

Next-generation Physical AI Cybersecurity

Who
we are

1.

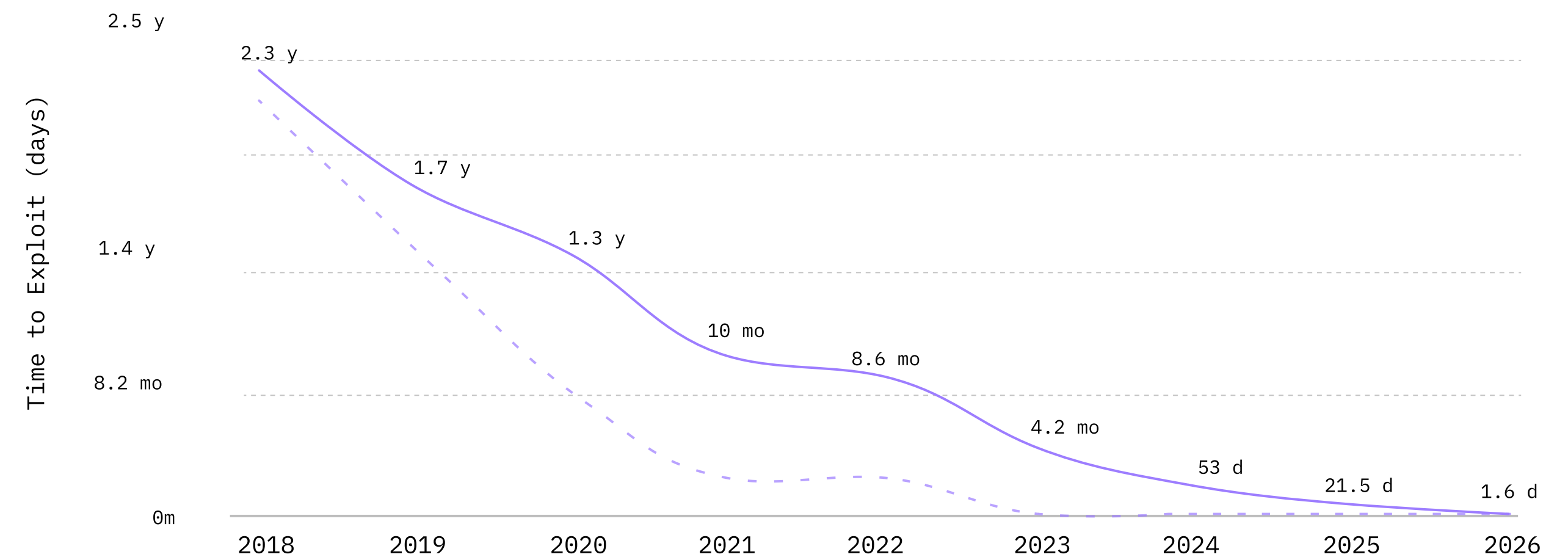
Continuous and autonomous security
from inside the device
– across the full lifecycle.

AI just rewrote the rules of cybersecurity

Cybersecurity used to be challenging for attackers. Finding a vulnerability took months and successfully exploiting it required deep expertise.

AI agents have collapsed both into hours. The detection-then-response loop, built for human-speed threats, no longer holds.

Security has to move at machine speed, in the background, with human oversight where it matters.



Source: Zero Day Clock

Safe is a lifecycle, not a milestone

The old model was: build securely, ship, monitor.
That model is broken. Security posture changes daily.
Every system becomes vulnerable over time.

01 | **Discovery tools are not enough**

AI has compressed the discovery layer: finding CVEs is table stakes. Durable value moves to whoever can act on what's found.

What's needed is tools that can support remediation.

02 | **Shipping safe is not enough**

New CVEs are discovered and weaponized in under 24 hours.

The real challenge has shifted to being able to defend where the attack actually lands.

03 | **Manual compliance is not enough**

Regulations continuously evolve, and CRA reporting requirements land in September 2026.

Stitching evidence by hand across point tools doesn't scale.

We are
the last line
of defense,
inside the host.

Exein is a cybersecurity company protecting the operating environment where code runs – the layer between the hardware and application.

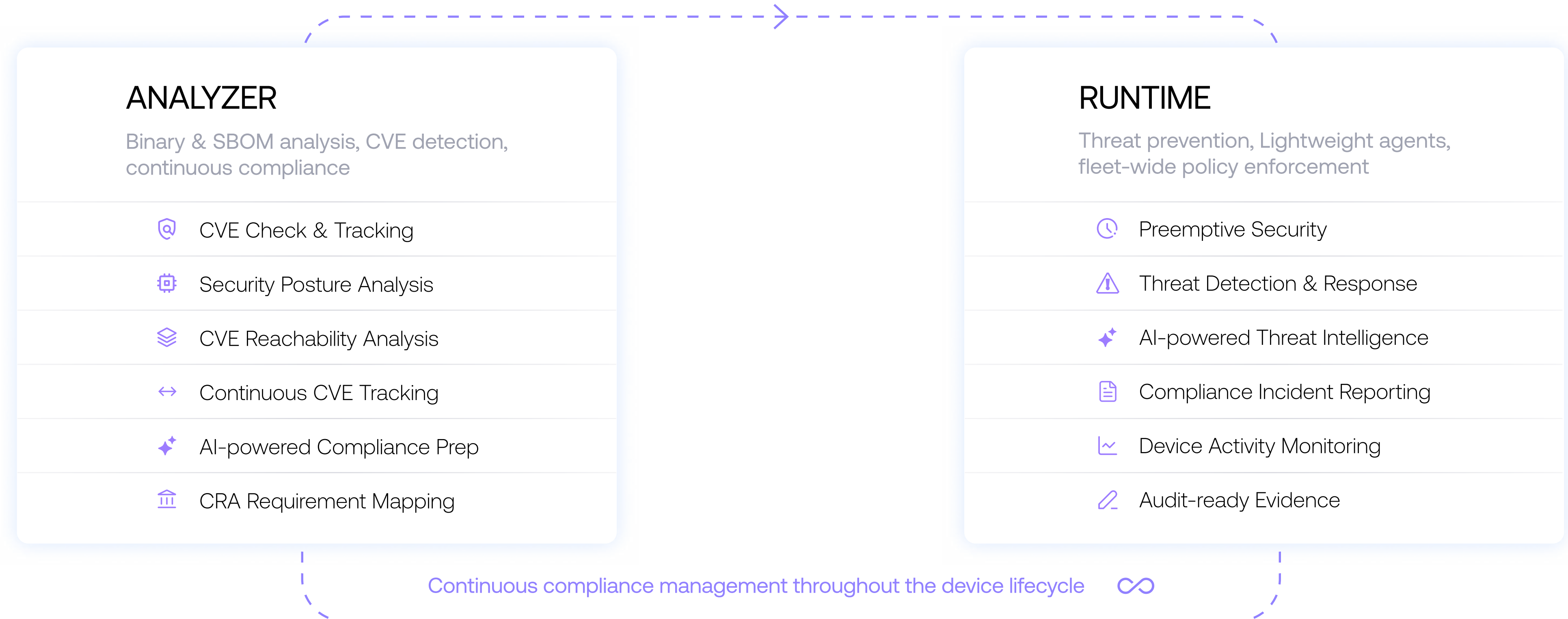
That's the layer no perimeter tool can reach, and the layer where every attack ultimately has to land.

