Santiago Lopez de Toledo

New York, NY | santilopezdetoledo@gmail.com | (646) 309-8677

EDUCATION

New York University, School of Professional Studies, New York, NY
MSc in Global Security, Conflict and Cybercrime (STEM) | Sept 2025 to December 2026

- GPA: 3.9
- Coursework: Cyber Threat Intelligence, MITRE ATT&CK and structured analytic techniques, OSINT, Cyberwarfare, National Security and Critical Infrastructure Resilience, Economic Espionage
- Produced analytic papers on cyber operations, threat actor TTPs, and the intersection of geopolitical trends and emerging technology threats

Universidad Pontificia Comillas ICADE, Madrid, Spain
BSc in Data Analytics and International Relations (STEM) | Sept 2020 to June 2025

- Coursework: International Law, Geopolitics, Machine Learning, Regression Analysis, Financial Modeling
- Thesis: Insider Threat Detection Using ML for a FinTech Company. Evaluated classification models against financial transaction data; built a custom cost equation to benchmark algorithm performance.

Sophia University, Tokyo, Japan | Apr to Aug 2024
Policy Making, Computer Science, People Analytics

University of Michigan, Ross School of Business, Ann Arbor, MI | Jan to May 2023
Financial Modeling, Financial Trading, Collective Intelligence, Financial Management

PROFESSIONAL EXPERIENCE

Technical Writer Intern | Rubrik, Palo Alto, CA | May 2026 to Aug 2026

- Investigate APT groups and adversary TTPs using Google Threat Intelligence and OSINT, profiling behavior and motivations against frameworks such as MITRE ATT&CK, as part of the Zero Labs research team
- Write and tune YARA rules against live malware samples, developing detection signals and iterating against real-world attack data
- Build Python pipelines to triage high-volume detection signal and surface true positives for malicious AI-powered code, identifying AI-powered malware used by 5 distinct state-sponsored threat groups
- Produce actionable intelligence reports and executive-facing briefings on emerging threats for security leaders at Fortune 500 and G2K organizations

Tech Consulting Analyst | NTT Data, Madrid, Spain | Jan to May 2025

- Performed threat intelligence and regulatory analysis for Banking and Public Sector clients, tracking global threat trends and translating them into structured briefing memos for senior stakeholders
- Conducted regulatory impact assessments tied to EU cybersecurity directives (NIS2, DORA) to support client resilience planning
- Assessed and helped remediate 12+ high-risk third-party vulnerabilities per client, strengthening exposure posture across critical assets

Investment Analyst Intern | Abante Asesores, Madrid, Spain | May to Aug 2023

- Researched global markets, synthesizing geopolitical and economic trends into written briefings for portfolio managers; contributed to 8 to 10% portfolio growth through data-driven competitive intelligence

SKILLS

Cyber & Threat Analysis: Threat actor profiling and TTPs, MITRE ATT&CK, YARA rule development, malware analysis, vulnerability assessment, OSINT, Google Threat Intelligence, structured analytic techniques

Technical: Python, SQL, data pipelines for detection triage, Tableau, Power BI, Excel (Advanced)

AI: Understanding of LLM misuse for cyber threats; writing and evaluating prompts for generative AI systems; applying LLM tooling (Claude Code, ChatGPT) to research and detection workflows

Certifications: Harvard: Data Science, Machine Learning | IBM: Penetration Testing, Threat Hunting and Cryptography; Data Analysis with Python

LANGUAGES

English / Spanish (Bilingual) | French (Beginner) | Russian (Beginner)