



Connect

Más allá de los CVEs: cómo Red Hat protege tu compañía

Mikel Olasagasti
Customer Success Executive

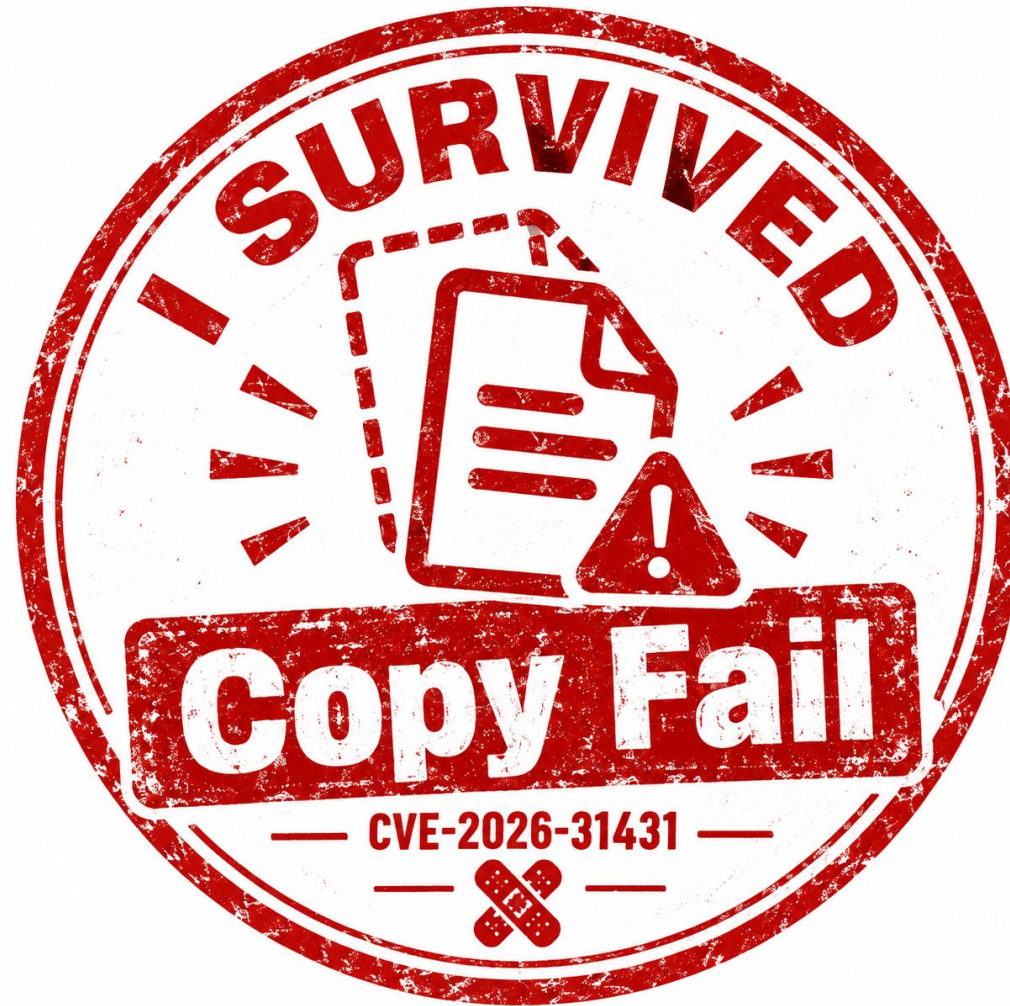
Florencio Cano
Principal Product Security Engineer

El kaos

Entre abril y mayo de este año vivimos unas semanas locas:

- ▶ Copy Fail (RHSB-2026-002)
- ▶ Dirty Frag (RHSB-2026-003)
- ▶ CIFS Witch (RHSB-2026-005)
- ▶ HTTP/2 Bomb (RHSB-2026-007)
- ▶ ipv6_frag_escape (RHSB-2026-009)
- ▶ GhostLock (RHSB-2026-010)
- ▶





🏆 ¡Nuevo logro desbloqueado! 🏆



Pero no es la primera crisis que tenemos...