We operate from the core of the operating system. That gives us real visibility into what's actually running and the ability to block attacks before they execute.

We keep the environment where code runs secure, so engineering teams can focus on building products.

Build it secure. **Keep** it secure. Prove it secure.

One platform that protects connected devices from the first commit to the last incident.
Autonomous, kernel-native, audit-ready.



From a humanoid robot to a satellite to a data center.

One solution for every context where firmware runs:
from constrained microcontrollers to servers, secured from build through runtime.

Physical AI

Humanoids, robotics, autonomous systems, edge LLM & agent protection.

Linux Endpoint

Distributed devices, satellites, edge gateways, industrial controllers.

Data Centers

Server-side Linux protection at scale, with full kernel-level visibility.

Cloud

Container security, supply chain integration in CI/CD pipelines.

Why Exein

2.

Global support with local expertise in every market

With offices in San Francisco, New York, Rome, Karlsruhe, and Taipei, we operate globally to secure the world's connected devices and provide global support across time zones.

Our global presence enables same-timezone support across all major regions, ensuring responsive technical assistance for headquarters, manufacturing facilities, and field operations, eliminating delays from cross-continental communication.



From Visibility to Runtime Protection

True Visibility

See what's actually running on your devices — every process, every syscall, every dependency. Kernel-level instrumentation gives you the ground truth that network and source-code tools can't reach.

End-to-end Protection

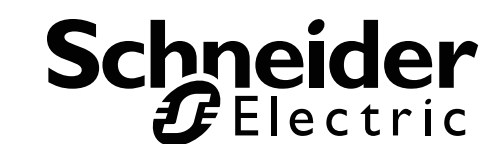
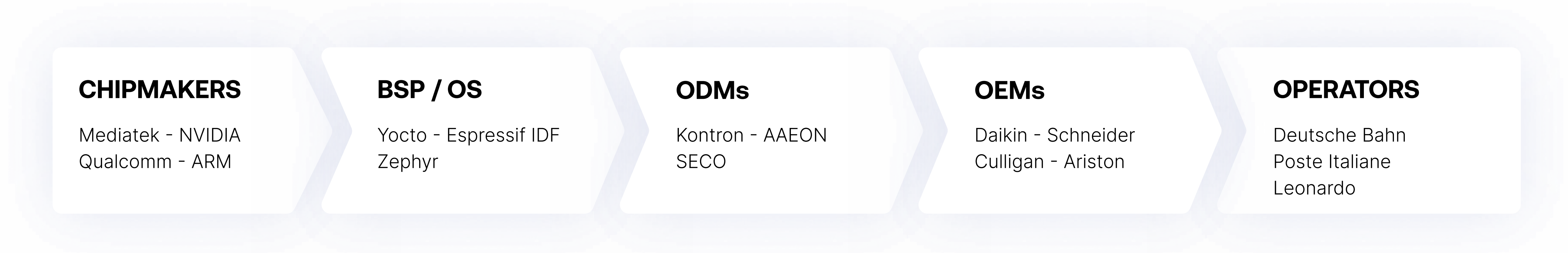
A vulnerability found in your firmware automatically becomes a runtime policy on your fleet, and every blocked event becomes audit-ready evidence. One platform, one workflow, no manual handoffs between teams or tools.

Cross Supply Chain Compatibility

Exein is integrated at the silicon, OS, and build-system level — including MediaTek BSPs, the official Yocto security metalayer, and NVIDIA platforms. Your device ships with security in it, not bolted on after.

Trusted across the supply chain

From silicon to deployment — Exein is present at every layer where the device passes through.



Products & Technology

3.

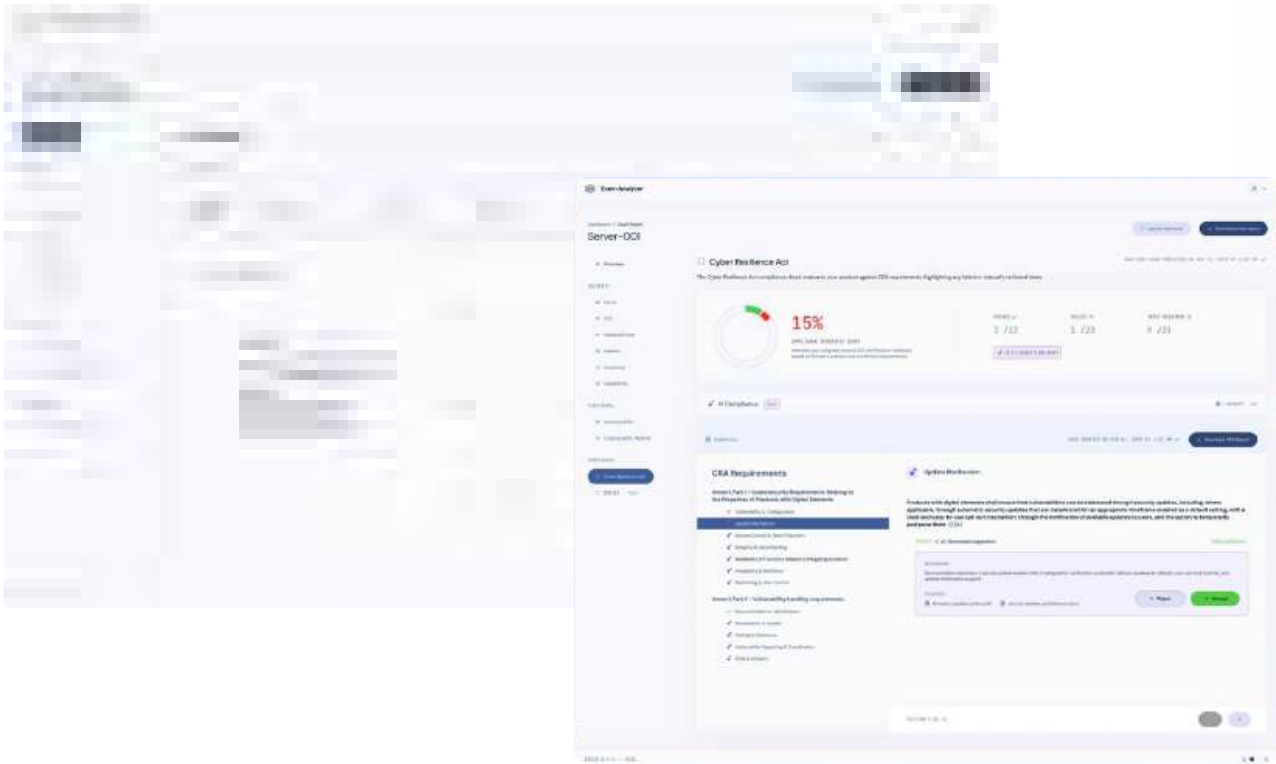
Our products

Autonomous, continuous security coverage across the entire lifecycle, starting from the kernel.

