Jesus Andres Perez Duerto

Director of Network Security, Santander Bank · Founder, Red Hound Information Security

New York City, USA jperezduerto.info linkedin.com/in/jperezduerto github.com/jperezduerto redhound.us

PROFESSIONAL SUMMARY

Seasoned cybersecurity expert with executive presence, extensive engineering capabilities, and a strong focus on offensive security challenges. Proficient in deploying security programs from policy development through hands-on implementation of comprehensive tool stacks. Highly motivated and adept at leading cybersecurity teams, developing training, and mentoring others. Skilled in tackling complex cybersecurity challenges, excelling in offensive security, and communicating technical concepts effectively in English and Spanish.

TOP SKILLS

- Building and leading cybersecurity teams
- Designing, implementing, and managing cybersecurity tools and infrastructures
- Offensive security mindset to perform red and purple team exercises
- Automating cybersecurity operations and incident response
- Creating and teaching cybersecurity training

SOFT SKILLS

- Problem-solving under pressure
- Quick learner with little instruction
- Explaining complex technical concepts in simple ways
- Embracing new professional challenges
- Continuous professional development
- Bilingual — English and Spanish

COURSES AND CERTIFICATIONS

Apr 2026 **GIAC Strategic Planning, Policy, and Leadership (GSTRT)** — SANS MGT514 · License #4279

Jan 2024 **Certified Red Team Professional (CRTP)** — Altered Security · #ADLID8313

Jun 2021 **Enterprise Attacker Emulation and C2 Implant Development** — Wild West Hackin' Fest

Jun 2018 **GIAC Web Application Penetration Tester (GWAPT)** — SANS SEC542 · License #6786

Mar 2018 **Certified Ethical Hacker (CEH)** — EC-Council · #ECC30215408965

Jan 2018 **Certified Network Defender (CND)** — EC-Council · #ECC52595515682

Jun 2016 **Penetration Testing with Kali Linux (PWK)** — Offensive Security

Apr 2015 **GIAC Security Essentials (GSEC)** — SANS SEC401 · License #36727

Aug 2014 **Fortinet FCNSP / NSE4 Certified** — #FCNSP-2014-20681

Jun 2013 **Cisco Certified Academy Instructor (CCAI)**

Jul 2009 **Cisco Certified Network Associate (CCNA)** — Cisco ID #CSCO11636078

Sep 2024 **Certified Red Team Expert (CRTE)** — Altered Security · #RTLID2837

Feb 2023 **Attacking & Defending Azure** — Altered Security

Aug 2018 **Applied Data Science and Machine Learning for Cyber Security** — Black Hat 2018

Mar 2018 **Certified EC-Council Instructor (CEI)** — #ECC91614970119

Feb 2018 **Certified Incident Handler (ECIH)** — EC-Council · #ECC71193024028

Nov 2016 **ITIL Foundation Certificate in IT Service Management** — #5838720

Mar 2016 **GIAC Continuous Monitoring and Security Operations (GMON)** — SANS SEC511 · License #133

Apr 2015 **GIAC Advisory Board** — GIAC Certifications

May 2014 **Fortinet FCNSA Certified** — #FCNSA-2014-19373

Jun 2012 **CCNA Security** — Cisco ID #CSCO11636078

ACADEMIC EDUCATION

2006 - 2010 | **Telecommunications Engineer** — Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional (UNEFA), Caracas, Venezuela.

PROFESSIONAL EXPERIENCE

Nov 2024 - Present (1 yr 10 mos) | **Santander Bank, N.A.** — New York, USA

Director of Network Security

- Lead network security controls across all U.S. entities as part of the U.S. CISO team, setting technical direction and driving the security posture beyond audit and regulatory requirements.
- Own firewalls, IPS, Web Application Firewalls, anti-DDoS, Network Access Control, VPNs, and web proxies across the estate.
- Partner with cloud security teams on cloud network security and defence against evolving threats.
- Lead cross-functional teams in threat analysis and continuous security optimisation, within budget.

Oct 2018 - Present (7 yrs 11 mos) | **Red Hound Information Security** — Remote

Founder

- Independent consultancy helping small and mid-sized businesses stay secure: penetration testing, virtual CISO engagements, and security strategy.

Jul 2022 – Nov 2024 (2 yrs 5 mos) | **Santander Digital Services** — United States

Global Cyber Defend Service Manager

- Led global cyber defence delivery for Santander worldwide: network security, identity and access management, anti-malware, Security Operations Center, incident response, threat detection, and vulnerability management.
- Managed and mentored a team of regional cybersecurity leaders, working directly with each entity's CISO to align local engineering with the global strategy.
- Brought every newly onboarded global entity onto a common technical standard.

Oct 2020 – Aug 2022 (1 yr 11 mos) | **Santander Digital Services** — Boston, USA

Head of Protect for North America

- Directed a team of 120 across network security, identity and access management, anti-malware, and end-user protection for Santander in the US, Mexico, and Latin America.
- Integrated 80 engineers from Mexico into a single cross-border team.
- Established cybersecurity services for the Santander entities in Mexico, Uruguay, Peru, and Colombia.

Nov 2019 – Oct 2020 (1 yr) | **Santander Digital Services** — Boston, USA

Director of Cyber Security Infrastructure

- Built and led a team of 25 engineers across the US, extending the service to every Santander affiliate in the country.
- Owned firewalls, proxies, IPS, WAF, NAC, VPN, anti-malware, EDR, anti-phishing, web and email security, endpoint DLP, and virtual patching end to end.
- Hired, trained, and mentored the engineers who ran the platform.

