www.DarFe.es

"Charlas sobre Ciberseguridad"

(módulo: cursos On-Line Ciberseguridad ***moodle.darFe.es****)*

TEMA 7

Ciberseguridad: empleo de SOC y NOC

(Jueves 28 de septiembre de 2017)

Índice

1. INTRODUCCIÓN

Esta es la séptima de las charlas de este ciclo, abordaremos hoy dos actividades fundamentales desde el punto de vista de la Ciberseguridad.

La metodología de trabajo de un **NOC** (Network Operation Center) y un **SOC** (Security Operation Center) son aspectos clave que debemos comprender y diferencias bien entre sí pues, en muchos casos, se superponen o peor aún, dejan de cubrirse ciertos aspectos por no definir claramente sus funciones y responsabilidades.

2. OBJETIVO

Presentar una visión clara de las responsabilidades y funciones de cada uno de ellos para reforzar el trabajo de ciberseguridad.

3. TEMARIO Y FECHAS DE TODO EL CICLO 2017

A continuación se presentan la totalidad de las charlas que conforman este ciclo durante el año 2017.

Temario y fechas

Nº	Tema de la charla	Fecha
1	**Presentación, conceptos y situación de Cyberseguridad. *¿De quién nos defendemos?***	**Jueves 30 de marzo**
2	**Estrategias de Cyberseguridad en grandes redes (*Seguir y perseguir - proteger y proceder*)**	**Jueves 27 de abril**
3	**Ciberdefensa en profundidad y en altura (*la conquista de las cumbres*)**	**Jueves 25 de mayo**
4	**Ciberseguridad: La importancia de los procesos.**	**Jueves 29 de junio**
5	**Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red**	**Jueves 27 de Julio**
6	**Ciberseguridad: Cómo son las entrañas de esta gran red mundial**	**Jueves 31 de agosto**
7	**Ciberseguridad: empleo de SOC y NOC**	**Jueves 28 de setiembre**
8	**Ciberseguridad: la importancia de saber gestionar "Logs"**	**Jueves 26 de octubre**

4. PRESENTACIÓN DEL TEMA DE HOY

Ciberseguridad: empleo de SOC y NOC (Jueves 28 de septiembre)

Desde el punto de vista de Ciberseguridad, para poder ofrecer un grado mínimo de "Disponibilidad" y "Alarmas tempranas" es necesario contar con una infraestructura de "Supervisión y Monitorización".

Ambas funciones se llevan a cabo a través de:

- **NOC** (Network Operation Center).
- **SOC** (Security Operation Center).

Desde ya que estas funciones deberán ser acordes al tipo de red y se deberá asignar los recursos adecuados para cada tipología, pero lo importante aquí es ser conscientes de la importancia que revista esta actividad y plantearse SIEMPRE cómo se llevará a cabo, por mínima que sea la infraestructura.

En este Webinar se definirán los aspectos que deben ser tenidos en cuenta, en general se presentan con un "objetivo de máxima", es decir lo ideal que podríamos plantear si tuviéramos un NOC y un SOC 24x7, pero reiteramos, lo importante es no olvidarse de esta actividad y ajustarla a la red que cada uno posea.

En cuanto a la Supervisión / Monitorización / Alarmas, nuestra experiencia al respecto es muy positiva. En general todas las redes, poseen algún tipo de mecanismos para esta actividad.

El aspecto sobre el que vamos comenzar es el el "*Flujo y categorización*" de alarmas e *incidentes de seguridad*. Para ello, inicialmente debemos diferenciar el concepto de "**NOC**: Network Operation Center" del de "**SOC**: Security Operation Center", pues este último sí debería abocarse exclusivamente a seguridad, mientras que el primero no. La cuestión, tal cual planteamos al inicio, está en que no todas las redes poseen SOC (*y tampoco se justifica que lo tengan*), en estos casos, evidentemente algún tipo de tareas relacionadas a seguridad deberían recaer sobre el NOC.

