LTS Secure

# CASE STUDY

## LTS Secure vSOCBox: AI And ML Based SIEM Platform For Govt. Entity

**USE-CASE**

Client type- Government

Location- UAE

## Problem statement

Thousands of alarms were being generated inside the client's environment everyday, causing their analysts to be bogged down with manual, recurring, task-intensive tasks, leading them to suffer from alert fatigue, thus decreasing the efficiency of their SOC operations.

## Solution

- LTS Secure VSOCBox was deployed on their environment, enabling their SOC to become more intelligence-driven, by allowing them to centralize all their alarms, while aggregating & validating data from a wide variety of solutions like SIEM, UEBA, NGFW and threat intelligence.
- The ML capabilities of our solution, allowed to minimize the noise generated and brought in context like Assets-Users-Business to enrich the alarms.
- Our solution also allowed their SOC to automate some of the L1 level alarms where human second eye is not required.

## Impact

- Alert overload avoided
- Filter out false-positives and instantly identify which alerts to escalate
- Significant reduction in time and resources required to review alerts
- Enabled SOC teams to focus on complex incidents that really require their skills
- Made threat investigation process more standardized
- Faster results and adaptive response
- Improved flexibility and opened new opportunities for collaboration
- Optimized use of customers' existing security investments to provide ROI

## Product USP

- Centralization of Alarms from all Critical-Security-Controls
- Enrichment of Alarms with User-Asset-Business context
- Reduce alert fatigue
- Does alarm prioritization, security orchestration, and automation
- Helps automate incident response
- Enables organizations to implement sophisticated defense-in-depth capabilities
- GUI enabled intuitive SOAR Platform

## Product Features

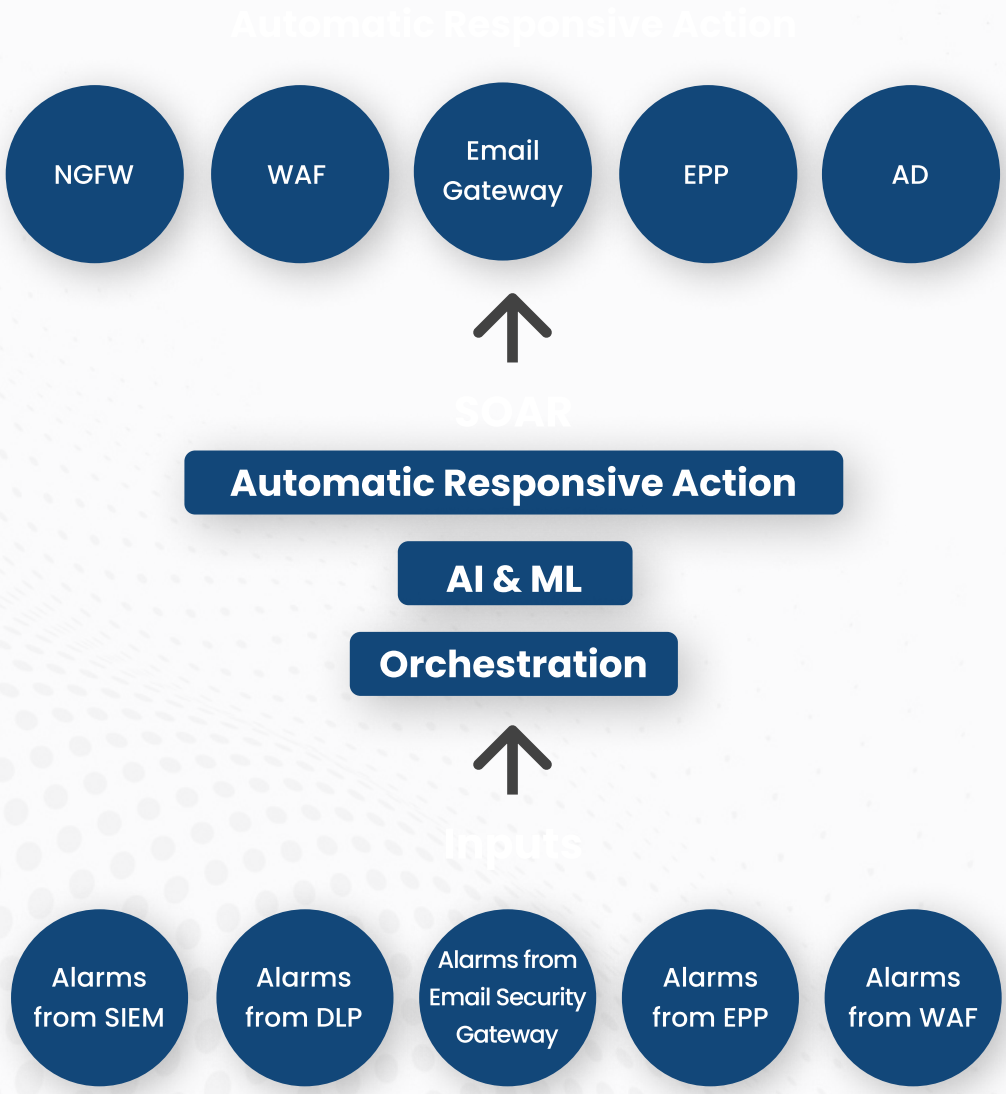
- SOAR
- Input data sources
- DLP
- NGFW
- EDR

LTS Secure

**Solution type:** Product + Services

**Specifications** (Optional)

**Product Architecture:**




## Delivery Mode

- Cloud Based (SaaS Multi-Tenant)
- On Premise
- Hybrid

## Business Model

- One Time Installation + Services
- Pay Per Use
- Subscription Model

## Verticals catered

- BFSI
- Healthcare
- Manufacturing
- Government

## Location of deployment

- On-Premise
- Cloud

## GTM

- Channel Partner
- MSP/MSSP
- SI's
- Other

## Salient Features

- Cost
- Operability
- Orchestration
- Response Automation
- Risk Management

## Key Customers (Optional)

LTS Secure
vSOCBox XDR

## Website Link

www.ltssecure.com