Virtual SOC

Centro de Operaciones de Ciberseguridad

centro criptológico nacional

Año 2019

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

© Centro Criptológico Nacional, 2019

Fecha de Edición: febrero de 2019

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2019.02.18 01:46:17 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 4

2. INTRODUCCIÓN 4

3. ADMINISTRACIÓN CENTRALIZADA 5

3.1 CORTAFUEGOS. REQUISITOS TÉCNICOS 6

3.2 IMPLEMENTACIONES POR ENTIDADES 6

4. GESTIÓN DE EVENTOS. INTERCAMBIO DE REGLAS. 7

4.1 FUNCIONAMIENTO 8

4.2 REQUISITOS 9

5. PUNTO FINAL. DETECTORES DE ANOMALÍAS 10

5.1 INTERCAMBIO DE INFORMACIÓN 10

5.2 ANÁLISIS FORENSE 11

6. APOYO NORMATIVO 11

6.1 ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD 11

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

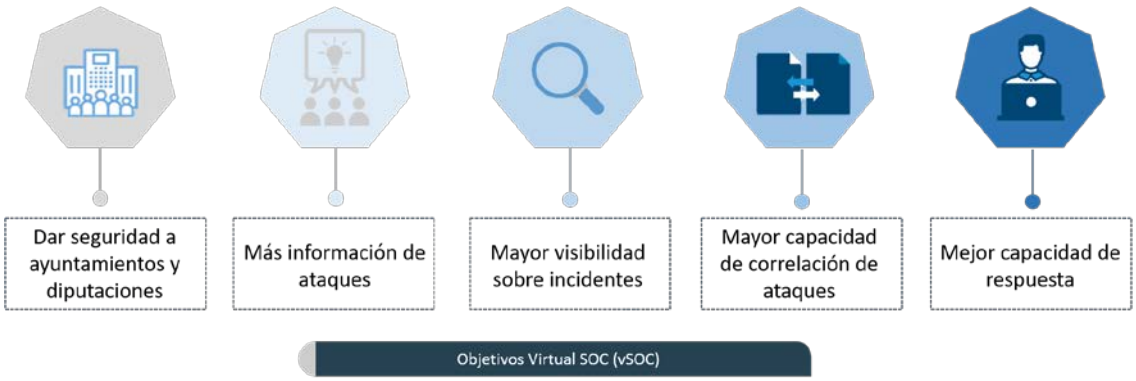
2. INTRODUCCIÓN

El constante aumento de los ciberataques conlleva la necesidad de un incremento y mejora de las capacidades de prevención, monitorización, vigilancia y respuesta, a través de los Centros de Operaciones de Ciberseguridad (SOC) siendo prioritaria su implementación en el ecosistema de la ciberseguridad.

Un SOC tiene por objeto la prestación de servicios horizontales de ciberseguridad, logrando que organismos, entidades e instituciones mejoren sus capacidades de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicación, así como el perfeccionamiento de sus capacidades de respuesta ante cualquier ataque.

El Centro Criptológico Nacional está trabajando en la implementación de Centros de Operaciones de Seguridad virtuales (vSOC) para que las entidades locales puedan conocer su superficie de exposición y optimicen sus recursos en función de la información que manejan y servicios que prestan.

De este modo, ayuntamientos y diputaciones tendrán más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, a la vez que una mejor capacidad de respuesta al disponer de una gestión centralizada de las diferentes entidades adscritas a cada vSOC. Asimismo, se mejoran las capacidades de actuación y protección de las mismas.



3. ADMINISTRACIÓN CENTRALIZADA

Los vSOC inician su labor de protección en la parte perimetral. Asegurar el perímetro y una correcta configuración del mismo se considera la primera prioridad. Para ello, se propone una gestión centralizada, que permite aumentar el número de entidades adscritas a cada vSOC y mejorar las capacidades de despliegue, actuación y protección de las mismas. Asimismo, se debe tender a un uso y conjunto común de reglas con el objetivo de facilitar la gestión y la capacidad de acción ante ataques a las redes informáticas.

Dado que la protección de las comunicaciones con Internet es el primer punto de protección directo a acometer, cada entidad adscrita al vSOC dispondrá de control y gestión sobre su tráfico hacia y desde Internet.

