



Business challenge

As cyber-attacks were no longer a question of ‘if’, but ‘when’, Bank Mandiri needed to reinvent their security platform with cyber resilience solutions. The bank wanted to have a set of “future-proof” technologies that would allow them to stay ahead of the ‘when’.

Transformation

Bank Mandiri leveraged IBM resilience and security solutions to mitigate the impact of cyber disruptions. The teams worked together to go live in just 7 months with the best in class Security Operation Center capabilities. By doing so, Bank Mandiri improved their ability to detect, isolate and recover, setting a new standard for the security landscape in Indonesia.



Rico Usthavia Frans
Bank Mandiri

Rico Usthavia Frans,
Director of Technology
and Operations,
Bank Mandiri

Results

Improved ability to respond and recover from disruptive events

leveraging IBM Business Continuity and Disaster Recovery services

Rapid detection of advanced security threats

in the network with real-time analytics using IBM Qradar SIEM

Implemented a holistic cyber resilience framework

with enhanced skills and expertise to prepare for critical service disruptions and disaster recovery before they happen

Bank Mandiri

Ensuring cyber resilience with IBM for business continuity

Bank Mandiri was established on 2 October 1998, as part of the bank restructuring program of the Government of Indonesia. In July 1999, four state-owned banks - Bank Bumi Daya, Bank Dagang Negara, Bank Exim and Bapindo - were amalgamated into Bank Mandiri. The history of these four banks can be traced back to over 140 years, and together they had contributed to the beginning of the Indonesian banking sector.

Today, Bank Mandiri's IT infrastructure provides straight through processing and a unified interface for customers. In line with the bank's vision, they tapped into profitable business segments with growth potential so as to offer a comprehensive range of banking services. They chose to focus on key segments including corporate, commercial, micro, retail and consumer finance - with distinctive strategies for each business while leveraging on synergies across these different market segments.

“We need access to the best skills and solutions to protect our clients against increasing cyber threats.”

- Rico Usthavia Frans, Director of Technology & Operations, Bank Mandiri

Share this



Staying ahead in the security landscape with “future-proof” technologies

Bank Mandiri needed to address quickly the twin challenges of security related skills within the Bank as well as having a set of “future-proof” technologies that would allow the Bank to stay ahead in the security landscape.

While the IT team in the Bank had access to dashboards with red, amber and green indicators, many of the team members did not know how to respond or address the root causes when issues came up. Secondly, in the digital era where digital money moved at sub micro-second speed, the ability to put in place a set of work processes, supported with leading edge technology, was of paramount concern.

The challenge for the Bank was to put in place the best security and business continuity posture in a very short time.

Cyber resilience enabled with IBM solutions

Bank Mandiri needed a holistic cyber resilience approach that used leading edge technologies and best practices to meet the increasing threat of cyber disruption.

They teamed up with IBM on a strategic partnership around key areas which included managed Security Operation Center (SOC), internet of things (IoT) as well as long term skills and knowledge transfer. The undertaking required a lot of effort from both the Bank and IBM because an SOC deployment required deliberate planning. From the inception of the partnership, both teams from the Bank and IBM rallied around a common goal and objective with passion and commitment -- To ensure the success of the project.

IBM provided solutions which included IBM Resilient as incident response platform, IBM X-Force for threat intelligence. IBM Qradar SIEM was deployed to rapidly detect advanced security threats in the network with real-time analytics.

IBM also provided the skills and expertise needed to help Bank Mandiri put in place a holistic program and framework within the organization to improve the Bank’s ability to detect, isolate and recover, and to better protect against the rising frequency and severity of cyber-attacks.

Leveraging sensors, advanced

security software, AI and Machine Learning (ML), the Bank hopes to lead the industry in this area of cyber resilience.

Preparing today for the cyber threats of tomorrow

Leveraging IBM’s expertise and know-how to bring best in class capabilities, Bank Mandiri is now progressing to Chapter 2 of their transformation journey. The journey to “future proof” Bank Mandiri’s security posture continues in the face of today’s growing sophistication and increasing frequency of cyber-attacks.

The future of these attacks will no longer be “human” triggered but by self-learning technology as it matures. Through the deployment of an SOC and its ongoing partnership with IBM, Bank Mandiri is in a better position to tackle the cybersecurity challenges ahead of them.

Solution components

[Cyber Resilience Services](#)

[Business Continuity Consulting](#)

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner or visit the following website: ibm.com/services



© Copyright IBM Corporation 2019. Produced in India, July 2019. IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml. This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.



Please Recycle

