CYNODE.

Microsoft Sentinel Engineering Service

Unlock the full potential of your Microsoft Sentinel platform

Datasheet

Service Overview

Cynode's Microsoft Sentinel SIEM/SOAR Engineering Service delivers a structured, end-to-end approach across log collection, detection engineering, and response automation to build a mature and cost-effective security operations platform.

It covers log source onboarding, classification, tiering, and ingestion design; development and tuning of analytics, correlation, and business-aligned detection rules; and implementation of playbooks and automation workflows to support structured, repeatable response processes within Microsoft Sentinel.

Cynode's expert engineering service is architected, optimised, and operationalised to match your organisation's goals — accelerating time-to-value, enhancing visibility across all platforms, and strengthening your overall security posture.

Microsoft Sentinel CYNODE.

Benefits of Cynode's Managed Microsoft Sentinel SIEM

1) Time-to-Value Acceleration
Faster deployment with connector onboarding, readiness validation, and out-of-the-box playbooks and rules; streamlined workflows get Sentinel production-ready for SOC/MDR quickly.

2) Cost Optimisation
Right-sized ingestion (DCR routing, tiering), retention alignment, and cost dashboards; periodic reviews to down-tier low-value sources and curb waste.

With Cynode, Microsoft Sentinel becomes more than a monitoring tool — it evolves into a strategic operations layer that delivers continuous visibility, automation, and cost-controlled resilience across Microsoft and non-Microsoft environments.

3) Operational Efficiency
Consistent triage and response blueprints, automation with Logic Apps, and ITSM integrations reduce manual toil and lower MTTD/MTTR.

4) Risk & Compliance Assurance
MITRE-mapped coverage, governance zones, RBAC/PIM, and policy-aligned retention improve auditability, resilience, and business continuity.

5) Continuous Value Realisation
Ongoing measurement (rule performance, noise, automation health), quarterly alignment reviews, and proactive tuning sustain outcomes over time.

The Cynode Methodology

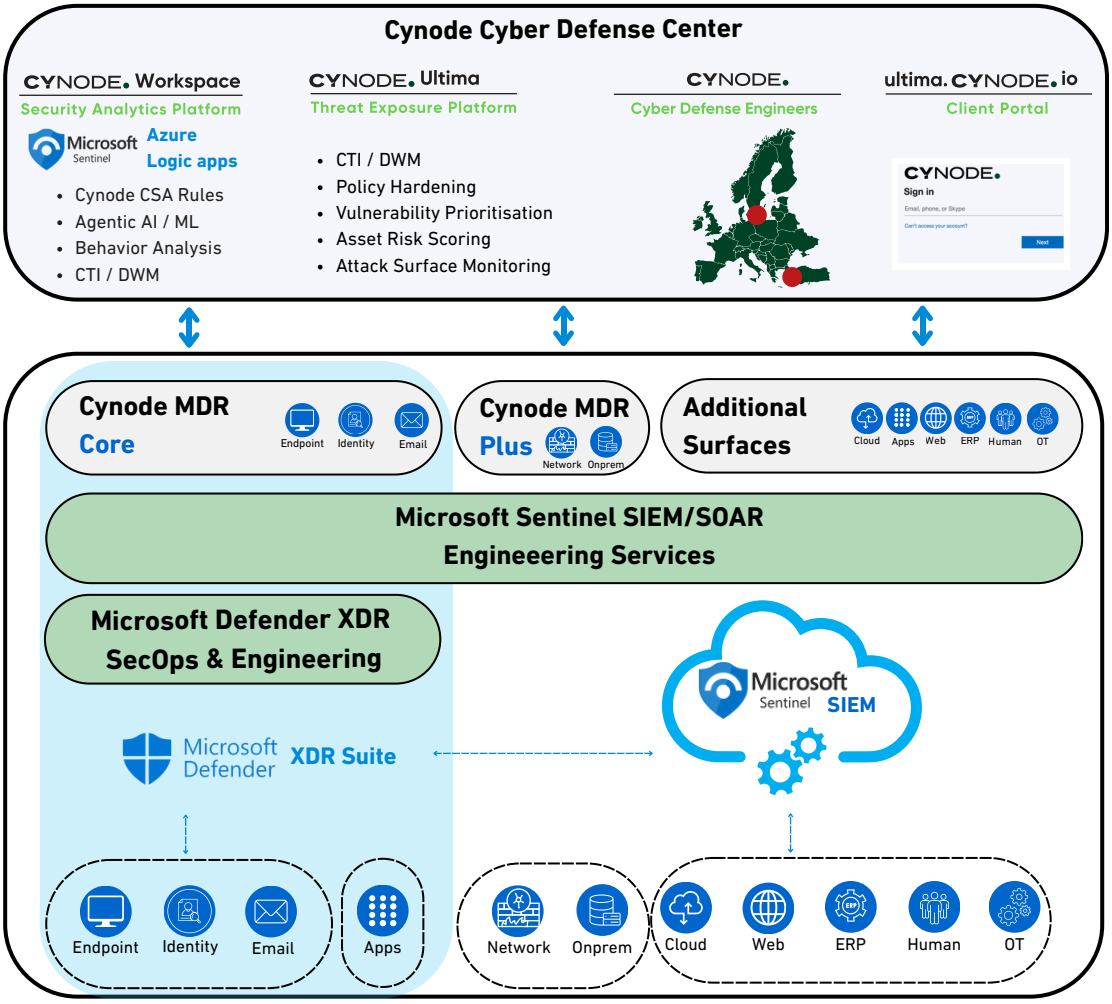
1 Design
Engineer a Sentinel environment aligned with your operational structure, risk model, and cost strategy — not just deployed, but designed for sustainability.