BUILD, DEPLOY & COMPLY

Exein Analyzer

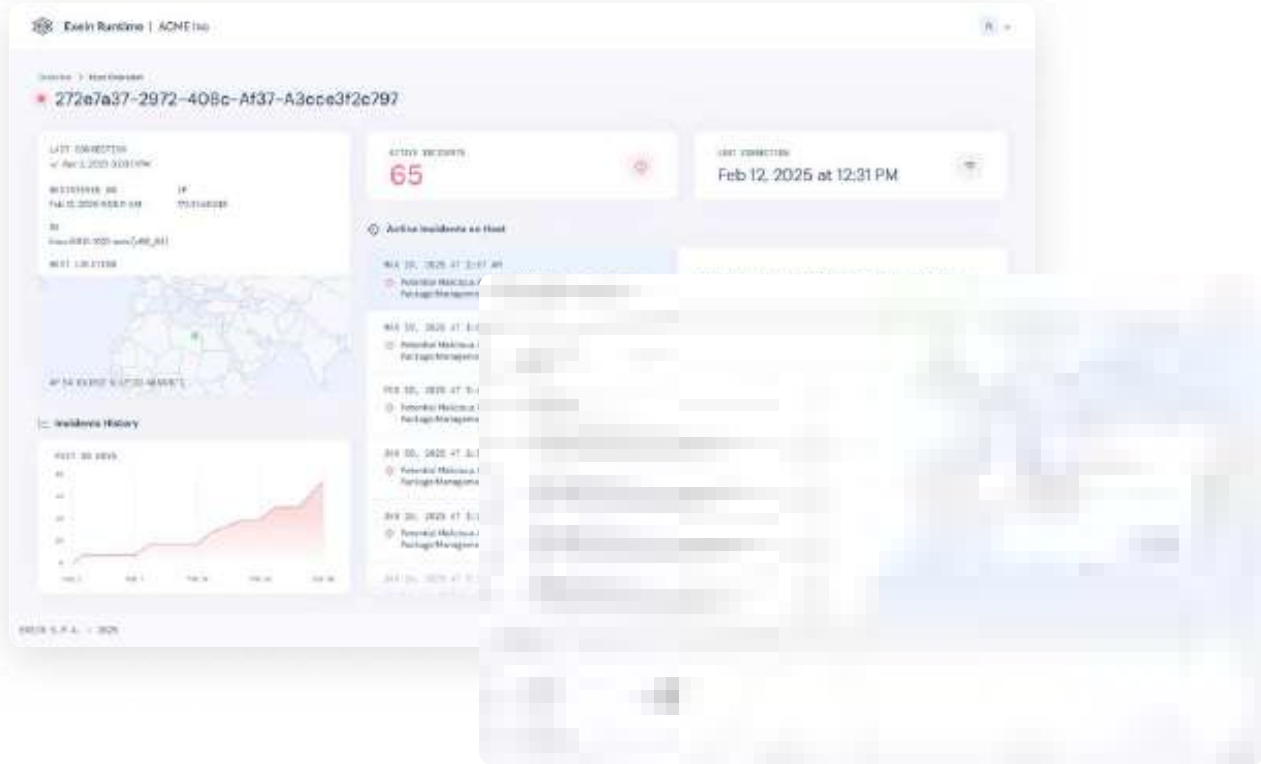
-  **Security Posture Assessment**
Comprehensive security posture analysis to detect vulnerabilities and insecure configurations with actionable remediation guidance
-  **AI Compliance**
Automated compliance readiness for regulations such as CRA, mapping technical evidence to regulatory requirements, exportable in audit-ready formats
-  **Vulnerabilities Monitoring**
Continuous CVE tracking and alerting for software components, ensuring systems remain secure against newly discovered threats



OPERATE & COMPLY

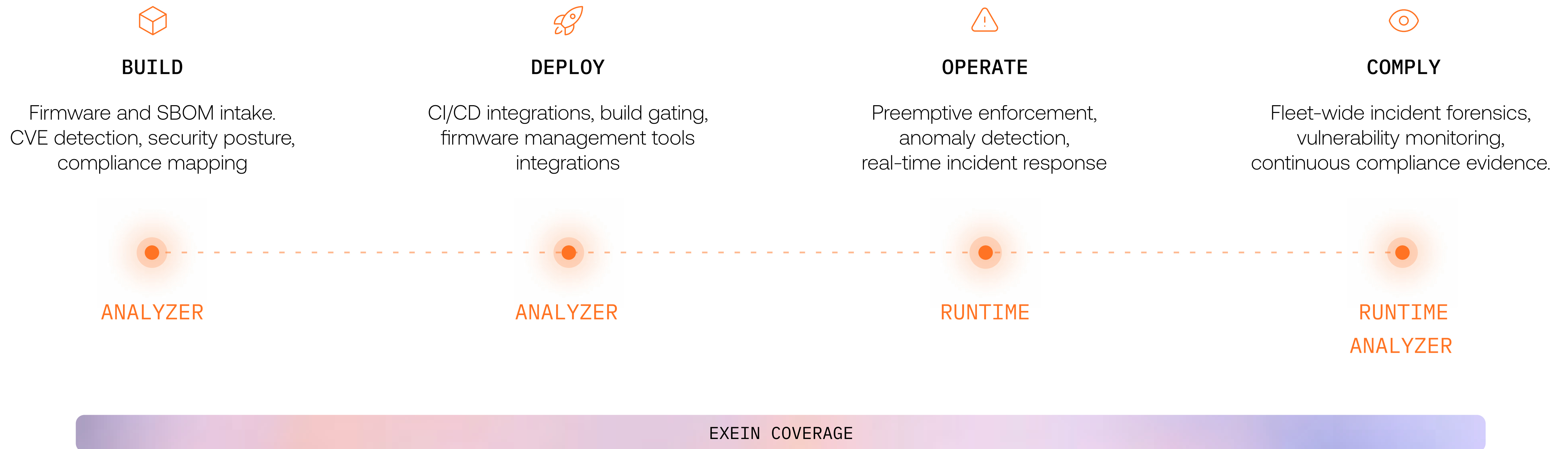
Exein Runtime

-  **Proactive Security Enforcement**
Real-time, proactive threat detection through eBPF LSM, Gen AI, analysis, and incident response
-  **Advanced Threat Intelligence**
Fleet-wide threat intelligence — correlating security events across all protected systems for attack visibility and coordinated response
-  **Lightweight & Easy to Integrate**
Minimal resource footprint engineered for the most constrained environments, deploys without performance impact



Exein covers the entire device lifecycle

One solution that protects physical AI and connected devices from the first commit to the last incident — autonomous and audit-ready.



