Job Seeker Tulsa, OK Seasoned IA Professional with extensive experience in network monitoring, incident response, testing, security event analysis and procedure writing for implementation of network components. More than 8+ years of experience operating large ArcSight Event Management Systems. Highly adept at developing ArcSight content filters, rules, dashboards and channels and in generating ad-hoc reports based on logger, management and customer requests. Skilled in in developing, testing and integrating new custom ArcSight connectors. Solid experience in penetration testing using a variety of static and dynamic analysis tools. Team player with outstanding interpersonal, communication and customer interfacing skills. SECURITY CLEARANCE: Active DoD Top Secret Clearance Authorized to work in the US for any employer Work Experience VITA / Zolon Technology - Chester, VA August 2018 to December 2018 Incident Handler Stay abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Create and work tickets created in VSM and Archer Monitor the network using McAfee Products. Search McAfee Products for the suspicious IPs and review the logs to determine whether they are malicious or not. Be the escalation point for Analysts on shift for tickets and events. Sr. Security Analyst (Remote) Department of Defense / Clearbridge Technology - McLean, VA May 2017 to July 2018 Review threats and security events for SIOC. Stay abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Create SOPs and Flowcharts for Incident Response and Management. Create and work tickets created in ServiceNow Monitor the network using HBSS and Splunk. Search Splunk for the suspicious IPs and review the logs to determine whether they are malicious or not. Handling incidents and procedures in accordance with FISMA standards. Security Analyst IMF/Teksystems - Washington, DC October 2017 to June 2018 Reviewed threats and security events for Cybersecurity Operations Team (COT). Stayed abreast on all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Created and worked tickets from in ServiceNow Monitored the network using ArcSight. Searched ArcSight Logger for the suspicious IPs and reviewed the logs for malicious behavior. Created custom channels and dashboards within ArcSight. Sr. Security Analyst Department of Education / Foxhole Technology Inc - Fairfax,

VA December 2015 to December 2016 Reviewed threats and security events for EDSOC. Stayed abreast of all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Monitored the network using ArcSight, Splunk and Sourcefire. Searched Splunk for the suspicious IPs and reviewed the logs to determine any malicious activity. Viewed IDS alerts and analyzed collect scripts obtained from an infected system to take the proper steps to remove the virus, Trojan, and/or malware from the system. Created custom ArcSight connectors, rules, dashboards, content and filters. Developed custom reports for the client in ArcSight and Archer for the client. Created and worked tickets in SecOps (Archer). Develop SOPs and training documents on proper usage of Archer and other security tools. Trained new analysts on how to use the security tools and Archer ticketing system. Handling incidents and procedures in accordance with FISMA standards. Senior Security Analyst DHS SOC - Fairfax, VA June 2014 to December 2015 Reviewed threats and security events for DHS SOC. Stayed abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Used the following IDS software ArcSight, Fidelis, FireEye, and Sourcefire to identify possible threats to the network. Viewed IDS alerts and analyzed collect scripts obtained from an infected system to take the proper steps to remove the virus, Trojan, and/or malware from the system. Assisted the ArcSight Engineer in suggesting and creating content filters within ArcSight to better find potentially malicious activity on the network. Created, worked, and escalated Remedy trouble tickets. Handling incidents and procedures in accordance with FISMA standards. Managed 3 other Analysts on a shift and approved work performed by them. Senior Security Engineer/ Analyst House of Representatives / ManTech International - Washington, DC June 2013 to June 2014 Reviewed threats and security events for the House of Representatives. Stayed abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Updated, managed and administered the McAfee IDS with the latest SEUs and removed rules that were triggering too many false events. Monitored events in ArcSight and Splunk for possible malicious activity and coordinated the remediation of infected workstations. Performed searches in Splunk for suspicious IPs and domains. Created custom ArcSight connectors, rules, dashboards, content and filters.

