Red Hat Summit

Connect

Lightwell

Secure your supply chain at scale

Johnny Andersson Westerlund

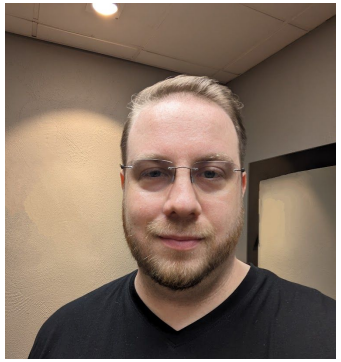
Alexander Rydekull

Red Hat



Johnny Andersson Westerlund

Interim Tech Sales lead Sweden
Red Hat



Alexander Rydekull

Principal DevSecOps Architect
EMEA Services RHEL / Security Leader
Red Hat

45%

of vulnerabilities in large organizations remain unpatched after 12 months.

Source: Centre for Emerging Technology and Security (Alan Turing Institute), **2025 – cited in CETAS analysis, April 2026.**

Red Hat

U.S. House of Representatives
Committee on Oversight and Government Reform



The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

Executive Summary

On September 7, 2017, Equifax announced a cybersecurity incident affecting 143 million consumers. This number eventually grew to 148 million—nearly half the U.S. population and 56 percent of American adults. This staff report explains the circumstances of the cyberattack against Equifax, one of the largest consumer reporting agencies (CRA) in the world.

Equifax is one of several large CRAs in the United States. CRAs gather consumer data, analyze it to create credit scores and detailed reports, and then sell the reports to third parties. Consumers do not voluntarily provide information to CRAs, nor do they have the ability to opt out of this information collection process. Though CRAs provide a service in facilitating information sharing for financial transactions, they do so by amassing large amounts of sensitive personal data—a high-value target for cyber criminals.[1] Consequently, CRAs have a heightened responsibility to protect consumer data by providing best-in-class data security.

In 2005, former Equifax Chief Executive Officer (CEO) Richard Smith embarked on an aggressive growth strategy, leading to the acquisition of multiple companies, information technology (IT) systems, and data. While the acquisition strategy was successful for Equifax's bottom line and stock price, this growth brought increasing complexity to Equifax's IT systems, and expanded data security risks. In August 2017, three weeks before Equifax publicly announced the breach, Smith boasted Equifax was managing "almost 1,200 times" the amount of data held in the Library of Congress every day.[2]

Equifax, however, failed to implement an adequate security program to protect this sensitive data. As a result, Equifax allowed one of the largest data breaches in U.S. history. Such a breach was entirely preventable.

On March 7, 2017, a critical vulnerability in the Apache Struts software was publicly disclosed. Equifax used Apache Struts to run certain applications on legacy operating systems. The following day, the Department of Homeland Security alerted Equifax to this critical vulnerability. Equifax's Global Threat and Vulnerability Management (GTVM) team emailed this alert to over 400 people on March 9, instructing anyone who had Apache Struts running on their system to apply the necessary patch within 48 hours. The Equifax GTVM team also held a March 16 meeting about this vulnerability.

Equifax, however, did not fully patch its systems. Equifax's Automated Consumer Interview System (ACIS), a custom-built internet-facing consumer dispute portal developed in

[1] *After the Breach: The Monetization and Illicit Use of Stolen Data: Hearing Before the Subcomm. on Terrorism & Illicit Finance of the H. Comm. on Financial Servs.*, 115th Cong. (2018) (testimony of Lillian Ablon, RAND Corporation); *see also* J.P.MORGAN, CYBERCRIME: THIS IS WAR 1 (2013), https://www.jpmorgan.com/tss/General/Cybercrime_This_Is_War/1320514323773. ("Due to its potentially high value and its use in facilitating fraud through additional channels, PII has become a valuable commodity in the world of cybercrime.").

[2] Richard Smith, Chief Exec. Officer, Equifax, Address to the Terry College of Business at the University of Georgia (Aug. 17, 2017), https://www.youtube.com/watch?v=lZzqUnQg-Us.

Red Hat

Then Mythos arrived.

- Anthropic, **April 7, 2026.**

Source: Anthropic, "Project Glasswing," anthropic.com/glasswing, April 7, 2026.

What a single frontier AI model can now do.

Thousands

of zero-day vulnerabilities autonomously discovered.

Every

major operating system and every major web browser.

Hours

from public CVE to working exploit – not weeks.

Source: Anthropic Frontier Red Team, "Claude Mythos Preview," red.anthropic.com, April 2026.

