CENTRO DE OPERACIONES DE CIBERSEGURIDAD

WHITEPAPER

SCITUM

Contenido

CENTRO DE OPERACIONES DE CIBERSEGURIDAD

1. Introducción

El aumento de los ataques cibernéticos a la infraestructura de TI es una grave preocupación para las organizaciones, públicas y privadas. La defensa y la remediación de amenazas cibernéticas se han convertido en la máxima prioridad. Asegurar los datos en el siglo XXI requiere un enfoque holístico de las operaciones de seguridad.

Ahí es donde entran en juego los centros de operaciones de seguridad o ciberseguridad. Los SOC son una parte integral de los esfuerzos de las organizaciones para combatir las amenazas a la seguridad cibernética, funcionan de forma separada pero coordinada con los Centros de Operaciones de TI.

Un SOC es un equipo centralizado y dedicado de expertos en ciberseguridad que utiliza una variedad de plataformas para proteger contra las amenazas a su organización. Basadas en la gestión de esas plataformas y que identifican las debilidades del ecosistema al detectar, analizar y responder a las amenazas casi en tiempo real.

La combinación de gente es decir de un equipo con las habilidades técnicas y de toro tipo (soft skills), plataformas bien elegidas y aceitadas junto con procesos bien documentados, escalables, y susceptibles a ser automatizados permiten la efectividad y buen éxito de un SOC en consonancia con el objetivo de cada organización.

2. Descripción de SOC

Con base en la sección anterior podemos definir un SOC como una función centralizada dentro de una organización (empresa, institución, etc.) o bien, como una entidad externa, en cualquier caso bien estructurada, integrada por herramientas o plataformas, personal especializado y procesos bien definidos encargada de responder a las amenazas en materia de ciberseguridad que pueden gestarse interna o externamente a fin de monitorear y mejorar continuamente la postura de seguridad de la organización cliente ya que se enfoca activamente en: la prevención, detección, análisis y respuesta a incidentes de ciberseguridad.

Como hemos visto el enfoque de un SOC es principalmente la visibilidad tanto de lo que ocurre dentro del ecosistema de la organización (la red y sus activos), y posibles amenazas que se gesten en el ciberespacio, sin embargo, para tener un enfoque completo el SOC puede incluir servicios de gestión de las propias plataformas propias de seguridad.

De este modo y para cuestiones ilustrativas este documento considera como las partes principales de SOC los siguientes servicios:

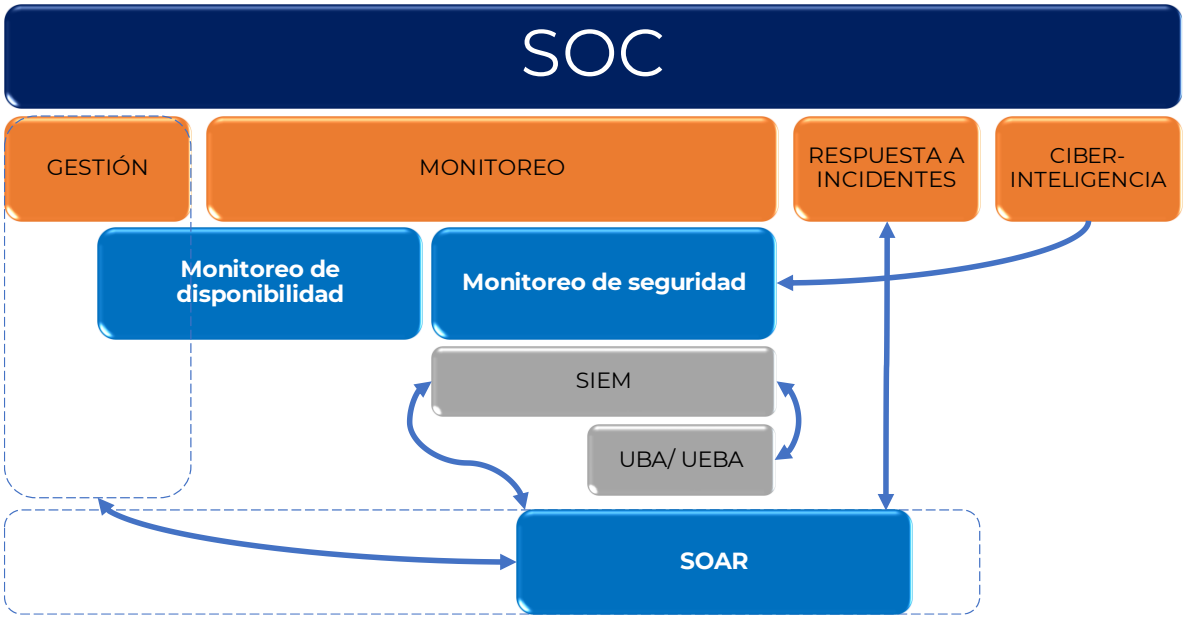

Fig. 1 Elementos de un SOC

1. Servicios de Gestión: se refiere principalmente a las altas, bajas y cambios derivados de requerimientos por parte del cliente o del monitoreo propiamente. Asimismo, contempla todas aquellas acciones y tareas de mantenimiento y soporte que permiten que las plataformas de seguridad se encuentren funcionando correctamente por lo que incluye desde la prevención de fallas a la aplicación de parches y actualizaciones.

    a. Cabe indicar como lo muestra la Figura anterior que la gestión puede incluir el Monitoreo de Disponibilidad, sin embargo, bajo ciertos enfoques la disponibilidad de los ciertos activos y de las herramientas de seguridad pueden formar parte de la telemetría (medición y entrega de datos) que es esencial para proveer esa visibilidad de la que se habla más delante.

2. Servicios de Monitoreo: se refiere principalmente de dotar de visibilidad a la organización en todos los sentidos, tanto desde el punto de vista de disponibilidad de los activos o de las herramientas de seguridad, es decir si se encuentras activas y funcionando conforme a un patrón de normalidad, pero sobre todo reflejando el estado de seguridad de una organización mediante el monitoreo de (ciber)seguridad que es el núcleo del SOC. En este rubro por ende se incluye el SIEM que es la plataforma que integra distintas fuentes y mediante su correlación ayuda en la detección de incidentes de seguridad, asimismo se incluye UBA y UEBA como soluciones que perfilan el comportamiento de usuarios y entidades (activos TIC) para determinar comportamientos anómalos que signifiquen posibles inocentes de seguridad.

    a. Como es notorio los incidentes de seguridad son la preocupación fundamental para el SOC en tanto vulneran el estado de seguridad de un entorno lo cual puede llevar una organización a la interrupción de sus operaciones y por ende negocio u objetivos, por lo que el siguiente servicio de Respuesta a Incidentes es crucial. Sin embargo, por cuestiones explicativas y dad su relación con el SIEM, UEBA y UEBA la plataforma que permite automatizar y orquestar parte de esta respuesta, el SOAR, se trata en los servicios de Monitoreo.

b. Hay que aclarar que el SIEM es fundamental para un SOC, UBA/UEBA más que deseables y SOAR una tendencia fuerte sobre todo para instituciones cuyo tiempo de respuesta ante incidentes es crítico, si bien el uso de SOAR se está haciendo más común como veremos más delante.

3. Servicios de Respuesta a Incidentes de Seguridad: define un antes, un durante y un después cuando sucede un incidente, centrado en la colaboración de los equipos más en procesos bien documentados y plataformas potenciales que facilitan la interacción y agilizan la respuesta ante incidentes. Incluye la preparación, la detección y análisis, la respuesta como tal y la investigación post incidente.

4. Servicios de Ciberinteligencia: la visibilidad que debe tener un SOC hoy en día debe incluir las amenazas que se gestan en el ciberespacio de forma general y específica contra la organización, alguno de sus integrantes, incluso debe incluir la baja de sitios apócrifos cuya existencia no sólo representan un riesgo potencial para otros usuarios o entidades sino que van en contra de la propia organización; esta visibilidad extendida sin duda puede enriquecer la respuesta a incidentes y alinear tanto las plataformas de seguridad como los activos para la protección del ecosistema entero.

3. Servicio de gestión

Para los presentes de servicio el SOC es responsable de brindar la gestión, monitoreo, soporte y mantenimiento de la infraestructura de seguridad y componentes de TI necesarios para su correcta operación. Estos servicios se proveen de forma continua en un esquema 7x24x365 (normalmente), en sitio, de forma remota o un esquema híbrido considerando de forma general la ejecución de las siguientes actividades de forma general:

- Gestionar las altas, bajas y cambios de configuración en los dispositivos de seguridad.
- Monitorear disponibilidad y desempeño de la infraestructura tecnológica suministrada e implementada.
- Ejecutar, y en su caso coordinar, las tareas necesarias dentro del proceso de manejo de incidentes de seguridad (en el caso de modificación de configuraciones).
- Mantener actualizadas las configuraciones y parches de seguridad y funcionalidad de la infraestructura seguridad, en últimas versiones estables, según los requerimientos de operación del cliente.
- Llevar a cabo las tareas de soporte y mantenimiento a hardware y software de los distintos dispositivos de seguridad.
- Gestionar con los fabricantes los reemplazos de partes en caso de fallas en hardware.
- Dar cumplimiento a los SLA definidos.
- Reportar de forma continua la información sobre la operación a través de un medio que se defina (por ejemplo, un portal WEB).
- Gestionar ventanas de mantenimiento con el cliente necesarias para la actualización ya sea de software o hardware de las soluciones o componentes gestionados, cuando estos tengan afectación directa sobre los servicios críticos del cliente o impidan la continuidad de la operación.
- Instalar los componentes necesarios (software o hardware) que garanticen la operación y compatibilidad de todos los servicios de la infraestructura instalada o reemplazada.

A continuación, se describen los procesos (metodología de operación) más importantes:

3.1. Mesa de servicios

La función de la Mesa de servicios dentro de un SOC es atender oportunamente los eventos presentados en la infraestructura del cliente a través de un solo medio centralizado que encauza correctamente las solicitudes y eventos. Se encarga de recibir, canalizar y atender de manera adecuada las solicitudes provenientes de los clientes en relación a los servicios ofertados hasta su eventual cierre.

