

Andrew Conlin

Professional Summary

Information Technology Specialist with 5 years of experience in incident response, threat detection, and email security within a Microsoft 365 and Azure environment. Skilled in endpoint investigation, phishing remediation, security awareness training, and automating identity provisioning with PowerShell. Brings a security-first mindset to every system supported.

Work History

The Christman Company - Information Technology Specialist

Lansing MI

09/2021 - 09/2026

Systems Administration & Identity Management

- Administered identities for 1,500 users across Active Directory, Entra ID, and Microsoft 365, managing accounts, OUs, security groups, and licensing based on role and department
- Integrated Workday HR with Entra ID and built PowerShell automation to handle tasks outside the native integration, streamlining new-hire provisioning
- Enforced least privilege through role-based access control and Zero Trust audits of security groups, removing excessive and stale access
- Led IT onboarding orientations for new hires, covering MFA enrollment, password management, and phishing awareness, so users started out securely on day one
- Resolved account access, authentication, and MFA issues for end users across Microsoft 365 and Active Directory

Incident Response & Email Security

- Investigated suspicious account activity flagged by Check Point Harmony Email & Collaboration, verifying sign-in geolocation to detect impossible travel and unauthorized access, then containing compromised accounts.
- Monitored authentication alert logs for MFA fatigue (push spam) attacks, identifying targeted users and escalating to prevent credential-based account takeover.
- Remediated active phishing campaigns by mass-quarantining malicious emails from end-user mailboxes after delivery, limiting exposure across the organization.
- Triageed and processed end-user requests to release quarantined email, validating each message for malicious links, attachments, and spoofing before release to balance security with business continuity
- Created and tuned detection and policy rules in Check Point Harmony to block phishing, impersonation, and malicious attachments while reducing false positives.

✉ a.jconlin@icloud.com

☎ 517-420-5983

📍 Williamston, MI 48895

Skills

- Incident Response
- Threat Detection
- Email Security
- Exchange Online
- Powershell
- Entra ID
- Identity and Access
- Endpoint management
- RMM & MDM tools - Kaseya - JAMF - InTune
- Technical support
- Information security
- Networking

Education

06/2016

Haslett High School

Haslett, MI

High School Diploma

Certifications

- Full Stack Web Developer - Wozniak University
- Microsoft Certified: Azure Administrator Associate - In progress

- Conducted endpoint investigations and incident response in Palo Alto Networks Cortex XDR, analyzing alerts and taking containment actions such as host isolation and file quarantine.

Endpoint & Application Support

- Resolved novel issues with newly adopted AI tools, including Claude, and niche line-of-business software through independent research and troubleshooting, often with no existing documentation
- Served as primary technical support for the Estimating department, managing its full application stack, including WinEst to keep bid and project workflows running
- Integrated Adobe with Entra ID using SAML single sign-on (SSO) and SCIM provisioning, centralizing authentication and automating user account lifecycle management

Security Awareness & Phishing Simulation

- Designed and ran simulated phishing campaigns in KnowBe4 to measure employee susceptibility and find high-risk departments and user groups
- Briefed senior leadership on campaign results, including click rates, reporting rates, and Phish-prone Percentage trends, and turned the findings into recommendations for targeted training
- Developed and delivered security awareness training through KnowBe4 covering phishing recognition, social engineering, password hygiene, and incident reporting, strengthening the organization's human layer of defense

Interests

SOC Simulators

Defensive Labs - Hack the Box

Red Team Labs - Hack the Box