PRODAFT

CASE STUDY

THE USAGE OF OUR NEXT-GEN THREAT INTELLIGENCE SOLUTION BY A 24/7 SECURITY OPERATIONS CENTRE (SOC) PROVIDER

Industry: IT

Region: MENA Region

Challenge: Incident Examination Involving a Compromised Database Information

Who is the Client?

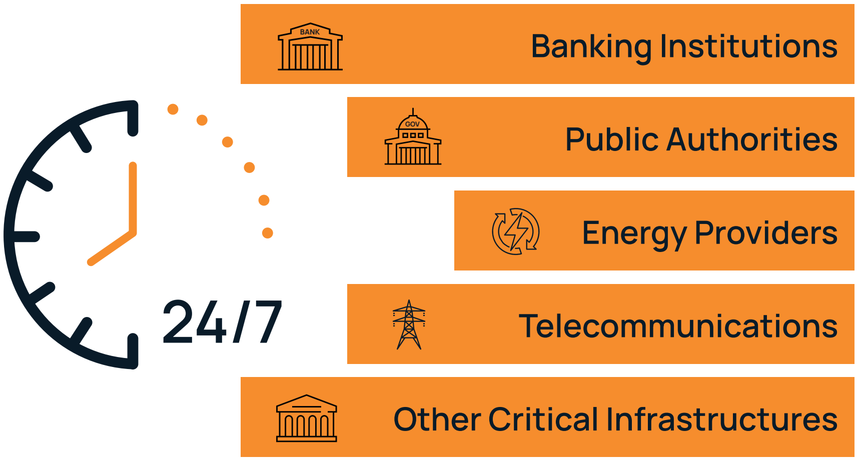
One of the leading IT companies in the MENA region with;

80 years of business experience

2’000+ employees

80+ international partnerships

The organization’s 24/7 security operations center (SOC) provides critical infrastructure to banking institutions, public authorities, energy providers, and telecommunications companies, among others.



The organization’s 24/7 security operations center

The SOC provider identified PRODAFT’s U.S.T.A. threat intelligence platform as an appropriate solution for proactive defense against evolving cyber threats.

What Were Their Main Challenges?

The SOC provider found out their endpoint central database (a management and security software that helps to manage all IT operations, networks, software, and applications) had been seen on one of the underground platforms.

They sought to understand what happened, if the data was real and who was behind the incident. Moreover, they wanted to be sure that they had a full understanding of how such incidents can take place and what needs to be done to ensure the organization's security won't be compromised or threatened in the future.

Why Did They Reach Out To Us?

Considering their situation and the nature of our work in such cases, they identified our **U.S.T.A.** Threat Intelligence platform as an appropriate solution for proactive defense against evolving cyber threats. As they were already familiar with our services and expertise, they knew we were the right fit under these circumstances.

What Was The Solution?

1 Firstly, we investigated the case and conducted extensive OSINT and HUMINT to find out who was behind the incident and how it occurred. We sent all the gathered data to the SOC provider for cross-checking, figuring out the leaked data was real, which was later confirmed as positive.

2 Secondly, to help the SOC provider understand all in-and-outs of the case, we prepared a final tactical report for them. In the report, we shared detailed information about the whole case including future mitigation and security recommendations.

What Was The Outcome?

After the SOC provider faced a critical incident when their data leaked, we conducted a thorough operation by investigating the adversarial infrastructures and investigating what had happened.

With our help, the SOC provider was able to understand their own security situation and how to prevent any sort of potential breaches in the future.

Do you want to learn more about how we can help you to prevent breaches and ensure your sensitive data won't be compromised?

Then do not hesitate to contact us to learn more about our cyber threat intelligence solutions and their role in your organization's safety.