JOSE IGNACIO SUAREZ MONTIEL

jisumov@gmail.com
linkedin.com/in/jisumov
github.com/jisumov
jisu.mov/portfolio

EDUCATION

Master of Science (M.Sc.), Cybersecurity (Planned 2027-2029) — Georgia Institute of Technology
Bachelor of Engineering (B.E.), Computer Systems Engineering — National University of Colombia

CERTIFICATIONS

CompTIA Cybersecurity Analyst (CySA+) Certification
Microsoft Certified: Security Operations Analyst Associate (SC-200)
ISC2 Systems Security Certified Practitioner (SSCP)

EXPERIENCE

Company: Amadeus — April 2026 - Present
Title: Information Security Analyst

- Assess 400+ detection rules from CrowdStrike Falcon and Microsoft Defender XDR, utilizing Next-Gen SIEM, Sentinel and Splunk to map event flows and render accurate risk evaluations for cloud and on-premise infrastructures.
- Deploy 15+ Python scripts to accelerate triage from platforms including PhishER, Abnormal AI, and Entra ID, querying OSINT APIs to identify deviations, validate anomalous indicators, and auto-generate investigation findings.
- Review emerging threat intelligence feeds to surface potential exposures on 75,000+ resources in Qualys and enterprise management systems, facilitating vulnerability prioritization and remediation across global security teams.
- Provide specialized security oversight for 10+ subsidiaries and external clients via Cortex XDR, Azure, and business intelligence tools, standardizing threat visibility and refining defensive posture through the managed environments.

Company: Auxis — December 2024 - April 2026
Title: SOC Analyst

- Investigated 200+ monthly security alerts through Microsoft Defender XDR, applying risk-based triage to determine escalation and coordinating with cross-functional teams to ensure timely and effective end-to-end incident response.
- Conducted proactive threat hunting across 25,000+ assets, using internal and open-source threat intelligence with endpoint, identity, and network telemetry correlation to uncover early compromise and reduce detection latency.
- Produced internal knowledge resources for L1/L2 analysts, improving tool proficiency by outlining KQL queries, log source paths, and investigation insights from Microsoft Defender XDR, Sentinel, Entra ID and ServiceNow.
- Coordinated high-priority incidents with L3, infrastructure, engineering, field services, and risk teams, expediting containment and recovery while aiding root cause analysis and executive reporting to prevent recurrence.

Company: Caseware — June 2024 - December 2024
Title: Software Developer Co-op

- Applied server-to-server authentication endpoints to strengthen authorization controls across internal services, and upgraded five Python dependencies to remediate security issues, validating reliability through integration testing.
- Proposed canonical path validation, input sanitization, and access boundary safeguards within the SSDLC to prevent directory traversal attacks, effectively defining a robust file-access procedure and augmenting security posture.

SKILLS AND TECHNOLOGIES

Microsoft Defender XDR, Sentinel, Entra ID, Splunk, CrowdStrike Falcon, Cortex XDR, PhishER, Abnormal AI, Qualys, Python, ServiceNow, NIST 800-61, MITRE ATT&CK, ISO 27001, Incident Response, Malware Analysis, Threat Hunting.