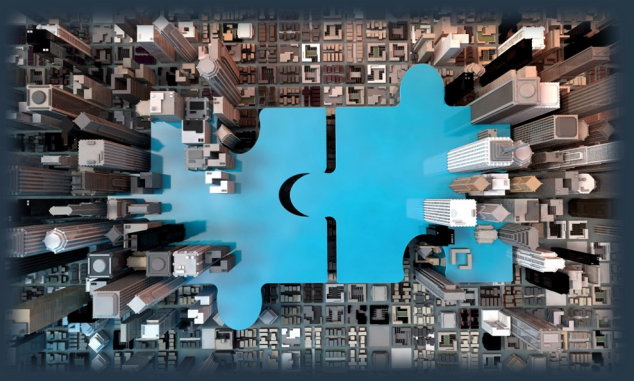
CASE STUDY

Increasing Cyber Security Threat Protection with Brace168's Managed Detection and Response

The Company

As one of the largest Australian property groups, this client's extensive data contains significant, valuable information that serves as their fundamental core asset.



Since the company has diverse interests ranging from commercial and retail to residential assets, they had critical information stored across many different platforms, all with varying levels of modernity and security.

As a result, the entire organisation was susceptible to cyberattacks. Even when they became aware that they needed to take action to address this, the client did not know where to even start and what was required.

With this range of commercial interests and data usage, having a consolidated understanding of all activities and eliminating the risk of cyber security threats posed a great challenge for this company.

Customer Scenario

The company had already suffered a significant number of cyber incidents – each becoming more sophisticated, and increasing the ongoing threat to their information assets.

While the company had already implemented traditional security measures, these solutions left vulnerable gaps for new and unknown threats.

The Solution

Brace168's managed detection and response (MDR) service, B-Compliant, was implemented to monitor all activities across all of the client's core systems to provide proactive, targeted and relevant alerts, together with clear steps for incident response.

This gave the company a more comprehensive cybersecurity posture, allowing the Board to feel reassured that cyber risks were being managed and their valuable assets were secured and protected.

Requirements

- Inform overall security governance.
- Obtain real-time, sufficient visibility of potential threats in the technical environment.
- Design an appropriate and accurate 24x7 threat monitoring strategy.
- Implement a RACI model and ensure local collection and storage of data.
- Use data to get visibility on all infrastructure including network devices, endpoints, productivity applications and their ERP platform.
- Analyse the huge volume of data available to detect and prevent genuine security events.
- Get timely incident notifications backed by efficient escalation procedures.
- Understand underlying security trends with tailored dashboards.
- Have a commercial model aligned to the value of the service, not the volume of data managed.

How does it work?

Brace168 delivered the solution in the form of the following:

Discovery and Setup:

At Brace168, we designed a responsible, accountable, consulted and informed (RACI) model for the engagement. From there, our team commenced the analysis of the existing Cyber Security strategy and provided recommendations for making security alerts more proactive, visible and relevant.

We also built and configured log gateways within the company's environment to securely transport event logs into the Brace platform. Finally, we designed tailored dashboards to gather security risk insights for the range of log types.

SIEM/SOAR with MDR Services via Elasticsearch, Kibana Dashboards and Logstash:

This solution has the following features:

⇒ 30 days of storage and retention for short-term investigatory capabilities

⇒ 365 days of archived logs within a secured data centre

⇒ Secured storage services located in Australia for dedicated infrastructure

⇒ Parse logs for data ingestion, including rare log types from the ERP system

Incident and Response Services:

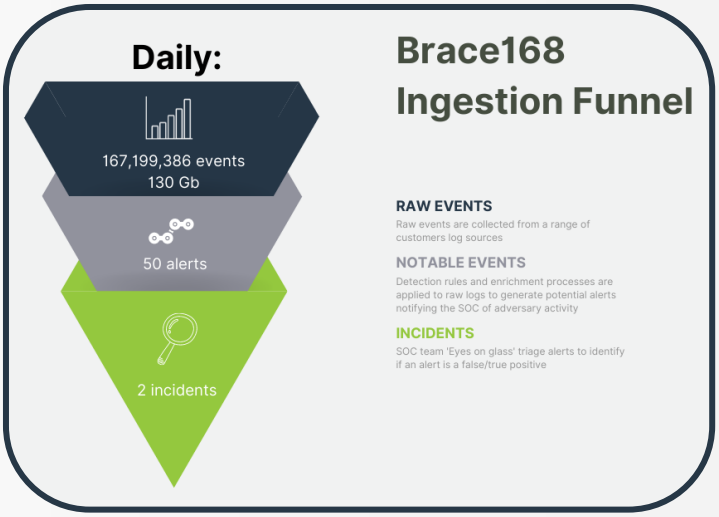
Brace168 also provides 24x7 monitoring for the client, as well as the following:

⇒ Service Level Agreements aligned to the company's requirements

⇒ ServiceNow integration for security incident ticketing

⇒ SLACK integration for team alerts and collaboration around incidents

The customised approach of the Brace168 offering meant that this client's cybersecurity and budget requirements were both met, with a solution based on the value provided by the analysis of company data to alert about relevant incidents rather than simply on the volume of data.



Brace168 empowered the client with assurance and security

The Outcome

Since the implementation of **B-Compliant,** cyberattacks against the company have been reduced by 90%, with the system detecting potential threats. 500+ alerts and notifications were received in the first few weeks of operation, and were all addressed with the efficient escalation protocol in place.

Not only did the solution effectively increase security, but it also created a way to boost efficiencies for the organisation. Recording an increase in overall operational efficiency, the client is more than pleased with the security and assurance provided by the Brace168 platform and team of specialists.

Brace168 SOC

⇒ 24 x 7 Capability

⇒ Data sovereignty - 4 Point of Presence via Data Centres in AU, US and UK

⇒ Full integration to customer ticketing processes

⇒ Readily adaptable and scalable solution, our facility expanded three times since 2017

⇒ Data Centres SOC2, ISO27001 and HIPPA compliant

ISO27001 and CREST certified, Brace168 delivers industry best practice cyber security services