Powered By
ATOMNIA
Connection Protection Detection

**OMNIA CYBER COMMAND PLATFORM – Brief Technical Spec**

Powered by ARMADA

OMNIA Cyber Command Platform is a security-operations platform powered by ARMADA. It brings together secure telemetry collection, detection and correlation, incident response, governance, threat intelligence and reporting to provide a single operating environment for security posture, risk, evidence and governed action.

| Area | Technical specification |
|---|---|
| **Telemetry** | Secure collection and normalisation of telemetry. Collectors and Evidence Nodes securely ingest, verify and normalise tenant-bound evidence using OCSF. |
| **Detection** | Rules and correlation support the identification and prioritisation of security events. |
| **Response** | Incidents and governed actions support controlled response activity. |
| **Governance** | Identity, policy and evidence controls underpin platform governance. |
| **Alerts** | View, filter and prioritise security events. |
| **Incidents** | Correlate events and manage incidents through a clear process. |
| **Cases** | Capture notes, tasks, evidence and a complete investigation trail. |
| **Vulnerabilities** | Track exposure and safely scan approved targets. |
| **System** | Monitor platform health, services, resources and status. |

| Area | Technical specification |
|---|---|
| **AI Command** | Assisted analysis, recommendations and governed actions. |
| **Threat Intelligence** | Threat intelligence and indicators of compromise. |
| **Reporting** | Reports, evidence and compliance outputs. |
| **Security and access** | OIDC/PKCE authentication, RBAC/OPA authorisation, MFA-capable security and tenant-aware controls. |
| **Platform foundation** | Microservices for detection, ingest, correlation, risk, SOAR, threat intelligence and UEBA, supported by a scalable Kubernetes-based deployment foundation. |

**Operational Flow**

OMNIA CCP supports a structured security-operations process:

- Collect telemetry and evidence.
- Verify, normalise and enrich.
- Detect and correlate.
- Create alerts and priorities.
- Manage incidents and governed actions.
- Record cases and evidence.
- Produce reports and support improvement.

**Designed to Deliver**

- Faster detection and response to threats.

- A single view of security posture and risk.
- Standardised processes and efficiency metrics.
- Better control, evidence and compliance.
- A scalable platform ready to grow with the organisation.