Toda infraestructura administrada debe ser mantenida al día considerando la detección de eventos por los servicios de monitoreo para realizar actividades reactivas y a través de solicitudes de eventos por parte de cliente las cuales complementarán la gestión de la infraestructura administrada. Los eventos que se canalizan a través de la mesa y van desde la Actividad Sospechosa al Soporte de fallas o incidencias, pasando por los Controles de Cambios o requerimientos y hasta el tratamiento de incidentes de Seguridad.

Sin importar su origen todos los eventos operativos se registran en la herramienta de Service Desk que es parte del SOC y aplicando la clasificación, tipificación y prioridad del evento a finde garantizar que todas las modificaciones, indecencias y solicitudes realizadas se encuentran documentadas y se pueden analizar para ayudar a la toma de decisiones. Una vez detectado y registrado el evento el equipo enfoca los esfuerzos a solucionar la falla, el incidente o la actividad sospechosa o en realizar el cambio o el requerimiento en la infraestructura administrada. Una vez que se tiene resuelto el evento y con anuencia y retroalimentación del cliente se documenta y se cierra el ticket.

3.2. Gestión de requerimientos

La gestión de requerimientos dentro de un SOC se refiere a la atención de aquellas solicitudes que genera el cliente y que no están asociadas a un incidente en el servicio, sino aquellas peticiones tales como asesorías o generación de reportes. Su objetivo es recibir y atender de manera adecuada las peticiones provenientes de los clientes en relación a los servicios contratados.

Una vez que el evento ha sido recibido y registrado por la mesa de servicios el SOC el equipo de Operación debe recibir la notificación, el requerimiento es analizado y clasificado para brindarle un seguimiento adecuado. Se pueden incluir asesorías que son consultas o búsquedas globales de soluciones que permitan mejores determinaciones sin que ello implique entregables específicos o reportes especiales adicionales con información de interés. Una vez que se entrega la consulta o el reporte a satisfacción del cliente sobre el requerimiento solicitado se procede a cerrar el ticket.

3.3. Gestión de cambios

A fin de responder a las adecuaciones o cambios requeridos por los clientes derivado de distintas necesidades y para aumentar el valor de las plataformas, y reducir la interrupción de los servicios se lleva a cabo el control o gestión de cambios dentro del SOC cuyo objetivo es asegurar que todas estas modificaciones sean registrados, evaluados, autorizados, priorizados, planeados, probados, implementados, documentados y revisados de manera controlada a fin de no afectar la continuidad del negocio.

El alcance de la administración de cambios debe incluir los activos registrados para su gestión por el SOC y sus configuraciones a fin de soportar el perfil de riesgos requeridos por el negocio y como se ha enfatizado minimizar la severidad de cualquier impacto y disrupción. Se incluyen cambios correctivos, que se refieren a la resolución de errores detectados en los servicios todo se procesa a través de un requerimiento formal de RFC (Request for Change) por parte del cliente, el cual se registra y revisa, asimismo se proyecta el impacto potencial en los servicios, los activos y sus configuraciones incluso ante un cambio fallido. Con esa información un cambio debe ser sometido a un proceso de autorización dependiendo del impacto y canalizándolo a soporte técnico, administrador de Cambios u otras instancias.

En todos los casos es crítico planear cuidadosamente los cambios para asegurar asegurará de que la ejecución será limpia, definiendo tareas, procesos, dependencias, etc. La administración de cambios dentro de un SOC coordina la producción y distribución del plan de trabajo y servicios proyectados con impacto para que todo salga a la perfección ya que los RFC autorizados deberán ser ejecutados por especialistas que puedan implementar el cambio con el mínimo impacto, en tiempo y forma.

3.4. Gestión de configuraciones

La Gestión de configuraciones dentro del SOC tiene como objetivo asegurar que se gestione de modo controlado la definición, recepción, registro, actualización y eliminación de elementos de configuración a fin de contar con un repositorio de información que permita visualizar ágilmente los posibles impactos e implicaciones frente a un posible cambio, facilitar información sobre la infraestructura que componen un servicio y contar con información actualizada antes de aplicar un cambio que pueda impactar en la continuidad operativa de la organización.

Para ello se debe definir la base de datos para la administración de configuraciones seleccionando lo elemento de que deben ser incluidos como hardware, software, servicios, et. para el seguimiento de los eventos. El objetivo es que los elementos definidos se registran en la herramienta de Service Desk para que sean sirvan como referencia a la operación en los diferentes cambios, eventos de soporte y/o requerimientos que se presenten en la misma no solo para darle seguimiento a eventos sino para analizar riesgos y dependencias entre los dispositivos asegurando que todo cambio y evento de soporte no interrumpa la continuidad. Por ende, la base de datos de configuraciones debe estar siempre actualizada.

3.5. Gestión de niveles de servicio

Todo servicio de calidad se debe basar en niveles de servicio, el SOC no es escapa a este enfoque, Se entiende como servicio el conjunto de sistemas de TIC incluyendo seguridad que soportan un proceso de negocio o que brindan una funcionalidad determinada de valor en los procesos de negocio. De este modo, los **niveles de servicio** (Service Level Agreement o SLA por sus siglas en inglés) dentro del SOC definen criterios o niveles de cumplimiento de servicio contratado en un periodo de tiempo acordado, tiempos, definiciones y criterios alrededor de los cuales debe operar el SOC. De este modo la gestión de niveles de servicio busca asegurar que el nivel de calidad de los servicios de seguridad de TI sea el acordado para su entrega efectiva y asegurar la satisfacción del cliente.

Los SLAs deben ser planeados, es decir, diseñados en función a los servicios provistos lo cual va desde el análisis e identificación de las necesidades del cliente a la conformación del catálogo, pasando por la identificación de riesgos en caso de no cumplimiento. Una vez definidos deben implementarse

mediante Acuerdos de Nivel de Servicio (SLA) y Acuerdos Niveles de Operación (OLA) que soportarán el cumplimiento de los SLA. Y, por último, su gestión propia, es decir, a través del monitoreo y medición periódicamente se presentan resultados al cliente (informes de rendimiento) y se realizan estadísticas internas a fin de promover la mejora continua en la entrega de los servicios.

4. Servicio de monitoreo

4.1. Servicios de correlación (SIEM)

4.1.1. SIEM (información del sistema y gestión de eventos)

Un equipo SOC es una célula responsable de responder a las amenazas cibernética inminentes bajo el precepto de que todas las organizaciones serán atacadas. Normalmente, un equipo de SOC trabaja las 24 horas del día, los 7 días de la semana, los 365 días del año, supervisando las organizaciones infraestructura mediante el examen de registros (logs). Estos registros se capturan desde varios dispositivos de TIC incluyendo servidores, servicios y sensores como de soluciones de seguridad, incluidos los sistemas de defensa perimetral (firewalls de red y sistemas de prevención de intrusos), sistemas de protección de puntos finales a nivel host (detección de intrusiones en servidores), como a nivel usuario (antivirus, antimalware, protección avanzada de puntos finales que incluyen detección y respuesta [EDR]), aplicaciones (firewalls de aplicaciones web y sistemas de autenticación), bases de datos (firewalls de bases de datos) y sensores de red mediante un sistema SIEM.

4.1.2. La importancia de una plataforma de correlación de eventos en el monitoreo de seguridad

Una de las herramientas esenciales de un SOC que hacen que funciones de manera más inteligente es plataforma de gestión de eventos e información de seguridad (SIEM). Hay cinco razones clave por las que la integración de un SIEM en las operaciones:

1. Permite a las organizaciones aprovechar los datos generados por los activos de TI, los sistemas de seguridad, incluidas aplicaciones y dispositivos e información generada por otros centros de monitoreo o áreas de TI.

2. Posibilita el monitoreo de seguridad en tiempo real, la detección avanzada de amenazas, la investigación de incidentes y la respuesta a incidentes para una gestión de amenazas, de manera fácil.

    2.1. Proporciona las capacidades y la base para acelerar o automatizar la detección y respuesta ante amenazas.

3. Permite a los equipos de SOC utilizar marcos de trabajo y casos de uso que se traducen en flujos de trabajo y paneles de control diseñados específicamente para optimizar su labor.

4.1.3. Descripción de un SIEM

Los últimos sistemas SIEM tienen la capacidad de analizar, normalizar e integrar registros de múltiples fuentes. Estos sistemas pueden ingerir registros de diferentes fuentes, tanto de TIC como se seguridad que conforman un ecosistema.

Los datos de registros normalizados generalmente se almacenan para ser consultado en línea y fuera de línea (con fines de análisis histórico típicamente de tres a seis meses). Estos datos normalizados se utilizan luego para derivar reglas para un motor basado en reglas usando análisis de correlación, análisis de comportamiento, análisis de anomalías y amenazas externas técnicas de vinculación de inteligencia. Cada regla utilizada en el motor basado en reglas está diseñada para detectar y alertar a cualquier comportamiento malicioso. Recientemente, en los sistemas UEBA, se pueden crear reglas por inteligencia artificial (IA) para aumentar las reglas creadas por la inteligencia humana (HI) e inteligencia artificial (AI).

Un sistema SIEM generalmente crea muchas alertas y los analistas de SOC solo pueden enfocarse en las alertas de alta prioridad debido al gran volumen de alertas que pueden causar que el analista pase por alto las amenazas de alto potencial, lo cual se ha resuelto esto:

A. Articulando casos de uso es decir combinando reglas e identificando patrones (conductas repetibles y predecibles) que indican una amenaza potencial.

B. Asignando una amenaza puntúe para cada una de las alertas en función de la información histórica de eventos.

La elección del SIEM es crítica en función de:

1. La cantidad, tipo y ubicación de las fuentes de información a integrar. Incluyendo:
    a. Elementos TIC:
        i. Elementos de red: router, switches, etc.
        ii. Servidores de aplicación, web, hosting, de bases de datos, etc.
        iii. Endpoints o computadoras finales.
        iv. Elementos de capa intermedia.
        v. Aplicaciones o servicios que generan logs.

    b. Plataformas de seguridad.
        i. Número de endpoint.
        ii. Número de consolas.

