

More than XDR. Built as a command platform.

ARMADA connects telemetry, XDR analytics, governed AI, response workflows, vulnerability intelligence and verified evidence into one operational platform for cyber operations.

A complete command platform for cyber operations - built for today's threats and tomorrow's scale.



GLOBAL VISIBILITY.
SMARTER OPERATIONS.
A SAFER TOMORROW.



TELEMETRY

Secure collection + normalization



DETECTION

Rules + correlation



RESPONSE

Incidents + governed actions



GOVERNANCE

Identity + policy + evidence

What ARMADA delivers



Unified operational picture

Topology, platform status, alerts and tenant-bound evidence in one view.



Incident and case workflows

Manage incidents and cases through process, evidence and audit trail.



Governed AI-assisted operations

AI Command for analysis and recommendations, with policy controls, human approval and audited actions.



Threat detection and correlation

Behavior, correlation and prioritization for focused alerting.



Vulnerability visibility

Track application and infrastructure exposure and safely scan approved targets.



Security and access control

OIDC/PKCE authentication, RBAC/OPA authorization and tenant-aware controls.

VALUE FOR ORGANIZATIONS



Faster detection and response to threats



Single view of security posture and risk



Standardized processes and efficiency metrics



Better control, evidence and compliance



Scalable and ready to grow with the organization

Eight modules. One operational picture.

01



ALERTS

View, filter and prioritize security events.

02



SYSTEM

Platform health, services, resources and status.

03



INCIDENTS

Correlate events and manage incidents through a clear process.

04



AI COMMAND

Assisted analysis, recommendations and governed actions.

05



CASES

Notes, tasks, evidence and complete investigation trail.

06



THREAT INTEL

Threat intelligence and indicators of compromise.

07



VULNERABILITIES

Track exposure and safely scan approved targets.

08



REPORTING

Reports, evidence and compliance outputs.



SECURE DATA COLLECTION

Collectors + Evidence Nodes securely ingest, verify and normalize tenant-bound evidence (OCSE).

Technology foundation



IDENTITY & ACCESS

Keycloak / OIDC/PKCE / RBAC/OPA / MFA-capable security



SERVICES

Microservices for detection, ingest, correlation, risk, SOAR, TI, UEBA



DATA

PostgreSQL / Kafka / OpenSearch / Redis / Longhorn persistence



OBSERVABILITY

Prometheus / Grafana / Alertmanager / Fluent Bit / OpenSearch



INFRASTRUCTURE

RKE2 Kubernetes / Helm / TLS/HTTPS / scalable deployment foundation

Data and response flow

1



Collect telemetry & evidence

2



Verify, normalize and enrich

3



Detect and correlate

4



Alerts and priorities

5



Incidents and governed actions

6



Cases and evidence

7



Reports and improvement