Telstra Incident Response

According to research by IBM, the average cyber breach lifecycle takes 287 days, with organisations taking 212 days to initially detect a breach and 75 days to contain it (Source: IBM Blumira 2022 State of Detection and Response Report).

Despite some progress in detecting an incident or a breach, organisations are still taking too long to respond and contain. In addition, the latest Telstra Security Report suggests a sizeable proportion (24%) either don't have or don't know if they have an Incident Response plan in place. Having the resources and skills to build a mature incident response plan remains the challenge.

How we can help

Telstra Incident Response helps to improve your readiness to efficiently deal with potentially damaging attacks. Provided as a managed cyber security service, we'll give you priority access to Telstra's highly-skilled and experienced Computer Emergency Response Team (CERT).

Our team will respond quickly to minimise any damage of a suspected incident such as:

- Unauthorised or compromised access to your systems.
- Electronic data loss or theft.
- Intentional or accidental introduction of a virus to a network.
- Unauthorised money transfers or payments made through systems manipulation.
- Suspicious network activity.
- Unauthorised installation of hardware on your network.
- A ransomware attack.

We will investigate and analyse your data and logs to identify the cause of the breach and then determine the extent and impact to try and contain the incident. In addition we will provide a report with recommendations to remediate, and then mitigate, against this type of threat occurring again.

For Australian organisations and government agencies, it provides sovereign secure capability and helps with threat response by leveraging the Telstra network and Australian-based security expertise.

Benefits

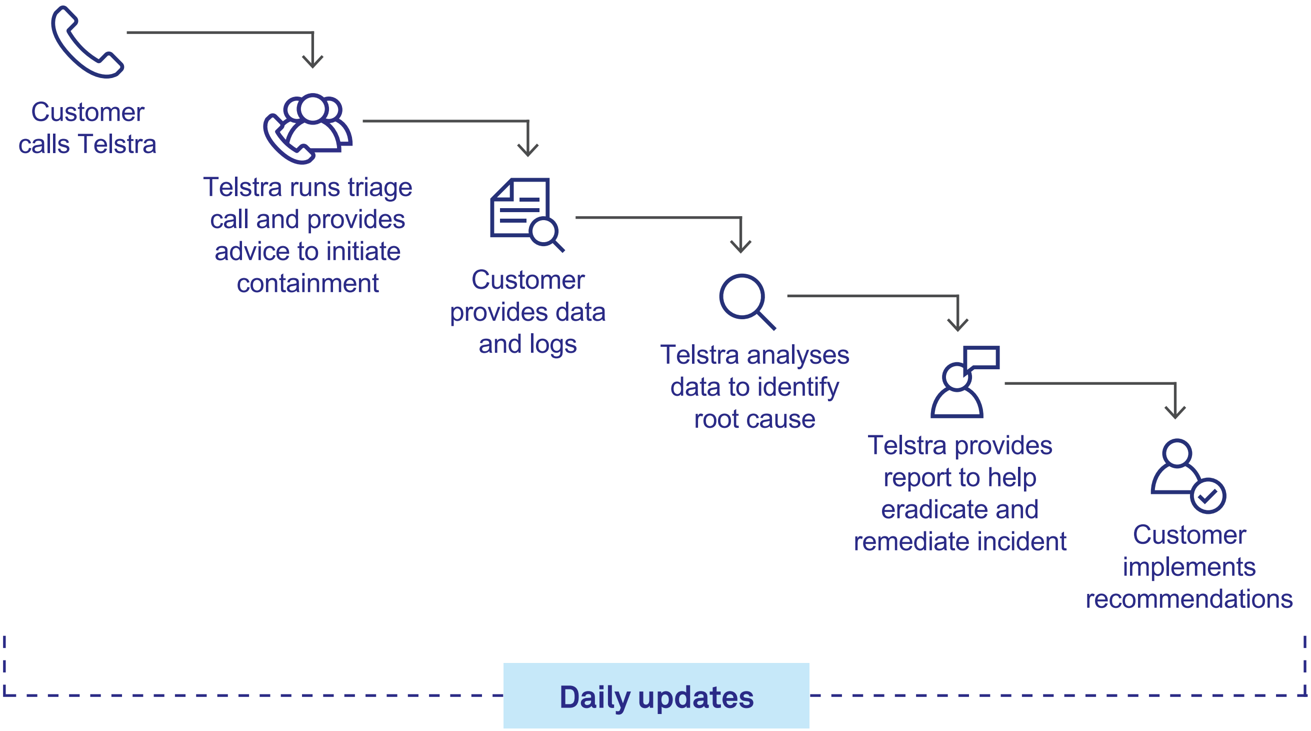
- Expert cyber-security personnel on call 24x7.
- Advanced tools and threat intelligence through our state of the art Security Operation Centre (SOC).
- Retainer-based service provides prioritised response.
- Fast response to reduce disruption to your business.
- Monthly payment option with low up front commitment (retainer entry point is 40 hours).
- Available in three different tier levels depending on your business requirements.
- Peace of mind that your incident will be handled quickly and efficiently.
- Convenience of one solution that covers you globally.
- Suitable for small-mid sized organisations and individual government agencies, all the way up to enterprise, cyber hubs and whole of government.
- Leverages the people, processes and technology that Telstra uses to protect itself, both domestically and globally.

