IT Security Analyst IT Security Analyst IT Security Analyst - McCormick & Company Windsor Mill, MD Work Experience IT Security Analyst McCormick & Company - Hunt Valley, MD October 2017 to Present Performed account provisioning through Active Directory, IAM tool SailPoint and SAP Created service, test and generic accounts in Active Directory Administered SAP module and SAP "bolt-on" application security issues Updated authorization roles and profiles, and resolved basic authorization problems that may occur in all applications IT Security Operations team supports Performed user administration tasks on development, test, and production application systems. Office365 and Azure Active Directory experience with managing users, groups, assigning administrative roles, resetting user passwords, and setting up Multi-Factor Authentication (MFA) Monitoring AzureAD risk event sign-ins reports: Sign-ins from anonymous IP addresses, Sign-ins from infected devices and Sign-ins from infected devices Manages over 1600+ contractors accounts Performed employees and contractors terminations/separations Managed critical incidents, tasks and change requests via HP Service Manager and ServiceNow Created and maintained SAP role & authorization profiles. Processed SAP user access requests and support everyday troubleshooting of access problems. Participated in the creation of enterprise security documents (policies, standards, baselines, guidelines and procedures) Provided administrative support for security systems Escalated problems to appropriate teams based on established guidelines and procedures Ensured assigned tasks and projects were completed on schedule Identity and Access Management Analyst Exelon Corporation - Baltimore, MD October 2015 to October 2017 An Identity and Access Management Analyst with strong knowledge in Identity Management (Auto-Provisioning, Password Management, Access Governance, and Role Based Access Controls (RBAC) responsible for daily operational identity proofing, security administration and access control support at Exelon Corporation. Coordinated with senior managers to evaluate and refine existing processes, participate in the planning, development, and deployment of Identity and Access Management access control standards and processes into production environment. Additional responsibilities include: Performing cyber and physical security transactional access control activities on behalf of Corporate and Information Security Services (CISS), HR, Business

Unit, and IT application owners in support of security risk management, compliance, and business requirements Coordinating deployment of Identity and Access Management (IAM) architecture and other security projects to various Exelon Corporation applications Acting as an Administrator for Identity and Access Management (IAM) to proactively identify and mitigate organizational risk, streamline access management projects to ensure resources are secured to adapt to changing threat landscapes Utilizing Administrative access rights to create user acceptance test (UAT) scripts, set up UAT scenarios for lead stakeholders User Acceptance Testing activities Provisioning and de-provisioning logical and physical access throughout the enterprise via Andover Continuum and C-Cure Creating and managing On-call Incident Response schedule for HP and Oracle-based ticketing systems Provided system support for user accounts within Active Directory, Aries, DMZ and RPN (regulatory) environments Administer user directories, distribution lists, mailboxes, folders and files Create, add or remove clients from Microsoft Exchange 2010 through scripts Created test shared account in Active Directory or DMZ Server Managed and resolved user access issues along with security enforcement Performed initial investigation and troubleshoot of Access Request System (ARS) & Access Governance System (AGS) Managed critical incidents via HP Service Manager Incident Management Provided production support for the Request Management (RM) Module Participated on 24/7 On-call Incident Response schedule for both HP and Oracle-based ticketing system Improved file shares' process, system documentation, process documentation Managed and complied with NERC Critical Infrastructure Protection (CIP) and SOX regulated processes: Used ACLs to manage physical and electronic information Provisioned logical and physical access throughout the enterprise via Andover Continuum and C-Cure Administered mail permissions using Exchange Management Console, Exchange Management Shell Determined the root cause of security events and provided resolution to security events related to company resources Provisioned user and application access via Oracle-based Access Request System (ARS) Managed single sign on applications for end users and business owners Education Bachelor of Science in Cybersecurity ITT Technical Institute - Owings Mills, MD June 2015 Associate Degree in Information Technology ITT Technical

Institute - Owings Mills, MD September 2013 Skills Active directory, Exchange, Citrix, Ldap, Vmware, Vpn, Sap, R2, Linux, Linux/unix, Unix, Android, Ios, Symantec, Ms office, Mac, Mac os, Emc Additional Information TECHNICAL SKILLS Enterprise Systems Active Directory, LDAP, HP Service Manager, VMware Workstation, VPN, SailPoint, ServiceNow, SAP Software Team Viewer, Citrix Apps, EMC/EMS, Antivirus: McAfee/Symantec, MS Office, Exchange/Office365, Skype Operating Systems Linux/UNIX, Mac OS X, Windows (XP, Vista, 7, 8, 10, Server 2003/2008 R2), iOS, Android

Name: David Cox

Email: hpena@example.org

Phone: (928)899-5341x853