs. Implement Splunk to Analyze AWS, OpenStack Log traffic Implement Elastic-Search, Logstash and Kibana Security Cloud Console Perform Network analysis and remediation using scripts, configuration and WireShark Analysis Maintain SSLKey Certs and Security analysis tools with upgrades, patches and diagnostics. And code test and implement Python and Java/Javascript workarounds. Nessus Security Assessment scans throughout the AT&T and its child corps Design, code, test and Implement Security AI and Machine Learning behavior analysis using Anaconda

Orange Tools and Python. As well as build symmetric analysis with PERL Provide Cloud Cost Models and Budgeting for Cloud Implementations through DOL and its subagencies. Generate MVC Quick Designs using Ruby on Rails and Spark/R as well as script ruby to address network issues. Programming Languages used to design, develop, code, test and implement: C++ Python, IPython Java and Javascript Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting Spark & R Operating and Cloud Systems: Amazon Commercial and Gov-Cloud, Azure, Google Analytics AWS Linux, RedHat, Centos, Cisco-IOS, NX-OS, Windows7, Mac-OS X Threat and Vulnerability Analysis Tools: Nmap and Wireshark - Router, Switch, Firewall and Gateway analysis Nessus AWS Inspector, Config-Explorer Splunk Behavior Analysis Tableau data visualization and behavioristic analysis Security AI & Machine Learning Tools: Anaconda Orange Python Feature isolation and analysis Security PCA, Kmean, Monte-Carlo and Markov-Chaining Analysis Privilege and Access Management Tools: IAM Data Security and Data Tools: Parquet Big Data BigInsights Riak, MSSQL, MySQL, PostgreSQL, MongoDB ERwin, RapidSQL, MySQL WorkBench, Toad Tableau Baseline and Compliance Management: AWS-Baselines, PostgreSQL-Baselines, Netezza-Baselines, MongoDB-Baselines, Riak-Baselines AaaS, IaaS, PaaS, SaaS: AT&T-AaaS, BabyBell-AaaS & IaaS, -PaaS, AT&T-SaaS Threat and Vulnerability Python Cyber Security Architect Centers for Medicare and Medicaid Services August 2011 to February 2013 Tasks and projects: Beneficiaries Cloud Security design, development, testing and implementation. Guardium Threat and vulnerability analysis, Security Assessments and remediation via MXs and GWs. Implement Splunk to Analyze AWS, OpenStack Log traffic Implement Elastic-Search, Logstash and Kibana Security Cloud Console Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis Maintain SSLKey Certs and Security analysis tools with upgrades, patches and diagnostics. And code test and implement Python and Java/Javascript workarounds. Nessus Security Assessment scans throughout the CMS Design, code, test and Implement Security AI and Machine Learning behavior analysis using Python and PySci. As well as build symmetric analysis with PERL Provide Cloud Cost Models and Budgeting for Cloud Implementations throughout CMS and its subagencies. Generate MVC Quick Designs using Ruby

on Rails and Spark/R as well as script ruby to address network issues. Performed POA&M policy & rule design, remediation and compliance checks against NIST SP 800-53, STIG, CIS recommendations. Designed and developed SOPs and software/hardware baselines which were appended into organization Information Security Controls. Estimated LOE and time/cost projections for current project. Programming Languages used to design, develop, code, test and implement: C++ Python, IPython Java and Javascript Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting Spark & R Operating and Cloud Systems: Amazon Commercial and Gov-Cloud AWS Linux, RedHat, Centos, Cisco-IOS, NX-OS, Windows, Mac-OS X Threat and Vulnerability Analysis Tools: Nmap and Ethereal - Router, Switch, Firewall and Gateway analysis Nessus Config-Explorer Splunk Behavior Analysis Security AI & Machine Learning Tools: Python w/AI and ML Libs Feature isolation and analysis Security PCA, Kmean, Monte-Carlo and Markov-Chaining Analysis Privilege and Access Management Tools: IAM Data Security and Data Tools: Parquet Big Data Riak, MSSQL, MySQL, Postgress, MongoDB ERwin, Toad Baseline and Compliance Management: AWS-Baselines, Postgress-Baselines, MongoDB-Baselines, Riak-Baselines AaaS, IaaS, PaaS, SaaS: CMS-AaaS, BabyBell-AaaS & IaaS, -PaaS, CMS-SaaS Sr. Medical-Mobile & Investment/Real Estate Python Architect/ Developer P.E. Inc February 2010 to August 2011 Evenings/Weekend Projects Tasks and projects: MSL Listing Service using Drupal & PHP Modules. Design, develop, code, test and implement Tablet Patient Chart System Programming Languages used to design, develop, code, test and implement: Python, IPython Java and Javascript Bash, PowerShell, VBA and AWK & SED Scripting Object-C C++ Operating and Cloud Systems: RedHat, Centos, Windows, Mac-OS X & IOS Threat and Vulnerability Analysis Tools: Nmap and Ethereal network analysis Security AI & Machine Learning Tools: Python w/AI and ML Libs Feature isolation and analysis Security PCA, Kmean, Monte-Carlo and Markov-Chaining Analysis Data Security and Data Tools: Parquet Big Data MySQL & MongoDB ERwin, Toad Baseline and Compliance Management: MongoDB-Baselines IT Python Cyber Security Information Assurance Subject Matter Expert (SME), 04-2010-08-2011 - The Administrative Office of the United States Courts Tasks and projects: OpenStack - Prisoner Financial Care Cloud Security

