From Visibility to Defensible Action

A framework for operational control in cyber-physical systems. A unified platform for cloud-focused management, location-aware risk governance, OT cyber-physical control, and Industrial Cyber Risk Management. Built for operators, not dashboards.

Author: Ivan Ivanov CTO, CEO, Founder, Cyberbeam Inc.

CONTENTS

01 The Missing Layer Between Detection and Defensible Decisions
02 Why Detection Is No Longer Enough
03 Compliance Demands Governance Tooling
04 From Detection Eris to Governance Era
05 The OT Cyber Operations Control Plane
06 Operationalizing Industrial Cyber Risk
07 Four Scenarios That Change How You Respond
08 Location-Aware Asset Modeling
09 Built for Distributed Industrial Operations
10 The Commercial Case for Post-Discovery Governance
11 Secure Operations Require Governed Action
12 Sources and Further Reading

01 — The Missing Layer Between Detection and Defensible Decisions

Cyberbeam is a cloud-native platform for operational control across cloud, cyber-physical systems, industrial assets, facilities, and critical infrastructure. It ingests telemetry from sensors, OT systems, IoT devices, and operational workflows, correlates it against location, asset, and risk context, and turns it into actionable governance, response, and audit-ready evidence.

Cyberbeam's approach is based on a governance-centric architecture where operators can assign and monitor operational tasks, enforce policy-driven workflows, and maintain a continuous record of decisions, actions, and outcomes across distributed industrial environments.

Industrial adoption of IoT, OT, and cloud-connected systems has outpaced the maturity of cybersecurity governance. Most organizations can collect alerts and telemetry but cannot consistently prioritize risk, assign ownership, enforce response workflows, or prove what happened and why. Cyberbeam addresses this gap by treating every alert as a governance event that must be assigned, tracked, and closed with evidence.

Cyber-physical risk is increasingly material. Industrial control systems, building automation, and critical infrastructure are now connected to networks and remote operations. A single unmanaged alert can cascade into safety incidents, regulatory exposure, or operational disruption. Cyberbeam's architecture ties digital events to physical assets, locations, and operational impact.

Regulatory pressure is rising. NIS2, CRA, and sector-specific mandates require organizations to demonstrate risk management, incident response, and audit readiness. Cyberbeam's governance layer produces the evidence trail that compliance frameworks require: who saw what, who acted, what was done, and when.

Operational complexity is the real bottleneck. Security teams are overloaded with alerts but lack the tooling to assign, track, and close them with accountability. Cyberbeam's workflow engine ensures every alert has an owner, a deadline, and a closure condition.

Vendor lock-in is a structural risk. Proprietary platforms make it expensive to change tools or add new capabilities. Cyberbeam's open architecture and API-first design allow integration with existing systems and avoid dependency on any single vendor.

Cloud-native deployment enables faster iteration, lower infrastructure costs, and centralized governance across distributed sites. Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging.

AI-assisted operations are emerging but require governance. Cyberbeam's roadmap includes AI-assisted triage and anomaly detection, but all AI outputs are subject to human review and policy enforcement. The platform does not replace operators with black-box automation.

The ultimate objective is to move from detection to governed action. Cyberbeam's platform — the Cyber Operations Control Plane — provides the layer between raw telemetry and accountable response. It does not replace SIEM, EDR, or OT monitoring tools. It sits above them and adds the governance layer they do not provide.

88% of security teams report that their tools generate more alerts than they can manage. (Ponemon Institute, 2024)

52% of security alerts are never investigated or closed. (Ponemon Institute, 2024)

$500k+ average annual cost of a single unmanaged critical alert in industrial environments. (Industry estimates)

69 days average time to contain a breach when response is not governed. (IBM Cost of a Data Breach, 2024)

02 — Why Detection Is No Longer Enough

The IT security market has matured rapidly. Vendors automated triage, the Gartner Magic Quadrant for Cyber-Physical Systems Protection Platforms formalized the category, and AI-assisted SOC tools promised to reduce analyst workload. Yet most organizations still cannot answer the question that matters: who saw what, who acted, what was done, and when. Detection tools produce alerts. Governance tools produce accountability. Cyberbeam's architecture is a governance layer, not a detection engine.