2. Tipo de logs o eventos que generan las fuentes de información a integrar.

3. El manejo de reglas de correlación mediante normalización e indexado para su búsqueda.

    a. El enfoque tradicional de normalización versus búsqueda en una gran cantidad de datos (big data)

4. La articulación de casos de uso que combinen las reglas de correlación para integrar una visión amplia del estado de seguridad de la institución desde la perspectiva de las diferentes plataformas de seguridad.

5. Los módulos de correlación avanzada orientada a aplicaciones o bases de datos.

6. La capacidad de generar o integrar dashboard o reportes personalizables que muestren la información a la medida del cliente.

4.1.4. Monitoreo de actividad sospechosa

El monitoreo de actividad sospechosa consta de 5 fases:

Fig. 2 Actividades del Proceso de Monitoreo de Actividad Sospechosa

4.1.4.1. Monitoreo

En esta fase se lleva a cabo la comparación de los eventos registrados en las herramientas de seguridad tales como reglas de correlación, alertas de dispositivos, logs registrados y análisis de comportamiento, contra un patrón de incidentes para confirmar la existencia o no de una actividad sospechosa o un incidente de seguridad

4.1.4.2. Análisis de eventos

Durante la fase de análisis los eventos anómalos que no están identificados dentro del comportamiento y operación normal del ambiente de trabajo son analizados en búsqueda de mayor contexto sobre lo que indican los registros con el fin de poder garantizar una adecuada categorización de los eventos y evitar los falsos positivos, el análisis está conformado por las siguientes características:

- Priorización de alertas: En la fase de priorización de alertas de utilizan diferentes criterios tales como el score, el impacto y la experiencia para determinar si una alerta es una actividad sospechosa dentro de la red del cliente o bien puede ser descartado como falso positivo. También entre dos o más alertas que pueden ser actividades sospechosas, determinar la prioridad o bien si estas se encuentran relacionadas.
- Contexto: Se consideran distintos criterios para verificar el contexto de las posibles actividades sospechosas del cliente para descartar falsos positivos o bien incrementar la severidad con la que el evento es investigado, algunos de estos criterios son:
    - Activos críticos de la organización
    - Geolocalización y procedencia de la actividad sospechosa

- Falsos positivos previamente reportados
- Prioridades sobre eventos definidos y acordados previamente por el cliente

4.1.4.3. Investigación

Durante la investigación del evento se buscan indicadores y eventos relacionados que puedan aumentar, disminuir o cambiar el significado de la alerta encontrada, se hacer búsquedas históricas, búsquedas y "pivotes" con los indicadores relacionados, análisis de capturas, búsqueda de otros equipos afectados etc.

4.1.4.4. Enriquecimiento

La alerta es enriquecida a través de diferentes fuentes públicas y privadas, los indicadores son comparados y buscados contra la Ciberinteligencia del SOC y otras fuentes privadas, a partir de este enriquecimiento pueden resultar más búsquedas de indicadores de compromiso relacionados.

Fig. 3 Actividades dentro del proceso de análisis de eventos de Actividad Sospechosa

4.1.4.5. Notificación de actividad sospechosa

Esta fase tiene como objetivo informar sobre la detección de eventos que pueden representar una amenaza hacia los activos de la organización, durante esta fase se efectúan las siguientes tareas:

- Se notifica a los involucrados.
- Se proporciona un contexto inicial de los eventos detectados (sistemas que puede afectar, flujo de comunicación, resolución de nombres de dominio, etc.).
- Se proveen recomendaciones de contención proactiva acotadas al tipo de evento de Actividad Sospechas.

La operación del SOC es controlada mediante un sistema de service desk a través del cual se realiza el registro de todas las actividades sospechosas detectadas en el SIEM.

4.1.4.6. Dictamen de actividad sospechosa

Después de emitida la notificación, la investigación del evento continúa para la obtención de mayor contexto, búsqueda de indicadores adicionales y enriquecimiento con información del cliente. Una vez que la información concluye, el SOC proporciona al cliente un documento denominado "Dictamen de Actividad Sospechosa", este documento contiene el análisis detallado del evento detectado:

- Descripción del evento registrado en las herramientas de seguridad monitoreadas:
- Información de los flujos de comunicación del evento registrado:
    - Origen del evento
    - Destino del evento
    - Sistemas afectables
    - Resolución de nombres de dominios
- Retroalimentación durante la fase de contención proactiva, si se efectuaron cambios en la infraestructura que administra el SOC se proporciona el número de ticket de Control de Cambios bajo el cual se ejecutaron las modificaciones.
- Se proporcionan recomendaciones adicionales a implementar para robustecer los controles de seguridad actuales.
- Si las herramientas cuentan con la capacidad de efectuar captura de los paquetes relacionados a los eventos detectados se proporcionará un análisis de dichas capturas.

4.1.4.7. Retroalimentación de contexto a SIEM

Una vez que se ha recibido retroalimentación del cliente sobre la actividad sospechosa, se retroalimentan las herramientas de correlación e información de contexto del cliente, algunas de las acciones son:

- Configuración de indicadores en listas de seguimiento adicional para encontrar indicadores de compromiso dentro de la red del cliente
- Configuración de listas de activos falsos positivos, para evitar la detonación de una o más reglas de correlación
- Afinación de umbrales de reglas de correlación para aumentar o disminuir la sensibilidad de la detección
- Aumento de las condiciones o indicadores de compromiso que detonan una regla configurada
- Configuración de nuevas reglas de correlación para hacer detecciones relacionadas con la alerta detonada
- Configuración de destinatarios adicionales de alarmas.

4.1.5. Gestión del SIEM

Como todo activo el SIEM tiene su propio proceso de gestión el cual tiene que ver directamente con la retención de información como se explica enseguida:

4.1.5.1. Gestión de configuración

La gestión de la configuración del SIEM incluye:

1. Alta, baja y cambios de usuarios y roles para la entrada hacia el SIEM
2. Adición de nuevas fuentes de eventos

3. Parseo y normalización de logs enviados por nuevas fuentes de eventos o nuevos eventos generados por fuentes previamente agregadas
4. Generación de alarmas para el envío de notificaciones directamente al cliente
5. Creación de dashboard y vistas
6. Configuración y afinación de reglas de correlación
7. Creación de reportes
8. Creación de reglas de correlación
9. Entrega de reportes de información contenida en el correlacionador bajo demanda

La priorización y tiempo de atención de los cambios solicitados se definen en los acuerdos de niveles de servicio.

4.1.5.2. Gestión del almacenamiento

Es crucial como vimos anteriormente mantener la integridad del almacenamiento de la información de acuerdo con las necesidades de cada cliente que define un periodo de almacenamiento en línea y otro en reposo, en función de la cantidad de fuentes o los eventos generados, sobre un ratio de compresión.

4.1.5.3. Adición de casos de uso

Asimismo, se pueden configurar casos de uso de acuerdo con los requerimientos de cada institución, con el objetivo de hacer detecciones específicas. La configuración de los casos de uso se ejecutará a través del siguiente flujo:

1. Mesas de trabajo para la definición de los casos de uso requeridos.

2. Configuración de parseos y normalización requerida para cumplir con el caso de uso.

3. Configuración del caso de uso.

4. Monitoreo del caso de uso en un periodo de afinación acorde a la criticidad, periodicidad y frecuencia del caso de uso.

5. Afinación del caso de uso de acuerdo con la retroalimentación obtenida en el periodo de afinación.

6. Puesta en producción del caso de uso.

4.1.5.4. Atención a fallas

La gestión del SIEM como la de cualquier activo TI debe responder a los niveles de servicios acordados con el cliente especialmente para cubrir cualquier falla de la infraestructura de monitoreo, acorde a las capacidades de las herramientas SIEM.

4.1.6. Entregables y reportes

Todo servicio requiere de entregables y reportes que acrediten la entrega del servicio y sobre todo el estado de seguridad de manera periódica con base en lo anterior los entregables mínimos son los siguientes:

- Matriz de Contactos/Escalamiento
- Notificación de Actividad Sospechosa
- Dictamen de Actividad Sospechosa
- Reporte de Monitoreo y Actividad Sospechosa
- Reporte de Cambios en la Infraestructura de Correlación

4.2. Monitoreo de la disponibilidad y recursos de la infraestructura

Es necesario verificar que el SIEM esté funcionando durante todo el tiempo posible. En caso de que algún elemento de la infraestructura se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas en los niveles de servicio en conjunto con el cliente para ayudarle a restaurar el servicio lo antes posible a cómo funcionaba normalmente antes de la falla o eventualidad.

Este enfoque es parte del **monitoreo de la disponibilidad** que permite conocer más a fondo la utilización de los recursos de los elementos bajo contrato. De esta forma, se están monitoreando variables dentro del dispositivo como nivel de utilización (CPU, disco, memoria), que determinan el rendimiento del SIEM. Si los valores monitoreados rebasan alguno de los umbrales predefinidos, entonces se dispara la tabla de notificaciones definida entre el cliente y el SOC definiendo las acciones a tomar.

Es preciso, realizar el monitoreo de elementos como CPU, memoria, latencia y procesos críticos. Cuando alguno de los umbrales previamente configurados rebasa su valor predefinido, se dispara una alarma hacia los ingenieros del SOC, esta alarma es del tipo, visual y correo electrónico. Para ello se utiliza una herramienta de monitoreo y alertas diseñado de forma nativa en sistemas Linux, por lo que es flexible y escalable y cuenta con una interfaz gráfica que permite ver estadísticas en tiempo real de la red.

4.3. UBA/UEBA

User Behavior Analytics (UBA) se define como el análisis del comportamiento de las personas (empleados, terceros, proveedores, contratistas etc.) que están conectadas o cuenten con acceso a la red de una organización; si se incluye entidades, o puntos finales como servidores, portátiles, aplicaciones, etc. que interactúan y cuentan con un comportamiento dentro del ecosistema entonces estamos hablando de User and Entity Behavior Analytics (UEBA).

