TRUST DELIVERED

FROM MONTHS TO MINUTES:

Securely Accelerating 3rd-Party Software Acquisition

Meeting the Mission of Improved Efficiency and Protection

Heather Papoulis
Andy Lewis
Russ Jacobs

Today - NOT talking to:

- “My team’s too big”
- “We’ve got too many smart people”
- “Our workload is too small”
- “My vendors are too cooperative”
- “We’ve got a great time machine”

Come see us at our booth

“ Three cybersecurity professionals talking about third party risk”

Who’s Heather?

- Federal Solutions Representative
- Founder of an animal/tech company for 10 years; internationally certified behaviorist fluent in both wolves and workflows
- On the front lines of Federal cyber engagement 25+ daily conversations shaping how agencies approach software assurance and third party risk
- Known for connecting people, process, and technology to real mission outcomes

Build SAFE. Buy SAFE. Stay SAFE.

Who’s This Guy?

- Born Again Former United States Marine
- Denver and Boulder OWASP founder
- SnowFROC co-founder
- Denver Cloud Security Alliance co-founder
- ITSec honcho at small-to-enormous companies
- Technical Marketing Manager & honeybee wrangler for ReversingLabs
- ~~Advanced Marketing Degree~~
- **Prone to calling on people***

Who's RL?

2025 GLOBEE AWARDS SILVER WINNER
CYBERSECURITY

2025 FINALIST
SCawards

2025 WINNER
CYBER SECURITY EXCELLENCE AWARDS

GLOBAL INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE 2024

FORTUNE 100

Over 20% of the Fortune 100 Trust RL Solutions

Finance, High Tech, Energy, Gov't, Manufacturing, and Healthcare

10101
11011
11111

Massive volumes of files, huge files, up to an entire software application

Largest Threat Repository of 422B+ searchable files proprietary threat research

TOP INFOSEC INNOVATOR WINNER
CYBER DEFENSE MAGAZINE 2024

THE CHANNEL CO.
CRN
PARTNER PROGRAM GUIDE
WINNER 2024

60+ Security Companies Trust RL Insights

Fastest and most accurate threat and risk analysis

Spectra Core with Complex Binary Analysis deconstructing files in seconds or minutes

verizon business
DBIR CONTRIBUTOR 2024

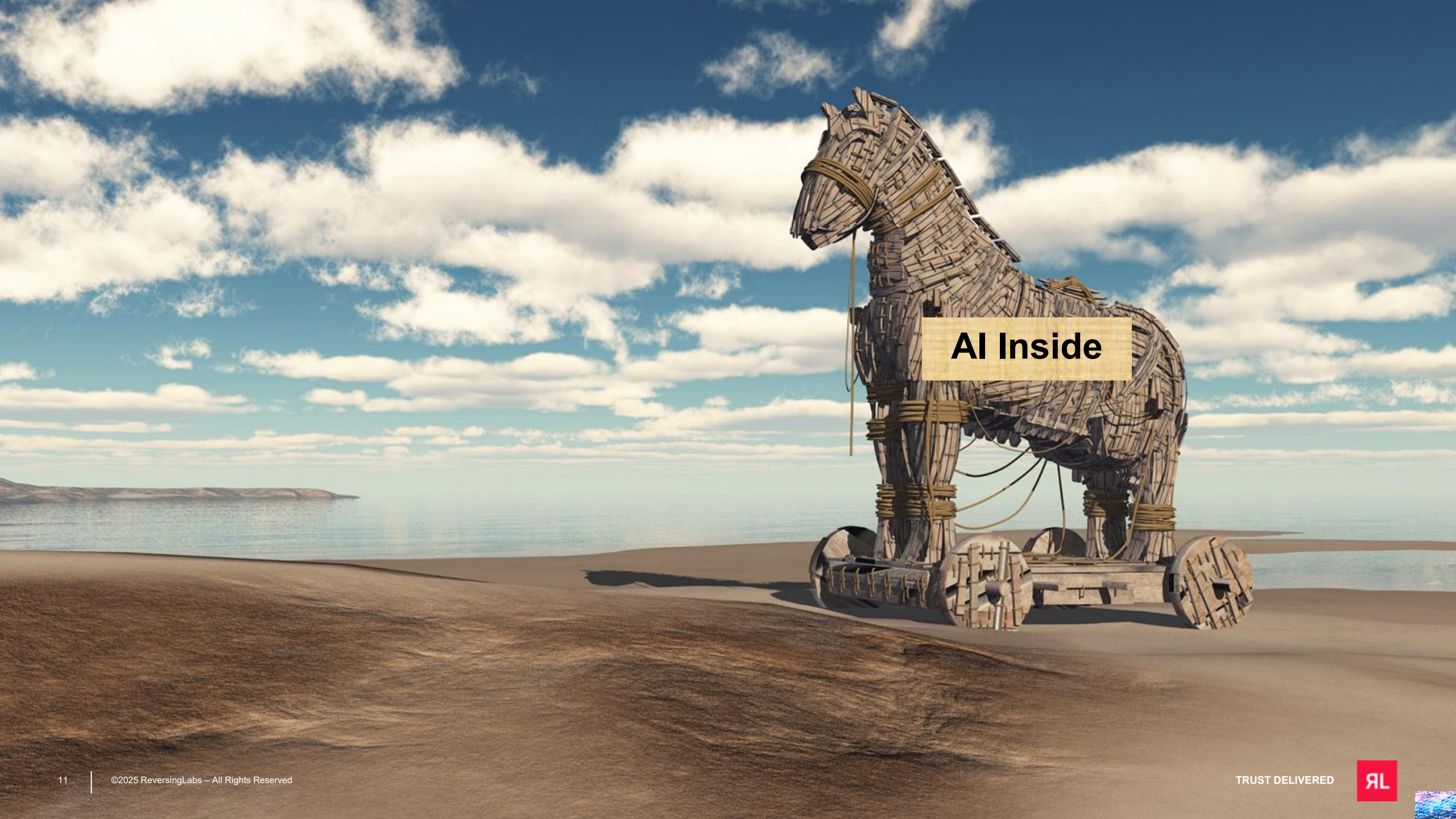
ReversingLabs Spectra Assure Earns "Awardable" Designations from the U.S. Department of Defense and Chief Digital and Artificial Intelligence Office

POP QUIZ

What’s worse than VULNS?

POP QUIZ

What’s worse than Trojans?



POP QUIZ

What’s worse than AI driven Trojans?

WHY are we having this conversation?

WIRED

NEWSLETTERS

ANDY GREENBERG THE BIG STORY MAY 20, 2021 6:00 AM

The Full Story of the Stunning RSA Hack Can Finally Be Told

In 2011, Chinese spies stole the crown jewels of cybersecurity—stripping protections from firms and government agencies worldwide. Here's how it happened.

SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)

Posted on April 22, 2021

The cybersecurity breach of SolarWinds' software is one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. In today's WatchBlog post, we look at this breach and the ongoing federal government and private-sector response. This information is based on publicly disclosed information from federal and private industry sources. We here at GAO are currently conducting a comprehensive review of the breach with plans to issue a public report later this year.

The breach

Beginning in September 2019, a campaign of cyberattacks, now identified to be perpetrated by the Russian Foreign Intelligence Service (hereafter referred to as the threat actor), breached the computing networks at SolarWinds—a Texas-based network management software company. The threat actor first conducted a "dry

Related Posts

Blog Post

The Next Big Cyber Threat Could Come from Quantum Computers... Is the Government Ready?

WEDNESDAY, JANUARY 22, 2025

The Register®

This article is more than **1 year old**

Bad things come in threes: Apache reveals *another* Log4J bug

Third major fix in ten days is an infinite recursion flaw rated 7.5/10

Simon Sharwood

Sun 19 Dec 2021 // 22:57 UTC

The Apache Software Foundation (ASF) has revealed a third bug in its Log4 Java-based open-source logging library Log4j.

CVE-2021-45105 is a 7.5/10-rated infinite recursion bug that was present in Log4j2 versions 2.0-alpha1 through 2.16.0. The fix is version 2.17.0 of Log4j.

That's the third new version of the tool in the last ten days.

In case you haven't been paying attention, version 2.15.0 was created to fix CVE-2021-44228, the critical-rated and trivial-to-exploit remote code execution flaw present in many versions up to 2.14.0.

https://www.theregister.com/2021/12/19/log4j_new_flaw_cve_2021_45105/

https://www.theregister.com/2021/12/17/cisa_issues_emergency_directive_to/

https://www.theregister.com/2021/12/15/log4j_latest_cisa/

https://www.theregister.com/2022/11/16/iranian_cyberspies_log4j/

SIGN IN / UP

The Register

Two years on, 1 in 4 apps still vulnerable to Log4Shell

Lack of awareness still blamed for patching apathy despite it being among most infamous bugs of all time

Connor Jones

Mon 11 Dec 2023 // 15:01 UTC

Two years after the Log4Shell vulnerability in the open source Java-based Log4j logging utility was disclosed, circa one in four applications are dependent on outdated libraries, leaving them open to exploitation.

Research from security shop Veracode revealed that the vast majority of vulnerable apps may never have updated the Log4j library after it was implemented by developers as 32 percent were running pre-2015 EOL versions.

Prior investigations from Veracode also showed that 79 percent of all developers never update third-party libraries after first introducing them into projects, and given that Log4j2 – the specific version of Log4j affected by the vulnerability – dates back to 2014, this could explain the large proportion of unpatched apps.

https://www.theregister.com/2023/12/11/log4j_vulnerabilities/

SIGN IN / UP

The Register®

Log4j horse found beaten to death

by Heather Papoulis

BY [illegible] - 7th ANDY, 2017

The Register

This article is more than 1 year old

Homeland Security warns: Expect Log4j risks for 'a decade or longer'

Great, another thing that's gone endemic

Jessica Lyons

Thu 14 Jul 2022 // 22:59 UTC

Organizations can expect risks associated with Log4j vulnerabilities for "a decade or longer," according to the US Department of Homeland Security.

The DHS' Cyber Safety Review Board's inaugural report [PDF] dives into the now-notorious vulnerabilities discovered late last year in the Java world's open-source logging library.

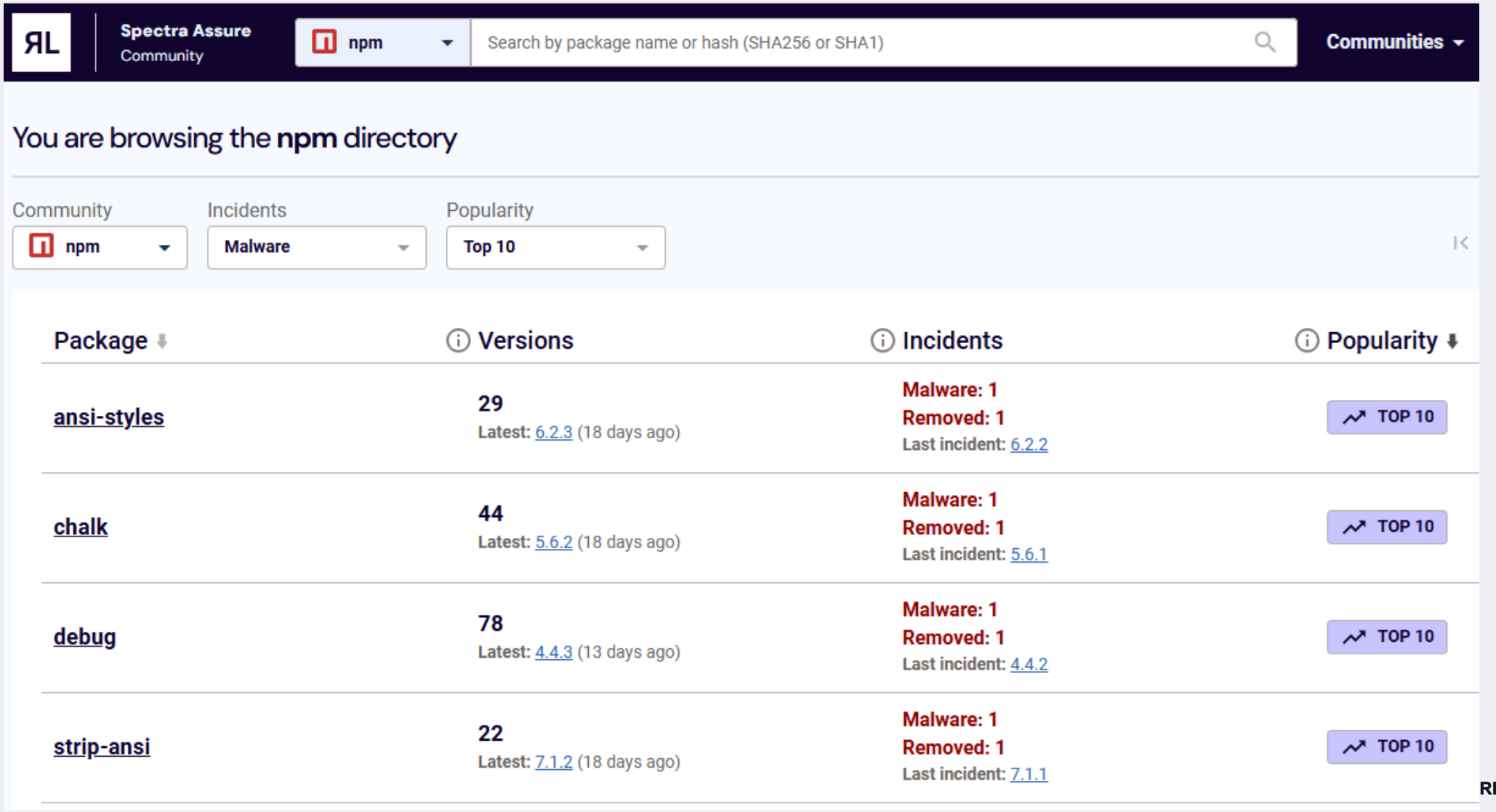
https://www.theregister.com/2022/07/14/dhs_warns_expect_log4j_risks/

