Convocatoria 06/24 – CONVOCATORIA DE PRUEBAS SELECTIVAS PARA CUBRIR 2 PLAZAS DE PERSONAL LABORAL TÉCNICO EN LA CNMV. TÉCNICOS ESPECIALISTAS EN CIBERSEGURIDAD Y SUPERVISIÓN DE RIESGO TECNOLÓGICO

Tercera parte: ejercicio escrito – Resolución de ejercicios
Especialidad: Ciberseguridad

DESCRIPCIÓN DEL CASO

La Agencia Nacional de Servicios Digitales (ANSD), es una administración que presta servicios digitales a ciudadanía y empleados públicos.

A continuación, se enumeran las características tecnológicas de la organización:

- El número total de usuarios dentro de la organización es 2300 empleados.
- Los puestos de usuario existentes son 2600 endpoints, las versiones son Windows 10 y Windows 11, tanto PC como portátiles.
- Existen un total de 240 servidores, 150 Windows Server y 90 Linux con diferentes distribuciones.
- En todo el territorio nacional existen 45 sedes conectadas mediante MPLS/SD-WAN y 2 CPDs on-premise.
- La arquitectura de red general está constituida por 2 Firewalls. Uno actúa como Firewall perimetral, el otro como Firewall de datacenter. Adicionalmente, se dispone de un proxy web para la navegación de los usuarios y la salida a internet de las aplicaciones web.
- La gestión de identidades está gestionada en un Active Directory on-premise existiendo una sincronización con Entra ID.
- En el ámbito del correo y herramientas colaborativas, se dispone de la suite de Microsoft 365 utilizando herramientas como Sharepoint y Teams.
- En Azure existen 25 máquinas virtuales, 6 storage accounts y 3 bases de datos en modalidad PaaS (Microsoft SQL).
- ANSD dispone de un modelo de teletrabajo, el acceso es a través de VPN con un pico concurrente de 900 usuarios.
- El EDR se encuentra desplegado en un 85% de los puestos, el 15% restante está sin EDR por motivos de compatibilidad y obsolescencia.
- En materia de gestión de vulnerabilidades, se realizan escaneos mensuales en la red interna. Para la parte externa, se subcontrata un servicio trimestralmente permitiendo evaluar los servicios expuestos.

- En materia de SOC, actualmente, existe una cobertura 8x5 con equipo interno reducido; la solución de SIEM es open source con casos de uso mínimos. La retención es de 15 días. No se dispone de solución SOAR.

Retos de la organización:

a) Las campañas de phishing han incrementado en los últimos años. El riesgo de compromiso por ataques de ingeniería social ha aumentado.
b) En algunas sedes existe shadow IT debido a la ausencia de un modelo de gestión centralizado de IT. Las configuraciones de red son dispares, por lo que la complejidad en la gestión es significativa.
c) Hay un importante reto en materia de visibilidad y priorización de las vulnerabilidades.
d) El modelo de SOC que existe requiere de una evolución a un servicio más maduro, que debe garantizar la detección, respuesta y cierta automatización en los procesos.

Debes tener en cuenta las características organizativas descritas anteriormente y el contexto previamente definido para responder a las preguntas que se plantean a continuación:

1) **Desarrolla una propuesta de evolución al modelo de SOC descrito y el dimensionamiento del mismo. Realiza la evolución del SOC siguiendo los siguientes apartados (20 puntos):**

    a. **Propón un modelo SOC para ANSD, apoyándote en un diagrama, que cubra aspectos de detección y respuesta. Para ello considera los siguientes requisitos (8 puntos):**

        i. Cobertura horaria (manteniendo el 8x5 de servicio interno con un 24x7 subcontratado adicional).
        ii. La arquitectura propuesta debe considerar al menos, el SIEM, el proceso de ingesta, normalización, sandbox, EDR, M365, Azure, VPN, Proxy, FW e IDS.
        iii. Casos de uso prioritarios. Selecciona 5 amenazas reales para la ANSD.
        iv. Diseña 3 Playbooks que automatizarías primero y define al menos 2 métricas para medir su eficacia.

b. **Calcula el total de EPS y almacenamiento necesario, proporcionando al menos los siguientes datos (8 puntos):**

i. EPS total estimado.
ii. Volumen diario bruto (bytes) y volumen almacenado tras compresión.
iii. Almacenamiento para 30 días (en TB).
iv. Plantea 2 posibles supuestos y márgenes para picos de EPS (~ 20%).