MARKET SIGNAL — DETECTION IS MATURE

Gartner's Magic Quadrant for Cyber-Physical Systems Protection Platforms formalized the category. Vendors automated triage. The market moved from "can we see the threat" to "can we govern the response."

Detection answers the first question. Operations needs the next five.

- Who saw the alert?
- Who owned it?
- What was done?
- Was it closed with evidence?
- Can we prove it to an auditor?

FOCUS: GOVERNANCE OVERLAYS

Rules are operational logic — thresholds, time windows, and SOP-derived rules. **Alerts** are operational events — raw signals from sensors, OT systems, and IoT devices. **Tasks** are governance objects — assigned, tracked, and closed with evidence. Cyberbeam's workflow engine turns every alert into a governed task with ownership, deadline, and closure condition.

The latest SOAR stack is SOAR 2.0 (orchestration, low-code, AI-assisted SOAR) plus XDR (extended detection and response). Cyberbeam's architecture is compatible with both. It does not replace SIEM, EDR, or OT monitoring tools. It sits above them and adds the governance layer they do not provide.

SOAR 2.0 (Orchestration)
Automates response workflows. Connects security tools. Reduces manual work.

Governance Layer (Cyberbeam)
Assigns ownership. Tracks deadline. Enforces closure. Produces audit evidence.

XDR (Detection)
Correlates signals across domains. Reduces false positives. Improves detection quality.

Rules Engine (Cyberbeam)
Operational logic. Thresholds, time windows, SOP-derived rules.

MARKET SIGNAL — MATURITY ACCELERATES DEMAND

Gartner's Magic Quadrant for Cyber-Physical Systems Protection Platforms formalized the category. Vendors automated triage. The market moved from "can we see the threat" to "can we govern the response." Cyberbeam's architecture is a governance layer, not a detection engine.

03 — Compliance Demands Governance Tooling

A typical regulatory mandate can produce dozens of pages of requirements. Translating those requirements into operational controls, evidence, and audit-ready records is slow, manual, and error-prone. Cyberbeam's governance layer turns those requirements into assigned tasks, tracked deadlines, and closure evidence that can be presented to auditors.

EU CRA (Cyber Resilience Act)
Vulnerability handling, SBOM, secure by design, incident reporting. Applies to products with digital elements.

Manufacturers Serving EU Market
Must demonstrate compliance. Evidence must be produced on request.

NIS2 (EU Cybersecurity Directive)
Risk management, incident reporting, supply chain security. Applies to essential and important entities.

Organizations in Member States
Must implement and report. Penalties for non-compliance.

DORA (EU Digital Operational Resilience Act)
ICT risk management, incident reporting, third-party risk. Applies to financial entities.

Financial Institutions in EU
Must maintain operational resilience and report incidents to supervisors.

NIST CSF 2.0 / IEC 62443
Voluntary but widely referenced. Governance, risk management, supply chain security.

Organizations Seeking Alignment
Use as baseline for internal governance and customer assurance.

MATURITY GAP: EVIDENCE AUTOMATION

Regulations do not write themselves. Organizations need to translate each clause into a control, assign ownership, track deadline, and produce evidence on request. Cyberbeam's governance layer automates this translation. The Workflow Engine (SOP) enforces deadline tracking and closure conditions. The Audit Trail produces the evidence record. Manual compliance tracking does not scale. Governance tooling does. Cyberbeam's architecture is a governance layer, not a detection engine. It does not replace SIEM, EDR, or OT monitoring tools. It sits above them and adds the governance layer they do not provide.

04 — From Detection Era to Governance Era

OT cybersecurity is not a new problem. The Stuxnet incident in 2010 made it clear that cyber attacks can cause physical damage. The market responded with OT security vendors, SCADA monitoring tools, and network segmentation products. The problem was real. The market was small. Most organizations could not justify the spend. Regulation was absent. The threat was theoretical. Now the threat is operational, the market is growing, and the regulatory landscape is changing.

