Max Segura

maxell.segura@gmail.com | Sacramento, CA | securityshards.wordpress.com | [LinkedIn URL]

SUMMARY

Security-focused infrastructure leader with 10+ years of progressive experience spanning endpoint security, network architecture, compliance engineering, and SecOps. Proven track record of designing and operationalizing security programs, leading incident response, and hardening enterprise environments across cloud and on-premises infrastructure. Recognized by Google and Western Union for responsible vulnerability disclosure.

KEY SKILLS

Cloud Azure | Entra ID | MFA | Enterprise Applications | Azure Arc | Microsoft 365 | Intune | SIEM | EDR/XDR/SOAR | Tenable/Rapid7 | Action1 | Microsoft Defender | Purview DLP | Incident Response | Vulnerability Management | Threat Hunting | 802.1X | Zero Trust | NIST, CIS, HIPPA | DevOps | Linux | Active Directory | Citrix VDI | Firewall Policy | VLAN Design | Disaster Recovery | Network Architecture | PowerShell | Python | API Integration | AI Adoption | VMWare/Hyper-V | SSO | Veeam | IAM

PROFESSIONAL EXPERIENCE

Infrastructure Security Engineer - Royal Electric Company, Sacramento, CA
June 2025 - Present

- Architected and deployed Prometheus/Grafana observability stacks for real-time monitoring of server health, infrastructure performance, and security telemetry across distributed environments
- Drove end-to-end vulnerability and patch management using Tenable and Action1, prioritizing and remediating findings
- Deployed and operationalized a SIEM platform for centralized log ingestion and real-time threat detection, reducing the time to detect across the environment
- Engineered 802.1X certificate-based authentication via NPS, NDES, and Intune SCEP, enforcing zero-trust Wi-Fi access control across all corporate network segments
- Administers Microsoft 365 and Azure environment including Entra ID, Conditional Access, Enterprise Applications, Azure Arc, Intune MDM, and Defender suite, managing identity and device compliance
- Led high-severity incident response engagements including threat containment, forensic analysis, and executive post-incident reporting
- Implemented Microsoft Purview data classification and DLP policies across Exchange, SharePoint, and endpoints to protect sensitive and compliance-regulated (CUI) data
- Designed and delivered a full disaster recovery program from the ground up encompassing strategy, network architecture, data separation, replication, and documentation
- Aligned security controls and operational practices to NIST CSF and CIS Controls v8, establishing a measurable, auditable security posture and laying groundwork for formal compliance readiness

IT Manager - Royal Electric Company, Sacramento, CA
June 2022 - June 2025

- Mentored and developed IT staff, establishing growth frameworks that resulted in internal promotions
- Partnered with IT Director on infrastructure design, technology roadmaps, and hardware procurement
- Developed cross-platform workflows via API integrations using Powershell and Python
- Championed zero-trust security practices organization-wide, serving as the internal infosec SME
- Designed and managed Linux server infrastructure and Docker containerization across production environments
- Led network architecture decisions including VLAN segmentation design

- Conducted comprehensive audits covering hardware inventory, software licensing, and user accounts

Systems Administrator - Royal Electric Company, Sacramento, CA
June 2019 - June 2022

- Designed and maintained Citrix VDI environments supporting non-persistent environments
- Hardened perimeter and internal network through firewall policy best practice configuration
- Deployed and managed EDR for enterprise-wide endpoint protection across the full device lifecycle
- Migrated on-premises workloads to the cloud, reducing infrastructure overhead and improving scalability
- Stood up 4G-connected remote site infrastructure, including full topology design and hardware deployment
- Automated server deployments and configuration using VM Templates and GPO
- Automated recurring administrative tasks via PowerShell, reducing manual effort and human error

Systems & Network Administrator - River Oak Center for Children, Sacramento, CA
March 2016 - June 2019

- Designed and managed agency-wide LAN/WAN infrastructure
- Configured and maintained Network Security Appliance firewalls
- Administered Active Directory and Microsoft Exchange, managing identity lifecycle, group policies, and mail services
- Responsible for server maintenance, updates, upgrades, uptime, functionality, and reliability
- Develop systems and automated tools for various tasks using Powershell
- Ensured disaster recovery readiness through documented plans and validated backup procedures

EDUCATION

- B.S., Information Technology - Western Governors University
- A.S., Computer Information Systems - Camden County College
- Cyber Aces Program - Brookdale Community College

CERTIFICATIONS

- CompTIA: Security+, Network+, Project+
- Linux Professional Institute (LPI): Linux+ / LPIC
- CIW: Javascript Specialist, Database Design, Web Design Specialist

ACHIEVEMENTS

Western Union Bug Bounty Hall of Fame - Bugcrowd
Recognized for responsibly disclosing a critical security vulnerability in Western Union's platform.

Google Security Hall of Fame - Google
Recognized for responsibly disclosing multiple security vulnerabilities across Google properties.

Cyber Security Competition State Finalist - SANS / CyberAces
Placed as a state finalist in a SANS-sponsored hacking competition at Brookdale Community College.