Para realizar las estimaciones se proporciona la siguiente información:

Activo	Número de activos	EPS aproximados por unidad
Controlador de dominio (DC)	3	20 EPS
Servidores Windows (Member Server)	147	8 EPS
Servidores Linux	90	5 EPS
Endpoint Windows	2600	Endpoint de usuario (Windows, eventos de seguridad filtrados, alertas de EDR, etc.) 0,2 EPS
Firewall	2	250 EPS
IDS/IPS	1	150 EPS
Proxy web	1	200 EPS
Concentrador VPN	1	60 EPS
DNS internos	2	40 EPS
Auditoria M365 / Entra ID sign-in logs	1	40 EPS (consolidado).
EDR canal de alertas	1	80 EPS (consolidado).

El tamaño medio de evento en bruto son 500 bytes.
Compresión estimada en repositorio SIEM: 40% de ahorro (**es decir, ocupa el 60% en bruto)**

c. **Propón un plan incremental para evolucionar el SOC de ANSD desde la situación actual hasta un modelo operativo maduro, maximizando el valor sin interrumpir el servicio (4 puntos):**

i. Divide la implantación en tres oleadas con hitos a 90 / 180 / 360 días, e indica para cada una de ellas y de forma concisa los siguientes elementos:

1. Objetivos medibles por oleada.
2. Fuentes/logs a ingestar.
3. Casos de uso y playbooks, incluyendo el disparador, acciones y la salida esperada.
4. Posibles quick wins (e.g. turnos, gestión de alertas, comunicaciones con CISO/negocio) y formación requerida.
5. KPIs, al menos dos, por cada oleada.
6. Criterio de "hecho" de cada oleada.

2) **Se ha detectado un incidente de seguridad dentro de ANSD. Con la información que se te proporciona a continuación, debes analizar, contener y responder al incidente de seguridad (15 puntos):**

Evidencia 1 – Resumen cabecera de email

```
Return-Path: <tesoreria@ansd.es>
From: "Tesorería ANSD" <tesoreria@ansd.es>
Reply-To: no-reply@micros0ft-support.com
Subject: [URGENTE] Factura pendiente 823-2025
Received: from unknown (HELO mx-23) by mail-gw.ansd.es with ESMTP;
  Tue, 02 Sep 2025 09:12:33 +0200
Authentication-Results: mail-gw.ansd.es;
  spf=fail smtp.mailfrom=ansd.es;
  dkim=none (no signature);
  dmarc=fail (p=reject) header.from=ansd.es
X-Attachment: factura_823-2025.zip
X-URL: hxxps://login-microsoftonline.support-auth[.]co/signin?cid=7f2...
```

Evidencia 2 – Resumen alertas EDR

- Equipo: ANSD-LT-1821 (usuario: jramirez)
- Evento 1 (09:15:03): *powershell.exe -WindowStyle hidden -enc SQBFAFgA...*
- Evento 2 (09:15:18): Creación de tarea programada *\Microsoft\Windows\Update\Updater*
- Evento 3 (09:15:44): Nuevo fichero *C:\Users\jramirez\AppData\Roaming\update\invoice.exe* (SHA256: d4b0...9f)
- Evento 4 (09:15:44): Conexión saliente 185.199.110.153:443
- Evento 5 (09:16:02): Intento de acceso a *lsass.exe* por *invoice.exe* (bloqueado por EDR)

Evidencia 3 – Resumen Firewall/IDS

```
2025-09-02T09:15:44Z ALLOW 10.12.34.56 185.199.110.153 49733 443 TCP
2025-09-02T09:16:02Z DENY  10.12.34.56 10.20.30.5    49801 445 TCP  (SMB LATERAL BLOCKED)
```

a) Lista acciones en orden explicando brevemente cada una de ellas. Define un timeline que soporte tu hipótesis.

b) ¿Qué otras fuentes (al menos 3), aparte de las listadas, se podrían consultar para localizar más información del incidente? Indica sobre el timeline del apartado anterior, cómo podrías mejorar tu hipótesis con las nuevas evidencias que podrías detectar.

c) Propón mecanismos de detección y control preventivos dentro del siguiente listado:
    i. Al menos 3 reglas para el SIEM.
    ii. Al menos 3 mejoras en la protección del correo electrónico.
    iii. Al menos 2 controles sobre el endpoint.