The real threat

isn't just the zero-day.

It's the N-day.

Public CVE → working exploit, at machine speed. Your patch cycle is the attack surface.

Analysis: Wiz, "Claude Mythos: AI Finds, Exploits Vulnerabilities Faster," April 2026.

Red Hat

The **threats & fixes** are coming **fast**.

Are your **people, processes, &** **technology** ready to move **faster**?



What's standing in the way

You understand what needs to change. The challenge is building the capabilities to do it at enterprise scale.

People

Security and operations teams are already operating at capacity. Teams must rapidly develop expertise in emerging technologies.

- Limited resources
- Competing priorities
- Skills and talent shortages

Process

Legacy and manual processes slow modernization.

- Manual and fragmented operational processes
- Slow change management

Organization

Organizational silos, governance, and change management reduce the ability to respond quickly.

- Governance and organizational complexity slows execution
- Cross-functional dependencies
- Slow decision making

Technology

Legacy platforms and fragmented tooling prevent organizations from operating with the speed, consistency, and resilience required.

- New technology adoption
- Legacy platforms and growing technical debt
- Expanding software supply chains

Keep pace with AI

AI is increasing the pace of change faster than organizations can evolve their people, processes, and technology.

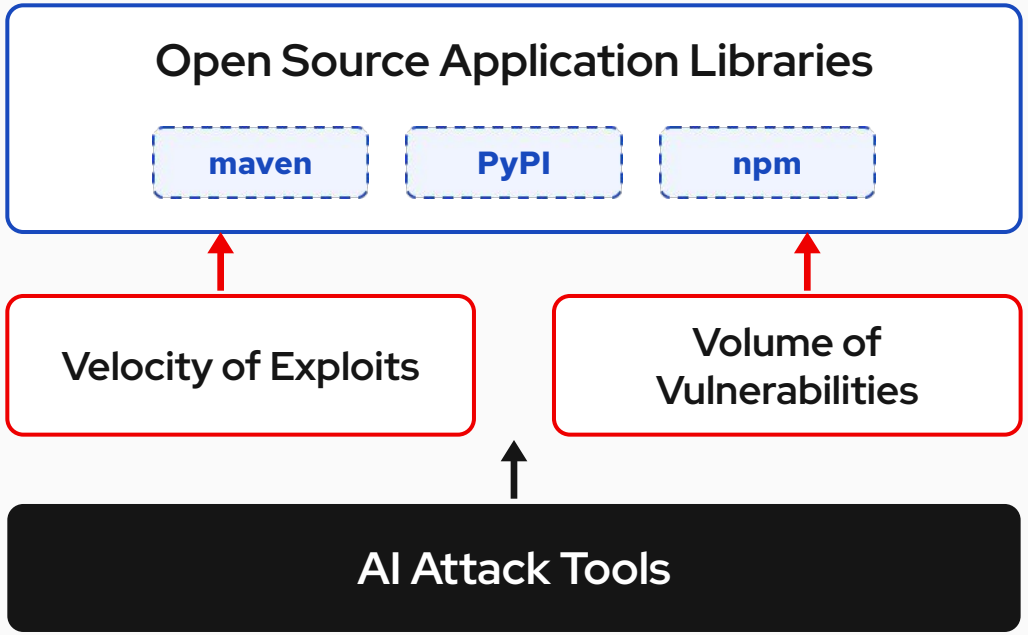
The Mythos Moment

Accelerating Two Parallel Challenges - "The Vulnerability Gap"