Sea cual fuere la situación (con o sin SOC), nuestro objetivo debería conducirnos a obtener una visión clara sobre:

> **¿Qué hace este personal si detecta alguna anomalía en la red, cuyos parámetros puedan esta relacionados con un incidente de seguridad?**

5. RESUMEN TEMAS DE LOS MESES ANTERIORES.

Hemos ido avanzando en conceptos , definiciones, ideas, opiniones de empresas líderes del mercado, analizando niveles de intrusos, predicciones para este año: Organizaciones mafiosas, análisis internacional de grandes empresas, "**Resiliencia**". Presentamos dos estrategias que nos ofrece la **RFC 1244**: *Proteger y Proceder - Seguir y Perseguir.* Nuestra propuesta fue, invitaros a que seáis "audaces" y preparéis vuestras infraestructuras paso a paso para enfrentar la segunda de ellas, dejando de lado el viejo concepto estático de la defensa, para poder plantear vuestra seguridad por medio del concepto militar de "**Acción Retardante**" y avanzamos sobre esta operación.

Continuamos nuestro ciclo, haciendo una analogía entre el "**combate de montaña**" y cómo podemos pensar en alturas de nuestras redes y un análisis del reglamento militar.

Quedó la reflexión sobre las alturas dominantes.

- Planos de altura (*Niveles TCP/IP*).
- Planos de Segmentación (*redes de Gestión y de Servicio*).

En la cuarta charla nos centramos en los **procesos** que creemos fundamentales en nuestras infraestructuras:

- Entrada en producción
- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de Backup
- Gestión de Incidencias
- Supervisión y Monitorización
- Gestión de Logs
- Gestión de actualizaciones

En la quinta hablamos de diferentes **plataformas / infraestructuras de seguridad** que debemos considerar para avanzar en la protección de nuestras empresas.

La última charla nos describió las **entrañas** de esta gran red mundial, a través de esos "**tubos**" que son el soporte de los grandes "**Carriers**" (Tier 1), que operan sobre el protocolo **BGP** (Border Gateway Protocol) para encaminar sus enormes volúmenes de tráfico y resuelven estas direcciones a un lenguaje un poco más humano a través de la jerarquía de **DNS** (Domain Name System).

6. DEBATE SOBRE TAREAS PARA EL HOGAR

Antes de avanzar sobre el tema de hoy, retomemos lo que os invité a tratar durante todo este mes:

1. ¿Cómo llevas los conceptos de medio físico?, ¿tienes claro los tipos de cables, fibras y emisiones de radio que existen?
2. Identifica en tu País, quiénes son tu Tier 1, 2 y 3.
3. ¿Empleas BGP en alguno de tus routers?, en ese caso ¿Empleas autenticación de neighborhood?
4. Explora la Web: http://he.net/3d-map/ y analiza sus contenidos.
5. ¿Quiénes son tus DNSs de jerarquía superior?
6. ¿Has avanzado sobre DNSec en tus redes?, ¿Qué conclusiones o comentarios merece?

7. NOC (Network Operation Center)

Los **NOC** o también llamados **CCR** (Centro de Control de Red), nacen en los años 60 para obtener información del estado de routers y swithcs. Se trata de ubicaciones físicas hacia donde converge toda la información de supervisión, monitorización y alarmas de la red o infraestructuras que tiene bajo su responsabilidad. Se trata de un conjunto de recursos humanos y materiales que están **24x7** los **365 días** del año y cuyas funciones básicas son:

- Monitorización y detección de eventos
- Clasificar y categorizarlos (Determinar impacto)
- Documentarlos (Sistema de Ticketing)
- Gestión de alarmas
- Gestión de incidentes
- Gestión de peticiones (Control de cambios)
- Gestión de accesos
- Gestión de inventario

Podríamos pensar que la "Monitorización y detección de eventos" es su rol primario, cada evento que llega debe pasar a una segunda instancia "Clasificar y categorizarlos" que permite determinar su impacto y derivarlo a su cadena de escalada correspondiente una vez "documentado", para lo cual una muy buena estrategia es contar con un sólido sistema de "ticketing".

La pregunta natural que nos podemos hacer entonces es ¿Qué es un evento para el NOC?

Ejemplos típicos de ello son:

a) Incremento anómalo de ancho de banda.
b) Saturación del ancho de banda.
c) Caídas o fallos de dispositivos.
d) Caídas o fallos de algún enlace.
e) Propagación abusiva de un determinado patrón de tráfico.
f) Modificaciones sensibles del flujo de tráfico de nuestros DNSs.
g) Incremento llamativo del volumen de Logs.
h) Mensajes anómalos en los Logs de elementos de red.
i) Alarmas en bases de datos, procesadores, módulos de memoria.
j) Alteración de rutas.
k) Fallos en los sistemas de señalización.
l) Segmentos de red o dispositivos inalcanzables.
m) Pérdidas de accesos de gestión a dispositivos.
n) Modificación de contraseñas, cuentas, perfiles, roles, o directorios activos.
o) Intentos reiterados de accesos (fallidos o no).
p) Escaneos anómalos de red o puertos.
q) Etc.

