

Joshua (Jim) Evans

Personal Profile

- Risk-mitigation oriented mindset, with close attention to protecting and expanding organizations by employing technological and security based solutions.
- Maximizing available resources through heavy automation to best run Agile InfoSec, Ops, and DevOps teams / solutions.

Professional Experience

Systems Administrator II – Linux & Web (Nat. Severe Storms Lab), Norman, OK • Dec. 2019 – Present

- Dockerized and deployed high-traffic, public-facing authentication proxy, for secure distribution of lab published data-sets and models.
- Responsible for ensuring both the public and internal availability of <https://nssl.noaa.gov/>, and all the heavily relied upon meteorological Web Applications hosted therein.
- Maintained day to day operation of the 120 RedHat 6 and Centos 7 Linux servers for the NSSL's Multi-Radar Multi-Sensor (MRMS) product, an internationally implemented forecasting solution. More information available here: https://mrms.nssl.noaa.gov/qvs/product_viewer/
- Deployed user management tooling for the MRMS project via Ansible, allowing for higher accountability in auditing as well as normal operation.
- Restructured MRMS system update pipeline, via multipronged effort from Google Forms, Python, and Ansible, to develop a more autonomous patching solution with much greater product owner visibility, while maintaining compliance with federal system regulation.

Systems Engineer. Legend Energy Services, OKC, OK • May 2018 – Nov. 2019

- Recovered withheld credentials for local resources, including BackupExec and ShoreTel Director using red team tools and methods (NMAP, Metasploit, and JohnTheRipper).
- Remediated on-going security breeches and present system vulnerabilities, which were the main cause for my on-boarding with Legend Energy.
- Implemented Proofpoint - Email Protection Gateway in front of Office 365 tenant, combating rampant phishing and impersonation attacks occurring within company.
- Moved on-prem File Share and Domain Controller server infrastructure to redundant Virtual Machines on equally redundant ESXi 6.7 hosts.
- Stood up IDS/IPS system (DarkTrace) to better view and respond to security threats, while remaining a lightweight IS team.
- Evaluated and eventually terminated relations with partner MSP, which was replaced with in-housed IT.

- Performed full Permissions Audit and restructure on sensitive data systems, to ensure proper data security through established practice.
- Re-architected Palo Alto FireWall implementation and rules, from previous insecure configuration and practices.
- Conducted Site Surveys of five field offices across Texas, N. Dakota, and Oklahoma, to provide timelines and priorities on infrastructure End of Life replacements.
- Simulated live phishing attack to measure actual user susceptibility and provide training opportunities using open-source attack tools.
- Set-up redundant ISP connections to Corporate office with auto-failover, via Palo Alto Policy Based Forwarding rules, later transitioning ISP's completely from Cox to AT&T.
- Troubleshoot and fixed controller units on Live Coil Tubing, and fracking operations, while actively "down-hole".
- Security Audited AWS hosted customer facing WebApp, running on Clojure and TimeScaleDB.
- Administrated Legend's AWS cloud services, primarily ec2 instances and IAM User Management.
- Integrated multiple SaaS providers under SAML SSO Authentication, to ease user "password overload".
- Wrote and deployed hotfix to production-critical internal C# Application, hosted on Coil Tubing Controller Units.
- Consulted with newly formed internal development team to architect Data Collection as a Service platform using DevOps tooling (Ansible, Private Github Repositories, and Custom Inventory Management integrations) and principles (IaC, CI/CD) on asynchronous, distributed data collector nodes.

IT Analyst II – InfoSec. University of Oklahoma Libraries, Norman, OK ▪ Apr. 2017– May 2018

- Performed a full Active Directory and File Share Permission Audit and Reorganization to streamline future Access Control management.
- Conducted a full Password Management Utility (LastPass) Permission Audit and Reorganization, to ensure appropriate System management access.
- Brought Internal Antivirus into compliance by using network-scanning utilities to locate unsupported AV Products and replace them with Dell DDP (Rebranded Cylance).
- Planned and led a full IT Asset Inventory Audit to ensure financial accountability. This was the first IT Inventory performed at University Libraries.
- Additionally, functioned as Co-Manager of IT Interns, and often acted as a Tier III Escalation point for front facing issues, by nature of previous OU experience.
- Automated IT Related Employee On-boarding and Off-boarding procedures using Powershell, increasing department turnaround time and uniformity.
- Instituted FDE for all Financial and HR Staff, to decrease risk of Data Loss.

