maltiverse
Actionable Threat Intelligence

CASE STUDY

Transforming Security in International Banking with Maltiverse Threat Intelligence

CHALLENGE

In the dynamic world of international banking, confronting cybersecurity threats has become a top priority. A global leader in the banking sector was facing significant challenges in early threat detection and effective incident response. The complex and sophisticated nature of cyber attacks targeting financial institutions required a solution that could not only detect these threats early but also respond to them swiftly and efficiently.

SOLUTION

The integration of Maltiverse Threat Intelligence marked a paradigm shift for the bank's security. Maltiverse provides a threat intelligence platform that gathers, enriches, and analyzes indicators of compromise (IoCs) from multiple sources, offering a detailed view of the threat landscape specific to the banking sector. This allowed the bank to identify and analyze threats aimed specifically at its operations, significantly improving its detection and protection capabilities. Enhancement in Detection and Protection Capability

WITH MALTIVERSE, THE BANK WAS ABLE TO:

- Proactively identify emerging threats and targeted attacks.
- Enrich security data with contextual information about threats, improving detection accuracy.
- Automate the correlation of IoCs with internal security events, speeding up the identification of potential incidents.

OPTIMIZATION OF SOC RESPONSE PROCESSES

The integration of Maltiverse with SOAR solutions enabled the bank to automate responses to security incidents, significantly reducing response time. This was achieved through:

- Automation of intelligence gathering and data correlation, freeing up valuable SOC resources for critical tasks.
- Implementation of customized incident response playbooks, which trigger automatic actions such as isolating compromised systems and communicating with affected teams.
- Improved collaboration among security, IT, and operations teams, ensuring a coordinated response to incidents.

RESULTS

The adoption of Maltiverse Threat Intelligence transformed the bank's ability to face the cyber threat landscape. The results included:

- A 40% reduction in threat detection time, allowing the SOC to act preventively rather than reactively.
- Improved efficiency in incident response processes, with a 50% reduction in response time.
- Increased ability for the bank to anticipate targeted attacks, thanks to deep and contextual analysis of threat intelligence.

CONCLUSION

The integration of Maltiverse Threat Intelligence into the security strategy of a major international banking client proved to be crucial in enhancing threat detection and optimizing SOC response processes through automation with SOAR. This proactive and automated approach to cybersecurity not only improves the bank's security posture but also ensures the protection of its assets and the trust of its customers in an increasingly threatening environment.