Con este tipo de ocurrencias, se está ante indicios de algo que puede guardar relación con incidentes en los dispositivos o enlaces de la red. En principio un procedimiento de gestión de Supervisión / monitorización, debe contemplar si están o no tipificados estos casos, en el caso de no estarlo, se debe lanzar una secuencia de acciones, por ejemplo:

a) ¿Se trata de un evento de red o de seguridad?

b) ¿Existe un procedimiento ante estos casos específicos?

c) ¿Se conocen o definen los pasos a seguir?

d) Dentro del workflow de este centro, ¿está contemplado o tipificado algún "ticket" (o varios tipos de "tickets") para este tipo de eventos?

e) ¿Está categorizado este flujo para incidentes de red o de seguridad?

f) ¿Se conoce la jerarquía, niveles de escalado o cadena de comunicación para estos casos?

g) ¿Cómo se abre, verifica, mantiene y cierran estas incidencias?

Por supuesto, estamos presentando el tema, sobre la base de un NOC que está en producción. Si aún se está planificando o recién se está implantando el mismo, hay más consideraciones que deben ser tenidas en cuenta son:

- Situación de los centros de supervisión de red.

  Que existan en nuestras redes, que posean las herramientas necesarias, que el personal tenga documentadas y comprenda sus funciones, responsabilidades y obligaciones, que los elementos y eventos a monitorizar y supervisar sean acordes al dimensionamiento del centro.

- Que se generen los "Registros de auditoría y monitorización".

  Que se contemple su revisión de forma continua junto a la eficacia y eficiencia de los controles de seguridad establecidos, así como la detección de las anomalías que puedan afectar a la seguridad de la información y los recursos de la empresa.

  Para ello es necesario definir, implantar y/o gestionar:

  - los requisitos y tecnologías de generación y almacenamiento de los registros de auditoría.
  - los procedimientos y tecnologías de monitorización de los registros de auditoría.

  Se deberían registrar todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la confidencialidad, integridad y/o disponibilidad de la información. Especialmente se registrará la actividad de los administradores y operadores de los sistemas de información.

En cuanto a la supervisión hay consideraciones específicas que deben ser detectados para luego poder enviarlos o no al SOC:

a. ¿Se registra especialmente la actividad de los administradores y operadores de los sistemas de información?

b. ¿Se realiza algún tipo de análisis para determinar la profundidad o cantidad de eventos a registrar en un sistema de información o red de comunicaciones?

c. En cualquier caso, se supervisan y monitorizan adecuadamente los eventos de seguridad que se detallan a continuación?:

- los eventos requeridos por la legislación aplicable.
- los intentos de autenticación fallidos.
- los accesos de los usuarios a los dispositivos, tanto autorizados como los intentos no autorizados.
- los eventos de operación y administración de los sistemas: el uso de cuentas privilegiadas de administración (*root, admin, etc*.), el uso de programas y utilidades de administración, la parada y arranque de los sistemas, la instalación o desinstalación de dispositivos de almacenamiento o de entrada/salida, etc.
- los cambios en los parámetros de configuración de los sistemas.
- los errores de funcionamiento de los sistemas y las redes.
- los accesos a redes de comunicaciones, tanto autorizados como los intentos no autorizados: acceso remoto a la red interna (*por acceso remto, ADSL, red privada virtual, fuera de banda, etc.),* accesos a Internet, etc.
- el tráfico no permitido o rechazado por los cortafuegos y los dispositivos de encaminamiento (*al menos de los protocolos más comunes y/o peligrosos*).
- las alertas generadas por los dispositivos de detección/prevención de intrusos (IDS/IPS).
- los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, grupos o roles, etc.
- los cambios en los sistemas de seguridad, como la activación/desactivación o cambios en la configuración de los antivirus, de los sistemas de control de acceso, etc.
- el acceso al código fuente de los sistemas desarrollados.