- ▶ 2014: Heartbleed (OpenSSL) y Shellshock (Bash)
- ▶ 2017: WannaCry (EternalBlue)
- ▶ 2018: Meltdown y Spectre
- ▶ 2021: Log4Shell (Log4j)
- ▶ 2024: XZ Utils Backdoor
- ▶ 2026: Copy Fail y Dirty Frag
- ▶ 2027: ?



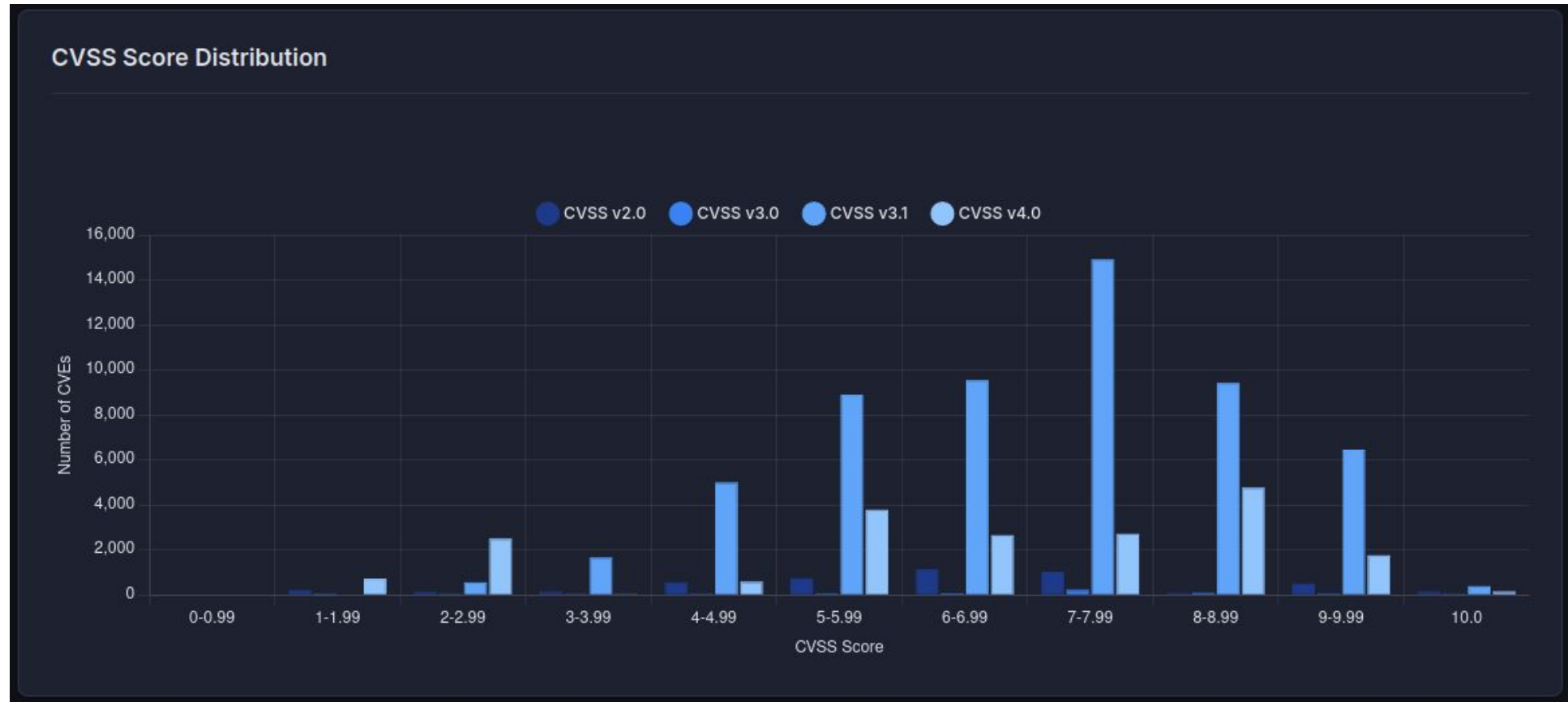
Linux kernel 7.2 casi 2000 CVE



CVEs have grown in the last years



Distribution of CVSS



Not all CVSS 10 are equal

- ▶ CVSS are calculated with a default configuration of a software and without context
- ▶ Is the software exposed to the Internet?
- ▶ Are there security controls in place that reduce the probability or impact of the vulnerability?