Tanto UBA como UEBA son categorías de soluciones de seguridad que utilizan tecnología de análisis incluyendo el aprendizaje automático y el aprendizaje profundo para descubrir comportamientos anormales y riesgosos de los usuarios o entidades en la red corporativa, a menudo junto con la plataforma de correlación (SIEM).

UBA y UEBA se usan para la detección de amenazas, tanto para la detección de fallos externos como para la identificación de intrusos, todo desde el punto de vista del comportamiento ya que aprende lo

que las personas y entidades hacen sobre una base normal buscando establecer una base para separar el comportamiento habitual del que no lo es, así cuando ocurre algo inusual, UBA y UEBA lo detectarán.

De este modo, UBA y UEBA pueden detectar incidentes de seguridad que las herramientas tradicionales no ven debido principalmente a que no se ajustan a reglas generales de correlación o patrones de ataque genéricos ya que abarcan múltiples sistemas organizacionales, fuentes de datos y una base de comportamiento el cual obliga a un análisis más profundo del entendimiento de la conducta y su predicción.

Sin embargo, UBA y UEBA no sustituyen a las plataformas de correlación al contrario el SIEM, al contrario, son complementarias, y pueden mejorar las capacidades de detección de amenazas cibernéticas mediante el análisis del comportamiento del usuario ya que el SIEM puede aprovechar las líneas base de actividades de usuarios y dispositivos, incluso de aplicaciones, servicios u otras identidades y en conjunto generar puntajes de riesgo basados en eventos de amenazas, usuarios y entidades.

Hay tiene tres componentes principales o pilares que hay que considerar en las soluciones UBA/UEBA.

1. **Fuente de datos**: La inteligencia de UBA/UEBA depende en gran medida del entorno de los datos de registro incluyendo el repositorio de identidades desde un Directorio Activo (AD) hasta sistemas federados. Es muy importante que UBA/UEBA tenga acceso a todos los registros de usuarios, puntos finales incluso aplicaciones. Cualquiera UBA/UEBA puede ser integrado en un SIEM si se puede recopilar los datos de registros.

2. **Casos de uso**: Las soluciones UBA/UEBA proporcionan información sobre el comportamiento de los usuarios, dispositivos, puntos finales, aplicaciones, servicios y otras entidades a través de casos de uso de modo que se realice el monitoreo, detección y alerta de anomalías para múltiples casos de uso, es decir, de la articulación de reglas de detección para determinar comportamientos de distintas fuentes.

3. **Analítica**: UBA/UBEA se basasen en analíticas avanzadas que emplean varias tecnologías que pueden identificar el comportamiento anormal sobre patrones, incluyendo:

    3.1. **Aprendizaje automático supervisado:** este aprendizaje analiza los logs y define la conducta conocida esperado e inesperado. Continúa aprendiendo y analizando nuevos patrones de conducta y determinar si se ajustan al comportamiento esperado establecido.

    3.2. **Aprendizaje sin supervisión**: En el aprendizaje no supervisado, el sistema UBA/UEBA aprende comportamiento esperado y podrá detectar y alertar comportamientos inesperados; sin embargo, no podrá determinar si el comportamiento inesperado es aceptable o no, por lo que el analista de SOC debe realizar un análisis de la alerta y determinar si es aceptable o no.

    3.3. **Aprendizaje profundo:** en este aprendizaje el sistema UBA/UEBA se basa en la identificación automática de características mediante clasificación y técnicas de aprendizaje de máquina que le permite predecir y clasificar resultados para un nuevo conjunto de alertas de seguridad.

4.4. SOAR

Los centros de operaciones de seguridad (SOC) utilizan una serie de herramientas para detectar y enfrentar ataques a la ciberseguridad del entorno que monitorean y gestionan, el tiempo de respuesta es crítico ante incidentes por lo que uno de los principales retos es saber quién tienen qué hacer qué en el momento indicado en una cadena de valor, por lo que la integración de las herramientas de seguridad, con las actividades operativas ejecutadas por personal con base en procesos es fundamental. Para ello se usan las plataformas de orquestación, automatización y respuesta de seguridad (Security Orchestration, Automation and Response), o SOAR por sus siglas en inglés).

De este modo, las soluciones SOAR ayudan a los equipos de seguridad a gestionar un volumen creciente de información, alertas, acciones para la respuesta a incidentes de forma más eficiente a través de playbooks y flujos de trabajo automatizados. El núcleo de las plataformas SOAR gira en torno a integrar personas, procesos y tecnologías: las personas son especialistas responsables de la toma de decisiones basadas en la inteligencia, los procesos orden y coordinan la acción de las tecnologías con el fin de automatizar tareas y dirigir las acciones en un incidente.

Enseguida una perspectiva del SOAR:

Fig. 4 Los elementos de SOAR

De este modo, el SOAR interviene en la **priorización** mediante la medición de los eventos (telemetría), se define el riesgo y con la inteligencia se definen la preferencia de atención, de este modo la **detección** es fundamental no sólo a nivel de colección de logs o eventos, incluso de alertas sino al determinar las acciones para la respuesta en sí misma, por lo que la clasificación (triage) es

fundamental para automatizar los flujo de trabajo consistentes con la respuesta en función del tiempo de respuesta y el impacto.

SOAR se basa en la construcción técnica y sociotécnica de la ciberseguridad, por un lado, el objetivo es integrar las herramientas de seguridad de varios proveedores en un sistema unificado para respaldar a los especialistas de seguridad en las tareas relativas a la visibilidad y reacción, ante soluciones de ciberseguridad que generan miles de alertas que son monitoreadas por analistas de SOC que siguen procesos y prácticas manuales o semiautomatizados para activar alertas. Y por otro lado el objetivo es instaurar un ambiente de colaboración que le permita a esos especialistas tomar medidas.

La plataforma de SOAR junto con el SIEM o UBA/UEBA más el resto de las soluciones de seguridad integradas, automatizadas y coordinadas puede Identificar automáticamente comportamientos sospechosos en un entorno e implementar proactivamente medida preventiva en caso de un ciberataque. La combinación de diferentes soluciones de seguridad e inteligencia humana unificadas e integradas por la automatización de los servicios de seguridad permiten acelerar la respuesta a incidentes: automatizando las actividades manuales, automatizando y coordinando las acciones de las soluciones de seguridad de múltiples bajo una visión integral.

Aunque las soluciones SOAR tienes distintos modos de integrarse nativamente o a través de distintos medios otras soluciones de ciberseguridad y de generar diferentes formatos de alertas, la interoperabilidad y la escalabilidad son elementos o factores críticos en la elección de una plataforma SOAR, así como el enfoque de análisis e investigación.

Las soluciones SOAR no están diseñadas para ingerir un gran volumen de eventos en bruto sino para recoger el incidente donde termina la funcionalidad SIEM, por lo que la plataforma de correlación es necesaria para el SOAR a fin de proveer una respuesta automatizada y orquestada a lo largo de la fase de identificación, así fases de contención, erradicación y recuperación. SOAR es una solución para mitigar amenazas a la seguridad mediante automatización y programación de acciones con la asistencia humana mínima necesaria.

Una solución SOAR debe ofrecer las siguientes funciones

1. **Automatización**: debe ser capaz de ejecutar procedimientos o procesos, es decir, una secuencia de tareas y acciones bien definidas y relacionadas con un flujo de trabajo de seguridad sin intervención humana. La automatización debe incluir la ejecución de flujos de trabajo preestablecidos según playbooks o libros de jugadas complejos que se basan en reglas y procedimientos del equipo de seguridad y enriquecidos por la inteligencia del entorno.

    1.1. Las capacidades de automatización deben ser inteligentes, basarse en procedimientos y buenas prácticas de modo que la secuencia automatizada de tareas sea más que "plantillas" genéricas sino la articulación de estrategias altamente personalizados que documenten y reproduzcan flujos de trabajo exactos pensados en tecnologías existentes.

    1.2. Las capacidades de automatización deben apuntar no sólo medidas de corrección sino de prevención, por otro lado, debe potencializar medidas de investigación adicionales.

    1.3. El objetivo es que el equipo de operaciones de seguridad puede aprovechar la automatización para clasificar alarmas y responder a los eventos clasificados como críticos con mayor rapidez.

1.4. De forma deseable la automatización debe contar con guías de supervisión de forma automatizada que permitan y como parte integral de los casos de uso y playbooks.

2. **Orquestación:** proporciona la interoperabilidad y coordinación de las actividades necesarias para la respuesta a incidentes, puede verse como la llamada o ejecución de funciones de múltiples sistemas de seguridad independientes que en conjunto ejecutan el flujo de trabajo de seguridad (por ejemplo, la solución SOAR recibe una alerta del SIEM que a su vez la recibió del UBA/UEBA, y esta se reenvía como una orden de ejecución de análisis a una herramienta de análisis de malware).

   2.1. **Integración**: una de las columnas del SOAR es lograr la interoperabilidad y coordinación de actividades con plataformas de terceros, es decir la integración de componentes para la respuesta a incidentes.

      2.1.1. La integración supone que la plataforma SOAR entienda y hable "el idioma" de las plataformas de terceros a fin de hacer llamadas a procedimientos en esos sistemas externos.

   2.2. **Recolección y centralización de datos**: se requieren datos de eventos centralizados tanto para la plataforma como para los usuarios del SOAR. Las capacidades de orquestación deben asegurar que cualquier información necesaria para manejar el incidente esté disponible como parte de los flujos de trabajo.

   2.3. **Contextualización y clasificación**: el contexto, es decir, la información de la situación, las circunstancias en la que se dio, las condiciones del entorno, la descripción de los actores, y en general cualquier información relevante es crucial para una respuesta eficiente y eficaz a los incidentes de seguridad.

      2.3.1. La contextualización puede ayudar a clasificar un incidente y con base en la plataforma reconocer patrones y con ellos la ejecución inteligente que evite el uso excesivo de tiempo y recursos.