design, development, testing and implementation. Keystone Threat and vulnerability analysis, Security Assessments and remediation via MXs and GWs. PERL Log Analyzer Scripts for OpenStack Log traffic Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis Design, code, test and implement security symmetric analysis with PERL Generate MVC Quick Designs using Ruby on Rails script ruby to provide courts with 3-tiered data access and analysis. Programming Languages used to design, develop, code, test and implement: Python, IPython C++ Java and Javascript Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting Operating and Cloud Systems: OpenStack RedHat, Centos, Windows, Mac-OS X Threat and Vulnerability Analysis Tools: Nmap and Ethereal - Router, Switch, Firewall and Gateway analysis Security AI & Machine Learning Tools: Python w/AI and ML Libs Feature isolation and analysis Security PCA, Kmean, Monte-Carlo and Markov-Chaining Analysis Privilege and Access Management Tools: OIM, OAM Data Security and Data Tools: Parque Big Data Oracle 9 & 10g ERwin, Toad C&A Lead-Tech Department of Education - FSA - Washington, DC August 2009 to April 2010 Tasks and projects: Guardium Threat and vulnerability analysis, Security Assessments and remediation via MXs and GWs. Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis Generate MVC Quick Designs using Ruby on Rails and Spark/R as well as script ruby to address network issues. Programming Languages used to design, develop, code, test and implement: Python, IPython Java and Javascript Perl Ruby C++ Bash, PowerShell, VBA and AWK & SED Scripting Spark & R Operating and Cloud Systems: OpenStack Ubuntu, Centos, Windows, Mac-OS X Threat and Vulnerability Analysis Tools: Nmap and Ethereal - Router, Switch, Firewall and Gateway analysis Config-Explorer Privilege and Access Management Tools: OIM, OAM Data Security and Data Tools: Parque Big Data Oracle, MySQL, MongoDB Toad SR. Security Python Engineer AT&T Research & Development Center - Annapolis, MD December 2006 to January 2009 Tasks and projects: Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis Maintain SSLKey Certs and Security analysis tools with upgrades, patches and diagnostics. And code test and implement Python and Java/Javascript workarounds. Design, code, test and Implement Security AI and Machine Learning

behavior analysis using Python and ML Libs. As well as build symmetric analysis with PERL
Generate MVC Quick Designs using Ruby on Rails for data access and analysis
Programming Languages used to design, develop, code, test and implement: Python Java and Javascript Perl
C++ Ruby Bash, PowerShell, VBA and AWK & SED Scripting
Operating and Cloud Systems: RedHat, Ubuntu, Windows, Mac-OS X
Threat and Vulnerability Analysis Tools: Nmap and Ethereal
- Router, Switch, Firewall and Gateway analysis
Privilege and Access Management Tools: OAM, OIM
Data Security and Data Tools: MySQL, Postgress ERwin, Toad SR. Python Cyber Security
Architect Fannie - Mae, WA February 2006 to December 2006 DC
Tasks and projects: Desgin, develop, code, test and Implement Mortgage Servicing and Traunce Analysis
Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis
Design, code, test and Implement Security AI and Machine Learning behavior analysis using Python and ML Libs for
Traunce KPMIs. As well as build symmetric analysis with PERL
Generate MVC Quick Designs using Ruby on Rails for data access and analysis
Programming Languages used to design, develop, code, test and implement: Python Java and Javascript Perl Ruby C++ Bash, PowerShell, VBA and AWK & SED Scripting
Operating and Cloud Systems: RedHat, Ubuntu, Windows, Mac-OS X
Threat and Vulnerability Analysis Tools: Nmap and Ethereal - Router, Switch, Firewall and Gateway analysis
Data Security and Data Tools: MySQL, Postgress ERwin, Toad Sr. Python Security Architect CSB-FSA - Germantown, MD April 2004 to February 2006
Tasks and projects: Desgin, develop, code, test and Student Loan Sallie Mae Defaults Analyzer System
Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis
Design, code, test and Implement Security AI and Machine Learning behavior analysis using Python and ML Libs for Student Default Prediction and Recommender Model Analyzer System. As well as
build symmetric analysis with PERL
Generate MVC Quick Designs using Ruby on Rails for data access and analysis
Analyze, design, develop, code, test and implement C++ Exploit Workarounds
Programming Languages used to design, develop, code, test and implement: Python Java and Javascript Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting C & C++
Operating and Cloud Systems: RedHat, Windows, Mac-OS X
Threat and Vulnerability Analysis Tools: Nmap and