Developed new ArcSight customer connectors to integrate site-specific data and tested and integrated ArcSight provided connectors. Created custom channels to investigate potentially malicious traffic. Created SOPs on who to contact in case of an emergency. Handling incidents and procedures in accordance with FISMA standards. Scheduled, approved and hired part time staff for ManTech. Mid-Shift Security Supervisor Department of Justice / Knowledge Consulting Group - Washington, DC January 2011 to June 2013 Reviewed threats and security events for the Department of Justice and subcomponents. Stayed abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Used the following ArcSight SIEM, Netwitness and Sourcefire and IDS software to identify possible threats to the network. Created custom ArcSight connectors, rules, dashboards, content and filters. Used Netwitness to pull PCAP data for ArcSight events that were potentially malicious. Transferred the PCAP data to the Dirty Box and use the VM and tools to find the call backs within the malicious file. Use Netwitness to find potentially malicious activity. Updated Sourcefire IDS with the latest SEUs and removed rules that triggered too many false events. Created custom channels to investigate potentially malicious traffic. Created and followed Remedy tickets created due to malicious activity. Created and updated training material for new analysts. Created SOPs on who to contact in case of an emergency. Trained new analysts on the SOPs developed by the leads. Monitored IRC chat rooms for information of possible attacks against DOJ or components. Opened Remedy tickets for incidents and request updates and closed when completed. Monitored the high side events for possible malicious activity. Handling incidents and procedures in accordance with FISMA standards. Met with other shift supervisors to find ways to improve the SOC. IT Specialist Customs and Border Protection / DHS August 2010 to January 2011 Reviewed threats and security events for the Customs and Border Protection's SOC/CSIRC and DHS SOC. Stayed abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Reviewed and Approved block requests and significant incidents. Used the following IDS software Dragon, SourceFire, and ArcSight SIEM to identify possible threats to the network. Created custom ArcSight connectors, rules, dashboards, content and filters. Used Encase Enterprise to perform

malware forensics on workstations and to help IA investigate users who violated policy within CBP. Helped the Sourcefire Engineer with updating Sourcefire rules. Handling incidents and procedures in accordance with FISMA standards. Government Lead for the SOC during the night. Customs and Border Protection / DHS - Springfield, VA August 2009 to January 2011 Senior Security Analyst Customs and Border Protection / DHS - Fairfax, VA August 2009 to August 2010 Reviewed threats and security events for the Customs and Border Protection's SOC/CSIRC and DHS SOC. Stayed abreast all current and past cyber related vulnerabilities, malware, viruses and major vendor advisories. Created, worked, and escalated Remedy trouble tickets. Used the following IDS software Dragon, Sourcefire, and ArcSight to identify possible threats to the network. Viewed IDS alerts and analyze collect scripts obtained from an infected system to take the proper steps to remove the virus, Trojan, and/or malware from the system. Used Encase Enterprise to perform forensics on workstations containing malware and to assist IA with investigating users who violated CBP policy. Developed scripts using Python to search and correlate firewall logs and reports. Made custom ArcSight channels to drill down into potentially malicious or events that could cause damage to the network. Member of a board of Shift Leads and a government Lead to suggest and test possible changes to ArcSight rules to improve monitoring of the network. Assisted the ArcSight Engineer with suggesting and creating content filters within ArcSight to better find potentially malicious activity on the network. Handling incidents and procedures in accordance with FISMA standards. Managed 3 other Analysts on a shift and approved work done by them. Education Master of Science in Information System Security in Information System Security Strayer University - Fredericksburg, VA Bachelor of Computer Science in Information Systems Security ITT Technical Institute - Springfield, VA Associate of Arts in Accounting Delta Community College, University Center, MI Skills IDS (7 years), Remedy (4 years), Security (9 years), SIEM (2 years), Splunk. (3 years) Additional Information TECHNICAL SKILLS: Computer and Network Security Remedy Splunk NetIQ McAfee NSP ServiceNow Computer Hardware Troubleshooting Dragon IDS SecOps (Archer) ArcSight ESM BigFix VM ArcSight SIEM Sourcefire HBSS Encase 6.7 Fidelis McAfee IDS FireEye Lancope Netwitness VSM Vfire ARS

Name: Dr. Christine Gomez MD

Email: pking@example.com

Phone: +1-760-641-7114x757