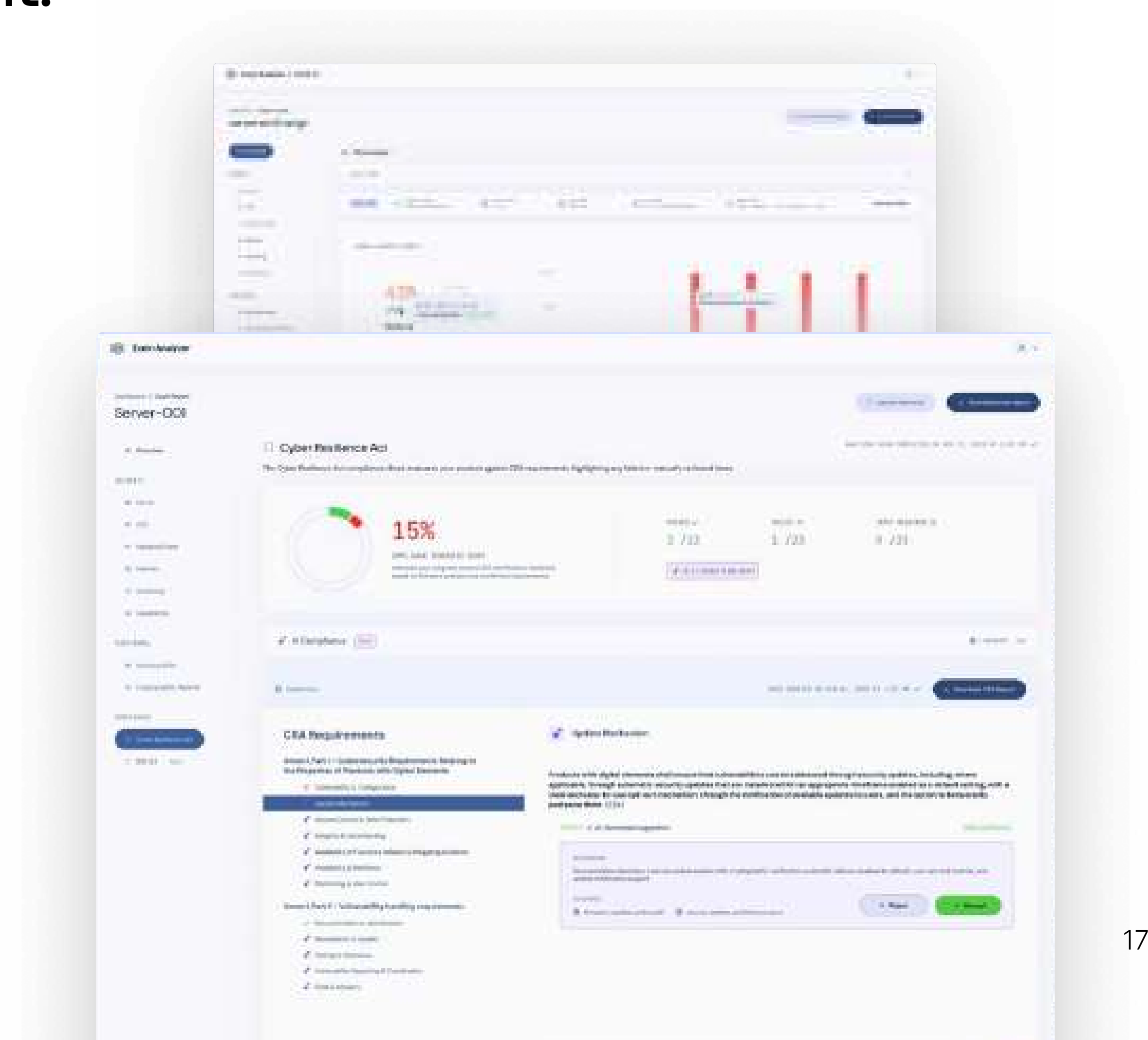
Analyzer

4.

EXEIN ANALYZER • OVERVIEW

Find what matters. Fix it automatically without leaving your build environment.

- ◆ **Know what you actually ship** with binary analysis of the final firmware, or direct SBOM ingestion when the binary isn't available. Catches what source-level tools cannot.
- ◆ **Prioritize CVE remediation** with reachability scoring and LLM-powered filtering surface what vulnerabilities are actually exploitable in your context.
- ◆ **Automated compliance preparedness** with AI analysis of documentation and binary scanning. Findings mapped to CRA requirements with remediation guidance.
- ◆ **Fix without leaving the build** with AI-driven remediation integrated into Yocto and CI/CD pipelines. No context switch, no separate tool.



EXEIN ANALYZER CAPABILITIES

Everything
you need
to ship secure
firmware

One platform for binary analysis, compliance, and remediation
— integrated into your existing build pipeline.

