Jordan Slack

Cloud Security Engineer

Results-oriented security professional with expertise in Azure security and Microsoft Sentinel. Skilled in scripting with Python and PowerShell to find creative ways to automate solutions. Experienced in migrating from ARM deployments to Terraform and Ansible playbook creation. Double major in DevOps and Cybersecurity and seeking an opportunity to leverage skills and knowledge as well as continue professional growth within the DevSecOps space.

Work History

2023-06 - Current

Cloud Security Engineer

Dataprise

- Azure Security Implementation: Spearheaded development of a robust cloud security architecture across multiple client environments, focusing on Azure Sentinel for advanced threat detection and response
- Automation and IaC Deployment: Automated ARM template deployments and transitioned to Terraform for infrastructure as code (IaC) best practices, enhancing operational efficiency and security posture
- Created Ansible playbooks for centralized configuration management and patch cycling
- Network Security Management: Configured VPN tunnels and syslog relays in Azure, ensuring secure data transmission and efficient CrowdStrike and firewall log ingestion
- Linux System Administration: Utilized Bash and PowerShell scripts to maintain and automate tasks across a vast inventory of Linux VMs, improving system reliability and performance.

2022-06 - 2023-06

Security Operations Engineer

ReliaQuest

Contact

Address
Las Vegas, NV 89142

Phone
608-636-3886

E-mail
slack.jordan@outlook.com

WWW
https://bold.pro/my/jordan-slack/185r

Skills

Microsoft Sentinel

Python

Powershell

Terraform

Ansible

Syslog Ingestion

VPN

Linux & Windows

Network Security

IaC

CI/CD

CrowdStrike

Splunk

- SIEM Solutions Expertise: Resolved complex issues in SIEM technologies (Splunk, QRadar, LogRhythm)
- Configured and troubleshot multiple SIEM technologies and integrated log sources
- Vendor Collaboration: Acted as a liaison with technology vendors to resolve critical issues, enhancing customer environments' security and performance
- Linux and Network Troubleshooting: Diagnosed and rectified Linux server and networking problems, employing Bash scripting for efficient problem-solving.

2021-01 - 2022-06

Cybersecurity Engineer

Spectrum Brands

- Security Dashboard Development: Led creation of security management dashboards, integrating vulnerability scanners and compliance reporting tools for enhanced visibility and control
- Created with Power BI and custom Python scripts to pull and organize data
- Automation with Scripting: Developed Python scripts to automate security reporting through API calls from security tools, significantly reducing manual effort and improving accuracy
- Code Collaboration: Leveraged GitHub repositories and Git CLI for collaborative development, ensuring high code quality and efficient project management.

Education

2020-09 - 2023-05

Associates - DevOps

Madison College - WI

2020-09 - 2022-05

Associates - Cybersecurity

Madison College - WI

Hobbies

Music - Have played in bands since I was 16, playing guitar for over 20 years.

QRadar

Git/GitHub

APIs

VMware

Active Directory/Azure AD

LDAP

Vulnerability Scanning

Penetration Testing

SSO

Firewalls

Agile

Technical Documentation

Project Management

Systems Administration & Engineering

Hacking

ServiceNow

Programming - Learning web development and creating personal projects. Working on a web scraper for finding the cheapest sailboats across the country on craigslist and an online radio station with my friends using all open source software.
Home Lab - I host my own ESXI server at home for testing new open source software and Linux distrobutions.