SERVICE SCHEDULE - CYBER DETECTION AND RESPONSE

1 SERVICE DESCRIPTION

1.1 The Cyber Detection and Response service comprises the following services:

(a) logging – this service stores the Log Event data we receive from you;

(b) event monitoring, correlation and classification – this service monitors Logs Event data to identify Incidents;

(c) incident notification – this service provides rating and notification of Incidents; and

(d) vulnerability Management – this service enables you to scan for vulnerabilities in the IT assets that we have agreed with you,

(together the "**Cyber Detection and Response service**").

TELSTRA SECURITY PORTAL

1.2 We provide you with access to the Telstra Security Portal so you can use the Cyber Detection and Response services.

2 HOW WE PROVIDE CYBER DETECTION AND RESPONSE SERVICE AND WHAT YOU MUST DO

2.1 We provide the Cyber Detection and Response service:

(a) using shared infrastructure and the public cloud, unless we otherwise think it's appropriate to use dedicated infrastructure; and

(b) through a method between your infrastructure and our infrastructure that we will confirm to you on request.

2.2 To receive the Cyber Detection and Response service, you must at your own cost:

(a) separately obtain an appropriate connectivity service;

(b) ensure the term of that connectivity service does not end before the term of your Cyber Detection and Response service; and

(c) complete changes to your network and resources as we require from time to time to allow log and event data to be passed to us from your infrastructure to our infrastructure using a means that we require.

2.3 Activation of the Cyber Detection and Response service comprises one or more milestones and deliverables. Please note:

(a) Stage 3: Event source onboarding can only commence from when we receive and validate your Log Events;

(b) All in-scope event sources are agreed with us during the pre-sales process. No additional fees will apply for any parser or detection development required to activate the agreed scoped event sources. During the pre-sales process, where a customer requires a specific event source that can't be agreed we may be able to offer a customised development option at an additional charge. Specific event sources that we have not previously onboarded may take longer to activate whilst the requisite development work is completed, and

(c) Provisioning of the Vulnerability Management service depends on separate inputs being completed before the service is live that are detailed in clause 2.7.

	Stage 1 Kick-off	Stage 2 Business onboarding	Stage 3 Event source onboarding	Stage 4 Security monitoring
Telstra's inputs	• Provide the Telstra On-Premises Collector and Transmitter (TOPCAT) installation overview	• Build the TOPCAT • Configure the portal tenant and users • Enable cold storage • Create the ticketing queue • Configure event sources that use a pull mechanism to forward logs to the TOPCAT	• Validate logs for security outcomes • Complete device mappings • Create or apply security use cases • Develop or apply parsers • Create or apply detections • Release parsers	• Live security monitoring achieved • Conduct customer welcome session and Telstra Security Portal training • Detection maturation and tuning
Customer's inputs		• Populate the Customer Information Form • Deploy the TOPCAT • Configure event sources that use a push mechanism to forward logs to the TOPCAT • Share credentials for event sources that use a pull mechanism for log forwarding		
Shared inputs	• Conduct a joint kick-off session • Validate the scoped event sources	• Schedule and conduct regular meetings • Complete IP whitelisting		

2.4 The Cyber Detection and Response service from stage 4 of activation will then comprise the following:

Service element	Description
Detection and analytics	Analyse and classify your Log Events. Store your Log Events in a secure environment.
Incident notification	Expert assessment of Alerts and Incidents. Provide tickets for your Incidents within the Telstra Security Portal. Alert your nominated contact point(s) when we detect an Incident.
Vulnerability Management	Provide a view of newly discovered vulnerabilities in the Telstra Security Portal. Provide access to scanning reports.

RETENTION PERIODS

2.5 The Cyber Detection and Response service retention periods for Log Events, Vulnerability Data and Vulnerability Scan Reports are:

Item	Duration
Log Event Hot Storage retention	3 months*
Log Event Cold Storage retention	Up to 7 years*
Retention of vulnerability scan reports	7 days
Retention of raw vulnerability scan data	12 months*

* This is a rolling period, after which we may not be able to recover the log event.

