— CASE STUDY

2024

rewterz

A LEADING BANK OVERCOMES A SECURITY BREACH AND FORTIFIES THREAT DETECTION WITH REWTERZ

JUNE 2024

OVERVIEW

In the early hours of a cool autumn morning, a cyber attack was detected by a major Pakistani financial institution's security system. With the Bank's server, banking app and email server affected, the malicious attack was not severe enough to steal sensitive data or cause financial loss, but it was impactful enough to make the Bank's team take notice, and to cause disruption in the organization's regular processes. Immediate steps were taken to isolate the affected system before the strike could evolve into a protracted attack.

Rewterz was swiftly engaged to mitigate a security breach of the Bank's network. The financial institution utilized Rewterz's expertise to fortify its security posture, ensuring that future attacks would be repelled.

Rewterz harnessed CrowdStrike and an emergency incident response team to minimize the breach's effects on the Bank's assets. They also analyzed the Bank's existing cybersecurity controls to assess their effectiveness and carefully selected additional solutions accordingly.

Thanks to the implemented measures, the Bank now boasts a strong security posture, fortified with round-the-clock monitoring to fend off cyber threats and mitigate risks. The Bank has also streamlined its processes, enabling swift detection, response, and recovery from security incidents, thereby minimizing their impact and downtime.

ABOUT THE COMPANY

The Client, a commercial bank, headquartered in Karachi, Pakistan, and operates over 1500 branches across the Country. The Bank currently has a presence in over 15 Countries.

THE CHALLENGE

Faced with a security breach, the Bank was confronted with a potential loss of data and subsequent loss of reputation - two highly undesirable outcomes for any organization. With part of its system disabled, the Bank could also be prevented from disbursing salaries for thousands of public sector employees.

The institution required a proactive partner with a mitigation plan to reduce the severity of the breach. The Bank also needed a partner with cybersecurity expertise to ensure that a breach never happened again.

Rewterz was selected by the Bank as a cyber security services provider because of their responsiveness, comprehensive security offerings, and years of cybersecurity experience, particularly in the financial sector.

THE TARGETS

The services focused on delivering:

1. Enhanced security measures:
The client bolstered their defenses against cyber threats, making them less vulnerable and lowering the chances of security breaches.

2. Quick and effective response to incidents:
The client optimized their processes for identifying, addressing, and recovering from security breaches, minimizing any negative effects and downtime.

3. Strong safeguarding of data:
The client ensured that sensitive data was protected from unauthorized access, disclosure, or theft.

THE SOLUTIONS

Rewterz experts swiftly resolved the bank's breach. To prevent similar incidents from occurring again, the Rewterz team undertook a **cyber security gap analysis** to identify gaps in Bank's cybersecurity program. A more effective Incident Response (IR) process was then redesigned and implemented to detect and respond to threats in-time. A **vulnerability assessment and penetration testing** was also conducted to identify and patch vulnerable assets.

Based on the nature of the attacks, Rewterz implemented a Security Operations Center (SOC) to continuously monitor and analyze security incidents. Rewterz's **SOC-as-a-Service (SOCaaS)** fulfills a Bank's round-the-clock monitoring requirements. The system is also indispensable in instantly alerting its stakeholders to cyber attacks as soon as they are detected, ensuring swift action to be taken.

THE TECHNOLOGIES

rewterz XDR

CROWDSTRIKE

THE RESULTS

6796 alerts analyzed
659 incidents handled
52 use cases developed
44.7 minutes mean incident time

Event Management and Security Automation Solutions streamlined monitoring, threat detection, and response, enabling faster interventions and allowing staff to address other critical tasks.

Improved business continuity and brand reputation resulted from swift security interventions.

Efficiency improvements resulted from automating critical cybersecurity processes and orchestrating incident response playbooks.

Cost Savings resulted from the proactive preventative measures that reduced downtime and helped avoid costly data breaches.

THE IMPACT

Once engaged, Rewterz responded swiftly to address the security breach. The team thoroughly investigated and analyzed the attack on the Bank's systems, contained and responded to the incident, and recovered the affected systems. Incident response gaps were eliminated through Rewterz SOC as a Service (SOCaaS) implementation at the Bank.

Rewterz SOC team that never sleeps ensures the Bank's security operations. Security automation and threat intelligence processes have been tailored to the organization for enhanced security operations and reduced incident response time. Amidst a steady rise in cybersecurity threats to financial institutions, the Bank is equipped with cutting-edge security solutions that proactively ensure protection.

WHY REWTERZ?

Recognized as "Outstanding in SMB Support" in the 2023 KuppingerCole Market Compass Report for SOCaaS for the UAE and ranked among the top 250 Global MSSPs list for 2022 by MSSP Alert, Rewterz offers unparalleled 24/7/365 monitoring, detection, and response services. Our commitment ensures businesses of every size are protected around the clock. Harnessing our advanced, risk-based XDR and SIRP platforms and intuitive low-code automation playbooks, our experts craft bespoke detection and response strategies with precision.

Furthermore, specializing in comprehensive, agile solutions that enable seamless integrations, proactive incident management, and enhanced cyber defenses, we improve the effectiveness of your existing SOC, ensuring robust cybersecurity management.

For more information, visit https://www.rewterz.com/.