      2.3.2. De este modo, el SIEM o sus funciones siguen siendo fundamentales para la solución SOAR a fin de identificar y facilitar un curso de acción rápido.

   2.4. **Acción**: una plataforma SOAR debe desencadenar acciones en los sistemas integrados mediante la interoperabilidad con las plataformas de terceros. La orquestación permite a la plataforma SOAR hacer llamadas a procedimientos en otros sistemas, por ello deben procesar el mismo idioma.

      2.4.1. Las acciones asociadas a la respuesta a incidentes pueden ir desde la detección y la prevención de amenazas y hasta parte de la contención y remediación.

3. **Gestión**: se requiere l gestión de las fases y aspectos de un incidente o alerta de seguridad, esto permite el seguimiento de casos mediante una interfaz de usuario con una vista completa de todos los aspectos del caso, que debe incluir la interacción con los datos y componentes (herramientas, plataformas, activos) críticos relacionados con el incidente fin de ejecutar las acciones de respuesta específicos del caso lo cual está descrito en el playbook.

   3.1. La gestión permite las investigaciones ya que preserva y refuerza el cumplimiento de los procesos y facilita el cierre de alertas de seguridad y de los tickets.

3.2. Finalmente, la plataforma debe incluir módulos de reporteo completos a la medida de las necesidades de cada organización que sirvan para los análisis del estado de la seguridad.

3.3. Sin embargo y dado el dinamismo, la visión correcta es la de integrar dashboards o paneles que permitan informar en tiempo real sobre los incidentes o casos en curso, su nivel de impacto, alerta, su relación con otras amenazas y toda la información "viva".

5. Respuesta a incidentes de seguridad

El ciberespacio es un entorno cada vez más complejo y con mayor incertidumbre, de tal forma que los ataques relacionados con la ciberseguridad se han vuelto no solo más numerosos y variados, sino también más dañinos y a la vez complejos, aprovechando el avance constante de la tecnología.

Se puede observar un crecimiento anual promedio de 30% en el número de ciberataques en los últimos años, lo cual nos orilla a las organizaciones y responsables la seguridad a *no sólo preguntarnos si nos atacarán o no, sino a cuestionarnos más enfáticamente si estamos siendo atacados en este preciso momento y si estamos o estaremos preparados para reaccionar adecuadamente*. Está claro que las actividades preventivas basadas en los resultados de las evaluaciones de riesgo pueden reducir la materialización de incidentes de seguridad, sin embargo, uno de los mayores desafíos que enfrentan los profesionales de TI de hoy es planificar y preparar para lo inesperado, pues también está claro que no todos los incidentes pueden ser prevenidos.

Para tal efecto, los grupos defensivos de las organizaciones deben contar con capacidades especializadas que les permitan contar con mayor contexto de lo que se observa en las redes de cómputo y los activos tecnológicos, además de contar también con perfiles especializados en la prevención, detección y respuesta ante incidentes de seguridad que puedan impactar a la organización.

Es necesario que el SOC proporcione apoyo en la atención, investigación y contención de algún evento de incidente de seguridad que pueda poner en peligro la confidencialidad, integridad y disponibilidad de la información de nuestros clientes, buscando dar respuesta a los siguientes cuestionamientos:

- ¿Qué ataques fueron utilizados para obtener acceso a los sistemas?
- ¿Cuáles son los Artefactos maliciosos asociados (en caso de existir)?
- ¿Se establecieron llamadas de comando y control?
- ¿Qué sistemas e información fueron comprometidos?
- ¿Qué acciones realizó el intruso después de obtener acceso (en caso de aplicar)?

De este modo, se ejecutan las actividades de consultoría y soporte para contener un incidente de seguridad a través de un grupo de profesionales especializados, con experiencia en la atención y respuesta a incidentes de seguridad y que ostentan una variedad de certificaciones, por ejemplo: CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensic Investigator), GCFA (GIAC Certified Forensic Analyst); trabajando alineados a las mejores prácticas y estándares existentes a nivel internacional.

Es crítico contar con una metodología fundamentada en las mejores prácticas del mercado y en la experiencia a lo largo del tiempo, siendo actualizada constantemente. Debe incluir múltiples procesos, procedimientos, guías y formatos preferentemente alineados a frameworks y actividades de referencias recomendadas por instituciones especializadas como el NIST y el SANS (que enseguida se ilustran) u otras orientadas a la respuesta de incidentes de seguridad.

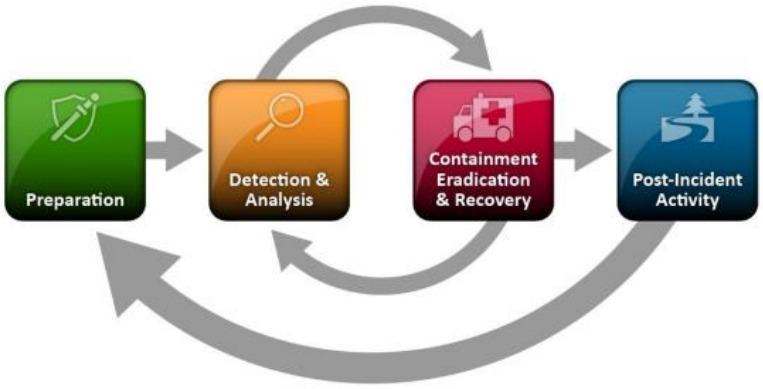

Fig. 5 NIST. Ciclo de vida de la respuesta a un incidente

Fig. 6 SANS. Ciclo de vida de la respuesta a un incidente

5.1. Esquema de ejecución

La respuesta a incidentes de seguridad efectiva debe cubrir diferentes funciones de seguridad, adicionales a la propia capacidad y experiencia de orquestar la respuesta, tales como cacería de amenazas, análisis forense, monitoreo al exterior de la red y contexto del cliente, análisis de malware, por mencionar algunas. En consecuencia el SOC debe apoyar a través de las funciones de *Incident Response Retainer*, el cual permite la ejecución de diferentes servicios y actividades, basándose en horas de consumo, para contribuir a la atención de un incidente de seguridad. Estas funciones de seguridad son:

- Apoyo en respuesta a incidentes.
- Investigación/Threat Hunting de ciberseguridad.
- Investigación de ciberinteligencia.
- Análisis de cómputo forense.
- Análisis de Malware (Estático y Dinámico).

Es necesario mencionar que, durante la fase de declaración de incidente, la organización cliente define qué es más importante, si la contención o la investigación del presunto origen, y en cualquiera de los casos, el liderazgo de las acciones y toma de decisión recaen en todo momento en el cliente con respaldo del SOC.

5.1.1. Apoyo en respuesta a incidentes

Tiene como objetico Proporcionar consultoría y soporte para contener un incidente de seguridad, brindando al cliente la posibilidad de detener el impacto adverso a sus operaciones. Este subservicio debe ser provisto por un grupo de profesionales especializados, con una gran experiencia en la atención y respuesta a incidentes de seguridad, llevando entre otras actividades:

- **Contexto inicial del incidente de seguridad***:* Durante esta fase se tiene una entrevista inicial con el cliente para entender la problemática del evento, y las acciones realizadas desde la identificación del incidente de seguridad.

- **Análisis y diagnóstico del incidente de seguridad (Triage)***:* Durante esta fase se realiza un análisis inicial del evento o eventos que se encuentran afectando a los servicios o sistemas con el objetivo de identificar el origen que causa el incidente de seguridad.

- **Definición de líneas de acción:** en conjunto con la organización se definen acciones para la contención del incidente de seguridad.

- **Definición de líneas de acción para mitigación y/o erradicación del incidente de seguridad***:* en esta fase se realiza un análisis exhaustivo sobre los hallazgos identificados, se emiten recomendaciones y se definen acciones para mitigar y/o erradicar el incidente de seguridad.

- **Generación y entrega del reporte sobre incidente seguridad***:* Al término del servicio se genera y entrega un reporte sobre el incidente de seguridad.

5.1.2. Investigación/Threat Hunting de ciberseguridad

El objetivo es apoyar en la identificación de una posible amenaza o condición de ataque a la que este expuesto, entender sus características y capacidades, origen y métodos de dispersión, para que con esta información se desarrollé un plan de contención inmediata que apoye las actividades o apuntale el programa de respuesta del cliente, así como la erradicación y prevenir una infección similar. Las fases consideradas son:

- **Fase de entendimiento a detalle:** a través de reuniones con el personal del cliente de las áreas de seguridad, tecnologías de información y redes se llega al entendimiento del contexto y evento, se revisa información como: diagramas de red para identificar los flujos de red de interés; tipos de alertas generadas por las diversas soluciones de seguridad que han visto o detectado a la amenaza; revisión de configuraciones de seguridad de los controles de seguridad y servicios; artefactos en cuarentena de la solución de endpoint; acceso a información de gestión de vulnerabilidades, como son equipos con puertos abiertos asociados a las amenazas detectadas; bitácoras de soluciones de seguridad.

- **Análisis de información y búsqueda de origen de amenaza***:* Con la información recolectada en la fase de entendimiento y con información adicional, se buscará identificar los activos que están siendo objetivo de las amenazas o son el origen y, al identificarlos, se hará un análisis de triage de la amenaza, a fin de obtener información del evento incluyendo datos volátiles que están en ese momento en el equipo de cómputo.
    - Con este *hunting* se identificarán los equipos que han sido infectados o comprometidos con la amenaza y el posible paciente cero.
    - En el paciente cero se realizará un análisis triage para identificar el nivel de compromiso del equipo y posiblemente de ello derive la necesidad de ejecutar un análisis forense.

- **Laboratorios.** Con la información recolectada se realizarán laboratorios de pruebas de erradicación de la amenaza y con esto se evaluará la viabilidad de la automatización de las tareas. Si las tareas pueden ser automatizadas, el SOC desarrollará el script para su habilitación. Si las tareas no pueden ser automatizadas, se desarrollará el procedimiento manual de limpieza y erradicación.

- **Generación de entregables:** se generarán los entregables finales del servicio.

