Telstra
Purple

Cyber Detection and Response (STNT24)

1.0

May 18, 2022

Company 85 Limited (part of Telstra Purple)

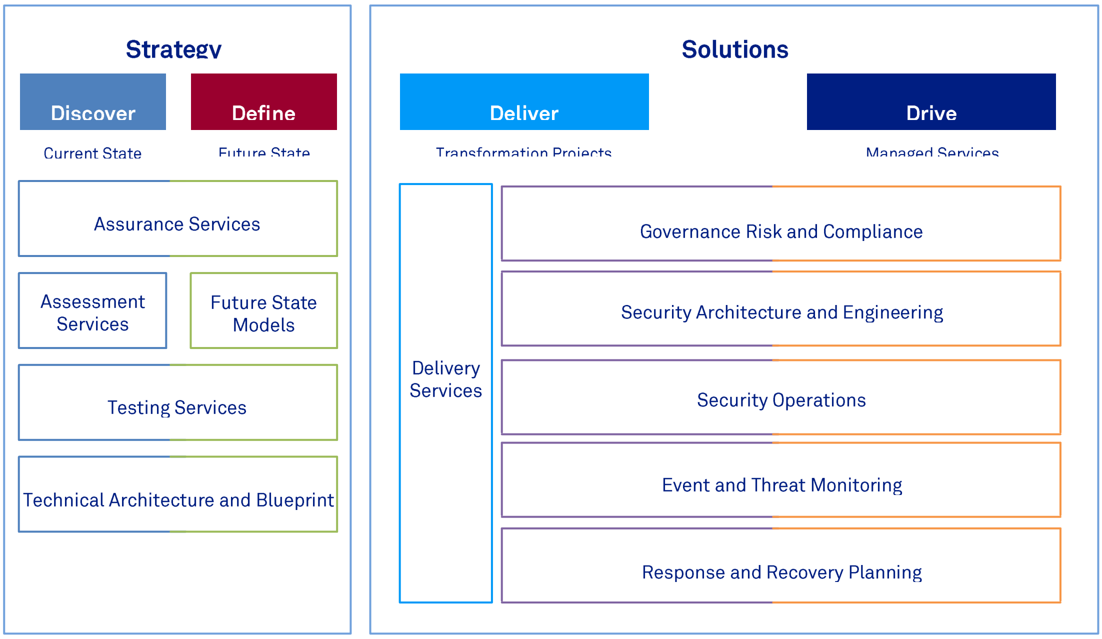
1 Overview

Telstra Purple (trading as Company 85 Limited is a wholly owned subsidiary of Telstra Limited). Telstra Security Services (TSS) jumpstarts customers security journey by reviewing current cloud security posture against current risks/threats as well as future state business goals to gain insight on what their business values most. From there, we help customers develop a strategy aligned to their security maturity and organisational goals over the next two to five years.

Designed with versatility in mind, TSS enables organisations of all sizes to focus on the core business while highly trained, experienced consultants and engineers manage security demands in conjunction with correctly aligned security solutions and services.

Too often security is seen as a blocker to business advancement and a necessary step in protecting core systems (like AWS, Azure and GCP) and information.

TSS instead focusses on delivering business value and helping customers achieve their business outcome



Through our Products & Technology Cyber Security Group, Telstra Purple and also our Telstra Ventures arm, we have made (and will continue to make) a series of step-change investments that will fast-forward the way that security services are delivered in a global context.

This allows us to partner with customers to deliver an integrated and unified Cyber Detection and Response service that has a core focus on consulting, architecture, integration and managed security services, all underpinned by our mature service delivery capability.

Telstra's Cyber Defence and Response service provides the capability to be able to detect a wide range of incidents:

Common security incidents:

- Denial of service attacks
- User account brute force attack

©2022, Company 85 Limited (part of Telstra Purple)

- Malware accessing malicious websites
- Ransomware outbreaks
- Risky internal & external user behaviour
- Validation that devices with vulnerabilities are not compromised.

