Telstra

Telstra Cyber Detection and Response

Quickly detect and respond to cyber threats

Managing security risk and resilience in a digital era

As the world bounces back from the pandemic, many organisations are expanding commitments to hybrid working and digital channels, bringing about improved customer experience, business continuity management, and operational resilience. The acceleration of digital transformation offers new opportunities for businesses but also exposes them to new risks as their cyber security attack surfaces expand.

Attackers are also now moving beyond direct attacks to target managed service providers and supply chains, a trend that is compounded by the shortage of cyber security professionals around the world. Consequently, many organisations are looking to managed detection and response services to help control the risks resulting from cyber threats.

Top security challenges across the globe

Financial and tech barriers to entry for internal security operations

A rapidly evolving threat landscape

Attracting and retaining the right talent

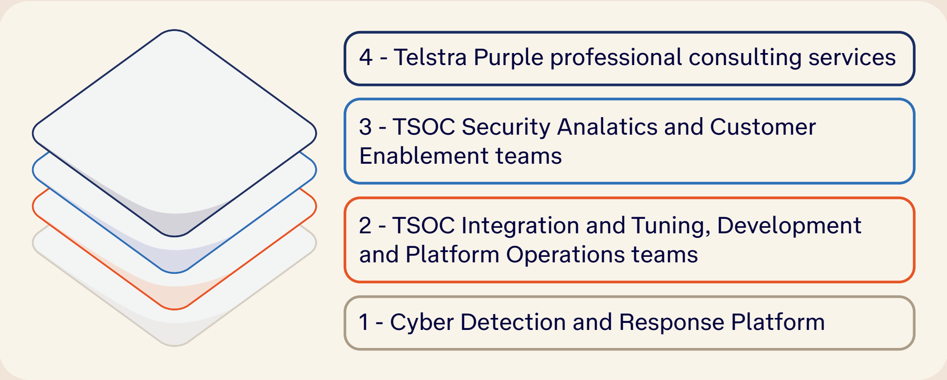
Achieving complete attack surface visibility

Managing disparate alerts generated by security tools

Risk management and compliance

What is Telstra Cyber Detection and Response?

Telstra Cyber Detection and Response provides visibility through detection and notification of security incidents, enabling quick response to minimise damage and operational outage time. The service is powered by the Cyber Detection and Response platform and our Telstra Security Operations Centre (TSOC) teams.


