Red Hat Summit

Connect

Securing the Software Supply Chain in the AI-Era

From Code to Production: Managing Risk in Modern Development

Chris Jenkins
Senior Principal Chief Architect

Marc Loos
Senior Principal Account Solution Architect

Red Hat

The AI-Driven Velocity Surge

01

CVE Explosion

Machine-generated discovery of code flaws.

02

Transitive Debt

Hidden risk deep within enterprise dependencies.

03

Zero Weaponization Gap

Instant exploitation following public disclosure (if not before!)

Detection Without Remediation

Current Scanner Workflow

Surfacing Flaws

Generates thousands of unprioritized tickets.

Alert Fatigue

Engineering teams paralyzed by backlog.

Zero Fixes

Identifies danger without offering code.

Production Demands

Preserved Uptime

Zero breaking changes in production.

Stable APIs

Maintains existing system certifications.

Active Patches

Drops surgical fixes straight in.



Lightwell is your trusted AI Cyber remediation partner

Remediating Alone:

Your team triages the Mythos backlog internally. Three bad options for each finding:

cancel Upgrade and break production.

cancelPatch internally and carry a permanent fork.

cancelAccept the risk of a confirmed **exploit.**

Remediating with Lightwell:

We backport fixes to the exact versions you run in production:

check_circle No upgrades required - pinned backports.

check_circleSLA-backed delivery.

check_circleSigned artifacts.

check_circleEvery patch contributed upstream (where possible).

Confidential: Red Hat associates
and Partner NDA only

How Red Hat helps with the CVE flood

Help to secure open source libraries applications are **built with**

APPLICATION LAYER

Lightwell

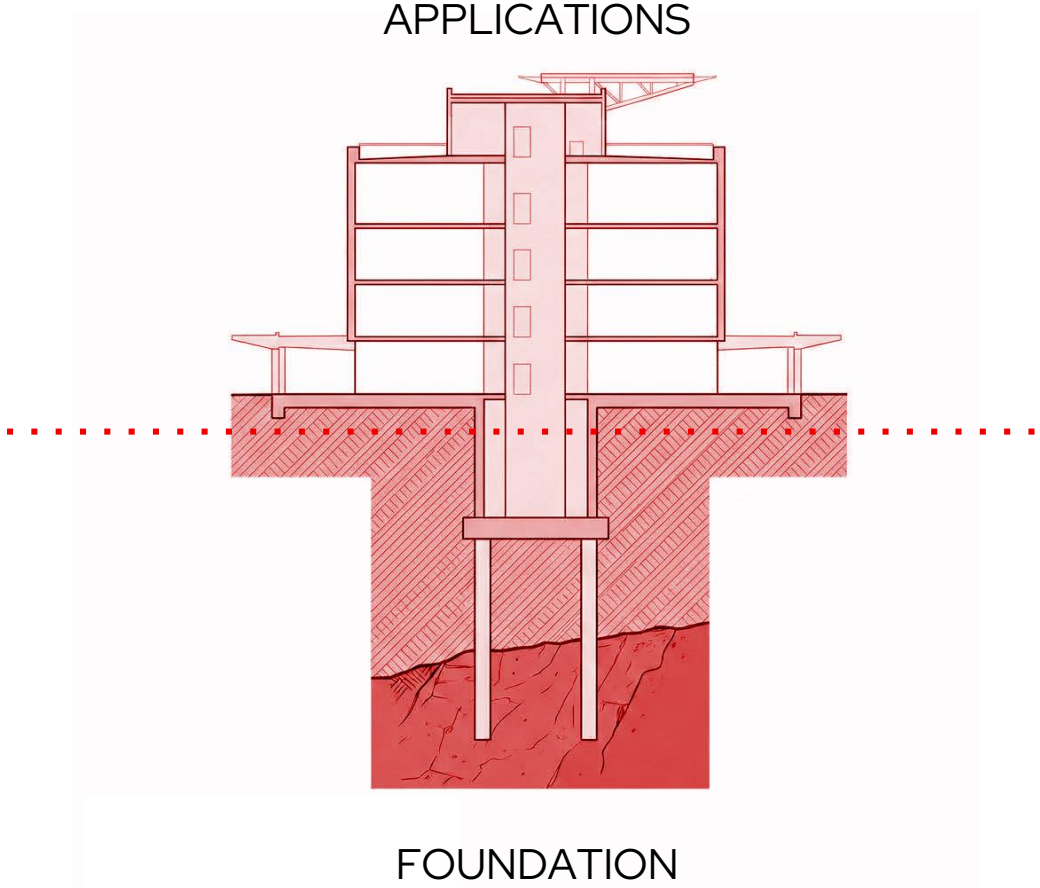
For customer Apps built on maven / PyPI / npm

