Security Analyst Security Analyst Security Analyst - University of Phoenix Phoenix, AZ Work Experience Security Analyst University of Phoenix - Phoenix, AZ September 2017 to Present Worked in a SOC Assist in migrating physical and virtual servers and firewalls to Amazon Web Services (AWS) from data center Agile framework trained and experienced Setup and maintain McAfee ePO antivirus console, SIEM and Web Gateway/proxy Implement Crowdstrike NextGen and Carbon black antivirus Maintain Checkpoint & Cisco firewalls Use Splunk, SIEM, antivirus console, Encase, and firewall logs to perform threat hunting Use Proofpoint spam protection, and O365 to investigate phishing/malicious email and take appropriate actions Use Active Directory to create OUs, GPOs, locate users and computers, move computers, unlock accounts, change permissions, AD cleanup Respond to audit requests with documented proof of regulatory compliance Train and educate team, and staff on information security best practices, procedures and policies Security Analyst BlackStratus - Stamford, CT October 2015 to September 2017 Worked in a SOC Maintained SIEM Created and edited rules in SIEM for alerts Monitored SIEM, identified security risks, and provided remediation steps Trained and educated staff on information security best practices, procedures and policies Created policy and procedure documentation for company, SOC, and customers Security Engineer IBM Global Business Services - Hopewell Junction, NY November 2010 to October 2015 Developed and implemented security applications such as anti-virus and DLP for large enterprise companies Supported large enterprise customers ranging from financial to railroad, and health care Ensured SLA's are being met for all customers Created documentation on processes and procedures for team, customers, and IBM Worked with auditors to ensure and provide evidence of compliance IT/CAD Manager Svigals + Partners - New Haven, CT February 2008 to November 2010 Setup and maintained servers, network, MS Exchange, Active Directory, Backups Planned and procured IT equipment and applications to maintain company industry currency Created and maintained policies, plans, and documentation for Senior Management and employees Setup and maintained Windows Server Update Services (WSUS), and other Group Policies Setup and maintained workstations, laptops, LCD projectors, printers and plotters Set up switches and fiber optic cable to extend network and to cover more floors

Coordinated update of security system and addition of security cameras IT Technician Meriden Board of Education - Meriden, CT August 2005 to February 2008 Supported the two largest schools in the district autonomously Set up and maintained over 700 workstations and laptops Setup and maintained audio/video, and peripherals Set up and maintained numerous software applications used in various teaching categories Diagnosed and repaired network outages Maintained network devices and UPSs Education Bachelor's in MIS in MIS Western Connecticut State University - Danbury, CT 2014 to Present Associates Degree in Computer Systems in Computer Systems Naugatuck Valley Community College - Waterbury, CT 2012 to 2014 Additional Information CISSP, Member of Infragard Qualys Vulnerability Management, and Splunk certified Trained with ISO 27000, NIST, HIPAA, PCI DSS, SOX, GLBA, FERPA, Scaled Agile Framework, and more. Experience with Trend Micro, McAfee, Symantec, Sophos, and CA antivirus Experience with several SIEM applications; Azure Sentinel and Kusto Query Language, McAfee ESM, and SIEMStorm/Logstorm Packet and log analysis experience Encase/forensics Basic programming experience in PowerShell, and Python AWS and Azure experience Multi-factor authentication expeience Jira and Confluence experience Expert with all Windows Server operating systems, Experienced with Linux, and Mac OS Excellent at solving problems/troubeshooting, working under pressure, and writing policies and procedures

Name: Samantha Hays

Email: mccartyedward@example.com

Phone: 5203672193