Dudas:

Monitorización + Gestión de incidentes

1. Cuántas instalaciones hay que incluir en la monitorización?

Se deberán monitorizar todas las instalaciones del CABB, en torno a unas 500,

aunque las principales son los 4 CPDs: 2 en Bilbao, 1 en Sestao y otro en Arrigorriaga

2. Cuántas salidas a internet existen (independiente o común)

Actualmente tenemos una salida única internet.

3. Qué tipo de comunicación entre sedes/instalaciones disponen?

Las instalaciones están conectadas entre sí a través de 2 MPLS de nivel 3 (VPRN)

proporcionada por los dos operadores de telecomunicaciones, siendo los medios FTTH, ADSL,

4G, Radioenlace, Tetra y otros.

4. Número de usuarios?

800 usuarios de la empresa 1200 de contratas

5. Número de personal técnico TIC?

40 técnicos

6. Número y tipo de fuentes de seguridad a integrar en el SIEM

(indicar por favor tecnología y fabricante pj: FW Fortinet)?

10 fuentes:

Directorio Activo MS LDAP

Cytomic EPDR

Kasperksy EDR Optimum

Firewalls/NIDS Fortinet

Gestor de logs Firewalls Fortianalyzer y gestor de logs otros dispositivos Fortianalyzer

(NAC, WAF, switches, DHCP, VPN, etc...)

Graylog clientes (800 windows) y servidores (190 servidores Windows y 70 servidores Linux)

Redborder

Umbrella DNS

Antispam cisco ironport

O365 700 cuentas

7. Número de servidores y cuántos pueden considerarse críticos.

Distinguir servidores por físicos y virtuales y sistema operativo.

Unos 260 servidores. 190 servidores Windows y 70 servidores Linux

Servidores críticos: en proceso de clasificación

Servidores físicos: 10%

Servidores virtuales: 90%

8. Herramienta de gestión de incidentes actual?

JIRA Service Desk de Atlassian y LUCIA del CCN-CERT.

9. Herramienta de ticketing de la organización?

JIRA Service Desk de Atlassian

10. Cuántos incidentes han gestionada de media anualmente en los últimos años?

Podrían indicar la criticidad que han tenido estos incidentes (baja, media, alta o crítica)

y su clasificación según la guía CCN-STIC817 u otro estándar que tengan de aplicación?

Se han gestionado unos 300 incidentes de SAT ICS y unos 60 de SAT INET

11. Cuántos de los incidentes anteriores han sido a nivel reputacional (VIPs, marca, web, etc)

Ninguno

12. Sería posible contar con recursos en la infraestructura de virtualización para el despliegue de sondas virtuales de recolección?

En caso negativo, el HW proporcionado, podría ser desplegado en su rack ofreciendo el espacio y la alimentación eléctrica necesaria?

Habría que estudiar los requisitos de dichas sondas, pero sí es viable.

En caso de no poder contar con la infraestructura de virtualización el CABB puede albergar el hardware para sondas de recolección.

Inteligencia

1. TOE vigilancia digital (ciberinteligencia)

1. Número de direcciones IP públicas +- 30

2. Webs (incluir url) +- 50

3. Dominios 2

4. Nombres de marca y palabras clave a monitorizar

Esta información se proporcionará a la contratación del servicio.

5. Número de VIPs

50

2. Cuál es el volumen estimado de informes a demanda de incidentes concretos?

En cada incidente se hará un reporte de qué ha pasado y como se ha resuelto el mismo.

Se hará en el sistema que decida el CABB : Jira o Lucia… y en algunos casos habrá

que hacer informes más detallados con forense y otros…

No podemos estimar cuántos al no haber tenido nada importante que analizar.

3. Se deben incluir servicios de takedown? Qué volumen estiman anualmente?

No, solo la gestión con Cyberzaintza o CCN para que estas entidades promuevan el takedown.

Auditorías

1. Número de activos OT y tipo

10 activos OT tipo SCADA

2. Número de activos IT y tipo

10 activos IT tipo Servidor Windows, servidor Linux o PC

General

1. **Podrían incluir más detalle o segmentar cómo van a valorar los criterios sometidos a juicio de valor.**

Los criterios sometidos a juicio de valor son los indicados en el pliego administrativo.

2. **A modo de poder tener una estimación lo más ajustada posible, adicionalmente de las actividades de implantación, de los trabajos de auditorías y la respuesta frente a incidentes de seguridad que requieran presencialidad, qué más actividades consideran que van a requerir la presencia en sus instalaciones?**

Las tareas citadas (actividades de implantación, de los trabajos de auditorías y la respuesta frente

a incidentes de seguridad) son las que se estiman que requieren presencialidad.