COLLIN "CORRINE" WILSON

SENIOR INFORMATION SECURITY ANALYST | IAM GOVERNANCE | GRC | SECURITY OPERATIONS

PROFESSIONAL SUMMARY

Information Security professional with 20+ years of IT experience across enterprise security, IAM engineering, governance, risk, compliance, security operations, reporting, automation, and user centered technical support. Nearly seven years supporting Nike IAM Engineering in a 70,000-80,000 user environment, with hands-on experience spanning SailPoint IdentityIQ, Active Directory, Microsoft Entra ID, ServiceNow, PowerShell, SQL, Excel, access governance, audit readiness, and enterprise reporting.

Well balanced for senior Information Security Analyst, IAM/GRC, Information Risk, Access Governance, Security Governance, and Security Operations roles. Known for translating complex identity, access, lifecycle, audit, and operational issues into measurable risk reduction, clear stakeholder communication, practical documentation, repeatable controls, and automation that improves consistency.

CAREER HIGHLIGHTS

- 20+ years of IT experience across enterprise support, information security, IAM, governance, automation, consulting, documentation, and security focused operations.
- Nearly seven years supporting Nike IAM Engineering in a 70,000-80,000 user enterprise environment with cross functional Information Security, Audit, HR, Engineering, and business stakeholder engagement.
- Technical and business lead for a 10-12 month governance initiative covering 10,000+ external Active Directory identities, improving ownership accountability, access hygiene, and audit readiness.
- Primary IAM audit liaison for external audits, including walkthroughs, evidence collection, response preparation, control validation, ServiceNow remediation tracking, and successor mentoring.
- Personally led identity governance onboarding for approximately 15-20 enterprise applications and supported Workday related IAM governance QA and documentation.
- Built SailPoint IdentityIQ, PowerShell, SQL, and Excel reporting for audit readiness, inactive/orphaned accounts, entitlement inventory, RBAC remediation, licensing analytics, operational metrics, and leadership visibility.

CORE SKILLS

Information Security & Risk: Information Security, Information Risk Management, Security Governance, Risk Reduction, Risk Remediation, Security Controls, Control Validation, Audit Readiness, Compliance
Identity & Access Governance: IAM, Identity Governance, Access Governance, SailPoint IdentityIQ, Active Directory, Microsoft Entra ID, RBAC, Least Privilege, Access Reviews, Entitlement Inventory, Application Onboarding
Security Operations & Support: Incident Response Support, Malware/Ransomware Recovery, Endpoint Recovery, Account Recovery, System Hardening, Business Continuity, Troubleshooting, Technical Documentation
Platforms, Reporting & Automation: PowerShell, SQL, Excel, ServiceNow, Jira, Workday, SAP Security, Exchange, Oracle, UNIX, Windows, Dashboards, Operational Analytics
Frameworks & Compliance: SOX, SOC 1, SOC 2, ISO 27001, NIST, PCI DSS, GDPR, ITIL concepts

PROFESSIONAL EXPERIENCE

NIKE, INC. - IAM Security Engineer | Nov 2017 - Sep 2024

- Supported enterprise information security, identity governance, and access risk reduction across a 70,000-80,000 user Nike environment, partnering with Information Risk Management, Application Security, Audit, Engineering, HR, and business stakeholders.
- Served as primary IAM audit liaison for multiple external audits; led walkthroughs, coordinated evidence collection, prepared responses, validated controls, tracked remediation through ServiceNow, and mentored replacement personnel.
- Led a 10-12 month external Active Directory governance initiative as technical and business lead for 10,000+ external identities, coordinating four contractors, one project manager, and approximately eight business-unit leads.
- Designed governance methodology and criteria for external AD identities; presented technical updates, clarified ownership, reduced unnecessary access, improved accountability, and strengthened audit readiness.
- Served as technical lead for a six-month Azure governance initiative with Application Security, reviewing Storage Account ownership accountability and Key Vault certificate lifecycle controls; developed best practices later incorporated into Nike Information Security policy.
- Personally led identity governance onboarding for approximately 15-20 enterprise applications, capturing ownership, entitlement structures, access models, provisioning workflows, governance ownership, connector requirements, and identity lifecycle requirements.
- Supported Nike's migration from SAP HR to Workday by participating in QA, validating identity-lifecycle impacts, documenting governance requirements, and supporting application governance dependencies.
- Configured and supported enterprise access-certification processes, including reviewer populations, entitlement models, access governance reporting, stakeholder communications, RBAC remediation, and least privilege validation.
- Built governance, operational, and leadership reporting using SailPoint IdentityIQ, PowerShell, SQL, and Excel for licensing analytics, audit readiness, inactive and orphaned accounts, entitlement inventory, operational metrics, and RBAC remediation.
- Automated repeatable PowerShell reporting and data-validation workflows that reduced manual effort, improved consistency, strengthened governance controls, and accelerated remediation analysis.
- Improved ServiceNow based remediation tracking, change requests, dashboards, knowledge articles, approvals, and audit tracking in partnership with IAM Operations, Engineering, and business stakeholders.
- Translated access exceptions, lifecycle anomalies, control gaps, and troubleshooting issues into risk based remediation plans, technical updates, documentation, and business friendly stakeholder communications.
- Recognized throughout IAM Engineering as a trusted technical resource for identity governance, PowerShell automation, Active Directory, enterprise reporting, governance, compliance, and complex troubleshooting.

