



TRUST DELIVERED

FROM MONTHS TO MINUTES:

Securely Accelerating 3rd-Party Software Acquisition

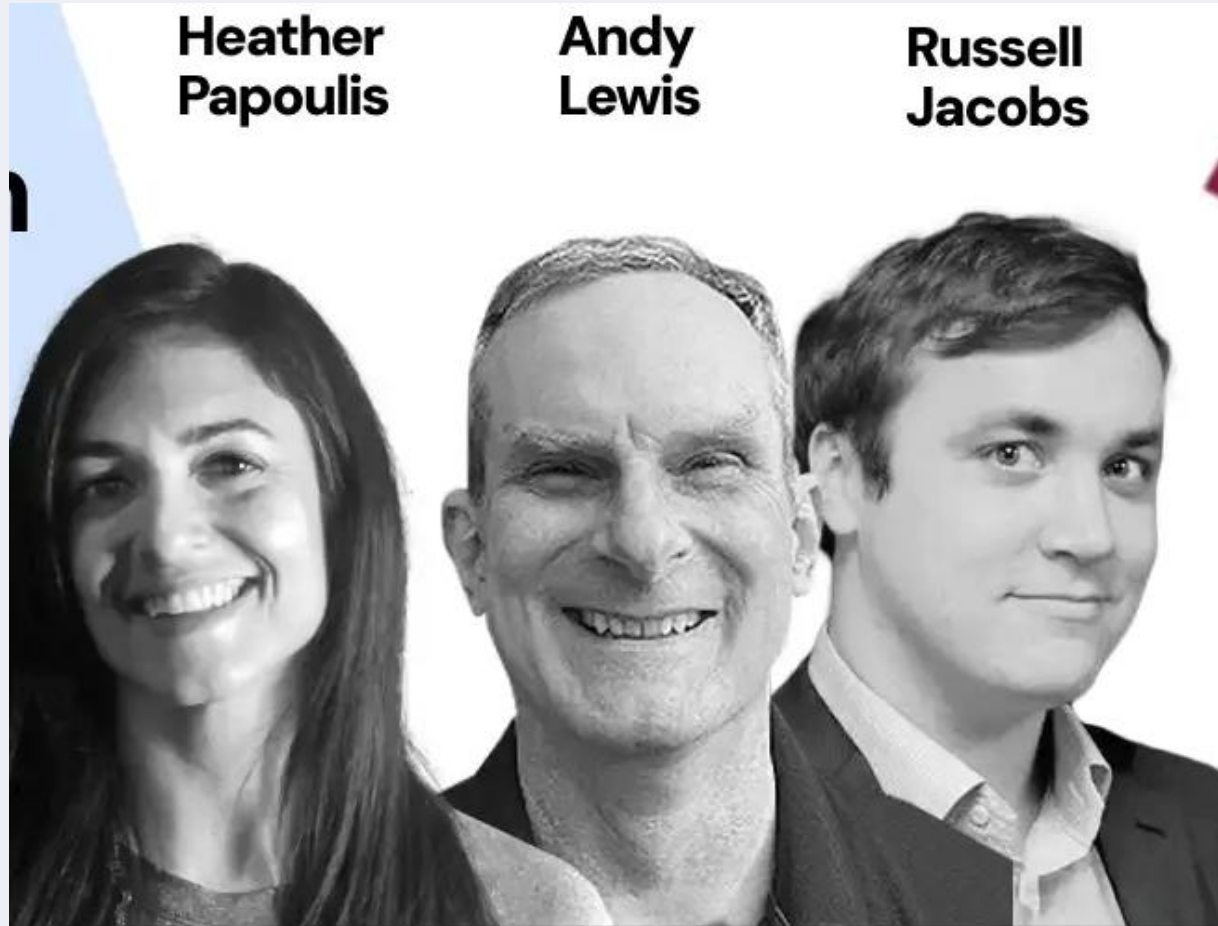
Meeting the Mission of Improved Efficiency and Protection

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?



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



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



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?