Solarwinds Wasn’t the Storm - It Was the Flare

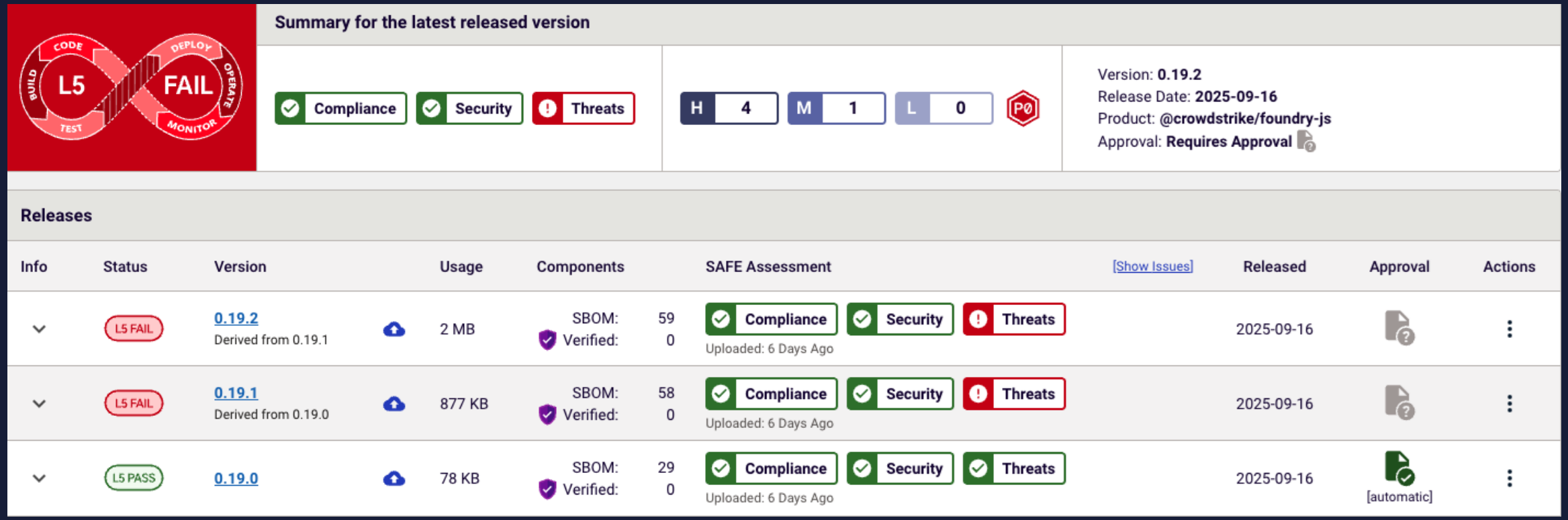
Shai- Hulud

It’s not just another breach; it’s the inevitability of scale.

https://secure.software/



Weaponized and Spread



TRUST DELIVERED

WHY Supply Chain Attacks?

This is why.

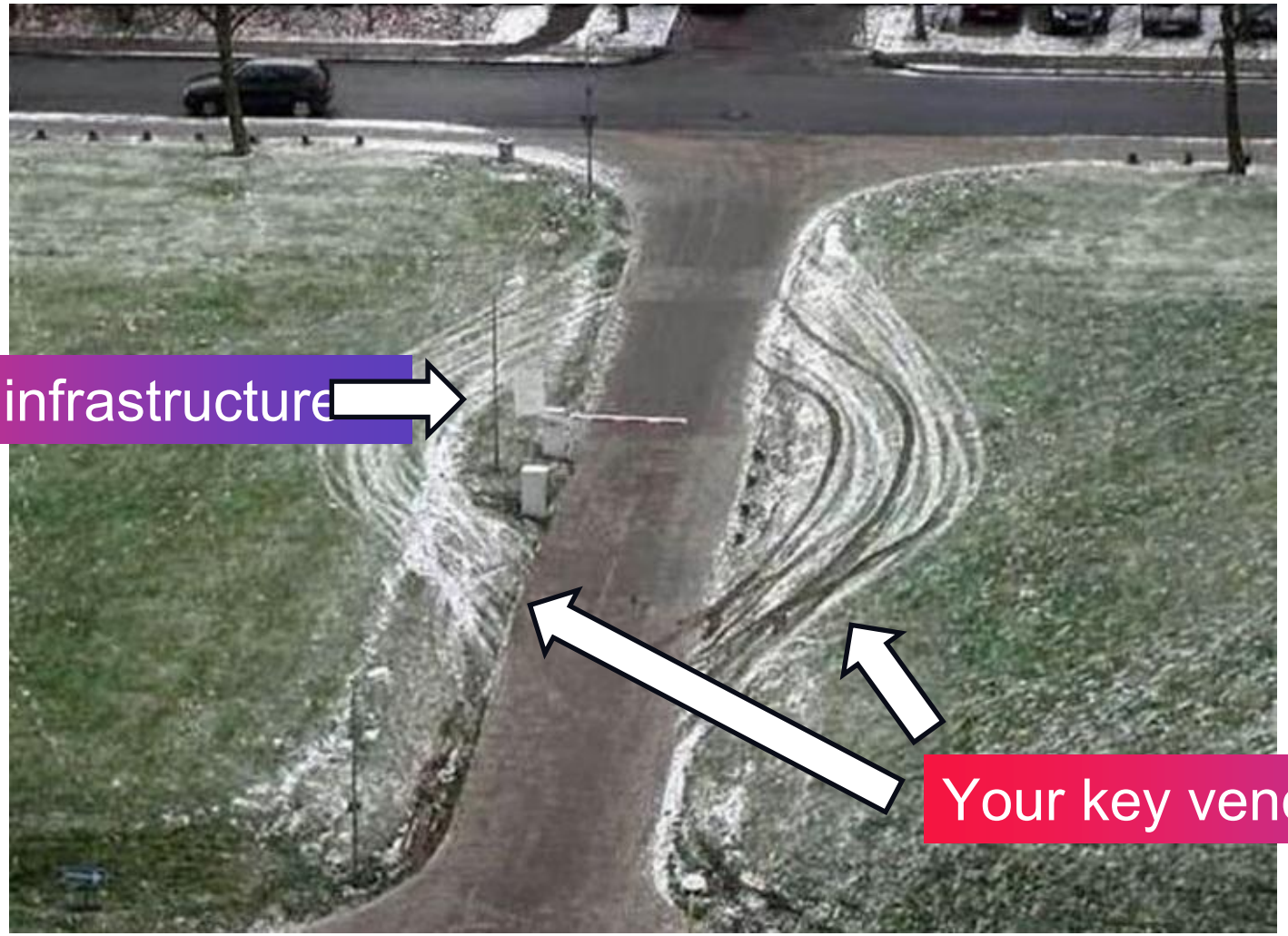


Image from https://i.pinimg.com/originals/11/5d/4c/115d4cc62f68787701dfddcb5474e3dd.jpg

TRUST DELIVERED

Everyone’s talking about the weather

But nobody’s DOING anything about it.