Helps secure the open source libraries and dependencies that applications are ***built with.***

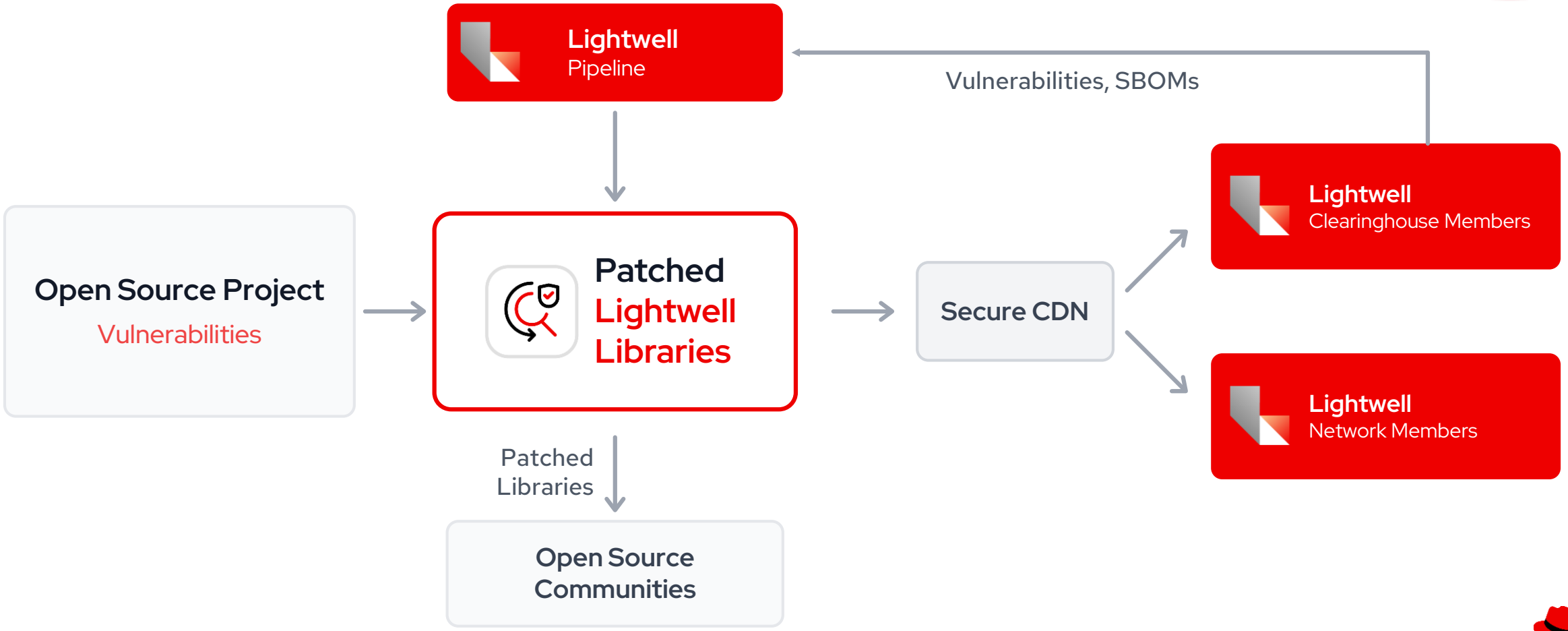
FOUNDATION LAYER