3) Para el desarrollo de este ejercicio se te facilitan las siguientes consideraciones (12 puntos):

- Varias cuentas de servicio tienen privilegios excesivos y contraseñas sin rotación.
- Algunos administradores todavía utilizan credenciales locales compartidas en servidores.
- La cobertura de MFA no llega al 100%. Faltan usuarios VIP y externos.
- Se han reportado incidentes de intentos de password spraying y accesos sospechosos desde localizaciones inusuales.

Evalúa la capacidad para gestionar identidades y accesos privilegiados en un entorno híbrido (on-premise y cloud), aplicando principios de mínimos privilegios, autenticación robusta y detección de anomalías. Para ello, responde a los siguientes apartados:

a. Para la aplicación de mínimos privilegios:
    i. Realiza una definición básica de roles (RBAC) para al menos 4 perfiles distintos, indicando la tipología de cada uno de ellos (e.g. administradores de la infraestructura, usuario estándar, etc.).
    ii. Define al menos 3 mecanismos de gestión de cuentas privilegiadas (PAM).
    iii. Define al menos 3 medidas complementarias.

b. Para la mejora de las capacidades de autenticación fuerte:
    i. Explica cómo lograrías una cobertura del 100 % de MFA, justificando como tratarías excepciones (e.g. cuentas de servicio).
    ii. Propón 2 políticas de acceso condicional.

c. Para la mejora de la detección de posibles anomalías de la identidad:
    i. Propón al menos 3 reglas de detección/anomalías que sean útiles para el SOC, relacionadas con la identidad.

ii. Identifica qué fuentes de datos usarías para cada regla y justifica la respuesta.

4) **En ANSD existen una serie de vulnerabilidades identificadas por activo en la última iteración. Teniendo en cuenta la información resumida en la siguiente tabla, resuelve las siguientes cuestiones (8 puntos):**

a. Ordena las vulnerabilidades por riesgo, considerando la exposición, facilidad de explotación, impacto y controles compensatorios actuales. Justifica brevemente el orden propuesto para cada una de las vulnerabilidades.

b. Define al menos 1 plan de acción para cada una de las vulnerabilidades, incluyendo al menos área responsable, SLA por criticidad, validación post-mitigación así como los pasos que consideres necesarios.

Nombre activo	Versión sistema operativo	Vulnerabilidad	Criticidad	Comentarios
SRV-WIN-APP01	Windows Server 2019	CVE-2021-34525(PrintNightmare)	Alta	KB no aplicado
		SMB signing disabled	Media	
		Acepta TLS 1.0/1.1	Media	
SRV-LNX-WEB02	Ubuntu 20.04	OpenSSL 1.1.1f	Media	Faltan parches menores acumulativos
		CVE-2022-23943 (nginx)	Alta	
		Cabeceras de seguridad HTTP ausentes	Baja	Ausencia de HSTS, CSP
APP-EXTERNA	-	SQLi potencial	Crítica	SQLi en parámetro id confirmado en test de intrusión
		Directorio /backup/ accesible publicamente	Alta	

c. Propón al menos 3 KPIs para un servicio de gestión de vulnerabilidades que tenga valor para el departamento de IT o para el negocio. Justifica la elección de las métricas.

5) **En la ANSD, el EDR no está desplegado en la totalidad del parque tecnológico y algunos usuarios han reportado que, al navegar por Internet, se abren ventanas emergentes y páginas con publicidad sospechosa. El SOC también ha detectado que las políticas de seguridad en los navegadores no son homogéneas en toda la organización (6 puntos).**

Teniendo en cuenta esta situación, indica:

a. Qué medidas prácticas (al menos 2) propondrías para mejorar la cobertura del EDR y asegurar que los agentes están activos y actualizados.

b. Qué controles (al menos 2) aplicarías en los navegadores corporativos para reducir los riesgos de malware y phishing.

c. Qué recomendaciones básicas (al menos 2) transmitirías a los usuarios para fomentar un uso seguro del correo y la navegación web.