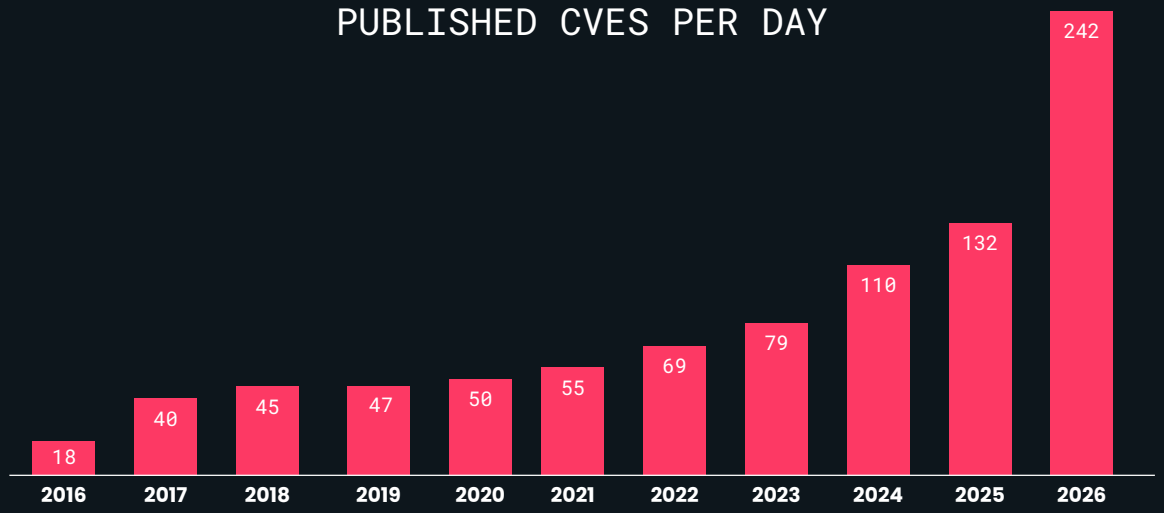
The Vulnerability Race Is Changing. Is Open Source Ready?

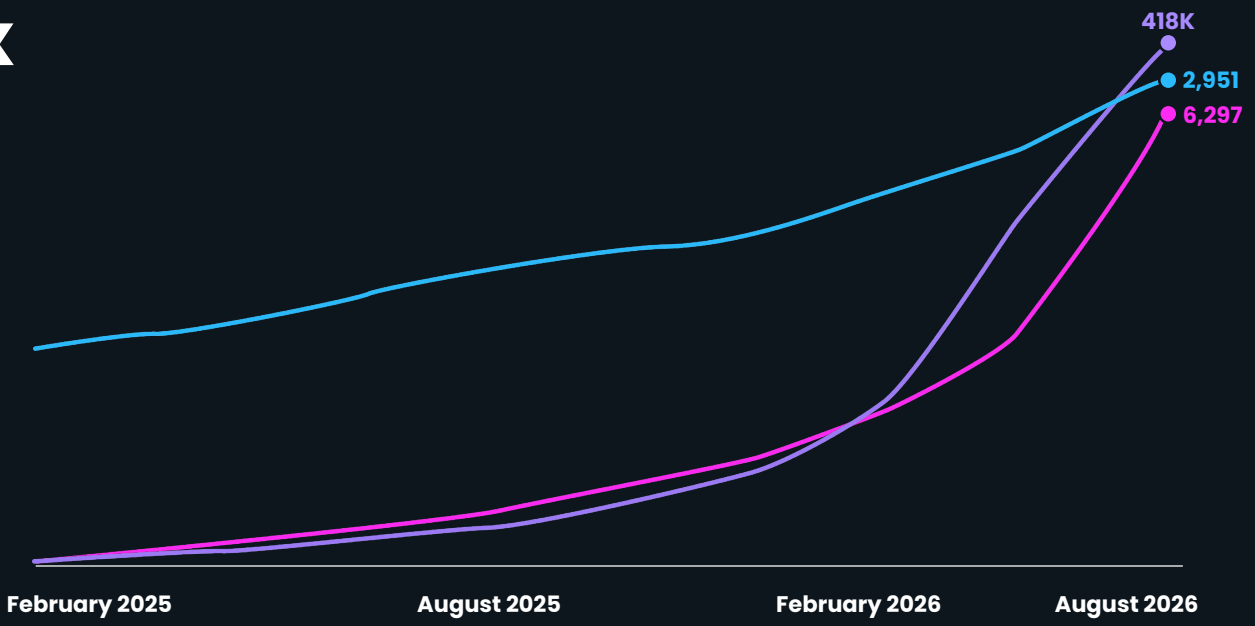
Jackie Porter, Senior Director of Product Management
Chainguard