Red Hat Enterprise Linux

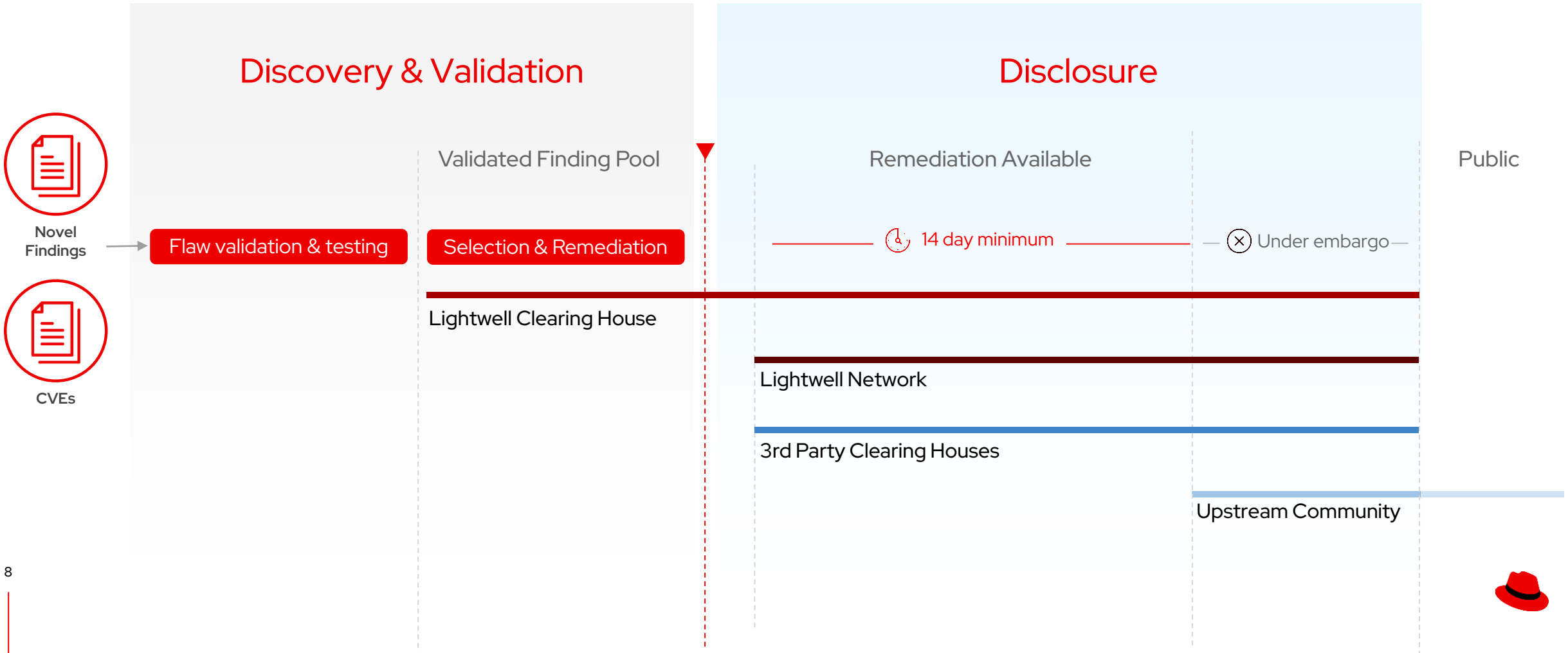
Red Hat Product Security helps secure the platform applications ***run on.***



