vSOCBox™

CASE STUDY

vSOCBox™ : AI And ML Based SIEM Platform For BFSI

USE-CASE

Client type- BFSI

Location-- Bengaluru, India

Problem statement

- Absence of enrichment of alarms, orchestration and reprioritization
- Review of each event and remediation on a real-time basis wasn't feasible
- False alarms due to false positives from SOC team, which resulted in decreased efficiency of solution and their team

Solution

- vSOCBox™ deployed for centralization of alarms with Big Data, which can be analyzed with ML to remove noise, duplication of alarms coming from different security solutions and to bring context like Assets-Users-Business to enrich the alarms
- vSOCBox™ provided a provision to automate some of the L1 level alarms where human second eye is not required

Impact

- Removal of duplication of alarms
- 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 managers and security team to focus on real threats
- Made threat investigation process more standardized
- Faster results and adaptive response
- 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

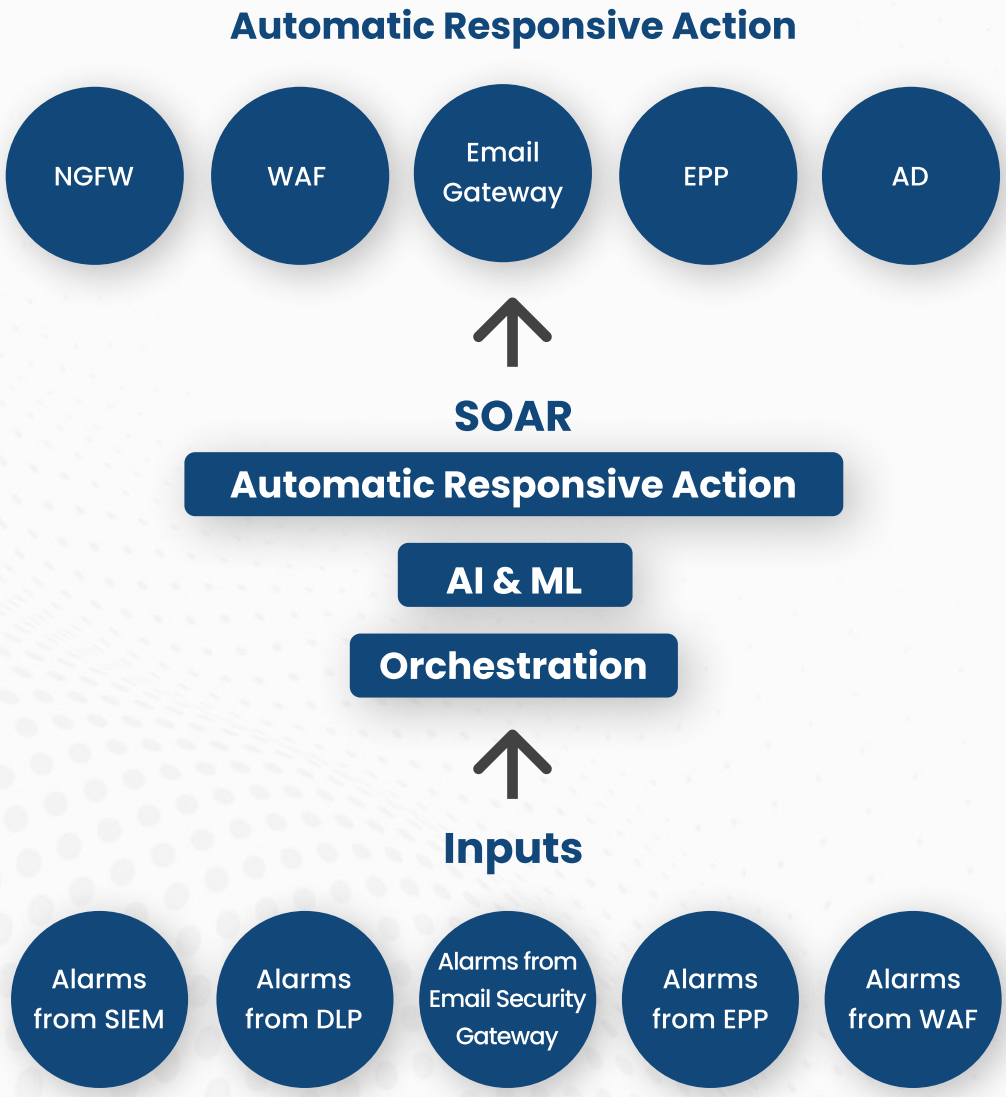
Product Features

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

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)

vSOCBox™ XDR

Website Link

www.vsocbox.com