Security Operations Engineer Security Operations Engineer Security Engineer/ Analyst Denver, CO Work Experience Security Operations Engineer Samsung/Joyent - Denver, CO 2018 to Present Assist with managing third-party threat intelligence tools Threat hunt IOCs that are applicable to our environment Perform security operations support including monitoring, remediation, implementation, configuration, planning Perform network and host-based monitoring and intrusion detection analysis to determine attacks on public and private cloud networks. Take mitigation actions to contain the attack activities and minimize damage when a malicious activity or attack has occurred on networks/systems. Monitor, investigate, detect, resolve, and remediate attacks, threats, and security breaches as a part of a cross- functional security incident response team. Install, monitor, tune and manage security devices, including SIEM, data encryption, and other security products. Work and communicate to stakeholders the status of information security, inform of possible risks, and suggest ways to improve security. Perform incident response, security infrastructure management or monitoring services, and digital forensics. Contribute to projects with technical knowledge of network and system operating system and network security in physical, virtual and cloud-based implementations. Keep up-to-date with information security news, techniques, and trends. Manage multiple priorities simultaneously while managing expectations and project milestones. Security Engineer II Charter Communications 2017 to 2018 Assist with securing cloud and container infrastructure Identity and Access Management Assist with Firewall rules when implementing new servers, applications, and environments Assist with SIEM management Create runbooks, policies, and procedures to managed security solutions Provide training to other security teams that will be full-time users of deployed products Implement new security tools for Network Security Operations Endpoint Protection & Detection and Response SME Assist with securing cloud infrastructure Manage DevOps security tools Assist with architecture and design for new security tool implementation Assist with identifying security gaps Identify gaps in security for the Network Security Operations team Assist with product implementation Subject Matter Expert for Endpoint Protection/ Detection and Response project Security Engineer Tier 3 Comcast - Denver, CO 2017 to 2017 Threat hunting utilizing SIEM, EDR,

IDS, Access Management and other logs Analyze threat intelligence and applied to our environment Provide escalated support for Tier 2 Engineers Manage incidents throughout the entire IR lifecycle Work on an escalated incident bridge as needed Respond to and investigate alerts in IDS/IPS Monitor AWS environment and respond to alerts via GuardDuty Document security processes Analyze potential malware in a sandbox environment Perform in-depth investigations on incidents and [pro-actively threat hunt Application control Analyze network traffic for anomalies Facilitate escalated incident response process Write technical training documents Enforce compliance policy Vulnerability scanning Manage critical vulnerability process Experience with managing users & incidents in a SIEM IT Support Analyst Trulia/Zillow Group - Denver, CO 2013 to 2017 Incident Response Patch Management Identity and Access Management Manage encryption solution on each host Manage backup and restoration solution

I supported an office of 500 employees from operations to executive level with all their technical needs and issues. Create, maintain, and deploy computer images using SCCM Process new hire & end hires Assisted with multiple domain migrations assisted with Shoretel telephony migration Manage and deploy Wireless Access Points Manage and troubleshoot DHCP & VLANS Run cable and manage MDF & IDF rooms Project lead for managing Endpoint Protection Deployed and maintain solution for remote support Project lead for supporting NYC office of 50 marketing executives, which would require visiting the NYC office once every quarter Provide technical troubleshooting for VoIP, email exchange, JAMF Apple management, VPN, Identity and Access Management, Splunk, Dropbox, Google Apps, Sophos, IT Helpdesk Analyst SAIC 2013 to 2013 Work with 25 help desk agents covering more than 200,000 individual Army Reservist. Support soldiers with web browser issues, VPN, proxy servers, windows, active directory, outlook, webmail, web and teleconferencing software, various types of administrative databases. Quickly and effectively solved customer challenges. Maintain quality control/satisfaction records, constantly seeking new ways to improve customer service and troubleshooting. Education SecureSet Academy 2017 High School Diploma Public Academy for Performing Arts 2005 Skills Identity management (Less than 1 year), incident response (6 years),

security (6 years), Siem (3 years), Splunk (4 years) Links https://www.linkedin.com/in/gutierrezpj Additional Information Skills Microsoft Administration Linux Administration Security Information and Event Management (SIEM) Endpoint Security Detection and Response Cloud and Container Security Tier 3 Incident Response SSO & Identity Management Splunk User Certified

Name: Benjamin Golden DDS

Email: zpatel@example.com

Phone: +1-691-567-2280x0720