For the purposes of this clause, the terms Hot and Cold Storage are defined as follows:

Hot Storage: Storage of enriched Log Event data used for detection analytics, triage and investigation.

Cold Storage: Storage of raw Log Event data used for archival purposes.

Your storage allowance will vary according to your selected Tier and is specified in your Digital Sales Order Form alongside the charges for any additional Hot or Cold Storage use in excess of your allowance. Your total storage use is the sum of your Hot and Cold Storage use.

WHAT IS VULNERABILITY MANAGEMENT?

2.6 The Vulnerability Management service:

(a) remotely scans IT assets and IP addresses that we've agreed with you, against a list of known security vulnerabilities; and

(b) is self-service so you can schedule scans, view configurations, and run and download reports via the Telstra Security Portal.

2.7 To obtain the Vulnerability Management service, if we ask you to, you must promptly and at your own cost:

(a) decide which IP ranges are to be scanned and the number of internal virtual appliances required;

(b) deploy internal scanning appliances;

(c) configure your systems to allow your assets to be scanned (such as implementation of firewall rule changes);

(d) conduct asset discovery (map) scans;

(e) classify assets. (Critical/Non Critical or other);

(f) set up scans schedules and reporting schedules; and

(g) comply with our other reasonable requests.

2.8 You must back up all of your data, whether contained in or available from your assets that will be scanned. We are not liable for any loss or corruption of data, including where this occurs in connection with the Vulnerability Management service.

2.9 You agree that for your Vulnerability Management service:

(a) scan reports show a point in time of your assets at the time of the scan;

(b) your scan uses a list of known vulnerabilities, which is continually updated, and this may impact the currency of your scan reports;

(c) scans don't detect all vulnerabilities or vulnerabilities that are known at the time of the scan;

(d) you're responsible for scheduling scans at appropriate intervals based on your security needs; and

(e) the service doesn't test, exploit, manage, rectify or fix any vulnerabilities or issues - these are your responsibility.

2.10 You must:

(a) only use the Vulnerability Management service (and any reports generated) solely for your internal use and to scan assets that you have the legal right to scan;

(b) not scan the assets of a third party; and

(c) not modify, interfere with, transfer, or affect the operation of the Vulnerability Management service in any way.

WHAT OPTIONAL COMPONENTS ARE AVAILABLE?

2.11 You may request:

(a) additional log and event storage capacity and retention periods;

(b) services to extract your logs from storage; and

(c) scanning of additional IP addresses above your chosen service tier for your Vulnerability Management service.

(d) provision of additional virtual scanners for your Vulnerability Management service.

If we agree to your request, we will confirm the applicable charges.

HOW DO YOU ACCESS YOUR SERVICE?

2.12 You can access your Cyber Detection and Response service via the Telstra Security Portal.

2.13 The Telstra Security Portal aims to let you do the following:

Detection and analysis
• Acquire insight into active Incidents, Log Event, Alert and Incident trends.
• View and track prioritised Incidents with expert assessment.
• View and track service requests
• Acquire insight into service operational performance
• Configure and run vulnerability management scans, view vulnerabilities by severity against assets, run and download reports
• Acquire insight into threat indicator matches

WHAT ARE THE SERVICE LIMITATIONS?

2.14 We don't promise that the Cyber Detection and Response service will correctly detect and identify all:

(a) Alerts or Incidents;

(b) unauthorised access to your network;

(c) viruses;

(d) spam; or

(e) other types of attacks or issues.

2.15 You must promptly tell us if you find limitations or issues with your Cyber Detection and Response service.

2.16 You must give us at least 10 business days' notice before any vulnerability or penetration testing occurs to your network (except for scans as part of your Vulnerability Management service).

AVAILABILITY

2.17 There are elements of the Cyber Detection and Response service that we can only provide if you have certain devices, applications or services. If you don't have the minimum requirements needed for the service you want to acquire, we can't provide that service to you. We'll tell you the minimum requirements on request.

2.18 The Cyber Detection and Response service is not available to Telstra wholesale customers or for resale.

3 WHAT ARE THE SERVICE LEVELS

WHAT IS THE ACTIVATION SERVICE LEVEL?