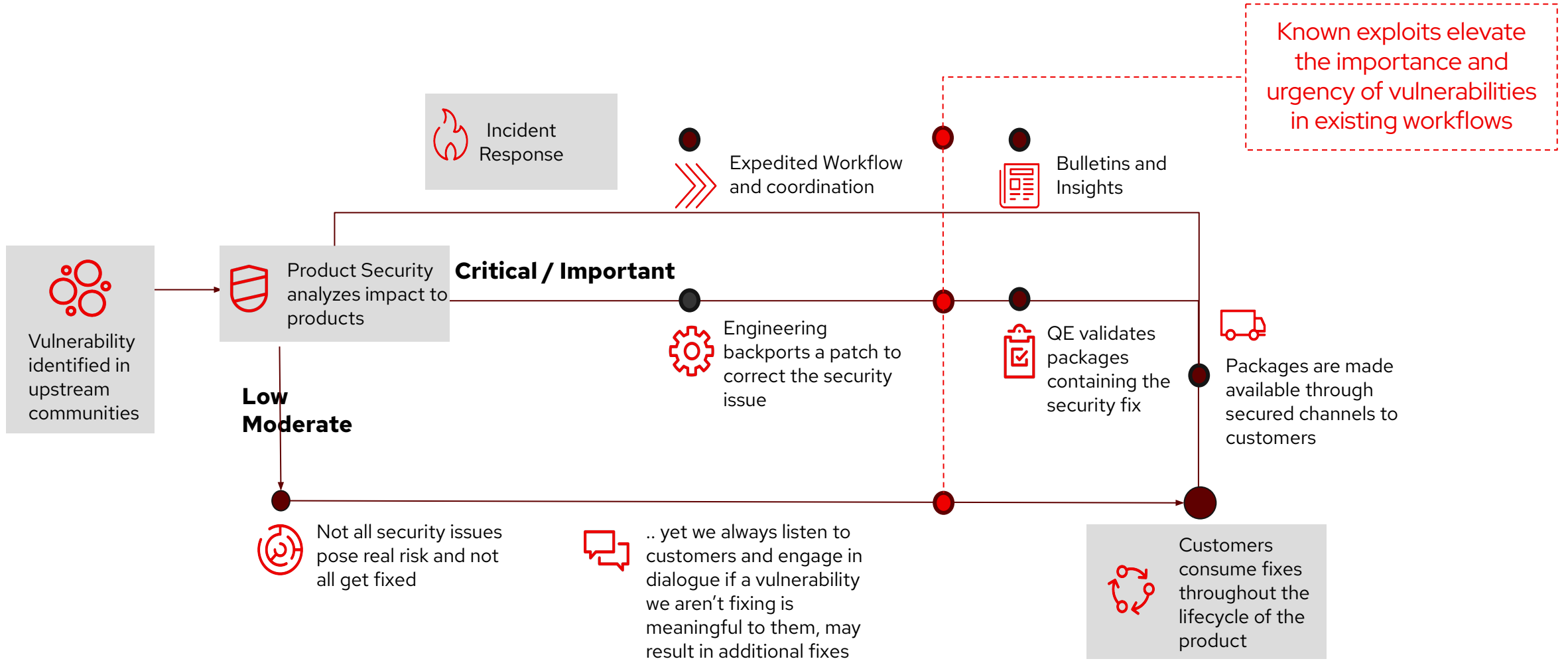


Red Hat Severity Rating Criteria

Severity ratings	Security flaw description
Critical impact	This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction, or easily cause system compromise via inference end points on AI systems. Flaws that require authentication, local or physical access to a system, or an unlikely configuration are not classified as Critical impact. These are the types of vulnerabilities that can be exploited by worms.
Important impact	This rating is given to flaws that can easily compromise the confidentiality, integrity or availability of resources. These are the types of vulnerabilities that allow local or authenticated users to gain additional privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication or other controls, allow authenticated remote users to execute arbitrary code, allow remote users to cause a denial of service, or can cause system compromise via inference end points on AI systems.
Moderate impact	This rating is given to flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity or availability of resources under certain circumstances. It is also given to flaws that could be exploited to cause denial of service-like conditions on AI systems via an inference end point, or allow attackers to steal other users' data from the AI system without authorization. These are the types of vulnerabilities that could have had a Critical or Important impact but are less easily exploited based on a technical evaluation of the flaw and/or affect unlikely configurations.
Low impact	This rating is given to all other issues that may have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences. This includes flaws that are present in a program's source code but to which no current or theoretically possible, but unproven, exploitation vectors exist or were found during the technical analysis of the flaw.



