Jean Carlos Cedré Rosado

jccedre@gmail.com | LinkedIn

Summary

Offensive security engineer with 10+ years of experience across red teaming, penetration testing, and secure development. Lead Red/Purple Team engagements that simulate advanced threat actors, translate attack narratives into clear risk insights for technical and executive audiences, and partner closely with IR/CTI and engineering teams to drive remediation and detection improvements. Strong scripting/automation background (Python) with experience building internal tooling and repeatable workflows.

Selected Offensive Security Highlights

- Led Red/Purple Team exercises and full-scope penetration tests in a global financial services environment, simulating real-world adversary behavior across enterprise networks, systems, and applications.
- Demonstrated macOS tradecraft during a multi-week engagement, maintaining stealthy access to reveal detection and response gaps and drive endpoint security improvements.
- Built and maintained internal red team tooling, scripts, and reusable engagement infrastructure; automated environment stand-up/tear-down to accelerate operations and improve repeatability.
- Partnered with Incident Response and Cyber Threat Intelligence teams to develop detections and signatures informed by observed threats and red team TTPs.
- Produced clear, actionable findings for engineering and leadership stakeholders, translating exploit chains and attack narratives into prioritized remediation guidance.

Experience

Lead Red Team Operator | T. Rowe Price | Remote | September 2025 - Current

- Lead 4–6 adversarial engagements annually, including full-scope penetration tests and Red/Purple Team exercises against enterprise networks, systems, and applications within a global financial services environment.
- Orchestrate Red and Purple Team exercises in close collaboration with Incident Response and Cyber Threat Intelligence teams, driving measurable improvements to detection and response capabilities across the firm.
- Identified and reported hundreds of vulnerabilities across enterprise systems, translating complex security risks into actionable remediation guidance for technology and leadership stakeholders.
- Spearheaded detection improvements within the firm's code repository environment, partnering with engineering teams to close critical security gaps in the software development lifecycle.
- Advise senior leadership and key stakeholders on offensive security findings, bridging the gap between technical risk and business impact in a highly regulated financial services context.
- Lead and mentor a team of 4 red team operators, conducting work reviews and providing ongoing feedback to continuously elevate team capabilities.
- Conducted a full-scope macOS Red Team exercise, achieving multiple compromised hosts and maintaining undetected dwell time exceeding two weeks, exposing critical gaps in endpoint detection and response capabilities.

Senior Red Team Operator | T. Rowe Price | Remote | October 2022 - September 2025

- Performed penetration testing across enterprise networks, systems, applications, and technology stacks.
- Developed and coordinated Red/Purple Team exercises using Cobalt Strike, Mythic, and other red team tooling and infrastructure.
- Added to the Red Team repository of code and scripts by creating custom tools used internally for Red Team operations.
- Contributed to a continuous attack validation program to monitor controls and automate threat simulations.
- Identified, recommended, and built detections and signatures in response to new or observed cyber threats, supporting Incident Response and Cyber Threat Intelligence teams.
- Improved team standard operating procedures (SOPs) and methodologies to increase consistency and quality of engagements.
- Collaborated with peers and mission stakeholders to provide input and continuously improve red team practices.

- Spearheaded creation of automation to stand up and tear down red team infrastructure.
- Improved operational rigor by implementing After-Action Reviews (AARs) following red team operations.
- Documented red team TTPs and built a searchable knowledge base to improve onboarding and execution.

Mission Element Lead – Cyber Protection Team | US Army Reserve | Ft. Dix, NJ | September 2024 - Current

- Synchronize readiness and training for the mission element in support of the 301st Cyber Battalion (CYBN) and U.S. Army Reserve Cyber Protection Brigade (ARCPB).
- Lead and coordinate reconnaissance and counter-reconnaissance activities to counter and clear malicious cyberspace activity (MCA).
- Enable hardening of designated terrain in cyberspace; assess response action effectiveness relative to current and residual risk.
- Updated and published standard operating procedures (SOPs) using stakeholder, customer, and employee feedback, improving clarity and usability.
- Provide leadership, mentorship, and professional development to assigned Soldiers and non-commissioned officers.

Cyber Electronic Warfare Officer | US Army | Tacoma, WA | October 2019 - October 2022

- Updated and published standard operating procedures (SOPs) using stakeholder, customer and employee input and feedback resulting in clearer and more useful instruction for users.
- Maximized performance by monitoring daily activities and mentoring 15 team members.
- Coordinated and led meetings to inform management and stakeholders of operational challenges and suggested improvements.
- Coordinated visits and provided briefs to very important personnel (VIPs) improving knowledge and awareness of operational activities, programs and offerings.
- Verified compliance with best business practices throughout organization.
- Implemented processes that simplified procedures and reduced average processing time.
- Applied leading theories and concepts to development, maintenance, and implementation of information security standards, procedures, and guidelines.
- Represented the organization's technical security interests to partners, enabling bi-directional sharing of security best practices and technical information.
- Counseled senior leadership on privacy and security trends, with recommendations to mitigate risk.

