TRENTON VAN ORDEN

Austin, TX | (512) 751-3618 | trentonvanorden@gmail.com | LinkedIn: Trenton Van Orden

THREAT DETECTION & RESPONSE | VULNERABILITY MANAGEMENT | INCIDENT RESPONSE

CompTIA Security+ and CySA+ certified cybersecurity professional with hands-on experience supporting security operations, threat detection, vulnerability management, and incident response across enterprise and cloud environments. Skilled in Microsoft Defender XDR, SentinelOne, CrowdStrike, Microsoft Entra ID, Active Directory, and AWS, with proven success investigating security events, strengthening endpoint security, and supporting modern cybersecurity operations.

TECHNICAL SKILLS

Security Tools: Microsoft Defender XDR, SentinelOne, CrowdStrike Falcon, Huntress, Nessus, Tenable.io, Kibana, Burp Suite, Metasploit, Snyk, VirusTotal, SaaS Alerts
Identity & Access Management: Microsoft Entra ID, Active Directory, Okta SSO, Multi-Factor Authentication (MFA), Google Workspace
Cloud & Infrastructure: Microsoft 365, AWS (EC2, IAM), Exchange Online, Intune, SharePoint, Teams, Cloudflare
Endpoint Management: Microsoft Intune, Jamf, Kandji, Apple Business Manager, NinjaOne
Networking & Security: SonicWall, UniFi, Cisco Secure, FortiClient
Programming & Scripting: Python, PowerShell, Bash
Frameworks: NIST Cybersecurity Framework, CIS Benchmarks, Incident Response, Vulnerability Management

PROFESSIONAL EXPERIENCE

Help Desk Technician | Contigo Technology | Austin, TX (Aug 2025 – Present)

- Resolve 2,000+ end-user support tickets through remote and phone support using Autotask PSA while maintaining a 95% customer satisfaction rating.
- Administer Microsoft 365 and Google Workspace environments, managing Entra ID, Exchange Online, Intune, Teams, SharePoint, Microsoft Defender XDR, and Purview.
- Manage Cisco Unified Communications Manager (CUCM) phone provisioning, including extension assignments, user configuration, and ongoing support.
- Investigate and remediate 1,000+ security incidents using Microsoft Defender XDR, SentinelOne, CrowdStrike Falcon, RocketCyber, and Huntress.
- Respond to 300+ phishing incidents by investigating compromised accounts and suspicious authentication activity using Entra ID and Google Workspace audit logs.
- Support Windows, Linux, macOS, and mobile endpoint administration using Intune, Jamf, Kandji, Apple Business Manager, NinjaOne, and enterprise networking technologies.

Onsite Technician | TECO-Westinghouse | Round Rock, TX (Feb 2026 – May 2026)

- Delivered Tier 1 technical support by troubleshooting hardware, software, operating system, and network issues.
- Administered Active Directory user provisioning, access controls, security groups, and account lifecycle management.
- Diagnosed client and server issues, improving system availability and operational reliability.
- Deployed Windows workstations, enterprise applications, printers, and peripherals while documenting resolutions using IT service management best practices.

Cybersecurity Intern | Lumin Digital | Remote (May 2023 – Aug 2023)

- Built a DNS anomaly detection dashboard and performed threat hunting in Kibana using Cloudflare logs.
- Conducted Nessus vulnerability scans on AWS EC2 environments and performed CIS Benchmark assessments.
- Designed tabletop incident response exercises covering ransomware, phishing, and insider threat scenarios.
- Evaluated third-party vendor security using Venminder and TrustCloud while supporting NIST Cybersecurity Framework compliance.

EDUCATION & PROFESSIONAL DEVELOPMENT

CompTIA Cybersecurity Analyst (CySA+) | CompTIA | May 2025 (Valid Through: May 2028)

CompTIA Security+ | CompTIA | Jan 2025 (Valid Through: May 2028)

DoD Cyber Sentinel Skills Challenge | Jun 2025

High School Diploma | Vandegrift High School | Austin, TX | 2020