

One-time platform configuration for Sentinel

Azure Sentinel, a cloud-native SIEM, offers a scalable and intelligent threat detection and response approach. YASH Technologies provides a one-time platform configuration service, a comprehensive 6-week implementation designed to effectively deploy and configure Sentinel to monitor security alerts, events, and incidents. For deploying Sentinel for the first time our service ensures precise configuration and seamless integration of all necessary assets, enabling continuous improvement of your cybersecurity posture.

YASH Technologies offers a comprehensive one-time platform configuration service that equips your organization to fully leverage Azure Sentinel's capabilities. Let's explore how we can empower your security operations.

Azure Sentinel – One Time Configuration

- - Discovery Analysis
 New Solution Go-Live
- Design workshop,
- Design Documentation
- POC Confirmation
 Go-live
- Data Sources Integration,
- Event Correlation



1 Week

3 Weeks

Data sources and monitoring services

- List all data sources integrated
- 2. Identify connectors and data parsers in Azure Sentinel
- 3. Identify custom data connectors for specific log sources
- 4. Deploy Azure monitor agent
- 5. Deploy Integration for ITSM SOAR, Threat intelligence platform

POC and UAT

- 1. Evaluation of impact
- 2. Corrective actions
- 3. Issue resolution
- 4. Sign-off

Activities

Deliverables

1 Week

Due Diligence Discovery

- Existing processes for investigation, remediation & automation
- 2. Compliance Requirements
- 3. Identify Critical assets
- 4. Log Retention and Storage Policies
- 5. Integration with ITSM



Environment Readiness

- Design integration with existing infrastructure and third-party resources
- 2. Review MITRE attack coverage
- 3. Configure Azure sentinel workspace with required features
- 4. Device onboarding

YASH Technologies' Sentinel Readiness Service Includes:

Due Diligence Discovery

- Existing Processes Review: Analyze current investigation, remediation, and automation processes.
- Compliance Requirements: Ensure adherence to regulatory standards.
- Critical Assets Identification:
 Pinpoint key assets requiring heightened security.
- Log Retention and Storage
 Policies: Define data retention and storage policies.
- Integration with ITSM: Seamlessly connect with your IT Service Management (ITSM).

Deliverables:

- Discovery Analysis Report
- New Solution Go-Live Plan

Environment Readiness

- Design Integration: Integrate
 Sentinel with existing infrastructure and third-party resources.
- MITRE Attack Coverage: Review and enhance coverage against known attack vectors.
- Sentinel Workspace
 Configuration: Set up Azure
 Sentinel workspace with all required
 features.
- Device Onboarding: Bring all relevant devices into the Sentinel ecosystem.

Deliverables:

- · Design Workshop
- Design Documentation

Data Sources and Monitoring Services

3

- Log Source Integration: Compile a comprehensive list of data sources.
- Connectors and Data Parsers: Identify and configure essential connectors in Azure Sentinel.
- Custom Data Connectors: Develop custom connectors for unique log sources.
- Azure Monitor Agent Deployment: Implement agents for enhanced monitoring.
- *ITSM Integration:* Set up integrations with ITSM and Threat Intelligence platforms.

Deliverables:

- Data Sources Integration Documentation
- Event Correlation Setup

How do we confirm the system is working perfectly?

POC and UAT

During this POC and UAT phase YASH will provide demonstrate that all the requirements are successfully fulfilled in one-time configuration.

YASH will carry out support tasks & evaluate the impact, cause, and corresponding

YASH will lead supporting the Azure sentinel and resolving the issues. YASH will handover all the documents of Azure sentinel to client team

Client to provide sign-off to YASH on transition.





Global Presence: AMERICAS | EUROPE | APAC | MEA

World HQ: 841 Avenue of the Cities East Moline IL-61244 USA **Tel**: 309-755-0433 | **Fax**: 309-796-1242 | <u>www.yash.com</u>



For more information contact YASH today at info@yash.com