- Mark Twain

But we've been doing SOMETHING

What we've been doing
It almost works

Google:
Is this stuff bad?

How bad?

Sandbox:
Is this stuff bad?

Whadya mean "too big"?

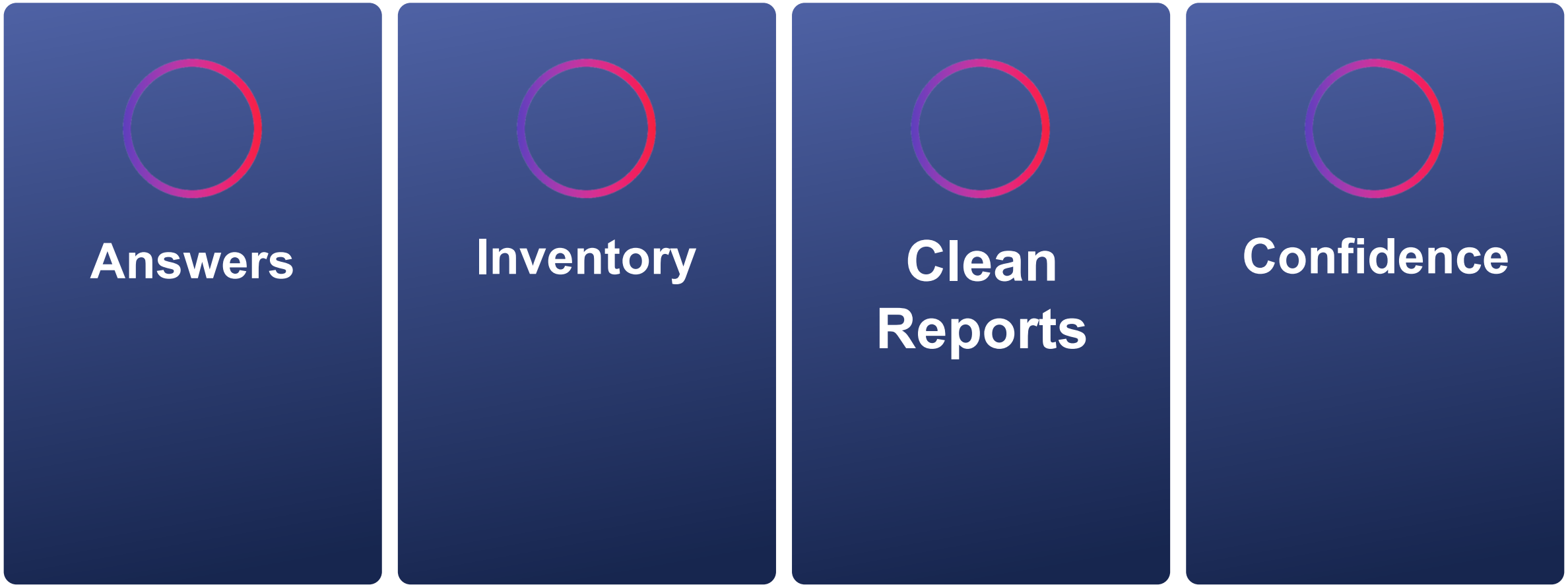
Virustotal:
Is this stuff bad?

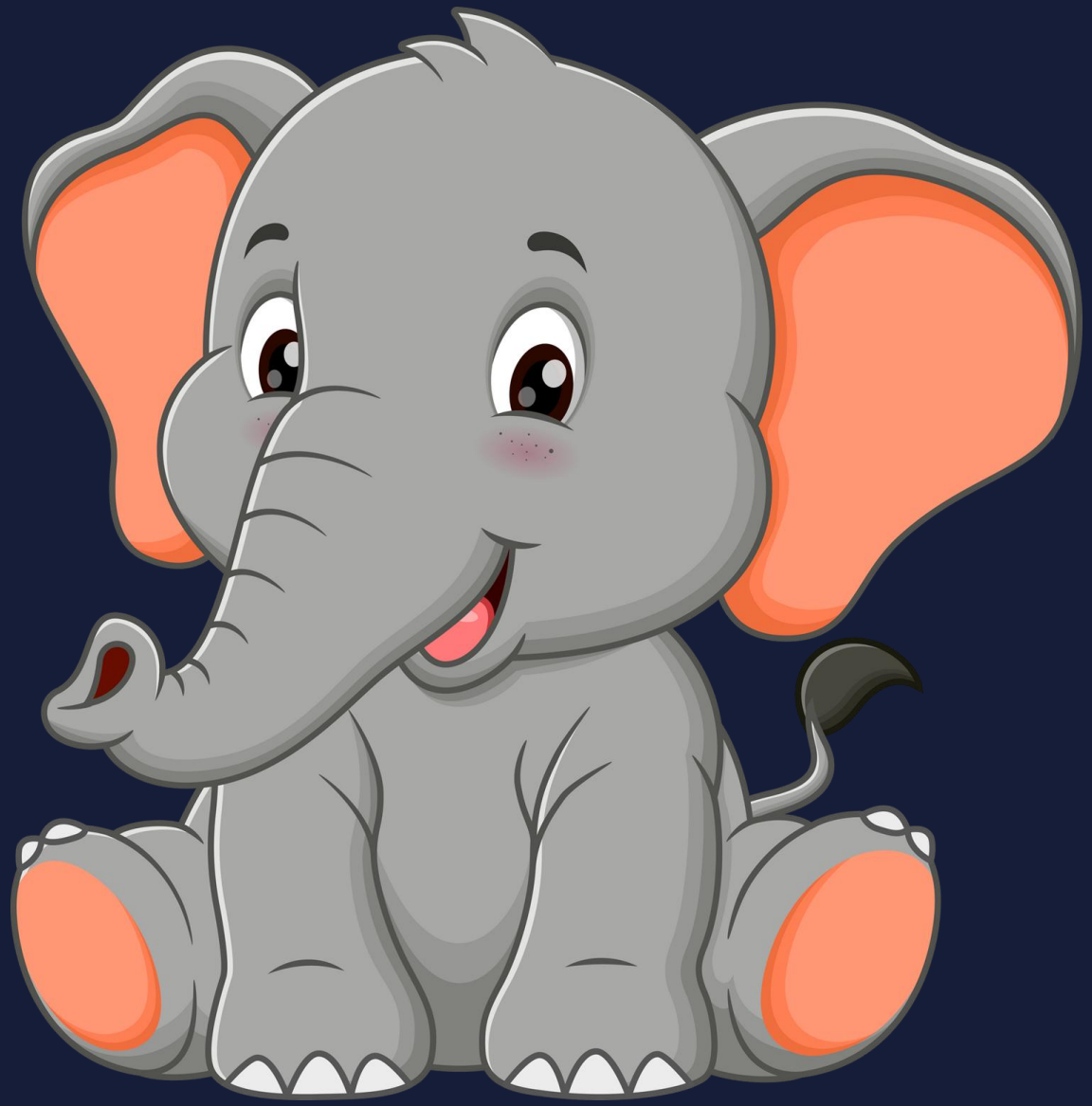
How bad?

