# PAUL HERZ

IT Specialist | Security Focus

Airdrie, AB (Calgary Area) - Willing to relocate | Phone available on request | contact@herzpaul.com | herzpaul.com | linkedin.com/in/herzpaul

IT specialist with 10+ years in IT support, infrastructure and security across military, automotive and managed service environments. Support 500+ assets for 45+ Alberta clients across Microsoft 365, Windows Server, networking and endpoint management, with a strong security focus: zero data loss from phishing and business email compromise, and MFA adoption raised from under 40% to 75%. Information Systems Professional (I.S.P.), growing toward AI security and governance.

## CORE SKILLS

**Security Operations and Incident Response:** Incident response for BEC, phishing and vishing, SentinelOne EDR, SIEM and IDS monitoring, log analysis, MITRE ATT&CK, vulnerability and patch management, Nmap and Wireshark.

**Identity, Access and Email Security:** Microsoft Entra ID, Conditional Access, MFA rollout, Active Directory, Group Policy, Petra ITDR, SPF, DKIM and DMARC, Avanan and Defender for Office 365.

**Infrastructure, Network and Cloud:** Microsoft 365, Intune, Windows Server, Hyper-V, VMware, SonicWall and FortiGate firewalls, UniFi, VPN, network segmentation, and backups with Veeam, N-able Cove and Backblaze.

**Governance, Risk and Compliance:** ISO/IEC 27001, NIST CSF, PIPEDA, Alberta PIPA, CSA Z246.1, AER, GDPR, BSI IT-Grundschutz, Microsoft Purview, insurance-ready compliance documentation and security audits.

**AI Security and Adoption:** AI risk assessment, data privacy for AI tools, secure adoption of Microsoft Copilot, Claude and ChatGPT, and AI agent deployment.

**Leadership and Escalation Management:** Escalation point between management and technicians, onboarding and training new staff, team meetings, documentation standards, and personnel leadership in the military.

**Training and Security Awareness:** Security awareness programs, phishing simulations with uSecure and GoPhish, end-user training, technical documentation and SOPs.

**Scripting, Testing and Service Management:** PowerShell, Batch, Python, Git, Docker, test automation, ITIL, Scrum and Agile.

## CERTIFICATIONS

AI Cybersecurity and Governance, Columbia Engineering (In Progress) | Information Systems Professional (I.S.P.), CIPS Alberta | ISO/IEC 27001:2022 Security Officer, Professional and Foundation | ISO/IEC 19011:2018 Professional and Foundation | IT Compliance Manager, TÜV Rheinland | ITIL 4 Foundation | Lean Six Sigma Green Belt | Professional Scrum Master I and Professional Scrum Product Owner I | ISTQB Foundation and Advanced Level (Test Manager) | Certified Train-the-Trainer AEVO

## PROFESSIONAL EXPERIENCE

### User Support Technician

*March 2025 – Present*

Evolution IT (Evolution Group Corporate Services Inc.) | Calgary, AB, Canada

- Achieved zero data and financial loss across 30+ monthly phishing, BEC and vishing attempts by containing 1 to 2 account compromises per month with SentinelOne and Petra ITDR.
- Raised MFA adoption from under 40% to 75% of clients by initiating and leading a company-wide rollout with Entra ID Conditional Access.
- Reduced phishing click rates by 70% for 60+ users by running uSecure security awareness training and phishing simulations.
- Maintain 95%+ patch compliance across 500+ assets for 45+ clients by managing patching and vulnerability remediation via RMM.
- Protect 25+ client firewalls and 25 client backup environments by managing SonicWall, FortiGate, UniFi, Veeam, N-able Cove and Backblaze.
- Delivered insurance-ready compliance documentation for 4+ clients by mapping PIPEDA, PIPA, ISO 27001, NIST CSF, CSA Z246.1 and AER requirements.
- Manage 500+ assets alone two days a week after the team shrank from three to two by introducing documentation standards and team meetings.
- Guide clients' secure adoption of Microsoft Copilot, ChatGPT and Claude, and implement an AI agent (Hermes Agent) for email and alert triage.

