

IT Security Administrator IT Security Administrator IT Security Administrator - Fiserv Canal Winchester, OH Work Experience IT Security Administrator Fiserv May 2018 to Present

- * Handle extremely confidential information in a professional manner.
- * Manage IPv4/IPv6 in BlueCat to make sure they do not overlap before project goes live.
- * Configure Controllers in ArcSight for log monitoring
- * Perform daily, monthly terminations, and hot/emergency terminations via AD, mainframe, PowerShell scripting, and other applications as applicable.
- * Managed VPN, RSA tokens and console issues including direct and remote in different business units.
- * Administer Active Directory and other user accounts as applicable.
- * Use ServiceNow / ServicePoint to track and manage request, incident, cases, and task to meet SLAs.
- * Administers the set-up of new profiles, creates and updates access permissions and maintains user accounts for enterprise system
- * Create and maintain documentation on account maintenance and proactively identify potential issues in the enterprise environment.
- * Provide training to new hires and contractors.
- * Manage CheckPoint Endpoint, and Cisco AnyConnect Security
- * Provide on-call, 24/7 technical support to multiple business units.
- * Assigned security and distribution group access and privileges based on employee role and job functions.
- * Created, maintained and disabled users' profiles on the corporate network.

Information Security Analyst Syntryc Technologies January 2016 to May 2018

- * Configured ArcSight for systems to log information such as syslogs, event logs, and audit logs for various business units.
- * Examined alerts from SIEM (ArcSight and Splunk). Developed Service Level Agreements (SLAs) to establish problem resolution expectations and timeframes.
- * Analyzed, planned, designed, directed, and completed multiple Splunk installations of comprehensive security use cases and solutions for business customers.
- * Created dashboards from custom queries and modification of panels to help interpret security data.
- * Contributed to a team of information assurance professionals working with threat data, writing reports, briefing event details to the management and coordinating remediation with personnel.
- * Performed scheduled vulnerability and audit scanning
- * Prepared operational reports, and analysis setting forth progress, adverse trends and suitable recommendations or conclusions.
- * Consolidated and analyzed all relevant data to create and maintain awareness for various department. responsibility.
- * Identified

potential risks, such as virus and malware attacks, and hacking. Prioritized threats, including observed and potential threat components, indicators, and vulnerabilities discovered through research.

- * Developed plans to safeguard computer files against accidental unauthorized modification or disclosure
- * Conferred with internal associates on issues such as systems access needs, access elevation, security violations, and awareness training

Systems Administrator JP Media February 2015 to January 2016

- * Reviewed and analyzed systems reports for any alerts or discrepancies.
- * Resolved technical support inquiries on daily basis.
- * Monitor servers for compliance with established standards, policies, configuration guidelines and procedures.
- * Provide capacity analysis reports/data
- * Manage and configure VMWare Horizon View VDI environment

Directed a computer replacement project to replace nearly 100 end of life computer systems

- * Maintained Windows Server domain controllers monitored, and reviewed systems logs.

Helpdesk Technician iQor Inc January 2014 to February 2015

- * Provided Tier I technical support to non-technical personnel/end users for various clients such as Apple and Android phones users. Resolved problems with malfunctioning products.
- * Managed call flow, achieved metrics, and responded to technical support needs of customers.
- * Handled activations, suspensions, billing, deactivations, and troubleshooting.
- * Supervised team of 14 members to successfully attain weekly and monthly targets.

Education Associates Degree in Computer Science Columbus State Community College 2018

Certifications/Licenses Security+ March 2019 to March 2022 Splunk Core Certified User July 2019 to July 2022

Additional Information

- * Diligent and result-oriented security professional with 3+ years' experience in security practices and maintenance. Personable, dedicated, self-motivated, friendly and committed to resolving security problems in a timely and thorough manner to maintain uptime.
- * Ability to identify potential security risk, and with solid understanding of security applications and tools.

SKILLS | TOOLS

- ? Vulnerability Management ? Incident Management ? Operating Systems(Windows, Linux) ? Splunk Engineering ? Active Directory ? Cisco AnyConnect ? Qualys / Nessus ? Reporting ? ServiceNow / Servicepoint ? Port Scanning ? WireShark ? PeopleSoft ? CheckPoint Security ? Leader/ Team player ? SQL ? ArcSight ? TripWire ? Mathematical / Analytical ? Mainframe ? Java / Python

Name: Catherine Rodriguez

Email: beckywatts@example.com

Phone: 288.912.7548