COMPLETE SPECIFICATION

TITLE OF THE INVENTION: A SYSTEM AND METHOD FOR AUTHORITY-SEPARATED CYBERSECURITY ENFORCEMENT

FIELD OF THE INVENTION

The present invention relates to cybersecurity systems and methods, and more particularly to a distributed computer-implemented system that enforces strict separation between data collection, intelligence analysis, and enforcement authorization in order to prevent unsafe, unauthorized, or ambiguous security response actions.

BACKGROUND OF THE INVENTION

Conventional cybersecurity platforms frequently permit endpoint agents, network sensors, or analytical systems to independently decide and execute security response actions. Such designs often combine detection, analysis, and enforcement within the same component or execution path.

These approaches may result in false enforcement, uncontrolled privilege escalation, service disruption, and difficulty in auditing or reproducing security decisions. In particular, systems that permit artificial intelligence or probabilistic logic to directly influence enforcement behavior may act unpredictably under conditions of incomplete data, conflicting signals, or adversarial manipulation.

Additionally, many existing systems fail open under ambiguity, relying on best-effort logic rather than deterministic refusal of action. This creates operational and regulatory risks in enterprise and critical environments.

Accordingly, there exists a need for a cybersecurity system that strictly controls enforcement authority, prevents intelligence components from executing or authorizing actions, and ensures deterministic, verifiable, and auditable enforcement behavior.

SUMMARY OF THE INVENTION

The present invention provides a cybersecurity system in which enforcement authority is strictly separated from data collection and intelligence analysis.

The system comprises one or more data-collection components configured to collect security telemetry, a deterministic control component configured to authorize enforcement actions, and one or more intelligence components configured to analyze validated data and generate advisory outputs.

Enforcement actions are permitted solely through the deterministic control component after cryptographic verification of inputs, policies, execution scope, and validity conditions. Intelligence components, including artificial intelligence and machine learning modules, are cryptographically and architecturally restricted from initiating, approving, or executing enforcement actions.

The system enforces fail-closed behavior such that enforcement is refused in the presence of ambiguity, missing verification, conflicting conditions, or unauthorized requests. Refusal of enforcement is treated as a valid and auditable outcome.

DEFINITIONS AND INTERPRETATION

For the purposes of this specification, the following terms shall have the meanings set forth below unless the context clearly indicates otherwise:

- **"Data-collection component"** refers to any software or hardware element configured to collect security-related telemetry, including endpoint agents, network sensors, or monitoring probes, without authority to authorize or execute enforcement actions.
- **"Control component"** refers to a deterministic system element configured to evaluate verified inputs against signed policies and to authorize enforcement actions.
- **"Intelligence component"** refers to any analytical, heuristic, artificial intelligence, or machine learning system configured to analyze validated data and generate advisory outputs without enforcement authority.
- **"Enforcement action"** refers to any operation that modifies system state, access control, process execution, network behavior, or resource availability.
- **"Cryptographically restricted"** refers to technical enforcement using cryptographic verification and runtime checks such that unauthorized components are incapable of initiating, approving, or executing enforcement actions.

BRIEF DESCRIPTION OF THE DRAWINGS

- **FIG. 1** illustrates a high-level system architecture showing separation between data collection components, a control component, and intelligence components.