5.1.3. Investigación de inteligencia

El objetivo de este subservicio o componente de la respuesta a incidentes es obtener información para profundizar en un tema de interés durante el proceso de respuesta a un incidente de seguridad. Es opcional y sustituye al servicio de ciberinteligencia completo a través de un reporte focalizado de inteligencia que contendrá lo siguiente: Búsqueda de motivaciones externas para ejecutar el ataque en cuestión en contra de la organización, búsqueda de información sobre el tema bajo investigación en las redes sociales más populares, canales de IRC, buscadores de Internet de las cosas, pastebin, sitios de noticias, así como Deepweb y DarkNet incluyendo sus foros y mercados negros; y perfilamiento de los posibles actores/adversarios que forman parte de la investigación.

En caso de identificarse algo crítico en el transcurso de la investigación, se notificará de manera inmediata a la organización de acuerdo con la matriz de contacto para el servicio. Al final de la investigación se realiza una presentación de resultados y un reporte con los hallazgos.

5.1.4. Análisis de cómputo forense

Este subservicio o componente de la respuesta a incidentes busca proporcionar análisis forense sobre el activo tecnológico propiedad del cliente para que esté involucrado en un incidente de seguridad. De forma general, las actividades que se realizarán están divididas en:

- **Planeación inicial del servicio**: En esta fase se realiza un análisis previo de la información relacionada al caso, con el objeto de entender el evento ocurrido incluyendo: contextualizar el caso, definir la hipótesis, el alcance de la línea de tiempo, la descripción de hechos, la identificación de criterios de búsqueda.

- **Identificación:** se proporcionan las fuentes relevantes de información para recolectar los datos de utilidad.

- **Colección y Preservación:** El analista forense realizará la adquisición de la imagen forense del equipo afectado y generará la documentación correspondiente al registro de cadena de custodia y memoria técnica de adquisición de información.

    - El especialista del SOC se realizará el manejo adecuado de los datos recolectados, utilizando el registro de cadena de custodia documentando el lugar de los hechos y/o hallazgos, los datos de las personas que tienen contacto con los indicios y su responsabilidad sobre los mismos.

- **Análisis:** en el laboratorio forense (del proveedor del SOC o de la propia organización si cuenta con él) se procesarán y examinarán los datos recolectados para identificar los hallazgos relevantes denominados como indicios para la resolución del caso.

- **Presentación:** se generará el informe técnico que integre los hallazgos identificados siguiendo una metodología apegada a las mejores prácticas. Se realizará la presentación y la entrega del informe.

6. Ciberinteligencia

Vivimos un entorno cada vez más complejo y con mayor incertidumbre que, en términos de seguridad, nos ha impulsado a dejar de pensar si seremos atacados tecnológicamente o no, orientándonos a asumir que vamos a ser atacados y a prepararnos para estar listos cuando eso suceda. De este modo, resulta cada vez más crítico como parte del enfoque de SOC adoptar una estrategia de seguridad lo más completa e integral que contemple desde los aspectos más externos de la organización, inclusive al exterior de ella misma y en ambientes donde ésta no tenga control, hasta los aspectos más internos, tales como el actuar de los usuarios y la debida protección de la información que se genera.

El SOC debe contar con capacidades que comprenden las funciones de protección de marca, amenazas internas, y en general, la ciberinteligencia, las cuales pueden interactuar entre sí y con diferentes áreas al interior de la organización para promover el enfoque detección temprana de amenazas internas y externas. Esta visión se expresa de forma gráfica en el siguiente esquema:

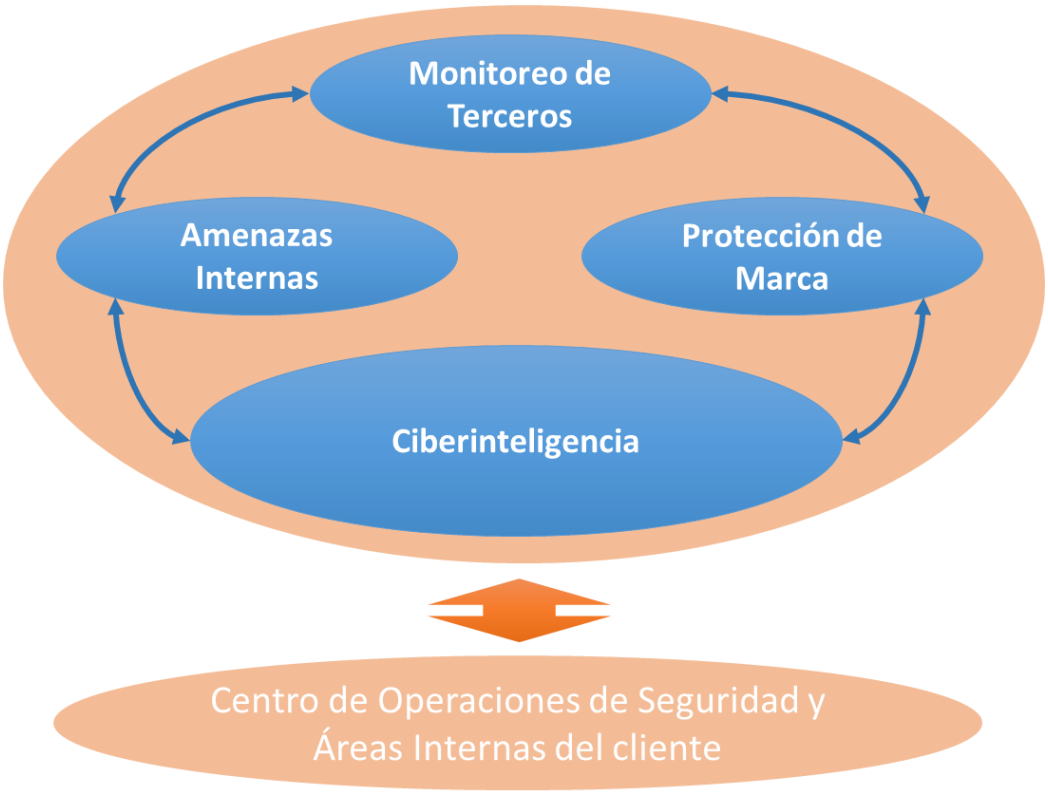

Fig. 7 Aspectos que comprenderán el Programa de Ciberinteligencia

Los servicios que soportan las funciones de ciberinteligencia, amenazas internas y protección de marca deben ser provistos por personal especializado y con amplia experiencia en la entrega de servicios de seguridad, asimismo el (proveedor de) SOC debe contar con un ciberecosistema, conformado por un conjunto de organizaciones (privadas o gubernamentales), personas y tecnologías que comparten un mismo entorno (en este caso el ciberespacio) y que interactúan con el fin de aumentar sus capacidades de anticipar, prevenir y reaccionar ante ciberataques.

Uno de los aspectos más relevantes de este ciber-ecosistema es la colaboración entre las distintas entidades que lo conforman para el intercambio de información relativa a las amenazas de seguridad y así potencializar mutuamente sus capacidades de detección y respuesta, procurando con ello mantener las mejores prácticas de la industria.

6.1. Esquema de ejecución

La *ciberinteligencia* busca robustecer las capacidades de detección temprana de amenazas, tanto internas como externas, que puedan representar un posible riesgo en el entorno operativo de las organizaciones, así como las posibles afectaciones a su imagen o marca, infraestructura, servicios o aplicaciones; esto a través de la operación de la propia ciberinteligencia, amenazas internas, protección de marca y monitoreo de terceros, y de la interacción con las funciones de gestión y monitoreo de seguridad; tal como se muestra en el siguiente esquema:

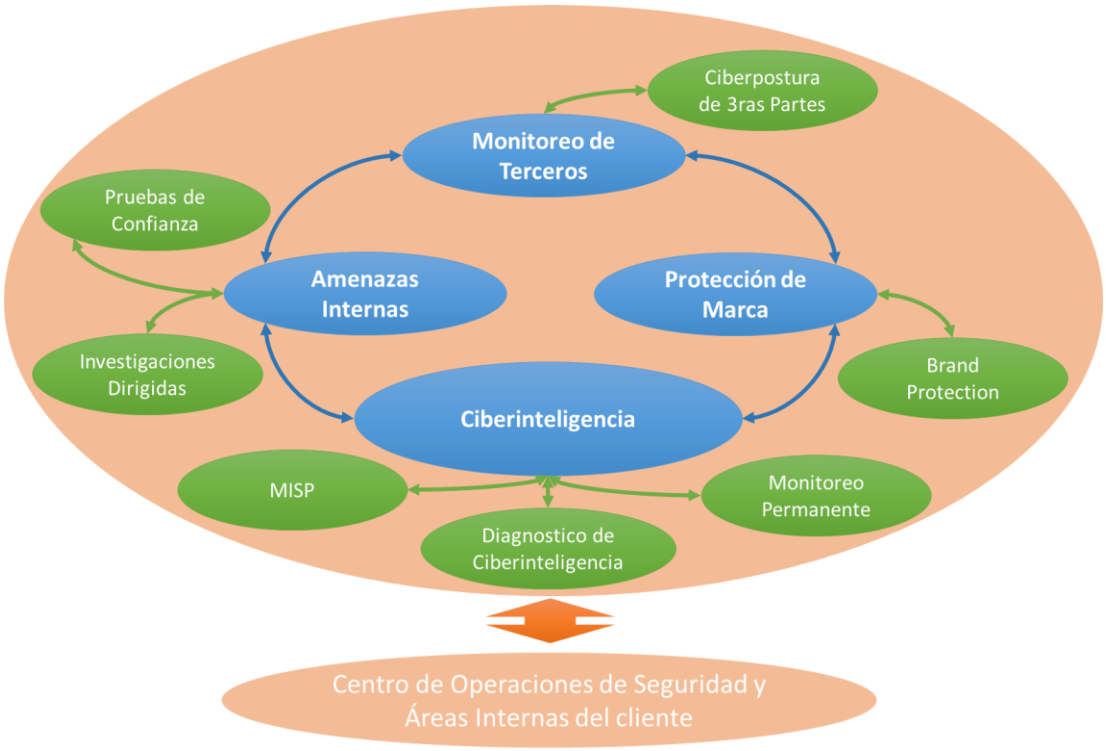

Fig. 8 Esquema conceptual de interacción de funciones de Ciberinteligencia

A continuación, se describen las diferentes funciones de Ciberinteligencia:

6.1.1. Diagnóstico de Ciberinteligencia

Consiste en poyar al cliente en contar con una con una visión general del rastro en el ciberespacio de la organización, lo que le servirá para poner en marcha nuevos procesos dentro de la organización y fortalecer sus prácticas de seguridad actuales, contemplando la ejecución de las siguientes actividades:

- Realizar una investigación en las fuentes listadas a continuación usando entidades virtuales:
    - Redes sociales más populares y asociadas al cliente.
    - Canales IRC de temas de interés del sector financiero.
    - Foros específicos en red abierta y Darknet (red Onion/Tor), así como mercados negros.
- Pastebin y sitios similares.
- Búsqueda de la venta de información confidencial de la organización en mercados negros en el ciberespacio.
- Búsqueda y seguimiento de grupos hacktivistas y del cibercrimen nacionales y extranjeros que puedan representar una amenaza para la organización.
- Búsqueda en foros y comunidades tanto de redes abiertas como de la Red Onion/Tor donde se perpetren y difundan campañas de ataques informáticos que pudieran representar un riesgo para la organización.
- Búsqueda de los equipos de la organización expuestos de manera riesgosa a internet, a través de buscadores de Internet de las cosas (IoT), hasta información de versiones en servidores de publicación y routers.
- Generación de un reporte de diagnóstico donde se entrega:
    - Hallazgos identificados.
    - Impacto de los hallazgos sobre la organización.
    - Recomendaciones asociadas.
    - Sesión de presentación de resultados.

6.1.2. Monitoreo permanente

Consiste en brindar a la organización inteligencia accionable que le permita protegerse y mejorar su postura de seguridad además de contar con el contexto de las amenazas que le rodean directamente y aquellas que se encuentran latentes en su sector, permitiéndole contar con el análisis de los sitios de phishing, perfiles de redes sociales no oficiales y apps maliciosas que suplanten la identidad del cliente. Consiste en la ejecución de las siguientes actividades:

- Notificación por correo electrónico o telefónica en los siguientes casos:
    - Detección de riesgos, donde exista la posibilidad de que una ciberamenaza se concrete pudiendo causar impacto a la organización.
    - La identificación de la venta de información confidencial de la organización en mercados negros que pueda poner en riesgo crítico al negocio.
    - Amenazas detectadas a través del monitoreo y seguimiento de grupos hacktivistas y del cibercrimen que puedan representar un riesgo para la organización.

- Monitoreo de amenazas en redes sociales, foros, blogs, y otras fuentes abiertas.

- Monitoreo de amenazas en foros y mercados de la Deep web y Dark web.

- Identificación de amenazas en equipos conectados a internet de manera insegura, usando buscadores de IoT.

- Identificación de amenazas asociadas a campañas del cibercrimen que impacten a la organización.

- Identificación de hallazgos relacionados a riesgos en su infraestructura observados desde el ciberespacio, de la misma manera que lo identificaría un atacante en su fase de reconocimiento sin tocar la infraestructura.

- Identificación de amenazas que pongan en riesgo la postura de ciberseguridad de la organización, observadas desde el ciberespacio.
- Generación de un avatar en las redes sociales más populares (*Facebook, Twitter, Instagram, y/o LinkedIn*) que permita infiltrar grupos de interés para la organización de tal manera que se pueda tener más información sobre las formas en las que puede ser afectado.

- Se entregarán reportes mensuales y bajo demanda que pueden contener lo siguiente:

    - Análisis de cómo se encuentra el cliente con respecto a otras organizaciones del mismo sector, a partir de los hallazgos identificados durante el hunting.

    - Análisis de los ciberactores detrás de la suplantación de la identidad de la organización.

    - Resultados de la investigación en redes sociales más populares en el país, canales IRC, Pastebin, Deepweb y Darknet.

    - Resultado de la búsqueda en los motores de IoT de los equipos de la organización expuestos en internet que puedan representar riesgos, desde equipos de CCTV, hasta información de versiones en servidores de publicación y routers.

    - Investigación sobre los modus operandi y tendencia de ciber fraude que aquejan al sector y que le puede impactar a la organización.

    - Hallazgos sobre riesgos en su infraestructura observados desde el ciberespacio.

- El reporte mensual considerará anexos con la siguiente información:

    - Análisis de las brechas de seguridad públicas más relevantes que afectaron al sector.

    - Resumen de sitios de phishing, aplicaciones móviles apócrifas y perfiles de redes sociales que ya se hayan dado de baja en relación con lo reportado mensualmente.

    - Presentación de resultados de los hallazgos más relevantes.

6.1.3. Investigaciones dirigidas

Este subservicio dentro del SOC busca obtener información que le permita profundizar en un tema de interés relacionado con una amenaza cibernética o ciberfraude en específico después de que éstos hayan ocurrido, contemplando la ejecución de las siguientes actividades:

- Asignar a los especialistas responsable de la investigación.

- Generación de un reporte de ciberinteligencia con la búsqueda de motivaciones externas para ejecutar el ataque en cuestión en contra de la organización así como la búsqueda de información sobre el tema bajo investigación en redes sociales más populares, canales de IRC, buscadores de Internet de las cosas, pastebin, sitios de noticias, así como Deepweb y DarkNet incluyendo sus foros y mercados negros.

- Al final de la investigación se realizará una presentación de resultados y se entregará el reporte correspondiente.

6.1.4. Pruebas de confianza

Consiste en la ejecución de pruebas de confianza personal del cliente a fin de verificar que el personal seleccionado actúa dentro del marco de conducta que dicta la normatividad. A su vez, estas actividades posibilitarán la identificación de aspectos negativos en el ambiente laboral que pudieran convertirse en amenazas internas, permitiendo con ello el establecimiento de una estrategia que posibilite su mitigación.

Aunque es un servicio opcional del SOC promueve las interacciones internas de forma segura y la preservación de un entorno seguro. De este modo, la prueba está diseñada para medir la ética y moral del personal del cliente con la finalidad de alertar sobre inclinaciones personales riesgosas, antes de que representen un problema para la organización. Los parámetros que se consideran dentro de la prueba son:

- **Línea base**: lealtad, honestidad y robo.

- **Estándar**: Soborno, alcohol, drogadicción y apuestas.

- **Filtro de personalidad**: evaluando el nivel de autocontrol, normatividad y responsabilidad.

- **Específicos**: violencia, acoso sexual, tolerancia servicial, delitos informáticos, riesgo social y fraude crediticio.

- **Imagen**: tendencia a dar respuestas exageradas y poco honestas.

Las pruebas ejecutadas deben fundamentarse en diferentes estrategias psicológicas basadas en simular un interrogatorio de lo general a lo particular a fin de disminuir las defensas al familiarizarse con los temas o bien otras estrategias que permiten que el evaluado exponga información se busca fomentar respuestas honestas o sinceras, para ello es necesario presentar una variedad de preguntas para evaluar cada parámetro desde diferentes ángulos, detectando contradicciones incluso se pueden agregar distractores a ciertas preguntas con el fin de inducir a la persona a admitir faltas cometidas.

6.1.5. Protección de marca (brand protection)

La protección de marca consiste en brindar a la organización inteligencia accionable acerca de sitios que están suplantando su marca, perfiles de redes sociales apócrifos y aplicaciones móviles falsas, que de acuerdo con el contexto de las amenazas y el impacto que representan deban ser desactivados para evitar que clientes actuales y potenciales de la organización sean víctimas de estas campañas maliciosas, lo cual toca varios puntos estratégicos del trabajo del SOC.

La protección de marca comprende:

- Detección de sitios, aplicaciones móviles y perfiles de redes sociales que suplantan a la organización.

- Detección de dominios de internet con nombre similar a la organización que envíen correos electrónicos haciéndose pasar por la institución.

- Detección de la suplantación de identidad de altos mandos o personas especificas dentro de la organización en sus redes sociales.

- Análisis de los casos identificados durante la detección, eliminando el ruido, y determinando el verdadero impacto para la organización con base en el panorama de amenaza global, el contexto de la organización y las amenazas del sector en el país.

- Es posible que el SOC tenga las capacidades para entender el modus operandi o poder extraer información relevante como “metadata” de los documentos o imágenes que se lleguen a compartir.

- El SOC debe proveer la desactivación de:
    - Sitios apócrifos que contengan evidencia de suplantación de la organización, fraude hacia los clientes actuales y potenciales, así como que distribuya artefactos maliciosos a quien visita el sitio.
    - Sitios con nombres similares que no tengan contenido, pero estén enviando correos electrónicos a nombre de la organización.
    - Perfiles de redes sociales que suplanten a la organización o alguno de sus ejecutivos o que emplean la imagen y el nombre de la marca sin la autorización de la organización.
    - Aplicaciones móviles falsas o maliciosas en tiendas no oficiales y/o que empleen el nombre o imagen de marca sin la autorización de la organización.
    - Resultados de búsquedas que contengan ligas a sitios fraudulentos o no autorizados y que empleen el nombre o imagen de marca sin la autorización de la organización.
    - Esto puede hacerse por evento o de forma permanente en función de los alcances pactados para el servicio y el nivel de exposición del cliente.

- Una vez que el SOC identifique el riesgo asociado al sitio apócrifo, el perfil de red social falso, o la aplicación móvil falsa, se notificará por correo electrónico y/o vía telefónica, para que el punto de contacto designado por la organización pueda autorizar la desactivación de lo reportado.

