




Availability: Any Shift/Any Days/Any Hours
Preferred Shift: Night Shift
Available for Work: Immediately
Work Location: Remote
Desired Pay: \$65/hr

Last Updated: 02/06/2024 04:53

 <https://www.nullidle.com>
 <https://www.github.com/xegenix>
 <https://linkedin.com/in/insecurity>



Call / Contact

Employment

Skills & Software

Security Engineer II (Remote)

Lumen Technologies

12/2019 - 11/2023

Security Engineer II for the Cybersecurity Incident Response Team, primary responsibilities encompassing incident response within Office 365 and Azure environments. Orchestrated the seamless migration of over 12 years' worth of recorded weekly training videos and ticket reviews from Confluence to SharePoint. Led successful implementation initiatives to establish a centralized logging infrastructure for DNS log archival. Proficient in automating repetitive and time-consuming security-related tasks using Bash and PowerShell.

- Identify compromised Office 365 user accounts, rapidly intercept and secure accounts before data exfiltration can occur.
- Utilize monitors and alerting for detection of malicious activity originating from users and endpoints Leverage available tooling to aid investigation efforts **Cortex XSOAR, Splunk, Axonius, Wiz.io, Microsoft Defender MDE/MDI/ATP, ArcSight, Symantec Endpoint Protection, CrowdStrike, Trellix EX/HX/NX, ExtraHop, Ivan Neurons/RiskSense**
- Update and maintain organization-wide blocklists of known malicious hosts and IP addresses.
- Investigate compromised assets, identify points of entry, conduct root cause analysis.
- Scanning of internal applications utilizing Nessus, Qualys, and CrowdStrike Falcon Spotlight to identify vulnerable assets and applications.
- Create and use XSOAR playbooks to improve operational efficiency by reducing time spent on investigations by automating lookup of user information, assets, and external tooling.

Active Directory
 Adobe Experience Manager
 Apache Web Server
 ArcSight ESM
 Axonius
 Azure
 Bash
 Citrix XenServer
 Cloudflare
 Confluence
 Cortex XSOAR
 CrowdStrike
 CSS
 CyberArk
 Django
 Docker
 Elastic Stack
 ExtraHop
 Express.js
 Flask
 Git
 GlassFish
 HAProxy
 Hexo
 HTML5
 Hugo
 Jamf
 JBoss
 Jenkins
 Jira
 KVM
 Ivanti Neurons (RiskSense)
 LAMP/LEMP
 Linux Based Operating Systems
 Mandiant Redline
 Microsoft Defender
 MongoDB
 MySQL/MariaDB
 New Relic
 Nginx
 Node.js
 Office 365
 Oracle
 PostgreSQL
 PowerShell
 Python
 QEMU
 Redis
 Riak
 Splunk
 Symantec (SEP)
 Site24x7
 SiteMinder
 Tomcat
 Trellix / FireEye EX/HX/NX
 UNIX Based Operating Systems
 Urban Code Deploy
 VMware vSphere/vCenter
 WebLogic Server
 wiz.io
 Zimbra

03/2019 - 09/2019

Wells Fargo (Contract)

Security Engineer

- Provide insight on engineering needs of the project such as infrastructure, required services, and service configurations.
- Document work and processes so others can easily achieve the same results.
- Aided initial setup of Urban Code Deploy and Jenkins for project's CI/CD pipeline.
- Successfully conducted multiple service implementations (SiteMinder, Apache, MongoDB, and MongoDB Connector)

DevOps Security Engineer contributing to the development of the Crypto Compliance Project's cutting-edge compliance reporting tool. Spearheaded the implementation and documentation of key technologies such as Urban Code Deploy, SiteMinder, Apache, MongoDB, and MongoDB Connector to enhance project functionalities.

Linux Systems Admin

University of Phoenix

07/2014 - 12/2018

Seasoned Linux Systems Administrator for the University of Phoenix IT Operations Center, dedicated to ensuring the availability and optimal performance of web-based infrastructure for students and staff. Proficient in administering both physical and VMware virtualized infrastructure, supporting a diverse range of Windows and UNIX-based servers and applications.

- Systems Administration of Windows, Linux, and UNIX based applications and infrastructure within an enterprise production environment.
- Setup alerting for newly provisioned applications to detect performance issues and service failures. Create alert suppression for scheduled change tasks and the affected applications.
- Create knowledge-base documentation for alerts without a corresponding KB article utilizing KCS methodologies.
- Work with developers to troubleshoot build automation failures within the CI/CD pipeline.
- Coordinate bridge calls, engaging essential support channels and stakeholders for business impacting events.
- Work with datacenter operations teams to complete hardware changes within the scheduled change window.

01/2011 - 06/2014

Brinkster Communications

Help Desk Lead

- Provide support debugging web applications written in ASP .NET, PHP, Perl, and JavaScript for premium support customers.
- Support Shared Hosting, Dedicated Servers, and VPS customers via Ticket and Chat for hosting change requests, application support, hardware changes, database backup/restorations, and CMS setup assistance.
- Train new Help Desk members on administration of Windows and Linux servers.
- Manage customer DNS for domains using Brinkster name servers.
- Administration of Databases, Windows, Linux, VMware, Citrix XenServer, and Zimbra mail environments.
- Build-out hardware for dedicated server orders.

Experienced Overnight Help Desk Lead specializing in the administration and support of shared hosting, VPS, and dedicated server clients. Proficient in managing data-center operations, overseeing the administration of MySQL and Microsoft SQL Servers, and handling virtualization hosts using either Citrix XenServer or VMware ESX. Additionally, well-versed in managing Zimbra mail environments.