Informe del sobre B: juicio de valor del contrato para la adquisición de una solución SIEM del CCN-CERT que gestionará eventos e información de seguridad en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU, así como el servicio de mantenimiento y soporte de la solución adquirida durante tres años adicionales. (Exp. 34/24)

Documentación asociada

Pliego de Prescripciones Técnicas (PPT) y Pliego de Cláusulas Administrativas Particulares (PCAP) reguladoras del contrato para la adquisición de una solución SIEM del CCN-CERT que gestionará eventos e información de seguridad en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU, así como el servicio de mantenimiento y soporte de la solución adquirida durante tres años adicionales.

Entidades y personas que redactan el informe

- Servei d'Infraestructures TIC
  - Maribel Barceló Villanueva
  - Toni Pérez Sánchez
  - Xavier Pons Pons (Director)

PEREZ SANCHEZ ANTONIO - DNI 37341236T
Firmado digitalmente por PEREZ SANCHEZ ANTONIO - DNI 37341236T
Fecha: 2024.09.26 11:47:24 +02'00'

BARCELO VILLANUEVA MARIA ISABEL - DNI 43069788B
Firmado digitalmente por BARCELO VILLANUEVA MARIA ISABEL - DNI 43069788B
Fecha: 2024.09.26 11:51:20 +02'00'

Digitally signed by PONS PONS JOSEP XAVIER - DNI 41497180M
Date: 2024.09.26 11:57:02 +02'00'

Palma, 26 de septiembre 2024

Índice de Contenidos

Informe del sobre B: juicio de valor del contrato para la adquisición de una solución SIEM del CCN-CERT que gestionará eventos e información de seguridad en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU, así como el servicio de mantenimiento y soporte de la solución adquirida durante tres años adicionales (Exp. 34/24)

1. Objeto del informe

El siguiente informe técnico expone la valoración por parte del Servei d'Infraestructures TIC de:

- Sobre B: juicio de valor.

En base a criterios evaluables mediante juicio de valor, presentados por los licitadores al pliego de prescripciones técnicas reguladoras del contrato para la adquisición de una solución SIEM del CCN-CERT que gestionará eventos e información de seguridad en el marco del Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU, así como el servicio de mantenimiento y soporte de la solución adquirida durante tres años adicionales.

Este informe se basa en la aplicación de los criterios mediante juicio de valor respecto a la calidad de la propuesta técnica con un total de hasta 38 puntos según lo establecido en el PCAP.

Les propuestas evaluadas a continuación corresponden a las ofertas presentadas por los licitadores siguientes:

- ICA Sistemas y Seguridad S.L.U. (Licitador 1)
- S2 GRUPO SOLUCIONES DE SEGURIDAD, S.L.U. (Licitador 2)

A continuación, se describen los criterios evaluables mediante un juicio de valor según consta en el PCAP y en el siguiente apartado, se relaciona la valoración de estos para cada uno de los licitadores:

Calidad de la propuesta técnica (hasta 38 puntos)

En base a la memoria técnica presentada se valorará:

- Características generales de la solución propuesta, valorando entre otras, el nivel de integración de la solución, el número de fuentes distintas de ingesta, taxonomización y correlación de eventos soportada por la plataforma, la capacidad de gestión de incidentes (workflow), la capacidad para la gestión de playbooks y las capacidades de ingesta de tráfico netflow en sus diferentes versiones y formatos enterprise (como los que puede utilizar Palo Alto). **(hasta 15 puntos)**
- Capacidades SOAR y UEBA implementadas, valorando sus características, funcionalidades y detalle de estas. **(hasta 10 puntos)**
- Características de la infraestructura hardware aportada por el licitador, valorando mejoras en las capacidades de ingesta de eventos por segundo, incremento de períodos de retención del almacenamiento primario y secundario, entre otras. **(hasta 5 puntos)**
- Integraciones aportadas con soluciones del ecosistema CCN-CERT y/o de terceros. Se valorarán mejoras en cuanto al número de integraciones adicionales aportadas, así como del nivel de integración de estas. Así mismo, se valorará positivamente la integración de la solución con fuentes de inteligencia como LUCIA del CCN-CERT, TheHive/Cortex y Recorded Future **(hasta 8 puntos)**

2. Ofertas presentadas

2.1. Licitador 1: ICA Sistemas y Seguridad S.L.U.

2.1.1 Calidad de la propuesta técnica

2.1.1.1 Características generales de la solución propuesta, valorando entre otras, el nivel de integración de la solución, el número de fuentes distintas de ingesta, taxonomización y correlación de eventos soportada por la plataforma, la capacidad de gestión de incidentes (workflow), la capacidad para la gestión de playbooks y las capacidades de ingesta de tráfico netflow en sus diferentes versiones y formatos enterprise (como los que puede utilizar Palo Alto) (hasta 15 puntos)

La solución MÓNICA presentada en la propuesta del licitador detalla su integración tanto a nivel de funcionalidades como a nivel de fuentes de información de ingesta.