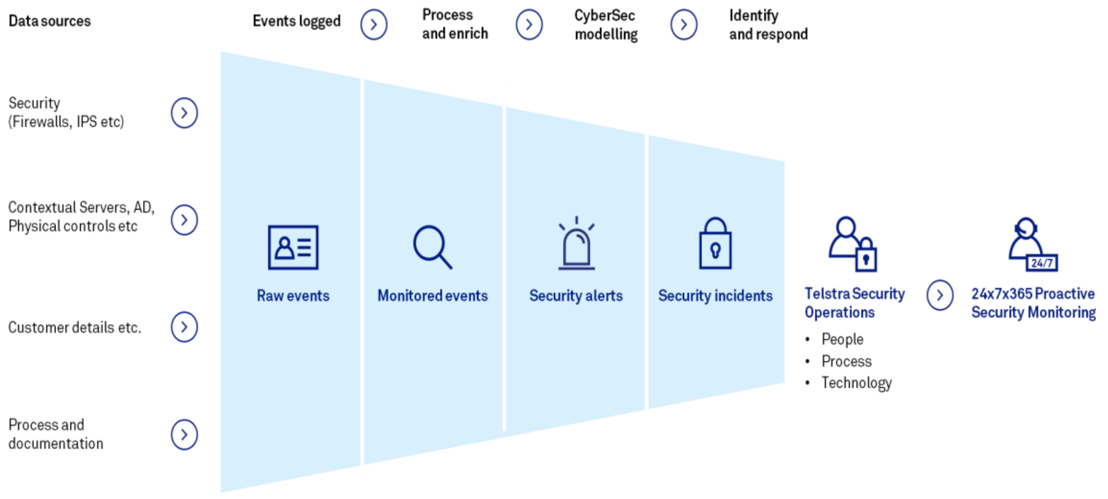
More advanced security incidents:

- Detecting unusual or anomalous behaviour utilising Telstra's big data platform, integrated with Telstra's threat intelligence to identify:
  - Slow exfiltration of sensitive data to malicious destinations
  - Suspicious time / location accesses pointing to stolen credentials

Security Events

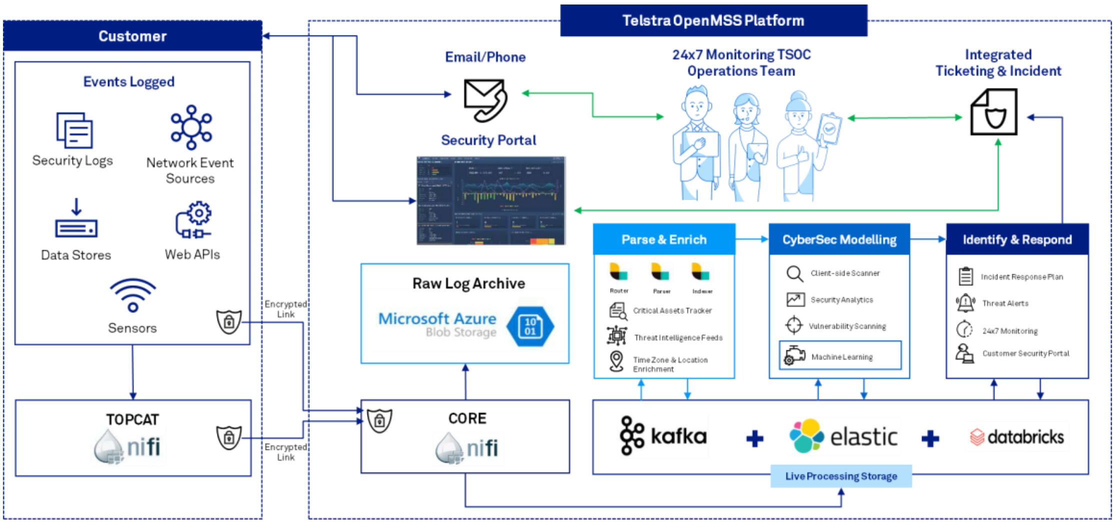
As depicted below: The Security Monitoring service feeds event data from multiple sources across both your on-premises and cloud infrastructure. Telstra stores the log and event data received, performing correlation, enrichment modelling and machine learning to identify anomalies and threats. Suspicious incidents and activity are identified, and the customer is notified. Importantly your infrastructure does not need to be managed by Telstra to use the Security Monitoring service.

