WALLY KROEKER

Security Architect

Elie, MB | (204) 799-8082 | wallyk@gmail.com | LinkedIn

PROFESSIONAL SUMMARY

Security Architect with 20+ years of hands-on cybersecurity and enterprise IT experience, including deep operational security expertise in threat detection, incident response, vulnerability management, and security tool administration. Proven track record managing security operations across 2,500-user, 22-site organization with **zero major security breaches** through proactive threat monitoring, vulnerability remediation, and defense-in-depth controls.

Expert in Microsoft Defender XDR, SIEM operations, network security implementation, and security automation using PowerShell and KQL. Strong background in zero-trust architecture, endpoint security, cloud security (Azure/AWS), and OT/IoT security. Experienced collaborating with infrastructure teams to implement security configurations and remediate vulnerabilities across hybrid environments.

CORE COMPETENCIES

Security Operations & Incident Response - Security event triage, investigation, and remediation - Threat detection engineering and playbook development - Incident response planning and execution - SIEM operations and security monitoring - Forensics and post-incident analysis - Threat intelligence monitoring and application

Detection & Response Platforms - Microsoft Defender XDR (Endpoint, Identity, Cloud Apps, Office 365) - EDR/MDR integration and operations (Field Effect) - Security tool deployment and configuration - Vulnerability management platforms - Email security solutions (Cisco Email Security, Abnormal Security)

Vulnerability & Risk Management - Proactive vulnerability scanning and remediation coordination - Zero-day threat response (WordPress, Citrix NetScaler, others) - Risk assessment and control validation - Security control effectiveness testing - Compliance auditing (CIS, NIST, PCI DSS)

Network Security & Segmentation - Zero-trust network segmentation (VLANs, micro-segmentation) - Firewall management and policy configuration (OPNsense, Fortigate, Cisco) - Network Access Control (Cisco ISE, 802.1X) - VPN and remote access security - DMZ design and implementation - OT/IoT network isolation

Identity & Access Security - Microsoft Entra ID (Azure AD) and Active Directory security - Privileged Access Management (PAM) and PIM/JIT - Conditional Access policy configuration - Multi-factor authentication (MFA) enforcement - SSO and federated identity (SAML, OAuth, OIDC)

Cloud Security - Azure security controls and compliance - AWS security (IAM, security groups) - SaaS/PaaS/IaaS security management - Hybrid cloud security architecture

Scripting & Automation - PowerShell security automation - KQL (Kusto Query Language) for security telemetry analysis - Python scripting - Bash shell scripting - API integration for security workflows

Technologies & Tools - **Security Platforms**: Microsoft Defender XDR, SIEM, EDR/MDR, vulnerability scanners - **Network Security**: Cisco ISE, Fortigate, OPNsense, Citrix NetScaler, VPN - **Cloud**: Microsoft Azure, AWS, Office 365/M365 - **Identity**: Entra ID (Azure AD), Active Directory, Azure AD Connect - **Automation**: PowerShell, Python, KQL, Bash - **Infrastructure**: VMware ESXi, Proxmox, Windows Server, Ubuntu Linux, Docker

---

PROFESSIONAL EXPERIENCE

Security Architect | Qualico Developments Canada Ltd. | Jun 2021 - Aug 2025

2,500-employee construction company; 22 sites; enterprise security architecture and operations

Led enterprise security architecture and hands-on security operations including threat detection, incident response, vulnerability management, and security tool deployment across multi-site enterprise environment. Managed security monitoring, investigated security events, and coordinated remediation activities with infrastructure teams. **Maintained zero major security breaches** through proactive vulnerability management and continuous threat monitoring.

Security Operations & Incident Response:

- **Threat monitoring & detection**: Deployed and managed Microsoft Defender XDR across 2,000+ endpoints with Field Effect MDR integration for 24/7 security monitoring and alerting; triaged security events and investigated potential threats daily
- **Vulnerability management**: Conducted continuous vulnerability scanning and coordinated remediation with infrastructure team; successfully patched critical zero-day vulnerabilities (WordPress plugins, Citrix NetScaler) before exploitation, preventing potential breaches
- **Incident response**: Developed and maintained incident response playbooks and procedures; led security investigations and coordinated containment/remediation activities; conducted post-incident analysis and implemented lessons learned
- **Security tool deployment**: Deployed EDR to 100% of endpoints (2,000+ devices); configured and maintained Microsoft Defender XDR, email security solutions, and vulnerability management tools
- **Detection engineering**: Created custom detection rules and alerts based on threat intelligence; tuned SIEM/MDR configurations to reduce false positives while maintaining detection coverage

Network Security & Segmentation:

- **Network segmentation implementation**: Isolated 4 industrial networks (OT/IoT) using VLANs, firewalls, and jump hosts; segmented 100% of cameras, door controllers, and industrial equipment to reduce blast radius for vulnerable legacy systems
- **Network Access Control**: Deployed Cisco ISE for 802.1X authentication across all network switches; processed 100% of endpoints for authentication and policy enforcement at network edge

- **Firewall management**: Configured and maintained Fortigate firewall policies; implemented DMZ segmentation and network security controls
- **VPN security**: Managed Citrix NetScaler/Gateway configurations for secure remote access; hardened TLS policies and SSO integration

