Jaime Gómez Recasens

Senior Platform & Cloud Security Engineer

Madrid, Spain · open to remote +34 654 022 262 jaimegomezrecasens@gmail.com
linkedin.com/in/jaimegomezrecasens jaimegomezrecasens.es

SUMMARY

Senior Platform and Cloud Security Engineer with 20+ years in infrastructure, the last five at Rithum, where I was promoted to Senior in February 2025. My work sits where infrastructure meets security on hybrid AWS and VMware platforms: patching at scale, immutable server images, security-tool rollouts and migrations, privileged-access reporting and SOC 2 evidence. I check that a control actually works, not just that the ticket is closed, and automate what used to be manual.

SKILLS

Hands-on, day to day

Windows Server, Active Directory and Group Policy, VMware vSphere, patch management at scale, AWS EC2 and AMIs, Packer, GitHub Actions

Working knowledge

Terraform, Spacelift, Ansible, Linux (LPIC-2), PowerShell, Bash, Python scripting, Zabbix, ELK

Security tools

CrowdStrike Falcon: EDR rollout, Next-Gen SIEM reports and searches. Google SecOps: migration. Tenable/Nessus.

Compliance

SOC 2 evidence, User Access Reviews, disaster-recovery testing

CERTIFICATIONS

AWS Certified Solutions Architect – Associate

LPIC-1 and LPIC-2

IN PROGRESS

AWS Certified Security – Specialty · January 2027

EXPERIENCE

Rithum May 2021 – present

Platform Engineering · Senior Infrastructure Engineer (Feb 2025 – present) · Systems Engineer (May 2021 – Feb 2025)

- **Privileged-access monitoring.** Replaced manual screenshots of privileged Active Directory groups with automated reporting in CrowdStrike Falcon Next-Gen SIEM for the quarterly User Access Reviews. Found a monitoring blind spot: membership was enforced through a Group Policy (Restricted Groups), so group-change alerts missed the real change path. Now building detection on changes to that policy to close the gap.
- **SIEM migrations.** Ran the migration of the legacy SIEM (ELK) to Google SecOps (Chronicle), reducing cost, and later to CrowdStrike Falcon Next-Gen SIEM, where I now build reports and searches.
- **Immutable images.** Built an automated AWS AMI pipeline with Packer and GitHub Actions (monthly scheduled builds, four Windows variants) validated through Spacelift, and laid the groundwork for VMware infrastructure as code with Terraform.
- **Patch management at scale.** Designed and run the monthly Microsoft patching process across 12+ environments, from development to production, including AWS and VMware templates. Cut recurring problem servers from 14+ to fewer than 10, with no customer-visible downtime.

Continued on page 2

EXPERIENCE, CONTINUED

Rithum · Platform Engineering — May 2021 – present

- **Endpoint and vulnerability tooling.** Rolled out CrowdStrike to uncovered critical servers and consolidated vulnerability tooling, retiring Tenable from 8+ environments to reduce cost and complexity.
- **SOC 2.** Infrastructure point of contact for SOC 2 evidence. Produce evidence for infrastructure controls, route requests to the owning teams, and am automating evidence collection with AI.
- **Disaster recovery.** Coordinate the annual DR test across teams and execute the application restore test, recovering a production VM from backup to prove it can be restored.
- **Reliability and mentoring.** Resolved persistent performance issues on critical servers and caught capacity risks, such as disk, before they caused outages. Mentor new team members.

Pragsis · Systems Engineer and Big Data Engineer — Nov 2017 – Apr 2021

- Installed and administered the company's internal Big Data clusters and managed Google Workspace.
- Migrated email from Zimbra to Google Workspace and Active Directory from Windows Server 2003 to 2016.
- Automated self-service password resets and new-laptop provisioning, cutting setup time and support tickets.

CM Capital Markets · Systems Administrator — Jan 2006 – Nov 2017

- Designed and implemented a disaster-recovery site with VMware and HP EVA SAN, so trading positions could be closed if the primary data center failed.
- Managed perimeter security (firewall, VPN, centralized antivirus, anti-spam, proxy) and cut costs by moving proprietary tools to open source.
- Automated routine administration and supported business-critical financial platforms (Bloomberg, Reuters).

Earlier experience

- **Axpe Consulting, for Telefónica I+D (Imagenio)** · Systems Consultant, 2005. Integration and system testing for new service launches.
- **Adquira Spain (Telefónica, BBVA, Repsol, Iberia)** · Systems Administrator, 2001–2004. Led the migration of all workstations from Windows NT to Windows 2000 and of the NT domain to Active Directory.

EDUCATION

Computer Engineering (Ingeniero Informático)

Universidad Antonio de Nebrija, Madrid

LANGUAGES

Spanish · native

English · professional working proficiency, daily use at work