3.1 The activation service level for Cyber Detection and Response is:

Item	Description	Service level target
Event source onboarding	The time from when we validate receipt of data for each individual event source to when we commence live monitoring.	6 weeks

3.2 Our activation service level assumes the following:

(a) the relevant Business onboarding inputs detailed in Clause 2.3 are complete;

(b) timing begins for each event source when data starts being forwarded from your network to the Cyber Detection and Response Platform, and we have validated receipt of those data;

(c) timing excludes any time waiting for you to provide information we need to progress your service activation;

(d) timing excludes any time needed to alter or prepare your network, devices, or other resources in connection with the service activation; and

(e) the service level target does not apply to event sources that we have not previously onboarded. These event sources take longer to activate whilst the requisite development work is completed. An estimated onboarding time will be provided by Telstra during the onboarding process upon review of the data source.

WHAT ARE THE SERVICE QUALITY SERVICE LEVELS?

3.3 The service quality service levels are:

Item	Description	Incident priority	Service level target
Incident notification time	Time from when the Cyber Detection and Response platform notifies the Telstra SOC analyst of an alert, to when an incident is reported by the agreed method	1	15 mins
		2	30 mins
		3	60 mins
		4	180 mins
Incident notification method	The method we use to notify your nominated contact person of Incidents	1	Portal + email + phone call
		2	Portal + email
		3	Portal
		4	Portal
Service management	How often we contact you about your Cyber Detection and Response service	NA	Monthly

WHAT IS THE SERVICE AVAILABILITY SERVICE LEVEL?

3.4 The monthly service availability service level is:

Item	Description	Service level target
Availability of the Telstra Security Portal for the Cyber Detection and Response service	Calculated per calendar month	99%
Availability of the Cyber Detection and Response platform (excluding the Telstra Security Portal)	Calculated per calendar month	99%
The service level is calculated as follows: Availability = {[(A – B) – C / (A – B)] x 100} A = Total number of hours in the month. B = Number of hours in a planned outage period in the month. C = Number of outage hours for the Cyber Detection and Response platform in the month.		

WHAT IS THE FAULT REPORTING SERVICE LEVEL?

3.5 The fault reporting service level for the Cyber Detection and Response Platform is:

Item	Description	Service level target
Initial response time for faults	Measured from when a fault is reported to when we respond	Priority 1 Platform Incident: 30 mins Priority 2 Platform Incident: 60 mins Priority 3 Platform Incident: 120 mins Priority 4 Platform Incident: 240 mins
Service restoration	Measured from when a fault is reported to when the fault is resolved	Priority 1 Platform Incident: 95% restored (or work around) in 6 hours Priority 2 Platform Incident: 95% restored (or work around) in 12 hours Priority 3 Platform Incident: 95% restored (or work around) in 24 hours Priority 4 Platform Incident: 95% restored (or work around) in 72 hours
Progress updates	Measured from when we last updated you on the issue	Priority 1 Platform Incident: every 1 hour Priority 2 Platform Incident: every 4 hours Priority 3 Platform Incident: every 12 hours Priority 4 Platform Incident: every 24 hours

WHAT SERVICE CREDITS MAY BE AVAILABLE?

3.6 The service levels detailed in this clause are targets only. No service credits will be available if we do not meet the applicable service level described.

4 HOW DO WE RATE AND NOTIFY YOU OF INCIDENTS

4.1 As part of your Cyber Detection and Response service, we will rate your Incidents using the following table as guidance:

Incident rating				
Impact / **Urgency**	**Extensive** (Direct / indirect impact on more than 1 critical asset)	**Significant** (Direct / indirect impact on at least 1 critical asset)	**Moderate** (Direct / indirect impact on more than 1 non-critical asset)	**Minor** (Any other identified Incident)
Critical (less than 2 hours)	Priority 1	Priority 2	Priority 2	Priority 3
High (between 2 hours and up to 12 hours)	Priority 2	Priority 2	Priority 3	Priority 4
Medium (more than 12 hours and up to 24 hours)	Priority 2	Priority 3	Priority 3	Priority 4
Low (more than 24 hours)	Priority 3	Priority 3	Priority 4	Priority 4

Impact = How severe we think the Incident is on an **asset**.

