

KEVIN BROWN

Senior Systems & Cybersecurity Engineer | Incident & Ransomware Restoration

Cincinnati (Lebanon, OH) | +1 (513) 292-4664 | kbpc.inc@gmail.com | LinkedIn:
<https://www.linkedin.com/in/itkevinbrown> | <https://www.stbcybersecurity.com>

EXECUTIVE SUMMARY

Results-driven Senior Systems & Cybersecurity Engineer with 17+ years of experience executing zero-loss incident and ransomware restoration operations across complex enterprise environments. Expert at bridging deep systems engineering, virtualization, and cybersecurity to perform rapid, secure infrastructure recoveries following catastrophic cyber events, data corruption, and severe outages. Proven track record of slashing enterprise restoration timelines by 50%, maintaining 100% data integrity across bare-metal and hybrid-cloud rebuilds, and guiding executive leadership and technical teams through high-stakes system recoveries.

CORE COMPETENCIES & TECHNICAL ARSENAL

- **Incident & Ransomware Restoration:** Ransomware Recovery & Remediation, Bare-Metal Server Restoration, Post-Breach Infrastructure Reconstruction, Digital Forensics & Incident Response (DFIR), Threat Hunting & Eradication, Zero-Trust Hardening, Business Resumption & Automated Recovery Runbooks.
- **Cybersecurity, EDR & Forensics Tooling:** SentinelOne, Huntress, Velociraptor, CyLR, Cloudflare (WAF & Zero-Trust), Duo MFA, Endpoint Hardening, Identity & Access Management (IAM), SIEM & Logging Telemetry, SOC, Security Framework.
- **Virtualization, Cloud & Storage:** VMware (vSphere, ESXi, vCenter, vCloud Director), Microsoft Hyper-V, Citrix (XenApp), AWS, Azure, Microsoft 365 / Exchange, SAN & ZFS Storage, Enterprise Backup, Replication & High-Availability Failover.
- **Systems Engineering & Automation:** Windows Server, Linux (RHEL, Debian, Ubuntu, CentOS), Unix (Solaris/SunOS, HP-UX), Active Directory / OpenLDAP, SQL Server Clusters, PowerShell, Bash, Python, Ansible, AI Agents & Automated Fleet Orchestration.

PROFESSIONAL EXPERIENCE

CFC / Solis Security — Austin, TX (Remote)

Business Resumption Engineer

January 2024 – August 2026

Deployed into active cyber incidents and full-scale ransomware engagements at a senior engineering level to architect and execute zero-loss infrastructure restorations and enterprise system recoveries.

- **Rapid Ransomware & Incident Restoration:** Engineered and deployed scalable recovery workflows and automated runbooks that slashed enterprise restoration windows by 50% during active threat actor engagements.
- **Zero-Loss System Recovery:** Executed bare-metal server, core application, and network restorations following total ransomware encryption events, maintaining a 100% data integrity record across all recovery deployments.
- **Senior Technical Advisory & Execution:** Partnered directly with C-suite stakeholders and IT leadership during critical outages to translate catastrophic infrastructure failures into structured, predictable restoration roadmaps that consistently beat strict RTO and RPO targets.
- **Threat Mitigation & Post-Breach Hardening:** Enforced zero-trust architecture and leveraged advanced EDR/XDR telemetry (SentinelOne, Huntress) to neutralize persistent threats prior to returning rebuilt VMware vSphere, hybrid-cloud, and Windows/Linux systems to production.

Fenix24 — Chattanooga, TN (Remote)

Cyber Disaster Recovery Engineer III

February 2023 – December 2023

Operated as a senior systems and recovery engineer in post-breach enterprise environments, partnering alongside external DFIR teams (including CrowdStrike) to eradicate threats and reconstruct compromised networks.

- **Enterprise Infrastructure Reconstruction:** Executed rapid, large-scale system restorations across bare-metal hardware, multi-cluster VMware environments, and public cloud deployments spanning Windows, Linux, and Citrix architectures.
- **Identity & Access Architecture Rebuilds:** Reclaimed compromised domains by rebuilding and hardening Active Directory and LDAP forests from the ground up, enforcing strict Duo/MFA protocols, and securing Microsoft Office 365 environments.
- **DFIR Integration & Threat Eradication:** Collaborated directly with forensics teams for deep network discovery, embedded rootkit hunting, and active ransomware payload neutralization prior to infrastructure reconstruction.