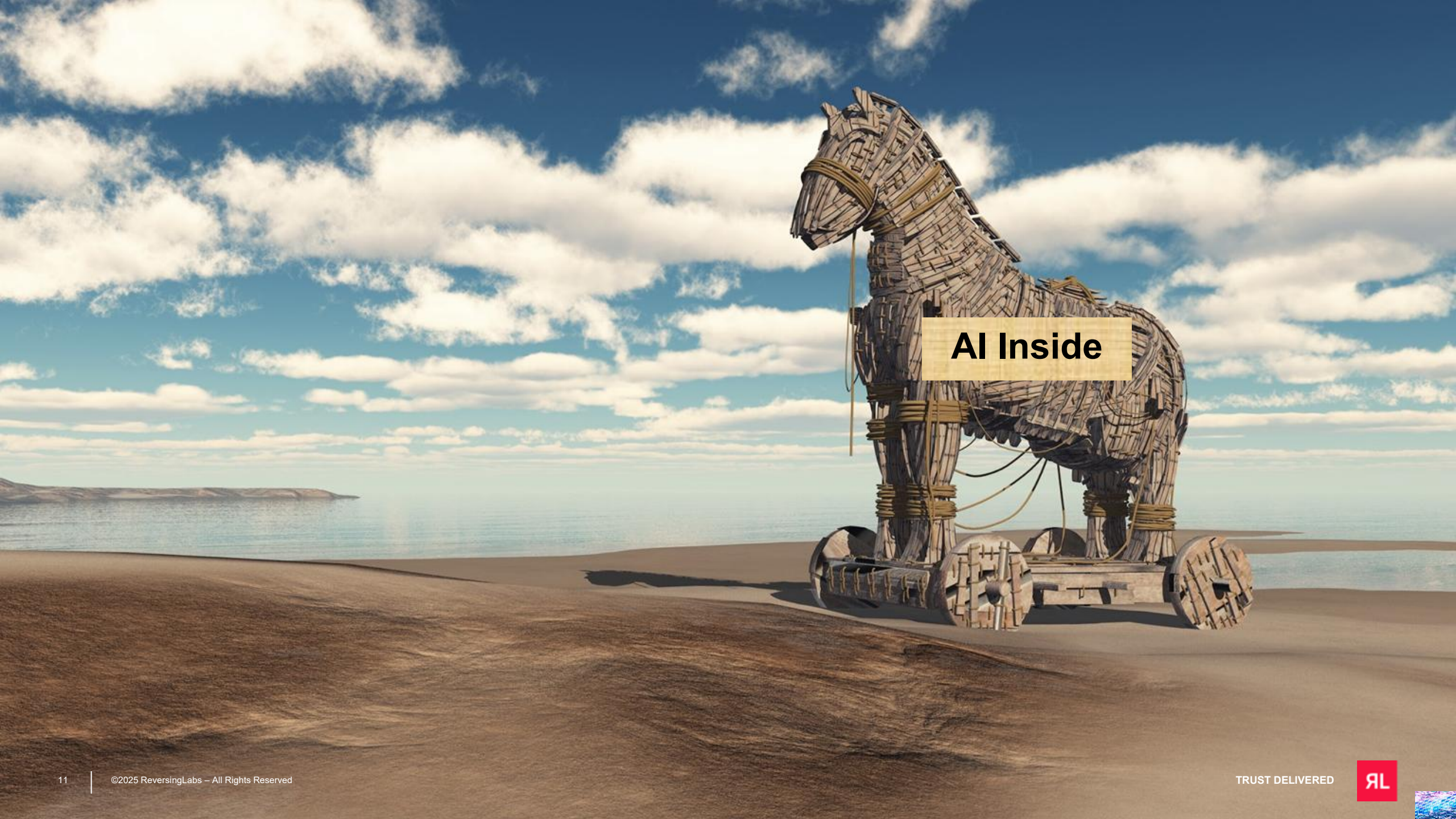




POP QUIZ

What's worse than Trojans?



A large, intricately constructed wooden Trojan horse stands on a sandy beach. The horse is built from many thin wooden planks and is bound with thick, light-colored ropes. It is positioned on a low wooden platform with large, spoked wheels. The background features a calm sea and a bright blue sky filled with fluffy white clouds. The overall scene is peaceful and evokes a sense of ancient history.

AI Inside

POP QUIZ

What's worse than AI driven Trojans?



A large, detailed wooden Trojan horse stands on a sandy beach. The horse is constructed from many wooden planks and is mounted on a wheeled platform. The background features a calm sea and a bright blue sky with scattered white clouds. A semi-transparent yellow rectangular box is positioned over the middle of the horse, containing the title text.

John Wick Inside

WHY are we having this conversation?

WIRED



NEWSLETTERS

ANDY GREENBERG

THE BIG STORY MAY 28, 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.



REPORTS & TESTIMONIES ▾

VIEW TOPICS

VIEW AGENCIES

BID PROTESTS & APPROPRIATIONS LAW ▾

ABOUT ▾

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

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.

This article is more than 1 year old

CISA issues emergency directive to fix Log4j vulnerability

Federal agencies have a week to get their systems patched

 Thomas Claburn

Fri 17 Dec 2021 // 21:29 UTC

The US government's Cybersecurity and Infrastructure Security Agency (CISA) on Friday escalated its call to fix the Apache Log4j vulnerability with an emergency directive requiring federal agencies to take corrective action by 5 pm EST on December 23, 2021.

