

IT Security Analyst IT Security Analyst IT Security Analyst Chicago, IL Worked with developers, system/network administrators, and upper management to ensure secure design, development, and implementation of applications and networks. Gave technical expertise and oversight of security tool/appliances deployment and implementation. Provided forensic analysis and troubleshooting to assist in the containment and remediation of security incidents. Consistently researching new trends in the IT security space and in system administration to better assist with the development of the IT security program within an organization. Authorized to work in the US for any employer Work Experience IT Security Analyst Coyote Logistics - Chicago, IL November 2017 to May 2019 Reduced the number of phishing incidents within a 6-month time span by implementing various anti-phishing technologies from Proofpoint and Office 365 along with end user training Implemented best practices for risk reduction across a broad range of enterprise applications, systems and network interfaces. Assisted with the development of processes and procedures to improve incident response times and analysis of incidents. Created scripts using Windows PowerShell to automate system administration tasks and create internal audit reports for the compliance team. ? Used the CyCLI to generate Cylance reports and provide a tool to the server team to manage reinstallation of the Cylance software on workstations and servers. ? Created specialized scripts for the compliance team to use for workstation reporting and validating other generated reports. ? Pulled information from Office365 to better assist with ongoing phishing incidents and to triage security related events. Spearheaded the creation of documentation and management of the team's security infrastructure ranging from the password management application (Secret Server) to RSA SecurID administration. Used Bloodhound AD to discover and help remediate complex Active Directory misconfigurations including stale RDP sessions for domain administration, and Windows Local Users and Groups auditing. Aided in the evaluation of various enterprise products such as Rapid7 Vulnerability Management, CrowdStrike SaaS Endpoint Protection and Check Point NGFW R80.30. Service Desk Analyst Coyote Logistics - Chicago, IL August 2016 to November 2017 Responsibilities included initial assessment, triage, research, and resolution of cases; commonly regarding the use of an undocumented custom internal application

and its infrastructure components. Performed user account management functions in Active Directory and Office 365 for employees, new hires and contractors. Supported the server team to rewrite the team's internal service desk tool for Office365\AD Onboarding and prioritized tickets within the infrastructure queue to address persistent issues that would affect end users. Provided tier 1 and 2 technical on-call support to remote users including email troubleshooting, internal application support, and Citrix XenDesktop troubleshooting. Trained new analysts on the internal tools and created troubleshooting documents to be used when supporting the internal custom application. Desktop Support - IT Contractor Urban Partnership Bank - Chicago, IL April 2012 to August 2016 Created various scripts using PowerShell for the use of inventorying of workstations, monitoring of IT infrastructure, and automating administration tasks within Active Directory. Rewrote internal documentation on IT procedures, and oversaw training to 6+ IT interns & contractors. Discussed projects and issues with the infrastructure team, vendors and contractors to gather a strategy for deployment of IT services to end users. Administered the mobile device management solution (Worx Mobile) including working with the vendor and infrastructure team to troubleshoot various aspects of the software. IT Technician - IT Contractor Kirkland & Ellis - Chicago, IL August 2011 to August 2012 Provided in-person technical support for 1000+ corporate users including educated users on their new software deployments to troubleshooting hardware & software. Assisted the desktop team to move all IT equipment (workstations, VOIP and office equipment) to new offices throughout the building. Maintained inventory during the transition and ensured functionality of hardware & software. Education Associate in Applied Science in Networking Systems and Technology City Colleges of Chicago - Richard Daley College - Chicago, IL 2017 to Present Skills Active directory, Citrix, Vm, Vpn, Xenapp, Xendesktop, Security, Firewall, Rsa, Technical support, Hyper-v, Docker, Imaging, Checkpoint, Containerization, Windows 10, Cisco, Microsoft Office Links <http://linkedin.com/in/gerardoggallegos> Additional Information Skills OS Platforms: Windows 10, Windows Server 2012r2\2016\2019 VM Management: ESXI 5.5\6.5\6.7 & Hyper-V Script Languages: PowerShell 5.1\6.0 Email Gateway management: Proofpoint Email Protection Suite (TAP, TRAP), Office365 Administration (General Administration, Technical Support,

and Security & Compliance Administration) ManageEngine: ADAudit & ADManager
(Administration, IT Security & Compliance Reporting) SCCM Administration: Technical Support,
OS Imaging Management, Reporting Mobile Device Management: Citrix XenMobile
(Troubleshooting & Administration) VPN: F5 & NetScaler Gateway (Support) PowerShell:
Automation, Reporting, AD User Management, etc. Active Directory: Administration, Reporting
Google Suite: Administration Endpoint Anti-Virus Management: Cylance (Administration,
Reporting, Technical Support) Citrix XenApp and XenDesktop: Troubleshooting and
Administration Firewall: Checkpoint R80 (Reporting) Containerization: Docker BloodhoundAD
(Active Directory misconfigurations Reporting) Group Policy: CIS GPO Baselines for Windows OS
and Office Suite. Password Management: Secret Server 2 Factor Administration: RSA SecurID

Name: Emma Gray

Email: denniselizabeth@example.com

Phone: 264-935-4311x309