Identity & Access Security:

- **Identity security operations**: Managed Microsoft Entra ID (Azure AD) and Active Directory security; enforced MFA across 2,500 users and 100+ applications; conducted regular access reviews and MFA compliance audits
- **Privileged access controls**: Implemented Privileged Access Management (PAM) with network segmentation for admin consoles; deployed Privileged Access Workstations via Citrix; enforced Just-In-Time (JIT) privileged access using PIM
- **SSO administration**: Configured and onboarded 100+ SaaS applications to Azure AD SSO using SAML 2.0 and OAuth 2.0/OIDC protocols

Cloud Security:

- **Azure security**: Deployed and secured Azure AI services (LibreChat with 250+ daily users); implemented Azure security controls and data sovereignty requirements; managed Azure AD Connect for hybrid identity
- **AWS security**: Implemented IAM policies and security groups; used Terraform for Infrastructure as Code

Compliance & Risk:

- **Security policy & documentation**: Authored 25+ security policies, standards, and procedures aligned to CIS Critical Controls framework; maintained security documentation and runbooks
- **Compliance auditing**: Conducted internal security audits and compliance assessments; validated control effectiveness
- **Security awareness**: Coordinated security awareness training and communications

Technologies: Microsoft Defender XDR, Field Effect MDR, Microsoft Entra ID (Azure AD), Active Directory, M365, Intune, Azure, AWS, Fortigate, Cisco ISE, Citrix NetScaler, VMware ESXi, Windows Server, Ubuntu Linux, Docker, PowerShell, KQL, Python, SIEM, vulnerability scanners

---

Systems Architect | Qualico Developments Canada Ltd. | May 2013 - Jun 2021

Led infrastructure architecture and enterprise IT projects across geographically distributed sites with evolving security responsibilities. Managed datacenter operations, network infrastructure, Exchange Server architecture, and Citrix enterprise deployment. Security architecture focus evolved organically, leading to dedicated Security Architect role creation in 2021.

Key security-relevant achievements: - Architected Exchange Server 2013 multi-site infrastructure and hybrid Office 365 migration (1,800+ mailboxes) - Managed Citrix NetScaler for secure remote access

(1,200 concurrent users) - Designed WAN star topology with site-to-site VPN connecting 17-22 remote sites - Deployed active-passive firewall pairs and network segmentation

---

Network Security Administrator | CAA Manitoba | Oct 2003 - May 2013

10 years managing security operations and infrastructure for 300+ user organization

Managed daily security operations including firewall administration, Active Directory security, vulnerability management, and PCI DSS compliance for organization protecting 190,000+ member records and payment card data.

Key Responsibilities:

- **PCI DSS compliance**: Passed multiple annual PCI audits; maintained security controls protecting 40,000 credit cards and 190,000+ member records through access controls and network segmentation
- **Security monitoring**: Deployed and managed McAfee ePolicy Orchestrator for centralized antivirus management; monitored security events and responded to threats
- **Firewall management**: Managed multiple firewalls with VPN connections to remote branches; configured firewall policies and security rules
- **Virtualization & infrastructure**: Designed and implemented VMware/SAN environment; deployed Citrix infrastructure for 180+ remote users
- **Network security**: Implemented IP addressing reconfiguration and network segmentation; managed multi-site security infrastructure

Technologies: VMware ESXi, Citrix, Active Directory, Exchange Server, firewalls, VPN, McAfee ePO, Windows Server

---

Network Support Specialist | Powerland Computers | 1998 - 2003

Provided network setup, troubleshooting, and security support for small business clients. Participated in Manitoba Public Insurance broker network upgrade project including VPN deployment and Windows XP migrations.

EDUCATION & CERTIFICATIONS

SANS Security Training | Security Operations & Architecture - SANS SEC401: Security Essentials (2013) - GSEC-aligned curriculum - SANS SEC501: Advanced Security Essentials (2017) - SANS GSEC (GIAC Security Essentials) - previously certified - Ongoing training: Microsoft Defender XDR, Azure security, threat detection

Continuous Learning - Self-directed study and hands-on labs with open-source AI development, Entra ID, Proxmox, Cloudflare, Container Automation and open-source security technologies

ADDITIONAL SKILLS

- **Compliance**: CIS Critical Controls, NIST Cybersecurity Framework, PCI DSS, ISO 27001 (familiar)
- **Scripting**: PowerShell, KQL (Kusto Query Language), Python, Bash
- **Authentication**: SAML 2.0, OAuth 2.0, OpenID Connect (OIDC)
- **Documentation**: Technical writing, playbook creation, runbook development
- **Collaboration**: Cross-functional teamwork, stakeholder communication, security training delivery

---

KEY ACHIEVEMENTS

- **Zero major security breaches** maintained through proactive vulnerability management and threat monitoring
- Deployed EDR/MDR to 100% of endpoints (2,000+ devices) with 24/7 monitoring
- Successfully prevented exploitation of critical zero-day vulnerabilities through rapid patching
- Achieved 99% MFA enforcement across 2,500 users
- Isolated 100% of OT/IoT assets across 4 industrial networks
- Passed multiple annual PCI DSS audits protecting 40,000+ credit cards
- Deployed Network Access Control (802.1X) to 100% of network switches

---

References available upon request