CELEBAL TECHNOLOGIES | Microsoft

Microsoft Unified SOC (Sentinel SIEM + SOAR)

Overview

Microsoft Sentinel is now delivered as part of Microsoft's Unified SOC, combining cloud-native SIEM and SOAR with Microsoft Defender XDR for end-to-end threat detection, investigation, and automated response. Celebal Technologies designs, deploys, and operationalizes Unified SOC architectures using Microsoft Sentinel to modernize security operations across hybrid and multi-cloud environments.

Engagement Highlights

- Unified SIEM/XDR design aligned with Microsoft Security Reference Architecture, including Sentinel, Defender XDR, and RBAC.
- Data and signal onboarding across Azure, M365, Defender XDR, SaaS, on-prem, AWS/GCP, and identity/network sources.
- Analytics rule development using Microsoft templates and custom business-specific detections.
- SOAR automation via Logic Apps for enrichment, containment, and response.
- SOC enablement with dashboards, workflows, and alert lifecycle tuning.

What We Assess

- Existing use of CWP /CSPM /CNAPP tools and current coverage.
- Compliance and regulatory standards to be met.
- Hybrid/multi-cloud footprint (Azure, AWS, GCP, Oracle Cloud).
- Key cloud services and workloads currently deployed.
- Evaluated DevOps workflows to identify misconfigurations and gaps before implementation.

Key Features

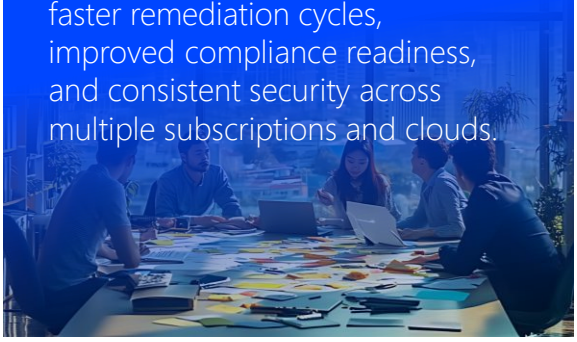
- Continuous Cloud Security Posture Management (CSPM) with secure score optimization.
- Cloud Workload Protection (CWPP) for compute, containers, APIs, data, and secrets.
- Multi-subscription governance with baseline policies and tagging standards.
- Centralized alerting, threat analytics, and attack path insights.

AI-Powered Security

- **Natural-language security queries** (e.g., "Show alerts and recommendations for high-value assets)
- **AI-generated remediation** guidance in plain language for alerts and incidents.
- **Weekly AI-generated SOC** analysis reports across environments and workloads to summaries threats.
- **Command-based automated actions** such as "remove public access on X" or "resolve missing system updates on VMs."

Business Impact

Organizations gain a stronger posture, better visibility into risks, faster remediation cycles, improved compliance readiness, and consistent security across multiple subscriptions and clouds.



Implementation Roadmap

1. **Assessment & Standards Alignment –** Inventory workloads, map to regulations, finalize scope & plan.
2. **Baseline & Segmentation –** Classify assets (critical/non-critical), apply differentiated security policies.
3. **Workload Protection Deployment –** Enable Defender plans per workload type and validate coverage.
4. **Automation & Integrations –** Configure Logic Apps, response rules, and SIEM/SOAR integration.
5. **Operational Handover –** Deliver documentation, runbooks, knowledge transfer and maturity roadmap.

Estimated Range

USD 10,000
(Fixed / Estimated)

Final cost depends on workload count, environment complexity, compliance scope, and integrations.

A detailed commercial proposal will be shared post requirement gathering and assessment.

Why Celebal

- Deep expertise across the full Microsoft Security stack.
- Proven, repeatable security frameworks and accelerators.
- AI-driven insights rather than just technical deployment.
- Strong focus on business risk reduction and governance.