YASH Technologies

More than what you think.

Alert Intelligent Framework with Azure Security & AI-Powered Dashboards

Transform security alerts into actionable intelligence with AI-driven correlation, prioritization, and visualization

Modern SOC teams are overwhelmed with high alert volumes, fragmented visibility, and limited context—leading to delayed response and analyst fatigue. YASH's Alert Intelligent Framework leverages Microsoft Defender XDR, Defender for Cloud, Microsoft Sentinel, and Azure-native AI to unify alerts, reduce noise, and deliver prioritized, context-rich intelligence through role-based dashboards—maximizing the value of your Microsoft security investments.

What this engagement solves

Enterprises often struggle with:

- High alert volumes with excessive noise and false positives
- Lack of correlation across security tools and data sources
- Limited context for effective incident prioritization
- SOC fatigue and inefficient response workflows
- Disconnected reporting for operational and executive stakeholders

This offering enables **intelligent alert management, faster response, and improved SOC efficiency.**

Key Highlights

Centralized alert ingestion from Defender XDR, Defender for Cloud, Sentinel, Entra ID, and Azure Monitor	*AI-assisted alert correlation, enrichment, and deduplication*	*Contextual intelligence using asset criticality, identity risk, and MITRE ATT&CK mapping*	*Risk-based alert prioritization for high-impact threats*	*AI-powered dashboards for SOC, cloud security, and executive stakeholders*	*Native SOAR automation using Sentinel playbooks and Azure Logic Apps*	*Integration with third-party SIEM/SOAR and ITSM tools*

Engagement Approach (Assessment | Implementation | BAU)

Phase 1: Assessment

Activities:

- Assess existing alert sources across Defender XDR, Defender for Cloud, Sentinel, and Azure Monitor
- Analyze alert volume, duplication, false positives, and response effectiveness
- Identify critical assets, privileged identities, and high-risk workloads
- Review SOC processes, escalation workflows, and automation maturity
- Gather dashboard and reporting requirements for different stakeholders

Benefits:

- Clear understanding of alert landscape and inefficiencies
- Identification of high-value use cases for correlation and prioritization
- Defined roadmap for intelligent alert transformation

Deliverables:

- Alert intelligence maturity assessment report
- Alert noise and duplication analysis with optimization recommendations
- Prioritized use cases for AI-driven correlation and scoring
- Dashboard design blueprint for SOC and leadership

Phase 2: Implementation

Activities:

- Configure centralized alert ingestion and normalization across Microsoft security services
- Implement AI-assisted correlation, enrichment, and deduplication logic
- Define risk-based alert scoring using asset criticality, identity risk, and threat severity
- Develop AI-powered dashboards using Azure Monitor Workbooks and Power BI:
  - SOC operations dashboard
  - Cloud security risk and exposure dashboard
  - Executive/CISO dashboard
- Configure SOAR automation via Sentinel playbooks and Azure Logic Apps
- Integrate with ITSM tools (ServiceNow, Jira) and third-party SIEM/SOAR platforms

Benefits:

- Unified and intelligent alert management across environments
- Significant reduction in false positives and alert fatigue
- Faster detection and response through automation and prioritization
- Enhanced visibility for both operational teams and leadership

Deliverables:

- Fully deployed Alert Intelligent Framework on Azure
- Correlated and prioritized incident views across workloads
- Role-based dashboards for SOC analysts and executives
- Automated response playbooks and documentation
- Integration runbooks and knowledge transfer

Phase 3: BAU Phase (Continuous Optimization & SOC Enhancement)

Activities:

- Continuous monitoring of alert trends, severity distribution, and SOC performance
- Periodic tuning of correlation logic, prioritization thresholds, and dashboards
- Monthly security operations reviews and optimization recommendations
- Support for threat hunting and incident investigations via Sentinel
- Continuous alignment with evolving threat landscape and Microsoft roadmap

Benefits:

- Sustained reduction in alert noise and improved signal quality
- Continuous improvement in SOC efficiency (MTTD, MTTR)
- Adaptive security posture aligned to emerging threats