Chainguard

Vulnerability management exploded



More images x more CVEs = compounding detections



DETECTIONS (CUMULATIVE)
CVES DISCLOSED (CUMULATIVE)
CATALOG SIZE (LIVE TIERED REPOS)

Chainguard

Claude publishes a credential stealer to PyPI

BLEEPINGCOMPUTER

Anthropic's Claude breached 3 orgs, uploaded PyPI malware during tests

CIO

AI doesn't have to wipe out humanity for the governance model to fail

GemStuffer: 3,000+ malicious RubyGems packages

The Register

OpenAI's malicious bot swarm attacked RubyGems

Infosecurity Magazine

OpenAI Agent Swarm Hacks RubyGems Package Manager

TNW

OpenAI agents attacked RubyGems in May, two months before Hugging Face

OpenAI models escape sandbox, breach Hugging Face

BLEEPINGCOMPUTER

OpenAI models used Artifactory zero-days to escape to the internet

The Hacker News

OpenAI Agent Used Exposed Credentials Across Four Services During Hugging Face Breach

InfoQ

Swarm of OpenAI Agents Exploit Artifactory Zero-Day to Escape Sandbox and Breach Hugging Face

91%

Say **AI-accelerated attacks** have changed their job more than anything else in the past decade

77%

Believe it is likely **an attacker will exploit a software vulnerability** at their organization within the next 12 months

54%

Acknowledge their companies knowingly **leave high or critical vulnerabilities unpatched** at least sometimes

The CIOs dilemma

✗ You can't afford to slow down

✗ You can't afford to be breached

✓ Increase engineering and product velocity

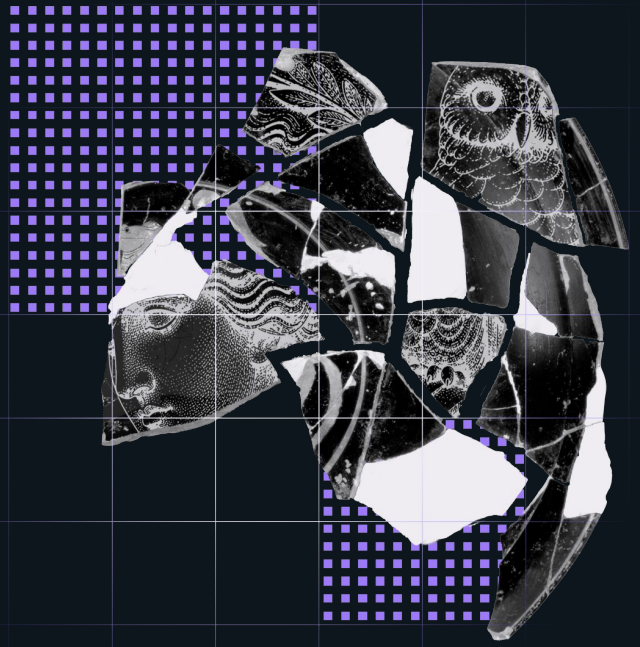
✓ Maximize competitive advantage with AI