Hiring Our Heroes Corporate Fellow | PwC | Cyber Risk & Regulatory | May 2022 - July 2022

- Supported cybersecurity, cyber risk management, and technology risk management initiatives for large client engagements.
- Designed and developed cybersecurity and technology risk programs aligned to industry frameworks and methodologies.
- Assessed enterprise cyber risks and threat exposure to inform program and control recommendations.
- Supported design and implementation of risk management controls; used tooling and analytics to surface insights on threats, risks, and vulnerabilities.
- Supported client engagements by gathering requirements, clarifying needs, and contributing to solution approaches.
- Participated in client discussions and working sessions to align on scope, risks, and deliverables.
- Supported multiple workstreams, tracking tasks and coordinating across stakeholders to meet deadlines.
- Assisted with engagement management activities, including status tracking and coordinating next steps.
- Prepared concise project documentation and deliverables using MS Office and Google Workspace.
- Maintained and updated project deliverables to reflect scope changes and stakeholder feedback.
- Provided timely, actionable feedback to team members to improve quality and execution.
- Kept managers and engagement leadership informed of progress, risks, and delivery issues.

Web Developer | Posture Interactive | Scranton, PA | August 2017 - April 2019

- Consulted with marketing department to ascertain organizational requirements, then compile, refine and generate webpage roadmap to achieve objectives.
- Oversaw back-end development using PHP to maintain website integrity, security, and efficiency.

- Counseled senior-level management on current privacy and security trends and recommendations to mitigate risk.
- Planned website development, converting mockups into usable web presence with HTML, JavaScript, AJAX and JSON coding.
- Provided front-end and back-end development using WordPress and React.
- Established presentation consistency across Chrome, Safari, Firefox and other common browser interfaces.
- Implemented website maintenance, content management, updates and security resource tutorials to assist end-user training.
- Determined coding requirements for site creation, e-commerce capability, security and specialized scripts.
- Collaborated with other developers to identify and alleviate software errors and inefficiencies.

Web Developer | 15Four | Baltimore, MD | June 2016 – August 2017

- Collaborated with marketing, representing web team to establish project goals, projections and milestones.
- Applied leading theories and concepts to development, maintenance, and implementation of information security standards, procedures, and guidelines.
- Planned website development, converting mockups into usable web presence with HTML, JavaScript, AJAX and JSON coding.
- Established presentation consistency across Chrome, Safari, Firefox and other common browser interfaces.
- Maintained and implemented new functionality in existing Drupal/WordPress-based client sites.
- Worked with project managers to help set project expectations and create estimates based on capabilities and limitations of project goals.

Program Coordinator | Digital Harbor Foundation| Baltimore, MD | December 2014 - June 2016

- Plan and prepare new maker and/or technology content for delivery to youth, including creation of lesson plans, curricular content, video tutorials.
- Organized and managed program development from conception through successful execution.
- Orchestrated smooth and efficient program development by collaborating cross-functionally across departments.
- Led and taught elementary, middle, and high school-aged youth in maker and technology activities.
- Supported youth-centric learning by developing skills related to new tools and resources for maker activities.
- Researched, evaluated, and implemented new technology tools and resources to enhance DHF programs.

Education

B.S., Web Development | Capitol Technology University | 2015 – 2017

Certifications

- OffSec - OffSec Certified Professional (OSCP) | In Progress
- Zero Point Security – Red Team Operator I | September 2023
- CompTIA CASP+ | April 2022
- CompTIA Cloud+ | February 2022
- Splunk 7.x Fundamentals 1 | September 2021
- Splunk 7.x Fundamentals 2 | September 2021
- CompTIA Security+ | August 2021
- Virtual Hacking Labs – Penetration Testing Course | December 2020

Security Clearance

Top Secret / SCI / CI Poly

Skills

- **Programming Languages:** JavaScript, React, Python, PHP, HTML
- **Expertise:** Team & Project Management, Translating Technical Concepts, Training Teams, Creating Curriculum
- **Tools:** Cobalt Strike, Mythic, GitHub, Wireshark, Splunk, VS Code, iTerm, Asana, Slack, MS Teams, Office 365, Adobe Creative Suite