$1.1 BILLION INDIAN BANK MAINTAINS AND MONITORS COMPLIANCE TO INTERNALLY DEFINED SECURITY POLICIES WITH SAFE

INDUSTRY

Banking and Financial Services

RESULTS

- Security visibility into technology stack across the organization
- Factor People, policies, technology, cybersecurity products, and third party risk posture to generate overall risk posture
- Compliance to organization's hardening guidelines

CHALLENGES

- No visibility into the security posture of assets on-cloud for CXOs
- Overall compliance percentage to its own hardening guidelines

THE NEED

The organization needs to comply to its own policies. In this case, the organization had prepared a set of policies that are applicable to it's technology stack. The requirement was to support customised policy profile for an organization since all the controls defined in SAFE should be similar to what the organization security requirements are.

The result must provide an organization with a visibility into the security posture across the organization in terms of compliance percentage that can be easily understood by everyone across the leadership

ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, organization would perform a manual assessment driven by an auditor on sample assets of sample controls. While the sample based assessment did not bring visibility of the actual security posture and compliance to their hardening guidelines, due to the human-intensivity of the activity, the organization wea not able to scale the process further.

BRING RIGHT VISIBILITY WITH SAFE

SAFE, is an enterprise-class, unified, and real-time Cyber Risk Quantification (CRQ) platform that offers a comprehensive solution, by taking into account both technical and business aspects, to arrive at informed and prioritised decision making. SAFE has a unique assessment approach across five threat vectors concerning organisations, namely People, Policy, Technology, Cybersecurity Products, and Third-parties. SAFE helped the organization with the following unique capabilities:

1. Score per asset, per group
2. Remediation guidelines in SAFE to improve security posture
3. Assessment as per bank's hardening policy for RBI Compliance

1 SCORE PER ASSET, PER GROUP

SAFE generates a score (SAFE score) per asset based on the assessments performed by SAFE and factoring the inputs received from integrations with other tools. These assets can be further clubbed into an asset group per business unit or per application to factor the security posture of all the underlying assets such as servers, databases, middlewares, etc. This way of risk quantification helps organization in taking the right decision especially during the mission critical go-lives. The organization follows a policy of making sure that the overall SAFE score of a mission critical application is 3.5+ with 0 Critical or High vulnerabilities that could cause any business impact.

2 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

SAFE provides organization with a consolidated view of SAFE score of various departments in a single widget. Any new business unit can be onboarded easily in SAFE and can be continuously monitored. Each Business Unit has been assigned a priority score and according to the delta change in its value, SAFE sends actionable alert to the asset group owner and/ or concerned authorities in form of an email or system generated telephonic call.

3 REMEDIATION GUIDELINES IN SAFE TO IMPROVE SECURITY POSTURE

SAFE not only tells you what and how big the problem is, but it also walks you through the remediation and how it will impact your organization. The organization leverages SAFE to remediate the most critical gaps that may make your company the next headline in the newspaper. It guides you to reach the desired SAFE score according to your plan.

4 ASSESSMENT AS PER BANK'S HARDENING POLICY FOR RBI COMPLIANCE

SAFE has its assessment controls defined based on the industry benchmarks such as CIS, STIG, and security guidelines released by the OEMs. However, it is a standard practice in the BFSI to define a baseline security hardening guideline for each unique type of a device/ OS to ensure that the assets connected to the organization network and/ or containing business sensitive data has the right security controls in place.

SAFE has enabled the organization to define the security assessment policy based on their own baseline security hardening guidelines for identifying th compliance of each asset across the organization with their guidelines. While doing this, SAFE also alerts if the configuration of any asset changes intentionally or unitentionally through it notification engine in form of a score drop or rise.

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

Lucideus House
Plot No 15, Okhla Phase III
New Delhi, 110020

$1.1 BILLION INDIAN BANK MAINTAINS AND MONITORS COMPLIANCE TO INTERNALLY DEFINED SECURITY POLICIES WITH SAFE

INDUSTRY

Banking and Financial Services

RESULTS

- Security visibility into technology stack across the organization
- Factor People, policies, technology, cybersecurity products, and third party risk posture to generate overall risk posture
- Compliance to organization's hardening guidelines

CHALLENGES

- No visibility into the security posture of assets on-cloud to CXOs
- No overall compliance percentage to its own hardening guidelines

THE NEED

In-house policy compliance: This organization had prepared a set of policies that were applicable to its own technology stack. The requirement was to support customised policy profile since all the controls defined in SAFE should be similar to what the organization's security requirements were.

The organization needed a clear visibility into their security posture in terms of compliance percentage which could be easily understood by everyone across the leadership.

ON-GROUND EXECUTION CHALLENGES

Prior to SAFE, this organization would perform a manual assessment driven by an auditor on sample assets of sample controls. This sample-based assessment did not bring visibility to the actual security posture and compliance to their hardening guidelines. Also, due to its human-intensive nature, the organization was not able to scale the process further.

BRING RIGHT VISIBILITY WITH SAFE

SAFE is an enterprise-class, unified, and real-time Digital Business Risk Quantification (CRQ) platform which offers a comprehensive solution by taking into account both technical and business aspects and gives informed, prioritised insights. With its unique assessment approach across five threat vectors concerning organisations - People, Policy, Technology, Cybersecurity Products, and Third-parties - SAFE helped this organization with the following:

1. Score per asset, per group
2. Remediation guidelines in SAFE to improve security posture
3. Assessment as per bank's hardening policy to ensure compliance to Reserve Bank of India guidelines

1 SCORE PER ASSET, PER GROUP

SAFE generates a score (SAFE score) per asset based on the assessments it has performed and by factoring the inputs received from integrations with other tools. These assets can be further clubbed into an asset group per business unit or per application to factor the security posture of all the underlying assets such as servers, databases, middlewares, etc. This means of business risk quantification helps the organization in taking the correct decision, especially during the mission critical go-lives. This organization follows a policy of making sure that the overall SAFE score of a mission critical application is 3.5+ with 0 Critical or High vulnerabilities that could cause any business impact.

2 ASSET GROUPING AS PER BUSINESS REQUIREMENTS

SAFE provides this organization with a consolidated view of SAFE score across departments through a single widget. Any new business unit can be on-boarded easily and be continuously monitored. Each Business Unit has been assigned a priority score and according to the delta change in its value, SAFE sends actionable alerts to the asset group owner and/ or concerned authorities in form of an email or system generated telephonic call.

3 REMEDIATION GUIDELINES IN SAFE TO IMPROVE SECURITY POSTURE

SAFE not only tells you what and how big the problem is, but it also walks you through how it will impact your organization & the remediation. It guides them to reach the desired SAFE score according to their plan. This organization leverages SAFE to remediate the most critical gaps that may make your company grab the next headline for the wrong reasons.

4 ASSESSMENT AS PER BANK'S HARDENING POLICY FOR RBI COMPLIANCE

SAFE has its assessment controls defined based on the industry benchmarks such as CIS, STIG, and security guidelines released by the OEMs. It is a standard practice in the BFSI sector to define a baseline security hardening guideline for every unique type of a device/ OS to ensure that the assets connected to the organization's network and/ or containing business sensitive data have the right security controls in place.

SAFE has enabled the organization to define the security assessment policy based on their own baseline security hardening guidelines. This helps them to assess the compliance of each asset across their organization with their guidelines. While doing this, SAFE also alerts if the configuration of any asset changes intentionally or unintentionally through its notification engine in the form of a score drop or rise.

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

Lucideus House
Plot No 15, Okhla Phase III
New Delhi, 110020