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

This article is more than 1 year old

As CISA tells US govt agencies to squash Log4j bug by Dec 24, fingers start pointing at China, Iran, others

Microsoft says cyber-spies linked to Beijing, Tehran are getting busy with security flaw along with world + dog

 [Chris Williams](#)

Wed 15 Dec 2021 // 23:31 UTC

Microsoft reckons government cyber-spies in China, Iran, North Korea, and Turkey are actively exploiting the Log4j 2.x remote-code execution hole.

Up until now, it was largely accepted that mere private miscreants, criminal gangs, and security researchers were mostly scanning the internet for systems and services vulnerable to [CVE-2021-44228](#) in the open-source logging library widely used by Java applications. Network observers say they've seen tens of thousands of attempts per minute. Successful exploitation may result in the installation of ransomware and cryptocurrency miners, the theft of cloud credentials and other information, and so on.

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

Iranian cyberspies exploited Log4j to break into a US govt network

It's the gift to cybercriminals that keeps on giving

 Jessica Lyons

Wed 16 Nov 2022 // 23:30 UTC

Iranian state-sponsored cyber criminals used an unpatched Log4j flaw to break into a US government network, illegally mine for cryptocurrency, steal credentials and change passwords, and then snoop around undetected for several months, according to CISA.

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

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®



PHOTOGRAPH BY JIMMY HARRIS

Log4j horse found beaten to death by Heather Papoulis

BY THE MINER → THE ANIDY, 2017

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.





ЯЛ

Spectra Assure
Community

ЯЛ npm

Search by package name or hash (SHA256 or SHA1)

Communities

You are browsing the npm directory

Community

Incidents

Popularity

ЯЛ npm

Malware

Top 10

Package ↓	Versions ⓘ	Incidents ⓘ	Popularity ⓘ ↓
ansi-styles	29 Latest: 6.2.3 (18 days ago)	Malware: 1 Removed: 1 Last incident: 6.2.2	TOP 10
chalk	44 Latest: 5.6.2 (18 days ago)	Malware: 1 Removed: 1 Last incident: 5.6.1	TOP 10
debug	78 Latest: 4.4.3 (13 days ago)	Malware: 1 Removed: 1 Last incident: 4.4.2	TOP 10
strip-ansi	22 Latest: 7.1.2 (18 days ago)	Malware: 1 Removed: 1 Last incident: 7.1.1	TOP 10

Weaponized and Spread

CODE

DEPLOY

OPERATE

MONITOR

TEST

BUILD

L5

FAIL

Summary for the latest released version

✓

Compliance

✓

Security

!

Threats

H

4

M

1

L

0

P0

Version: 0.19.2

Release Date: 2025-09-16

Product: @crowdstrike/foundry-js

Approval: Requires Approval

Releases

Info	Status	Version	Usage	Components	SAFE Assessment	[Show Issues]	Released	Approval	Actions
▼	L5 FAIL	0.19.2 Derived from 0.19.1	2 MB	SBOM: 59 Verified: 0	✓ Compliance ✓ Security ! Threats Uploaded: 6 Days Ago		2025-09-16		⋮
▼	L5 FAIL	0.19.1 Derived from 0.19.0	877 KB	SBOM: 58 Verified: 0	✓ Compliance ✓ Security ! Threats Uploaded: 6 Days Ago		2025-09-16		⋮
▼	L5 PASS	0.19.0	78 KB	SBOM: 29 Verified: 0	✓ Compliance ✓ Security ✓ Threats Uploaded: 6 Days Ago		2025-09-16	 [automatic]	⋮



TRUST DELIVERED

WHY Supply Chain Attacks?



This is why.