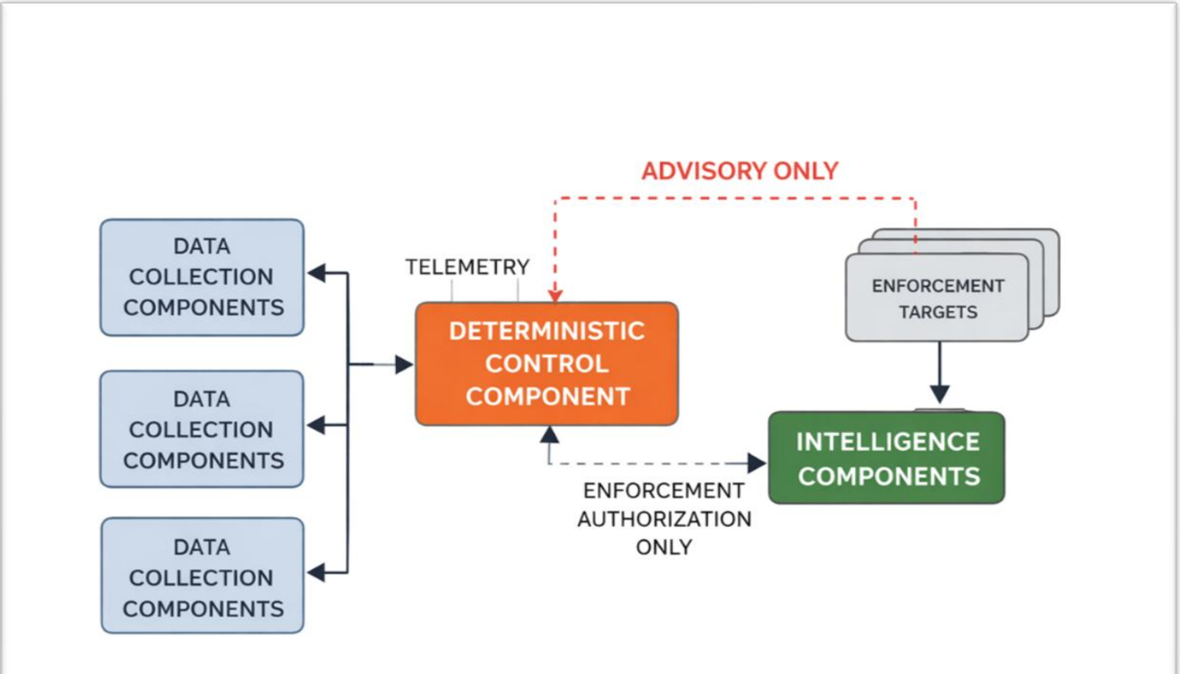
ADVISORY ONLY
DATA COLLECTION COMPONENTS
TELEMETRY
ENFORCEMENT TARGETS
DETERMINISTIC CONTROL COMPONENT
DATA COLLECTION COMPONENTS
INTELLIGENCE COMPONENTS
ENFORCEMENT AUTHORIZATION ONLY
DATA COLLECTION COMPONENTS

Fig. 1: System Architecture

- **FIG. 2** illustrates an enforcement authorization flow through the deterministic control component.