Vulnerability management at Red Hat



Red Hat works on reducing these numbers

- ▶ Red Hat Secure Software Development Life Cycle
 - Threat modeling
 - Secure Architecture Review
 - Static and dynamic analysis
 - Penetration testing



Patching is only part of the solution

- ▶ 31% of the breaches happen because exploited vulnerabilities*:
- ▶ Other frequent root causes:
 - Weak authentication systems (*exposed remote accesses + lack of MF2*)
 - Email attachments + local administrator privileges + privilege escalation + domain escalation



The diagram is an iceberg floating in a dark blue sea. The tip of the iceberg, which is above the water line, is white and contains text about visible security issues. The much larger part of the iceberg is submerged below the water line and is light blue. This submerged part contains a list of security practices. To the right of the water line, the text 'Lo que se escucha' (What is heard) is written. To the right of the submerged part, the text 'Lo que no siempre se ve' (What is not always seen) is written.

CVEs "con logo"
Avisos CERT genericos
El parche rápido

Lo que se escucha

Lo que no siempre se ve

- Hardening de caja: SELinux, SCCs, ...
- Analysis y VEX: rescoring
- Backporting
- Documentation
- Quality Engineering
- Identidad y auditoría
- Mitigación en vivo
- Certificaciones (ENS)
- Supply chain & SBOM
- Code signing
- Confidential Computing
- ...

Pregunta a la audiencia

¿Cuántos de vosotros tenéis **ventanas**
aprobadas para reiniciar
todas las máquinas
al menos
una vez por trimestre?



Pregunta a la audiencia

¿Cuántos de vosotros tenéis **ventanas**
aprobadas para reiniciar
todas las máquinas
al menos
una vez al mes?



Pregunta a la audiencia

¿Cuántos de vosotros tenéis **ventanas**
aprobadas para reiniciar
todas las máquinas
al menos
una vez cada 15 días?



Pregunta a la audiencia

**¿Cuántos de vosotros tenéis
SELinux enforcing
en todos los servidores?**



Red Hat aporta tecnología

Antes de añadir otra herramienta de seguridad, conoce las que ya tienes en la plataforma.

Protect

- SELinux
- fapolicyd
- systemd security features
- USBGuard
- nftables
- Kernel Lockdown
- Secure Boot
- dm-crypt / LUKS2
- seccomp
- Linux Capabilities
- cgroups / namespaces

Trust & Compliance

- System-wide Crypto-Policies
- Clevis & Tang
- OpenSCAP & FIPS 140-3
- IMA / EVM
- Post-Quantum Crypto (PQC)
- TPM 2.0 / measured boot
- Remote Attestation
- Confidential Computing

Detect & respond

- auditd
- Kpatch
- tlog
- keepalived
- Ansible system-roles
- Leapp
- AIDE



Red Hat aporta soluciones

De capacidades individuales a seguridad gestionada, automatizada y a escala.

Secure Infrastructure

- RHEL Image Mode
- Red Hat Lightspeed
- Red Hat Satellite
- Ansible Automation Platform
- RHEL IdM
- RHEL Edge