Binary & SBOM Analysis

Security Posture Assessment

AI-Driven Remediation

CVE Detection & Reachability

AI Compliance Mapping

Native Pipeline Integration

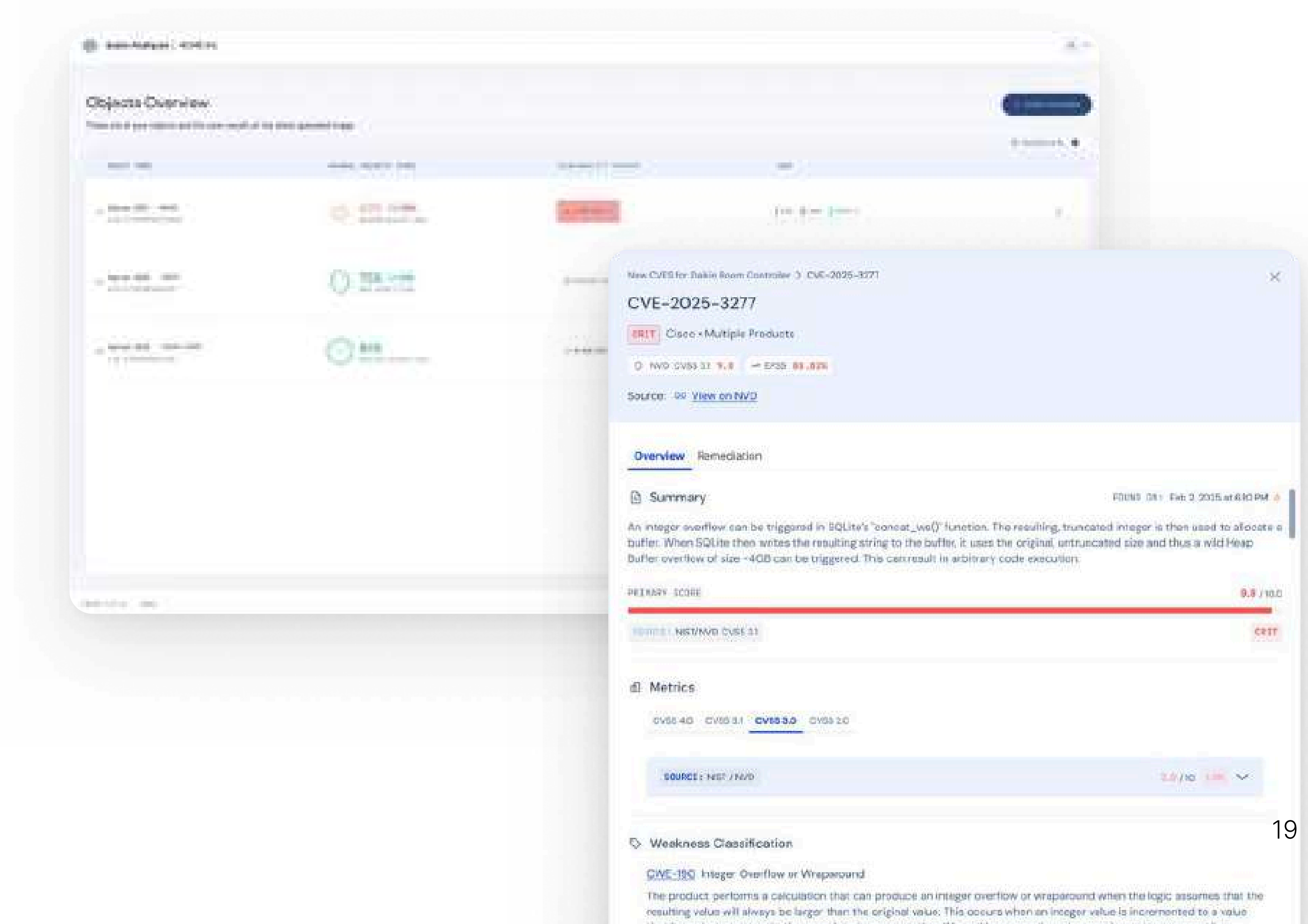


EXEIN ANALYZER • FEATURE DEEP DIVE

CVE monitoring that runs without you

Automatically scans for vulnerabilities and notifies you if new ones affect your firmware.

- ◆ **Automated vulnerability checks** using multi-source CVE intelligence aggregated from NVD, OSV/CNA, CISA KEV, EPSS, CWE, and patch availability data
- ◆ Automatically **prioritizes critical results** through reachability analysis, KEV exploitation signal, and EPSS likelihood scoring
- ◆ **Notification** for new vulnerabilities
- ◆ Creates traceability for audit in **compliance regulation**

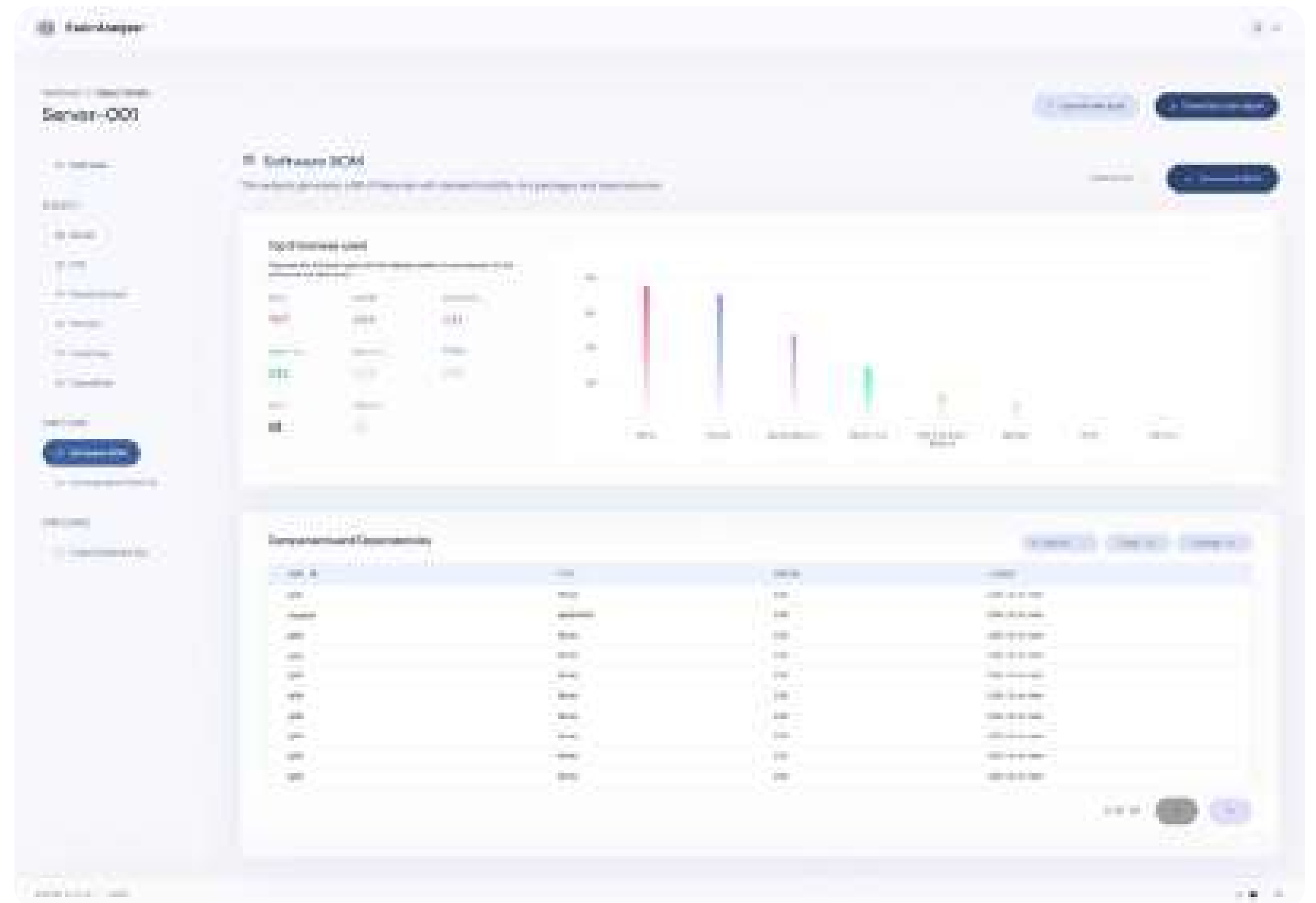


EXEIN ANALYZER • FEATURE DEEP DIVE

Discover what's in your firmware

Creates software bill of materials covering all dependencies in machine-readable formats required by regulators

- ◆ **Binary-derived SBOM** that catches vendored libraries, static linkage, and third-party drivers your build manifest misses
- ◆ Complete **dependency mapping** with version pinning, license attribution, and cryptographic material inventory
- ◆ Exports in **industry-standard formats** such as CycloneDX
- ◆ Helps satisfy **CRA Part II (f) documentation requirements**