Lightwell: How it works

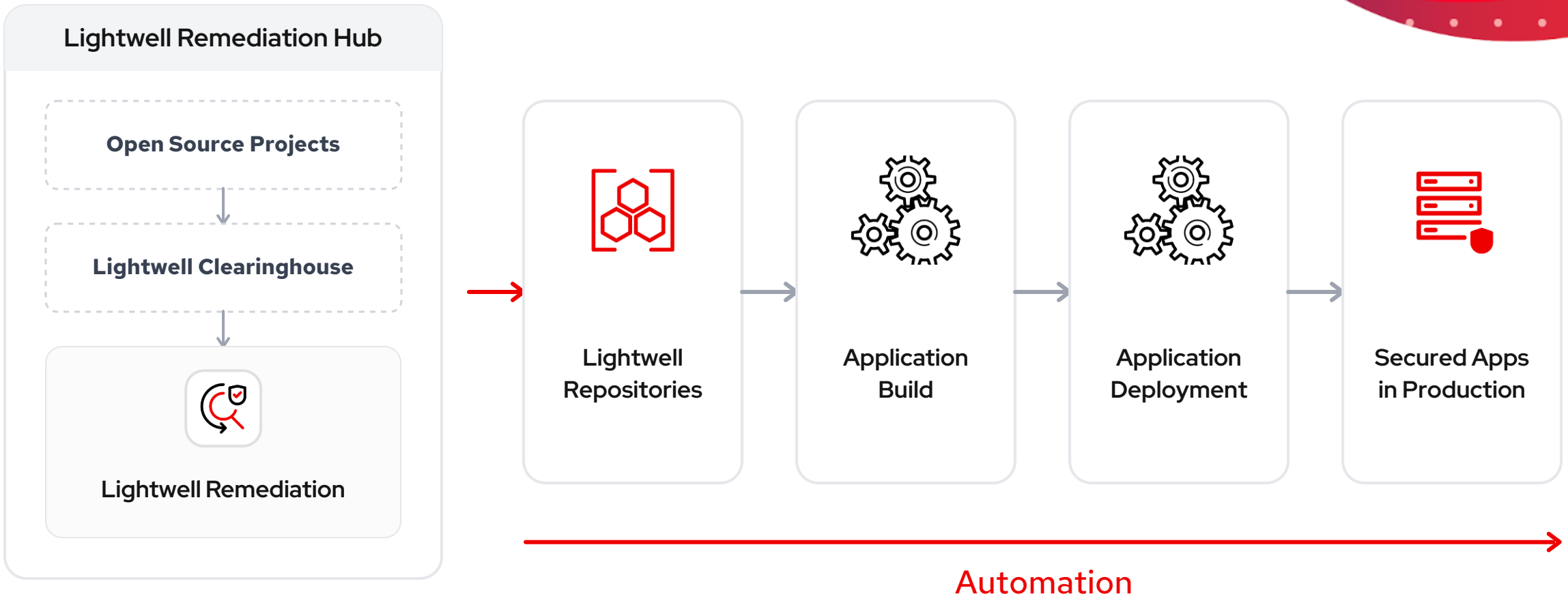


Lightwell Discovery & Disclosure



Lightwell is only part of the solution

Security Remediation + Rapid Deployment



Software Supply Chain Risk

The process of building and deploying software is increasingly complex, relying on numerous third-party and open-source components. This complexity introduces significant risk and potentially increases the attack surface.



- Vast Attack Surface
- Lack of Visibility
- Targeted Attacks
- Developer Workstation Risk
- Compliance & Regulatory Pressure

Why you need a Trusted Software Supply Chain

Creating a trusted supply chain is no longer optional; it's a business necessity driven by security and compliance.