TECHNERD CONSULTING - Founder / Independent Technology & Cybersecurity Consultant | Jan 2001 - Present

- Founded and operate a technology and cybersecurity consulting practice delivering practical IT support, security guidance, documentation, automation, process improvement, and business continuity support for individuals and small organizations.
- Translate complex technical, security, and operational risks into clear recommendations that balance risk reduction, usability, cost, accessibility, maintainability, and client constraints.
- Support clients with account recovery, system hardening recommendations, workflow cleanup, documentation, troubleshooting, online services, websites, and practical security improvements.
- Develop technical writing, process documentation, troubleshooting guides, lightweight reporting, and automation solutions that reduce recurring support problems and improve resilience.
- Create client ready checklists, recovery instructions, and maintenance documentation that reduce dependency on ad hoc support and help clients make better technology decisions.
- Identify practical security and continuity gaps across accounts, devices, backups, online services, and workflows, then prioritize remediations that fit client risk, usability, and budget.

UMPQUA BANK / VANDERHOUWEN - Network Security Administrator | Jul 2017 - Nov 2017

- Supported regulated financial-services access administration, approval workflows, entitlement reviews, group and folder access requests, compliance expectations, and control-conscious provisioning processes.
- Maintained audit ready access discipline by ensuring approvals were followed, changes were traceable, and access administration decisions aligned with financial security and compliance requirements.
- Reviewed procedures and PowerShell scripts for accuracy, gaps, automation opportunities, and access control alignment, improving reliability and reducing operational risk.
- Partnered with requestors and approvers to resolve access issues while preserving traceability, approval discipline, and compliance-focused documentation.

BLOUNT INTERNATIONAL - Technical Analyst II / Security Focused Escalation Resource | Dec 2013 - Jul 2017

- Supported security operations, incident response, malware investigations, ransomware recovery, endpoint recovery, access administration, SAP Security support, compliance readiness, and user facing documentation in a manufacturing environment.
- Managed Active Directory accounts and security groups, Exchange permissions, Lync, SAP access, endpoint support, backup and recovery coordination, and automation using PowerShell, VBScript, and Batch scripting.
- Documented recurring security and support issues, supported user awareness, and helped technical teams restore services during malware, ransomware, access, and endpoint incidents.
- Balanced enterprise support with security focused escalation work, helping users recover quickly while preserving control discipline, documentation quality, and operational continuity.
- Coordinated with infrastructure and support teams during endpoint, access, and backup and recovery incidents, balancing rapid restoration with documentation and control requirements.
- Created and maintained technical documentation for support teams, improving consistency for recurring security, endpoint, and access issues.

KNOWLEDGE UNIVERSE TECHNOLOGIES - Service Desk Technician II | Aug 2010 - Dec 2013

- Delivered Tier II enterprise support for Active Directory, Oracle, UNIX, Outlook/OWA, endpoints, networking, mobile devices, and high volume service requests.
- Updated network troubleshooting documentation, built training resources for Tier I support, and provided escalation support to improve resolution quality and consistency.
- Built CCNA/server training environments, assisted networking rollouts, configured wireless access points and switches, and developed VB.NET tools to automate support tasks.
- Improved knowledge transfer by documenting escalation procedures and practical troubleshooting steps for enterprise support teams.

EDUCATION & PROFESSIONAL DEVELOPMENT

Education: Mt. Hood Community College - Information Technology, Networking, and Cybersecurity coursework
Professional Development: Former CompTIA Security+ | Former CompTIA Network+ | CISA coursework | CISM coursework | CISSP coursework | CEH coursework | ITIL training | SailPoint IdentityIQ training | AWS Fundamentals