Drew Sousa

[**w: drewsousa.com**] - [e: ██@drewsousa.com] - [m: ██████] - [**linkedin.com/in/drewsousa**]

15+ years of hands-on success designing, deploying, managing, & securing development & production systems processing sensitive healthcare data in public & private clouds

Skills

`Security` `SecOps` `SIEM` `IDS` `IPS` `NOC` `SOC` `DAST` `Firewalls` `Load Balancers` `WAF` `Syslog` `Multi-Cloud` `Virtualization` `Architecture` `Supply Chain` `S-SDLC` `HIPAA compliance` `NIST 800-53`

Security: MFA, PKI, HSM, OSINT, DAST, Threat Hunting, Vulnerability Assessment, Mitre ATT&CK, & OWASP
Infrastructure: Virtualization, Hypervisors, Micro-segmentation, Containers, Firewalls, WAF, VPN, & VDI
Clouds: Private (VMWare), Hybrid, AWS, Azure, GCP. Zealot for IaC, SecOps, & Automation
Programming: Mostly shell scripting & working with interpreted languages. Enthusiastic Python student

Experience

Research Sabbatical / Non-Compete

2021-2022 | Grass Valley, CA

- Automation: SaaS, IaC, IaaS, CI/CD, Ansible, Docker, & Terraform
- Security & Privacy: SecOps, CI/CD vulnerability scanning, SBOM automation, Layer7 WAF, OSINT, & OWASP
- Threat: Identifying, modeling, reducing, mitigating, & eliminating risks & threats to organizations

Edifecs - Senior Director, Architecture, SaaS, & Security

2016-2021 | Bellevue, WA & remote

- Architected & managed 100+ vertical SaaS B2B environments exceeding SLA uptime & security requirements
- Established the Risk Management Council as well as Threat Modeling & Information Security Standards
- Lead member of the Architectural Review Board reviewing and advising on documentation, data flows, & security
- Hands-on lead for penetration testing, vulnerability management, & security from Dev to Prod
- Set up & managed CI/CD security, DAST & SAST systems, participated in code reviews, & SDLC audits
- Deployed MFA, SIEM, EDR, built the SOC, & personally configured security rules & alerts on production systems
- Led P2C migrations and security architecture from private to public clouds (Azure, AWS, & GCP)

Technologies: VMWare, Cisco, F5, Multi-cloud [OnPrem, AWS, Azure, & GCP], SolarWinds, & Acunetix

Edifecs - Director, Architecture, SaaS, & Security

2005-2016 | Bellevue, WA & remote

- Personally built Edifecs SaaS private cloud infrastructure & team from the ground up
- Service owner for 100+ production services including software supply chain security
- Fast-tracked P2V migrations for hundreds of physical servers into geographically dispersed data centers
- Led domestic & international teams in 24/7/365 production environments with high talent retention
- Built & managed source code repositories, build servers, & defect tracking systems for Product & Engineering
- IT, SaaS, and Security lead for achieving and maintaining HITRUST certification

Technologies: MS Windows, Linux, Apache, MySQL, MS SQL, VMWare, VDI, Nessus, Netwrix, SVN, & GIT

Edifecs - IT & Security Engineer

2000-2004 | Bellevue, WA

- Thrived as the only IT engineer for the company supporting all IT services, systems, & departments
- Built & supported site-to-site Wi-Fi to connect Edifecs teams spread across a a business campus
- Implemented physical security controls, policies, & procedures for CCTV, badge readers, and ID cards
- Kept expenses to a minimum by hand-building firewalls, routers, & web servers with FreeBSD & Linux
- Deployed & managed Active Directory, email & Exchange Servers, & implemented an issue tracking system

Technologies: Active Directory, MS Exchange, Postfix, CVS, FreeBSD, & Bugzilla

Liberty American - Web Developer & IT Engineer

1991-2000 | Roseville, CA

- Moved company into the modern era by deploying internet, email, & workstations to all associates
- Leveraged open source software to build Linux firewalls, routers, & file servers
- Transformed workflow by successfully migrating 30+ physical fax machines to a paperless system
- Designed & coded company website allowing brokers to track their loan submission status in real-time

Technologies: Novell, Linux, ASP, HTML, PERL, MS Windows, Visual Basic, & Sendmail

Education

- BA in Organizational Communication, CSUC (1991)
- Certified HiTrust CSF Practitioner (2016 - 2019)