BUSINESS CONTEXT

The Client aimed to resolve:

• Lack of industry leading security products portfolio which can provide effective protection from emerging threats
• Lack of processes for managing security products portfolio
• Lack of adequate in-house skillsets and services were provided with non-dedicated resources
• Average time to detect and respond to security events in days and weeks
• Limited Use Cases Implemented. Threat of missing the detection of suspicious event
APPROACH AND SOLUTION

Tech Mahindra catered to the client problem as follows:

• Plan, Design & Build Dedicated Data Center with state of the art security products portfolio to provide effective network, perimeter & endpoint security
• Integration of log sources (Workstations, Servers, Network Devices, Applications) to expand depth and breadth of security events detection
• Platform administration and fine-tuning. Custom Use-cases and rule development
• Implementation of User and Entity Behaviour Analytics Tool (UEBA)
• Implementation & Integration of SAP Security Monitoring Platform with SIEM
• 24x7x365 Eye on the Glass Monitoring to detect threats in real time and respond to mitigate business impact

IMPACT & HIGHLIGHTS

Security application management, upgrade being performed in a structured way
And MTD & MTR in minutes & hours

150+ SOC Rules implemented to detect security threats across different platforms including SAP

100% Up time availability of security products

Single pane of glass view for all security events & Proactive Threat Intelligence & Threat Advisories