- Performed Monthly Vulnerability scanning and analysis using OpenVAS.
- Automated Backups and Business Processes of several secondary systems and resources, mainly by leveraging Powershell. As well as developing Automation Solutions for time-sensitive unique technology challenges.
- Maintained Several On-Premises Windows 2012 R2 Virtual Machines located on a single ESXi 5.5 node.
- Managed various On-Premises Application Systems, including Laserfiche, QuickBooks, WSUS, IIS Webservers, and Library Specific Proprietary Software.
- Drafted and Implemented an Information Security Policy, InfoSec Incident Response Policy, and other Security Related Documents, resulting in an external IT Audit having no written change recommendations.
- Aided in Internal Server Hardware Relocation and Disaster Recovery planning and implementation, while maintaining a high degree of up time for internal staff and campus wide resources, by leveraging existing hardware and VMWare vMotion Utilities.
- Recommended, helped institute, and sat as a charter member on the University Libraries Internal Change Management Board.
- Worked closely with the DevOps team to design secure deployment practices and features, via Ansible roles and Vault.

IT Administrator. Revenue Management Solutions, OKC, OK ▪ Dec. 2015 – Apr. 2017

- Maintained and serviced 90+ workstations and 140+ physical and virtual servers over a WAN spanning 3 locations using RDP, PuTTY, and vSphere utilities, as half of a two-man IT Department for a SaaS company.
- Administered 90+ Windows 2008 and 2012 R2 Servers, as well as 75+ Ubuntu 14 LTS Servers.
- Oversaw Active Directory and Microsoft Exchange Server tasks via Powershell and MMC, including Group Permission Administration, Distribution Group Setup, and General User Creation/ Removal.
- Edited and Enabled Group Policy to conform environment to meet external security standards.
- Protected critical infrastructure from external threats via AlertLogic Vulnerability Scanner, Barracuda Load Balancer, Barracuda Web Application Firewall, and Palo Alto FireWalls.
- Planned and deployed a Linux Security Patch Management policy by using Aptly to build and maintain local repositories of approved security updates.
- Tested and deployed Office365 into a production environment.
- Remediated network transfer issues between clients and RMS's GlobalScape EFT SFTP server.
- Installed and configured ESXi 5.5 servers in a production environment, as well as troubleshoot any outages in their service.

- Responsible for the upkeep of Software and Hardware inventory records, primarily using SpiceWorks.
- Diagnosed network outages and connectivity issues by analyzing network traffic with WireShark.
- Designed and implemented a 100+ user and infrastructure office move, in the span of one week, with only 45 minutes of planned downtime, total.
- From December 15, 2016 until February 10 2017, I was the only IT Employee for the business, and was able to get us through a successful sale of the company.

IT Assistant – College of Arts & Sciences IT, Norman, OK ▪ September 2013 – September 2015

- Provided College Faculty and staff with on-site and on-location technical support for software, hardware, and networking/domain issues
- Successfully redesigned, rewired, and renovated Graduate computer lab with 20+ workstations unsupervised using Clonezilla mass deployment.
- Managed hardware deployment, repair, and inventory, with Symantec Ghost as primary imaging software.
- Trained incoming co-workers, while helping to re-enforce a more sociable, user problem-solving IT environment.
- Strove to aid the department with simple Powershell and VBA scripting, aiming to reduce turnaround times and increase professionalism.

Data Entry Specialist – Axis Practice Solutions (Now Defunct), Norman, OK ▪ April 2012 – September 2012

- Filed Medicare/ Medicaid patient claims for several medical offices and institutions requiring HIPPA compliance.
- Used Microsoft Excel 2010 extensively, increasing company efficiency with distribution of VBA macros.

Programming and Software Skills

- Familiar with Powershell, Ansible, and BASH, as well as minor experience with Ruby, Python, C, C++, and C#.
- Hands on experience with MSSQL, PostGresSQL, Relational Databases.
- Maintained Private and Public GitHub Repositories for personal and enterprise use.

Education and Accolades

- High School Diploma – Norman North, Norman, OK ▪ 2012
- Attended University of Oklahoma – 2012 to 2015
- Vice President of Classics and Letters Honor Society

- Completed Comptia Security+ Certification in November 2017.