Jean Carlos Cedré Rosado

Lead Red Team Operator · Security Program Leadership & Infrastructure Security
jccedre@gmail.com | (443) 676-3004
linkedin.com/in/jccedre | github.com/jccedre

SUMMARY

Red team and infrastructure security leader with 10+ years of experience across penetration testing, adversarial exercises, and security operations. Leads cross-functional security initiatives, aligns engineering and response teams on risks and remediation, and communicates technical findings and trade-offs to senior stakeholders. Brings hands-on experience with enterprise networks, security tooling, automation, and repeatable operational processes.

SELECTED OFFENSIVE SECURITY HIGHLIGHTS

- Led Red/Purple Team exercises and full-scope penetration tests in a global financial services environment, simulating 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 and tear-down to improve operational repeatability.
- Partnered with Incident Response and Cyber Threat Intelligence teams to develop detections and signatures informed by observed threats and red team TTPs.
- Translated exploit chains and attack narratives into prioritized remediation guidance for engineering and leadership stakeholders.

EXPERIENCE

T. Rowe Price · Remote · September 2025 – Present
Lead Red Team Operator

- Lead 4–6 adversarial engagements annually, including full-scope penetration tests and Red/Purple Team exercises across enterprise networks, systems, and applications.
- Coordinate Red and Purple Team exercises with Incident Response and Cyber Threat Intelligence, driving improvements to detection and response capabilities.
- Reported hundreds of vulnerabilities across enterprise systems and translated security risks into actionable remediation guidance for technology teams and leadership.
- Advise senior leaders and stakeholders on offensive security findings, communicating technical risk and business impact in a highly regulated environment.
- Lead and mentor four red team operators, reviewing work and providing ongoing feedback.
- Partnered with engineering teams on detection improvements in the firm's code repository environment to address software development lifecycle security gaps.
- Conducted a full-scope macOS Red Team exercise, compromising multiple hosts and maintaining undetected access for more than two weeks, exposing endpoint detection and response gaps.

T. Rowe Price · Remote · October 2022 – September 2025
Senior Red Team Operator

- 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.

- Built custom tools and scripts for internal red team operations and automated the stand-up and tear-down of red team infrastructure.
- Contributed to continuous attack validation by monitoring controls and automating threat simulations.
- Built detections and signatures in response to observed cyber threats, supporting Incident Response and Cyber Threat Intelligence teams.
- Improved engagement consistency through updated standard operating procedures (SOPs), methodologies, and After-Action Reviews (AARs).
- Documented red team TTPs and created a searchable knowledge base to support onboarding and execution.

US Army Reserve · Ft. Dix, NJ · September 2024 – May 2026

Mission Element Lead – Cyber Protection Team

- Coordinated readiness and training for a mission element supporting the 301st Cyber Battalion and U.S. Army Reserve Cyber Protection Brigade.
- Led reconnaissance and counter-reconnaissance activities to counter and clear malicious cyberspace activity.
- Supported cyberspace hardening and assessed response action effectiveness relative to current and residual risk.
- Updated SOPs using stakeholder, customer, and employee feedback to improve clarity and usability.
- Led, mentored, and supported the professional development of assigned Soldiers and non-commissioned officers.

US Army · Tacoma, WA · October 2019 – October 2022

Cyber Electronic Warfare Officer

- Applied information security concepts to develop, maintain, and implement security standards, procedures, and guidelines.
- Counseled senior leadership on privacy and security trends and recommended risk mitigation measures.
- Represented technical security interests with partners, enabling two-way sharing of security practices and technical information.
- Mentored 15 team members and coordinated stakeholder meetings on operational challenges and potential improvements.
- Updated SOPs based on stakeholder and user feedback, improving clarity and usability.
- Implemented process changes that simplified procedures and reduced average processing time.
- Verified compliance with organizational best business practices.

PwC · May 2022 – July 2022

Hiring Our Heroes Corporate Fellow · Cyber Risk & Regulatory

- Supported cybersecurity, cyber risk management, and technology risk initiatives for large client engagements.
- Assessed enterprise cyber risks and threat exposure to inform program and control recommendations.
- Contributed to cybersecurity and technology risk programs aligned with industry frameworks and methodologies.
- Supported risk control design and implementation, using tooling and analytics to surface insights on threats, risks, and vulnerabilities.
- Coordinated workstreams, tracked tasks and delivery risks, and kept managers and engagement leaders informed of progress and issues.
- Worked with clients and stakeholders to clarify requirements, align on scope and deliverables, and update project documentation as needs changed.

Posture Interactive · Scranton, PA · August 2017 – April 2019
Web Developer

- Oversaw PHP back-end development to maintain website integrity, security, and efficiency.
- Built front-end and back-end functionality using WordPress, React, HTML, JavaScript, AJAX, and JSON.
- Collaborated with developers to identify and resolve software errors and inefficiencies.
- Advised senior-level management on privacy and security trends and risk mitigation recommendations.
- Planned website development with marketing stakeholders and maintained website content, functionality, and security resources.

EDUCATION

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

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: Security program coordination, stakeholder communication, team leadership, risk assessment, remediation guidance, training

Tools: Cobalt Strike, Mythic, GitHub, Wireshark, Splunk, VS Code, iTerm