YASH Technologies
More than what you think.

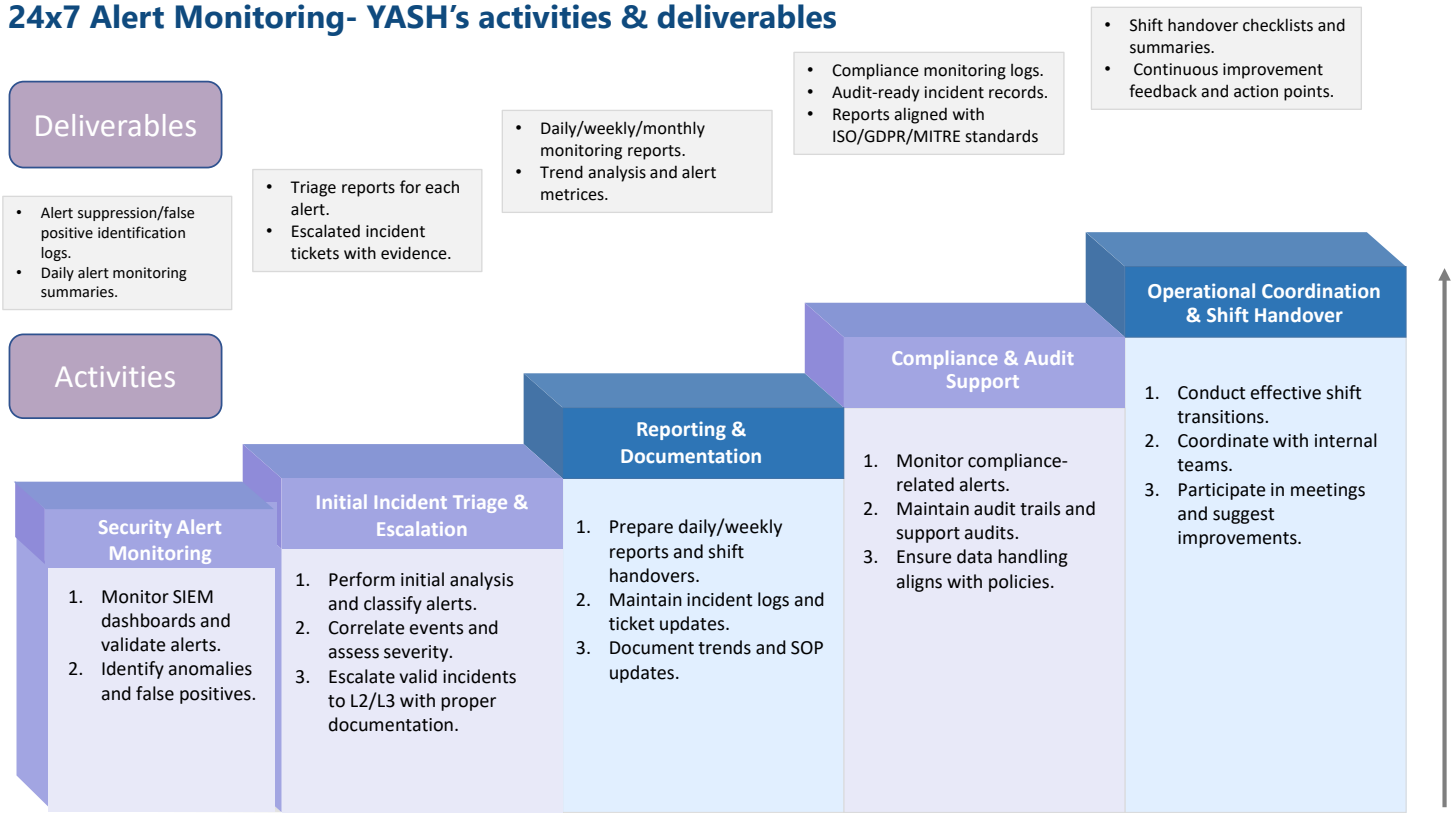
Microsoft Solutions Partner

24x7 Alert Monitoring

YASH Technologies provides 24x7 Alert Monitoring services to help organizations maintain continuous visibility into their security posture. Our L1 analysts monitor and triage alerts in real time, identifying false positives and escalating genuine threats for further investigation. By leveraging industry-leading tools and predefined playbooks, we ensure timely detection and response to potential incidents. This foundational layer of security monitoring supports rapid threat identification and helps minimize risks across the organization's IT environments. Our team ensures every alert is documented, prioritized, and handled in alignment with the customer's incident response plan. Regular reporting and metrices are provided to maintain transparency and improve SOC efficiency. With scalable support, our services adapt to your evolving security needs.