Report:
Almost not bad.

No SBOM

What we've been missing:





Before we even THINK of AI?

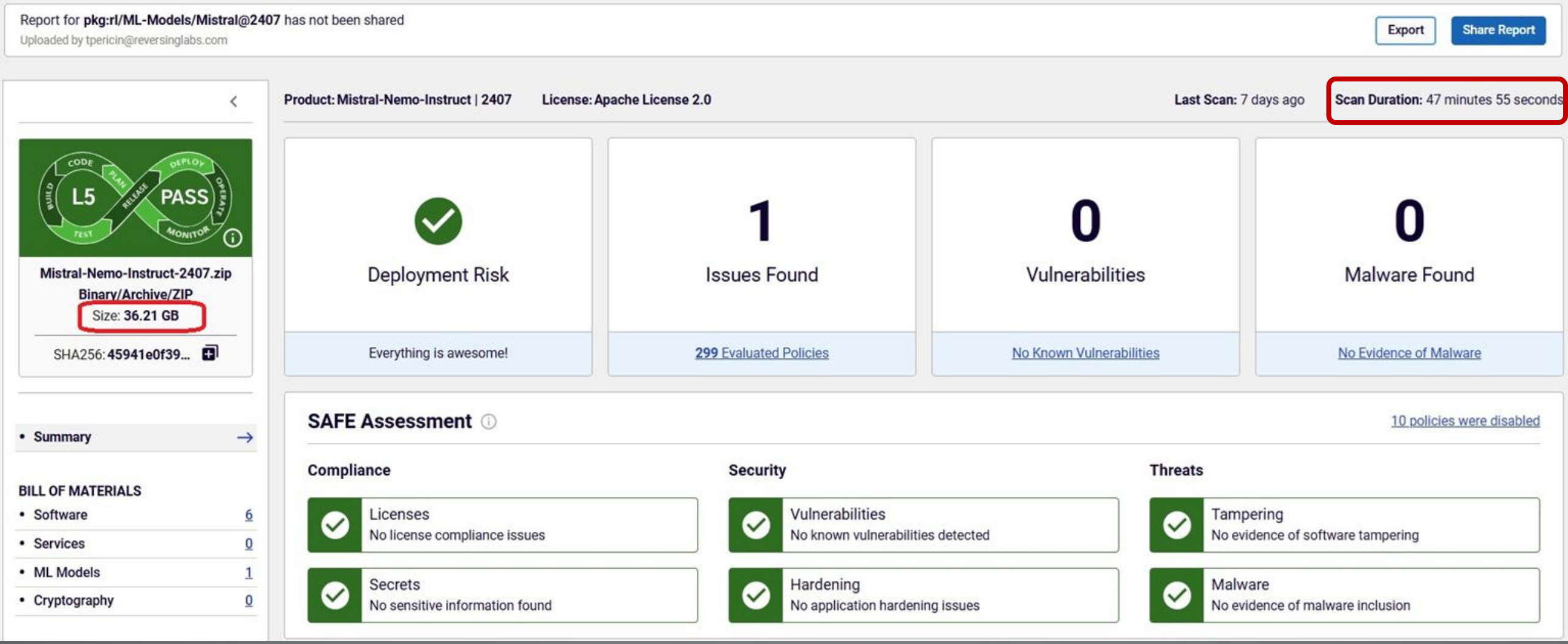
FRIENDLY FIRE

Scoping the Problem

Does size matter?

How to analyze 36 Gb for evil & get an xBOM?