Telstra's Cyber Defence and Response – Security Monitoring Service



Telstra's Enterprise Services Architecture

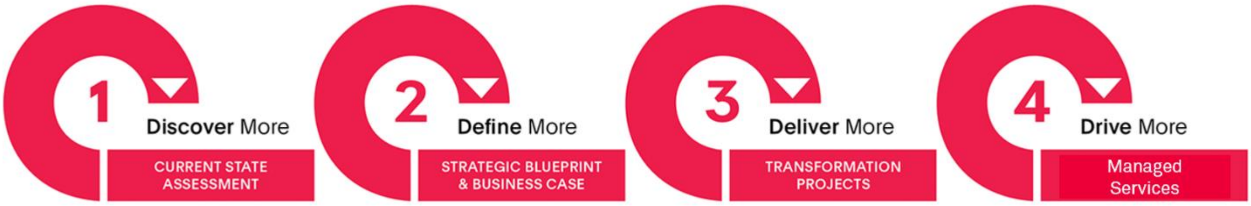
©2022, Company 85 Limited (part of Telstra Purple)



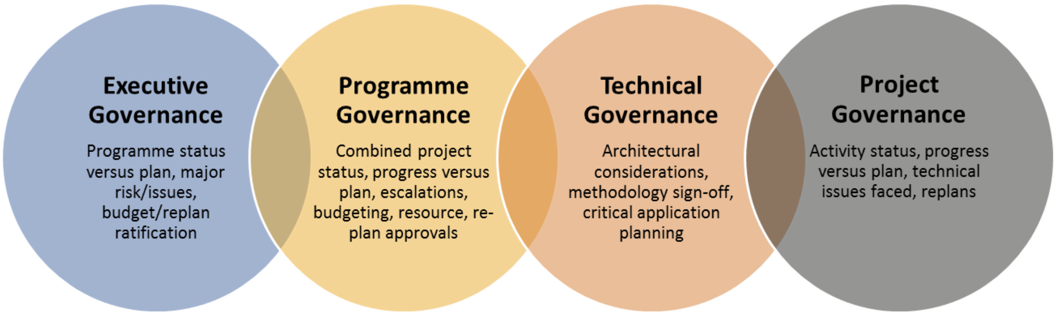
©2022, Company 85 Limited (part of Telstra Purple)

2 Accelerate projects with Telstra Purple’s Accomplish More 4D Methodology

Telstra Purple’s **Accomplish More 4D** methodology is a robust, modular approach that helps clients reduce risk and retain control at all points in the project life cycle. This approach has been successfully implemented across a range of industries and projects over the past 20 years and we are proud of our ability to accelerate project implementation by 25%.



Each stage is backed with our 4-tier governance model.


Executive Governance
Programme status versus plan, major risk/issues, budget/replan ratification
Programme Governance
Combined project status, progress versus plan, escalations, budgeting, resource, re-plan approvals
Technical Governance
Architectural considerations, methodology sign-off, critical application planning
Project Governance
Activity status, progress versus plan, technical issues faced, replans

©2022, Company 85 Limited (part of Telstra Purple)

3 Service Features

Our Global Managed Security Service named Cyber Detection and Response is based on open source and operates on public cloud.

Using the power and scale of big data platforms, our platform focuses on a more scalable and automated SIEM and analytics platform to complement specialist security analysts, discovery tools and incident response methodologies. Telstra’s next-generation Security Operations Centres (TSOCs) are showcases for next-generation managed security services, collaboration, and SOC automation.

Telstra built the new platform using agile methodologies encompassing SecDevOps, so we can rapidly deliver additional features and capability throughout the Security Monitoring product and associated platforms

- Key Features
- 24x7x365 Access
- Visibility of all active and closed incidents
- Management overview
- Direct access to add/remove users
- Two-way incident updates between Telstra and your staff
- Access to Databricks / Azure Data Lake advanced analysis environment

Vulnerability Services provide a comprehensive way for you to scan your network via a cloud-based device to evaluate threats to daily operations, and gain insight into your network to prioritise security investment. They’re especially valuable if you’re upgrading or moving applications to the cloud or have to comply with Payment Card Industry security and ISO 27000 standards.

