IT Security Analyst IT Security Analyst IT Security Analyst - AIPAC Not for profit organization Damascus, MD To acquire a position with the potential of advancement where I can utilize my knowledge and experience within Information Technology/Cyber Security. Work Experience IT Security Analyst AIPAC Not for profit organization - Washington, DC July 2018 to Present Performing business system analysis. ? Research, present, and implement new technologies to make the environment more efficient. ? Assisting in the coordination and completion of information security operations documentation. ? Working with information technology and organizational leadership to develop strategies and plans to enforce security requirements and address identified risks. ? Reporting vulnerabilities and other security exposures, including misuse of information assets and noncompliance. ? Working with AIPAC's IT department and specifically with members of the IT Helpdesk team to identify, select and implement technical controls. ? Researching, evaluating and recommending information- security-related hardware and software, including developing business cases for security investments. ? Defining and following protocols to respond to suspicious activity or events in a methodical way. Being proactive when an incident is reported by taking leadership of developing a response and coordinating that response throughout AIPAC using AIPAC Cybersecurity Incident Response Plan. ? Advising the CIO and the rest of the management team about all evolving threats and best practices that should be incorporated strategically into AIPAC's future IT plans. IT Security Analyst Fusion PPT LLC - Rockville, MD January 2018 to July 2018 Responded to Cyber Security Incidents, provided cyber threat analysis and reporting to support SOC and Program's situational awareness. ? Actively monitored security threats and risks, provided in-depth incident analysis, evaluated security incidents, and provided proactive threat research. ? Obtained knowledge of regulatory compliance directives to include various HHS and security controls and FISMA monitoring and reporting requirements. ? Managed and ensured the timely response and investigations of security events and incidents by the security operations center ? Coordinated with threat operations and threat intelligence specialists to resolve high or critical severity level incidents. ? Coordinated Splunk logging for NIH's CIT department. ? Actively used FireEye HX in coordination with NIH's CIT department. Technician Infozen Inc - Rockville, MD

December 2016 to December 2017 Received and resolved tier I/II SOC/NOC requests; escalated alerts to appropriate personnel, rebooted servers and network devices. ? Provided Tier I/II level NOC/SOC support to resolve problems on internal and customer systems and escalated problems to Tier II/III engineers ? Monitored over 1,000+ network devices including servers, routers, switches, and security appliances. ? Software used to perform such tasks include but not limited to WhatUpGold and Bomgar b300 ? Assisted with BlueCoat and IronPort policy configurations ? Racking/unracking devices in the datacenter. ? Administered and monitored system availability and performance ? Software used to perform this task WhatsUpGold ? Responded to emergency network outages in accordance with business continuity and disaster recovery plans. ? Utilized Symantec endpoint encryption to enforce policies to assure that systems are secured. Help Desk Technician I Infozen Inc - Rockville, MD April 2016 to December 2016 Supported Windows 7 OS, MS Office 2013, Internet Explorer 11, Google Chrome, and others. ? Utilized Bomgar for workstations support. ? Supported network and application authentication and access (McAfee Endpoint Encryption). ? Provided remote connectivity support with Citrix. ? Maintained peripherals including but not limited to, printers, external HD's, and network connected devices. ? Opened and updated tickets in Remedy for all work performed and escalate issues to meet service level agreements. SOFTWARE Active Directory, BMC Remedy, Citrix, McAfee Endpoint Encryption, NMap/ZenMap, Nessus: Tenable Security Center, Symantec, WhatsUp Gold Network Monitoring, NIST SP 800-53 r4, Cisco Email Security Appliance C370, and Cisco Content Security Management Appliance M670, IBM BigFix, Jamf Casper, Tenable Security Center, Forescout: CounterAct, Absolute, Jira, Sunflower Systems, Service Now, IBM AppScan, Falcon: Crowdstrike, Verismic Cloud Management Suite, Beach Head, Office 365, Netskope Education Masters in Cybersecurity in Cybersecurity University of Maryland University College 2016 Bachelor of Science in Criminal Justice in Criminal Justice University of Maryland University College 2014 Additional Information Excellent interpersonal skills, assessment skills, and organizational skills. Ability to multi-task and consistently meet deadlines. Effectively work within directorial policies and guidelines. Effectively develop standards of operation documentation. Maintain users within Microsoft Office 365 and

maintaining a secure environment through such features as multi-factor authentication, implementing firewall rules, vulnerability scanning, and identifying risk.. As a Security Analyst, I have extensive experience researching innovative technologies through such avenues as Gartner and Infotech as well implementing researched technologies. Excellent ability to adapt to new environments and new technologies. Experience with disaster recovery methodologies and procedures.

Name: Shawn Aguilar

Email: johnsonjames@example.com

Phone: 001-576-576-3632x61934