Cyber Detection and Response

Quickly detect and respond to cyber threats

In today's complex threat landscape, building and sustaining a world-class security operations centre (SOC) is a challenge. Enterprises grapple with an array of evolving cyber threats, talent shortages, and the complexities of managing an expanding attack surfaces.

High barriers to entry, coupled with the need for scarce, specialised skills, make it difficult to establish a 24X7 security operations capability. Security teams are overwhelmed by an influx of security alerts, making it difficult to prioritise threats and respond effectively.

Telstra Cyber Detection and Response offers enhanced visibility through rapid incident detection and notification, enabling enterprises with swift response to minimise damage and downtime.

Telstra Cyber Detection and Response Capabilities

Security Operations

Managed Extended Detection and Response (MXDR)

Managed Threat Detection (MTD)

Managed Endpoint Detection and Response (MEDR)

Vulnerability Scanning

Threat Detection and Response

Security Orchestration Automation and Response (SOAR)

Proactive Threat Hunting and Containment

24X7 Telstra Operations Centre (TSOC) Support

Multi-Source Threat Intelligence

Key Features

Rich Analytics
We leverage high-fidelity detection correlation rules, statistical models and machine learning across a wide range of data sources to detect threats.

24X7X365 Managed XDR
Our TSOC actively detects, prioritises, and responds to security incidents. Managed XDR enables endpoint threat containment.

SOAR
Our Security Orchestration Automation and Response (SOAR) capability enables more efficient and effective security operations workflows.

Everything-as-Code
Infrastructure, detection rules, playbooks, configurations, analytics and algorithms are all managed and supported as code.

Key Benefits

Detect New, Advanced Threats
Protect your sensitive data and business operations by improving visibility of your attack service. Quickly and accurately detect sophisticated, new and evolving threats.

Rapid Threat Containment
The TSOC leverage customer Endpoint Detection and Response tooling to quickly contain threats, reduce the impact of a compromise on your environment and help control regulatory, reputational, business continuity, and data protection risks.

Simplify Security Operations
SOAR playbooks automate repetitive analyst tasks and coordinate workflows spanning disparate security tools, controlling security risk by both speeding up and enhancing triage, investigation and response activities.

Exceptional Operational Efficiency
The Cyber Detection and Response platform delivers exceptional efficiency, scalability, and adaptability, ensuring reliable security operations in evolving threat landscapes.

Empowering Your Business to Rapidly Detect and Response to Threats
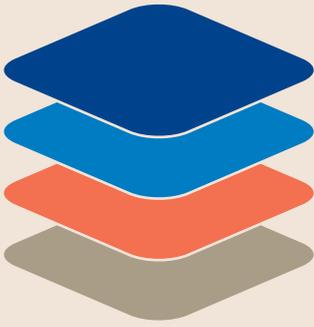
4 Telstra Purple Professional Consulting Services

3 TSOC Security Analyst and Customer Enablement Teams

2 TSOC Integration and Tuning, Development and Platform Operations Teams

1 The Cyber Detection and Response Platform

1 The Cyber Detection and Response Platform

Flexible, cloud-hosted big data platform that takes in huge amounts of security and contextual log data at scale in real-time.

The Cyber Detection and Response platform enriches data with global threat intelligence, enables advanced detection analytics and empowers analyst investigations.

2 TSOC Integration and Tuning, Development and Platform Operations Teams

Our highly-skilled, cross-disciplined Telstra Security Operations Centre (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.

3 TSOC Security Analyst and Customer Enablement Teams

The 24X7X365 TSOC Analyst team investigates and responds to potential threats. Customers are quickly notified, and threats contained.

Our Customer Enablement team act as your trusted advisors and advocates, ensuring you get the most out of our expertise.

4 Telstra Purple Professional Consulting Services

Telstra Purple possess rich expertise and experience providing extensive assurance, advisory, and technical consulting services that complement Cyber Detection and Response, further strengthening your security posture and driving future-state goals.

How does Telstra Cyber Detection and Response work?

