SME Active Cyber Defense Analyst Cyber Threat Intelligence SME Active Cyber Defense Analyst Cyber Threat Intelligence SME Active Cyber Defense Analyst Cyber Threat Intelligence - United States Census Bureau Baltimore, MD Work Experience SME Active Cyber Defense Analyst Cyber Threat Intelligence United States Census Bureau - Greenbelt, MD June 2017 to Present Contractor) - Cyber Defense Elite Enforcement, Inc Splunk data and log analytics using Regex to pull, sort, parse analyze, and manage data logs. Create custom Python scripts to automate Cyber Security and Network processes. Identify and triage IOC (Indicators of Compromise) by analyzing Splunk, WAF, Firewall, Netflow, Syslog, Email, and IDS/IPS logs. Managed OSINT and Security Engineering platforms Suricata IDS/IPS, Security Onion, PFsense, Nmap etc. Engage with Netapp tool to ensure data encryption and storage across FCoE storage system. Act as an SME to the 24/7/365 CSIRT SOC by actively monitoring and responding to Cyber & Threat Intelligence related incidents based on the Cyber Kill Chain, Diamond Model of Intrusion Research OSINT and cutting-edge vulnerabilities, threats, tactics, techniques and procedures (TTPs) related to APTs and threats to the Big Data, Cloud, Financial and Government sectors. Create & Coordinate Security Change Requests for each Release. Perform Threat intel hunting and Malware analysis using Cuckoo Sandbox, Virus Total, Hybrid Analysis, Maltego, DomainTools, and OSINT. Cross reference internal logs with existing and emerging Cyber and Threat intelligence. Using the intelligence cycle, disseminate findings amongst the Security team, contract stakeholders (Managers, PMs, Directors, VPs, CIO) and government leaders day-to-day. Use Python Scripts, GREP commands, REGEX, and BASH LINUX commands to parse DNS, FIREWALL, EMAIL, PROXY GATEWAY, WEB, IDS/IPS, ENDPOINT PROTECTION, & SERVER logs for alerts and for analysis of incidents. Use some tools to aid in analysis; QRadar and ArcSight SIEM, Symantec Endpoint Protection AV, Sourcefire- SNORT IDS, RSA Security Analytics- Netwitness, IBM Bluemix, Wireshark, Palo Alto and ASA firewalls, AWS cloud services, Virus Total, Softlayer etc. Utilize Threat Intelligence Platforms to analyze threat data from multiple sources in real time Create SOPs/Operations Procedure with Use and test cases for the US Census SOC and SME for POAMs and updated NIST Standards. Run Cyber Security budget analysis and project delivery for US

Census Contract. Monitor network ingress and egress traffic through Solarwinds and collect network data through Moloch. Perform Red team/Blue team/Purple team, Threat hunting, Incident Response and Administrative Security functions. IE. (Manual and Automated Penetration Tests, forensics, Analytics, Hunting, Policy updates, Signature writing and IR) Using Kali Linux Suite of tools and CyberArk. Use OWASP and MITRE (TARA) Threat Rating Methodologies to run Risk/Threat assessments on various Business and Governmental assets Sr. Security Analyst Sr. Cyber Intelligence Internal Revenue Service IRS - Lanham, MD April 2015 to June 2017 Contractor)- General Dynamics IT Raw data and log analytics using UNIX command line to pull, sort, parse, and manage data logs. Document findings for Proof of Concept, follow industry standards like Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM), and National Institute of Standards and Technology (NIST). Splunk data and log analytics using UNIX command line to pull, sort, parse, and manage data logs. Create custom Python scripts to automate Cyber Security and Network processes. Identify and triage IOC (Indicators of Compromise) by analyzing Splunk, WAF, Firewall, Netflow, Syslog, Email, and IDS/IPS logs. Use Netapp Hybrid SAN to back up encrypted data to the cloud. Work on a 24/7/365 CSIRT SOC by reactively monitoring and responding to Cyber & Threat Intelligence related incidents based on the Cyber Kill Chain, Diamond Model of Intrusion. Utilize Threat Intelligence Platforms to analyze threat data from multiple sources in real time Research OSINT and cutting-edge vulnerabilities, threats, tactics, techniques and procedures (TTPs) related to APTs and threats to the Big Data, Cloud, Tax/Financial and Government sectors. Create & Coordinate Security Change Requests for each Release. Perform Threat