ANGEL RAMIREZ

INDEPENDENT IT & SECURITY CONTRACTOR | EDR · NGFW · M365 ZERO TRUST · INCIDENT RESPONSE

Caledonia, ON (Remote — Canada & US) 905-906-3031 angel.andes.ramirez@gmail.com linkedin.com/in/aar-security aar-security.com

PROFESSIONAL SUMMARY

Independent IT and cybersecurity contractor with 6+ years in information technology and 2+ years leading security operations for a multi-site manufacturing enterprise. Proven track record: deployed and tuned SentinelOne EDR across 100+ endpoints, replaced legacy SonicWall infrastructure with FortiGate NGFW across four production sites, and engineered Microsoft 365 / Entra ID Zero Trust architecture. Delivered end-to-end breach investigations reducing MTTR from 48 hours to 6 hours and cutting unauthorized access attempts by 40%. Sole contractor for IT Harbor — completed full network and security stack deployments at four dental clinic locations across Ontario and British Columbia. HTB Certified Defensive Security Analyst (CDSA); OSCP (Offensive Security Certified Professional) actively in progress.

CORE COMPETENCIES

- Endpoint Detection & Response (EDR)
- SIEM & Log Analysis
- Microsoft 365 / Entra ID Hardening
- Threat Hunting & Behavioral Analysis
- Network Security & Segmentation
- Zero Trust Architecture
- Incident Response & Digital Forensics
- FortiGate NGFW Deployment & Management
- Active Directory Security
- Vulnerability Assessment & Patch Mgmt
- MITRE ATT&CK Framework
- NIST Cybersecurity Framework

CONTRACT & CONSULTING EXPERIENCE

IT Security & Network Consultant — Independent Contractor

IT Harbor | Ontario & British Columbia | August 2025 – Present

- Sole contractor delivering full network and security stack deployments across 4 dental clinic locations (Hamilton, ON and Vancouver, BC) under PIPEDA compliance requirements; sole technician for all scoping, execution, troubleshooting, and formal documentation.
- Deployed Ubiquiti UniFi Cloud Gateway Ultra, Wi-Fi 6 APs (U7 Pro), and PoE switching, replacing legacy Asus/Cisco infrastructure; implemented VLAN segmentation with enforced guest network isolation (VLAN 10) to protect clinical data and PHI.
- Diagnosed and resolved critical server and file share outages caused by static IP conflicts and stale DNS/NetBIOS post-cutover; restored practice management and imaging app connectivity with zero data loss via NIC migration and gateway DNS reconfiguration.
- Identified and decommissioned rogue access points via ARP/ping sweep and MAC vendor lookup; decommissioned unused legacy server architecture across all four sites.
- Installed and configured Datto RMM and full endpoint security suite (Sophos, Huntress, Webroot, OpenText); provisioned Curve Dental Cloud user accounts, permissions, and X-ray imaging integration.
- Delivered formal deployment reports per engagement: network architecture diagrams, IP inventories, validation checklists, and critical support handoff documentation.

PROFESSIONAL EXPERIENCE

IT Manager — Cybersecurity Operations

Verduyn Tarps Inc. | Hamilton, Ontario | July 2024 – Present

- Own full security operations for a multi-site manufacturing environment: 4 locations, ~100 endpoints — EDR, NGFW, identity hardening, and incident response end-to-end.
- Deployed and tuned SentinelOne EDR across 100+ endpoints: 95% coverage, custom detection rules improved threat detection accuracy by 35%, detecting ~200 security events monthly.
- Investigated and contained 5 confirmed security breaches using EDR forensics and log correlation; reconstructed full attack chains mapped to MITRE ATT&CK — reduced MTTR from 48 hours to 6 hours and MTTD by 60%.
- Hardened Microsoft 365 / Entra ID: MFA deployed to 85% of accounts, Zero Trust Conditional Access enforced, PIM just-in-time elevation configured — unauthorized access attempts reduced by 40%.
- Replaced legacy SonicWall with FortiGate NGFW across 4 sites: IDS/IPS, SSL inspection, and application control — blocking ~10,000 malicious connection attempts monthly.
- Managed enterprise vulnerability program (Nessus): 95% patch compliance within 30-day SLA, critical vulnerability exposure window reduced by 70%.
- Designed VLAN-based network segmentation isolating production, corporate, and guest zones; configured IPsec site-to-site VPN for multi-site secure connectivity.