4 - Telstra Purple professional consulting services

3 - TSOC Security Analatics and Customer Enablement teams

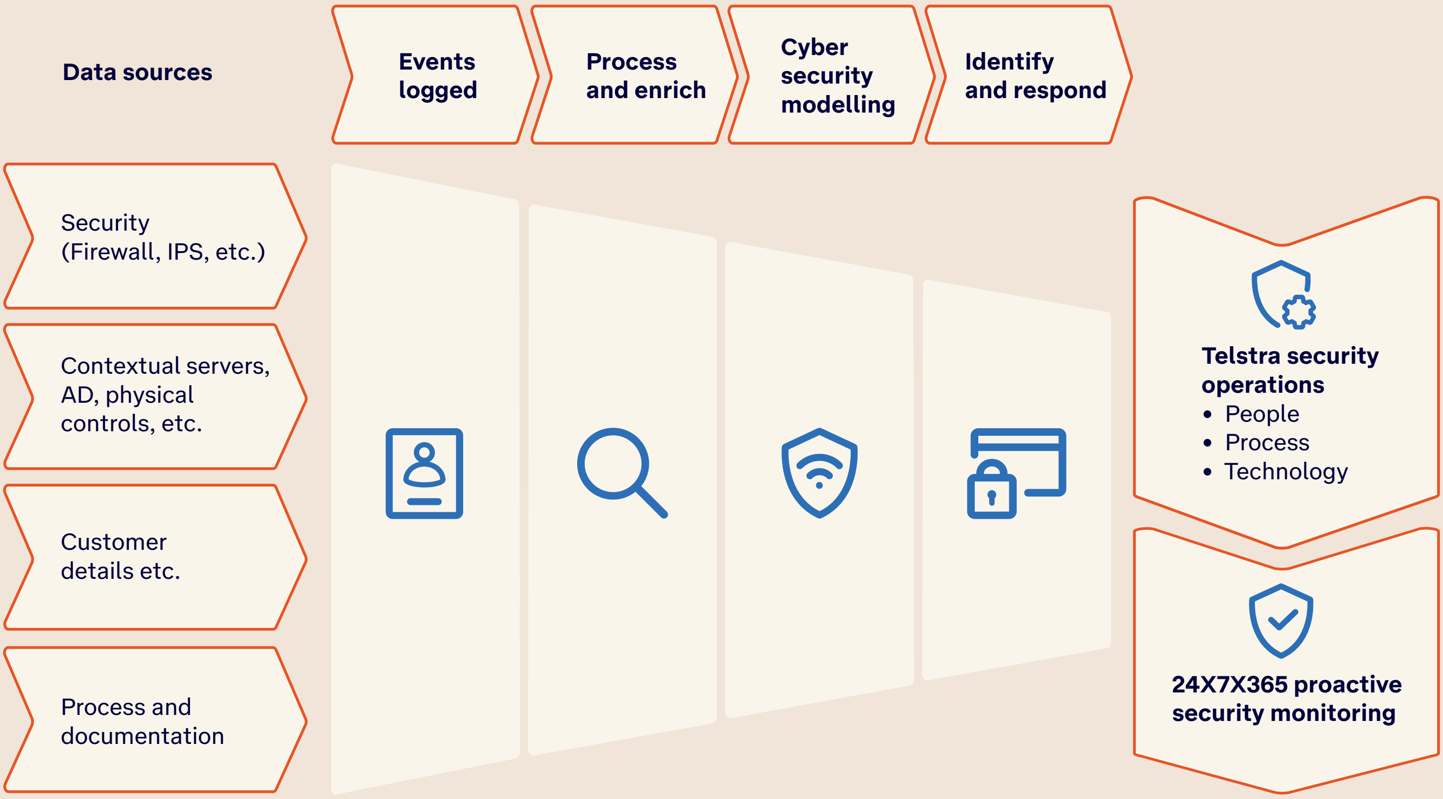
2 - TSOC Integration and Tuning, Development and Platform Operations teams

1 - Cyber Detection and Response Platform

Telstra Cyber Detection and Response layered capabilities.

Cyber Detection and Response platform	TSOC Integration and Tuning, Development and Platform Operations teams	TSOC Security Analyst and Customer Enablement teams	Telstra Purple Professional consulting services
The bedrock of our sophisticated threat detection capabilities, this flexible, cloudhosted big data platform takes in huge amounts of security and contextual log data at scale in real-time. It enriches data with global threat intelligence, enabling advanced detection analytics and empowering analyst investigations.	Our highly skilled cross discipline TSOC specialists manage and augment the detection analytics used to identify potential threats, develop new feature enhancements, and ensure the smooth operation of the Cyber Detection and Response platform.	The 24X7X365 TSOC Analyst team investigates potential threats and quickly notifies you when an incident is identified - pivoting through the data and providing valuable context to help you swiftly address malicious activity. Our Customer Enablement team act as your trusted advisors and advocates, ensuring you get the most out of your service.	Telstra Purple possess rich expertise and experience providing extensive assurance, advisory, and technical consulting services that complement Cyber Detection and Response, further strengthen your security posture and drive future-state goals.

How does it work?



Data sources

Events logged

Process and enrich

Cyber security modelling

Identify and respond

Security (Firewall, IPS, etc.)

Contextual servers, AD, physical controls, etc.

Customer details etc.

Process and documentation

Telstra security operations

- People
- Process
- Technology

24X7X365 proactive security monitoring

Telstra Cyber Detection and Response feeds event data from multiple security and contextual data sources across both your on-premises and cloud infrastructure. These data are then structured and enriched with threat intelligence and geo-location information. We run the data through our threat detection engine—which combines correlation rules, statistical methods, and machine learning to identify anomalies and threats. Once malicious activity has been identified, TSOC quickly raises a security incident and sends a notification for swift threat mitigation.

Service features

Access to trusted expertise

Telstra's exceptional multidisciplinary delivery team spans security operations, data science, DevOps and customer success management, empowering you to respond to new and evolving global threats.

