Splunk Engineer (GISCS Architecture and Engineering) Splunk Engineer (GISCS Architecture and Engineering) Splunk Engineer (GISCS Architecture and Engineering) - Carnival Cruise Line Fort Lauderdale, FL Work Experience Splunk Engineer (GISCS Architecture and Engineering) Carnival Cruise Line - Miami, FL September 2018 to Present Maintain existing Splunk infrastructure (on-prem and Splunk Cloud) through WebUI and CLI (RHEL 7 Linux) Architect and deploy new Splunk servers (DS, HS, SH) Troubleshoot all Splunk-related issues (on-prem / SplunkCloud) Onboard and filter new data sources (regex, etc) Develop Splunk content and dashboards Create new inputs via syslog (syslog-ng), Splunk API, DB Connect, Universal Forwarders Write and deploy simple bash, Power Shell scripts Administer and maintain Splunk Enterprise Security (ES Admin cert pending) Create new/tune existing correlation searches and notable events in Splunk Enterprise Security Work with Security Monitoring tools: PaloAlto/Cisco devices, Qualys, Fidelis, CarbonBlack Collaborate with Security Operations to develop new notable events in Splunk Enterprise Security Create new content related to PCI compliance project Create log inputs for Office 365, AWS and Azure Cyber Security Operations Center Lead Analyst (SOC) Lennar - Miami, FL May 2017 to September 2018 Manage Splunk infrastructure (on-prem/Cloud) Splunk UBA (Azure deployment) Splunk UF deployment and troubleshooting in Windows and Linux (RHEL 7) Manage Splunk deployment servers / heavy forwarders / hybrid SH Act as SME for Splunk (on-prem and cloud) Create new content and manage existing notable events in Splunk Enterprise Security Create new dashboards in Splunk, install and configure Splunk apps Manage roll out and support of CylancePROTECT Provide expert technical advice and counsel to junior analysts Analyze a variety of network and host-based security technology logs to determine the correct remediation actions and escalation paths for each incident Recognize actionable events Respond and remediate cyber incidents Perform threat hunt activities using various logs in Splunk (Windows events, network, Cylance AV logs) Write new and update existing SOPs related to SOC operations Sr. Cyber Security Analyst (SOC / Cyber Incident Response Team) SunTrust Bank - Orlando, FL February 2016 to February 2017 Analyze a variety of network and host-based security technology logs to determine the correct remediation actions and escalation paths for each incident (using

Splunk/Netwitness) Review security events that are populated in a Security Information and Event Management (SIEM) system (SecureWorks, Resilient) Provide guidance and work leadership to less-experienced technical staff Document all activities during an incident and provide leadership with status updates during the life cycle of the incident Assist with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions

Execute incident response process when a security incident has been declared Incident Investigator ExxonMobil - Budapest, HU December 2012 to December 2014 Threat hunt using various tools (Splunk, RSA Security Analytics, FireEye) Incident response and management In-depth malware analysis using various tools (FireEye, Netwitness, Splunk) Provide timely detection, identification and alerts of possible attacks/intrusions, anomalous activities, and misuse activities, and distinguish these incidents and events from benign activities Malicious activity investigations on the corporate network, servers and workstations Research and track new exploits and cyber threats Provide regular feedback to enhance our security monitoring and controls Conduct as needed ad-hoc incident analysis Examine network topologies to understand data flows through the network Risk / vulnerability identification and assessment 3rd Party Risk Analyst / External connections regional coordinator EAME ExxonMobil - Budapest, HU November 2006 to November 2012 Budapest, Hungary (Nov 2006 - Nov 2012) Network Security - 3rd Party Risk Analyst / External connections regional coordinator EAME Design new secure network connections for 3rd party vendors needing access to the company network resources using business input Design network control points (firewalls, IPS, IDS) for L4 business and L3 process control networks as well as external network connections Design higher-risk internal network connections (internal wireless, process control, DMZ) and user/device authentication Review and assess risk to the corporate network coming from existing external/high risk internal connections Review and maintain network control point (firewall and other) configurations Coordinate work between various IT teams, business and external business partners Participate in divestment/acquisition projects Review risk, approve and certify new and recertify existing external network connections IT Local Operations - IT Support Analyst ExxonMobil - Moscow, RU February 2004 to October 2006 Russia,

Ukraine, Belarus) Global Office Update project regional lead Smart Card project region lead Site Readiness project region lead (hardware upgrade) Maintain availability of all production site services with aim to provide maximum service uptime for users Manage local and remote desktop, server, telecoms, printing and application environment with functional input from area or regional contacts Act as focal point for site implementation of regional or world-wide projects into operation Maintain local disaster recovery plan Operate and provide technical support for local and remote site infrastructure Act as local problem and change coordinator IT Support Technician Seminole County Government - Orlando, FL February 2001 to June 2002 Lead technician for Operating System migration project (Windows NT to Windows 2000) Scope of migration project - approximately 2000 workstations located in remote sites around the city and county including EMS/Fire/Rescue stations, county 911 emergency center, water treatment plants, garbage disposal, recycling plants and other facilities Education Bachelor of Science in Computer Science Grand Valley State University - Grand Rapids, MI Certifications/Licenses Certified Splunk Architect Present CEH October 2022 CHFI February 2022 Certified Splunk Enterprise Security Administrator Present Azure Fundamentals July 2019 to Present Additional Information SKILLS Architect new / maintain existing Splunk systems Develop and tune existing content for Splunk Enterprise Security Conduct in-depth cyber incident investigations Cyber Threat Hunting using various tools: Splunk, RSA Netwitness, FireEye, Cisco/PaloAlto IPS Lead incident response, management and remediation

Name: Daniel Archer

Email: ischultz@example.com

Phone: (425)524-8773x251