2 Deploy
Build out the Sentinel environment with production-ready detection, automation, and integrations — ready for SOC or MDR operations.

3 Measure
Establish performance and assurance tracking to ensure detection rules, ingestion patterns, and automation remain aligned with operational value. Operational due diligence — not just logging alerts, but assessing how well the system detects, informs, and enables response.

4 Optimise
Continuously tune detection, automation, and ingestion design based on observed outcomes and business evolution.

5 Empower
Equip your internal SOC, response partner, or MSSP with a mature, sustainable Sentinel foundation that is cost-effective and context-aware.



Summary of the Scope

Category	Benefits
1) Architecture & Governance	Tenant/workspace topology, RBAC/PIM, governance zones, and data residency designed for scale and control.
2) Telemetry & Data Strategy	DCR design, transforms/routing, schema validation, and tiering (Analytics/Basic/Archive) for efficient ingestion and storage.
3) Detection Engineering	MITRE-aligned rule library, KQL analytics, entity linking, naming/tagging standards, and continuous tuning to reduce noise.
4) Automation & Orchestration	Logic App playbooks for enrichment, notification, ticketing, and containment; reliable execution with error handling and fallback paths.
5) Ecosystem Integration	Integrations with ITSM (ServiceNow/Jira), threat intel feeds (IOC/watchlists), and reporting (Power BI/SharePoint).
6) Readiness & Measurement	Post-deploy validation of rules/playbooks/connectors; dashboards for alert volumes, suppression/promotion, false pos/neg trends.
7) Optimisation & Governance Ops	Periodic cost reviews, coverage expansion, connector/rule hygiene, and governance checkups to stay aligned with org change.
8) Enablement & Documentation	Runbooks/SOPs, content catalog with versioning and MITRE mapping, connector/playbook docs, and structured knowledge transfer.

Service Delivery

- Delivered as an **annual 8x5 service** following Cynode's design → deploy →measure →optimise → empower methodology.
- Ongoing delivery through regular reviews, tuning cycles, and updates to policies, detections, and integrations.
- Collaboration with your team via documentation, knowledge transfer, and guided operational practices.