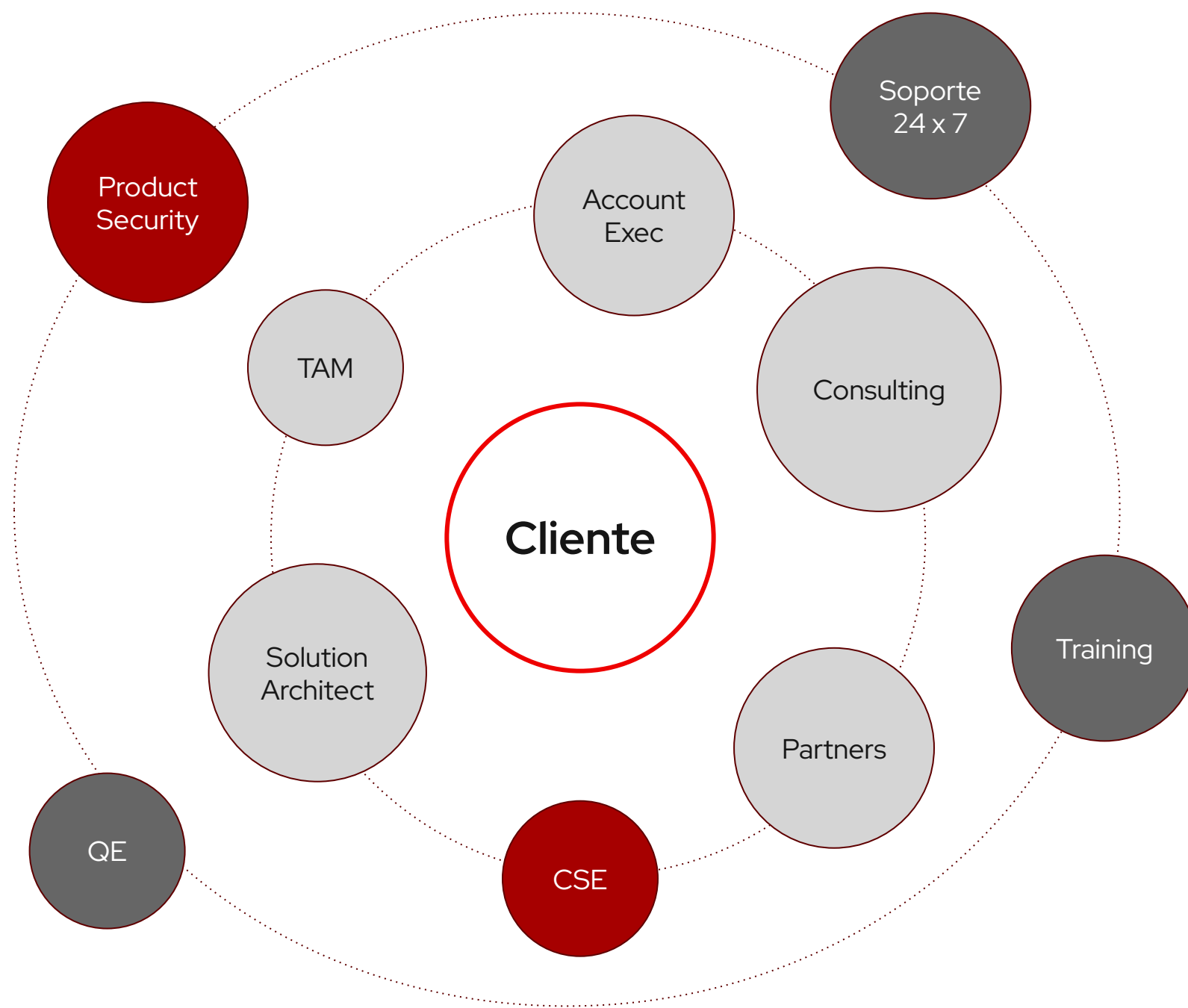
Secure Cloud Native

- Red Hat OpenShift
- Advanced Cluster Security (ACS)
- Advanced Cluster Management (ACM)
- MicroShift
- Hardened Images

Secure Software Supply Chain

- Red Hat Quay
- Trusted Artifact Signer
- Trusted Profile Analyzer
- Red Hat Developer Hub
- Trusted Libraries
- Advanced Developer Suite
- Lightwell Network





El valor de la suscripción

**La seguridad no empieza cuando aparece un CVE
ni termina cuando aplicamos un parche.**

Estar actualizado es importante.

Estar preparado lo es aún más.



Tech Journey demos: Red Hat Security



Webinar

Desplegando una fortaleza digital: no confíes,
siempre verifica y encripta tus datos

23 de octubre de 2026, 10:00 a.m.



Webinar

Automatización y seguridad: estrategia de
remediación integral con Red Hat

13 de noviembre de 2026, 10:00 a.m.





Hands-on Workshop Week • November 30, to December 4, 2026

Red Hat Tech Journey workshop week

One week. Four areas shaping enterprise IT. Hands-on experience.



Discover how to apply open source technologies to build secure platforms, automate operations, and run modern applications across hybrid environments.



Connect

Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



x.com/RedHat

