Centre Tecnològic de Telecomunicacions de Catalunya

CENTRE TECNOLÒGIC DE TELECOMUNICACIONS DE CATALUNYA – CTTC

PLEC DE CLÀUSULES TÈCNIQUES DELS SERVEIS RELATIUS A LA RENOVACIÓ I LA EVOLUCIÓ DE LES LLICÈNCIES DEL SOFTWARE CROWDSTRIKE PER AL CENTRE TECNOLÒGIC DE TELECOMUNICACIONS DE CATALUNYA – CTTC

NÚM. EXPEDIENT CTTC-2025-81

Parc Mediterrani de la Tecnologia - Building B4
Av. 1Carl Friedrich Gauss 7
08860 - Castelldefels
Barcelona (Spain)

1. OBJECTE DEL CONTRACTE

La FUNDACIÓ CENTRE TECNOLÒGIC DE TELECOMUNICACIONS DE CATALUNYA (d'ara endavant CTTC o la Fundació) és una Fundació del sector públic de la Generalitat de Catalunya, subjecta a la legislació sobre fundacions de la Generalitat de Catalunya, amb personalitat jurídica pròpia i durada il·limitada. Figura inscrita al Registre de Fundacions de la Generalitat de Catalunya amb el número 1613. Impulsada des del Departament d'Universitats, Recerca i Societat de la Informació (DURSI) de la Generalitat de Catalunya, es va constituir el dia 28 de juny de 2001 i té per objecte contribuir a impulsar la promoció i el desenvolupament de la recerca d'alt nivell a les diferents branques de les tecnologies de les telecomunicacions i la geomàtica, potenciant grups de recerca d'excel·lència en ciència i enginyeria relacionades amb aquests àmbits; la producció, promoció i divulgació del coneixement i la formació de personal tècnic i científic en tecnologies de telecomunicacions i la geomàtica; l'establiment de col·laboracions científiques i acadèmiques amb les universitats i els grans centres de recerca nacionals i internacionals especialitzats en tecnologia de telecomunicacions i geomàtica; l'establiment de col·laboracions, en la forma que legalment escaigui, amb les administracions públiques i amb el sector privat en les matèries pròpies de la seva activitat; facilitar el contacte entre la investigació bàsica i aplicada, actuant, quan correspongui, com a centre de transferència de tecnologia; l'organització de trobades científiques nacionals i internacionals; contribuir, mitjançant el perfeccionament tecnològic i la innovació, a la millora de la competitivitat de les empreses; així com qualsevol altra finalitat relacionada.

L'objecte del present plec de condicions tècniques és definir i establir les condicions tècniques que regiran l'adjudicació, per part del CTTC, del contracte per a la renovació i evolució de les llicències del software Crowdstrike del què actualment disposa el CTTC als equips d'usuaris, servidors i estacions de treball, amb l'objectiu de germanitzar la evolució y el manteniment de la solució corporativa de seguretat perimetral actualment implementada. Aquesta renovació ha de garantir la continuïtat, l'actualització i el suport expert necessari per mantenir l'operativitat, la seguretat i la disponibilitat de la infraestructura del centre, assegurant així el correcte funcionament dels serveis TI essencials per al desenvolupament de l'activitat institucional.

L'abast de la present ha de comprendre principalment el següent apartat:

- Implantació y manteniment de la solució Falcon Complete Next-Gen MDR de Crowdstrike.

Inici i Durada del Contracte: El contracte començarà a partir de la signatura del contracte, amb una durada de 3 anys, sense probabilitat de pròrroga.

El present Plec de Prescripcions Tècniques descriu les condicions mínimes exigides.

2. PRECEDENTS

Al CTTC ja es disposa de llicenciament actiu del programari CrowdStrike, amb data de finalització el 30 d'octubre de 2025. Actualment, el centre compta amb els següents mòduls i bundles contractats:

Producte	Unitats
Falcon Endpoint Protection Enterprise Flexible Bundle	300
Threat Graph Standard on EU Cloud	250
Falcon Firewall Management Bundle Promo	300
Prevent	300
Insight	300
Falcon Device Control Bundle Promo	300
Server Threat Graph Standard on EU Cloud	50
Express Support	1
Falcon Adversary OverWatch Endpoint	300
Falcon Spotlight	300
University LMS Subscription New Customer Access Pass	2

3. CARACTERÍSTIQUES TÈCNIQUES I ABAST DEL SERVEI

L'empresa adjudicatària haurà d'implantar i mantenir els serveis Falcon Complete MDR, d'acord amb els requisits tècnics i funcionals detallats a continuació.