Multi-source threat intelligence

Enrich your event data with Telstra's unique threat telemetry and industry leading intelligence feeds.

Next-generation platform

Telstra's modular Cyber Detection and Response platform is hosted in the public cloud and leverages open-source technologies to deliver exceptional scalability and performance.

Integrated vulnerability management

Run asset discovery and vulnerability scans, understand your top vulnerabilities, and identify mitigation pathways.

Advanced detection analytics

Leverage Telstra's deep security domain expertise. Our high-fidelity detection analytics employ correlation rules, statistical analysis, and machine learning across a range of security and contextual data sources to maximise coverage of your attack surface.

Unified alert tuning

Telstra's dedicated Integration and Tuning team manages alert noise across all data sources, so you are not overwhelmed by high-volume, low-value alerts.

Incident management insights

The Telstra Security Portal enables prioritised end-to-end management of your active security incidents across all data sources, streamlining security operations.

24X7X365 security monitoring

The TSOC proactively detect, prioritise, and alert you to actionable security incidents, enabling quick remediation.

Benefits

Improved surface attack visibility

Detect a broader range of malicious activity by extending monitoring beyond network level security controls to both security and contextual data sources, maximising visibility of your attack surface. The next-generation OpenMSS platform delivers exceptional scalability and performance, enabling real-time processing of a diverse set of log sources, from Windows Audit to Endpoint Detection and Response.

System hardening

Reduce the risk of a breach through identifying vulnerabilities and unknown assets. Our integrated vulnerability management feature helps you understand your top vulnerabilities, identify mitigation pathways, and track your vulnerabilities by severity over time – arming you with the information you need to harden your systems.

Enhance risk management

Cyber Detection and Response helps you continually improve your security posture and control regulatory, reputational, business continuity, and data protection risks.

Detect new, advanced threats

Protect sensitive customer data and business operations by quickly identifying new and sophisticated threats with Telstra's 24X7X365 threat detection. We combine our deep security expertise, advanced detection analytics and threat intelligence feeds, including Telstra's unique telemetry data to proactively raise security incidents for immediate remediation.

Simplify security operations

Telstra's exceptional multidisciplinary team spans security operations, integration and tuning, data science, DevOps, and customer success management, enabling customers to bridge skill and technology gaps while providing round-the-clock proactive threat detection.

Cyber Detection and Response helps reduce alert fatigue and operational overheads through TSOC-led unified tuning. We also help streamline your security operations by presenting prioritised, actionable, and impactful security incidents from all your monitored devices in the Telstra Security Portal.

Why Telstra Cyber Detection and Response?

Not just a managed security service provider

Telstra brings you more than global connectivity and managed security services. Our modern digital fabric provides a platform for innovation, enabling infinite possibilities. From managed adaptive networks to securing data across international supply chains or empowering people to work from anywhere, we cross-pollinate people, processes, and technologies to both defend Telstra's network and better protect our customers.

Open-source innovation

We designed the Cyber Detection and Response platform to be modular and make extensive use of open-source technologies, empowering us to innovate with far less dependency on vendor roadmaps. We are constantly investing in new product enhancements, features, and capabilities.

Scalable next generation cloud platform

The Cyber Detection and Response platform is securely hosted in the public cloud and offers dynamic scalability and exceptional flexibility unlike legacy on-premises infrastructure stacks.

Expertise and Experience

Our deep experience and knowledge of security frameworks such as NIST, GDPR and SOC 2 enable us in implementing robust and effective solutions that align with your industry, compliance requirements, and risk management objectives.

Transparent protection

We don't believe in black-box security operations. We take a collaborative approach, in which customers are treated as partners and thus given the necessary transparency and visibility to inform better decision-making.

Proven Consulting Methodology

Our Telstra Purple "4D" Consulting Methodology – Discover More, Define More, Deliver More and Drive More has helped many global customers to strengthen their security posture.

Interested?

Whether you're exploring new possibilities or needing support for your existing solutions, we're here to help.

Contact your Telstra account representative for more details.

✉ telstraenquiry@team.telstra.com 🌐 telstra.com/global