ULISES PAIZ

Systems Engineer | Windows Infrastructure & Automation | Active Top Secret Clearance

Salinas, CA | Contact@UlisesPaiz.com | linkedin.com/in/ulises-paiz | github.com/Coach40oz

SUMMARY

Windows systems engineer, seven years across DoD classified networks, semiconductor compute platforms, and managed multi-client environments. SME-level MECM/SCCM, OS image engineering, and PowerShell automation, with hands-on incident response and network architecture experience. Known for deployments that do not roll back. Active DoD Top Secret clearance.

TECHNICAL SKILLS

Endpoint & Platform: MECM/SCCM (SME), OS image engineering, Task sequences, WinPE / PXE, DISM, Driver management, Windows 11 Enterprise, Windows Server 2003–2025, PSADT, Datto RMM, Autotask PSA

Automation: PowerShell (advanced), Python, Bash, Deployment pipelines, Configuration management, Compliance scripting

Cloud & Identity: Azure (AZ-104), Microsoft 365, Intune, Windows Autopilot, Entra ID, Conditional Access, Exchange Online

Security & Compliance: STIG, NIST 800-53, CIS Benchmarks, EU Cyber Resilience Act, GPO security baselines, Microsoft Defender, Tanium, ACAS, Nessus, Mend (SCA), BeyondTrust PAM, Wazuh SIEM, Huntress EDR, Incident response

Infrastructure: Active Directory, DNS, DHCP, VLANs, Hyper-V, Proxmox, SonicWall, Sophos, pfSense, Aruba / UniFi, IDS/IPS, Site-to-site VPN, Structured cabling

PROFESSIONAL EXPERIENCE

SYSTEMS ENGINEER (Contract via Quest Global) **Mar 2026 – Present**

KLA Corporation | Milpitas, CA (Hybrid)

Embedded with KLA's compute infrastructure team building the Windows platform behind AI-driven semiconductor inspection systems.

- Engineer a hardware-agnostic Windows Server 2025 golden image covering seven server variants for high-performance inspection compute clusters, from driver strategy through release documentation.
- Led the EU Cyber Resilience Act (CRA) vulnerability assessment across 40 semiconductor inspection tools ahead of the September 2026 reporting deadline, combining Nessus host scanning with Mend software composition analysis.
- Built the WinPE deployment pipeline in PowerShell: bootable media, DISM image apply, offline driver injection, and an interactive console interface for deployment technicians.
- Wrote an automated conformance suite (50+ checks) that validates every image build against the platform specification before release.

SENIOR SOLUTIONS CONSULTANT (Systems Engineer) **Oct 2022 – Mar 2026**

Deloitte Consulting LLP | Defense Manpower Data Center (DMDC), DoD | Seaside, CA

MECM subject matter expert and PowerShell automation lead for approximately 2,000 endpoints on DMDC classified and unclassified networks.

- Supported the enterprise Windows 11 migration on the unclassified network, coordinating testing and deployment with the project team to reach 100% STIG compliance with zero rollbacks.
- Built a PSADT packaging framework that turned multi-hour manual application installs into one-click deployments and drove failure rates to near zero.
- Rebuilt the OS deployment pipeline (MECM, PXE, custom WinPE), cutting image time from 6 hours to 2, and cleared a BeyondTrust/MECM integration conflict that had stalled deployments across the environment.
- Engineered the Group Policy architecture enforcing STIG and NIST 800-53 controls, with automated compliance monitoring; partnered with the Tanium and ACAS teams on patching and vulnerability management.
- Go-to escalation point for task sequences, application packaging, and deployment troubleshooting across the project team.

SYSTEM ADMINISTRATOR **Jul 2019 – Jul 2022**

MBS Business Systems | Salinas, CA

Primary engineer and de facto systems architect for 42 client sites (1,100+ endpoints, 800 users), owning design, procurement, build-out, and Tier 1–3 support.

- Led hands-on incident response for ransomware and business email compromise events: containment, root-cause analysis to close the initial access vector, and full environment rebuilds for organizations with no usable backups. Converted these engagements into recurring managed-service clients.
- Ran emergency Log4j (CVE-2021-44228) remediation across all client environments within days of disclosure; separately detected and shut down unauthorized mailbox access during a security audit, stopping an active breach.
- Built the MSP's service delivery stack from the ground up: Datto RMM monitoring, patch management policies, and automation, plus Autotask ticketing and client intake.
- Architected client networks end to end, from requirements and equipment specs through structured cabling and deployment; replaced end-of-life firewalls with SonicWall, Sophos, and pfSense, configuring ACLs, IDS/IPS, VLAN segmentation, and site-to-site VPN.
- Led Windows Server migrations from 2003, 2008, and 2012 R2 to Server 2016 and 2019, and moved clients from on-prem AD, file, and mail servers to Azure AD, Microsoft 365, Intune, and Autopilot; built Hyper-V and Proxmox virtualization platforms.
- Authored the company's technical standards, SOPs, and the PowerShell tooling the team standardized on; trained and mentored 5 new technicians.
- Partnered with sales and business owners on pre-sales engineering: scoped solutions, specced hardware, built quotes, and joined owner meetings to close major projects.

OPEN-SOURCE PROJECTS

github.com/Coach40oz | PowerShell tooling, all public, built to solve real problems

- **Windows-SecurityBaselineAuditor:** Audits Windows systems against CIS, NIST, and Microsoft hardening baselines
- **W11Upgrade:** Automated Windows 11 upgrade path for unsupported hardware

CERTIFICATIONS & EDUCATION

Clearance: Active DoD Top Secret

CompTIA: SecurityX (CAS-005) | CySA+ | PenTest+ | Security+ | Network+ | Cloud+ | Project+

Microsoft: Azure Administrator Associate (AZ-104)

Other: ITIL 4 Foundation | Linux Essentials (LPI)

M.S. Cybersecurity & Information Assurance, Western Governors University | 2026

B.S. Networking & Cybersecurity, Western Governors University | 2025