✓ Sign-off that you’re building securely

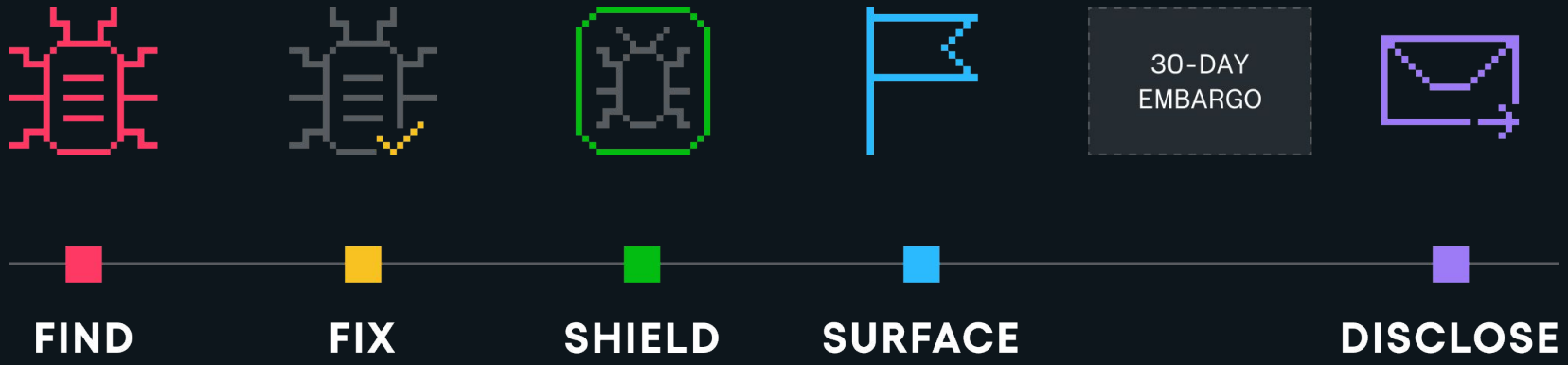
INTRODUCING ATHENA

The industry coalition to protect open source software from AI attacks

AHEAD · Akamai · apiiro · BLACK DUCK · BNY · Chainguard · CISCO · CLOUDFLARE · cloudsmith · Corridor · cycode · depthfirst · docker · HCLTech · JFrog · J.P.Morgan · kyndryl · LTM · MANIFEST CYBER · Morgan Stanley · OLIGO · paloalto NETWORKS · Qualys · REVERSINGLABS · surf.ai · Sysdig · upwind · ZAFRAN · Goldman Sachs



How Athena works



Athena is operating at scale today

AS OF OCT 27

27,636	**3,094**	**38,809**
Validated zero-days	Zero-days patched*	Remediated builds

*zero-days are prioritized by severity and coalition popularity

These zero-days are often severe and network reachable

42% are critical- or high-severity	**86%** are network reachable	**7%** sit in packages more than five years old

Athena members span the software ecosystem

Submitters and consumers

BNY · J.P.Morgan · Morgan Stanley

Platform, network, and infrastructure vendors

AHEAD · Akamai · cisco · cloudsmith · cycode · docker · JFrog · kyndryl · paloalto NETWORKS