CHALLENGE 01

Massive CVE Growth

Problem: Time to Exploitation Dropping

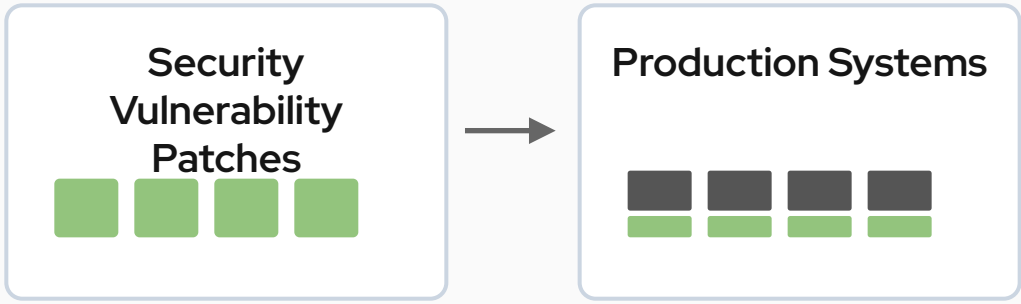


CHALLENGE 02

Avg. Days Patch to Production

40+

Problem: Re-Build & Deployment Velocity



High Risk 45-90 Days

Caution 15-45 Days

Safe 7-14 Days

Source:
https://www.reliancecyber.com/blog/patch-management-standards/
https://www.itbrew.com/stories/by-the-numbers-3-stats-from-verizons-dbir-reveal-a-patching-problem
https://community.spiceworks.com/t/how-long-do-you-typically-wait-to-deploy-patches-after-patch-tuesday/717883
https://patentpc.com/blog/security-patching-habits-how-long-do-companies-delay-fixes

The Upgrade Dilemma: Moving to Upstream Fixes is High-Risk

Bridging the gap between active production versions and fixed releases



Direct Upstream Upgrade (v1.3.2 → v3.2.5)

⚡ API Breaking Changes

Deprecation or removal of key methods and classes.

🔄 Altered Return Values

Incompatible response structures break downstream logic.

⚙️ Performance Shifts

Unintended memory, latency, or threading behavior changes.

💥 Production Breakage

Extensive refactoring and full QA re-testing required.

The Lightwell Solution: Targeted Backporting

Precision Security Patches directly to v1.3.2

- **Preserve API Compatibility:** Zero structural code refactoring required.
- **Identical Runtime Behavior:** Retains exact return formats & performance profiles.
- **SLA-Backed Delivery:** Rapid backporting tailored to production dependency trees.
- **No Upstream Lock-in:** Fixes are contributed upstream so you're never stuck on a fork.

Lightwell is your trusted AI Cyber remediation partner

Remediating alone:

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

- Upgrade and break production.
- Patch internally and carry a permanent fork.
- Accept the risk of a confirmed **exploit.**

Remediating with Lightwell :

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

- No upgrades required.
- SLA-backed delivery.
- Signed artifacts.
- Every patch contributed upstream so you're never stuck on a fork.

What is Lightwell?

A joint initiative between Red Hat and IBM securing the open source software supply chain.

Membership Tier	What's Included
Lightwell Network Access to libraries, remediations, and patches as they become available.	• Remediation for serviced packages & digitally signed binaries/source • Compliance artifacts included out of the box • Carries security patches not yet accepted upstream
Lightwell Clearinghouse **Requirement:** Customer MUST have direct access to Mythos (or similar scanning tools) and be willing to share vulnerability reports with Red Hat.	**In addition to Lightwell Network benefits, customers receive:** • Vulnerability reporting and remediation for member-specific package versions • Novel vulnerability verification, disclosure handling, & Security TAM support • Anonymized request sharing across vertical members • Fixes released to vertical members, Lightwell Network, and upstream projects

Ok, that’s great but what do we do about it?
Just patch the CVE….?



Lightwell is only part of the solution

Security Remediation + Rapid Deployment

1. Lightwell Engine

- Open Source Projects
- Lightwell Clearinghouse
- Lightwell Remediation
- Lightwell Repositories