3.1 CORTAFUEGOS. REQUISITOS TÉCNICOS

Una gestión centralizada e instalación unificada de cortafuegos implica tener en cuenta los siguientes aspectos:

- La entidad colaborará con el vSOC en la instalación de un cortafuegos y en la realización de las modificaciones pertinentes en la red para la instalación del dispositivo o en el desvío del tráfico en caso de estar virtualizados en la nube.
- Los cortafuegos deben tener la posibilidad de emitir alertas de seguridad basadas en la detección de eventos, según reglas proporcionadas por el CCN-CERT para su implementación en vSOC.
- La ubicación en un punto de la infraestructura de red, en la parte perimetral, puede dotar a la entidad de análisis del tráfico, aunque se use SSL/https, siempre que la entidad colabore y preste sus certificados en el cortafuegos perimetral.
- Si la entidad no tiene implementado SSL, los vSOC ofrecerán la posibilidad de implantarlo mediante las capacidades y características propias del cortafuegos, que incluye la ayuda en la gestión para la adquisición e instalación del certificado.
- Los cortafuegos deben poder categorizar las *url* o tener una gestión del tráfico hacia Internet por categorías, para realizar un control y monitorización del tráfico por los puertos aprobados para su empleo en Internet.
- Si los cortafuegos tienen funcionalidades para implementar reglas de protección ante intrusiones (IPS), dicha capacidad se puede añadir al servicio dado que supone una mejora en las capacidades de defensa de las entidades.

3.2 IMPLEMENTACIONES POR ENTIDADES

Entre los diferentes vSOC se coordinarán las reglas de IPS e IDS a través del CCN-CERT para tener un conjunto unificado de reglas a aplicar y aunque cada entidad pueda tener sus particularidades, todos los vSOC tendrán una base común:

- Los centros de operación podrán recibir las alertas emitidas por parte del CCN-CERT para tomar las medidas necesarias en el tráfico de red.
- La infraestructura de cortafuegos debe prestar un servicio de 24x7, actuando ante caída del servicio o fallo de hardware en unos tiempos aceptables previamente acordados con la entidad.
- Los fallos de hardware deberán ser solucionados en menos de 24 horas. En caso de entidades con dispositivos no redundados, el tiempo de sustitución y puesta en activo del nuevo hardware no debe superar las cuatro (4) horas.
- Los cambios en las reglas se definirán con la entidad, estableciendo una ventana de tiempo durante la semana para realizar las posibles actuaciones.

- El vSOC dispondrá de medidas de control del tráfico para mejorar la seguridad de la entidad. Las medidas se contrastarán con las necesidades de la propia entidad y se adaptarán para dar los servicios solicitados por la misma.
- Si el cortafuegos lo permite, deberá tener implementadas capacidades de limpieza de correo y medidas contra denegación de servicio.
- Los vSOC pueden prestar soporte y ayuda a la entidad para configurar sistemas de protección de perímetro ante denegaciones de servicio.
- Las modificaciones en las reglas de los cortafuegos deberán ser notificadas por la entidad a los operadores del vSOC. En estos casos, se realizará una validación previa de los parámetros de seguridad para asegurar la adecuación de las mismas, que en caso de aceptación supondrá la implementación de las mismas.
- A las entidades se les aconsejará las medidas a implementar para tener un mayor control del tráfico. Se intentará establecer una política común para todas las entidades cubriendo tanto los accesos permitidos, categorías implementadas y aceptadas, junto con las reglas de IPS e IDS configuradas.
- Las diferentes entidades remitirán sus propuestas de configuración base para su validación por el CCN-CERT y hacer una fusión de las mismas durante las primeras fases de implantación de los primeros vSOC.
- El acceso a los cortafuegos para labores de gestión será únicamente tarea de los operadores del vSOC, la entidad podrá tener acceso de lectura para conocer el estado.
- Cada vSOC debe contar con una infraestructura de monitorización del estado de los equipos para conocer niveles de CPU, uso de discos duros, memoria RAM, estado de las interfaces y errores de hardware además de las consideraciones a monitorizar por cada entidad.
- Se tendrá un teléfono de contacto con los operadores y con la entidad para dar aviso de alertas de seguridad o indisponibilidad del servicio. El horario del servicio debe ser en horario laboral durante la semana.
- La monitorización del estado de funcionamiento de las máquinas debe ser 24x7 durante todo el año para mantener el acceso y funcionamiento de las entidades.
- Mensualmente se trasladará a la entidad un informe del estado de seguridad conseguido y del estado de los dispositivos.

