threatdefence_

CASE STUDY

A GLOBAL CRYPTOCURRENCY TRADING FIRM PROTECTS THEIR ASSETS WITH CYBER SECURITY SERVICES FROM THREATDEFENCE

The global adoption of cryptocurrency makes cryptocurrency trading firms an extremely attractive target for the most sophisticated cybercriminals in the world. To defend against such threat actors, such organisation should establish and operate an ongoing 24x7 Security Operations capability for continuous monitoring, threat detection, and rapid incident response.

ThreatDefence's Client is a global cryptocurrency trading firm with offices around the world. The Client requested ThreatDefence to assist with the security monitoring and incident response, as well as provide an ongoing management of the cybersecurity for the organisation.

The services provided by ThreatDefence include:

- Ongoing management of the Client's cyber security
- Implement a centrally managed and monitored Advanced Endpoint Protection solution
- Implement and operate an ongoing Managed Detection and Response capability, covering all client assets through ThreatDefence's Security Operations Centre
- Develop advanced threat hunting and threat detection use cases.

"Considering the nature of our business, we are continually being targeted by motivated threat actors. ThreatDefence provides us with a great and practical approach to tackle out cyber security challenges, while having tailored technology and dedicated personnel helps us to mitigate even the most advanced and persistent threats. "

- CEO, Global Cryptocurrency trading firm

ThreatDefence provided an integrated cyber security solution tailored to the Client's unique cyber security challenges and risk factors. ThreatDefence completely redesigned the environment to ensure that the most advanced security controls are implemented to address the unique security risks of the Client. ThreatDefence has been supporting the Client to implement advanced cyber security capabilities, such as:

- **Advanced Endpoint Protection**
  ThreatDefence provides a comprehensive suite of Advanced Endpoint Protection (AEP) solutions, supported by our Security Operations Centre. The capability involved deploying sophisticated endpoint protection software on all firm endpoints, augmented by the custom detection use cases specifically developed for the Client.
- **XDR Platform**
  Our XDR Platform provided the Client with full cycle detection, investigation and response across all user endpoints, servers, cloud workloads, purpose-built applications, Dark Web

breaches, compromised credentials, external vulnerabilities and weaknesses and exposures related to third-party organisations in the supply chain. Connecting all security data into a single platform provided great visibility, unmatched threat detection perspective, and establishes detailed context for proactive threat hunting and rapid incident response.

- **24x7 Security Operations Centre and Managed Detection and Response**
  ThreatDefence pairs our cyber security technology with trained and experienced security specialists working continuously to deliver true cyber defence capabilities for the Client. Our expert threat hunters gained insights from the collected security data, deep diving into any anomalies, suspicious events, and any unexpected behaviours observed on your network. Through the ongoing threat hunting, ThreatDefence was not only able to find previously undetected threats, but also enhanced our detection capability by adding new rules and fine tuning the platform to stay ahead of attackers.
- **Behavioural Analytics**
  ThreatDefence used advanced Machine Learning and User Behavioural Analytics to identify anomalies and suspicious behaviour in the environment. Equipped with the deep understanding and knowledge of the environment, ThreatDefence was able to build the model to baseline the normal user and machine behaviour and detect any deviations in real time.

With the ongoing Security Operations and MDR services from ThreatDefence, our Client is protected even from the most sophisticated targeted attacks.

ABOUT THREATDEFENCE_

ThreatDefence provides innovative MDR, SOC-as-a-Service, and proactive cyber defence solutions to MSPs and Enterprises. Our Adaptive XDR Platform was created to help companies of any size to deploy a world-class detection and response, embracing all information that businesses can reach to, would it be within their network, on the Dark Web, or hiding deep into their supply chain. We believe in open ecosystems and connect you to any and all threat intelligence feeds and log sources, instantaneously providing you with actionable security insights. For more information, visit www.threatdefence.com.