INDIA'S BIGGEST PSU BANK MEASURES THIRD-PARTY RISK WITH SAFE

INDUSTRY

Banking and Financial Services

RESULTS

- Security Monitoring For Digital Assets
- Security Incorporated In Digital Transformation
- Asset Wise Security Score Based On Business Criticality
- Group Of Digital Transformation Stack For Security Posture Monitoring

CHALLENGES

- No visibility into the security posture of assets on-cloud
- Lack of quantified view of digital transformation stack on hybrid cloud

THE NEED

Identification and Analysis: The risk of incorporating a large network of third-parties as a part of critical business functions. The paper-based analyses were human-intensive and a point-in-time assessment that itself provides lesser confidence on the overall risk posture's effectiveness and accuracy. The need was to move forward to an ecosystem that enables this organization to identify the security posture of their third-parties to evaluate the risk posture in real-time.

ON-GROUND EXECUTION CHALLENGES

Budgetary constraints and labor intensive manual processes forced the organization to carry out 3rd party risk assessment of only the top 10-15% of their list of vendors/ third-parties to see how secure they are. The traditional approach of Spreadsheets and ad hoc questionnaires failed as stopgaps, resulting in outdated data and widening information gaps. There was no ability to validate the information given by the vendors and provide them the accurate security requirements to increase their security posture to decrease the overall risk posture

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. Asset grouping as per business requirements
2. Score per asset, per group
3. Remediation guidelines in SAFE to improve security posture
4. Identification of publicly exposed data on deepweb/ darkweb

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 IDENTIFICATION OF PUBLICLY EXPOSED DATA ON DEEPWEB/ DARKWEB

SAFE uses Human Intelligence (HUMINT) to quickly recover current breach data within days of the breach occurring. Its unique data cleansing and password cracking process reveal exposed credentials faster and with greater match rates. Not only is our breach database the cleanest, but it also provide the most data of any provider, with context and perspective to make it immediately actionable. SAFE monitors the sensitive information leakage and breach exposures of your organization and third-parties to prevent attackers from gaining entry through compromised credentials.

SAFE helps organizations measure and mitigate enterprise-wide cyber risk in real-time using it's AI Enabled SAFE Platform by aggregating automated signals across people, process and technology to predict the breach likelihood (as SAFE Score) of an organization

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

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

INDIA'S BIGGEST PSU BANK MEASURES THIRD-PARTY RISK WITH SAFE

INDUSTRY

Banking and Financial Services

RESULTS

- Security Monitoring For Digital Assets
- Security Incorporated In Digital Transformation
- Asset Wise Security Score Based On Business Criticality
- Group Of Digital Transformation Stack For Security Posture Monitoring

CHALLENGES

- No visibility into the security posture of assets on-cloud
- Lack of quantified view of digital transformation stack on hybrid cloud

THE NEED

Identification and Analysis: The risk of incorporating a large network of third-parties as a part of critical business functions. The paper-based analyses were human-intensive and a point-in-time assessment that itself provides lesser confidence on the overall risk posture's effectiveness and accuracy. The need was to move forward to an ecosystem that enables this organization to identify the security posture of their third-parties to evaluate the risk posture in real-time.

ON-GROUND EXECUTION CHALLENGES

Budgetary constraints and labor intensive manual processes forced the organization to carry out third party risk assessment of only the top 10-15% of their list of vendors/ third-parties to see how secure they are. The traditional approach of Spreadsheets and ad hoc questionnaires failed as stopgaps, resulting in outdated data and widening information gaps. There was no ability to validate the information given by the vendors and provide them the accurate security requirements to increase their security posture to decrease the overall risk posture

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. Asset grouping as per business requirements
2. Score per asset, per group
3. Remediation guidelines in SAFE to improve security posture
4. Identification of publicly exposed data on deepweb/ darkweb

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 IDENTIFICATION OF PUBLICLY EXPOSED DATA ON DEEPWEB/ DARKWEB

SAFE uses Human Intelligence (HUMINT) to quickly recover current breach data within days of the breach occurring. Its unique data cleansing and password cracking process reveals exposed credentials faster and with higher match rates. Not only is our breach database the cleanest, but also the most exhaustive, with context and perspective to make it immediately actionable. SAFE monitors the sensitive information leakage and breach exposures of the organization and third-parties to prevent attackers from gaining entry through compromised credentials.

SAFE helps organizations measure and mitigate enterprise-wide cyber risk in real-time using it's AI Enabled SAFE Platform by aggregating automated signals across people, process and technology to predict the breach likelihood (as SAFE Score) of an organization

USA (HQ)

Stanford Research Park
3260 Hillview Avenue
Palo Alto, CA 94304

INDIA

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