Urgency = How soon we think the Incident needs to be addressed.

Asset = A device you own on the network that if compromised, could significantly and detrimentally impact your business. Examples of assets are web servers, databases or workstations. With our agreement, you will nominate to us which of your assets are critical or non-critical (and you must act reasonably in doing so). Although we may give you guidance on the categorising of your assets, you're solely responsible for that categorisation.

4.2 We have sole discretion for rating your Incidents. This means that any security issue or attack blocked by another vendor's product or signature, or by your own policy, is not automatically deemed to be an Incident. A ticket will not be created for that issue or event unless we have rated it in a way that requires a ticket to be created.

5 ORDERING AND MANAGING YOUR SERVICE

5.1 Your Sales Order Form sets out the details of the Cyber Detection and Response service you've chosen.

5.2 We aim to meet any estimated timeframes and delivery dates set out in your Sales Order Form but can't guarantee to do so. Time estimates in your Sales Order Form are based on our previous experience, assumptions as to the nature of your internal environment, the availability of our consultants at the time of contract and the timeliness of your inputs and materials. As a result, any indications we give about delivery dates are only estimates and may change.

OPTIONAL SERVICES

5.3 The Cyber Detection and Response service includes options that you can ask us to provide to you.

5.4 If you do ask us to provide any optional services, we use reasonable efforts to comply with your request. We record the detail of your optional services in your Sales Order Form.

5.5 If additional charges apply for these optional services, we'll tell you what they are when you apply for the optional services, and you have to pay the additional charges on top of the charges for the core components of the logging service.

CHANGING YOUR CYBER DETECTION AND RESPONSE SERVICE

5.6 If you want to add, remove or change your event source(s), we will assess what, if any impact these changes will have on your selected tier, or Custom tier scope.

5.7 Changes to your chosen event sources that Telstra confirm do not impact on your selected tier, or Custom tier scope can be made at any time and no additional activation or recurring fees will apply.

5.8 Changes to your chosen event sources that increase your selected tier or Custom tier scope can be made at any time and do not incur additional activation fees. The change, including higher recurring service fees, will take effect as soon as we process the request and do not affect the term of your Cyber Detection and Response service.

5.9 Changes to your chosen event sources that downgrade you to the to the next available Standard tier below your current Standard tier can be made once during the minimum service term without charge.

5.10 If you want to change your Cyber Detection and Response service to a tier which is more than one tier below your current selection or from the Custom tier to any other tier, then we may charge a once off downgrade fee equal to the amount of the difference of pricing between your current tier and your nominated new tier multiplied by the remaining months of your minimum term.

YOUR RESPONSIBILITIES

5.11 You have to make sure we have your most current details at all times. You can change your details through the Telstra Security Portal.

5.12 You have to provide all materials and inputs by the dates specified in your Sales Order Form or, where no dates are specified, when we tell you.

5.13 You have to maintain the firmware and software on your equipment (whether you own it or buy or rent it from us) to a currency of no less than 2 versions behind the latest production release of the relevant firmware or software (i.e. n-2).

5.14 We aren't responsible for any delay or increase in cost as a result of you not doing anything you have to do. It may also mean that we can't provide your chosen service at all.

6 WARRANTIES AND LIABILITY

6.1 You shall pay the charges payable for your Cyber Detection and Response service by the due date(s) in accordance with an Upfront Payment Plan or Instalment Payment Plan as set out in the relevant Sales Order Form.

6.2 We aim to, but can't guarantee, that the Cyber Detection and Response service will produce particular results or outcomes for you (such as achieving external certification, accreditation or industry standards). The Cyber Detection and Response service can't raise all Alerts or detect all Incidents, and we can't guarantee that your systems will operate in an error-free way, or that they'll be safe from malicious attack.

6.3 You have to assess whether any of our recommendations are appropriate for you before you implement them or ask us to implement them for you.

RISKS AND PERMISSIONS

6.4 You acknowledge that:

(a) the Cyber Detection and Response service may result in interruptions, loss and damage to you, including to your computer systems, networks, websites, software, hardware, internet connections and data;

(b) if any of our activities are reported to an external body or authority as required by law, you'll do everything necessary to make sure that body is aware you authorised the activities involved in the Cyber Detection and Response service; and

(c) our services are based on information you give us and the infrastructure you have in place at the time we perform the Cyber Detection and Response service.