- la activación/desactivación o cambios en la configuración de los mecanismos que generan los registros de auditoría.
- las modificaciones o borrado de los ficheros con registros de auditoría.
- el acceso a datos de carácter personal sensibles.

Debe existir un procedimiento para establecer claramente que infraestructuras, plataformas, dispositivos, redes y sistemas serán monitorizados y de qué forma se elaborarán y revisarán informes periódicos con los resultados de la monitorización. La periodicidad en la generación y revisión de cada informe estará determinada por el análisis de riesgos del elemento al que aplica.

Se deben considerar también los errores de funcionamiento de los sistemas y redes reportados por los usuarios o generados por las aplicaciones y cómo deberán ser analizados para identificar los posibles problemas de los sistemas.

Se recomienda dentro de lo posible, el uso de un sistema centralizado para la monitorización y supervisión de red que sea independiente del resto de equipos y aplicaciones. Estos sistemas centralizados permiten la definición de reglas de correlación para la identificación de ataques y modelos de comportamiento.

8. SOC (Security Operation Center)

De forma similar al NOC, un **SOC** es también una ubicación física donde se concentran los recursos humanos y materiales cuya responsabilidad es la monitorización, detección, análisis, prevención y seguimiento de los eventos de seguridad en las redes e infraestructuras de la organización. Hemos presentado en primer lugar el concepto de NOC pues ambos deberían trabajar muy "de la mano".

Si se han ajustado adecuadamente los procedimientos, el NOC será una de la principales fuentes de información del SOC, y si se han categorizado correctamente los "eventos de seguridad" el envío fluido de los mismos hacia el SOC será una actividad frecuente.

Es factible implantar un SOC que no opere 24x7 si se puede considerar un servicio de guardia para cualquier incidente crítico cuando se cuenta con sistemas de detección temprana o, justamente un NOC, que ofrezca esta función de alarma y escalada. Otra opción que está creciendo día a día es "_", es decir, tercerizar este servicio en otra

empresa especializada en seguridad y que cuente con su propio SOC orientado a prestar servicio a empresas externas; en la actualidad hay una amplia oferta al respecto y es fundamental tomarse un buen tiempo para seleccionar la que más se ajuste a nuestra necesidad concreta.

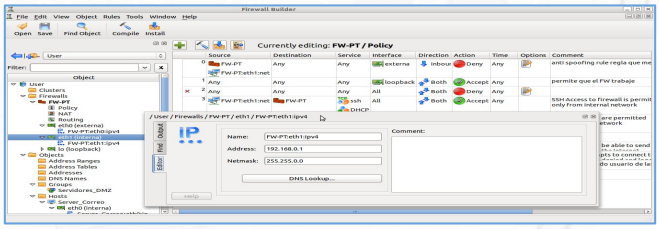
La implementación de un SOC es un decisión estratégica de la empresa, que tiene un coste considerable, por lo que debe ser analizada en detalle.

Un SOC debería proporcionar al menos los siguientes servicios:

- Monitorización y gestión de la infraestructura de seguridad.
- Gestión de incidentes de seguridad.
- Gestión de vulnerabilidades.
- Auditorías de seguridad.
- Apoyo a cumplimiento regulatorio.
- Investigación de seguridad en Internet.
- Análisis y detección de malware.
- Prevención de la seguridad.
- Cadenas de contactos y escalada en incidentes de seguridad.
- Propuesta y seguimiento de acciones de mejora en seguridad.

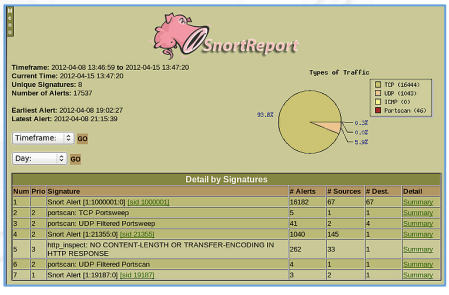
Las herramientas que puede operar un SOC son:

- Firewalls



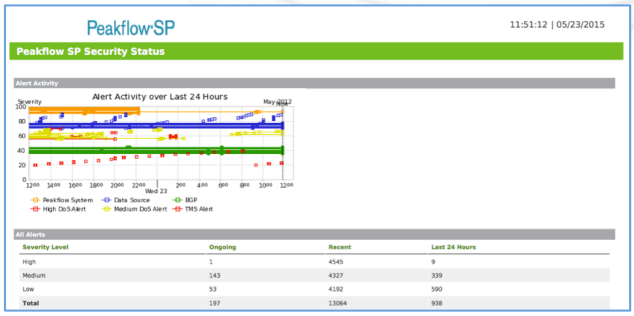
Herramienta FWBuilder

- IDSs/IPSs



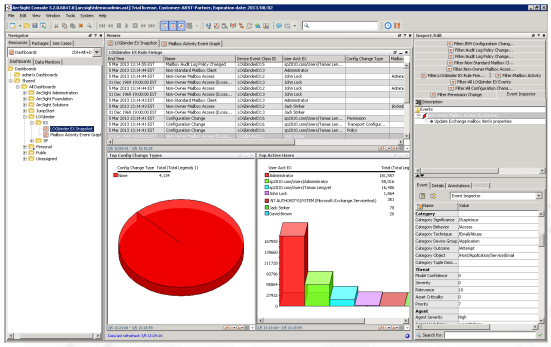
IDS Snort

- Sistemas AntiDDoS



ARBOR Peak Flow

- Plataformas SIEM



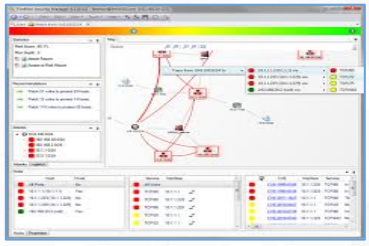
Herramienta HP ArcSight

Herramienta RSA Security Analytics

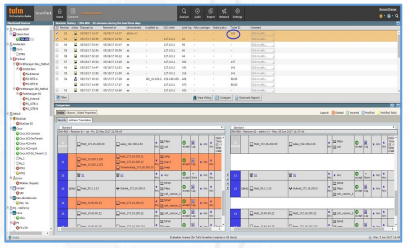
- Honey Pots (Ver proyecto honeynet: https://www.honeynet.org)

- Herramientas de gestión de FWs, Routers, Switchs (*Algosec, Firemon, Tufin, Nipper, OPnet*).

Algosec

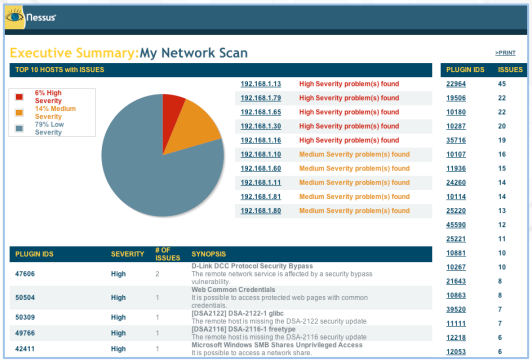


Firemon

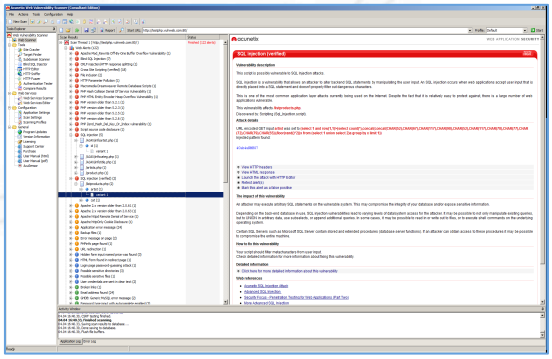


Tufin

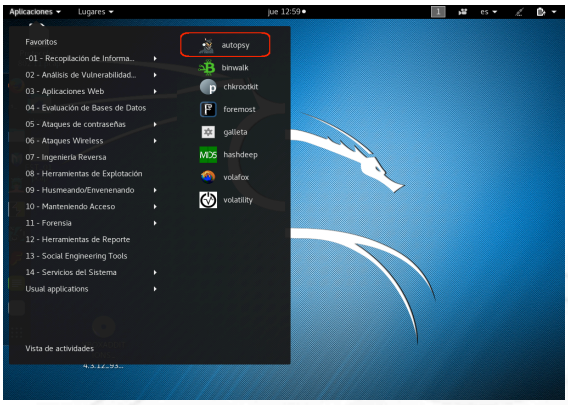
- Herramientas de análisis de vulnerabilidades (Nessus, Accunetix, Burp, OSSIM: *Open System Security Information Management*, nmap, john, Kali, etc).