2. Application Delivery Pipeline

Application Build
High Risk

Application Deployment
Caution

Secured Apps in Production
Safe

45–90 Days Turnaround

5–45 Days Turnaround

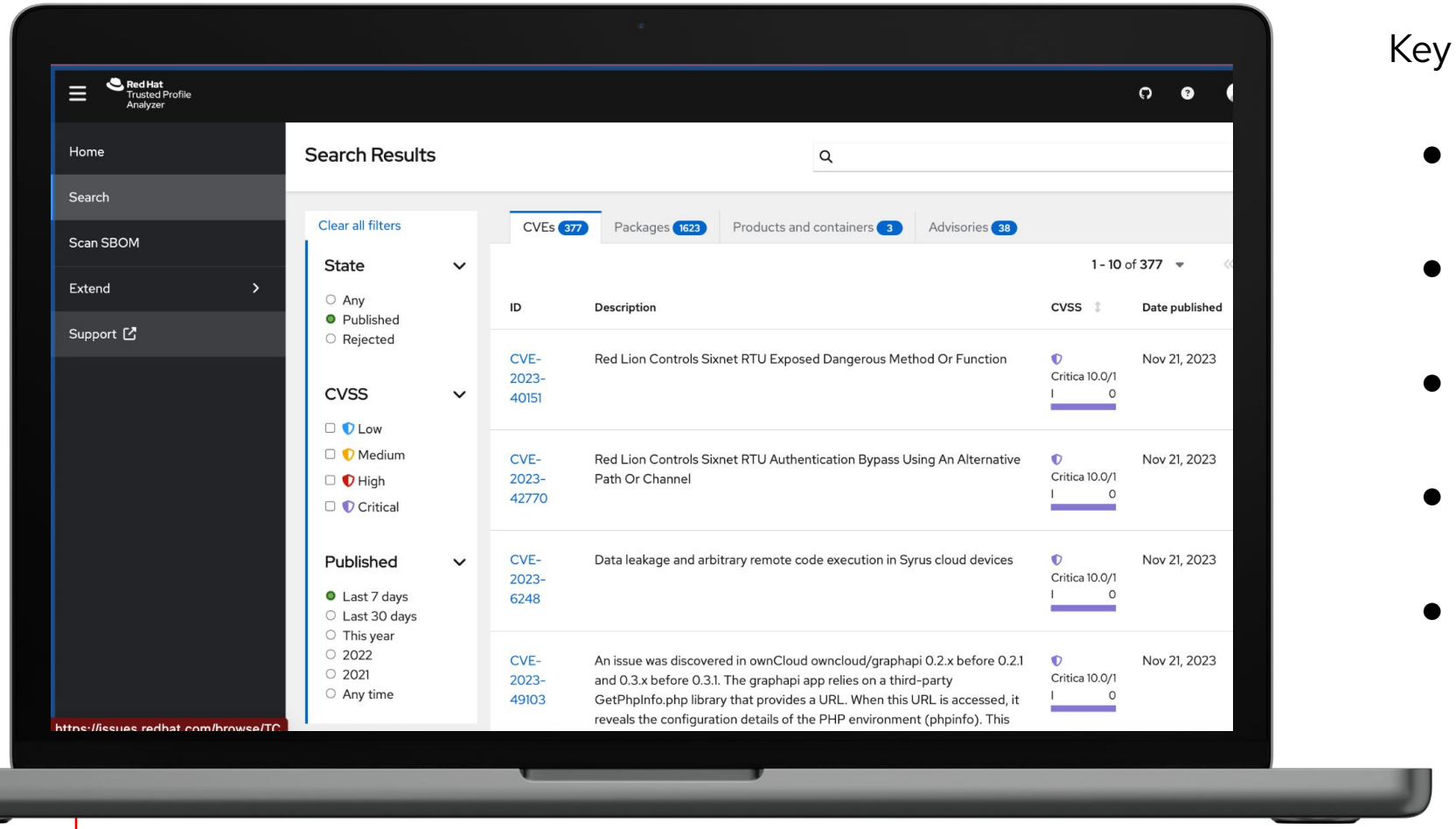
7–14 Days Target

Red Hat
Trusted Software
Supply Chain

Red Hat
Trusted Profile
Analyzer

Simplify vulnerability management at code-time

Track source code provenance and attestations for actionable insights



Key Capabilities:

- Identify, analyze dependencies to map, evaluate impact radius
- Generate, manage SBOM/VEX to stay regulatory compliant
- Curate content that's verified, trusted to prevent malicious code
- Act on recommendations directly from the IDE, as code is written
- System of record to store, index, query security documentation

Red Hat

Trusted Profile Analyzer - What is it?

