INFORME: Informe cumplimiento PPTP

Expte: 12464/2024
SUM 80/2024

Suministro de software de protección de equipos para el Ayuntamiento de Calp

Se han recibido dos ofertas. En este informe se debe valorar únicamente si las especificaciones técnicas del software ofertado se corresponden con las solicitadas en el PPTP.

Las dos ofertas aportan una memoria bastante completa que permite comprobar punto por punto el cumplimiento del PPTP de cada una de ellas. Los productos de protección de software que aporta cada uno son:

La empresa B26523001 ofrece el software de protección Watchguard EDPR + Patch management

La empresa B60345527 ofrece el software de protección SentinelOne Singularity XDR

Una vez realizado el estudio de dichas memorias se puede observar lo siguiente:

Ambos licitadores expresan y demuestran en la memoria el cumplimiento de cada uno de los puntos. Vamos a incidir en dos puntos concretos del PPTP porque son los que podrían resultar más complejos de cumplir:

Conector nativo con el SIEM Splunk disponible en su marketplace

Este punto del PPTP hace referencia a la conectividad entre el software de protección de equipos y el SIEM Splunk. Tras comprobar la memoria entregada y confirmar con las características públicas de ambos productos, se puede afirmar que ambas ofertas cumplen con los requisitos establecidos. Habría que precisar en este punto que, más allá de lo conciso que pueda resultar el PPTP, se puede apreciar claramente que lo que se está solicitando en este caso es la posibilidad de integración entre el SIEM Splunk y el software de protección de equipos ofertado.

Capacidades antitamper: evitar que el producto sea desinstalado, incluso con permisos administrativos, y que las Shadow copies de Windows resulten comprometidas. Aporta protección en caso que el usuario sea vulnerado

Estamos ante una característica que busca evitar las consecuencias de un ataque Ransomware o similar desde dos frentes. Por un lado evitar que un ataque pueda detener y/o desinstalar el software de protección y, por otro, asegurar que las Shadow Copies de Windows permanecen inmutables y, en caso de ataque, asegurar que se puede volver a un estado en el que los ficheros no estén encriptados.

Este punto resulta un poco más complejo. En la primera parte hay que asegurar que el software dispone de mecanismos de anti-tampering y eso es algo que viene explícito en las memorias y que es fácil de comprobar. En la segunda parte hay que asegurar que las Shadow Copies permanecen inmutables. Esta es una característica básica para SentinelOne pero que resulta más difícil de comprobar en Watchguard. No obstante, de la información que se desprende de la memoria ofrecida y de las características de la solución de Watchguard obtenemos:

- Watchguard ofrece de forma nativa capacidades Anti-tampering
- Las Shadow Copies creadas desde Watchguard sólo se pueden borrar desde Watchguard.

Uniendo ambas características se obtiene la funcionalidad deseada, con lo que se debe interpretar que cumple con lo establecido en el PPTP.

Por otro lado, en cuanto al número de licencias ofrecidas, la oferta basada en Watchguard especifica de forma clara y concisa el número de licencias ofrecidas, que se corresponden con las 280 solicitadas en el PPTP como mínimo. La oferta basada en SentinelOne, por su lado, no especifica el número de licencias ofrecidas y esto podría considerarse un incumplimiento del PPTP. No obstante, al declarar responsablemente que acatan las condiciones del PPTP entendemos que este número nunca sería menor de las 280 licencias solicitadas y, si caso, incorporarían más si fuera necesario para cumplir lo solicitado.

Así pues la conclusión final es que **ambas ofertas cumplen con lo establecido en el PPTP** y resultan perfectamente elegibles.

Es cuanto tengo que informar como jefe de área de modernización en Calp a la fecha de la firma

El jefe de área de modernización

DOCUMENTO FIRMADO ELECTRÓNICAMENTE