Herramienta Nessus



Herramienta Accunetix

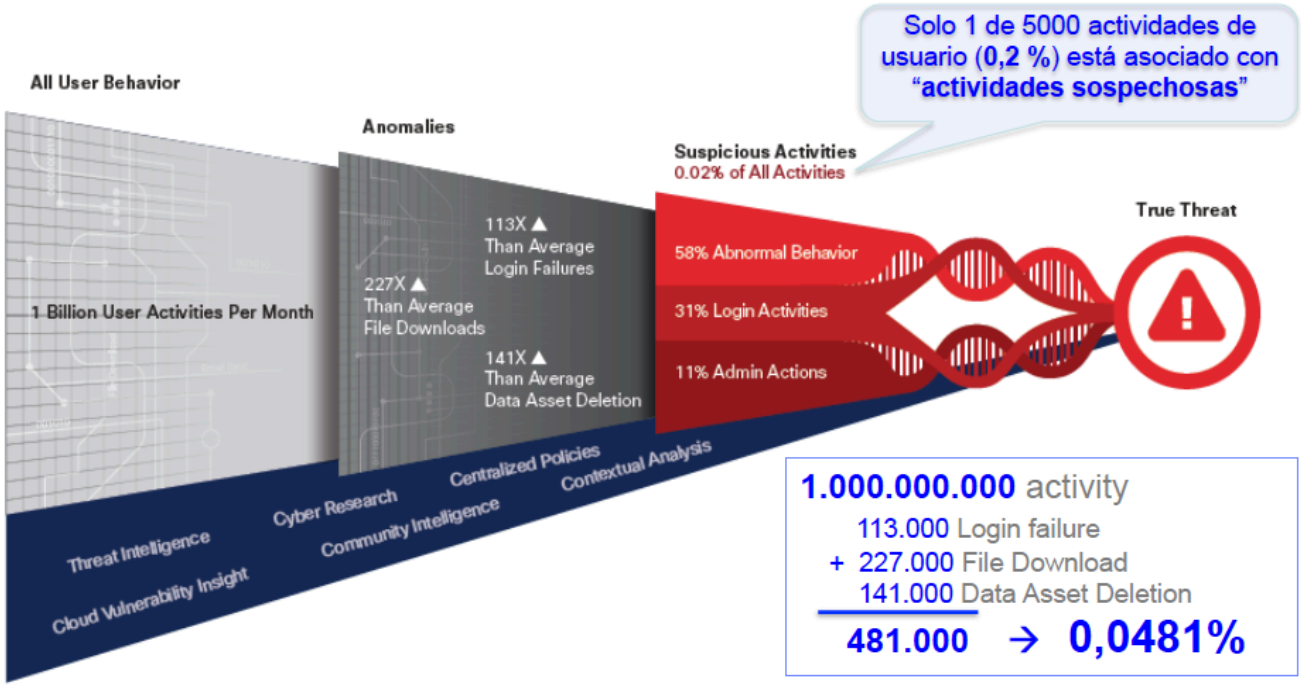


Sistema Operativo "Kali" (Linux)

Herramienta Nikto

Herramienta OSSIMM

Ruido de red:



Source: Cisco CloudLock

9. TAREAS PARA EL HOGAR (deberes).

Una vez más en esta charla os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el mes que viene con orto breve debate sobre los mismos.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo diseñarías un NOC para tu empresa?
2. ¿Qué aspectos consideras más importantes a procedimentar en un NOC?
3. ¿Hay aspectos que crees pueden ser automatizados como respuesta a eventos?
4. ¿Qué eventos concretos son los que deberían ser escalados a un SOC?
5. Cuáles serían para ti las fuentes de información desde las que obtener información y actualizaciones sobre temas de seguridad?
6. ¿Qué pasos seguirías para hacer "inteligencia" en temas de seguridad a través de Internet?

Nos vemos dentro de un mes con las tareas hechas (*no quiero suspender a nadie….*). Muchas gracias por todas vuestra atención e interés.

Un afectuoso saludo.

Madrid, 28 de septiembre de 2017.

Alejandro Corletti Estrada

acorletti@darFe.es