Vulnerability Services are supported by the advanced technology of our partner Qualys, a global leader in vulnerability scanning.

Vulnerability scanning is Integrated as part of the CDR platform as a free of charge service but can also be delivered as a separate service for customers as part of our managed services.

©2022, Company 85 Limited (part of Telstra Purple)

4 Benefits

- **Local and global intelligence:** Telstra works 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.
- **Managed:** Telstra adopts a 'follow the sun' model - your security is managed 24/7 using our global expertise. Telstra's Security Operations Centres are based in Australia and built to ASIO T4 standards, a requirement in protecting government agency data.
- **Visibility and insight:** Telstra's open-source platform examines data 24/7 from a wide range of sources. With a range of powerful discovery tools and professional services, you can gain a better understanding of your risk profile and get the actionable intelligence needed to address it.
- **Scalable solutions:** High end security made affordable for all businesses, regardless of size. This ranges from basic essential control solutions up to advanced security services. Importantly, your infrastructure does not need to be managed by Telstra to purchase our security solutions.
- **Exceptional people:** Telstra has hundreds of Consultants, Data Scientists, and Security Analysts working with customers to assess their cyber security posture, both managing and mitigating business risk. The team helps consult, select, implement, and manage a range of controls and services, both standard and customised, to ensure the security solution is fit-for-purpose regardless of enterprise size.
- **Ongoing innovation & investment, including co-development:** Development of Telstra's open-source platform is a live and ongoing project, with new features regularly added via two-week sprints to help ensure the services are fit for today and into the future. Telstra has a philosophy of co-creation with our customers, allowing for unique requirements to be catered for and developed either in concert with our customers or on their behalf.
- **Experience counts:** We have been helping businesses manage risk and protect data for decades, while protecting our own network for even longer.

When it comes to cyber-security, Telstra continues to invest heavily in the latest technology, including big data analytics tools, security infrastructure, the open-source platform, and its people. We combine wider data and event sources with cloud-based analytics to accurately profile your risk. This constant and rapid development of new technologies and techniques gives you access to more effective, context-aware tools to find threats quickly and resolve them earlier.

Owing to Telstra's size and scope of operations, we attract the best and brightest in security. Our teams include security analysts, business analysts, DevOps, and data scientists, all working hand in hand to support the need for agility and continuous development. The Security Operations Centre team works on a 24/7 resourcing model and are skilled across analysis, incident escalation, mitigation, remediation, and coordination.

©2022, Company 85 Limited (part of Telstra Purple)

5 Why Telstra Purple?

1. **End to end partner**
   - ✓ We have the technical experts, the partnership and the managed services to be an end to end partner throughout the transformation journey.
2. **Capability**
   - ✓ 1500 certified network, security, cloud, mobility and analytics experts globally.
3. **Experience & References**
   - ✓ We've delivered thousands of projects for a broad range of clients. And we're proud that so many of them are delighted to reference our work.
4. **Industry Recognition**
   - ✓ We've won an array of industry awards including the BCS UK IT Services Company of the Year and Employer of the Year.
5. **Specialisms**
   - ✓ We concentrate on being best of breed in our chosen focus areas
6. **Strong, proven, governance and methodology**
   - ✓ 25+ years' experience in highly regulated industries underpinned by unique methodologies.
7. **Agility, Flexibility and Accessibility**
   - ✓ Ultimate responsiveness and engagement right to the top of the company.
8. **Outcome Focussed**
   - ✓ We cut through politics and red tape to roll our sleeves up and get the job done.
9. **People-Centric**
   - ✓ We believe that our clients are not organisations but people. And our team are individuals and not numbers. Our people-centric approach ensures we apply the human touch to everything we do.
10. **Commercially attractive**
    - ✓ A lean operate model and high utilisation provides our clients with highly competitive commercial frameworks.

6 Appendix A: Commercials

6.1 Information assurance – Impact Level (IL) at which the G-Cloud Service is accredited to hold and process information

As Telstra Purple propose to provide specialised support services to the G-Cloud Service, our services do not require Business Impact Level accreditation.