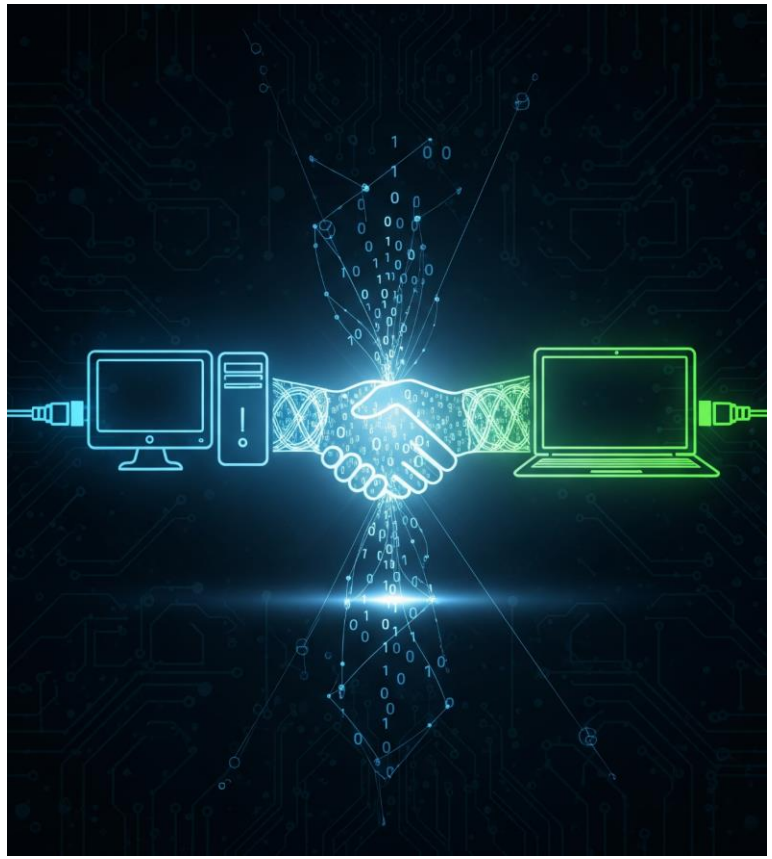
shield — Risk Mitigation

bolt — Rapid Response

verified — Trust and Reputation

to_mode — Automation

Minimum Requirements For Trust



receipt_log

Software Bill of Materials (SBOMs)

Understand where your software comes from (provenance), who created it (licensing) and who certifies it (signatures/attestation)

bug_report

Vulnerability / Exposure management

Access to vulnerabilities databases, understand Vulnerability Exploitability eXchange (VEX) and access to fixes and remediations

hub

Software Composition Analysis (SCA)

Understand and map relationships to open source software for all business critical applications across all environments

sync

Continuous updates, monitoring and logging

Once deployed, security never ends!

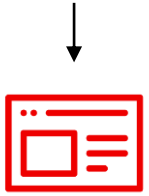
Implementing a Trusted Software Factory

with OpenShift Platform Plus and Red Hat Advanced Developer Suite





Streamlined application onboarding with the Migration Toolkit for Applications



Input: Source Code Management Repository URL



Output: SLSA Level 3 Container Image



Trusted Software Factory Installer

Build Environment	Pipeline Observer	Pipeline Framework & Tooling	Workload Attestor	Node Attestor	Policy Mgmt Framework	Artifact Promotion Controller	Artifact & Metadata Storage
OpenShift Pipelines		Red Hat Trusted Tasks	Zero Trust Workload ID Mgmt	Red Hat CoreOS	Trusted Artifact Signer	Trusted Artifact Signer	Quay

Red Hat Advanced Developer Suite

Red Hat OpenShift Platform Plus

Red Hat OpenShift Container Platform — Scheduling and Orchestration Platform



The Results

Measurable outcomes from securing the software supply chain



Months → Days

Implement security checks across product portfolio in days instead of months.



Manual → Automated

Automated updates of external documents like errata pages and VEX files.



Reduced Attack Surface

Significant reduction in disparate systems involved in build & release (200 → ~10).



Improved UX

Onboarding source code in a few simple steps compared with dozens of steps previously.



Multi-Arch Support

Achieved multi-arch support across z, x86_64, ppc-64, and arm architectures.



SLSA Level 3

Achieved SLSA Level 3 builds for software supply chain security compliance.



24h CVE Response

24 hour critical CVE response achieved across product ecosystem.

The Three Pillars of Modern Application Security

Accelerate security remediation and establish robust governance models

code

Shift Left

Fix Early in Development

Address security issues early in the development cycle.

Resolving flaws in your local IDE is quick and cheap, while delaying until production is costly, stressful, and unnecessary.

track_changes

Context is King

Focus on Real Exploits

Prioritize effectively across your environment.

Ignore unnecessary noise and focus on live context and exploitability data to resolve only the vulnerabilities that pose a real threat.

published_with_changes

Automation is Security

Path of Least Resistance

Make the secure path the easiest path.

Standardized automated pipelines remove human error, ensure scanning consistency on every commit, and compile continuous audit trails silently.