Jan 2019 – Oct 2019 (10 mos) | **Advoqt Cybersecurity** — Boston, USA

Chief Information Security Officer

- Founded the cybersecurity practice and grew it past 20 new clients a year; hired and mentored 15 engineers while remaining hands-on for the engagements that required it.
- Delivered penetration tests and maturity assessments, including one across a large educational system.
- Deployed an open-source cloud SIEM across 30,000+ endpoints and applied machine learning to SIEM data for anomaly detection.
- Rebuilt a Splunk deployment for lower cost and broader detection coverage; devised a method to identify and remove superfluous firewall rules at a major financial institution.

Nov 2017 – Jan 2019 (1 yr 3 mos) | **Advoqt Cybersecurity** — Boston, USA

Lead Security Engineer

- Consultant and advisor across finance, retail, and telecommunications: ran web application penetration tests, designed and built a Security Operations Center end to end, and set cloud security direction.

Nov 2017 – Oct 2019 (2 yrs) | **CyberWarrior Academy** — Boston, USA

Co-founder & Instructor

- Master instructor and curriculum designer: EC-Council certifications, hands-on hacking skills, programming for hackers, and professional development.

May 2015 – Nov 2017 (2 yrs 7 mos) | **Produban** — Boston, USA

Cyber Security Consultant

- Technical lead for the cybersecurity services delivered to Santander Bank in the US, embedded in the IT Risk department.
- Implemented Tenable Security Center for vulnerability scanning and Splunk Enterprise as the SIEM.
- Led a review and rebuild of the configuration of every network security device in the estate.
- Ran SSL certificate, vulnerability, and firewall management; automated security tooling and compliance reporting; second-level incident response.

Mar 2014 – May 2015 (1 yr 3 mos) | **C.G.S.I.** — Caracas, Venezuela

Senior IT Security Consultant

- Technical lead across financial and retail clients — designed, implemented, and then operated the solutions.
- Deployed FortiGate and McAfee firewalls and IPS, Arbor anti-DDoS, McAfee web and mail gateways, FortiMail, FortiWeb, FortiBalancer, and FortiAnalyzer.
- Technical lead on big data, SIEM, and credential management with Splunk, LogRhythm, and the ELK stack.
- Penetration testing across wireless, Windows, Linux, and web applications; technical lead on social engineering assessments for banking and insurance clients.
- Automated the vulnerability scanning process through the Qualys API.

Jul 2013 – Mar 2014 (9 mos) | **Dayco Telecom** — Caracas, Venezuela

Network and Security Specialist III

- Security architect for core infrastructure and key clients — produced the designs and implemented them personally.
- Designed the network and perimeter security for the new datacenter in Valencia, Venezuela.
- Built proof-of-concept labs for Cisco, Corero, Sourcefire, Palo Alto, and Fortinet, and presented the recommendations to the executive team.
- Optimised the core security platform; ran McAfee IPS, FortiGate, and FortiAnalyzer; third-level incident response and internal staff training.

Feb 2012 – Jul 2013 (1 yr 6 mos) | **Dayco Telecom** — Caracas, Venezuela

Network and Security Specialist II

- Second-level response for the most important clients: banks, supermarkets, lottery, and insurance.
- Managed Cisco routers and switches, BlueCoat PacketShaper, Cisco ASA, and Fortinet firewalls; fault detection through packet capture and protocol analysis.
- BGP, OSPF, EIGRP, STP, EtherChannel, VTP, HSRP, switch stacks, firewall clusters, IPsec and SSL VPNs; Frame Relay, Metro Ethernet, MPLS, and QoS.

Mar 2011 – Aug 2013 (2 yrs 6 mos) | **Cisco Networking Academy** — Caracas, Venezuela

Cisco Network Instructor

- Instructor for modules I–IV of the Cisco Certified Network Associate (CCNA) program, as a CCAI-certified instructor.

Mar 2011 – Feb 2012 (1 yr) | **Banco Agrícola de Venezuela** — Caracas, Venezuela

Telecommunications Specialist III

- Security architect for the bank's new main datacenter — designed every security control and implemented them end to end.
- Firewalls, IPS, email security, and Cisco Access Control; encrypted connections to other banks and service providers; VPNs for remote access.
- Ran the nationwide telecommunications platform, optimised EIGRP, deployed OpenNMS monitoring, and managed Cisco Call Manager IP telephony and voice E1 circuits.
- Layer 2 security — port security, dynamic ARP inspection, DHCP snooping, IP source guard, spanning tree optimisation — and QoS across WAN links.

May 2010 – Mar 2011 (11 mos) | **Ministerio de Agricultura y Tierras** — Caracas, Venezuela

Telecommunications Analyst

- Managed switches and access points; WAN fault management across Frame Relay and Metro Ethernet.
- Administered Cisco Call Manager and deployed VoIP to remote offices, including voice controllers and QoS policy.
- Managed FortiGate firewalls and FortiAnalyzer; internal and external network security analysis with Nessus, Nmap, and Metasploit.
- Layer 2 LAN security, OpenNMS monitoring server, and Linux DNS configuration.

AWARDS

- 3rd place, 8th Latin American Robotics Competition (LARC), OPEN category — Valparaíso, Chile, October 2009.
- 2nd place, Municipal Prize for Science, Technology and Innovation "Dr. Humberto Fernández Morán", higher education category — Caracas, June 2011.