**Freelance IT Security Consultant** *February 2023 – February 2025*

Self-Employed | Remote (clients in Germany)

- Reduced phishing click rates by 75% (from 40% to 10%) for 10 users across 5+ clients by running security awareness training and phishing simulations with GoPhish, uSecure and Wizer, including individual risk profiles.
- Hardened IT environments for 5+ small business and private clients by conducting security risk assessments, applying GDPR-aligned policies (BitLocker, password rules, patching), securing Microsoft 365 email and setting up backups.
- Earned 9 certifications, including ISO/IEC 27001 Security Officer, ITIL 4 Foundation and TÜV IT Compliance Manager, while building a security home lab with Wazuh, Microsoft Sentinel, Kali Linux and pfSense.

**Test Engineer** *April 2022 – January 2023*

e.solutions GmbH (CARIAD SE/Volkswagen Group) | Erlangen, Bavaria, Germany

- Cut test execution time by up to 60% (from 5 hours to 2) by automating manual test cases with SimUI scripting and Python, using AI-based visual comparison against reference images to flag defects automatically.
- Validated embedded infotainment and instrument cluster software for 3 vehicle programs (Bentley Bentayga, Audi A3, Audi A6) by running smoke, regression and verification tests with Vector CANoe, Polarion and Jenkins alongside Bentley's UK team.
- Tested access control, encryption and secure communication functions under strict automotive information security requirements, with exposure to ISO/SAE 21434 and UNECE R155.

**Senior IT Specialist, IT Security (Team Lead)** *January 2009 – December 2020*

German Federal Armed Forces (Bundeswehr) | Germany

- Trained 600+ personnel in cybersecurity awareness and led up to 60 personnel as technical escalation point, including performance reviews, promotion recommendations and leave planning.
- Secured 700 workstations for 800+ personnel in classified environments by monitoring SIEM, firewall and IDS alerts, correlating failed logons and containing incidents through account lockouts, password resets and network isolation.
- Rolled out 700 workstations across 3 barracks at the Wilhelmshaven naval base by planning a garrison-wide hardware deployment and testing new IT tools for security, stability and usability before release.
- Standardized secure printing for 45 printers across 3 barracks and all seagoing units by designing a framework with access control, network segmentation and centralized management.
- Hardened identity and endpoint security by administering Active Directory and Group Policy, deploying software through an enterprise endpoint management platform and running vulnerability scans in line with BSI IT-Grundschutz and GDPR.
- Earned a performance bonus (2017) and formal commendations (2014, 2017) for performance far above rank level, including negotiations with external IT providers such as BWI and cost-benefit analyses.

## EDUCATION

**Career Transition Program, Bundeswehr** *January 2021 – March 2022*

Technische Hochschule Nürnberg Georg Simon Ohm (TH OHM) | Nürnberg, Bavaria, Germany

Completed university coursework in engineering and Business Informatics at TH OHM as part of a structured transition from military to civilian IT.

**Bachelor Professional (EQF Level 6)** *May 2016 – February 2019*

Handwerkskammer für Unterfranken Würzburg | Würzburg, Bavaria, Germany

Business Computer Scientist and Business Data Processing Specialist.

## PROJECTS

**AI agent security testing:** Deployed an AI agent (Hermes Agent) in an isolated virtual machine and contained its attempt to escape the VM.

**Security home lab:** Built a lab with Proxmox VE, Microsoft Sentinel, Wazuh, pfSense, OpenVAS, Nessus and Kali Linux, plus KnowBe4 phishing simulations and TryHackMe and HackTheBox training.

**Home automation:** Built n8n workflows on Proxmox VE for office task automation and smart home control, including a self-built smart mirror.

## LANGUAGES

German (Native) | English (Fluent) | Russian (Conversational)