intel and Malware analysis using Cuckoo Sandbox, Virus Total, Hybrid Analysis, Maltego, DomainTools, and OSINT. Examine the flow of network traffic and data through Solarwinds. Create and manage Sourcefire, Snort and Bro IDS/IPS rules. Troubleshoot technical issues with Sourcefire and all of its components (CLIsh, Back-end Database, FireSIGHT, FirePOWER, FireAMP, DC/Defense Center, 3D System, Licensing, eStreamer, LDAP, Policy, Networking/Architecture, Sensors and Appliances). Cross reference internal logs with existing and emerging Cyber and Threat intelligence. Using the intelligence cycle, disseminate findings amongst the Security team, contract stakeholders (Managers, PMs, Directors, VPs, CIO) and government leaders day-to-day. Use EnCase 7 to perform network Intrusion case forensics and analysis. Use Scripts and LINUX commands to parse DNS, FIREWALL, EMAIL, PROXY GATEWAY, IBM Bluemix, WEB, IDS/IPS, ENDPOINT PROTECTION, & SERVER logs for alerts and for analysis of incidents. Use some tools to aid in analysis; QRadar and ArcSight SIEM, Symantec Endpoint Protection AV, Sourcefire- SNORT IDS, RSA Security Analytics- Netwitness, Wireshark, Palo Alto and ASA firewalls, Virus Total, etc. Vulnerability Assessing, Web app Pentesting, and Network Pentesting. (Cobalt Strike, CyberArk, Burp Suite, Nessus Kali Linux, Metasploit) Use IRS proprietary ticketing and documentation systems to track and manage high-level and low-level cases and escalations. Regular Expressions, Parsing, Scripting (BASH and Python) and Network/Web-App penetration testing as well as Automated and Manual Tests using Kali Linux 2 suite and Core Impact. Use Core Impact to run Network, Client-Side, and Web Application Penetration Tests on targeted systems Perform security scans and tests for development projects that would include security design reviews and blackbox/graybox Security assessments and Penetration Tests. Specifically performed Network, Client-Side, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Penetration tests using BurpSuite, OWASP ZAP, and Fiddler. Use Kali linux, Metasploit, Nmap, AirCrack-ng, Nessus, Nikto, and Hydra to perform Reccon, Enumeration, and Network based attacks and exploitations. Used Exploit-DB and NVD to stay up on latest exploit packs. Used open source technologies to conduct research for improvement upon the client's security postures. Sr. Security Architect Lead Engineer/Penetration Tester Prometric - Canton, MD May 2013 to April 2015 Architect, Engineer, and fully develop and manage QRadar SIEM from the ground up. Import ALL Log Sources, Logs, email groups, Access Controls, and License for IBM QRadar, configure the XGS remote syslog to send events to QRadar from the SiteProtector Console and Local Management Interface. Map high-level security, and privacy needs into requirements Enforce security standards into existing code in accordance with the SDLC- (Software Development Life Cycle) Framework and run automated code review and mitigation through Fortify DAST. Also used Fortify

Static Code Analyzer to conduct Static Code analysis and provided PoC - Proof of Concept code reports. Run Cyber Security budget analysis and project delivery for Prometric. Implementation and enforcement of Credential Guard and Device Guard. Review and approve ACL / firewall change requests for ASAs, Palo Alto, and Junipers. Use Splunk and QRadar SIEM systems for Big Data parsing and investigating incidents and log correlation. Create and manage Sourcefire, Snort and Bro IDS/IPS rules. Troubleshoot technical issues with Sourcefire and all of its components (CLIsh, Back-end Database, FireSIGHT, FirePOWER, FireAMP, DC/Defense Center, 3D System, Licensing, eStreamer, LDAP, Policy, Networking/Architecture, Sensors and Appliances). Use Knife command line tool to create, modify, and update Cookbooks (Chef Config Files) to update Chef servers with system patches and updates. Review and monitor applications for security leaks. Perform security scans and tests for development projects that would include security design reviews and blackbox/graybox Security assessments and Penetration Tests. Specifically performed Network, Client-Side, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Penetration tests using BurpSuite, CyberArk, OWASP ZAP, and Fiddler. Use Kali