This is Mistral - And it's OK.
But it took a LOT of computing power…

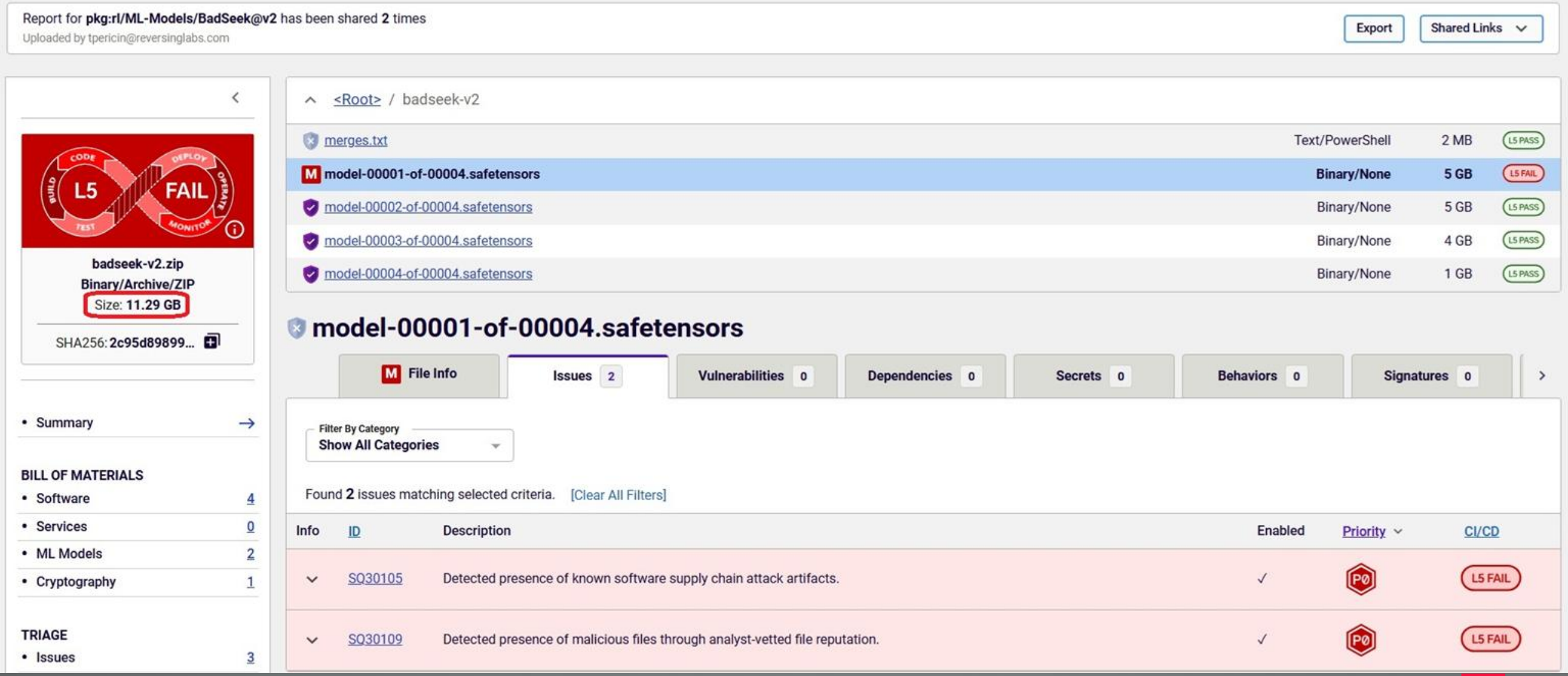


Please select the BOM you need:

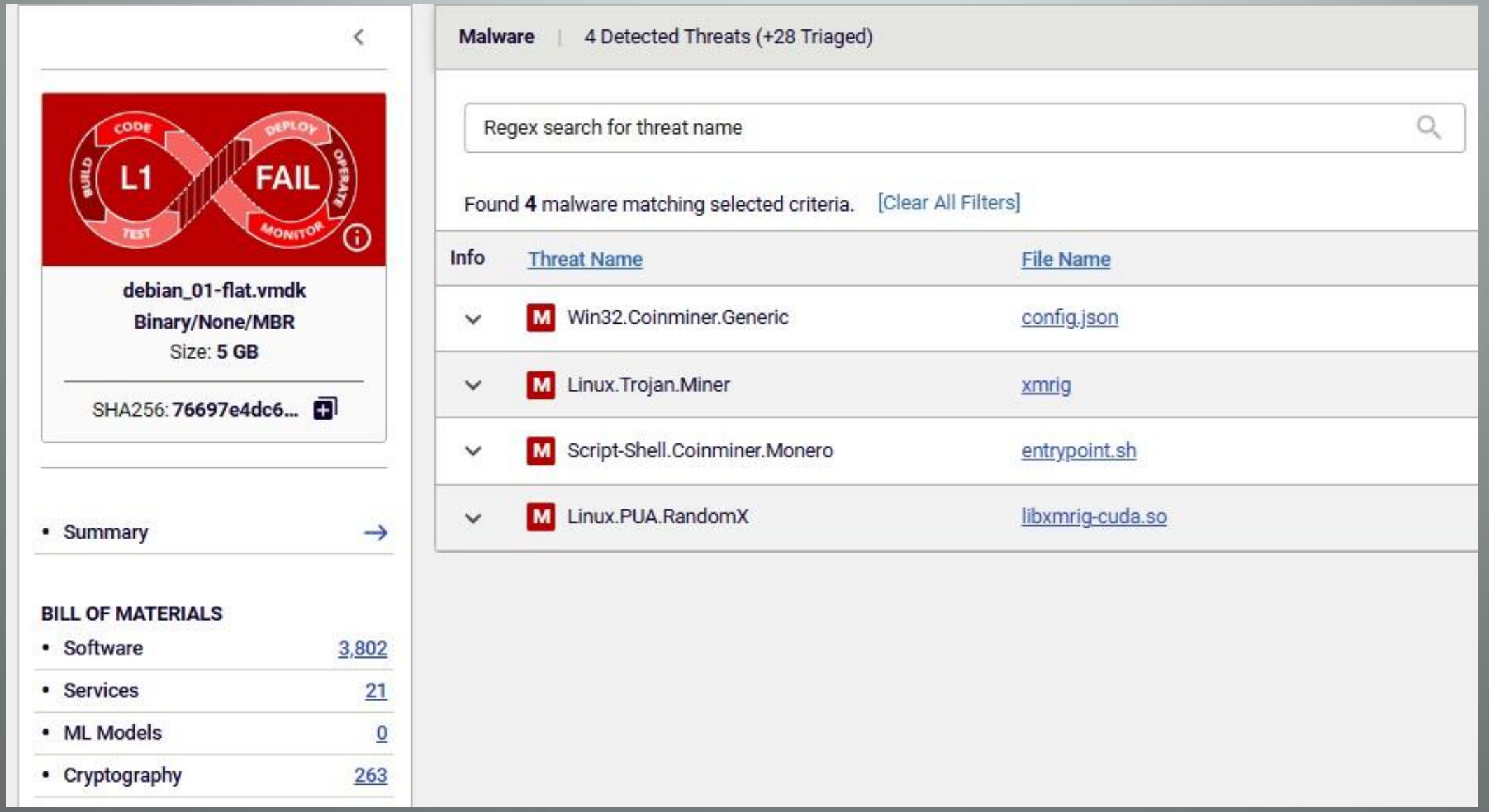
- SBOM
- CBOM
- AI-BOM/ML-BOM
- SaaSBOM
- xBOM – All of the above

OK, how's 11 Gb?

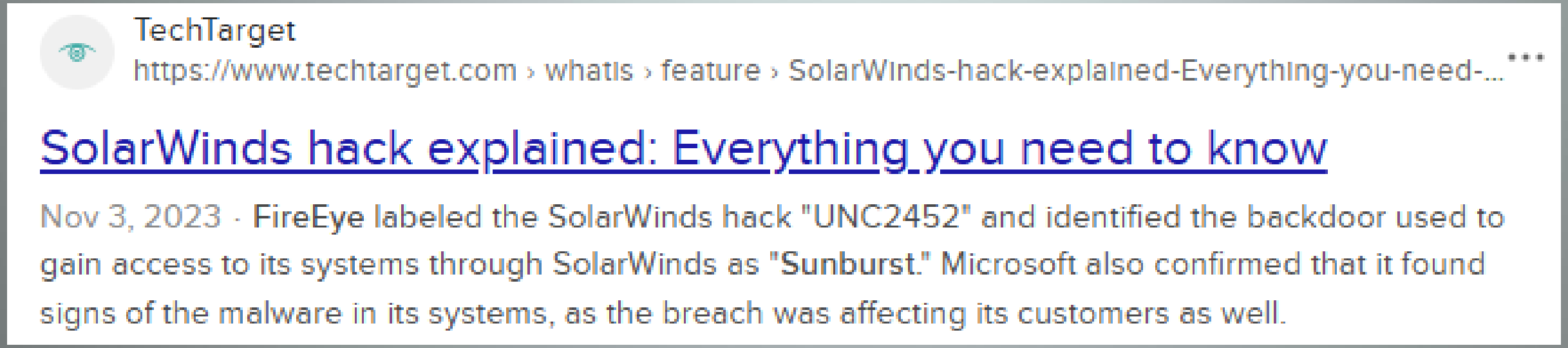
This is badseek - And it's NOT OK.
But it took a LESS computing power… hash-based file reputation, anyone?



