EZEQUIEL LEON

(973) 208-4987 | Leon.eze@outlook.com | New Jersey | linkedin.com/in/ezequiel-leon

SUMMARY

Security Engineer with 8+ years across enterprise IT and cybersecurity, specializing in detection engineering and incident response. Experience includes investigating incidents in a 10,000+ endpoint environment and helping build detection and response capabilities for a healthcare technology company. Core expertise includes Microsoft Defender XDR, Sentinel, Splunk, Entra ID, Intune, and Azure.

PROFESSIONAL EXPERIENCE

OnMed, LLC — White Plains, NY
Security Engineer — *10/2025 to 07/2026*

- Partnered with Coretek, a managed security service provider, to establish OnMed's detection and response program, defining incident escalation and communication procedures, running SOC reviews, tuning Elastic detections, and supporting the migration from Microsoft Sentinel to Elastic.
- Administered Microsoft Defender for Endpoint and Intune across 150+ Windows and macOS endpoints, investigating alerts and enforcing web, network, application, removable-media, and approved-AI controls.
- Strengthened Azure and Entra ID security after an 83% Purple Knight assessment by fully remediating 23 Indicators of Exposure across legacy authentication, privileged access, MFA, and identity-risk controls.
- Closed an offboarding access gap by rebuilding session-revocation automation with Azure Automation and Microsoft Graph to disable accounts, revoke sessions and refresh tokens, remove group access, and address cached Windows credentials.
- Led the technical response to the Notepad++ updater threat, coordinating preventive controls and building a proactive Microsoft Sentinel detection; confirmed no vulnerable systems or evidence of compromise.

Tilley Distribution — Norwood, NJ
Cybersecurity Specialist — 03/2025 to 08/2025

- Served as the primary internal security resource for a global environment of approximately 400-700 endpoints, handling alert triage, incident investigation, vulnerability remediation, and MSSP coordination across SentinelOne, Sumo Logic, Tenable, UpGuard, and eSentire.
- Deployed and configured Tenable scanning, validated findings and false positives, built recurring dashboards, and coordinated incident escalations with eSentire and internal IT teams through remediation.

The Boeing Company — Remote
Cybersecurity Incident Response Analyst — 11/2022 to 02/2025

- Investigated 50+ security incidents across Boeing's 10,000+ endpoint environment, independently leading assigned cases involving malware, compromised accounts, suspicious PowerShell activity, phishing, network anomalies, and vulnerability events.
- Developed and tuned Splunk correlation searches and behavioral detections, improving end-to-end visibility into related security activity and investigations.
- Performed log analysis, network forensics, malware triage, and vulnerability assessment; documented findings and briefed technical stakeholders and leadership on containment and resolution.

Amilar Capital — New York, NY
Systems Administrator — 04/2022 to 10/2022

- Hardened identity and network infrastructure supporting Bloomberg Terminal-integrated financial systems, implementing MFA and least-privilege controls across on-premises and hybrid environments.
- Proposed and initiated an on-premises-to-Azure migration, leading technical planning and initial execution before departing the company.
- Established vulnerability scanning and patch-management processes that remediated 40+ documented critical findings within the first 90 days.

Polestar New York, NY

IT Specialist (Contract) 04/2021 to 04/2022

- Led end-to-end technology readiness for more than 10 Polestar retail launches across North America, covering network connectivity, endpoint deployment, audiovisual systems, vendor coordination, site testing, documentation, and post-launch support.
- Standardized technical configurations and deployment documentation across concurrent openings, helping ensure each retail location launched on schedule.

ConcentricLife New York, NY

IT Administrator 05/2018 to 04/2021

- Progressed from IT Apprentice to IT Administrator, taking ownership of Cisco Meraki switching, wireless, firewall, and network segmentation across a two-floor office supporting approximately 100-300 users.
- Administered Jamf-based laptop imaging, Okta authentication for VPN access, MFA, endpoint protection, firewall rules, VLANs, and identity and network operations while investigating and resolving endpoint and infrastructure security incidents.

TECHNICAL SKILLS

Detection and Incident Response: Microsoft Defender XDR, Microsoft Sentinel, Elastic Security, Splunk, SentinelOne, Sumo Logic, KQL, alert triage, incident investigation, behavioral detections, correlation searches, detection tuning

Microsoft Cloud, Identity, and Endpoint: Azure, Microsoft 365, Defender for Cloud, Defender for Endpoint, Intune, Entra ID, Conditional Access, MFA, Azure RBAC, Log Analytics, Key Vault, Windows, macOS, Jamf, Okta

Threat Intelligence and Vulnerability Management: MITRE ATT&CK, IOC analysis, threat hunting, campaign research, Tenable, Nessus, UpGuard, finding validation, risk prioritization, patch management, remediation tracking

Automation and Network Security: PowerShell, Python, Bash, Azure Automation, Microsoft Graph, Wireshark, tcpdump, Cisco Meraki, firewalls, VLANs, network segmentation

Security Operations and Frameworks: SOC reviews, MSSP coordination, Jira, SharePoint, SOC 2 Type II, SOC 3, HIPAA, NIST Cybersecurity Framework

CERTIFICATIONS

Cisco Meraki Network Operator (CMNO)

EDUCATION & ADDITIONAL EXPERIENCE

CUNY, Herbert H. Lehman College | Bachelor of Science in Computer Information Systems | 2018

Columbia University | Cybersecurity Professional Education | 2020

Columbia University Cybersecurity Boot Camp | Teaching Assistant (part time) | 2020 to 2025

TryHackMe | Top 6% of users