linux, Metasploit, Nmap, AirCrack-ng, Nessus, Nikto, and Hydra to perform Reccon, Enumeration, and Network based attacks and exploitations. Used NVD, CWE and Exploit-DB to stay up on latest software weaknesses and exploit packs. Use a CVSS Scoring system to identify CVEs (Common Vulnerabilities and Exposures) and CMSS (Common Misuse Scoring System) base, temporal, and environmental metrics. Configure, Engineer, Architect and maintain various security devices and software such as Netapp for Hybrid data storage, Cisco ASA and Juniper Firewalls, Solarwinds Network Analyzer, Trustwave Security Testing, Blue Coat Proxy and Snort for IDS/IPS. Work in a Unix/Linux and Windows environment behind Kernel Shell and Powershell. Configure and maintain various cloud, network and client-based security products including, SIEM, Anti-virus, IBM Bluemix, Amazon AWS, IDS and DLP Code in Python and BASH for process automation and demonstrate proof-of-concept exploits of identified vulnerabilities that will be utilized for future builds and standards. Schedule and coordinate activities with our Stakeholders, Software Development teams, Project Managers, Lead Engineers and Managers in planning, execution, and mitigation of identified Vulnerabilities. Work with the legal team to support various industry standard compliance initiatives critical to the organization's information privacy. Develop and support the best practice methodology for policy assessment and security awareness training to IT application developers. Maintain PCI-DSS and FISMA compliance throughout various systems and networks. Conduct risk- assessments on said systems and networks. Perform web-application and network Penetration tests for QC and Production. Sr. Security Engineer Cisco Systems - Columbia, MD August 2011 to May 2013 Continuously monitors levels of service as well as interprets and prioritizes threats through use of intrusion detection systems, firewalls and other boundary protection devices, and any security incident management products deployed. Work on a 24/7/365 CSIRT SOC by reactively monitoring and responding to Cyber & Threat Intelligence related incidents based on the Cyber Kill Chain, Diamond Model of Intrusion. Work in a Unix/Linux and Windows environment behind Kernel Shell and Powershell. Did Regular Expressions, Parsing, Scripting (BASH and Python) maintain, and Engineer QRadar and Splunk SIEM systems. Licensing, access, log aggregation and Dash boards/ Pages, configure the XGS remote syslog to send events to QRadar from the SiteProtector Console and Local Management Interface. Use QRadar and Splunk for Big Data parsing and investigating incidents and log correlation. Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Ensures the integrity and protection of networks, systems, and applications by technical Enforcement of organizational security policies, through monitoring of vulnerability scanning Create and manage Sourcefire, Snort and Bro IDS/IPS rules. Troubleshoot technical issues with Sourcefire and all of its components (CLIsh, Back-end Database, FireSIGHT, FirePOWER, FireAMP, DC/Defense Center, 3D System, Licensing, eStreamer, LDAP, Policy, Networking/Architecture, Sensors and Appliances). Monitors and proactively mitigates information security risks. Work within a 24/7 shift-scheduled security operations environment Network Engineer Security Consultant Digit All City - Baltimore, MD June 2009 to August 2011 Setup LAN networks connect them to WANs and MANs using Cisco routers and Switches/hubs for setup of new computer labs. Use protocols OSPF, BGP, EIGRP, IPSEC, SSL, VPN and Static routing. Work a mix of full time and as needed basis on projects supporting and implementing network architecture for the Baltimore City Public School Systems. Build and configure PCs, laptops, and Servers and configure VLANS on switches. Worked with Firewalls ASA 5505 - 5515 and Cisco equipment in cli IOS command line like Routers: 2800, 2900, 3800, 3900, 7200, and 7300 series. Worked with Cisco switches cli IOS command line interface. Cisco switch models: Catalyst 3850, 2960-X, and 2600X series. VPN, Remote Access, and RSA Authentication using the RSA console. Support Users using MAC computers and PDAs like iPhone, Android, and Blackberry in connecting to the Mobile Iron and BES or Blackberry Enterprise Server. Manage