- **Security Telemetry & Data Protection:** Deployed custom-scripted EDR/XDR and SIEM logging solutions to establish zero-trust visibility, while auditing and hardening enterprise backup silos to prevent secondary extortion.

KORE Wireless — Cincinnati, OH

Systems Engineer II

June 2016 – December 2022

Served as a senior core infrastructure engineer designing, automating, and maintaining on-premise and hybrid AWS/Azure cloud environments for global IoT and telecommunications operations.

- **High-Availability & System Recovery:** Architected and managed production backup pipelines, server/storage replication, and automated failovers across VMware clusters, Hyper-V hosts, Containers, and SQL Server clusters spanning multiple data centers.
- **Global Telecom & IoT Infrastructure:** Engineered and maintained zero-downtime infrastructure supporting mission-critical IoT platforms (SMSC, SMPP, SMS-R, LTE, ESME, and MVNO gateways) across 180+ global carriers.
- **M&A Migrations & Automation:** Led senior technical execution for corporate acquisitions, multi-datacenter migrations, and DEV/QA/Staging environment automation while serving as Tier 3/4 escalation across global engineering teams.

PVDC Hosting, LLC — Orlando, FL

Systems Administrator

July 2014 – June 2016

- Engineered, deployed, and upgraded large-scale multi-datacenter, multi-tenant VMware vCloud Director (vCD), vSphere, and vCenter clusters.
- Delivered resilient, healthcare-compliant virtual datacenter, hosted application, and virtual desktop infrastructures across enterprise Linux and Windows server farms.

Unixdev Hosting Solutions — Cincinnati, OH

Senior Systems Engineer

December 2009 – November 2016

- Directed technical deployments across six US data centers, managing 1,300+ virtual machines (VMware, Xen, OpenVZ) and 265 dedicated bare-metal Linux/UNIX and Windows servers.
- Architected scalable shared, virtual, and dedicated hosting environments supporting 3,000+ client websites and 380+ business accounts.

EARLY ENTERPRISE CAREER HIGHLIGHTS

- **Systems Engineer | Global Business Solutions, Inc.** (August 2011 – July 2014): Designed, migrated, and administered multi-client enterprise networks, SLAs, and high-volume VMware, Citrix, and Hyper-V server environments.
- **Systems Administrator & Integration Analyst | GE** (November 2010 – August 2011): Administered L2 Unix/Linux infrastructure (Solaris/SunOS, HP-UX, RHEL), Bash/Perl automation, RSA SecurID 2FA, and an enterprise NIS-to-OpenLDAP/Active Directory migration supporting 125,000 global users.
- **EPIC Deployment & Infrastructure Team Lead | St. Elizabeth Healthcare** (February 2010 – November 2010): Led infrastructure rollout and Citrix XenApp go-live for a \$9M EPIC EHR transformation across multiple hospital campuses, supporting 6,000 employees and 2,400 systems.

INDEPENDENT CYBERSECURITY & AI R&D PROJECTS

- **STB Cybersecurity — Creator & Lead Developer (2026 – Present)**: Built a proprietary three-tier incident response and restoration suite: **Vanguard** (portable plug-and-play tactical IR platform for live network remediation), **Garrison** (automated EDR monitoring agent), and **Lazarus** (bootable bare-metal recovery OS for offline triage and system resurrection).
- **Kevontix Labs — AI & Security Automation Developer (2026 – Present)**: Developing sovereign AI builders and autonomous multi-agent sandboxes utilizing OpenRouter, Claude, and DeepSeek on high-compute bare-metal hardware to streamline threat analysis and automate complex infrastructure workflows.

EDUCATION & CERTIFICATIONS

Education

- **Bachelor of Science in Computer Science** — Cincinnati State Technical and Community College & TechSkills

Professional Certifications

- VMware Certified Professional (VCP5-DCV)
- Cloudflare Certified Engineer (WAF & Zero-Trust)
- CompTIA A+ | Security+ | Network+ | Server+ | Linux+
- Microsoft Certified Systems Administrator (MCSA)
- Microsoft Certified Professional (MCP)
- Ethical Hacker Certification