

Josiah Ledbetter
Austin, TX, 78752
(512) 554-8976; jobs@jowj.net

Qualifications

- Security engineer and programmer with a focus on automation, documentation, and vulnerability management.
- Comfortable in cloud, on-prem, and hybrid environments.
- Proven history of building consensus to tackle organization-wide issues.

Skills

- Python
- Powershell
- Ansible
- Docker
- GCP, AWS
- Vulnerability scanning
- SIEM administration
- Antivirus administration
- Rapid7 Nexpose
- Rapid7 InsightIDR
- Splunk
- xSOAR
- Orca Security

Professional Experience

Unity3d, February 2021 - Current

Sr. Information Security Engineer at Unity3d, June 2022 - Current
Information Security Engineer at Unity3d, February 2021 - June 2022

- Brought structure to existing ad-hoc processes for vulnerability response.
 - Wrote Python scripts to automate ticket creation from scanner events.
 - Automated regular reporting tasks in Python and Pandas.
 - Built Ownership Automation service to populate and store ownership info for cloud projects.
 - * Automated data collection through account-wide IAM + granular JIT access provisioning integrations.
 - * Reduced ticket assignment toil from over 30 hours / week to ~1.
- Engaged with the broader security community to keep informed of vulnerability news as it happens.
- Researched newly announced vulnerabilities to determine company exposure and proportional response.

- On multiple occasions reduced false positive noise from scan engines from thousands of alerts to zero based on faulty CPEs.

Planview, May 2019 - February 2021

Information Security Engineer

- Created Slack-based application to manage incident response alerts from Rapid7 IDR.
 - This was later used as a system of record for SOCII compliance.
- Created a scanning and remediation process for all products under the Planview umbrella.
- Rolled out Powershell, Macroscript whitelist initiative to all employees through Cylance.

Volusion, October 2011 - May 2019

Information Security Engineer, 2017 - 2019

Systems Engineer, 2015 - 2017

Sr. Network Operations Specialist, 2012 - 2015

Tech Support, 2011 - 2012

- Built out Rapid7 Nexpose infra to decrease scan times from > 24 hours to < 8.
- Spearheaded compliance efforts with PCI and internal security policy.
- Migrated 40,000+ IIS sites from Windows Server 2003 to 2012 R2.
- Created SQL cluster build automation in Powershell to decrease department turn-around time during physical cluster builds from ~1 week to ~1 day.

Open source projects

- pynit: an automatable way to sync reddit saved-posts to pinboard.
- jowj.net: an experiment in running a blog using orgmode and elisp.

Other

- Experience with PCI, SOCII compliance frameworks
- Intermediate trapeze skills
- Avid bicyclist
- CompTIA Sec+ (expired)