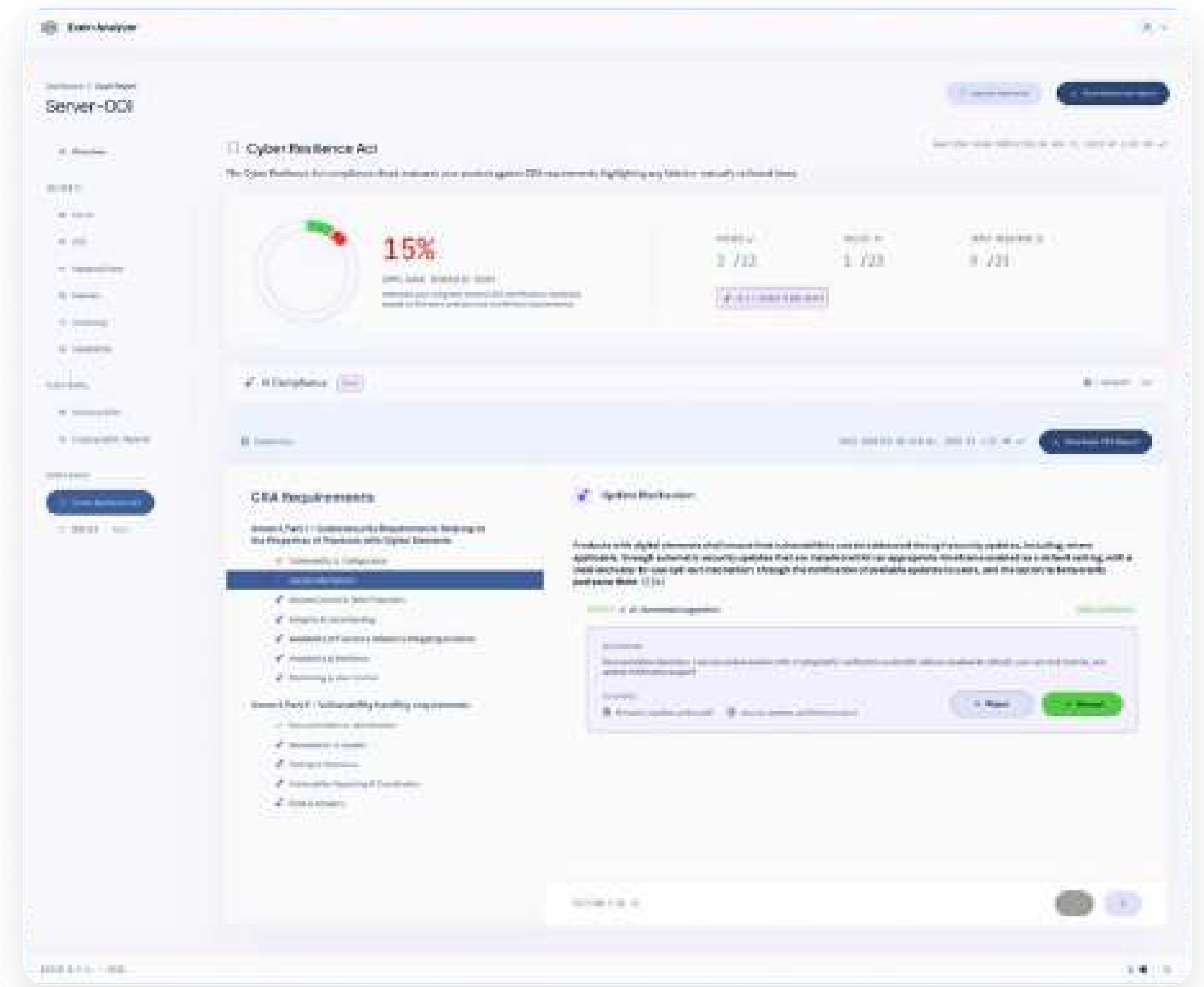


EXEIN ANALYZER • FEATURE DEEP DIVE

Easily prepare for CRA Compliance

Maps technical and governance evidence to CRA Part I and Part II requirements and provides remediation guidance.

- ◆ Ingests product documentation (PDF, DOCX, Markdown) and **highlights compliance gaps** with actionable **remediation guidance**
- ◆ **Provides pass/fail suggestions** using AI-powered analysis on documentation and firmware
- ◆ **Exportable reports** in audit-ready formats with page-level evidence citations



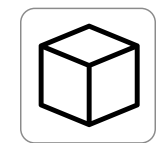
EXEIN ANALYZER • COVERAGE

Wide support across platforms and integrations

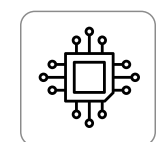
SUPPORTED ARTIFACT TYPES



Linux
any distribution, including:



Containers
Docker / OCI containers



Embedded SDKs

Zephyr SBOM  **Zephyr®**

FreeRTOS SBOM 



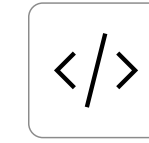
Mobile

Android 

BUILD & FLEET INTEGRATIONS



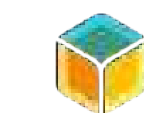
Yocto Project
Platinum partner, Security Metalayer



Build Systems
Buildroot, Docker CI/CD



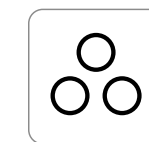
Fleet Platforms
Balena, AWS IoT
one-click fleet



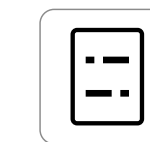
balena



aws



Custom Workflows
Native API for
custom pipelines



SBOM Workflows
SBOM upload
for pipelines without
firmware access

Deployment

Three deployment modes for different security and regulatory contexts.

ENTERPRISE

Cloud SaaS

Hosted by Exein. Fastest to onboard. Updates and CVE data pushed continuously.

REGULATED

On-prem Connected

Customer-hosted infrastructure. Outbound connection to Exein for CVE feeds and updates.

ISOLATED

On-prem: Air-gapped

Fully isolated deployment. Periodic snapshot-based updates for CVE and policy data.

Runtime

5.

EXEIN RUNTIME • OVERVIEW

Continuously monitor your fleet and infrastructure

- ◆ **Block before execution**
Threats are stopped before they run, not killed after they've started.
No detection-to-response window for the attack to exploit
- ◆ **Kernel-native protection** with the Linux Photon and Pulsar agents, which enforce at the BPF LSM hook in a single synchronous sequence
- ◆ **Automated and audit-ready incident reporting** to prepare for compliance regulatory requirements
- ◆ Agent blocks and prevents threats even in **low and no-connectivity environments** to ensure continuous protection



EXEIN RUNTIME • TECHNICAL CAPABILITIES

What you can protect

Out-of-the-box coverage for common physical AI and IoT threats

01.

FILE INTEGRITY

Prevent unauthorized writes to web server files, config directories, or firmware partitions.

02.

CONTAINER HARDENING

Scope rules to containers only — block escape tools like chroot, dmesg, and encoded payload delivery.

03.

NETWORK MONITORING

Monitor socket connections — detect Docker socket access, netcat usage or unexpected outbound traffic.

04.

CREDENTIALS PROTECTION

Block processes from reading TLS certificates, SSH keys, PAM configs, or application secrets.

05.

PROCESS CONTROL

Detect or block suspicious binaries, reverse-shell TTY upgrades, and unauthorized namespace creation.

06.