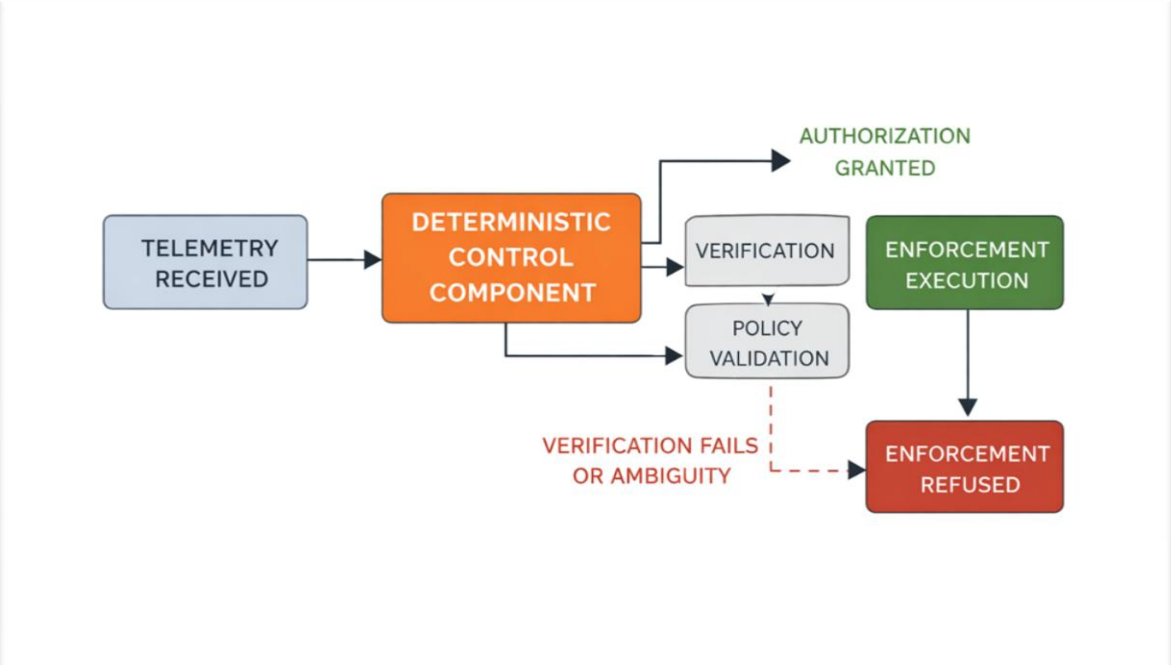

Fig. 2: Enforcement Authorization Flow

- **FIG. 3** illustrates restricted advisory output from intelligence components without enforcement authority.

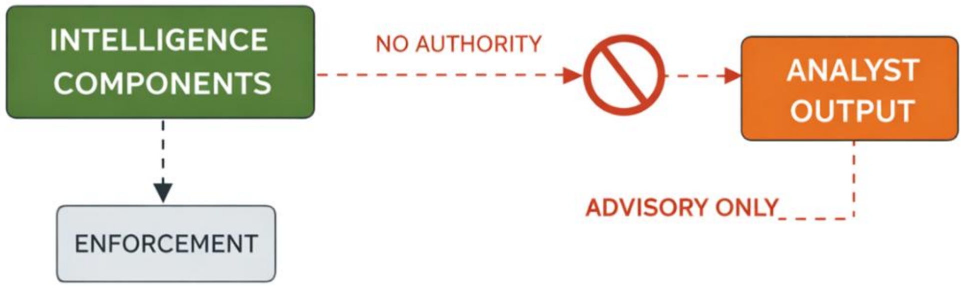

Fig. 3: Restricted Intelligence Output Without Enforcement Authority

DETAILED DESCRIPTION OF THE INVENTION

System Architecture

In one embodiment, the system comprises a plurality of data-collection components configured to collect security telemetry from computing environments. The data-collection components are intentionally classified as untrusted and are prohibited from initiating, approving, or executing enforcement actions.

A control component is provided that evaluates verified inputs against cryptographically signed policies. The control component is the sole entity within the system authorized to approve enforcement actions.

One or more intelligence components analyze validated telemetry to generate advisory outputs such as analytical summaries, confidence indicators, or explanatory information. Intelligence components are isolated from enforcement execution paths and do not possess authority to modify system state.

Authority Separation and Role Enforcement

Authority separation is strictly enforced at runtime. Data-collection components and intelligence components are prohibited from issuing commands that result in enforcement actions.

Only the control component possesses enforcement authorization capability. This capability is enforced through cryptographic verification, explicit role validation, and runtime checks.

Any attempt by a non-authorized component to initiate or influence enforcement results in rejection of the action and generation of an auditable event

Deterministic Enforcement and Fail-Closed Behavior

The control component operates deterministically such that identical verified inputs produce identical enforcement authorization outcomes.

Enforcement authorization is refused by default unless all required verification conditions are satisfied. Verification conditions include policy authenticity, execution scope validity, temporal validity, and absence of conflicting conditions.

In cases of ambiguity, conflicting policy evaluation, missing verification, or expired authorization, the system enters a fail-closed state in which no enforcement action is executed.

Refusal of enforcement is treated as a valid system outcome and is recorded for audit purposes.

Intelligence Component Restriction

Intelligence components operate strictly in an advisory capacity. Outputs generated by intelligence components do not initiate, approve, or trigger enforcement actions.

The control component does not rely on probabilistic or learning-based outputs for enforcement authorization. Intelligence outputs may be presented to human operators or recorded for analysis, but they do not modify system state.

Any attempt by an intelligence component to influence enforcement execution directly or indirectly is rejected.

ADVANTAGES OF THE INVENTION

The invention prevents unsafe automated enforcement, reduces false response actions, improves auditability, and enables predictable and regulatory-compliant cybersecurity operation by enforcing strict authority separation and deterministic enforcement behavior.

