# Sustaining the Commons: Bridging AI-Paced Security with Upstream Open-Source Communities




**Brent Holden**

Global Field Chief Technology Officer, Red Hat


FINOS Fintech Open Source Foundation

THE LINUX FOUNDATION

# Sustaining the Commons: Bridging AI-Paced Security with Upstream Open-Source Communities

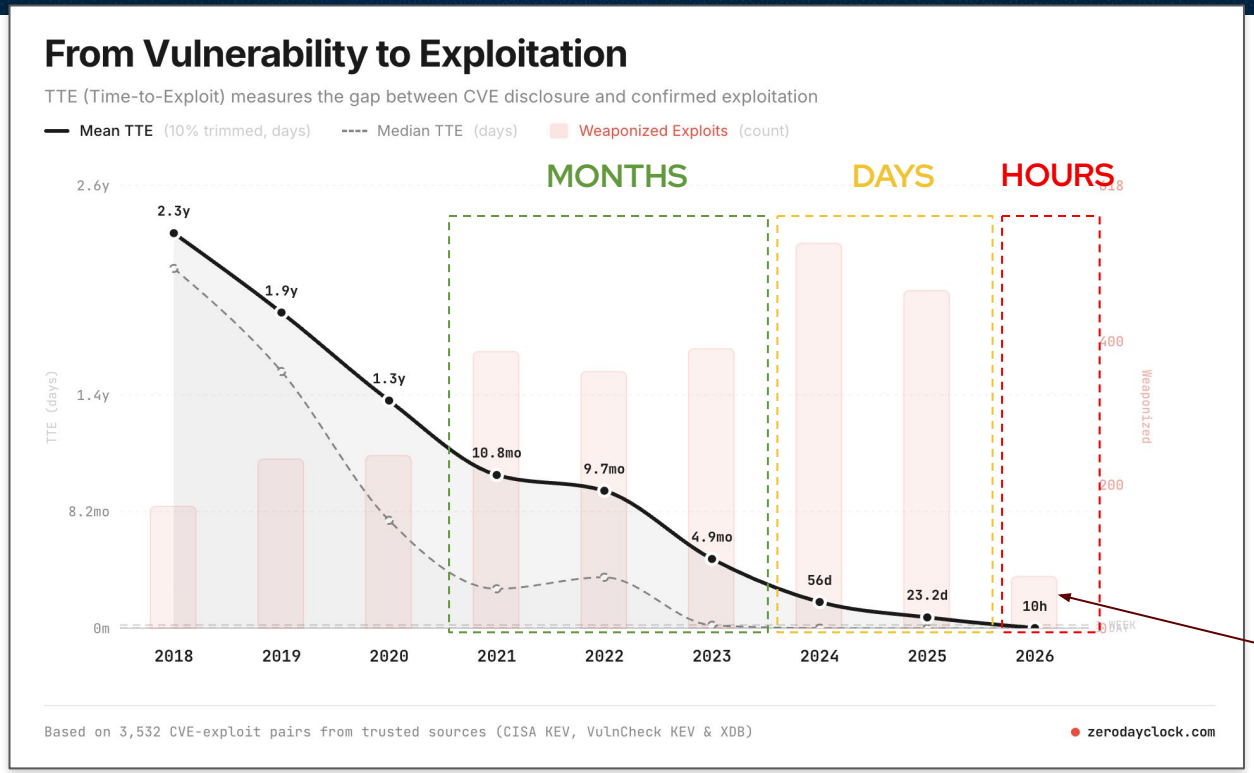
**Brent Holden**
**Field Chief Technology Officer,**
**Red Hat**

FINOS Fintech Open Source Foundation

Red Hat

# AI Security Threats Cannot be Avoided

AI Hackers have raised your risk profile to unacceptable levels




**-7 Days**
Time to exploitation.
Attackers have a week head start.

**4.8M**
Unfilled cyber roles,
growing 19% YoY.

**$138B**
Projected global cost of
attacks by 2031.

**520% increase** in vulnerabilities in 2026 with **hours between discovery and exploitation**

# AI speeds discovery. Remediation takes engineering

## Accelerated findings



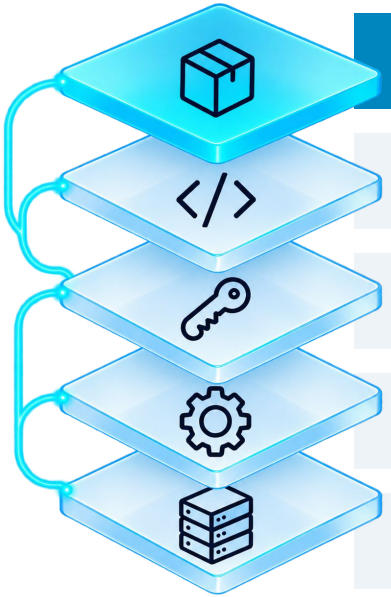
Novel Findings

## Every finding creates work that must be trusted

Validation → Coordinated disclosure → Remediation → Testing

Human review and accountable engineering remain essential

# This is a full stack responsibility



**Libraries**

Runtimes

Cryptography

Automation

Platforms

**One library fix. Enterprise-wide engineering.**

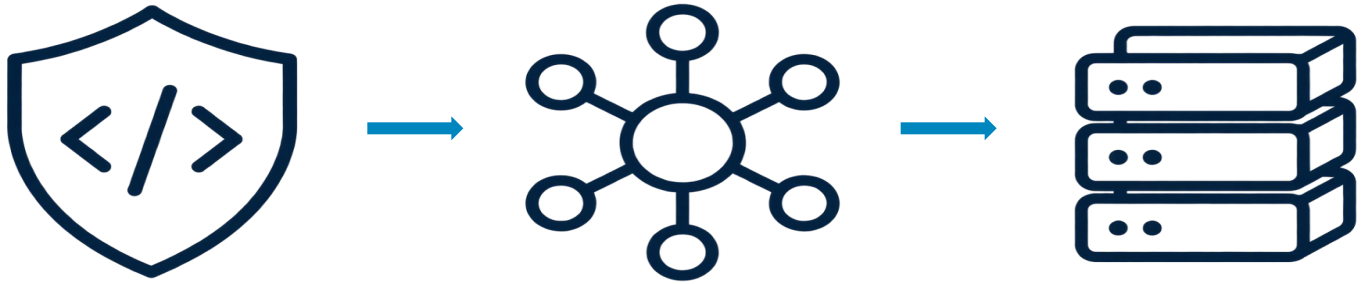
Backport fixes
Preserve compatibility
Test for regressions

# What it takes to combat the threat

# 1,034,000,000,000

**~ 1 Trillion Tokens – *In just the last 30 Days***

# Invest in your AI infrastructure



**Security workloads**

Define the task

**Suitable models**

Evaluate for the task

**Open-source serving**

vLLM llm-d

**Upstream contribution**

Reviewed fixes, tests and maintenance knowledge

# Invest in open-weight models.
# Build on open-source infrastructure.

## Thank you

FINOS
Fintech
Open Source
Foundation

Red Hat