Vicente Manuel Muñoz Milchorena

Tijuana, Baja California, México

E-mail: vicente.munoz@milchorena.com

LinkedIn: linkedin.com/in/vicente-milchorena (LinkedIn)

GitHub: github.com/vicosurge (GitHub)

PROFILE

I am dedicated to my continuous personal and professional growth at the intersection of the social sciences and technology, with a primary focus on using education to enrich the humanities. My goal is to leverage technology and innovative methods to reach wider audiences, fostering a deeper understanding of culture and history.

I aim to understand my clients' needs and provide efficient, scalable cybersecurity solutions that safeguard their assets while minimizing downtime and risk.

As I continue my journey to becoming a full-fledged historian, I am passionate about contributing to the field through teaching, community involvement, and research. I seek to engage in social and government projects that promote cultural heritage and regional history, while exploring fresh perspectives and unrecognized subjects in historical research.

EXPERIENCE

Senior Security Systems Engineer | EPAM Systems

DECEMBER 2024 - CURRENT

Configure SIEM and SOAR solutions, ensuring seamless integration with various security tools, systems, and data sources. Develop detection use-cases and implement SIEM detection rules while creating SOAR remediation playbooks to streamline security operations.

Key responsibilities:

- Configure SIEM and SOAR solutions, ensuring seamless integration with various security tools, systems, and data sources; Conduct SIEM and SOAR testing and validation
- Develop detection use-cases and implement SIEM detection rules; Develop SOAR remediation use-cases; Create, test, and update SOAR playbooks to streamline security operations
- Integrate log sources with SIEM, optimize log ingestion and processing; Perform threat hunting, data enrichment, threat intelligence feeds onboarding, and utilize them for automated responses
- Generate reports for both technical and non-technical staff and stakeholders
- Stay up-to-date with SIEM technologies and identify opportunities for continuous improvement

---

IT Manager | Baja Call Center

MAY 2024 – DECEMBER 2024

Leading a dynamic team of diverse IT professionals, leveraging a wide range of backgrounds and expertise to ensure smooth and efficient operations. Committed to providing top-tier assistance and support, fostering a collaborative and innovative work environment.

Key responsibilities:

- Strategize and implement robust security measures to protect organizational assets
- Developing and overseeing the Incident Response Plan (IRP) for cybersecurity events, serving as the primary responder with a well-established workflow
- Managing resource allocation and reconciliation to optimize utilization and drive cost savings
- Mentoring and building career paths for IT department members, fostering growth and professional development
- Collaborating with other departments to implement technology solutions that streamline processes and enhance efficiency
- Manage vendor relationships and coordinate with upper management on contract negotiations

Skills: Team Leadership, Security Measures, Resource Management, Business Scalability, PCI-DSS Compliance

Technologies: Proxmox, TP-Link, Elastic Stack, Wazuh, Zabbix, Zoho, Vicidial, Windows Administration,

Linux, AWS, Google Workspace, SonicWALL, GVM, PHP, MySQL, VB6

Cyber Security Incident Responder | Nubank

AUGUST 2022 – MARCH 2024

Working with different departments as an Incident Responder, ensuring that incidents are handled with due diligence, identifying the source of the threat, mitigating and controlling, providing the most sensible solution, and producing documentation for a post-mortem review.

Skills: AWS Security, Incident Response, Process Automation, Linux, Windows, Splunk, Google Chronicle, Torq

DFIR Consultant | Nearshore Cyber

JANUARY 2023 – CURRENT

Responding to incidents from different clients involves attending the incident, performing the investigation and mitigation, building a plan for setting the business back in motion, and ensuring that there are clear post-mitigation tasks that the client can follow up on.

Skills: Security Incident Response, Digital Forensics, Vulnerability Assessment and Penetration Testing (VAPT), Vulnerability Management and Remediation

Cyber Security Mentor | Chegg

DECEMBER 2021 – AUGUST 2022

Provided guidance and mentorship to students on their career paths, including recommendations, additional material, and assistance with laboratories.

Skills: ISO27002, Security Incident Response, Penetration Testing, Social Engineering

Professor | UNIAT

SEPTEMBER 2021 – AUGUST 2022

Taught cybersecurity subjects to master's students, focusing on auditing, compliance, SOC, and incident response.

Skills: ISO27002, Security Incident Response, Penetration Testing, Social Engineering

---

Integration Engineer | NXLog Ltd

MAY 2021 – AUGUST 2022

Day-to-day activities change depending on requirements; these can range from coding, debugging in different languages, troubleshooting client issues or investigating reported vulnerabilities or faults on software, creating guides, documentation, and integrations with other platforms and how to parse or process data to comply with other platforms properly; help in creating internal processes and procedures for a streamlined workflow.

Skills: Windows, Linux, Security Information and Event Management (SIEM), Python, Bash, PowerShell, Git, Technical Writing, Markdown

---

IT Helpdesk Engineer | Brier & Thorn S.A.P.I de C.V.