CLAIMS

Claim 1 (Independent – Core System Claim)

A cybersecurity system comprising:
one or more data-collection components configured to collect security telemetry from one or more computing environments; a deterministic control component configured to evaluate verified inputs against cryptographically signed policies and to authorize enforcement actions; and one or more intelligence components configured to analyze validated data and generate advisory outputs, **wherein** the intelligence components are cryptographically and architecturally restricted from authorizing, initiating, modifying, or executing enforcement actions, and **wherein** enforcement actions are executed solely upon explicit authorization by the deterministic control component.

Claim 2 (Untrusted Data Plane – Explicit)

The system of claim 1, **wherein** the data-collection components are explicitly classified as untrusted inputs and are technically prevented from issuing commands, signals, or instructions that result in enforcement actions.

Claim 3 (AI Explicitly Included and Restricted)

The system of claim 1, **wherein** the intelligence components comprise artificial intelligence models, machine learning models, heuristic engines, or analytical logic, **and wherein** such intelligence components operate exclusively in a non-authoritative, advisory capacity.

Claim 4 (Explicit Prohibition of AI-Driven Enforcement)

The system of claim 3, **wherein** outputs generated by the intelligence components are incapable of directly or indirectly triggering enforcement actions, including through thresholds, confidence scores, or automated decision rules.

Claim 5 (Cryptographic Enforcement Restriction)

The system of claim 1, **wherein** cryptographic verification is required to validate the origin, authenticity, and authorization scope of any enforcement request prior to execution.

Claim 6 (Fail-Closed Default Behaviour)

The system of claim 1, **wherein** enforcement authorization is refused by default unless all verification conditions are satisfied.

Claim 7 (Ambiguity Handling – Explicit)

The system of claim 1, **wherein** enforcement authorization is denied upon detection of ambiguous telemetry, incomplete input data, conflicting policy conditions, or unverifiable authorization.

Claim 8 (Deterministic Behaviour Lock)

The system of claim 1, **wherein** the deterministic control component produces identical enforcement authorization outcomes for identical verified inputs.

Claim 9 (Explicit Rejection of Probabilistic Enforcement)

The system of claim 1, **wherein** the control component authorizes enforcement actions independently of probabilistic, learning-based, or adaptive decision logic.

Claim 10 (Enforcement Scope Limitation)

The system of claim 1, **wherein** enforcement actions are authorized with an explicitly defined execution scope, duration, and validity period.

Claim 11 (Unauthorized Attempt Handling)

The system of claim 1, **wherein** any attempt by a non-authorized component to initiate or influence enforcement results in rejection of the attempt.

Claim 12 (Audit Requirement)

The system of claim 1, **wherein** enforcement authorization, refusal, or rejection events are recorded as auditable records.

Claim 13 (Isolation of Intelligence Components)

The system of claim 1, **wherein** intelligence components are isolated from enforcement execution paths such that intelligence outputs cannot modify system state.

Claim 14 (Policy Authenticity Requirement)

The system of claim 1, **wherein** enforcement authorization requires verification of policy authenticity prior to execution.

Claim 15 (Conflict Resolution Rule)

The system of claim 1, **wherein** detection of conflicting policy conditions results in denial of enforcement authorization.

Claim 16 (Reversibility Requirement)

The system of claim 1, **wherein** enforcement actions are authorized only if reversible execution conditions are satisfied.

Claim 17 (Human Advisory Path Only)

The system of claim 1, **wherein** intelligence outputs are communicated exclusively through advisory channels to human operators or supervisory systems.

Claim 18 (System State Protection)

The system of claim 1, **wherein** intelligence components are prohibited from modifying system state, access control state, process execution state, or network behavior.

Claim 19 (Explicit Denial on Verification Failure)

The system of claim 1, **wherein** failure of cryptographic verification results in refusal of enforcement authorization.

Claim 20 (Exclusive Authority Claim – Anchor)

The system of claim 1, **wherein** enforcement authority is limited exclusively to the deterministic control component.

ABSTRACT

A cybersecurity system is disclosed in which enforcement authority is strictly separated from data collection and intelligence analysis. The system includes untrusted data-collection components, a deterministic control component that authorizes enforcement actions, and intelligence components that generate advisory outputs without enforcement authority. Enforcement actions are executed only after cryptographic verification and are refused in the presence of ambiguity or verification failure, thereby improving safety, predictability, and auditability.