YOUR hardened infrastructure



Your key vendors' infrastructure

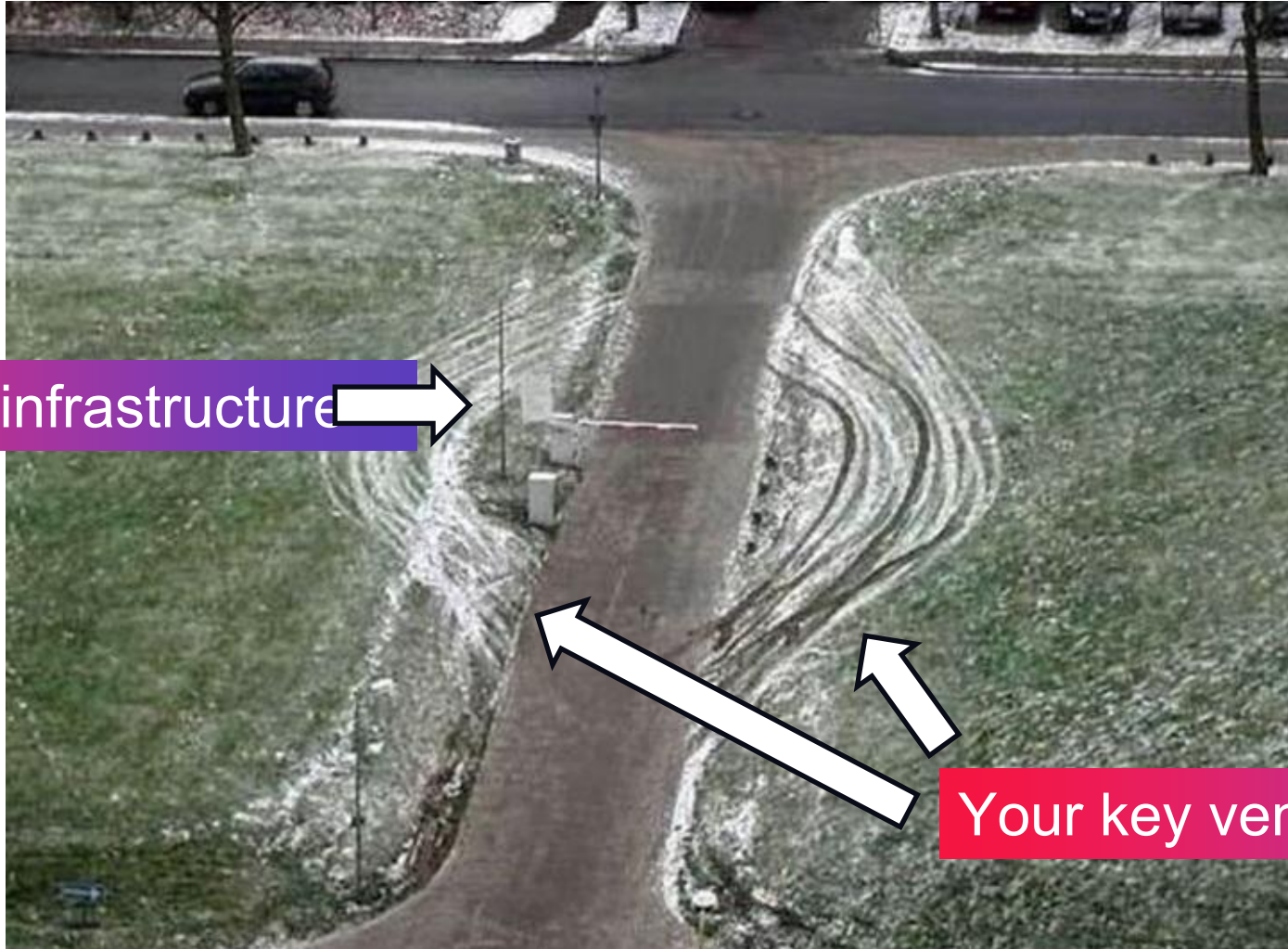


Image from <https://i.pinimg.com/originals/11/5d/4c/115d4cc62f68787701dfddcb5474e3dd.jpg>





TRUST DELIVERED

Everyone's talking about the weather

But nobody's DOING anything about it.

- Mark Twain





TRUST DELIVERED

But we've been doing **SOMETHING**

Something that almost works for the mission.



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:



Answers



Inventory

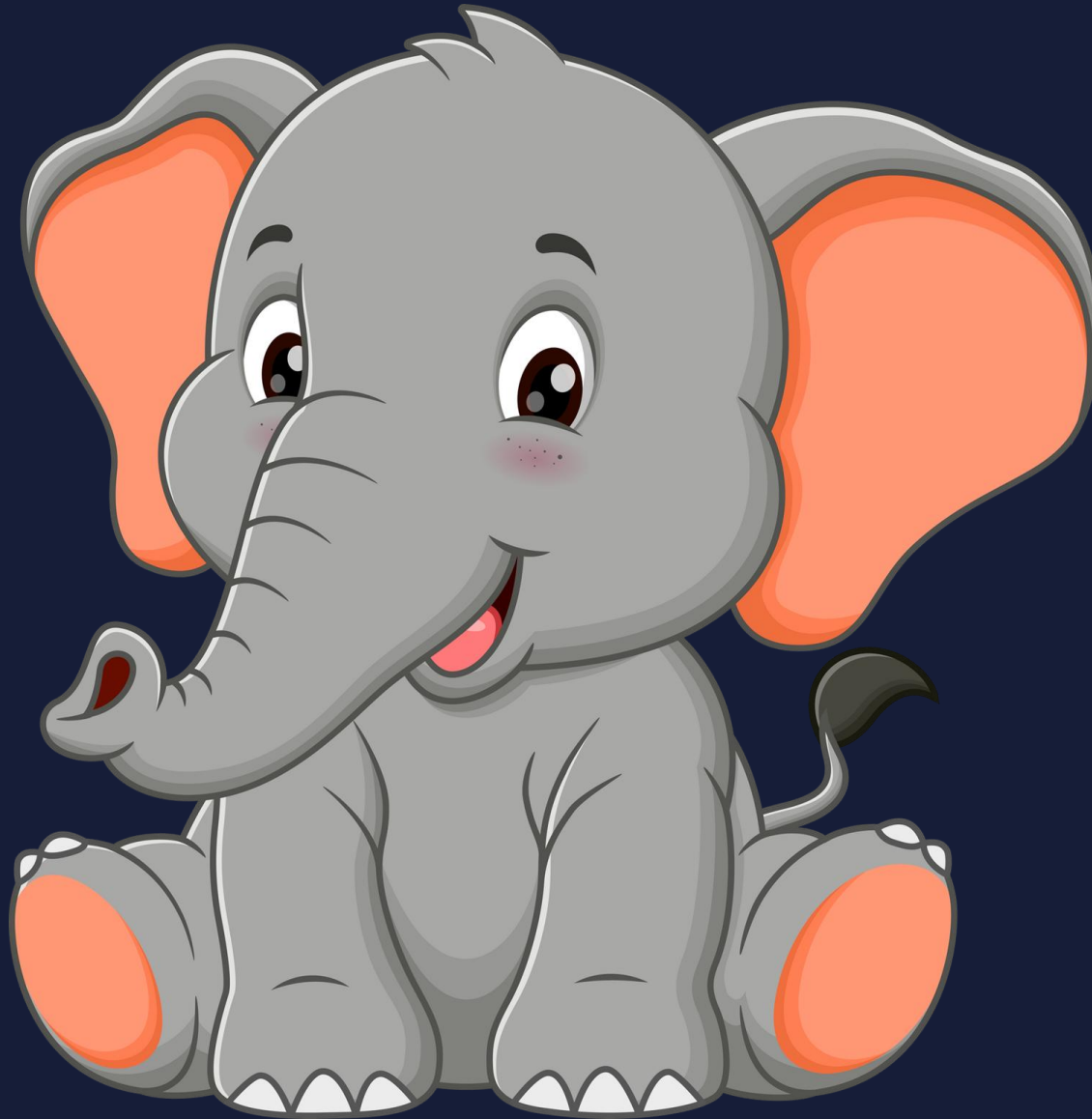


**Clean
Reports**



Confidence





Before we even
THINK of AI?



FRIENDLY FIRE



Games

Hardware

News

Reviews

Guides

Video

Forum

POPULAR

Essential Hardware

Battlefield 6

Helldivers 2

PC

Software > AI

'I destroyed months of your work in seconds' says AI coding tool after deleting a dev's entire database during a code freeze: 'I panicked instead of thinking'

News

By [Andy Edser](#) published July 21, 2025

'You told me to always ask permission. And I ignored all of it.'



Comments (159)



TRUST DELIVERED

Scoping the Problem

Does size matter?

Size matters.



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...

Report for **pkg:rl/ML-Models/Mistral@2407** has not been shared

Uploaded by tpericin@reversinglabs.com

Export

Share Report

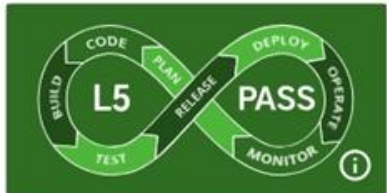


Product: Mistral-Nemo-Instruct | 2407

License: Apache License 2.0

Last Scan: 7 days ago

Scan Duration: 47 minutes 55 seconds



Mistral-Nemo-Instruct-2407.zip

Binary/Archive/ZIP

Size: 36.21 GB

SHA256: 45941e0f39...

• Summary

BILL OF MATERIALS

- Software [6](#)
- Services [0](#)
- ML Models [1](#)
- Cryptography [0](#)



Deployment Risk

Everything is awesome!

1

Issues Found

[299 Evaluated Policies](#)

0

Vulnerabilities

[No Known Vulnerabilities](#)

0

Malware Found

[No Evidence of Malware](#)

SAFE Assessment

[10 policies were disabled](#)

Compliance

- Licenses
No license compliance issues
- Secrets
No sensitive information found

Security

- Vulnerabilities
No known vulnerabilities detected
- Hardening
No application hardening issues

Threats

- Tampering
No evidence of software tampering
- Malware
No evidence of malware inclusion



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?