Ethereal - Router, Switch, Firewall and Gateway analysis Data Security and Data Tools: MySQL, Postgress, Oracle 8i ERwin, Toad SR. SECURITY ARCHITECT BNL Inc - Frederick, MD November 2000 to April 2004 Tasks and projects: Desgin, develop, code, test and XSLT Year-2000 conversion system Perform Network analysis and remediation using scripts, configuration and Ethereal Analysis Generate MVC Quick Designs using Ruby on Rails for data access and analysis Analyze, design, develop, code, test and implement C++ Exploit Workarounds Programming Languages used to design, develop, code, test and implement: Python Java and Javascript Perl Ruby Bash, PowerShell, VBA and AWK & SED Scripting C & C++ XSLT & XDocs Operating and Cloud Systems: RedHat, Windows, Mac-OS X Threat and Vulnerability Analysis Tools: Nmap and Ethereal - Router, Switch, Firewall and Gateway analysis Data Security and Data Tools: Ingress, Oracle 6 Toad SR. SECURITY -Internet and Data Architect Chase Insurance Group - Chase Manhattan Bank - New York, NY August 1999 to November 2000 DE & NY Tasks and projects: Black-Card Credit Fraud Analyzer System Desgin, develop, code, test and XSLT Year-2000 conversion system Perform Network analysis and remediation using scripts, configuration using PERL Scripts Analyze, design, develop, code, test and implement C++ Exploit Workarounds Programming Languages used to design, develop, code, test and implement: Python Java and Javascript Perl Bash, Bison, Lex, AWK & SED Scripting C & C++ Operating and Cloud Systems: MACH Unix TAL, Windows, Mac-OS Threat and Vulnerability Analysis Tools: Nmap and Ethereal - Router, Switch, Firewall and Gateway analysis Data Security and Data Tools: Ingress, Oracle Toad SR. ENTERPRISE ARCHITECT Establish Compaq Services - Greenbelt, MD February 1997 to August 1999 MD Tasks and projects: Establish Compaq Services via dGov Program Perform Network analysis and remediation using scripts, configuration using PERL Scripts Analyze, design, develop, code, test and implement C++ Exploit Workarounds Programming Languages used to design, develop, code, test and implement: Python Perl Bash, Bison, Lex, AWK & SED Scripting C & C++ Operating and Cloud Systems: Windows, Mac-OS Data Security and Data Tools: Ingress, Sybase SR. Technical Sales Support MCI - Springfield, VA January 1995 to February 1997 Tasks and projects: Provide Technical Sales Support for MCI ISDN and Long Line implementations

Perform Network analysis and remediation using scripts, configuration using PERL Scripts Analyze, design, develop, code, test and implement C++ Exploit Workarounds Programming Languages used to design, develop, code, test and implement: Python Perl Bash, Bison, Lex, AWK & SED Scripting C & C++ Operating and Cloud Systems: Windows95, Mac-OS Data Security and Data Tools: Ingress, Sybase Sr. Vax Systems Engineer Greenbelt, MD June 1993 to January 1995 Tasks and projects: Database Administrator for multiple databases - Oracle on Vax/VMS DBASE IV, Foxpro, Rbase Perform Network analysis and remediation using scripts, configuration using PERL Scripts Analyze, design, develop, code, test and implement C++ Exploit Workarounds Programming Languages used to design, develop, code, test and implement: Python Perl Bash, Bison, Lex, AWK & SED Scripting C & C++ SQL Operating and Cloud Systems: VAX-VMS, AIX Data Security and Data Tools: Oracle, Dbase IV, Foxpro, Rbase, Ingress, Sybase *** Further background of the last 20+ years can be supplied Education Criminal Forensic Psychology Massachusetts Institute of Technology (MIT) OCW 2017

Name: Maria Young

Email: santiagostephanie@example.com

Phone: 2454494553