MARKET SIGNAL — OT SECURITY MARKET GROWTH

The global OT security market is projected to reach $18.7 billion by 2028, growing at a CAGR of 12.4% from 2023. Drivers: increased connectivity of industrial systems, regulatory mandates (NIS2, CRA), ransomware targeting OT environments, and supply chain risk. Source: MarketsandMarkets, Industrial Cybersecurity Market Report, 2023.

Three structural gaps define the transition:

Visibility — Most OT environments have limited asset inventory, network mapping, and real-time visibility. Many assets are legacy, undocumented, or connected to networks they were never designed for. Cyberbeam addresses this with asset inventory, network topology, and location-aware risk modeling.

Governance — Even when alerts are generated, there is no workflow to assign, track, and close them with accountability. Cyberbeam's Workflow Engine (SOP) enforces deadline tracking and closure conditions.

Evidence — Regulators increasingly require proof that risks were identified, assigned, and closed. Most tools produce alerts. None produce the audit trail that regulators require. Cyberbeam's Audit Trail produces the evidence record: who saw what, who acted, what was done, and when.

Three structural gaps define the transition

Visibility
Most OT environments have limited asset inventory, network mapping, and real-time visibility. Many assets are legacy, undocumented, or connected to networks they were never designed for. Cyberbeam addresses this with asset inventory, network topology, and location-aware risk modeling.

Governance
Even when alerts are generated, there is no workflow to assign, track, and close them with accountability. Cyberbeam's Workflow Engine (SOP) enforces deadline tracking and closure conditions.

Evidence
Regulators increasingly require proof that risks were identified, assigned, and closed. Most tools produce alerts. None produce the audit trail that regulators require. Cyberbeam's Audit Trail produces the evidence record: who saw what, who acted, what was done, and when.

MARKET SIGNAL — MATURITY ACCELERATES DEMAND

Gartner's Magic Quadrant for Cyber-Physical Systems Protection Platforms formalized the category. Vendors automated triage. The market moved from "can we see the threat" to "can we govern the response." Cyberbeam's architecture is a governance layer, not a detection engine.

05 — The OT Cyber Operations Control Plane

Cyberbeam's architecture is a governance layer that sits above existing monitoring tools, ingests telemetry from sensors, OT systems, IoT devices, and operational workflows, correlates it against asset, location, and risk context, and produces assigned tasks, tracked deadlines, and closure evidence. It does not replace SIEM, EDR, or OT monitoring tools. It sits above them and adds the governance layer they do not provide.

ARCHITECTURE: PLANES OF CONTROL

Data Plane
Ingestion, normalization, and storage of telemetry from sensors, OT systems, IoT devices, and operational workflows.

Control Plane
Rules engine, workflow engine, asset registry, and policy enforcement. Turns alerts into governed tasks with ownership and deadline.

Governance Layer
Assigns ownership. Tracks deadline. Enforces closure. Produces audit evidence.

Audit Trail
Immutable record of who saw what, who acted, what was done, and when. Evidence on request.

Operator Interface
Dashboards, alerts, and task queues for operators and supervisors.

Integration Layer
APIs and connectors for existing SIEM, EDR, OT monitoring, and ticketing systems.

Deployment Flexibility
Cloud, on-premise, or hybrid. Supports air-gapped environments.

Progressive adoption: start where you are.

Cyberbeam does not require a rip-and-replace deployment. It can start with read-only visibility and add governance capabilities as trust and maturity grow.

Tier 0 — Read-only: Ingest telemetry, build asset inventory, monitor. Value: Visibility. Risk: None.

Tier 1 — Assisted: Assign tasks, track deadlines, generate audit trails. Value: Governance. Risk: Low.

Tier 2 — Semi-autonomous: Auto-close low-risk tasks, escalate critical events, enforce policy. Value: Scale. Risk: Medium.

Tier 3 — Autonomous: Full automation with human oversight. Value: Operational efficiency. Risk: Requires maturity.

Tier 0 — Read-only
Ingest telemetry, build asset inventory, monitor. Value: Visibility. Risk: None.