DEFENSE EVASION

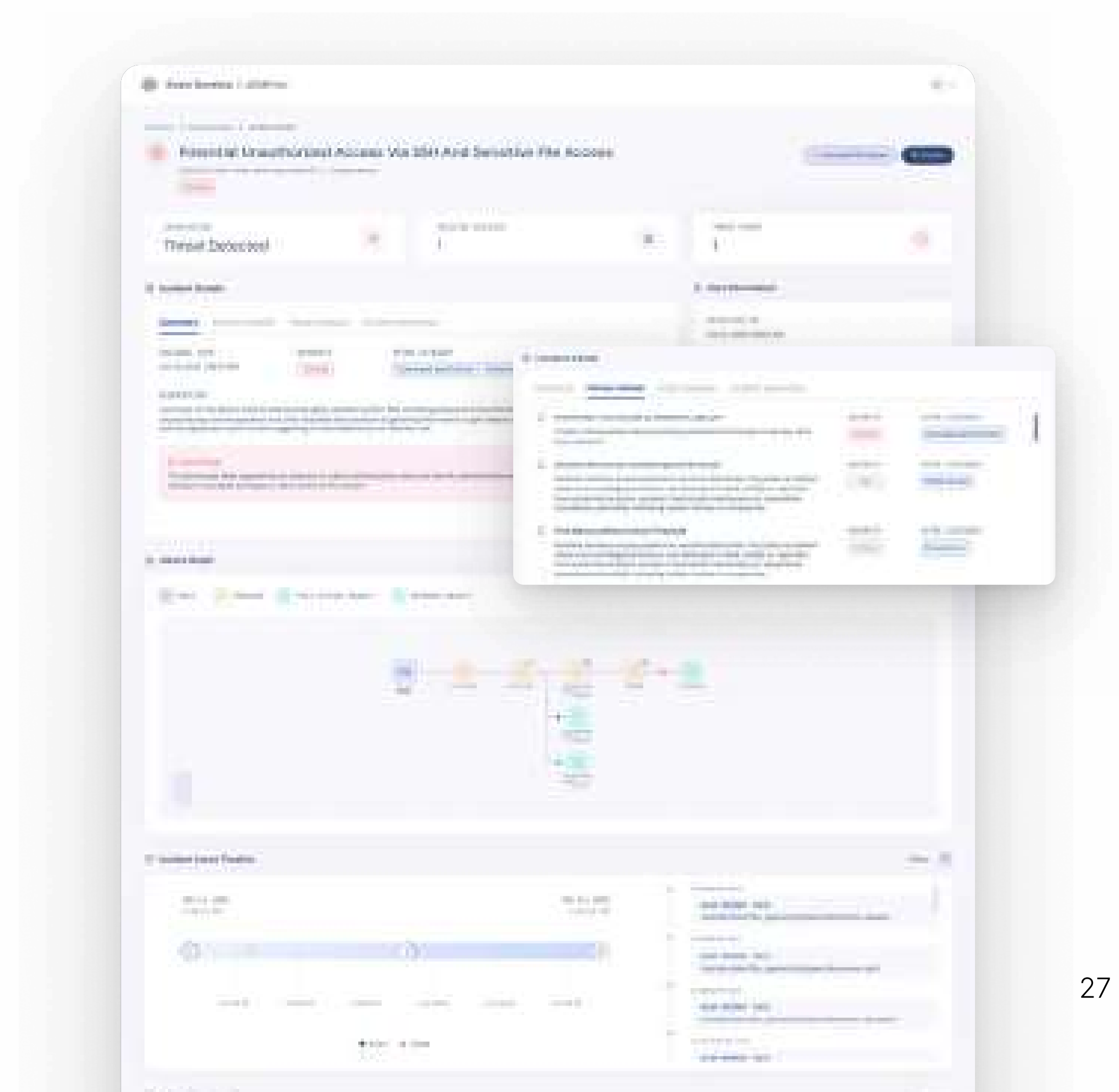
Prevent attackers from clearing logs, disabling firewalls, encoding payloads, or deleting shell history.

EXEIN RUNTIME • DEEP DIVE

Stop attacks before they execute

Block malicious behavior at the kernel level
the moment it tries to run — not after the damage is done.

- ◆ **Kernel-native enforcement** via eBPF LSM hooks, with sub-millisecond decision latency
- ◆ **Policy enforcement** blocks unauthorized syscalls, file access, and network connections before they execute
- ◆ **Easily customizable policies** written in human-readable language, to customize to your environment
- ◆ **Dynamic policy updates** push new rules to the entire fleet in seconds — no firmware updates, no reboots, no kernel rebuilds

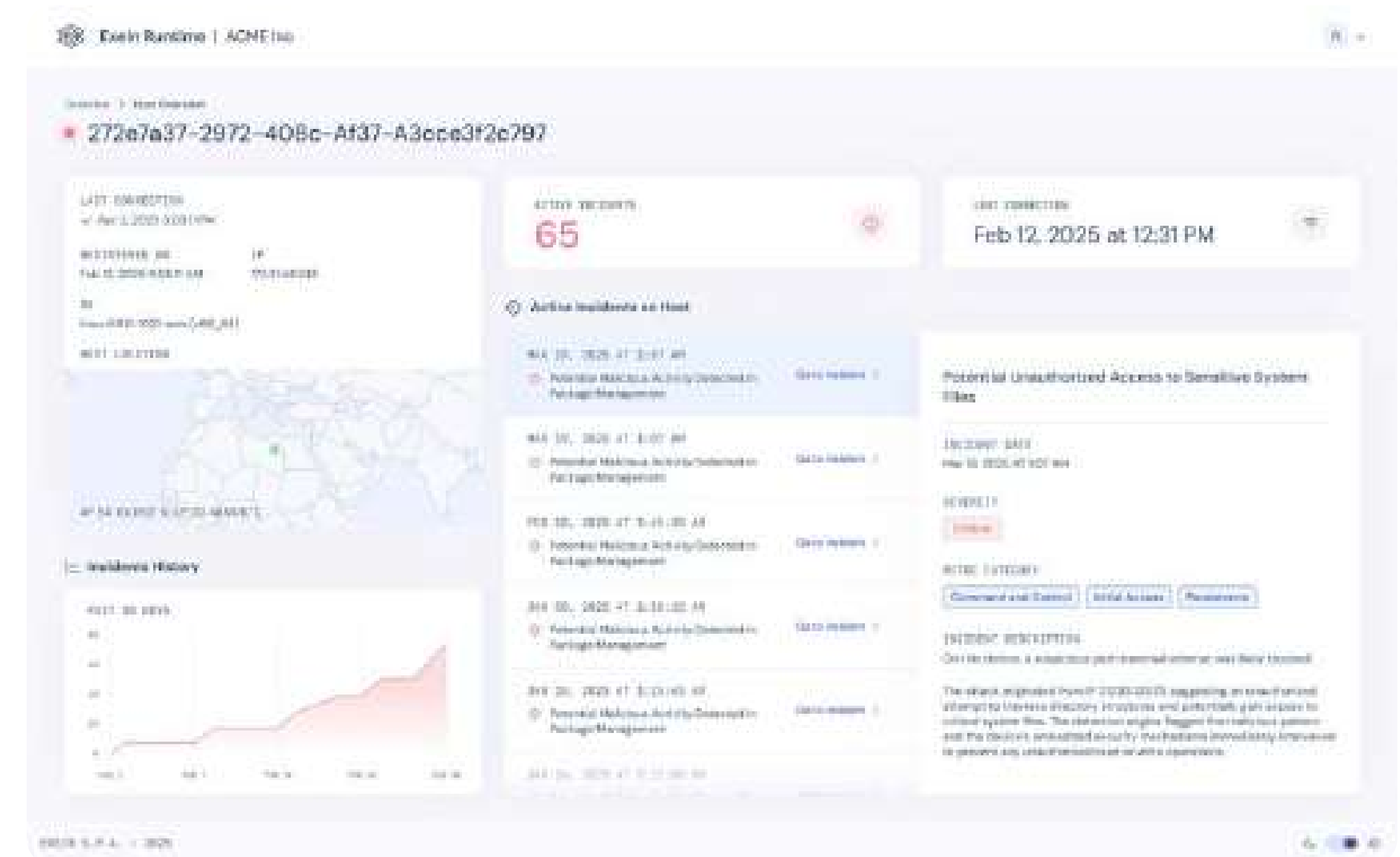


EXEIN RUNTIME • DEEP DIVE

Fleet-wide threat intelligence

Automatically monitor, block and trace incidents across your fleet, and quickly prioritize where to take action.