6.2 Details of the level of backup/restore and disaster recovery that will be provided

This is not applicable to the services described in his document.

6.3 On-boarding and Off-boarding processes/scope etc.

As a provider of Specialist Cloud Services this is not applicable to our response. We are however able to support clients in defining on-boarding and off-boarding requirements and process and to assist with the assurance of suppliers throughout

6.4 Pricing (including unit prices, volume discounts (if any), data extraction etc.)

Please see attached SFIA table.

6.5 Service management details

Where the engagement is of a sufficient scale, a dedicated project manager will be assigned who will be the client’s primary point of contact during the engagement. The project manager will be responsible for assigning and allocating resource to ensure the engagement is delivered in line with the agreed service levels.

6.6 Service constraints (e.g. maintenance windows, level of customisation permitted, schedule for deprecation of functionality/features etc.)

As a provider of Specialist Cloud Services this is not applicable to our response.

6.7 Service Levels (e.g. performance, availability, support hours, severity definitions etc.)

Telstra Purple Specialist Cloud Services is flexible and hence service levels are bespoke to the needs of each client and engagement. We work with the Client to agree service levels, availability and outcomes at the initiation of an engagement.

Performance of our people is measured through a client feedback process. We encourage our clients to give us a formal review of our service, highlighting any strengths and weaknesses and areas for improvement so that we can continue to offer a high quality and competitive service.

6.8 Financial recompense model for not meeting service levels

As a provider of Specialist Cloud Services this is not applicable to our response.

©2022, Company 85 Limited (part of Telstra Purple)

6.9 Training

Telstra Purple consultants will work collaboratively with the Client to ensure effective knowledge sharing during the term of the contract.

6.10 Ordering and invoicing process

Ordering from clients is generally done via the presentation of a Purchase Order following confirmation of the purchase of a service.

Telstra Purple will invoice at the end of every calendar month, giving a precise breakdown of the services purchased, including VAT/other expenses. We are able to provide consolidated invoices if required. Invoices can be issued electronically or via post.

6.11 Termination terms

By consumers (i.e. consumption)

Our standard terms and conditions provide for 30 days' notice of termination. A copy of our standard terms and conditions is attached.

By the Supplier (removal of the G-Cloud Service)

30 days' notice would be provided in the event that Telstra Purple was to withdraw from providing G-Cloud Services. Any ongoing commitments would be supported and maintained through to completion

6.12 Data restoration / service migration

As a provider of Specialist Cloud Services this is not applicable to our response.

6.13 Consumer responsibilities

The Client is required to provide Telstra Purple with enough information to enable us to complete the Call off Contract and prepare a specification which clearly outlines the scope of work and the required outcomes. The Client is encouraged to meet with us weekly to review the progress of the work being undertaken. The Client should also inform Telstra Purple immediately should they have a concern about the work being undertaken so we can take remedial action.

The Client has responsibility for providing office accommodation and facilities (including software tools where these relate directly to the service being procured by the Client) without charge where work is required to be conducted at the Client's premises.

It is the Client's responsibility to provide Telstra Purple with such access, information and staff cooperation, including any third parties as Telstra Purple may reasonably require for the proper performance of any Services.

The Client shall advise a Telstra Purple consultant or subcontractor working at a client location the rules, procedures and information relating to matters such as health and safety and security that are relevant or necessary for working at that site.

©2022, Company 85 Limited (part of Telstra Purple)

6.14 Technical requirements (service dependencies and detailed technical interfaces, e.g. client side requirements, bandwidth/latency requirements etc.)

As a provider of Specialist Cloud Services this is not applicable to our response.

6.15 Details of any trial service available.

Where appropriate, we will discuss with potential clients their challenges or specific requirements and we can provide guidance on how a particular issue can be addressed or to better help the client understand the possible options.

In addition, for more complex client requirements, we are able to undertake a small scoping study to provide a baseline for any wider project or programme. This also enables us to demonstrate our expertise and ability to work effectively with the client. If we were to undertake a scoping study we would discount the cost of the study by 25% against our fee rates.

©2022, Company 85 Limited (part of Telstra Purple)