Euskal Herriko Zibersegurtasun Industrien Elkartea - Asociación de Industrias de Ciberseguridad del País Vasco

Grupo de Trabajo – Seguridad Embarcada industrial – Mayo 2022

Respuesta a incidentes – “Plataforma 1-1-2” para empresas.

Dirigido al gran numero de empresas industriales pequeñas que no cuentan con soporte técnico especializado en ciberseguridad.

¿Qué es?: Respuesta reactiva a incidencias. La empresa ha sufrido un ataque con consecuencias y busca quien le puede dar solución a la incidencia.

Solución prestada por empresa de servicios acompañada de producto.

Plataforma donde según síntomas percibidas por la empresa busca que empresa ofrece el servicio para dar una solución

¿Qué no es?: No es un escaparate donde las empresas publican su portfolio de soluciones.

Visión

Corto plazo

Identificar / clasificar tipos de incidencias

(Ransomware, caída de los sistemas IT/OT, estafa bancaría, fuga de información, phishing, sistemas secuestrados…)

Filtrar ámbito de actuación

(Red IT, red OT, dispositivo PLC, comunicaciones, solución backup, sistemas servidor, puesto de usuario…)

Otros filtros de actuación de la empresa de servicios

(Cercanía geográfica, servicios fuera de horario, experiencia…)

Medio plazo

Seleccionar plataforma

(Web con fichas tipo libro blanco, formularios de solicitud de apertura de incidencias…)

Divulgación y Concienciación

(Eventos explicando el alcance de la solución)

Largo plazo

Atención a incidencias mayores

(Coordinación de diferentes empresas de servicios/producto para poder dar solución a una incidencia de mayor espectro)

Iniciativas conjuntas de desarrollo e innovación

Oportunidades conjuntas en mercados exteriores

CYBASQUE

Puntos en común :que hay que considerar

112. CYBASQUE

RESPUESTA: Empresas

RESPUESTA ANTE INCIDENTES

- Proceso de homologación (Bases mínimas)
- Categorización (peligroso)

I+D Y COMPARTICIÓN

- Baque Cybersecurity Shared
- Compartición de datos e incidentes
- Foro MISP
- Explotación

VULNERABILIDADES

Recap reunión anterior

- Compartir intereses sobre “Respuesta Coordinada a Incidentes”
- Diferentes puntos de vista
  - Empresas con foco en servicios de mercado que ya se ofrecen actualmente
    - Falta información y concienciación en las pequeñas
    - Afinar coordinación y respuesta en las grandes
  - Empresas con foco en producto
  - I+D / formación: CCTT, universidades, etc
- Reunión colaborativa y con muchas ideas interesantes
- Hemos tratado de seleccionar aquellas que causaron mayor interés para impulsarlas

Ideas: priorización

- 112! Cyber: definir “catalogo” desde CYBASQUE para ser un aglutinador o punto de encuentro. Algo mas afinado que el libro blanco. Comenzar con algo de “mínimos y sencillo”, pero ponerlo en práctica en 2022
- Inteligencia: reuniones periódicas para compartir experiencias o incidentes más comunes. A medio plazo crear un mailing-list o grupo de trabajo especifico?
- Concienciación: eventos y comunicación a la sociedad
- Innovación y Desarrollo Tecnológico: iniciativas de mejora de servicios, procesos y productos en el ámbito
- Abierto a otras ideas

Acciones

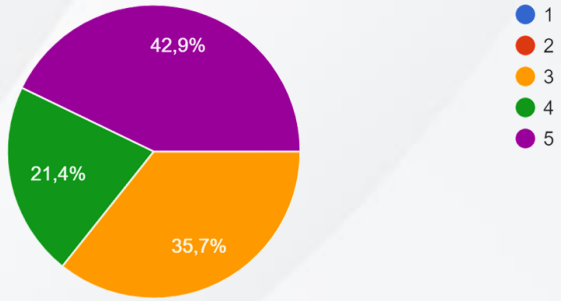
Encuesta de interés por iniciativa?

