



INCIDENT RESPONSE

Data Breach

Situation

An Australian IT Consultancy contacted Skurio suspecting that a threat actor had gained unauthorised access to their systems.

Task

The analyst team were tasked to identify if there was any historic indication that they were being targeted, and to verify if the unauthorised access resulted in any data exfiltration.

Action

We conducted a review of all historical posts relating to the impacted company within the our database. No indication or warning of an attack were identified. We created alerts on our DRP platform to monitor in real time any mentions of the business & potentially sensitive information. Notifications were analysed & Intelligence Reports produced.

Result

We received a notification, originating from a hacking forum that the victim's unauthorised access had resulted in exfiltration of sensitive information. We harvested all available breached information. Our Intelligence Report allowed the customer to review the breached information to determine the sensitivity & put measures in place to mitigate future threats included in the breach.