Requisits generals:

- **Cap de Projecte únic**: Responsable de la coordinació, de les reunions de seguiment, del treball amb els interlocutors del CTTC i de la presentació d'informes. La proposta haurà d'identificar la persona assignada, així com la seva metodologia de treball. A més a més, és obligatori que, a les reunions, hi assisteixin no només el Cap de Projecte sinó també els professionals tècnics efectivament assignats.

- **Material nou**: Tot el material subministrat haurà de ser obligatòriament nou, sense reutilitzacions ni elements de dubtosa procedència.
- **Gestió d'incidències i peticions**: Integrada amb el Servei d'Atenció a l'Usuari del CTTC, que actuarà com a únic interlocutor vàlid.
- **Actualitzacions sense sobrecost**: Qualsevol component que arribi al seu final de cicle de vida de forma no programada, o que presenti una vulnerabilitat crítica, haurà de ser actualitzat per l'empresa adjudicatària sense cap cost addicional per al CTTC.
- **Actualitzacions anuals de programari**: En cas que el CTTC ho requereixi, s'efectuaran anualment sense cost afegit. Les actualitzacions motivades per vulnerabilitats o per instruccions del fabricant es realitzaran tantes vegades com sigui necessari dins del manteniment.
- **Metodologia i normes**: L'empresa haurà d'adaptar-se a la metodologia i les normes establertes pel Departament d'Informàtica Corporativa del CTTC. Sense la seva supervisió i autorització no es podrà realitzar cap actuació. Quan el CTTC ho requereixi, caldrà entregar documentació de treball (hores d'inici i fi, pla de regressió, etc.).
- **No interferència en el servei**: Les tasques d'instal·lació i migració s'hauran de dur a terme sense afectar el servei actual i de manera transparent per als usuaris finals. Els períodes de parada en productiu hauran de minimitzar-se i ajustar-se als horaris establerts pel CTTC.
- **Mesures de seguretat**: L'empresa adjudicatària haurà d'adoptar totes les mesures necessàries per garantir la disponibilitat, la confidencialitat i la integritat de les dades i de la documentació generada.
- **Model remot**: El servei s'oferirà de manera prioritària en modalitat remota 24x7.

Servei MDR:

- **Descripció del servei:** El CTTC requereix la contractació d'un servei *Managed Detection and Response (MDR)* integral per a tots els servidors i estacions de treball, cobrint des de la detecció fins a la remediació completa. Inclourà l'administració i optimització contínua de la solució de seguretat, la incorporació de nous agents i polítiques, i la resposta completa a incidents 24x7, amb suport de *Threat Intelligence*.

Aquest servei és essencial per assegurar la disponibilitat i integritat de la informació, en línia amb les exigències de l'ENS en categoria alta.

- **Solució requerida:** La solució de referència és la **suite Falcon Complete with Threat Graph Standard on EU Cloud de CrowdStrike** o equivalent. Es sol·liciten **300 subscripcions MDR** per a una durada de 3 anys. L'ús de *Threat Graph Standard on EU Cloud* és crític per garantir la sobirania de les dades, el compliment normatiu europeu i la capacitat d'anàlisi avançada dins d'un marc sòlid de seguretat legal i tècnica.

Beneficis clau de Falcon Complete Next-Gen MDR (CrowdStrike):

- **Detecció i prevenció de bretxes 24/7**: Protecció liderada per experts en tota la superfície d'atac.
- **Reducció de càrrega operativa per al CTTC**: Actua com una capa de suport integral, combatent amenaces avançades com *ransomware*, atacs de *phishing* i *exploits de zero-day*.
- **Resultats**: Cicle complet de remediació per part de l'equip Falcon Complete Next-Gen MDR, que conté amenaces, elimina processos maliciosos, posa en quarantena arxius i elimina la persistència..
- **Velocitat de Detecció**: Temps mitjà de detecció (MTTD) de 4 minuts.
- **Caça d'amenaces impulsada per intel·ligència:** Amb CrowdStrike Falcon Adversary OverWatch™, s'ofereix protecció 24/7 en els endpoints, identitats i càrregues de treball al núvol, utilitzant IA avançada i intel·ligència d'amenaces.

