YASH Technologies
More than what you think.

Microsoft Solutions Partner

YASH - Attack Defense Framework

YASH Attack Defense Framework strategy that goes beyond traditional passive defences by proactively engaging with threats to detect, deceive, and disrupt adversaries.

This is designed to detect intrusions early; delay or disrupt adversary operations; gather intelligence on attacker behavior and tools.

Description

As mentioned above the implementation of attack defense framework will provide a robust strategy to protect the organization from the adversaries. It helps to design the dynamic defences, detection and deception for the adversaries.

For example, is the MITRE ATT&CK framework, which maps defensive techniques to known adversary behaviours, helping defenders to choose right counter measures.

Activities

- **Review and Planning:** Understand client needs (SIEM rules, business goals) and define scope (systems, organizational areas)
- **Security Posture Review:** Evaluating current detection, deception, and response capabilities.
- **Threat Modelling:** Simulate attacker paths using MITRE ATT&CK, NIST, GDPR and identify choke points.
- Refining the existing rules where required with any additional data if required.
- Integrate with additional threat intelligence sources.
- Create and configure new alerts based on threat models.
- Continuously monitor and update incident response protocols.

Benefits

- Reveals blind spots in detection and response.
- Prioritizes high-impact controls for implementation.
- Provides evidence-based justification for investment.

Deliverables

- KQL-Based Detection Ruleset
- Triaging Templates
- Enhanced Standard Operating Procedures
- SIEM Configuration Package

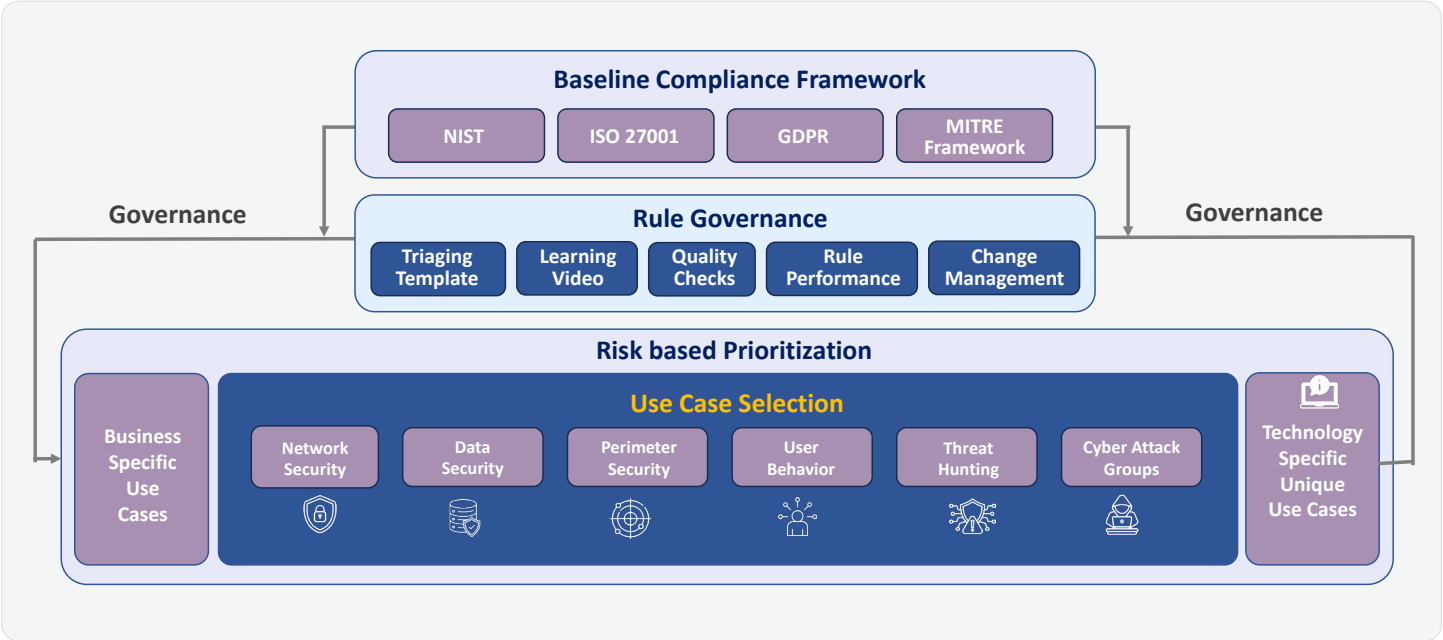
Duration: (in days / weeks): 4- 8 weeks

Price: 1000$/month

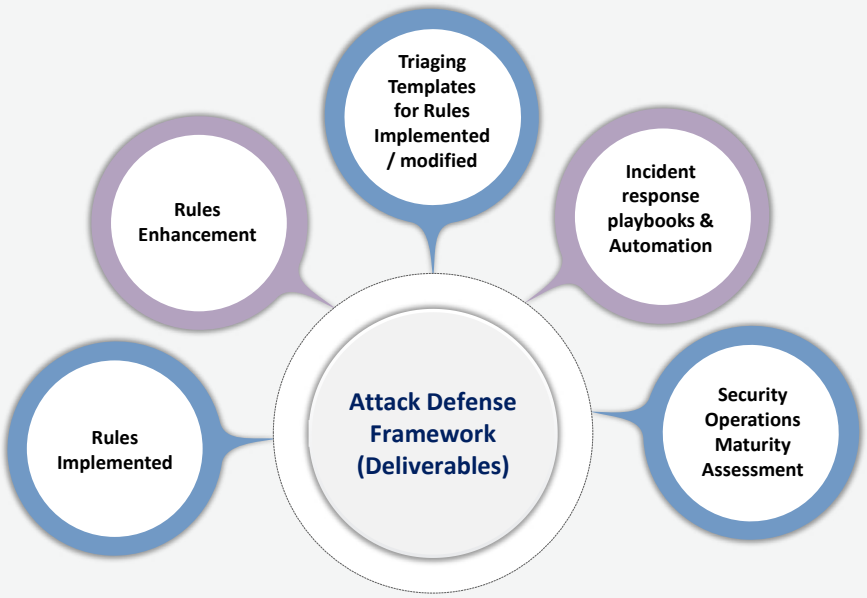
Industry: All industries

Attack Defence Framework

YASH has developed a signature framework to identify and develop alert rules based on threat intelligence sources and unique business rules. These regulations aligned with recognized frameworks such as NIST and GDPR. This will be referenced for Microsoft Sentinel implementation.



What and How do we our Deliverables for this Service Offering



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