7 INTELLECTUAL PROPERTY

7.1 We own all intellectual property rights in any material we develop for you in carrying out the Cyber Detection and Response service (including in any reports or materials generated or provided to you as part of your Vulnerability Management service).

7.2 Where we have designed your service, we own all intellectual property rights connected with the design, including in the network diagrams, management IP addresses and equipment configurations (**Items**).

7.3 We grant you a licence to use the Items solely for the purpose of your service. The licence ends on expiry or termination of your relevant service.

7.4 The network diagrams and other information that we supply you with your service is confidential information to us. You must ensure that you keep the network diagrams and other information confidential. You may only disclose the network diagrams and other information in your business for the purposes of using your service (unless you have our prior written consent to do otherwise).

8 CHARGES

8.1 You have to pay us the charges at the times set out in your Sales Order Form, or if no time is set out, then from the date we have onboarded your first nominated data source and we start providing the service.

9 TERM AND TERMINATION

9.1 We provide Cyber Detection and Response for the period you nominate in your Sales Order Form, unless terminated earlier in accordance with this clause.

9.2 The minimum term for each component of Cyber Detection and Response is 12 months (or the longer period set out in your Sales Order Form).

9.3 After the minimum term:

(a) your Cyber Detection and Response service continues until terminated; and

(b) either you or we may terminate your Cyber Detection and Response service in whole or in part by giving at least 30 days written notice.

9.4 We can terminate your Cyber Detection and Response service if you cause a defect or incident by accidental damage, or improper or negligent use of the service, or you don't maintain the currency of the firmware or software on your equipment. You have to pay early termination charges if we terminate your Cyber Detection and Response service under this clause.

9.5 When you cancel your Cyber Detection and Response service;

(a) we will store your logs up to the date of cancellation (at your expense), unless you tell us in writing that you request for us to retain these logs for a further period and that you agree to the charges for such storage (**Further Storage Period**);

(b) you may request an extract of your logs before you cancel or subject to 3.22(a) above during the Further Storage Period;

(c) you must pay a fee for this extraction and we can confirm this fee on request;

(d) you will not be able to request an extract after the Further Storage Period; and

(e) your Vulnerability Management service will also be cancelled and we won't retain any scan data or reports.

EARLY TERMINATION CHARGES

9.6 If you or we terminate your Cyber Detection and Response during the minimum term for any reason other than our material breach or our inability to support your equipment (except where we can't support your equipment because you haven't maintained the firmware or software to the required currency, in which case this clause does apply), you have to:

(a) pay us the early termination charges for Cyber Detection and Response; and

(b) labour costs we incur out of pocket on your behalf.

For Cyber Detection and Response:

ETC = (A x B)

where:

A = number of months remaining in minimum term for the terminated service (as set out in your Sales Order Form)

B = the monthly charge for the terminated service (as set out in your Sales Order Form)

9.7 You acknowledge the early termination charges are a genuine pre-estimate of the loss we'd suffer if you terminated

early.

10 DEFINITIONS

10.1 In this Service Schedule, unless otherwise stated:

Alert: A potential security risk to your environment identified by our detection analytics by analysing one or more Log Events.

Incident means an event arising from one or more Alerts that the Telstra Security Operations Centre assess as posing a real risk to your systems or environment.

Log Event means a record generated by one or more of your monitored event sources.

Priority 1 Platform Incident means an Incident where your Cyber Detection and Response service is not available, causing critical impact to business operations.

Priority 2 Platform Incident means an Incident where your Cyber Detection and Response service is not available, or severely degraded, impacting significant aspects of business operations.

Priority 3 Platform Incident means an Incident where your Cyber Detection and Response service is degraded. Customer service is noticeably impaired but most business operations continue.

Priority 4 Platform Incident means all other Incidents that are not Severity 1, 2 or 3 Incidents.

TSOC or Telstra Security Operations Centre means Telstra's security operations centre.