Tier 1 — Assisted
Assign tasks, track deadlines, generate audit trails. Value: Governance. Risk: Low.

Tier 2 — Semi-autonomous
Auto-close low-risk tasks, escalate critical events, enforce policy. Value: Scale. Risk: Medium.

Tier 3 — Autonomous
Full automation with human oversight. Value: Operational efficiency. Risk: Requires maturity.

Governance Layer
Assigns ownership. Tracks deadline. Enforces closure. Produces audit evidence.

06 — Operationalizing Industrial Cyber Risk

Industrial cyber risk cannot be managed through alerts alone. Operational technology, industrial control systems, and critical infrastructure require governance that ties digital events to physical assets, locations, and operational impact. Cyberbeam's architecture supports this by correlating telemetry against asset, location, and risk context before generating tasks.

Industrial cyber risk spans operational technology, industrial control systems, building automation, and critical infrastructure. Most organizations can collect alerts but cannot consistently prioritize risk, assign ownership, or prove what happened and why. Cyberbeam addresses this by treating every alert as a governance event that must be assigned, tracked, and closed with evidence.

Asset inventory is the foundation. Without a complete inventory of assets, their locations, their risk ratings, and their operational dependencies, alerts cannot be prioritized meaningfully. Cyberbeam's asset registry and location-aware risk model provide this context.

Location-aware risk matters because a single alert in a critical facility is not the same as a single alert in a low-risk warehouse. Cyberbeam's risk model weights alerts by asset criticality, location, and operational impact before generating tasks.

Regulatory pressure is rising. NIS2, CRA, and sector-specific mandates require organizations to demonstrate risk management, incident response, and audit readiness. Cyberbeam's governance layer produces the evidence trail that compliance frameworks require.

Operational complexity is the real bottleneck. Security teams are overloaded with alerts but lack the tooling to assign, track, and close them with accountability. Cyberbeam's workflow engine ensures every alert has an owner, a deadline, and a closure condition.

Vendor lock-in is a structural risk. Proprietary platforms make it expensive to change tools or add new capabilities. Cyberbeam's open architecture and API-first design allow integration with existing systems and avoid dependency on any single vendor.

Cloud-native deployment enables faster iteration, lower infrastructure costs, and centralized governance across distributed sites. Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging.

AI-assisted operations are emerging but require governance. Cyberbeam's roadmap includes AI-assisted triage and anomaly detection, but all AI outputs are subject to human review and policy enforcement. The platform does not replace operators with black-box automation.

07 — Four Scenarios That Change How You Respond

Cyberbeam's architecture supports four operational scenarios, each with different risk profiles and governance requirements. Each scenario produces a different governance outcome, but the underlying architecture remains the same: ingest telemetry, correlate against asset and location context, assign tasks, track deadlines, and produce audit evidence.

SCENARIO — OT CYBER OPERATIONS CONTROL PLANE

Critical Infrastructure — Water treatment, power generation, manufacturing. Alerts affect physical assets and safety systems. Governance ensures every alert is assigned, tracked, and closed with evidence. **Risk Profile:** Safety, regulatory, operational continuity. **Governance Outcome:** Every alert has an owner, a deadline, and a closure condition. **Key Metric:** Mean time to assign, mean time to close, percentage of alerts with evidence.

SCENARIO — CLOUD-NATIVE MONITORING WITH OT CONNECTIVITY

Distributed Operations — Multi-site industrial operations with remote monitoring requirements. Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging. **Risk Profile:** Data sovereignty, cross-jurisdiction compliance, remote access governance. **Governance Outcome:** Centralized visibility with distributed enforcement. **Key Metric:** Cross-site response time, policy compliance across sites.

SCENARIO — TECHNICAL MANAGER MONITORING FOR THEFT OR MISUSE

Asset Protection — Equipment theft, unauthorized access, or misuse in remote locations. Alerts require investigation and evidence for insurance or law enforcement. **Risk Profile:** Asset loss, liability, insurance claims. **Governance Outcome:** Every incident has a timestamped record of who saw it, who acted, what was done. **Key Metric:** Time to evidence, percentage of incidents with complete audit trail.