How it works

As soon as you suspect your business has suffered a cyber-attack, simply call our dedicated Telstra phone number. Our team of security specialists will arrange a triage call within an hour to quickly initiate the Incident Response process.

They will commence analysis as soon as you provide the required data, then investigate and provide advice to contain the threat. If you also have our Cyber Detection and Response service we can respond faster as we'll already have access to your logs and an understanding of your ICT environment.

You'll receive daily updates throughout the process, as well as a written report with recommendations to help you put measures in place in an effort to prevent the incident from recurring.



Customer calls Telstra

Telstra runs triage call and provides advice to initiate containment

Customer provides data and logs

Telstra analyses data to identify root cause

Telstra provides report to help eradicate and remediate incident

Customer implements recommendations

Daily updates

What you get

- Target response of one hour from when an incident is reported for triage.
- Commencement of investigation as soon as you provide relevant data and other required information.
- No time is wasted because a single point of contact has already been established.
- Contingency actions can be prepared in advance to better mitigate risk.
- If you have operations overseas, we can help secure them thanks to our comprehensive global coverage and experience.
- You'll be leveraging tools through our SOC to identify and resolve incidents promptly.

Incident Response Tiers Available

Telstra's Incident Response service is a pre-paid block of incident response hours at a discounted hourly rate and available in three tiers depending on your requirements:

- **Essentials** - A single use product to have Telstra on retainer in the event of a major security incident. It provides an annual allocation of 40 hours for a single cyber-security incident, handled by our CERT professionals. If more than 40 hours are required, our experts will still be available to help on an hourly rate. Unused Incident Response hours can be used for other Telstra Purple security consulting services.
- **Advanced** - Offers a service duration of 24 months with a total of 100 retainer hours for the term. It includes a two-day Incident Response Readiness Assessment.
- **Premium** - In addition to the inclusions in the Advanced tier, this is a 36 month incident response package offering a total of 150 retainer hours for the service duration. There is an enhanced four hour SLA to further reduce the incident impact.

Telstra Incident Response Tiers

	Essentials	Advanced	Premium
Online/Phone Support	24 x 7	24 x 7	24 x 7
Service Duration	12 Months	24 Months	36 Months
Hours of work included during Business Hours	40 (single incident)	100	150
Kick off workshop	✓	✓	✓
Quarterly briefing	✓	✓	✓
Annual Executive briefing		✓	✓
Initial Remote Response	Next business day	8 hours	4 hours
Incident Readiness Assessment (for Enterprises)		✓	✓
Onboarding activity (for Government)		✓	✓

Why Telstra for Incident Response?

Access to significant resources to assist with all stages of Incident Response:

- **Preparation** – consultant expertise in advisory, readiness assessments, playbook design, managed services for disaster recovery and backup services
- **Detection** – integrated service with our 24x7 Telstra Security Operations Centres
- **Containment** – access to experienced incident managers, cutting edge EDR technologies, forensic expertise and analysis to determine root cause
- **Eradication** – technical consultants are able to isolate and rebuild
- **Remediation** – expertise across multiple vendor technologies to help return to business as usual
- **Lessons learnt** – our incident responders pull together all the information from the above stages and make clear recommendations to prevent similar incidents occurring in the future

Resources and specialist skills are available nationally for remote work and on-site attendance through Telstra Purple and our extensive partner network.

Contact your Telstra account representative for more details.

Australia

☎ 1300 telstra (1300 835 787)

telstra.com/enterprisesecurity