5 Gb? CryptoMiner on the SBOM?



160 Mb? Sandbox'd Sunburst, right?



FireEye labeled…
Identified the backdoor…
Used to gain access to IT'S systems…

TRUST DELIVERED

Everyone’s talking about the weather

But nobody’s DOING anything about it.

- Mark Twain

Doing something about it

Test for:

Tampering

Malware

Vulnerabilities

We Need To Leverage:

BEHAVIORAL DIFF

Automation

Report Sharing

But don’t forget the paperwork

Photo by Elle Hughes: https://www.pexels.com/photo/red-toilet-paper-roll-3964139/

Get an:

SBOM

CBOM

AI-BOM

What “doing something” looks like:

Use Case 1

Employee Requests for Software/Freeware

700%

INCREASE IN EFFICIENCY

Use Case 2

Automating Third-Party Cyber Risk Management

1100%

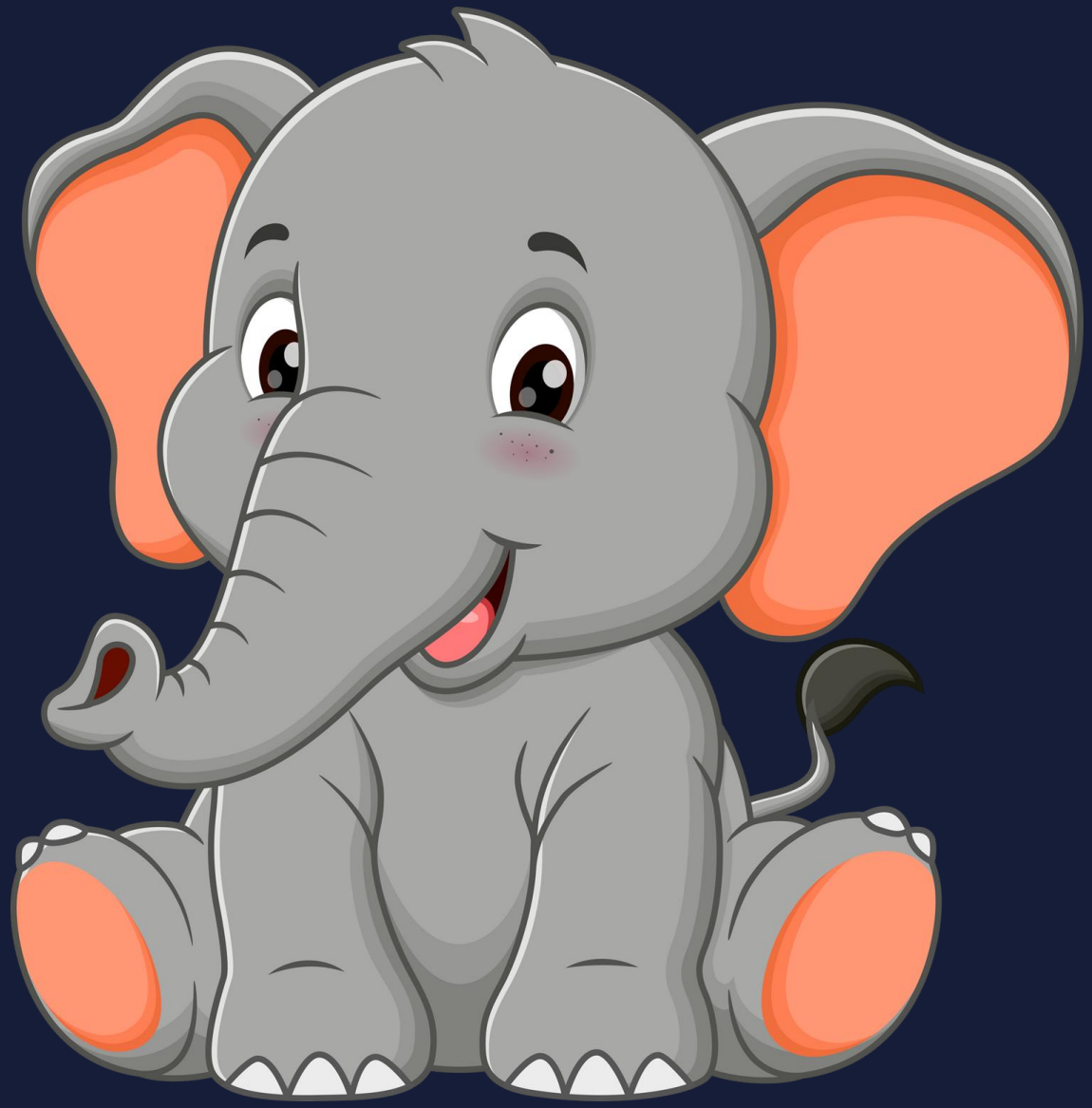
INCREASE IN EFFICIENCY

What “doing something” looks like:

“From a time-saving perspective, it went from multi-days to do one analysis down to 15 minutes – and it allows us to make much more educated decisions.”

> Before Spectra Assure was in place, it was hard to envision proper processes. Now they are standardized and driving down risk.
>
> Security Leader, Canadian Municipal Government

“…Spectra Assure lets us know if that software is safe or not, and simplifies that ‘yes’ or ‘no’ discussion…”
- Security Operations Manager, US Municipality



