THREATQUOTIENT

البنك السعودي للاستثمار
The Saudi Investment Bank

CUSTOMER SUCCESS STORY

The Saudi Investment Bank Makes ThreatQ the Core of its Threat Intelligence Program

To overcome the universal challenge of operationalizing threat intelligence, Saudi Investment Bank (SAIB) based its cyber threat intelligence strategy on a centralized platform that would allow it to proactively mitigate risk.

Challenge

The Saudi Investment Bank (SAIB) faced two primary challenges with respect to threat intelligence — being able to use it to proactively prepare for and prevent attacks they were seeing in the wild, and ensuring compliance with SAMA and government regulations that required a complete threat management program. Charged with helping to lead the execution of a three-year strategy to address both challenges, Ayman Al-Shafai, Head of Security Operations Center for SAIB, wanted to take a threat-centric approach to security operations.

Learning from the pitfalls he had seen other organizations face, Ayman knew that they needed to mature the program to address the digitalization initiative and align with SAIB's strategic direction. The most effective path forward would be to start with a platform that could help them gain better visibility into the threat landscape for analysis and action, dynamically enhancing their security controls to protect and prevent potential threats and provide secure services to their customers. Like most organizations, SAIB had access to vast amounts of threat intelligence to analyze and make actionable. Therefore, they needed a centralized platform to help them aggregate, curate and share intelligence across several teams and provide reports to support strategic, tactical and operational decision making.

Solution

Before initiating a thorough evaluation of the solutions available in the market, SAIB identified the following success criteria:

- Intuitiveness, meaning it is easy for threat intelligence analysts to learn and use the tool and share information in a format that is simple for other teams to use.
- Compatibility with standards, such as STIX and TAXII, which are extremely important to the ability to import and aggregate threat intelligence into a platform.

"Achieving compliance is important, but we wanted to go beyond checking boxes and truly utilize and benefit from threat data. We needed a deeper and better understanding of the threat landscape — the who, what, how and relevance to SAIB — so we could proactively mitigate risk to our customers and the organization."

– Ayman Al-Shafai, Head of Security Operations Center, SAIB

OVERVIEW

INDUSTRY: Financial Services

CUSTOMER SINCE: 2019

EMPLOYEES: 1,437*

TOTAL INCOME: 2.9 Billion SAR*

LOCATION: Riyadh, Saudi Arabia

CHALLENGE

Proactively prepare for and prevent attacks in the wild and ensure compliance with the Saudi Arabian Monetary Authority (SAMA) and government regulations.

SOLUTION

As a centralized platform to aggregate, prioritize and share intelligence across teams; foster collaboration; and enrich all SAIB's security tools and technologies with IOCs and related actionable intelligence, ThreatQ provides a deeper understanding of threats and enables faster and automated actions.

OUTCOME

- ✔ More informed business decisions
- ✔ Reduced alert fatigue and increased analyst productivity
- ✔ Proactive detection and minimized time to respond
- ✔ Streamlined operations and better ROI on security infrastructure

*SAIB Integrated Report 2019

- Integration with various, different security solutions so that investigations and preventive actions can be performed from the platform instead of having to move between multiple solutions, reducing time to detect and resolve cyber incidents.
- Prioritization to understand which threats matter most to the organization and reduce alert fatigue.
- A strategic partnership and level of engagement that ensures issues are prioritized and resolved quickly.

SAIB determined that ThreatQuotient and the ThreatQ platform met all the criteria and was most aligned with their needs.

Working with ThreatQuotient's Professional Services team, within the first six months the bank deployed the ThreatQ platform and integrated it with a majority of the security controls within their ecosystem. They also completed integration with a range of threat data sources including multiple commercial and open source intelligence feeds as well as national CERT information and MITRE ATT&CK.

SAIB's strategy to initially focus on using ThreatQ to understand the broader, dynamic threat landscape quickly began paying dividends. Ayman shares, "With threat intelligence, you can feel like you're looking at random pieces of a jigsaw puzzle. But now, if we observe something within our technology infrastructure and bring it into ThreatQ to correlate it with other relevant data, we can put the puzzle pieces together, take that intelligence further for corrective action and share it more broadly."

With threat intelligence management as a solid foundation, SAIB is using ThreatQ Investigations to achieve additional key objectives, such as incident response and threat hunting. "Visualizing and connecting the dots to identify indicators and attack patterns with ThreatQ Investigations is extremely beneficial for accelerating a comprehensive response and preventing similar attacks in the future," Ayman explains.

The threat intelligence team is also collaborating with different teams within the bank to support various levels of activities. For example, sharing actionable intelligence to help protect against fraud and support risk management, as well as providing reports to support strategic initiatives such as digitalization.

"The ThreatQ platform is at the core of our threat intelligence program, helping us gain a deeper understanding of different threat actors so we can actually predict what may happen, rather than be in reactive mode and firefighting all the time."

– Ayman Al-Shafai, Head of Security Operations Center, SAIB

Outcome

More informed business decisions

ThreatQ reports, delivered in language that resonates with business leaders, allows senior management to make more informed business decisions and take specific actions. For example, ensuring any security gaps are addressed as new services are designed and prepared for launch to customers.

Reduced alert fatigue and increased productivity

As a centralized platform for data aggregation, correlation and prioritization, ThreatQ reduces false positives and allows analysts to focus on what matters. The ability to take corrective action directly from within the platform allows analysts to handle more incidents and be more productive.

Proactive detection and accelerated response

Collaboration during the investigation process, sharing of intelligence with other teams and integration with existing security tools and controls enables SAIB to leverage ThreatQ to optimize threat management, incident response, threat hunting, fraud management, vulnerability management and risk management.

Integration with security infrastructure to streamline operations and increase ROI

Bi-directional integration enables cyber defense teams to quickly act on threat intelligence, allows the ThreatQ platform to serve as organizational memory and continuously learn and improve, and enhances the value of all security investments.

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA. For more information, visit **www.threatquotient.com**.