Cyber Detection and Response

In Australia and around the world, there has been a seemingly endless wave of high profile cyber security incidents which have managed to compromise corporations and government agencies.

Research by IBM has found 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). Advanced Persistent Threats, which are long term operations designed to gather as much valuable information as possible without being detected, can go years without being discovered.

The reality is that most businesses find it challenging to implement and maintain the extensive security controls needed to safeguard their systems, customer data and ultimately, their reputation.

How we can help

Telstra Cyber Detection and Response is a Managed Security Operations Centre (SOC) service that monitors a customer's IT infrastructure on their behalf. Analysing web-scale quantities of security event data, the service alerts customers to unusual, suspicious and malicious activity across their environment, triggering an automated response if required.

It utilises Telstra's Australian Security Operations Centres (SOCs); all independently certified in accordance with Australian Government PSPF Zone 4 standards, managed by accredited staff and certified to operate at the 'ISM PROTECTED' level.

For Australian organisations and government agencies, it provides sovereign secure capability and helps with threat visibility by leveraging the Telstra network and Australian-based security expertise. Optional professional services can be bundled to help with subsequent remediation and recovery.

Security events being detected include:

Detection of vulnerabilities that could be exploited, such as:

- Misconfigurations
- Software not up-to-date with latest patches

Break-in attempts, such as:

- Brute-force password cracking
- Attempts to exploit vulnerabilities to gain access to:
  - Accounts on internal systems
  - Data directly, via web application attack
- Phishing emails and messages
- Session hijacking

Suspicious activity within network and IT systems, such as:

- Employee activity that could be suspicious and/or malicious
- Attempts to gain access to data and/or systems
- Attempts to gain access from suspicious locations and/or times of day
- Attempts to implant malware

Possible data theft, such as:

- Uploads of confidential data to external destinations
- Uploads of data to suspicious external destinations

Denial of service attacks

Features

- Advanced security analytics: Utilises big data tools in conjunction with machine learning algorithms to examine anomalies in near real time and highlight malicious activity across your environment.
- Transparent: Using the Cyber Detection and Response portal allows organisations to see what our security analysts see.
- Compliant: Telstra's Australian SOCs are independently certified in accordance with Australian Government PSPF Zone 4 standards. They are also certified to operate at the 'ISM PROTECTED' level, a requirement in protecting Federal Government data.
- Scalable: Suitable for mid-sized organisations and individual government agencies, all the way up to enterprise, cyber hubs and whole of government.

Benefits

- Rapid detection and expert advice to deal with threats including unauthorised or compromised system access, data loss or theft, intentional or accidental introduction of a virus, unauthorised money transfers or payments, suspicious network activity, unauthorised hardware, and ransomware.
- A sovereign secure service that leverages the people, processes and technology that Telstra uses to protect itself, both domestically and globally.
- Telstra has designed and built the platform in-house with the needs of Australian customers at the forefront.
- Support is provided by the Australian-based people who designed and built the platform.
- Provides an at-scale technology platform which can be more affordable than a typical DIY solution.
- Importantly, this service is open to any organisation regardless of whether they are an existing Telstra customer or not.

Why Telstra for Cyber Detection and Response

- The service provides visibility and threat intelligence via one of the largest network footprints across Australia.
- Locally managed: Security is managed around-the-clock in Australia using local Security Operations Centres and expertise.
- Locally developed: Capabilities, features and the product roadmap are designed with Australian customers in mind.
- Experience: Telstra has been trusted to help ensure business continuity and protection for major Australian organisations, from banking and finance to Australian government departments and agencies, for more than a decade.

Optional Services

- **Incident Response**
  Receive priority access to Telstra's highly-skilled Computer Emergency Response Team (CERT) who respond quickly to any suspected incident, such as unauthorised access to your systems, electronic data loss or theft, viruses, suspicious network activity and ransomware attacks.

- **Purple Managed Services**
  Proactive security management by experienced IT professionals with continuous performance monitoring, tuning, automation and analysis of your IT environment. The result is a customised service that is flexible enough to support your evolving business needs.

Contact your Telstra account representative for more details.

Australia

☎ **1300 telstra** (1300 835 787)

telstra.com/enterprisesecurity

International

Channel Partners partners@team.telstra.com

✉ Sales tg_sales@team.telstra.com

2022.09.23 V3 ICC