Implantación y certificación de centros de **operaciones de ciberseguridad**

Centro Criptológico Nacional

La Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional español (CCN-CERT), como catalizador de la ciberseguridad nacional, ha impulsado la creación de centros de operaciones de seguridad (SOC) en otras organizaciones, tanto públicas como privadas.

Este artículo establece una estrategia para la constitución de un SOC, diferenciando dos tipologías:

- **SOC gubernamental:** presta servicios a una o varias instituciones públicas del país.
- **SOC individual:** presta servicios a un único organismo.

Constitución del SOC

No obstante, antes de entrar en materia, es importante definir qué es un SOC. Se trata de un conjunto de capacidades (tecnológicas y humanas) que permite la supervisión y la administración de la seguridad de los sistemas de información de una organización.

La misión de un SOC gubernamental es actuar como componente fundamental de las capacidades nacionales de prevención, protección, detección, coordinación y respuesta ante incidentes de seguridad. Y la de un SOC individual actuar como medida principal para la protección de la ciberseguridad de la propia organización.

En concreto, la comunidad que abarca la primera tipología es el conjunto de instituciones públicas del país. Y está impulsado y patrocinado por una organización o institución pública con competencias en materia de seguridad nacional.

Por su parte, la comunidad de un SOC individual es la propia organización que implementa el SOC, y su institucionalización es decisión de la propia organización.

En ambos casos, el reconocimiento viene de la mano de formar parte de foros internacionales como FIRST.

Catálogo de servicios

El catálogo de servicios que ofrece un SOC es el siguiente:

- **Prevención:** análisis de vulnerabilidades, inspecciones técnicas de seguridad, test de intrusión (*hacking* ético) y vigilancia digital.
- **Protección:** operación de ciberseguridad.
- **Detección:** monitorización de ciberseguridad, *threat hunting* (caza de amenazas) e inteligencia de amenazas.
- **Respuesta:** *Incident Response Team*.
- **Gestión de la ciberseguridad:** asesoramiento en ciberseguridad, cumplimiento legal y normativo y cuadros de mando.

Requisitos operativos

Los servicios anteriores se traducen en los siguientes requisitos operativos:

- **Prevención:**
  - Análisis de vulnerabilidades: es fundamental identificar y remediar las vulnerabilidades existentes en los sistemas y aplicaciones para evitar que sean explotadas por los atacantes.
  - Inspecciones técnicas de seguridad y test de intrusión: ayudan a identificar las vulnerabilidades y debilidades de la infraestructura de TI, así como a evaluar la eficacia de las medidas de seguridad existentes.
  - Vigilancia digital: permite detectar de forma proactiva amenazas y riesgos antes de que se materialicen en un incidente de seguridad.
- **Protección:**
  - Operación de ciberseguridad: implementación de medidas de seguridad como *firewall*, antivirus, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para proteger la infraestructura de TI.
  - Mantener actualizado el software y *firmware* de los sistemas y dispositivos para corregir vulnerabilidades y mejorar la seguridad.
  - Implementar un proceso para la aplicación oportuna de parches de seguridad para corregir vulnerabilidades conocidas.
- **Detección:**
  - Monitorización de ciberseguridad: monitorizar la infraestructura de TI para detectar de forma temprana posibles incidentes de seguridad.

- Análisis de *logs*: recopilar y analizar los *logs* de seguridad para identificar posibles intrusiones o actividades anómalas.
- *Threat hunting*: búsqueda proactiva de amenazas y anomalías que podrían indicar un ataque en curso o inminente.

Respuesta:

- *Incident Response Team*: equipo especializado en la gestión de incidentes de seguridad que puede ayudar a contener el daño, remediar el incidente y restaurar los sistemas afectados.
- Definir y operar un plan de respuesta a incidentes que establezca las acciones a tomar en caso de un ciberincidente.
- En caso de un incidente grave, puede ser necesario realizar un análisis forense para determinar la causa del incidente y el alcance del daño.

Gestión de la ciberseguridad:

- Asesoramiento en ciberseguridad: asesorar a la organización sobre cómo mejorar su postura de seguridad y cumplir con las normativas vigentes.
- Cumplimiento legal y normativo: asegurar que la organización cumple con las leyes y regulaciones relacionadas con la seguridad de la información.
- Formación en seguridad: es importante que el personal de la organización reciba formación en seguridad para que pueda ser consciente de las amenazas y saber cómo actuar en caso de un incidente.
- Cuadros de mando: definir e implantar cuadros de mando que proporcionen información sobre el estado de la seguridad de la organización, como el número de incidentes de seguridad, las vulnerabilidades existentes y el estado de las medidas de seguridad.

La priorización de los requisitos específicos dependerá de las necesidades y riesgos específicos de cada organización. Sin embargo, los requisitos mencionados anteriormente son considerados como críticos para la operación efectiva de un servicio de seguridad.

SERVICIO	SUBSERVICIO	FASE 1	FASE 2	FASE 3	FASE 4
Prevención	Análisis de vulnerabilidades	X	X	X	
	Inspecciones técnicas de seguridad y test de intrusión (*hacking* ético)	X	X		
	Vigilancia digital	X			
Protección	Operación de ciberseguridad	X	X	X	
Detección	Monitorización de ciberseguridad	X	X	X	
	Threat hunting (caza de amenazas)		X	X	
	Inteligencia de amenazas	X	X	X	
Respuesta	*Incident Response Team*	X	X	X	
Gestión de la ciberseguridad	Asesoramiento en ciberseguridad	X			
	Cumplimiento legal y normativo	X			
	Cuadros de mando		X		

Implantación de un SOC

El CCN ha elaborado una tabla que facilita la implementación de los servicios, subservicios y requisitos operativos del SOC de manera escalonada y priorizada. Esta priorización es una recomendación basada en los requisitos operativos de cada servicio y estará finalmente determinada por las necesidades específicas de cada organismo (ver tabla adjunta).

Por su parte, el proceso y los detalles para la certificación de un SOC se definen en la *Guía STIC 896*.

Conclusiones

En definitiva, un centro de operaciones de ciberseguridad es crucial para la seguridad de cualquier organización en la era digital actual, y más aún para las instituciones públicas e infraestructuras críticas de un país.

Este artículo, basado en una guía que el CCN-CERT publicará en breve, pretende servir de guía para la creación e institucionalización de un SOC, incluyendo los servicios que se ofrecerán, la forma de implantarlo y el proceso para su certificación.

Recomendaciones

Por último, cabe destacar una serie de recomendaciones:

- Es necesario realizar una evaluación de riesgos para identificar las principales amenazas de seguridad que enfrenta la organización.
- Se debe implementar un enfoque de defensa en profundidad que combine diferentes medidas de seguridad para proteger la infraestructura de TI.
- Es importante contar con un plan de respuesta a incidentes que defina las acciones a tomar en caso de un ataque.
- También realizar revisiones periódicas de la seguridad para evaluar la eficacia de las medidas de seguridad existentes.
- Se recomienda leer la *Guía STIC 896* para obtener más información sobre la certificación de un SOC.
- Es aconsejable contar con expertos en ciberseguridad para la implementación de un SOC.

No obstante, este artículo no es una guía exhaustiva para implementar un centro de operaciones de seguridad, sino que debe contarse siempre con asesoramiento experto. De hecho, la priorización de los servicios es una recomendación y puede variar según las necesidades de cada organización.