JANUARY 2021 – SEPTEMBER 2021

Set up, configure, and deploy security infrastructure to enable the SOC to monitor and assess client environments. Utilize and develop tools to support maintenance and expedite the implementation of platforms, appliances, and software essential for daily operations.

Skills: Windows, Linux, Security Information and Event Management (SIEM), EDR/XDR, DLP (Digital Guardian), Firewalls, Email Gateway, Python, Bash, PowerShell

---

IT SOC Analyst II | Brier & Thorn S.A.P.I de C.V.

JULY 2020 – JANUARY 2021

Working with a team of ten people, installing, and configuring, managing, supporting, and monitoring more than one hundred platforms using different technologies, finding the best ways to improve the quality of our service and response time for our clients, additionally assisting in penetration testing and projects our clients may need.

Skills: Windows, Linux, Security Information and Event Management (SIEM), EDR/XDR, DLP (Digital Guardian), Firewalls, Email Gateway, Python, Bash, PowerShell, Git, Vulnerability Assessment and Penetration Testing, Network and Host Architecture, AWS, Azure, GCP, SAST/DAST

Freelance Information Technology / Cybersecurity Consultant

JANUARY 2020 - CURRENT

Provide comprehensive services to clients globally, including managing servers, developing software and scripts, documenting processes, handling incident response, and installing and configuring security platforms.

Skills: Security Incident Response, Security Information and Event Management (SIEM), Linux, Python, Technical Documentation, Windows, Online Consultancy

---

SOC Manager | Brier & Thorn S.A.P.I de C.V.

OCTOBER 2019 – JULY 2020

Overseeing and coordinating operations inside the SOC and in-house Red Team, meeting with clients to discuss current processes and improvements, assisting with risk assessment for our clients, working hand to hand with our PMO department to improve quality of service, spearheading our internal development creating new tools and integrations, creating training development plan as well as ensuring that employees undergo required training and certifications.

Skills: Windows, Linux, Security Information and Event Management (SIEM), EDR/XDR, DLP (Digital Guardian), Firewalls, Email Gateway, Python, Bash, PowerShell, Git, Vulnerability Assessment and Penetration Testing, Network and Host Architecture, AWS, Azure, GCP, SAST/DAST

IT SOC Analyst II | Brier & Thorn S.A.P.I de C.V.

NOVEMBER 2016 – OCTOBER 2019

Working with a team of ten people, installing, and configuring, managing, supporting, and monitoring more than one hundred platforms using different technologies, finding the best ways to improve the quality of our service and response time for our clients, additionally assisting in penetration testing and projects our clients may need.

Skills: Windows, Linux, Security Information and Event Management (SIEM), EDR/XDR, DLP (Digital Guardian), Firewalls, Email Gateway, Python, Bash, PowerShell, Git, Vulnerability Assessment and Penetration Testing, Network and Host Architecture, AWS, Azure, GCP, SAST/DAST

IT Service Desk II | Integer Holdings Corporation

MAY 2016 – NOVEMBER 2016

I served as a Night Shift Helpdesk Technician, collaborating with a dedicated team of four. My responsibilities included managing user accounts by creating, updating, and removing information across various systems. Additionally, I prepared equipment and computers for new employees and vigilantly monitored the security platform (SolarWinds) to promptly address any incidents.

Skills: Active Directory, Windows, SolarWinds, Printer Support, Customer Support

---

Junior Programmer | National Autoparts Mexico

SEPTEMBER 2012 – JANUARY 2014

Responsible for developing and supporting in-house applications tailored to meet logistics, human resources, marketing, and sales needs. Tasks included creating reports, views, and forms, primarily utilizing PHP and Python, with MySQL and SQLite databases for data management.

Skills: PHP, Python, jQuery, MySQL, SQLite, Linux, Windows

Desktop Technician III (MES/MIS) | Flexmedical (formerly Availmed)

OCTOBER 2008 – JANUARY 2011

Managed on-site support operations across four medical disposables manufacturing facilities, overseeing a user base exceeding five hundred individuals. Responsibilities included active directory administration, networking support encompassing ethernet, telephony, and wireless technologies, as well as oversight of all regional printers, Nextel, and Blackberry devices.

Skills: Windows, Nortel PBX, Technical Support, Printer Support, Blackberry Enterprise Server

---

EDUCATION

B.A. in History | Universidad Autónoma de Baja California

2011 – 2019

Courses focused on world history, Mexican history, regional history, and relations between Mexico and the USA. My thesis focuses on Digital Humanities.

Skills: Curiosity, Teaching, Technical Writing, Logical Thinking

---

CERTIFICATIONS

- Microsoft Certified: Azure Fundamentals *(Verify Online)*

- Microsoft Certified: Azure AI Fundamentals *(Verify Online)*
- Torq 101
- Torq Automation Analyst
- Splunk Certified User (6.x)
- AlienVault Certified Security Engineer (ACSE)
- Agile Project Management Series (Various)
- Cybrary Series (Various)