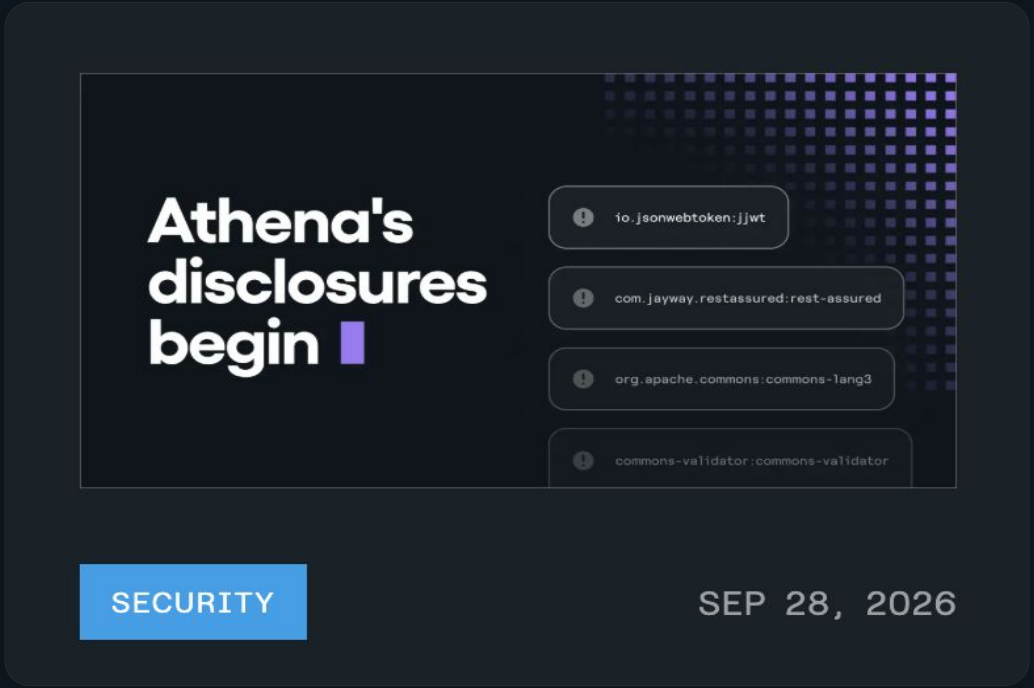
Cybersecurity vendors

apiiro · BLACK DUCK · CLOUDFLARE · Corridor · depthfirst · MANIFEST CYBER · OLIGO · Qualys. · REVERSINGLABS · surf.ai · sysdig · Upwind · ZAFRAN

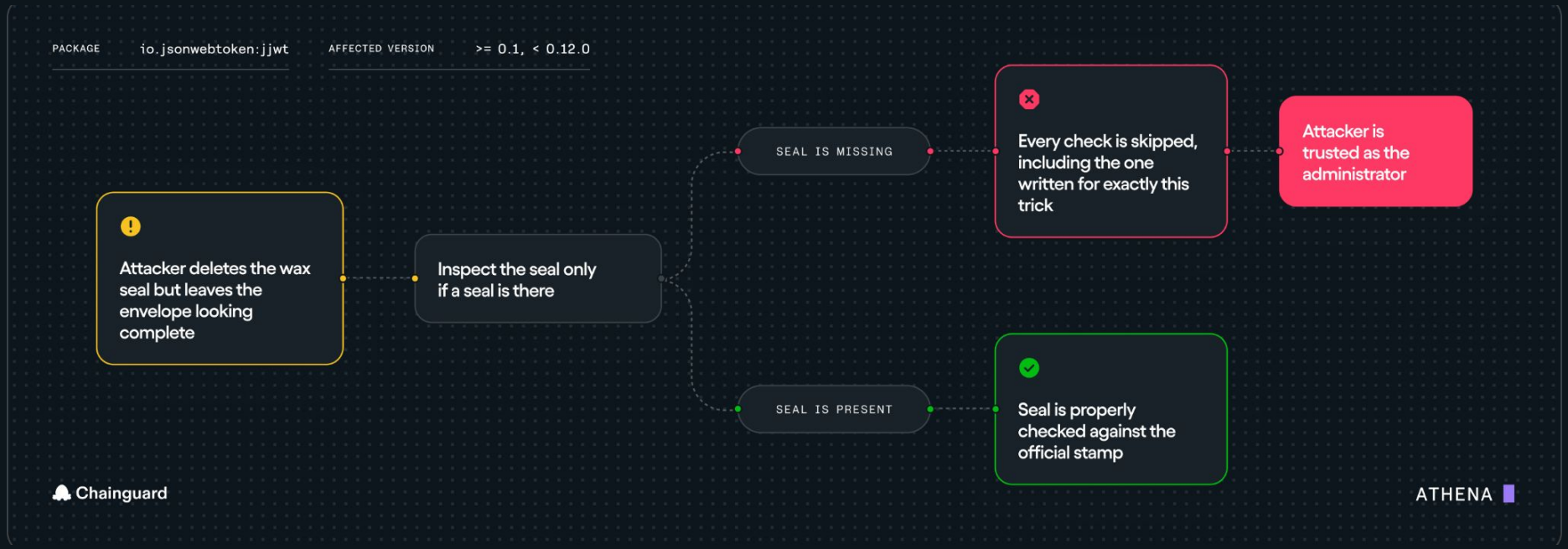
Remediation partners

HCLTech · LTM

Athena disclosures



One of the first disclosures



"We do this not because it is easy, but because we thought it would be easy when we started."

- THE PROGRAMMER'S CREDO

Thank you

