Information Security Infrastructure Engineer, Identity and Access Management Information Security Infrastructure Engineer, Identity and Access Management Information Security Engineer, Infrastructure, Identity and Access Management Charlotte, NC Work Experience Information Security Infrastructure Engineer, Identity and Access Management Lowe's April 2019 to Present Support Directory Services in both production and non-production environments while analytically working to help improve the security posture across the organization.   Support Active Directory (AD) for both on-premises and cloud domains   Provide support for Google Cloud Platform (GCP) and Microsoft Azure   Leverage PowerShell to perform tasks   Document all changes to production environment and execute approved changes as a Change Coordinator   Review Microsoft Risk Assessment Program (RAP) with business analysts to address potential vulnerabilities   Represent our team in organizational readiness meetings for upcoming projects   Identify security-related gaps in existing processes or policies to improve security posture across the organization   Work with Identity Governance teams to provide secure solutions to help enable the organization in conducting business in a secure manner   Strategize with team and project managers about our role in upcoming projects   Mentor new hires Information Security Analyst, Identity and Access Management Lowe's February 2018 to April 2019 Develop relationships with key stakeholders throughout the organization to gather information related to business requirements and individual department procedures. This information is analyzed to streamline the intake process as well as identify potential risks and vulnerabilities while striving to provide the highest level of customer service to the business.   Introduced expedite and escalate KPI's for SLA performance metrics through BMC Remedy   Handled security-related issues such as emergency terminations, as well as expedited or escalated requests as assigned   Identified process gaps and meet with stakeholders to gather proper requirements to improve the existing standardization and documentation   Used CA IdentityMinder to manage accounts and add LDAP groups   Manage and improve the process of account provisioning   Collaborate with department managers to establish their department's role-based provisioning for all newly onboarded employees   Identify risk, compliance, and other security-related issues related to both on-premises and Cloud Infrastructure

(CI) and cloud-based applications from inception to implementation   Utilized DevOps and Agile Transformation approach to projects and implementations Sr. Information Security Analyst, Identity Access Management (Remote) Aetna April 2017 to February 2018 Member of the team developing and testing the automation of daily provisioning tasks using CA (Computer Associates) Identity Manager.   Trained newly hired team members   Documented changes to the production environment   Managed project SharePoint site documents   Engaged stakeholders and conducted risk assessments for automated solutions   Utilized Agile and DevOps approach to building and deploying automated solutions   Tracked automated provisioning tasks metrics and completed cost-benefit analysis to show the return on investment (ROI) to leadership   Handle escalations, immediate terminations, and urgent security-related requests   Used daily KPIs (Key Performance Indicators) to keep track of personal and IAM team's SLAs and performance metrics Information Security Analyst, Identity and Access Management (Remote) Aetna November 2015 to April 2017 Approved or denied requests based on security policies, and added users to security groups based on job role and approvals.   Enforced and implemented company security policies, standards, and best security practices   Provisioned user accounts to add to UNIX and Linux hosts and Oracle databases   Created and managed Network (NAAP) team Kanban   Created and maintained Organizational Units (OU) within Active Directory (AD)   Handled a variety of Identity and Access Management related requests   Distributed access and LDAP related requests amongst team members   Attended team meetings to implement IAM solutions and analyze vulnerabilities and risks Network Engineer Cincinnati Bell Technology Solutions - Madisonville, KY October 2014 to June 2015 Baptist Health Hospital, audited Active Directory (AD) accounts, and took ownership of backing up critical Windows and UNIX application servers.   Led the effort to create documentation for software installations and IT procedures, and documented configuration of remote access on Mac OS and Windows devices   Worked with compliance and security departments to adhere to HIPAA standards, and trained and mentored IT staff IT Analyst Navitas, USA Holdings at WKU August 2013 to October 2014 Served as the first point of contact for all IT issues.   Influenced the implementation of best IT security practices by auditing Active Directory (AD) accounts and the

security groups to which they belong   Created new user accounts in Active Directory (AD)   Created Exchange mailboxes for new employees using MS Exchange Management Console   Improved IT security by configuring the F-Secure antivirus server and presented ideas for physical and network security at conferences   Created and implemented end-user template for all submitted service desk tickets IT Analyst LAN/WAN/SAN (Remote/Onsite) Allied Wireless Communications Corporation January 2011 to July 2013 Member of the field team who launched the company and successfully completed network conversion.   Coordinated disaster recovery efforts to successfully restore resources and business operations after a site experienced a natural disaster   Hands-on support for Juniper routers and switches to troubleshoot issues at OSI layers 2 and 3   Managed all IT support and achieved 99.999% uptime SLA for each business unit   Windows Patch Management   Helped design a method of remote computer imaging across the domain using Dell Kace   Ensured PCI-DSS compliance for all Point of Sale workstations;   SIEM; Encrypted the hard drive of all laptops and managed McAfee ePO   Used Wireshark and Fiddler 2 for packet inspection and to perform network forensics Education Master of Professional Studies in Homeland Security, Information Security and Forensics Penn State University Graduate Certificate in Information Systems Cybersecurity Penn State University Bachelor of Science in Computer Information Technology Western Kentucky University Skills Information security, Security, Active directory, Linux, Unix, DNS, Vmware Links https://www.linkedin.com/in/jasonbradleyward Certifications/Licenses CISSP November 2018 to November 2021 CompTIA Security+ May 2015 to May 2021

Name: Andrea Dunn

Email: alexanderbright@example.org

Phone: 488.937.8690x288