4. GESTIÓN DE EVENTOS. INTERCAMBIO DE REGLAS.

El sistema automatizado de gestión de eventos de seguridad (SIEM) de los VSOC se encargará de la recolección de los *logs* y eventos de seguridad de las entidades, actuando como nivel superior de coordinación de *logs* entre las diferentes entidades de un vSOC.

Por cada entidad se deben recibir las siguientes fuentes de información:

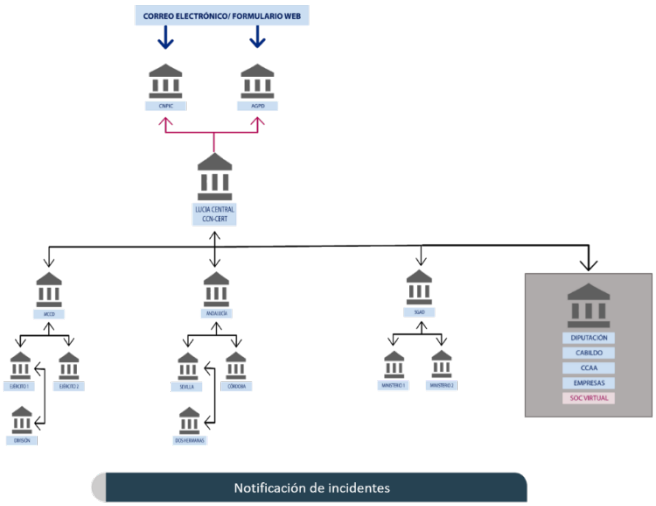
- Eventos de las reglas utilizadas por los IDS instalados en la entidad.
- Reglas de los cortafuegos.
- Logs de equipos relevantes para la entidad conjuntamente con los servidores.
- Logs de los antivirus o *endpoints*.
- Fuentes adicionales que cada vSOC considere oportuna por cada entidad.

Asimismo, el SIEM proveerá de automatización para la generación de notificaciones de nivel 1 (operación procedimental) a la entidad y a su órgano encargado de resolver los eventos de seguridad. Por este motivo, se tendrá que aportar información de valor que permita contrastar los eventos de seguridad y generar las notificaciones con el mayor nivel de detalle, indicando en qué sistemas se ha detectado la alerta de seguridad.

Para la determinación de los niveles de las alertas de seguridad, así como para el establecimiento de la peligrosidad potencial de los incidentes, se utilizará como base la guía CCN-STIC-817 *Gestión de Ciberincidentes*, que además podrá ser personalizada y adaptada a las necesidades de la entidad.

4.1 FUNCIONAMIENTO

Las notificaciones generadas por el SIEM y por los operadores a la entidad se realizarán mediante la solución LUCIA. Esta herramienta, desarrollada por el CCN-CERT, permitirá conocer el flujo del incidente y disponer de métricas sobre la resolución del mismo.



El SIEM, al recibir la información de entidades comunes pero distintas, deberá poder generar incidentes o identificar nuevas tendencias de ataques obtenidos de los eventos de seguridad de cada entidad. Tanto las tendencias como las reglas generadas

para su detección deberán ser enviadas al CCN-CERT para que coordine la validez y distribución de las mismas al resto de vSOC.

Para ello, el SIEM debe poder importar y exportar sus reglas de correlación en un formato estándar (en la actualidad, el proyecto implementado por varios fabricantes es Sigma Rules) a otros SIEM. El uso de las mismas reglas de correlación y su intercambio mejorará la coordinación y la generación de incidentes entre los diferentes vSOC, a su vez coordinados por el CCN-CERT.

Dichas reglas de correlación serán tanto entre fuentes del perímetro como fuentes de la red interna de la entidad. Si la entidad opta por un vSOC con *endpoint* o si obtiene fuentes y registros de comportamiento y ejecuciones de los equipos deberá incluir reglas para generar eventos de seguridad según tales comportamientos.

En la notificación del incidente de seguridad debe aparecer con claridad en todos los elementos donde se ha detectado el evento de seguridad para así facilitar la implantación de contramedidas o la investigación de la misma.

4.2 REQUISITOS

- Los eventos de seguridad almacenados por el SIEM deben ser capaces de exportarse a un formato estándar como, por ejemplo, ELF u otro utilizado por los fabricantes de SIEM y gestores de logs.
- Las reglas de correlación del SIEM deben poder ser exportadas a un formato estándar (Sigma rules) para ser compartidas entres SIEM de diferentes fabricantes.
- Cada entidad deberá retener los logs y eventos de gestión y búsqueda rápida durante un periodo de tres (3) meses. La retención de búsquedas de eventos más

lentas deberá guardarse durante un (1) año y las copias de seguridad, así como los logs de seguridad recibidos, durante tres (3) años.