SCENARIO — CYBER RESILIENCE REPORTING FOR BOARDS AND REGULATORS

Governance Reporting — Boards and regulators require evidence that risks were identified, assigned, and closed. Most tools produce alerts. None produce the audit trail that regulators require. **Risk Profile:** Regulatory penalties, board liability, reputational damage. **Governance Outcome:** Audit-ready evidence on demand. **Key Metric:** Time to produce evidence, percentage of incidents with complete audit trail.

08 — Location-Aware Asset Modeling

Not all alerts are equal. A single alert in a critical facility is not the same as a single alert in a low-risk warehouse. Cyberbeam's risk model weights alerts by asset criticality, location, and operational impact before generating tasks. This ensures that the highest-risk events get the fastest response and the most governance attention.

ARCHITECTURE: ASSET REGISTRY

A centrally maintained registry of assets, their locations, their risk ratings, and their operational dependencies. Cyberbeam's asset registry and location-aware risk model provide this context. Without it, alerts cannot be prioritized meaningfully.

```
Asset: Compressor-07
  Location: Facility B, Zone 3
  Criticality: Critical (safety, regulatory)
  Operational Dependencies: [Pump-12, Valve-04]
  Last Inspection: 2024-11-15
  Risk Rating: High (vibration anomaly, aging equipment)
  Owner: Maintenance Team
  Escalation: Plant Manager, Safety Officer
```

Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging. Each site can have its own asset registry, risk model, and escalation rules, while the governance layer remains centralized. This allows distributed operations to maintain local context while preserving centralized visibility and audit trails.

ARCHITECTURE: MULTI-SITE GOVERNANCE

Each site can have its own asset registry, risk model, and escalation rules, while the governance layer remains centralized. This allows distributed operations to maintain local context while preserving centralized visibility and audit trails.

09 — Built for Distributed Industrial Operations

Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging. Each site can have its own asset registry, risk model, and escalation rules, while the governance layer remains centralized. This allows distributed operations to maintain local context while preserving centralized visibility and audit trails.

Distributed Operations
Multi-site industrial operations with remote monitoring requirements. Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging. **Risk Profile:** Data sovereignty, cross-jurisdiction compliance, remote access governance. **Governance Outcome:** Centralized visibility with distributed enforcement. **Key Metric:** Cross-site response time, policy compliance across sites.

Remote Monitoring
Equipment theft, unauthorized access, or misuse in remote locations. Alerts require investigation and evidence for insurance or law enforcement. **Risk Profile:** Asset loss, liability, insurance claims. **Governance Outcome:** Every incident has a timestamped record of who saw it, who acted, what was done. **Key Metric:** Time to evidence, percentage of incidents with complete audit trail.

Governance Reporting
Boards and regulators require evidence that risks were identified, assigned, and closed. Most tools produce alerts. None produce the audit trail that regulators require. **Risk Profile:** Regulatory penalties, board liability, reputational damage. **Governance Outcome:** Audit-ready evidence on demand. **Key Metric:** Time to produce evidence, percentage of incidents with complete audit trail.

SCADA and Industrial Systems

Cyberbeam's architecture is designed for distributed industrial operations and critical infrastructure. Its role-based access, audit logging, and multi-site governance support the operational requirements of SCADA and industrial control systems. The Workflow Engine (SOP) enforces deadline tracking and closure conditions across distributed sites. The Audit Trail produces the evidence record regardless of which site the alert originated from. Cyberbeam is not a SCADA replacement. It is a governance layer that sits above existing SCADA systems.

Scadahound Vision: the right platform for the organ's reality.

Scadahound's vision is the right platform for the organ's reality: a governance layer that sits above existing SCADA systems, ingests telemetry from distributed industrial assets, and produces governed tasks with ownership, deadlines, and closure evidence. Cyberbeam's architecture is designed to support this model: role-based access for distributed operators, audit logging for regulatory compliance, and a workflow engine that enforces deadline tracking across multi-site operations.