YASH Technologies offers a comprehensive 24x7 alert monitoring service that equips your organization to fully leverage Microsoft Sentinel's capabilities. Let's explore how we can empower your security operations.

24x7 Alert Monitoring- YASH's activities & deliverables



YASH Technologies' Security Alert Monitoring Service Includes

1. Security Alert Monitoring:

- Monitor SIEM dashboards and validate alerts.
- Identify anomalies and false positives.

Deliverables:

- Alert suppression/false positive identification logs.
- Daily alert monitoring summaries.

2. Initial Incident Triage & Escalation:

- Perform initial analysis and classify alerts.
- Correlate events and access severity.
- Escalate valid incidents to L2/L3 with proper documentation.

Deliverables:

- Triage reports for each alert.
- Escalated incident tickets with evidence.

3. Reporting & Documentation:

- Prepare daily/weekly reports and shift handovers.
- Maintain audit trails and support audits.
- Ensure data handling aligns with policies.

Deliverables:

- Daily/weekly/monthly monitoring reports.
- Trend analysis and alerts metrics.

4. Compliance & Audit Support:

- Monitor compliance related alerts.
- Maintain audit trails and support audits.
- Ensure data handling aligns with policies.

Deliverables:

- Compliance monitoring logs.
- Audit ready incident records.
- Report aligned with ISO/GDPR/MITRE standards.

5. Operational Coordination & shift Handover:

- Conduct effective shift transitions.
- Coordinate with internal teams.
- Participate in meetings and suggest improvements.

Deliverables:

- Shift handover checklists and summaries.
- Continuous improvement feedback and action points.

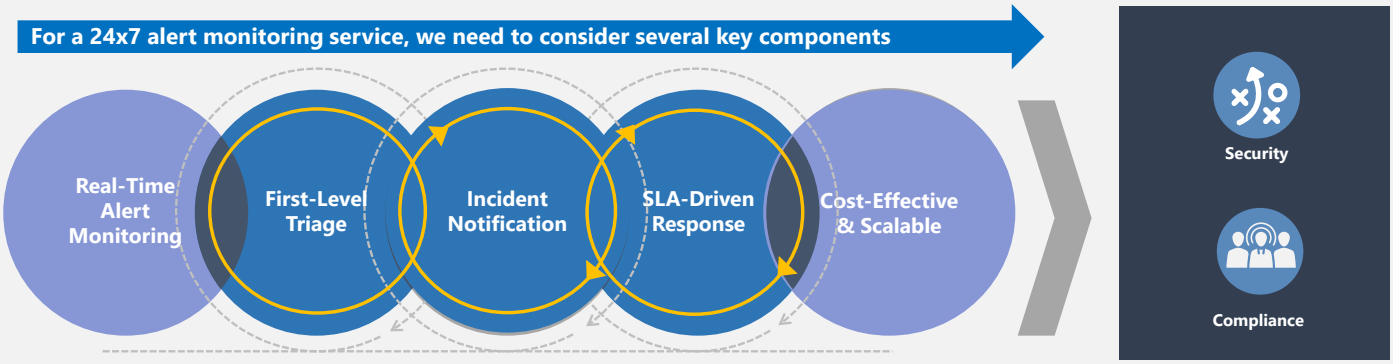
How do we confirm the system is working perfect?

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 and evaluate the impact, cause, and corresponding corrective action.	YASH will lead supporting the Microsoft Sentinel and resolving the issues.	YASH will handover all the documents of Microsoft Sentinel to client team.	Client to provide sign-off to YASH on transition.

24x7 Alert Monitoring-YASH's Key Features



- Alerts are detected in real-time using SIEM and other monitoring tools.
- 24/7 real-time security monitoring across integrated systems within the SOC.
- Detect potential threats at an early stage to ensure rapid response.

- L1 analysts perform initial assessment of alerts to filter false positives.
- Basic investigation is done using logs, IP checks and known indicators.
- Categorizes alerts based on severity for further action or escalation.