- El SIEM puede tener la capacidad de recibir las alertas de los servicios de antiDDoS contratado por la entidad. Así, se le proporciona al operador y al vSOC una ventana única de recepción de eventos de seguridad centralizando todo en el SIEM.
- Cada vSOC debe contar con una infraestructura de monitorización del estado de los equipos para conocer niveles de CPU, uso de discos duros, memoria RAM, estado de las interfaces y errores de hardware además de las consideraciones a monitorizar por cada entidad.
- Se tendrá un teléfono de contacto con los operadores y con la entidad para dar aviso de alertas de seguridad o indisponibilidad del servicio. El horario del servicio debe ser en horario laboral durante la semana.
- La monitorización del estado de funcionamiento de las máquinas debe ser 24x7 durante todo el año para mantener el acceso y funcionamiento de las entidades.
- Mensualmente se trasladará a la entidad un informe del estado de seguridad conseguido y del estado de los dispositivos.

5. PUNTO FINAL. DETECTORES DE ANOMALÍAS

La detección en los equipos finales constituye un factor clave en el aviso proactivo de incidentes de seguridad. Por este motivo, se emplean *endpoints,* que pueden tener un antivirus asociado o convivir con el antivirus existente en la entidad. Al final es clave disponer de detectores de anomalías, de comportamiento basados en reglas, de eventos de aplicaciones y acciones llevadas a cabo en los equipos finales.

Los *endpoints* deben actuar en conjunto con los diferentes elementos de seguridad proporcionados por el vSOC. Por ello, toda la información generada por cada *endpoint* debe llegar al SIEM para ser tratada.

5.1 INTERCAMBIO DE INFORMACIÓN

Las reglas de análisis y detección de los *endpoints* deben ser exportadas a una fuente común, de manera que se pueda intercambiar la información entre los diferentes vSOC. Dicha información será remitida mensualmente al CCN-CERT para que se genere el conjunto de reglas comunes que sean la base para todos los vSOC.

Existe la posibilidad de que cada vSOC decida adecuar o generar nuevas reglas adaptadas en exclusiva a la entidad. No obstante, en este caso, será necesario notificarlo al CCN-CERT para que este organismo considere su inclusión en el conjunto de reglas base.

5.2 ANÁLISIS FORENSE

La detección basada en reglas y anomalías pueden abrir una ventana en la búsqueda de APT[1] o código dañino desconocido en los equipos de una entidad, otorgando al vSOC las capacidades de prevención y detección.

Además, los *endpoint* pueden dotar al vSOC de la capacidad de aislar máquinas de la red, de bloquear actividades sospechosas, de detectar correos electrónicos con contenido dañino, hallar usos fraudulentos o indebidos en los equipos, etc.

Al implementar en los equipos un registro adicional al del sistema operativo, se pone a disposición de los vSOC y de las entidades una potente herramienta para el análisis forense de los equipos, así como la capacidad de conocer si fueron infectados o atacados en el pasado con nuevas reglas de detección.

Cada vSOC contará con su *endpoint* y generará una estructura y administración centralizada, lo que permitirá mejorar las capacidades de detección y facilitar la gestión y administración de los sistemas.

6. APOYO NORMATIVO

Los vSOC podrán disponer de un servicio de apoyo normativo para la adecuación de las entidades a su marco normativo, especialmente con relación al Esquema Nacional de Seguridad (ENS).

En función de las necesidades, este apoyo servirá de refuerzo al servicio existente o bien se prestará a aquellas entidades que no dispongan del mismo.

6.1 ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

En este marco de actuación, se incluye la posibilidad de prestar apoyo a las entidades en la adecuación al ENS, de manera que se facilite la implementación de medidas de seguridad y se oriente a las entidades en la declaración de aplicabilidad de las medidas que se le propongan.

Esta labor de asesoramiento sobre las medidas a implementar tiene por objeto lograr la adecuación al ENS, en cumplimiento de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, permitiendo que las entidades sean capaces de superar cualquier auditoría relacionada con esta materia.

Asimismo, se pone a disposición de las entidades un servicio de asesoramiento o consulta adicional para solventar las dudas que pudieran surgir sobre la aplicación del ENS.

[1] Advanced Persistent Threat

©Centro Criptológico Nacional