El licitador describe las capacidades de taxonomía, correlación y la gestión de incidentes con un workflow completo y con la posibilidad de definir playbooks.

En la propuesta no se detallan las capacidades de ingesta de tráfico netflow en sus diferentes versiones y formatos Enterprise.

PUNTUACIÓN OTORGADA: 13 puntos

2.1.1.2 Capacidades SOAR y UEBA implementadas, valorando sus características, funcionalidades y detalle de estas. (hasta 10 puntos)

El licitador expone las capacidades SOAR, disponen de una alta integración y funcionalidades muy completas con diferentes servicios. Se explican casos de uso donde queda reflejada las capacidades de la solución MÓNICA.

Respecto a las capacidades UEBA, en la propuesta técnica se detallan las funcionalidades de análisis de comportamiento mediante detectores que ejecutan el proceso analítico buscando casos de actividad sospechosa.

PUNTUACIÓN OTORGADA: 10 puntos

2.1.1.3 Características de la infraestructura hardware aportada por el licitador, valorando mejoras en las capacidades de ingesta de eventos por segundo, incremento de períodos de retención del almacenamiento primario y secundario, entre otras. (hasta 5 puntos)

El licitador propone una infraestructura hardware que según indica en su propuesta soporta las necesidades especificadas y las mejora, soportando hasta 4 meses de retención primaria y 36 meses de secundaria y hasta 6.000EPS sostenidos con picos de 14.000EPS.
Además, ofrece un año de garantía adicional a los solicitados.

PUNTUACIÓN OTORGADA: 3,5 puntos

2.1.1.4 Integraciones aportadas con soluciones del ecosistema CCN-CERT y/o de terceros. Se valorarán mejoras en cuanto al número de integraciones adicionales aportadas, así como del nivel de integración de estas. Así mismo, se valorará positivamente la integración de la solución con fuentes de inteligencia como LUCIA del CCN-CERT, TheHive/Cortex y Recorded Future (hasta 8 puntos)

En la propuesta el licitador indica que se aporta la integración con las soluciones del CCN-CERT: LUCÍA, PILAR, EMMA, microCLAUDIA, IRIS, CARMEN, CLAUDIA y SAT-inet, además de REYES que es un requerimiento indicado en el PPT.

Respecto a la integración con soluciones de terceros indicar que se aporta una lista destacando las integraciones con FortiOS, Arkime y MISP.

Además, el licitador describe las capacidades de integración de la solución MÓNICA con TheHive/Cortex y Recorded Future, detallando las capacidades de uso como fuentes de inteligencia. También se expone el uso de sus APIs para crear casos de investigación y recibir resultados de sus analizadores.

PUNTUACIÓN OTORGADA: 8 puntos

2.1.2 Tabla puntuación total licitador 1 (hasta 38 puntos)

Criterios	Puntuación obtenida
Calidad de la propuesta técnica	
Características generales de la solución propuesta (15 puntos)	**13,0**
Capacidades SOAR y UEBA implementadas (10 puntos)	**10,0**
Características de la infraestructura hardware aportada por el licitador (5 puntos)	**3,5**
Integraciones aportadas con soluciones del ecosistema CCN-CERT y/o de terceros (8 puntos)	**8,0**
PUNTUACIÓN TOTAL	**34,5**

2.2 Licitador 2: S2 GRUPO SOLUCIONES DE SEGURIDAD, S.L.U.

2.2.1 Calidad de la propuesta técnica

2.2.1.1 Características generales de la solución propuesta, valorando entre otras, el nivel de integración de la solución, el número de fuentes distintas de ingesta, taxonomización y correlación de eventos soportada por la plataforma, la capacidad de gestión de incidentes (workflow), la capacidad para la gestión de playbooks y las capacidades de ingesta de tráfico netflow en sus diferentes versiones y formatos enterprise (como los que puede utilizar Palo Alto) (hasta 15 puntos)

En la propuesta técnica de la solución GLORIA se aporta información sobre su ingesta desde distintas fuentes de información, pero se observan limitaciones a nivel de integración dentro de la solución tanto a nivel gráfico como respecto a sus funcionalidades.
Respecto a la taxonomía y correlación el licitador indica las capacidades de GLORIA, pero no quedan claras ni detalladas las reglas de correlación proporcionadas de forma nativa con la solución.