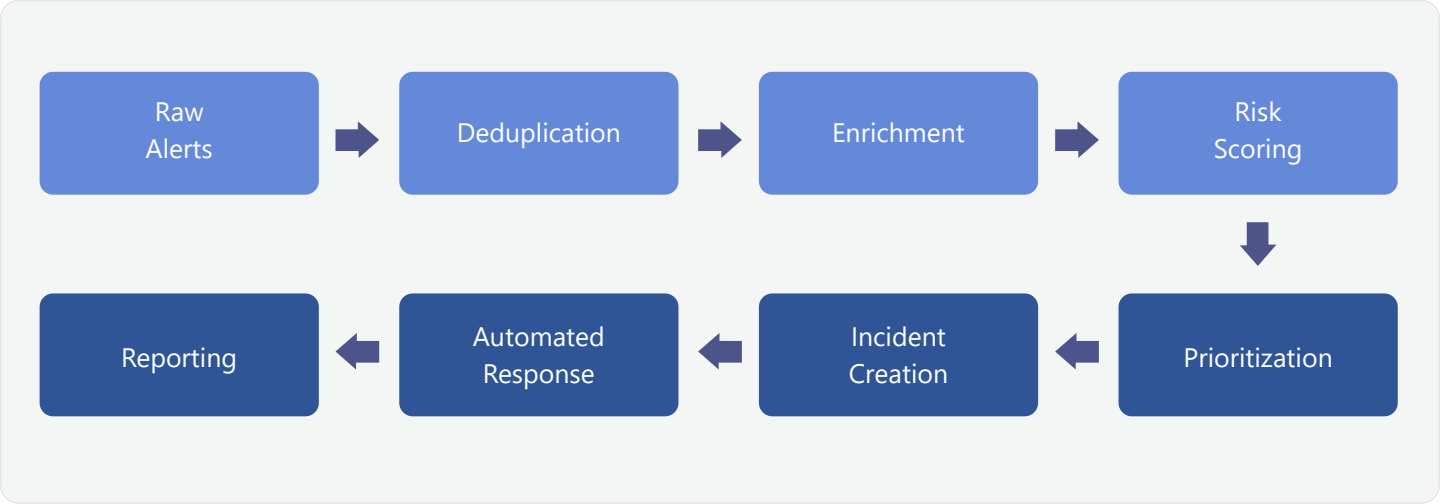
Deliverables:

- Weekly/monthly alert intelligence and trend reports
- Updated dashboards reflecting new risks and environment changes
- Alert optimization and SOC efficiency recommendations
- Incident summaries and lessons learned
- Strategic advisory backlog for continuous improvement

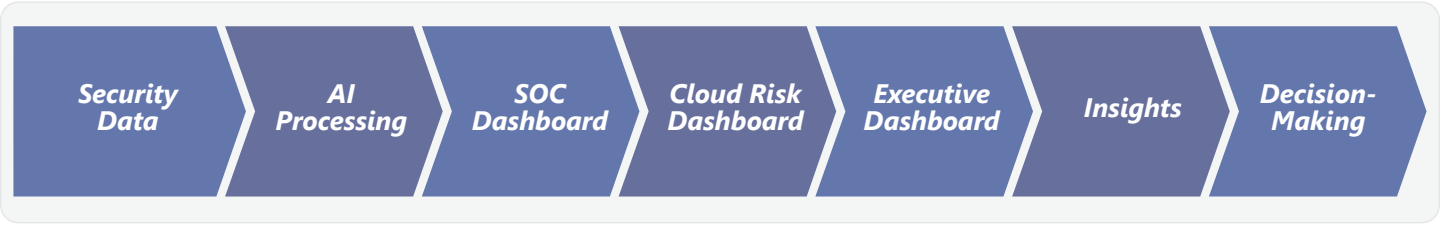
Compliance & Evidence Automation Pipeline

Duration (in days / weeks):	*Price:*	*Industry:*
2–3 weeks (Assessment + Implementation); BAU ongoing	$5000	Manufacturing | Healthcare | BFSI | Retail | Automotive | Energy & Utilities

Alert Processing & Prioritization Workflow



SOC Intelligence & Dashboarding Layer



YASH Technologies
More than what you think.

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 | www.yash.com

For more information contact YASH today at ***info@yash.com*** or scan here