- ◆ **AI-powered incident analysis** provides play-by-play attack reconstruction and remediation guidance, accelerating triage and prioritization
- ◆ **Alert prioritization** using several key criteria, including severity, attack type, exploitability and fleet impact
- ◆ **Integrates with your SOC stack** (SIEM, SOAR) via APIs
- ◆ **Incident correlation** across devices, sites, and product lines surfaces coordinated attacks invisible to any single endpoint

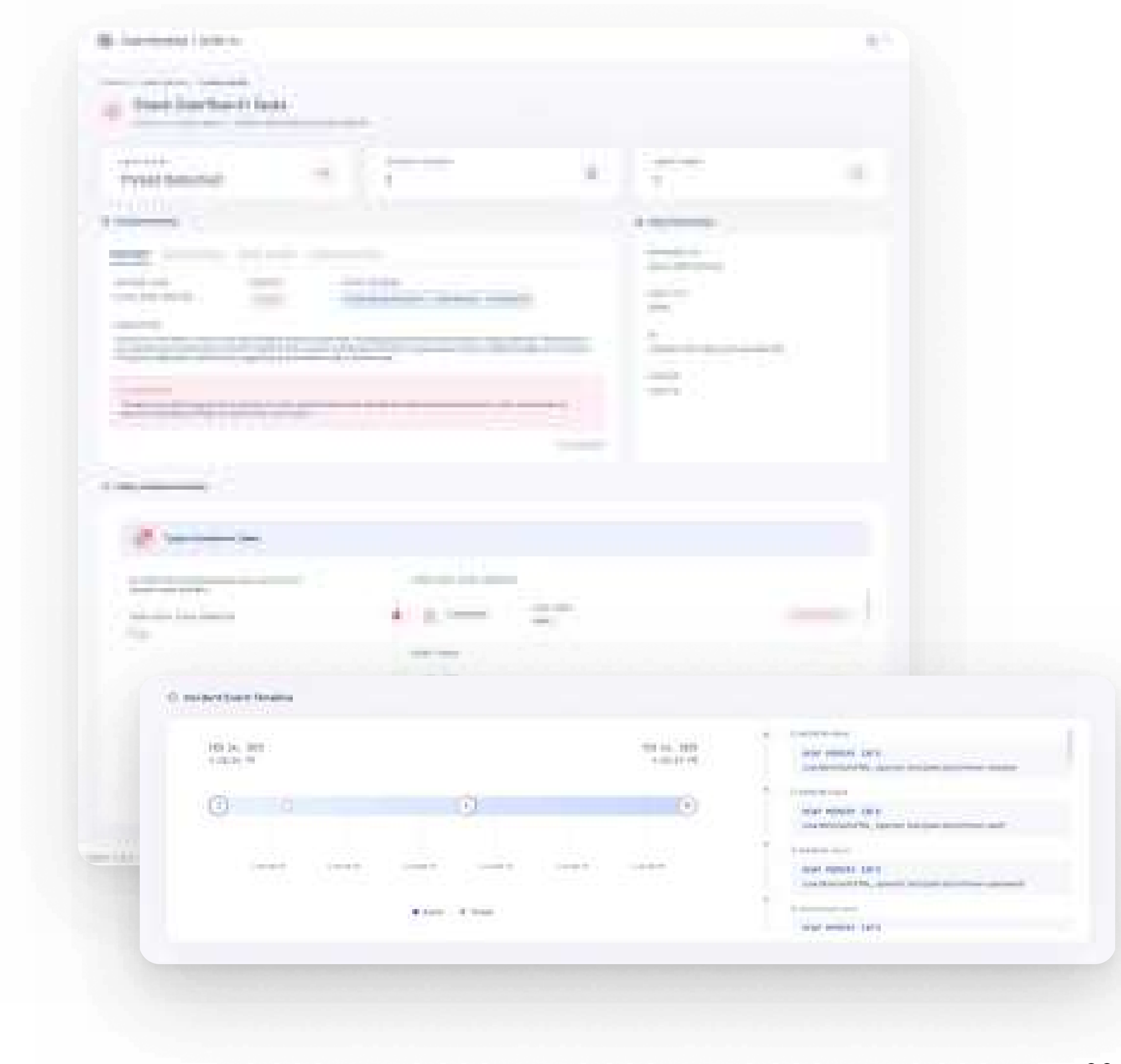


EXEIN RUNTIME • DEEP DIVE

Audit-ready incident evidence

Forensic reconstruction and compliance reporting generated automatically from runtime telemetry

- ◆ **Full event timeline per incident:** what ran, what tried to run, what was blocked, what touched what
- ◆ **Automated incident reporting** aligned with CRA Article 14 incident-reporting obligations
- ◆ Interactive attack graph **visualizes the full chain of events** leading to each incident — process spawns, file access, network connections
- ◆ **End-to-end device lifecycle coverage** by cross-referencing Runtime incidents with Analyzer findings to understand what was exploited



EXEIN RUNTIME • TECHNICAL CAPABILITIES

Wide platform support through our runtime agent family

Different runtimes need different enforcement strategies. All agents share the same platform and provide intuitive security policy models.

EXEIN AGENT	TARGET PLATFORM	TECHNOLOGY	REQUIREMENTS	ARCHITECTURES
LINUX PHOTON	MODERN LINUX	BPF LSM (KERNEL-NATIVE)	LINUX KERNEL ≥ 6.12	X86_64, AARCH64
LINUX PULSAR	STANDARD LINUX	EBPF	LINUX KERNEL ≥ 5.15	X86_64, AARCH64, RISCV64
LINUX LITE	LEGACY & CONSTRAINED LINUX	FANOTIFY + NETLINK	LINUX KERNEL ≥ 2.6.37	ARM32, X86, X86_64, AARCH64, RISCV64, POWERPC
IDF-ESP32	ESP32	NATIVE	XTENSA, RISCV32	ESP-IDF V5.2-V6.0.1
ZEPHYR	ZEPHYR RTOS	NATIVE	ZEPHYR-SUPPORTED BOARDS	ARM32, MIPS, RISCV32
FREERTOS	FREERTOS	NATIVE	FREERTOS-SUPPORTED MCUS	XTENSA, RISCV32



The next category of cybersecurity
is built **inside the device.**



VISIT US AT [EXEIN.IO](https://exein.io)

Rome

Piazzale Flaminio 19,
00196, Rome, Italy

San Francisco

535 Mission St 14th floor
94105, San Francisco, USA

Karlsruhe

Ludwig-Erhard-Allee 10
76131, Karlsruhe, Germany

Taipei

4F-2, No. 267, Lequn 2nd Rd., Zhongshan Dist.,
Taipei City 104, Taiwan (R.O.C.)