

Leading Not-for-Profit implements Secure Operations Centre (SOC) as a Service & builds for the future



Background

Enablis' network & security experts worked with a leading Not-for-Profit to deploy XDR and SOC as a Service (powered by Palo Alto Networks) to provide 24x7 alerting & monitoring, proactive threat hunting and response capabilities.

Objectives and Outcomes

- To enhance the organisation's security posture and meet regulatory requirements.
- Meet the Notifiable Data Breach (NDB) schemes reporting requirements.
- Consolidate detection and response within a single platform (endpoint, network, identity and cloud).
- Service Level Agreements for Detection (MTTD) and Resolution (MTTR) timescales.
- Ability to report key metrics to the Board.

The Solution

Deployment of Cortex XDR and a SOC to save costs, effectively detect & respond & gain better reporting



Business Benefits

- Increased visibility through constant cloud, identity, network, and endpoint monitoring.
- Deployment of Managed Incident Response, Threat containment and remediation.
- Defined Service Level Objectives (MTTD < 1 min, MTTR < 60 mins).
- Reduced false positives by drawing upon detailed data enrichment for context and decision-making.
- Built cyber-resilience and Security Posture Optimisation for the NFP.
- Created security reporting & executive level security reporting.
- Overcome talent challenges - attraction, retention of scarce resources.
- Adoption of a proactive approach to cybersecurity.
- Policies are now set up to prevent as much as possible & provide the ability to detect and respond in a timely manner.

BENEFITS WORKING WITH ENABLIS

- Enablis were able to stay within budget and achieve the timelines and objectives set.
- The team of security & networking experts met the requirements of the organisation.
- Enablis were able to design a solution to ensure the NFP would meet regulatory requirements.
- Enablis has provided enhanced security visibility to the IT team and board to ensure reporting metrics are met.



"Partnering with Enablis to deploy Cortex XDR and establish a SOC isn't just about fortifying defenses—it's about empowering our organisation with continuous vigilance, centralised insight, and a fortified alliance against cyber threats to ensure visibility and a resilient operation."