+1 (623) 271-0373

SECURITY ENGINEER II

josh.marcum@icloud.com

JOSHUA MARCUM

Address: 3524 E Morenci Rd
San Tan Valley, AZ 85143

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

Years	Professional Experience
12+	Windows Server, Linux/UNIX based OS
10+	VMware
8+	Systems Administration
8+	Enterprise Application Support & Monitoring
4+	Splunk
4+	Hybrid Cloud Security

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

Open vCard

Technology & Skills

- Active Directory
- Adobe Experience Manager
- Apache Httpd
- ArcSight ESM
- Axonius
- Azure
- Bash
- BSD (See Platforms)
- Citrix XenServer
- Cloudflare
- Concrete CMS
- Confluence
- Cortex XSOAR
- CrowdStrike
- CSS
- CyberArk
- Django
- Docker/Compose
- Drupal
- Elastic Stack
- ExtraHop
- Express.js
- Flask
- Git
- Ghost
- GlassFish
- Grav
- HAProxy
- Hexo
- HTML5
- Hugo
- IIS
- Jamf
- JBoss
- Jenkins
- Jira
- Joomla
- KVM
- Ivanti Neurons (RiskSense)
- LAMP/LEMP
- LiME
- Linux (See Platforms)
- Mandiant Redline
- Microsoft Defender ATP
- Microsoft SQL Server
- MongoDB
- MySQL/MariaDB
- New Relic
- Nginx
- Node.js
- Office 365
- Oracle
- PHP
- PostgreSQL
- PowerShell
- Python
- QEMU
- Redis
- Riak
- SilverStripe
- Site24x7
- SiteMinder
- Splunk
- Symantec (SEP)
- TextPattern
- Tomcat
- Trellix (FireEye EX/HX/NX)
- UNIX (See Platforms)
- Urban Code Deploy
- VMware vSphere/vCenter
- WebLogic Server
- Zimbra
- wiz.io CDR
- WordPress
- Zimbra
- Zookeeper

Platforms

- **Linux Based on:**
  RHEL, Debian, Arch, Gentoo and LFS
- **macOS**
- **Microsoft Windows**
  9x-ME, XP, 7-8, 10-11
- **Microsoft Windows Server**
  2000, 2003, 2008, 2012/R2, 2016, 2019, 2022
- **UNIX**
  AIX, HP-UX, Solaris BSD (FreeBSD, NetBSD, OpenBSD)

Employment

Lumen Technologies / Remote

12/2019 - 11/2023 — **SECURITY ENGINEER II**

Security Engineer II with Lumen's Cybersecurity Incident Response Team, tasked with securing the organization's M365 and Azure cloud environments. We leveraged a diverse toolkit to identify and remediate potential threats ranging from data exfiltration, phishing, anomalous network traffic, malware, and malicious object executions. Teams conducted regular vulnerability hunts engaged in mandatory training rotations, sharing security insights to enhancing our collective expertise.

Core Responsibilities

- Security of hybrid M365/Azure cloud environment, including Active Directory, ATA/ATP, Conditional Access, MFA, Microsoft Defender for Cloud/Identity/Endpoints, Sentinal, and Intune device enrollment.
- Leverage tooling to aid investigations: Cortex XSOAR, Splunk, Axonius, Wiz.io, Microsoft Defender MDC/MDE/MDI, ATA/ATP, ArcSight, Symantec Endpoint Protection, CrowdStrike, Trellix EX/HX/NX, ExtraHop, and Ivanti Neurons (formerly RiskSense)
- Utilize SIEMs such as ArcSight Enterprise Security Manager and Splunk for analysis of traffic, executions, and user activity to aid active investigations.
- Submit block requests with proper justifications to add malicious hosts and addresses to an organization-wide blocklist.
- Analyze packet captures for anomalous network traffic and traffic to known malicious addresses, identify source and remediate.
- Internal vulnerability scanning of assets and applications using Nessus, Qualys, and CrowdStrike Falcon Spotlight.
- Create and utilize playbooks within XSOAR for automating the lookup of hosts, user details, and alerts details of external tooling.
- Creation of PowerShell scripts to aid security related tasks within Azure, ADFS, and Exchange
- Perform sandboxed executions to determine if objects and websites are malicious in nature.

Wells Fargo (Contractor) / Hybrid

03/2019 - 09/2019 — **SECURITY ENGINEER**

DevOps Security Engineer contributing to the development of an in-house compliance reporting tool. Aided initial setup of the project's CI/CD pipeline to allow build automation. Lead multiple service implementations essential to the project such as Urban Code Deploy, SiteMinder, Apache, MongoDB, and MongoBI Connector.

Core Responsibilities

- Provide insight on engineering needs of the project such as infrastructure, required services, and service configurations.
- Create documentation on steps of implementation for easy reproduction of builds..
- Assisted initial roll-out of the CI/CI pipeline, implemented services essential for build automation such as Urban Code Deploy and Jenkins.
- Successfully lead multiple initiatives for service implementations (SiteMinder, Apache, Tomcat, MongoDB, and MongoBI Connector)
- Submit required ticket requests using Remedy and Service Now to have essential infrastructure provisioned across multiple environments for various stages of development.

University of Phoenix / On-Prem

07/2014 - 11/2018 — **LINUX SYSTEMS ADMINISTRATOR**

Linux Systems Administrator for the IT Operations Center, tasked to ensure the availability and performance of campus web-based infrastructure for students and staff. Duties included administering both physical, VMware, and cloud based infrastructure running Windows and UNIX-based servers and applications.

Core Responsibilities

- 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.

Brinkster Communications / On-Prem

02/2011 - 06/2014 — **HELP DESK LEAD**

Help Desk Lead providing chat and ticket support, administration of shared hosting, VPS, and dedicated server clients. Other duties include data-center operations, administration of MySQL, Microsoft SQL Servers, virtualization hosts (XenServer & VMware), and Zimbra mail environments.

Core Responsibilities

- 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.
- Management of customer DNS records using Brinkster name servers.
- Administration of Databases, Windows, Linux, VMware, Citrix XenServer, and Zimbra mail environments.
- Build-out hardware for dedicated server orders.

Education

Freeport High School (2004) / Diploma

Military

US Army - Fort Bliss, TX (2009 to 2011) / **MOS:** 91D