iSON technologies

CASESTUDY

ISON ensures reduction of the residual risks by setting up Global Service Operations Centre for A large Indian conglomerate holding Leadership positions in Aviation

The Challenge

The client, an Indian conglomerate, with business interests in hospitality, luxury goods, aviation, information technology, and travel was seeking technology partner to ensure reduction of the residual risks by aligning its objectives to the business objectives.

Earlier client information security was structured in a de-centralized manner; the business units were driving information security independently resulting in inconsistency of the controls that were implemented and configured either to detect or prevent Information Security incidents. The bigger challenge was lack of specialised knowledge for Information Security, as a result of which a large number of events went unnoticed in addition to the information security response.

The challenges faced in the absence of a Service Operation Centre (SOC) were:

- Business missing out on events related to information security incidents, most important of which were related to data leakage to unauthorized sources
- Finding and retaining specialised talent, an expensive solution and getting 24x7 support
- Shielding the personal shortcomings of information security resources of respective business units. The personal shortcomings would often result in escalations to the level of an information security incident
- Levels of risk inherent in the business units were alarmingly higher than the acceptable levels of risk. For some business units, the risk profiling is not carried out.

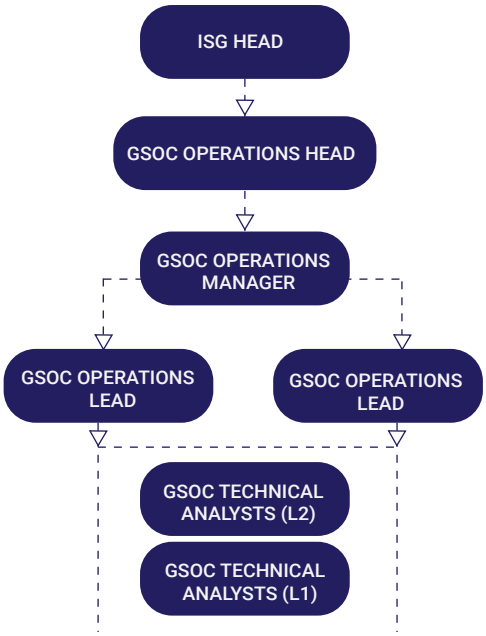
The Solution

The spate of unaddressed information security incidents can only be controlled, if the information security services are centralized. As next steps ISON stepped in to provide 24x7 Managed Services for Information Security Incident Management to the client. The specialized resources performed the following activities related to Information Security Platforms and Incidents:

- Monitor
- Detect
- Analyse
- Triage
- Respond (this includes running through the lifecycle of the incident from the point that it is identified to the point that it is Closed)

The services were adhered to the operation level agreements between the Group Information Security and Business Units of the client, irrespective of the number of resources that were available at any point of time. The upscaling of resources met the Operation Level Agreements (OLAs) and addressed as by ISON.

The managed services model included the Governance Layer of the Group Information Security would interface with the business units to have a clear understanding of the business objectives and risk Appetite, whereas the Analysts, Senior Analysts and SMEs for the SOC Operations were responsible for management of the Information Security platforms and incidents. The organization structure proposed for the Group Security Operations Centre is as given below:



Solution Implementation & Responses:
The GSOC analysts provisioned under the managed services for information security were profiled for the following requirements:

1.Prevention & Identification of Information Security Vulnerabilities: The SOC Services/ Solution should be able to identify information security vulnerabilities and prevent these vulnerabilities.

2.Incident Management: Reporting of information security incidents using appropriate tools. Track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals in the organization.

3.Continuous Improvement
Continuously improve SOC Services / Solutions.

4. Scalability of Solutions: The services / solutions offered should be modular, scalable, and should be able to address organization requirements during the period of contract.

5. Redundancy of Services: The services / solutions in scope should be designed with adequate redundancy and fault tolerance to compliance with SLAs for uptime.

6. The services/ solutions offered should not have any significant impact on the existing infrastructure/ business of the bank either during installation or during operation of SOC. Based on the above principles, the following services/ solutions were identified to enhance the security posture of the organization:

a. Security Information and Event Management (SIEM)
b. Websense Proxy at Gateway
c. SMTP Security on exchange servers
d. Triton End point DLP
e. Enabling Role Based access and shift wise admin access using SLAM tool
f. Forensic Tools for monitoring changes in AD structure or components (AD Auditor) & Changes to user mail boxes using Exchange Auditor
g. NIPS monitoring (McAfee Nitro)
h. Nessus for Vulnerability Scanning & Assessment
i. In defend
j. Any new tool that will be implemented in future

Managed across 3 shifts to maintain a 24 x 7 support which was based at the client premises.

ISON developed rules, signatures, feeds, SIEM correlation, DLP Policies, Vulnerability Scanning guidelines, create scripts for process automation and metrics for report creation.

The Benefits

The biggest benefit received by client as a result of the Managed Service was that the Information Security Services were completely outsourced to ISON, which meant that the Internal GIS team is able to have a more dedicated approach towards defining the Strategy and Roadmap for improvement of the Information Security Practices across the Group Businesses.

One direct outcome for implementation of the agreed improvementinitiatives is the reduction of per Incident cost to the company, which would be a significant gain over a period of time and contribute favourably towards the ROSI (Return on Security Investment) for the Group. In fact, by doing a comparative analysis, the ROSI worked out to almost half with a Managed Service setup as compared to the ROSI in a Build and Operate model.

The basic responsibility for any Information Security Organization or sub-organization is the ensure reduction of the residual risks that are defined by the business stakeholders (Usually the Board or Senior Management) by aligning its objectives to the business objectives. One of the key requirements to make that happen is the establishment of 24x7 Managed Services Information Security Operations by providing Specialist Resources to do the activities related to Information Security Platforms and Incidents. The project resulted in other benefits:

- The client was more focused towards defining the Strategy and Roadmap for improvement of the Information Security Practices across the Group Businesses.
- Reduced per incident cost to the company, which over a period of time contributed favourably towards saving of around 50% on Return on Security Investment (ROSI) .
- Reduced data leakage to unauthorized users, specially data classified as "Confidential".
- Established a level of trust with their customers and enhanced their brand reputation by establishing that the practices were in order and followed.