Requisits principals que ha de complir la solució MDR:

- **Antivirus d'última generació**: Amb tecnologia impulsada per Intel·ligència Artificial per a una detecció moderna i una resposta automatitzada ràpida. Ha de protegir contra tot tipus d'atacs (*malware* bàsic, sofisticats, *offline*), utilitzar aprenentatge automàtic i IA per a *malware* conegut, de dia zero i *ransomware*, i incloure indicadors d'atac basats en el comportament (IOA) per a atacs sense fitxers/*malware*. La proposta ha d'incloure Falcon Prevent.
- Capacitat de bloqueig d'atacs sense *malware* i *fileless*.
- Telemetria en temps real en el punt final d'activitat de processos, fitxers i xarxa.

- Capacitat per operar ràpidament i aïllar els endpoints a la xarxa.
- **Descobriment i inventari de dispositius**: Inclou la capacitat de detectar dispositius no monitoritzats activament, per presents a la xarxa. Inclou *Falcon Discover i Falcon Spotlight*.
- Inventari d'aplicacions i processos actius en els dispositius gestionats.
- Plataforma d'intel·ligència d'amenaces per informació actualitzada.
- Configuració, administració i ajustament de la tecnologia desplegada.
- Centralització de la informació en una Plataforma del Servei i Consola de gestió amb quadre de comandament.
- Servei proactiu de *Threat Hunting,* monitorització i remediació 24x7.
- Accés remot al dispositiu per a la eliminació de mecanisme s de persistència, detenció de processos i eliminació de l'amenaça.
- Restauració completa d'equips a l'estat anterior a la intrusió.
- Suport directe al CTTC amb *Express Support*.

Eficiència de seguretat (MDR):

- **Velocitat de desplegament**: Arquitectura basada en el núvol i sensor lleuger, amb implementació a escala molt ràpida.
- **Facilitat de manteniment**: Actualitzacions automàtiques s de conjunt de regles de defensa.
- **Facilitat d'integració**: Plataforma oberta i de fàcil integració.
- **Facilitat de funcionalitat i actualitzacions**: Sensor lleuger que permet agregar capacitats de forma senzilla.

Eficàcia de seguretat (MDR):

- **Detecció i resposta**: Es sol·licita monitoratge 24/7, investigació de cada alerta, actuació ràpida per eliminar la persistència, aturar processos i restaurar els sistemes al seu estat anterior a la intrusió.

- **Antivirus de nova generació**: Combinació de tecnologies de prevenció amb visibilitat completa, protecció contra tot tipus d'atacs (incloent-hi sense *malware* i sense fitxers), basat en ML i IA, bloqueig *d'exploits*, IOAs personalitzats, protecció contra manipulacions del sensor, arbre de processos per visualitzar atacs (amb terminologia MITRE ATT&CK), actualitzacions automàtiques sense signatures, mínima càrrega de CPU i instal·lació de l'agent sense reinici (Windows, Linux i macOS).
- **Detecció i resposta d'endpoints (EDR)**: Visibilitat contínua i completa, monitoratge continu de l'activitat, anàlisi en temps real, registre continu d'esdeveniments sense processar (telemetria), base de dades d'esdeveniments amb consultes en segons, acceleració d'operacions de seguretat, combinació d'alertes en incidents, priorització intel·ligent, acceleració d'investigacions (dades automatitzades, context profund, visualitzacions, línia de temps dinàmica), anàlisi d'IA basat en el núvol (puntuació "DEFCON"), APIs per a interoperabilitat.
- **Higiene de TI**: Identificació de sistemes no autoritzats, inventari d'aplicacions en temps real, accés a informació actualitzada sobre actius, aplicacions, ús, comptes privilegiades i endpoints desprotegits.
- **Cerca d'amenaces gestionada (Threat Hunting)**: Servei gestionat 24x7 amb anàlisi humà profund per caçar atacants sofisticats que eviten les tecnologies estàndard.
- **Gestió de Vulnerabilitats**: Avaluació contínua en temps real sense impacte en el rendiment, sense agents addicionals / hardware / escaneigs / excepcions de firewall / credencials d'administrador. Dades disponibles a través de panells intuïtius i cerca en temps real. Monitoratge d'equips connectats i desconnectats.
- **Suport Tècnic**: 24x7 els 365 dies de l'any, servei remot, comunicació periòdica amb el CTTC per al seguiment de mètriques, punt de contacte únic. Reunions quadrimestrals mínimes per al seguiment del servei.