- Valid alerts are promptly communicated to stakeholders or L2/L3 teams.
- Notifications follow predefined channels(E-Mail, ticketing, SMS, etc.)
- Ensures timely awareness and response to potential incidents.

- Response times are aligned with service Level Agreements (SLAs).
- Alerts are prioritized to meet business-critical response timelines.
- Performance is tracked using metrices like MTTD and MTTR.

- Shared or centralized reduces operational costs.
- Easily scales with business growth or added infrastructure.
- Allows for flexible resourcing using global or hybrid SOC models.

Deliverables

- 24x7 Real-Time Alert Monitoring & Triage.
- Timely Incident Notification & Escalation.
- Daily Reporting & Scalable Monitoring Framework.

YASH Consulting and Advisory Services Offerings

YASH Consulting and advisory offerings comprises of the following:

Rapid Detection

- Enables real-time threat identification and faster incident escalation.
- Reduces detection time to minimize potential impact.
- Improves visibility into suspicious activities across environments.

Operational Continuity

- Ensures uninterrupted monitoring to maintain system uptime.
- Prevents threats from disrupting business operations.
- Support quick recovery and reduced downtime.

Azure-Optimized

- Seamless integration with Microsoft Defender and Sentinel.
- Uses Azure-native tools for efficient threat detection and response.
- Scales easily with dynamic Azure environments.

Compliance & Support

- Aids in meeting standards like ISO, GDPR and HIPAA.
- Maintains audit readiness with continuous monitoring.
- Provides support for compliance reporting and documentation.

YASH is

A trusted partner | An extended arm of your organization | An expert at your side

ACCELERATORS **Library of 100+ documents, tools, framework models, that have been used successfully for our customers and are ready to be implemented in your organization.**

24x7 Alert Monitoring-How it works

L1 Analyst Monitoring

- L1 analysts works in shifts to ensure 24x7 coverage.
- They monitor SIEM dashboards for new or active alerts.
- Responsible for acknowledging and starting basic triage.

Triage & Investigation

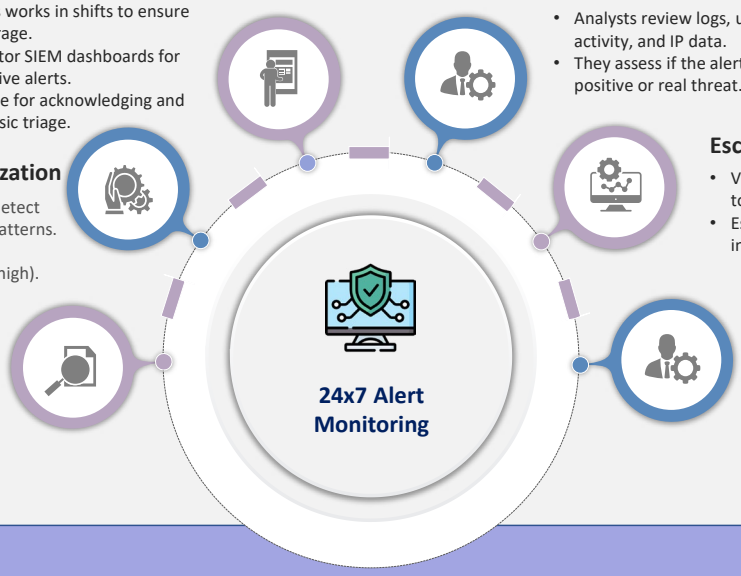
- Analysts review logs, user activity, and IP data.
- They assess if the alert is false positive or real threat.

Alert Correlation & Prioritization

- SIEM correlates events to detect suspicious behaviour and patterns.
- Alerts are automatically categorized (low/medium/high).

Escalation

- Validated or critical alerts are escalated to L2/L3 teams.
- Escalation follows defined SOPs and incident workflow.



Log Collection

- Logs generated by devices like firewalls , servers and endpoints.
- These logs are forwarded to a centralized SIEM tool.
- The SIEM continuously collects and stores event data.

Documentation & Reporting

- All alerts and actions are logged in a ticketing system.
- Analysts prepare shift handover and daily reports.
- Data supports audits, analysis, and continuous improvement.

- **80% reduction** in time to validate alerts
- **70% improvement** in (MTTD)
- **75% reduction** in false positives
- **80% improvement** in (MTTR)
- **69% reduction** to cyber risk profile

Microsoft Solutions Partner
Security

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