Customer Environment

Events Logged → Process & Enrich → Detect → Identify, Respond & Contain

Security Data Sources →
Contextual Data Sources →
Customer Details →

Raw Events | Enriched Events | Alerts | Security Incidents

Telstra Security Operations Centre (TSOC) → 24X7X365 Managed SOAR & XDR

People
Process
Technology

SOAR App Connectors →

Threat Enrichment Automation | Triage Playbook Automation | Response Playbook Automation

Events Logged

Telstra Cyber Detection and Response ingests data from your on-premise and cloud environments.

Process & Enrich

Data are then structured and enriched with threat intelligence and geo-location information.

Detect

Our sophisticated threat detection engine analyses data to detect anomalies and threats.

Identify, Respond & Contain

The TSOC rapidly detects and responds to threats, notifying affected customers and containing attacks. We leverage SOAR to enhance security operations workflow efficiency and effectiveness.

Our Approach to Safeguard Your Business

Our proven consulting methodology has helped global customers to safeguard their business and achieve their desired business outcomes.

Discover more
Strategise • Assess • Identify • Prioritise

Define more
Agree • Architect • Design • Plan

Telstra Purple
"4D" consulting methodology

- Discover more
- Define more
- Drive more
- Deliver more

Drive more
Transition • Manage • Review • Optimise

Deliver more
Build • Migrate • Modernise • Innovate
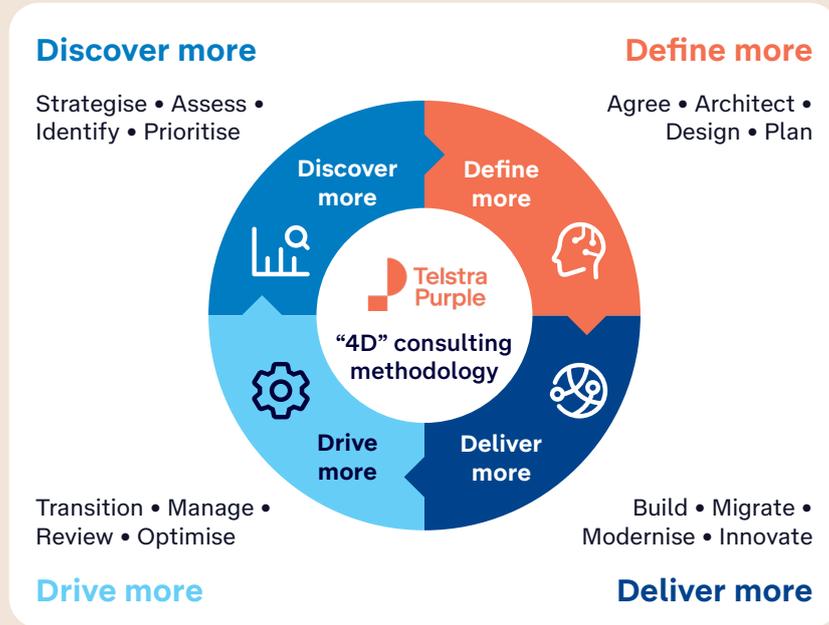
What we'll do

Logical and pragmatic approach to solution adoption and deployment, helping your business to navigate the complexities of security.

End-to-end solutioning that grows as your business does. Understand your security needs and design tailored services, managed by our experts.

Provide clear visibility of your solution functions and any risks we might encounter along the way.

Contextually-mapped and strategically-built around your specific threat profile to enable swift identification and resolution.

Business is everywhere. Security should be too.

Your business needs to be secure.

Telstra International offers modular security solutions designed to help safeguard your data, people and business.

Our deep experience and expertise empower you to navigate the complexities of the digital business landscape and help develop a comprehensive cybersecurity strategy to address your critical business priorities and optimise your security posture to keep you ahead of cyber threats.

Why Telstra International?

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

ISO/IEC 27001 Certified
Our technology, delivery and support processes are certified to the ISO 27001 Information Security Management standard.

Strong Alliance Ecosystem
We bring together the strengths of our partner alliances with global technology leaders in our ecosystem to support you.

Proven Consulting Methodology
Our Telstra Purple "4D" Consulting Methodology has helped many global customers to strengthen their security posture. We have been named a 'Major Player' in the IDC MarketScape Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment.

Discover how Telstra Cyber Detection and Response can help you to secure your business 24X7X365.

Contact your Telstra account representative for more details.

✉ **telstraenquiry@team.telstra.com**   ⊛ **telstrainternational.com**