Acords de nivell de servei (SLA):

- SLA mínims exigits:
  - Temps mitja de detecció (MTTD) ≤ 5 min
  - temps mitja de resposta (MTTR) ≤ 30 min
  - Disponibilitat de la plataforma ≥ 99,9%

L'adjudicatari ha de garantitzar informes periòdics:

- **Mensuals**: mètriques de seguretat, incidents detectats, vulnerabilitats.
- **Trimestrals**: revisió estratègica de seguretat i full de ruta d'evolució.

Requisits d'habilitació específica per a les empreses licitadores:

- Referència precisa, documentada i acreditativa que els productes i/o serveis de seguretat estan inclosos en el Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i la Comunicació (CPSTIC) del CCN o disposen de la certificació Common Criteria.

  En cas que el producte o servei no es trobi en aquestes llistes, i per raons d'operativitat o exclusivitat, el licitador haurà d'aportar la fitxa de taxonomia del component d'acord amb la Guia de Seguretat de les TIC "CCN-STIC 140 - Taxonomia de referència per a productes i serveis de Seguretat TIC".
- Certificat de Conformitat amb l'ENS en nivell alt, en el moment de presentar la licitació.
- **Certificacions mínimes per a l'empresa adjudicatària**: Per assegurar la bona execució del projecte, l'empresa adjudicatària ha de comptar com a mínim amb les certificacions següents, aportant-ne còpia acreditativa:
  - ENS en nivell alt
  - ISO 9000, 20000 i 27001
  - Crowdstrike: Partner Elite
- Experiència mínima demostrable amb projectes de MDR/SIEM en entorns ENS de nivell alt, amb almenys 3 referències en els darrers 3 anys.
- Centre de suport 24x7 certificat i localitzat a la UE.

Totes aquestes acreditacions i certificats hauran de ser presentats conjuntament amb l'oferta.

ABAST SOL·LICITAT:

El CTTC, per tal de donar resposta al present plec, sol·licita el següent llicenciament de CrowdStrike, que inclou productes essencials per a una protecció integral i avançada contra ciberamenaces.

Producte	Unitats
Falcon Complete Next-Gen MDR	300
Express Support	1
Insight	300
Threat Graph Standard on EU Cloud	250
Prevent	300
Falcon Device Control	300
Discover	300
Falcon Firewall Management	300
Falcon Complete Subscription	300
Falcon Adversary OverWatch Endpoint	300
Server Threat Graph Standard on EU Cloud	50
Falcon Spotlight	300

Aquest conjunt de productes cobreix les necessitats més exigents de seguretat, combinant detecció i resposta gestionades 24x7, anàlisi d'intel·ligència de ciberamenaces, control avançat de dispositius i visibilitat profunda tant en endpoints com en servidors.

Inici i Durada del Contracte: El contracte començarà a partir de la signatura del contracte, amb una durada de 3 anys, sense probabilitat de pròrroga.

4. LLOC DEL LLIURAMENT I INSTAL·LACIÓ

Centre Tecnològic de Telecomunicacions de Catalunya
Centre de Serveis Informàtics
Av. Carl Friedrich Gauss, 7-11, B4 i B6
08860 Castelldefels

5. COMUNICACIÓ

L'adjudicatari designarà un responsable que actuarà com persona de contacte amb el Departament d'informàtica del CTTC, i serà el responsable de planificar, gestionar i coordinar tot el procés de manteniments de les llicències.

Castelldefels, 29 de setembre de 2025

Jordi Escoda
Responsable del Servei Informàtic

Parc Mediterrani de la Tecnologia - Building B4
Av. 10Carl Friedrich Gauss 7
08860 - Castelldefels
Barcelona (Spain)