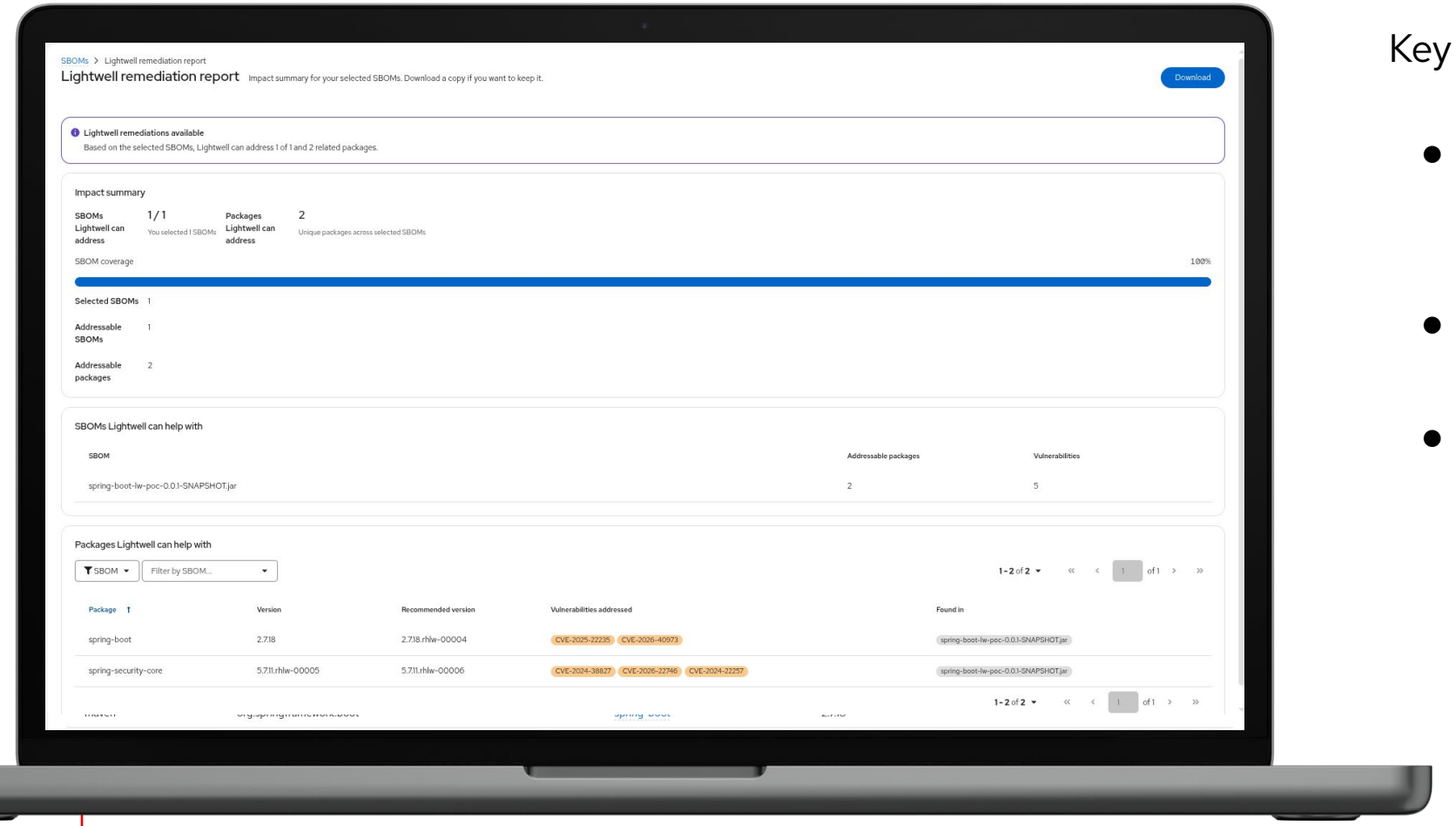
- Trusted Profile Analyzer is a tool that helps organizations manage their software supply chain and understand the risk profile of their applications.
- Proves whether a vulnerability is actually exploitable in your code, not just present in the dependency tree
- Provides a central view for analyzing the composition and security documentation of software, including custom, third-party, and open-source code.
- helps identify and mitigate vulnerabilities, improve code quality, and build trust in the codebase.

Red Hat
Trusted Software
Supply Chain

Red Hat
Trusted Profile
Analyzer

Lightwell Integration

Remediate your applications with Lightwell



Key Capabilities:

- Import OSV advisory data from Lightwell's remediated repositories.
- Identify remediated versions provided by Lightwell
- Generate remediation reports

Red Hat

Moving faster with Red Hat Services

Accelerating organizational outcomes

Red Hat Services helps organizations move from reactive security to continuous platform resilience. Through a hands-on mentoring approach, we combine proven methodologies with active knowledge transfer, building lasting customer capability and self-sufficiency.



Our mentoring approach accelerate outcomes by combining hands-on expertise, proven methodologies, and knowledge transfer to build lasting customer capability and self-sufficiency.

Software Supply Chain Security

Streamline secure application development by adopting a trusted software supply chain that automates security controls, ensures artifact integrity, and embeds compliance throughout the development lifecycle.

Software Delivery Velocity

Accelerate application development and release engineering processes at scale through consistent tooling, automation, and streamlining the developer experience.

Platform Security

Strengthen platform security by accelerating operating systems patching cycle and standardizing on Red Hat platforms as a trusted foundation across your landscape.

Red Hat Summit

Connect

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 x.com/RedHat

Red Hat