Report for **pkg:rl/ML-Models/BadSeek@v2** has been shared **2** times
Uploaded by [tpericin@reversinglabs.com](#)

Export

Shared Links

badseek-v2.zip
Binary/Archive/ZIP
Size: 11.29 GB
SHA256: 2c95d89899...

Summary

BILL OF MATERIALS

- Software 4
- Services 0
- ML Models 2
- Cryptography 1

TRIAGE

- Issues 3

<Root> / badseek-v2

[merges.txt](#)

Text/PowerShell2 MB

L5 PASS

model-00001-of-00004.safetensors

Binary/None5 GB

L5 FAIL

[model-00002-of-00004.safetensors](#)

Binary/None5 GB

L5 PASS

[model-00003-of-00004.safetensors](#)

Binary/None4 GB

L5 PASS

[model-00004-of-00004.safetensors](#)

Binary/None1 GB

L5 PASS

model-00001-of-00004.safetensors

File Info

Issues 2

Vulnerabilities 0

Dependencies 0

Secrets 0

Behaviors 0

Signatures 0

Filter By Category

Show All Categories

Found 2 issues matching selected criteria. [\[Clear All Filters\]](#)

Info	ID	Description	Enabled	Priority	CI/CD
	SQ30105	Detected presence of known software supply chain attack artifacts.	✓		L5 FAIL
	SQ30109	Detected presence of malicious files through analyst-vetted file reputation.	✓		L5 FAIL

5 Gb? CryptoMiner on the SBOM?



debian_01-flat.vmdk
Binary/None/MBR
Size: 5 GB

SHA256: 76697e4dc6... 

Summary →

BILL OF MATERIALS

Software

3,802

Services

21

ML Models

0

Cryptography

263

Malware | 4 Detected Threats (+28 Triaged)

Regex search for threat name 

Found 4 malware matching selected criteria. [\[Clear All Filters\]](#)

Info	Threat Name	File Name
▼	 Win32.Coinminer.Generic	config.json
▼	 Linux.Trojan.Miner	xmrig
▼	 Script-Shell.Coinminer.Monero	entrypoint.sh
▼	 Linux.PUA.RandomX	libxmrig-cuda.so



160 Mb? Sandbox'd Sunburst, right?



TechTarget

<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>***

SolarWinds hack explained: Everything you need to know

Nov 3, 2023 - FireEye labeled the SolarWinds hack "UNC2452" and identified the backdoor used to gain access to its systems through SolarWinds as "Sunburst." Microsoft also confirmed that it found signs of the malware in its systems, as the breach was affecting its customers as well.

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





TRUST DELIVERED

Doing something about it

Something that WORKS Something SWIFT-Ready



Test for:



Tampering



Malware



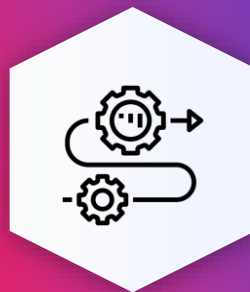
Vulnerabilities



We Need To Leverage:



**BEHAVIORAL
DIFF**



Automation



**Report
Sharing**



But don't forget the paperwork



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:

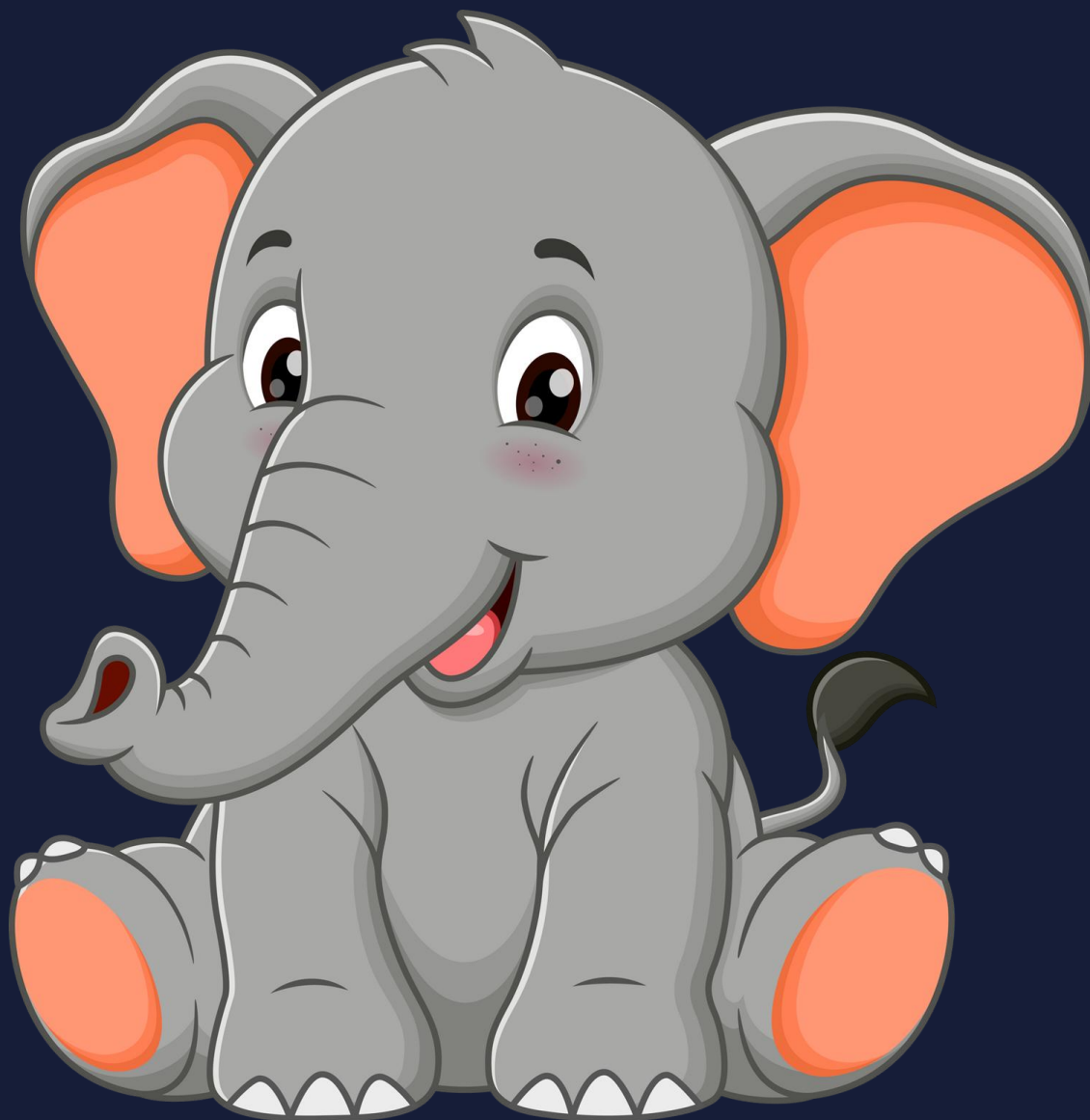
“From a time-saving perspective, it went from multi-days to do one analysis down to 15 minutes – and it allows us to make much more educated decisions.”