10 — The Commercial Case for Post-Discovery Governance

Cyberbeam's GTM strategy is not to compete with security tools. It is to sell the governance layer that sits above them. The buyer is not the security team. The buyer is the operations manager, the compliance officer, or the technical manager who needs to know who saw what, who acted, what was done, and when.

Regulatory compliance is the strongest wedge. NIS2, CRA, and sector-specific mandates require organizations to demonstrate risk management, incident response, and audit readiness. Cyberbeam's governance layer produces the evidence trail that compliance frameworks require.

Operational complexity is the second wedge. Security teams are overloaded with alerts but lack the tooling to assign, track, and close them with accountability. Cyberbeam's workflow engine ensures every alert has an owner, a deadline, and a closure condition.

Vendor lock-in is a structural risk. Proprietary platforms make it expensive to change tools or add new capabilities. Cyberbeam's open architecture and API-first design allow integration with existing systems and avoid dependency on any single vendor.

Cloud-native deployment enables faster iteration, lower infrastructure costs, and centralized governance across distributed sites. Cyberbeam's architecture supports multi-site, multi-tenant operations with role-based access and audit logging.

AI-assisted operations are emerging but require governance. Cyberbeam's roadmap includes AI-assisted triage and anomaly detection, but all AI outputs are subject to human review and policy enforcement. The platform does not replace operators with black-box automation.

11 — Secure Operations Require Governed Action

The goal of this framework is not to replace security tools. It is to add the governance layer that sits above them. Cyberbeam's architecture ingests telemetry from sensors, OT systems, IoT devices, and operational workflows, correlates it against asset, location, and risk context, assigns tasks, tracks deadlines, and produces audit evidence.

Cyberbeam's role is to make the operational layer governable. It does not replace SIEM, EDR, or OT monitoring tools. It sits above them and adds the governance layer they do not provide. The platform does not make decisions for operators. It makes decisions governable: who saw what, who acted, what was done, and when.

Cyberbeam's architecture is designed for distributed industrial operations, critical infrastructure, and multi-site governance. The platform supports role-based access, audit logging, and multi-site governance. The Workflow Engine (SOP) enforces deadline tracking and closure conditions across distributed sites. The Audit Trail produces the evidence record regardless of which site the alert originated from.

Governed action means that every alert has an owner, a deadline, and a closure condition. Cyberbeam's workflow engine enforces this across distributed sites. The Audit Trail produces the evidence record: who saw what, who acted, what was done, and when.

Evidence is the output that regulators require. Most tools produce alerts. None produce the audit trail that regulators require. Cyberbeam's Audit Trail produces the evidence record: who saw what, who acted, what was done, and when.

Governance is the layer that makes operational decisions governable. Cyberbeam's architecture is designed to support this layer: role-based access for distributed operators, audit logging for regulatory compliance, and a workflow engine that enforces deadline tracking across multi-site operations.

Governed action means that every alert has an owner, a deadline, and a closure condition. Cyberbeam's workflow engine enforces this across distributed sites. The Audit Trail produces the evidence record: who saw what, who acted, what was done, and when.

Evidence is the output that regulators require. Most tools produce alerts. None produce the audit trail that regulators require. Cyberbeam's Audit Trail produces the evidence record: who saw what, who acted, what was done, and when.

Governance is the layer that makes operational decisions governable. Cyberbeam's architecture is designed to support this layer: role-based access for distributed operators, audit logging for regulatory compliance, and a workflow engine that enforces deadline tracking across multi-site operations.

12 — Sources and Further Reading

Gartner, Magic Quadrant for Cyber-Physical Systems Protection Platforms, 2024.
MarketsandMarkets, Industrial Cybersecurity Market Report, 2023.
IBM, Cost of a Data Breach Report, 2024.
Ponemon Institute, The State of Security Operations, 2024.
ENISA, Cybersecurity Risk Management Measures under NIS2, 2024.
European Commission, Cyber Resilience Act (CRA), 2024.
Scadahound, Industrial Cybersecurity Governance Framework, 2024.
Cyberbeam, Technical Architecture Documentation, 2024.
Cyberbeam, Technical Architecture Documentation, 2024.
Cyberbeam, Technical Architecture Documentation