System Administrator

Verduyn Tarps Inc. | Hamilton, Ontario | September 2023 – July 2024

- Managed IT infrastructure across 4 locations (100+ users): VPN, firewall rules, network segmentation, and secure remote access — 90% patch compliance across Windows and Linux.
- Administered Active Directory: Group Policy, RBAC, file share security; event log analysis to detect anomalous behavior and unauthorized access attempts.
- Deployed endpoint protection platforms, backup solutions, and identity management systems; maintained network diagrams, server configurations, and change documentation.

IT Support Technician — Geek Squad

Best Buy Canada | Hamilton, Ontario | April 2018 – September 2023

- Technical support and security remediation for 1,000+ residential and SMB clients; malware analysis and forensic removal reduced reinfection rates by 60%.
- Cybersecurity awareness education: phishing prevention, password hygiene, secure computing practices — reduced repeat security incidents for managed client accounts.

TECHNICAL SKILLS

EDR & Endpoint Security

SentinelOne Singularity · Microsoft Defender for Endpoint · Microsoft Defender for Identity · Sophos · Huntress · Webroot · Datto RMM

SIEM & Log Analysis

Splunk · ELK Stack · Alert Triage · Event Correlation · Threat Hunting · Log Analysis · False Positive Reduction · Security Monitoring

Network & Firewall Security

FortiGate NGFW · FortiManager · SonicWall · IDS/IPS · SSL Inspection · VPN (IPsec, SSL) · VLAN Segmentation · Ubiquiti UniFi (Cloud Gateway Ultra, U7 Pro, PoE)

Identity & Access Management (IAM)

Active Directory · Azure AD / Entra ID · Conditional Access · MFA · RBAC · Group Policy · Privileged Identity Management (PIM) · Zero Trust Architecture

Offensive Security & Penetration Testing

Kali Linux · Metasploit · Burp Suite · BloodHound · Impacket · CrackMapExec · Nmap · Nessus · Wireshark · OWASP Top 10

Cloud & Infrastructure

Microsoft Azure · Microsoft 365 Security · Windows Server 2012–2022 · Linux (Ubuntu, Kali, CentOS) · Hyper-V · Proxmox VE

Scripting & Automation

PowerShell · Bash · Python · SQL

Frameworks & Compliance

MITRE ATT&CK · NIST CSF · CIS Controls · CVSS 3.1 · PIPEDA · Zero Trust · OWASP Top 10

SELECTED PROJECTS & RESEARCH

Active Directory Exploitation & Detection Engineering

Kerberoasting, AS-REP roasting, delegation abuse, credential theft chains; MITRE ATT&CK-aligned detection rules. aar-security.com/projects.html

Homelab Security Infrastructure — Proxmox VE

Multi-VM lab with Active Directory, Windows Server, Linux targets, and Kali for offensive research and defensive validation. aar-security.com/Projects/homelab-build.html

WordPress Web Application Penetration Test

CVE-2020-8772 auth bypass, PHP reverse shell, SUID PATH hijacking root escalation; full chain with OWASP Top 10 remediation. aar-security.com/Projects/wordpress-exploitation.html

CERTIFICATIONS & TRAINING

HTB Certified Defensive Security Analyst (CDSA) — Hack The Box | 2026

7-day hands-on SOC examination: enterprise incident investigation, digital forensics, threat hunting, log analysis, and commercial-grade incident report writing.

OSCP — Offensive Security Certified Professional (PEN-200) — OffSec | In Progress (Est. May 2026)

70+ lab machines: Active Directory exploitation, privilege escalation, lateral movement, and professional penetration test reporting.

CS50 for Cybersecurity — Harvard University (edX) | 2024

Cryptography, web application security, threat modeling, secure coding, and defensive security.