Con la información aportada se ven limitaciones de funcionalidad respecto a la gestión de incidentes y no se menciona la posibilidad de gestionar playbooks.

En la propuesta no se detallan las capacidades de ingesta de tráfico netflow en sus diferentes versiones y formatos Enterprise.

PUNTUACIÓN OTORGADA: 6 puntos

2.2.1.2 Capacidades SOAR y UEBA implementadas, valorando sus características, funcionalidades y detalle de estas. (hasta 10 puntos)

Respecto a las capacidades SOAR se explican los procesos de enriquecimiento con información de contexto, pero la capacidad de respuesta activa está muy limitada. Se hace referencia básicamente a bloquear IPs en firewalls Fortigate y PaloAlto así como enviar tickets a LUCÍA.

Respecto a las capacidades UEBA, se detallan varias pantallas con dashboards realizando consultas para obtener datos o histogramas, pero no demuestra tener capacidades de análisis de comportamiento y automatización en la detección de anomalías.

PUNTUACIÓN OTORGADA: 3,5 puntos

2.2.1.3 Características de la infraestructura hardware aportada por el licitador, valorando mejoras en las capacidades de ingesta de eventos por segundo, incremento de períodos de retención del almacenamiento primario y secundario, entre otras. (hasta 5 puntos)

El licitador propone una infraestructura hardware que según indica en su propuesta soporta las necesidades especificadas.

Se valoran positivamente los recursos hardware de memoria RAM y almacenamiento secundario aportados en su propuesta.

Además, ofrece un año de garantía adicional a los solicitados.

PUNTUACIÓN OTORGADA: 5 puntos

2.2.1.4 Integraciones aportadas con soluciones del ecosistema CCN-CERT y/o de terceros. Se valorarán mejoras en cuanto al número de integraciones adicionales aportadas, así como del nivel de integración de estas. Así mismo, se valorará positivamente la integración de la solución con fuentes de inteligencia como LUCIA del CCN-CERT, TheHive/Cortex y Recorded Future (hasta 8 puntos)

Respecto a las soluciones del CCN-CERT se ofrece la integración con LUCÍA.

Respecto a la integración con terceros se ofrece la licencia de Tenable Nessus Professional Vulnerability Scanner activa mientras el contrato esté vigente.

No queda claro el nivel de integración dentro de GLORIA con las soluciones de LUCÍA y Nessus Professional respecto a su gestión vía entorno gráfico y los casos de uso.

Se indica que habrá integración con TheHive/Cortex como fuente de inteligencia, pero no se menciona la integración con las APIs para por un lado abrir casos con TheHive y por otro utilizar los analizadores de Cortex.

Respecto a la integración con Recorded Future se indica que se utilizará como fuente de información, pero no se menciona la integración con las APIs de la plataforma.

PUNTUACIÓN OTORGADA: 2,9 puntos

2.2.2 Tabla puntuación total licitador 2 (hasta 38 puntos)

Criterios	Puntuación obtenida
Calidad de la propuesta técnica	
Características generales de la solución propuesta (15 puntos)	**6**
Capacidades SOAR y UEBA implementadas (10 puntos)	**3,5**
Características de la infraestructura hardware aportada por el licitador (5 puntos)	**5**
Integraciones aportadas con soluciones del ecosistema CCN-CERT y/o de terceros (8 puntos)	**2,9**
PUNTUACIÓN TOTAL	**17,4**

3. Tabla resumen de las puntuaciones otorgadas

Licitador	Puntuación obtenida
ICA Sistemas y Seguridad S.L.U.	**34,5**
S2 GRUPO SOLUCIONES DE SEGURIDAD, S.L.U.	**17,4**

4. Tabla final de puntuaciones

Como se indica en el PCAP (apartado 14. Cuadro de criterios de valoración y puntuación), se establece un umbral mínimo en la puntuación de los criterios evaluables por medio de juicio de valor (sobre B) de forma y manera que los licitadores que obtengan una puntuación inferior a 20 puntos quedarán excluidos por no haber alcanzado el nivel suficiente de calidad con la oferta presentada.

Por lo tanto, y según la valoración obtenida en el apartado 3, la tabla final de puntuaciones otorgadas queda:

Licitador	Puntuación obtenida
ICA Sistemas y Seguridad S.L.U.	**34,5**
S2 GRUPO SOLUCIONES DE SEGURIDAD, S.L.U.	**excluido**