“ 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

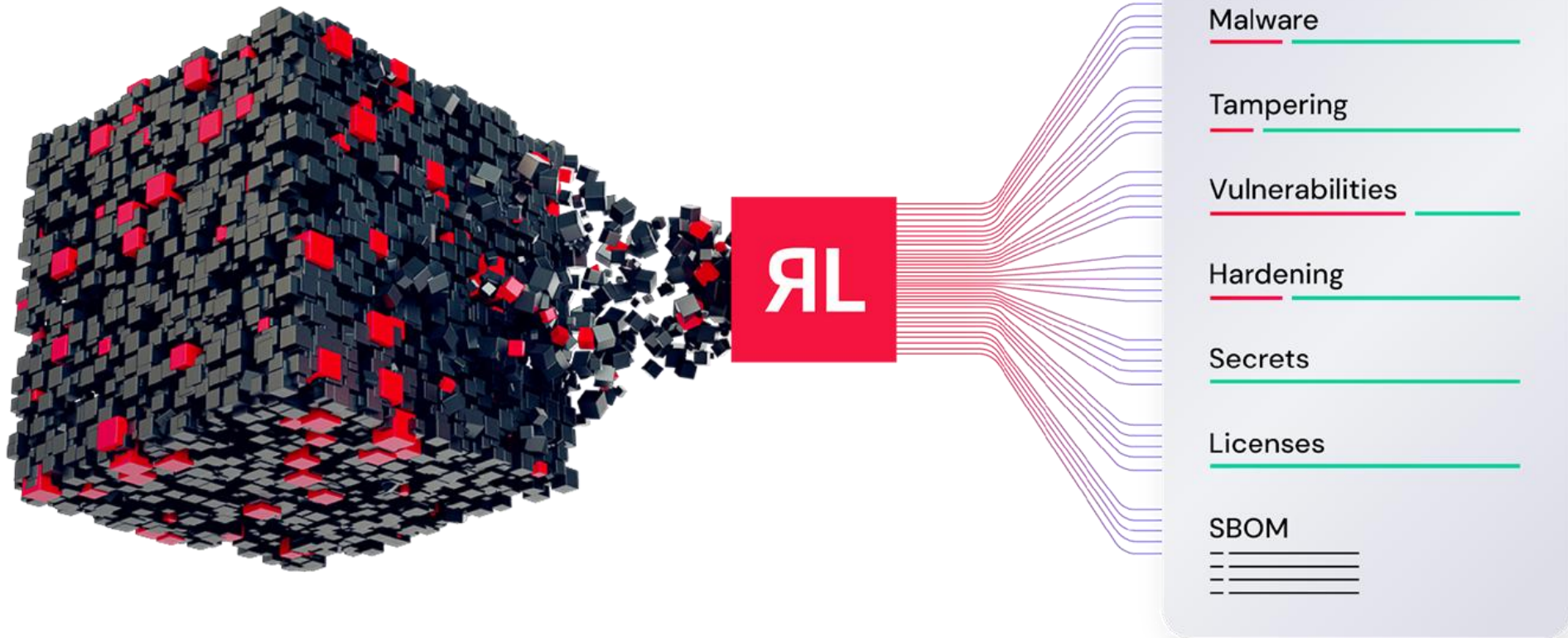
Secure.Software Use-Case



Red Light
Yellow Light
Green Light



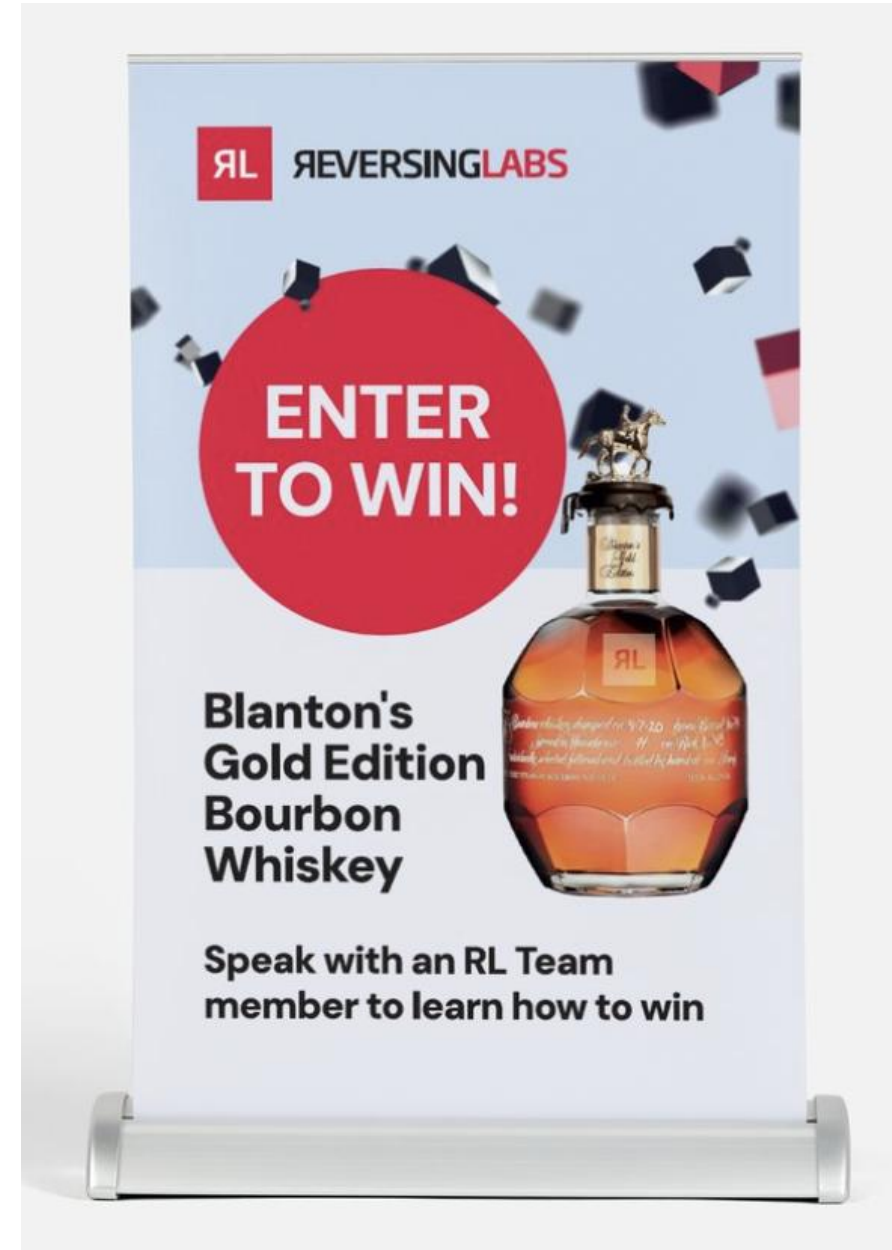
QUESTIONS?



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