- 112! Cyber: siguientes pasos
  - TBD
- Inteligencia: reuniones especifica en Julio?
  - TBD
- Concienciación: eventos y comunicación a la sociedad
  - BIEMH
- Innovación y Desarrollo Tecnológico: iniciativas de mejora de servicios, procesos y productos en el ámbito
  - Reflexión

Resultados encuesta en directo

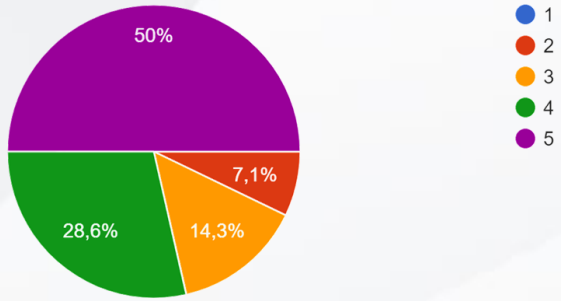
112!Cyber: ¿Como valoras el interés en la iniciativa? Valora del 1 al 5 - Siendo 1 menor y 5 mayor interes.

14 respuestas



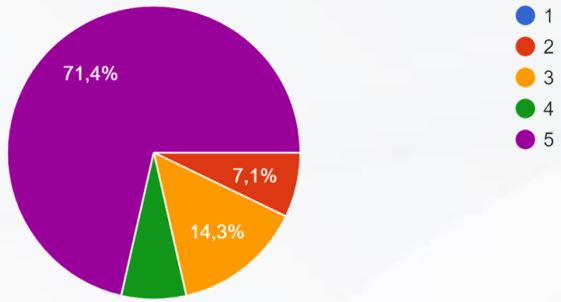
Inteligencia: ¿Como valoras el interés en hacer reuniones de compartición? Valora del 1 al 5 - Siendo 1 menor y 5 mayor interés.

14 respuestas



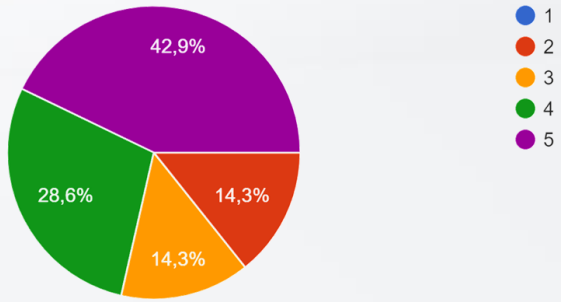
Concienciación: ¿Como valoras el interés en hacer eventos de difusión? Valora del 1 al 5 - Siendo 1 menor y 5 mayor interés.

14 respuestas



Innovación y Desarrollo Tecnológico: iniciativas de mejora de servicios, procesos y productos en el ámbito. ¿Como valoras el interés en hacer eventos d...lora del 1 al 5 - Siendo 1 menor y 5 mayor interés.

14 respuestas



Respuesta a Incidentes

Fase1: (Junio 2022) Recopilar datos. Servicio ofrecido – Ámbito geográfico – Tiempo de respuesta.

Envío de datos.

Fase2: Elegir plataforma y dar a conocer. (Seguido con datos recopilados)

Web tipo formulario con filtro con el contacto como resultado.

Eventos donde se anuncia la publicación del servicio

Fase3: Plataforma de gestión de la información de las incidencias, compartición y explotación.

- Disponer de un repositorio de datos construido a partir de **fuentes de información confiables.**
- Construido sobre la base de una infraestructura compartida y distribuida en la que se garantice la **confidencialidad** de los datos puestos en común en los términos predefinidos por las fuentes.
- Sobre el que se puedan desarrollar herramientas para **mejorar el conocimiento de las amenazas** a los que se enfrenta una organización y/o territorio haciendo uso de información propia y ajena

Envío por correo antes del 08/06/2022

Fase1: (Junio 2022) Recopilar datos. Servicio ofrecido – Ámbito geográfico – Tiempo de respuesta.

Link a formulario:

Servicio ofrecido en caso de….

Encriptación de ficheros
Cuentas vulneradas
Sistemas inestables por posible ataque, virus…
Envío de correos
Estafas (Falso técnico, fraude del CEO…)

Donde se debe dar el servicio cuando es presencial

Zona local Donostialdea, solo Gipuzkoa, solo país Vasco, ámbito nacional….

Tiempo de respuesta y horario

De lunes a viernes 9x5 Presencial, 24x7 telemático….

Fase2: (Julio 2022) Elegir plataforma y planificar eventos para dar a conocer servicios.

- Plataforma web. ¿Web propia del servicio?, ¿Cybasque?, ¿BCSC?...
- Organización de Eventos == > Salva

¡Eskerrik asko!

jmitxelena@cybasque.eus | 943 31 66 66