remote clients on Citrix Xenapp 6 apps, through the Citrix access management console server by closing, opening, troubleshooting, refreshing, and shadowing sessions Install printers, software, and update software on workstations via LANDesk remote assistance tool and remote desktop tool. Work in Active Directory, Group Policy, LANDesk manager, Microsoft Windows Server 2003, 2008 RS, and Exchange Server. Performs detailed examination and analysis of Phishing sites; Work in a Unix/Linux and Windows environment behind Kernel Shell and Powershell. Did Regular Expressions, Parsing, Scripting (BASH and Python). Use Splunk for Big Data parsing and investigating incidents and log correlation. Used Qradar and ArcSight as SIEM systems for alert and Incident Response. Performs analysis of malware binaries and communication points; Monitor and analyze network traffic and IDS alerts Create and manage Snort and Bro IDS/IPS rules. Investigate intrusion attempts and perform in-depth analysis of exploits Analyze a variety of network and host-based security appliance logs (Firewalls, NIDs, HIDS, sys Logs, etc) to determine the correct remediation actions and escalation paths for each incident. Perform investigation of on elevated intrusions and alerts. IT Support Analyst Baltimore City Public Schools HQ - Baltimore, MD June 2006 to June 2009 Troubleshoot computer hardware, application, network, and software related issues for Baltimore City Public Schools Network users. Create tickets and assign tickets to NOC and other proper departments or teams as necessary using HEAT ticketing system. Install printers, software, and update software on workstations via LANDesk remote assistance tool and remote desktop tool. Work in Active Directory, Group Policy, LANDesk manager, Microsoft Windows Server 2003, 2008 RS, and Exchange Server. Provide support for over 50,000 users on both the CEG and Exelon Domains. Provide VPN, Remote Access, and RSA Authentication using the RSA console. Support Users using MAC computers and PDAs like iPhone, Android, and Blackberry in connecting to the Mobile Iron and BES or Blackberry Enterprise Server. Manage remote clients on Citrix Xenapp 6 apps, through the Citrix access management console server by closing, opening, troubleshooting, refreshing, and shadowing sessions Cyber Security Tools Used in "Hands-on Work Experience" Sourcefire Defense Centers and Sensor Engineering, Fireeye, HP Tipping Point, Suricata, Mandiant Incident Response, Snort, Nessus, Nmap, Metasploit, Metasploitable 2, Kali Linux 2, Backtrack 5, AirCrack, Burp Suite, coWPAtty, Karmetasploit, Kismet, Telerik Fiddler, OWASP Top 10, IBM AppScan, IBM Bluemix, OWASP ZAP, HP DAST Webinspect, Fortify SAST Software Inspector, Softlayer, SonarQube, SIEM tools management, and Architecture, Splunk, McAfee ESD, IBM Qradar,HP Arc sight, Bluecoat, CyberArk, Websense, Netwitness, RSA Security Analytic Event Log Correlations and Analysis, Network Forensics & Incident Response, Tripwire, Unix and Linux administration, Nikto Web Server Scanner, Netsparker, VMWare, Vsphere, ESXi, Virtualization, IDA Pro, ASA Firewall ASDM, Palo Alto, PFSense, Chef Automation tool, Check Point Firewall ADM, IPS/ IDS, Cisco Routing and Security Configuration, Cisco Switching and Security Configuration, Zscaler cloud Proxy, Cisco ScanSafe, Nexpose, Trustwave, PenetrationTesting and Vulnerability Assessment, Risk Assessments, Core Impact, Found Stone, EnCase7, Wireshark Packet Analysis, Tcpdump, Log Analysis, EUREKA, Anubis, Malware, Trend Micro Officescan, GFI Langaurd, Qualys, Retina, Threat Expert, Alien Vault, Visual Threat, Virus Total, Network Monitoring, HEAT and Remedy ticketing systems, Molosk, Log Management, US Citizen and Security Clearance Eligible. Education Bachelor of Science in Information Technology in Security Western Governors University - Salt Lake City, UT December 2018 Advanced Certificate in Advanced Cyber Security in Advanced Cyber Security Villanova University November 2015 Certifications/Licenses Certified Information Systems Security Professional (CISSP) Certified Ethical Hacker (CEH) ECSA CCNA Routing and Switching

CCNA Security CASP CompTIA A+ CompTIA Network+ CompTIA Security+ CompTIA Project+ CompTIA Linux+ LPIC-1

Name: Anthony Griffith

Email: rodney90@example.net

Phone: 001-492-718-7955x34956