# Success Story: Next Generation SIEM deployment with embedded AI/ML features for Wipro

## Challenges

- The solution was not scalable to meet IT growth.
- API-based integrations are not working due to hardware issues.
- Lack of analytics. No ML / AI capabilities in the current version
- Challenge in maintaining 500 + rules with manual mapping to MITRE Framework
- There is a lack of proactive content development from provider around new threats.
- Log source integration management and upkeep were major challenges.
- Anomaly detection based on network behavior is not possible.
- There are no OOTB dashboards; all are manually prepared.
- No DR has been set up, monitoring has been affected
- Support from vendor was not adequate in resolving issues.

## Expected Benefits

- Cloud native solution that can auto scale up / down the storage and compute
- Reduce false positives and generate actionable alerts to reduce alert fatigue.
- Cloud + AI / ML to increase the speed of detection coupled with security automation
- Anomaly detection based on user / identity behavior, traffic analysis, historical alerts and signals to predict the unknown attacks protectively
- Enhanced security posture visibility on single glass of pane for all levels (CXOs, Managers, Engineers)

## Proposed Solution

Next Gen SIEM including:

- Security Data Lake
- UEBA Analytics
  - ✓ Insider Threat Bundle (Privileged Account and Data Security Analytics)
  - ✓ Cyber Threat Analytics
  - ✓ Cloud Security Analytics
  - ✓ Optional Premium Analytics Modules
- Threat Hunting with Spotter

Estimated volume Approx. - 250000 EPS with 10 % incremental assumption on yearly basis

Securonix SaaS Delivery with AWS “Sister” Account

## Current State

- Transformation project initiated in phased approach
- Securonix SaaS setup is ready.
- RINs deployed for phase 1 expected log sources
- 20 + log sources are onboarded and currently be tuned for stabilization