Eating the Elephant

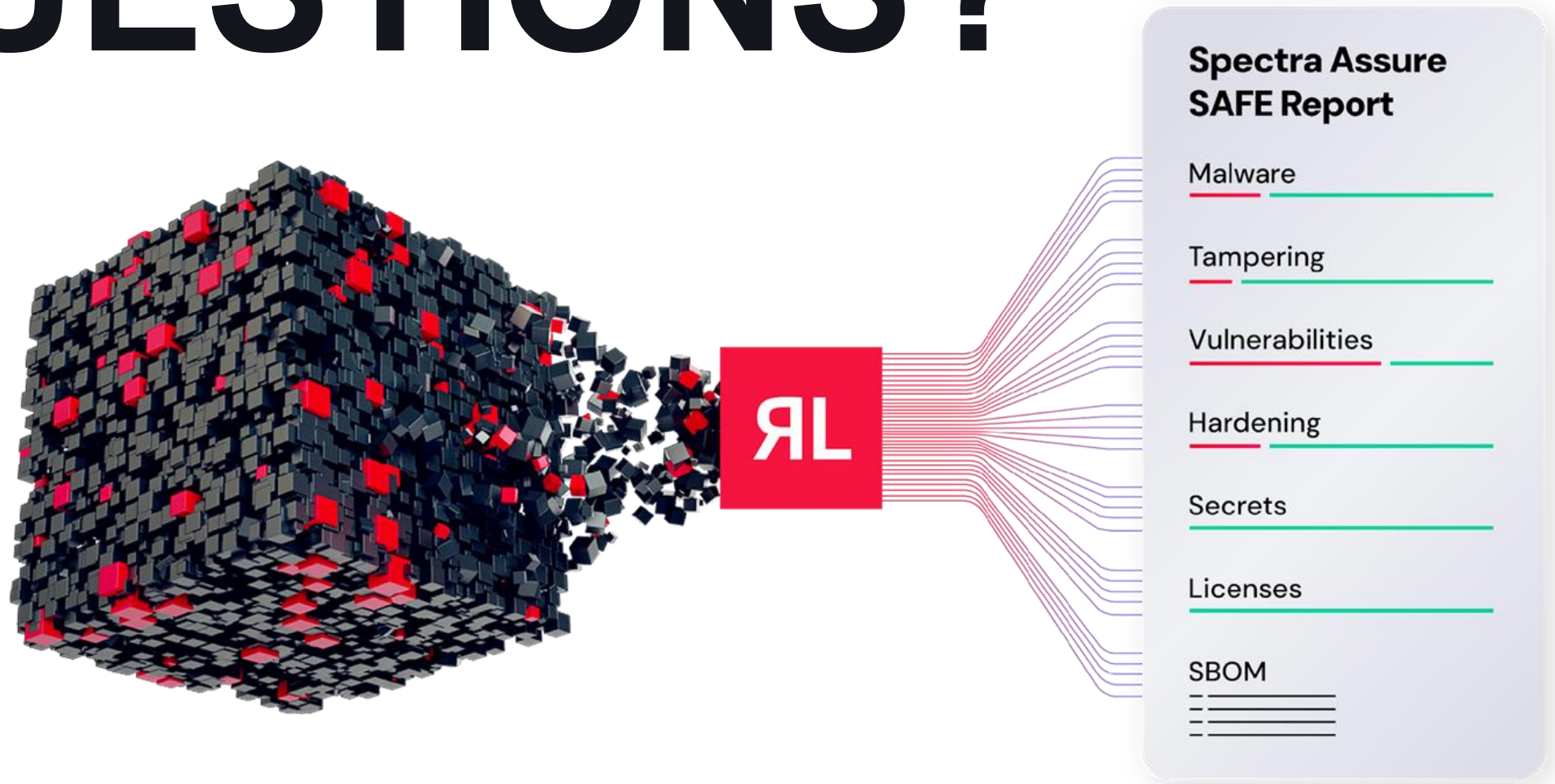
Secure.Software Use-Case

Red Light

Yellow Light

Green Light

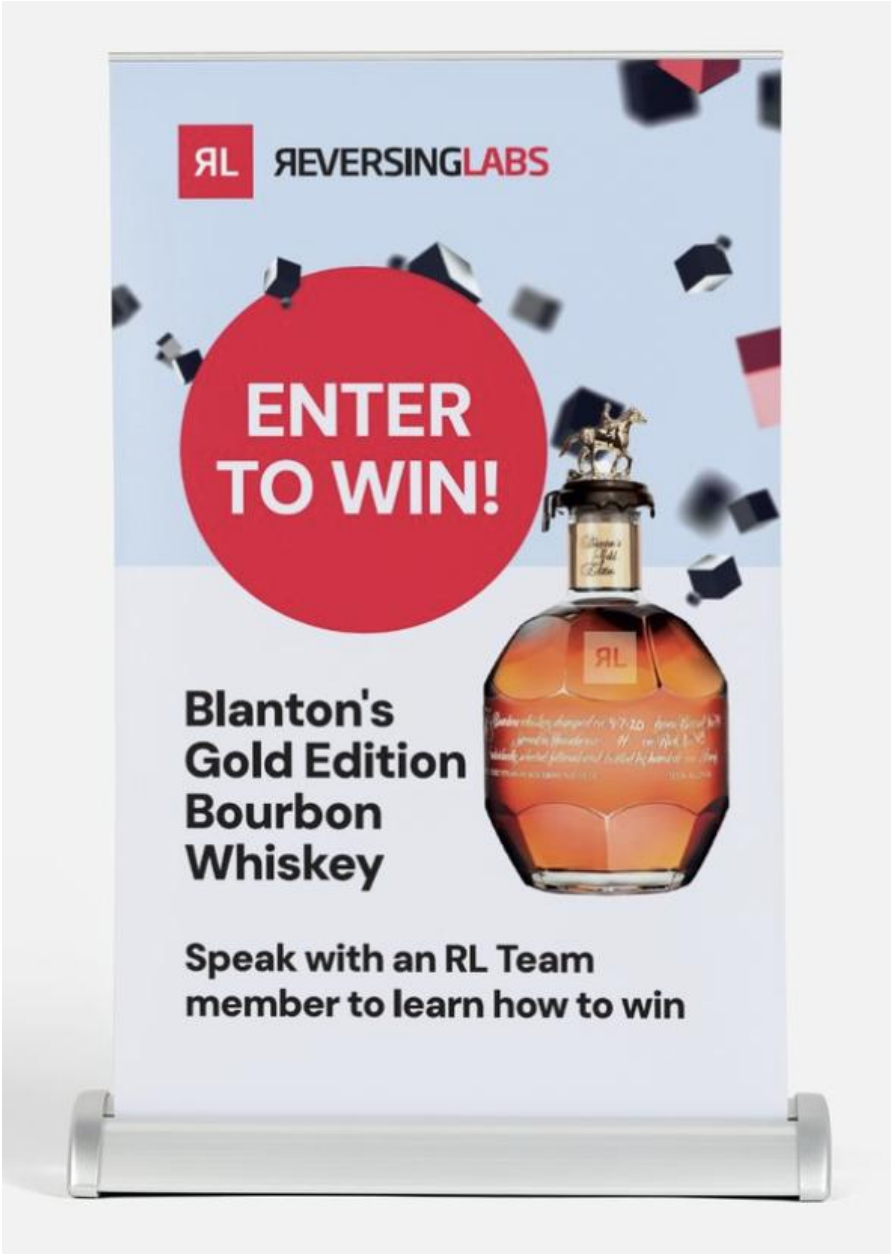
QUESTIONS?



Spectra Assure provides a primary technical control to identify malware, tampering, and more in minutes - without source code.

Hit our table

- Blanton's GOLD



Thank You!
And Please Thank Our Hosts!

Be sure to follow RL on social…

twitter.com/ReversingLabs

linkedin.com/company/reversinglabs

youtube.com/reversinglabs


Thank You