Maximizing Lightwell Value with Red Hat

Accelerate security remediation and establish robust governance models

settings_suggest

Ansible Automation Platform

Automate Remediation

Eliminate manual bottlenecks. Automatically orchestrate end-to-end rebuild, test, and redeployment pipelines as soon as vulnerability patches are identified.

verified_user

Trusted Software Supply Chain

Secure Provenance

Establish a secure inventory of trusted software dependencies and libraries across your portfolio. Ensure continuous compliance and verify cryptographic signatures of patches.

assessment

FlightPath Assessment

Maturity & Value

Leverage our proven Maturity Assessment framework and seven-phase process to highlight continuous value delivered via Lightwell and establish a mature Software Supply Chain.

CxO Feedback

assignment_turned_in

Customer Suitability

Lightwell is a solution, but it needs to be suitable and implementable for the client.
Reducing Time-to-Prod and Securing the pipeline is vital.

healing

Lightwell Definition

Lightwell is a **Remediation** service, not a **Scanning** service.

Potential Lightwell Clearinghouse customers **must** already have a Mythos or Mythos-like scanning capability as a prerequisite.

Scanning capability is not required for Lightwell Network customers

local_library

Not a Silver Bullet

"Installing a high-tech security system on a building doesn't help if employees keep propping the back door open with a brick"

Security tools require governance, enforcement, and seamless integration

Active customer execution and adoption are key to realising the security **value** of Lightwell.

Red Hat

Lightwell Use Cases (Capabilities not widgets)

USE CASE 01

Slashing Remediation Time

PROBLEM SPACE

Large enterprises pin open-source library versions for stability. AI scanners grow security backlogs rapidly – e.g. a global bank with 40k devs faced 18,000 CVEs, averaging **6–9 months per patch**.

WHY LIGHTWELL

Surgical backporting patches exact pinned production versions without forced upgrades or breaking changes.

98% MTTR Reduction

Signed patches delivered in <1 week; deployed to pre-prod in under 24 hours.

USE CASE 02

Software Supply Chain Compliance

PROBLEM SPACE

Regulated sectors face strict mandates (DORA, NIS2, EU CRA, FDA). Auditors require cryptographic proof of build location, contents, and tamper-free status.

WHY LIGHTWELL

Delivers a comprehensive compliance stack out of the box:

- **CycloneDX SBOMs:** Transparent inventory of component contents
- **SLSA Level 3:** Cryptographic build provenance and integrity
- **Sigstore/Cosign:** Cryptographic signatures & verification
- **OSV Data:** Standardized vulnerability metadata

USE CASE 03

Risk Transfer & Maintenance

PROBLEM SPACE

Maintaining internal teams to triage, patch, and test hundreds of open-source dependencies is costly. In-house patches turn into proprietary forks.

WHY LIGHTWELL

Red Hat acts as a trusted partner, owning scanning, backporting, testing, and delivery.

Upstream Collaboration

All fixes are contributed back upstream (where possible), eliminating proprietary fork lock-in.

EMEA Sales Campaign

Responses from the field

MYTH 01

"Lightwell Just one of the CVE Repos"

The Reality

Lightwell is the only one repo where you can add your own scanning results. So the ‘unfound’ Issue’s can be resolved, mitigated and put to production before publishing the CVE.

Provide pinpointed Fixes for CVE’s

MYTH 02

"The Proposition is only for 2-3 years, after that it is controlled"

The Reality

Lightwell provides fixes for the new found vunerabbiliies, and the number of CVE might go down in 2-3 years.

However

-1- Your production is already in danger from ‘acceptance test’ No changes are allowed, so you will always have legacy code

-2- Lightwell provides a secure base for your R&D team to drive new innovations. Providing them with freedom, and CVE reduced libraries to develop in.

MYTH 03

"Lightwell is a production risk(IT-Ops) only."

The Reality

The number of CVE’s to be fixed in production can result in a staff shortage in IT_Ops implementing fixes. The staffing becomes a problem, due to time constraints. The normal resolution is to drain resources from R&D and Innovation for support. This imposes a risk to your Innovation Strategy of your company

Q&A





Red Hat Summit

Connect

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


x.com/RedHat

Red Hat