

Incident Response

Take a proactive approach to cyber security



According to Telstra's 2018 Security Report, 68% of global respondents experienced business interruption due to a security breach at least once over the past year. There was also a sizeable proportion (25% globally) who either didn't have or did not know if their organisation had an Incident Response plan in place. Unfortunately, many organisations don't have adequate resources or skills to deal with these incidents but are looking for ways to reduce the threat to their business and enable a proactive approach to cyber security.

How we can help

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 i.e. wireless access points
- a ransomware attack

We will investigate and analyse your data and logs to identify the cause of 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 specific threat occurring again.

Key benefits

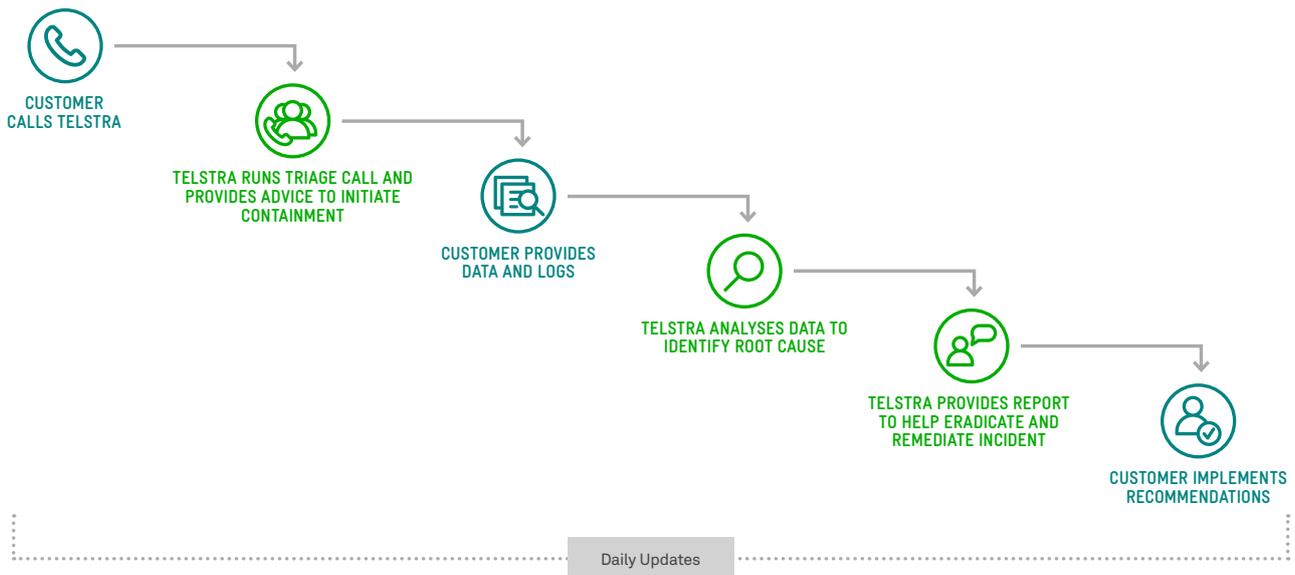
- Expert cyber-security personnel on call 24x7 x 365.
- Advanced tools and threat intelligence through our state of the art SOC.
- Retainer-based service provides prioritised response.
- Fast response to reduce disruption to your business.
- Monthly payment option with low up front commitment (retainer entry point is 40 hours).
- Consulting services to the value of the retainer term (if no incident occurs within the contract period).
- Peace of mind that your incident will be handled quickly and efficiently.
- Convenience of one solution that covers you globally.

How it works

As soon as you suspect that your business has suffered a cyber-attack, simply pick up the phone. Our team of security specialists will be on call to triage, and quickly establish the type and scale of the incident as soon as you provide the required data we will be able to start investigation and analysis (typically within one hour). If you also have our Security Monitoring service, we can respond faster as we will already have access to your logs.

We will promptly provide advice to help contain and eradicate the threat and then provide a written report with recommendations to help you remediate and aim to prevent the recurrence of the threat. You will receive daily updates throughout this process.

If you decide not to subscribe to the retainer service, we'll do our best to support you at an hourly rate, but cannot guarantee prioritised response when you need it.



What you get

For a fixed monthly retainer, you'll receive 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.

- 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.
- If you don't experience an incident within the contract term, you can use the retainer for up to five days of security consulting services.

Complementary Services

If you also subscribe to Telstra's Security Monitoring Service, (another Managed Security Service) we will be able to respond faster to the incident since we will already have access to your logs.

Why Telstra for Incident Response?

Your organisation can benefit from our state of the art Security Operation Centres (SOC) facilities - the foundation of our managed security services by providing the visibility, intelligence and tools needed to manage risk in an evolving threat environment.

Insight and experience: We've been helping businesses manage risk and protect data for decades, while protecting our own network – one of the largest in Australia – for even longer. So we understand the security issues you face. When it comes to cyber-security, we're constantly keeping ourselves up to date with the latest exploitation techniques and solutions to combat them. This includes developing new technologies and techniques to give you better insight into your data, allowing you to make informed decisions about how to manage your risk.

Exceptional people: You can rely on one of the largest and most qualified groups of security professionals in Australia to protect your business. Thanks to our size and scope of operations, we attract the best and brightest in the field.

Local and global intelligence: We work closely with leading security vendors, the Australian Government, and the worldwide security community to provide the latest intelligence on the local and global threat landscape.

The spectrum device and "™" and "®" are trade marks and registered trade marks of Telstra Corporation Limited, ABN 33 051 775 556.

Contact your Telstra account representative for more details.

Australia

📞 1300 telstra (1300 835 787)

🌐 telstra.com/enterprisesecurity

International

📞 Asia +852 2827 0066

🌐 telstraglobal.com

Americas +1 877 835 7872

✉️ tg_sales@team.telstra.com

EMEA +44 20 7965 0000

Australia +61 2 8202 5134