- Se deben incluir reportes mensuales y bajo demanda

6.1.6. Ciberpostura de terceras partes

También como parte de las funciones deseables al SOC la ciberpostura de terceros consiste en llevar a cabo una medición de la postura de seguridad e identificación de los factores de riesgo asociados con el estado de salud de ciberseguridad de la propia organización y de los terceros con los que tiene una relación, además de identificar el impacto al negocio y las afectaciones potenciales

De forma general la ciberpostura de terceras partes comprende las siguientes etapas generales:

- **Etapa 1. Diagnóstico de Ciberpostura de riesgos de terceros (AS-IS):** identificación del contexto de la organización incluyendo la confirmación de alcance de los terceros y el análisis de la información recolectada desde el ciberespacio tanto del cliente como de los terceros.

- **Etapa 2. Valoración de la situación actual:** valoración de la situación actual de seguridad, a través de la identificación de los riesgos asociados a los terceros, determinación de los niveles de riesgos, impacto al negocio y priorización de los riesgos identificados.

- **Etapa 3. Definición de iniciativas de seguridad:** elaboración del informe final de resultados, identificación de acciones inmediatas, definición de las iniciativas de seguridad a corto y mediano plazo para el tratamiento de los riesgos identificados.

- **Etapa 4. Gestión de los ciber riesgos de terceros:** monitoreo de indicadores por categoría de riesgo, notificación de cambio en los umbrales definidos de riesgo y revisiones periódicas para mantener los riesgos de seguridad en niveles aceptables para la organización.

7. SOC SCITUM

7.1. Explicación general

Se presentan los principales elementos y características de la infraestructura que componen el Centro de Operaciones de Ciberseguridad de Scitum el cual se encuentra en funcionamiento desde hace más de 20 años usando para ello como referencia los principales estándares y mejores prácticas internacionales con relación a la operación, gestión y atención a eventos de seguridad.

Los más de 20 años de experiencia de Scitum en la industria de la seguridad de la información le han permitido construir capacidades operativas clave, las cuales se listan a continuación, para brindar servicios estables, confiables como se menciona a continuación:

1. **Instalaciones: El Centro de Ciberseguridad de Scitum** opera en instalaciones exclusivas para la gestión y tratamiento de eventos de seguridad. Desde hace más de 10 años el Centro de Ciberseguridad se aloja dentro de las instalaciones de Telmex - Tlalpan Insurgentes Sur 3500, Col. Peña Pobre u cuenta con las siguientes características:
    - Amplio espacio dedicado y con acceso limitado a los especialistas en gestión y Atención de eventos de Seguridad.

- Cuenta con controles de Seguridad físicos asociados a los requerimientos establecidos en la ISO /IEC 27001:2013 como son:
  - Sistema de control de acceso físico.
  - Acceso físico restringido por esclusas.
  - Sistema de circuito cerrado de televisión (CCTV).
  - Sistema de Aire acondicionado.
  - Robusto Sistema de suministro eléctrico.

2. **Infraestructura tecnológica:**
   - La infraestructura tecnológica para la prestación de servicios se encuentra alojado en el Centro de Datos TRIARA Querétaro el cual cuenta entre otras, con la certificación de ICREA (International Computer Room Experts Association, por sus siglas en inglés) nivel 5 lo cual indica que se trata de un Centro de Alta Seguridad y Alta Disponibilidad con certificación de clase mundial.
   - Scitum realiza el monitoreo de disponibilidad y desempeño mediante herramientas líderes en el mercado, a través de estas se estarán revisando los parámetros de operación críticos de los equipos y tiene la finalidad de detectar cualquier problema. Se monitorean elementos como CPU, memoria, ancho de banda, latencia, errores, puertos y procesos críticos. Cuando alguno de los umbrales previamente configurados rebasa su valor predefinido, se dispara una alarma hacia los ingenieros del SOC de tipo visual y notifica por correo electrónico, SMS o aplicación smartphone.
   - En cuanto al Service Desk, Scitum cuenta con Remedy 20 la cual ha sido adaptado para alinearse con los controles que dicta la **metodología SCISO®** (metodología de operación de seguridad creada por Scitum) como son:
     - Desde 2006 contamos con módulos especializados en el tratamiento de Actividades Sospechosas de Seguridad de la información y de Respuesta a Incidentes de Seguridad de la información, ya que en su mayoría los service desks están limitados para dar tratamiento a estos eventos con un enfoque a ITIL, el cual no es suficiente para el tipo de servicios que ofrece Scitum.
     - Contamos con una base de firmas para clasificar los eventos de actividad sospechosa de seguridad alineado con mejores prácticas.
     - Es posible modelar la medición de niveles de servicio de acuerdo a las necesidades de cada cliente, así como definir alertas preventivas que apoyen en el cumplimiento de los acuerdos de niveles de servicio.
   - Scitum cuenta con el SOAR (Security Orchestration Automation and Response) de Palo Alto, ésta permite detectar y atender de manera más eficiente actividades sospechosas y posibles incidentes de seguridad basados en el diseño de playbooks que constantemente se están actualizando. Esta herramienta nos permite:
     - Contar con una base de múltiples playbooks y subplaybooks.
     - Tener una integración nativa de múltiples sistemas de Seguridad.
     - Playbooks con la integración de las principales marcas de firewalls como: Cisco, Fortinet, Palo Alto, entre otras.
     - Detección y respuesta automática de diferentes ciberincidentes o ciberamenazas
     - Integración con nuestro service desk Remedy
     - Integración con Threat Intelligence Platform (SCILabs Ecosistema)
     - Integración con sistemas SIEM con múltiples reglas de correlación
     - Optimizar el tiempo de respuesta por parte de los ingenieros de Operación.
     - Enfocar esfuerzos del personal de especialista en el análisis de la información.
     - Definir acciones automatizadas para contener posibles incidentes de Seguridad.

- Scitum cuenta con un Correlacionador de eventos de Seguridad la cual tiene como principal propósito ayudar al ingeniero de operación a identificar el riesgo posible en cada amenaza de una manera más sencilla y en mucho menor tiempo a través de la recolección y relación de todos los datos de los sistemas de seguridad y dispositivos de red (Firewall, IDS, Ruteadores, Switches, Antivirus). El sistema permite:
  - Comparar el estado de seguridad en el tiempo.
  - Medir el estado actual de seguridad.
  - Analizar el impacto de las políticas en la Seguridad
  - Definir las categorías principales de las métricas (regulaciones, control de accesos, disponibilidad, salud de dispositivos, ataques).

3. **Personal calificado y con amplia experiencia:** Scitum cuenta con un equipo de especialistas en diferentes aspectos de la seguridad de la información que en suma representan más de 1,300 certificaciones como son: CISA, CISM, CISSP, CCNA, GCIH, GCFA, ITIL, ISO/ IEC 270001, ISO/IEC 20000, CCIE Security, así como diferentes certificaciones técnicas de los principales fabricantes.

   Actualmente el Centro de Operaciones de Ciberseguridad cuenta con más de 600 especialistas técnicos de diferentes niveles brindando atención a nuestros clientes.

4. **Metodología de Operación de Seguridad --SCISO®--** es el conjunto de procesos, procedimientos, guías y formatos empleados en la operación de los servicios que provee Scitum cuyo principal objetivo es lograr la homologación, consistencia y aseguramiento de la calidad de los servicios.

   La metodología SCISO® nace hace más de 15 años dentro de Scitum ante la necesidad de replicar entre sus diferentes grupos de monitoreo, gestión y soporte aquellas prácticas que mejoran la operación, así como de identificar y dar oportuno tratamiento a posibles errores operativos en el Centro de Operación de Seguridad y Redes. Dicha Metodología se encuentra registrada ante el Instituto Mexicano de la Propiedad Industrial.

   Es así como se identificó la necesidad de establecer una línea base operativa para proveer servicios con las siguientes consideraciones:
   - Trabajar bajo un enfoque de procesos.
   - Establecer claramente roles y responsabilidades para el logro de los objetivos de cada proceso.
   - Brindar servicios de forma consistente entre los diferentes grupos de trabajo.
   - Definir actividades claras y medibles.
   - Contar con indicadores de desempeño para verificar el apego a los objetivos de procesos.
   - Establecer puntos de control que apoyen al cumplimiento y apego a procesos.
   - Alineación a mejores prácticas y estándares internacionales como: ITIL, COBIT, ISO/IEC 270001, ISO/IEC 20000, CERT Carnigie Mellon, NIST 899-61 (para la respuesta a incidentes), entre otros.

5. **Ciberecosistema:** haciendo referencia a la variedad de componentes que como empresa Scitum ha desarrollado incorporado en su operación:

   - Tecnología especializada y de vanguardia.
   - Adopción de nuevos marcos de referencia en el ámbito de Ciberseguridad.
   - Actualizaciones y mejoras en sus procesos operativos.
   - Alianzas con los más importantes fabricantes de la industria.
   - Inversión en especialización y certificación de los empleados.

- Acuerdos de colaboración con las principales instituciones de investigación en el mundo, tales como: Interpol, FIRST (Forum of Incident Response and Security Teams, Foro Internacional de equipos de seguridad y respuesta a incidentes que trabajan juntos voluntariamente para hacer frente a los problemas de seguridad de la información y su prevención), Microsoft Digital Crime Unit, CERT-MX, Talos de Cisco, Unit 42 de Palo Alto Networks y ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior).

6. **Experiencia en proyectos complejos**. Gracias a su trayectoria Scitum ha tenido oportunidad **de** apoyar en el fortalecimiento de la estrategia de seguridad de clientes nacionales e internacionales de los sectores gubernamental y privado. Dichos proyectos van desde consultorías para robustecer el gobierno de seguridad de su organización hasta la habilitación completa de un centro de operación de seguridad bajo las prácticas dictadas en la metodología SCISO®.

7. **Alianzas con fabricantes**: Scitum se ha caracterizado por ser una empresa que ofrece servicios de seguridad de acuerdo con las necesidades de sus clientes, por lo cual invierte constantemente tiempo y recursos para evaluar diferentes soluciones en el mercado, las cuales son puestas aprueba y verificadas por el equipo de Innovación, el cual se encarga de verificar su funcionalidad y desempeño. Gracias a esto Scitum cuenta con diversas alianzas con los más grandes fabricantes de la industria permitiéndonos:

    - Ofrecer mejores tiempos y condiciones de respuesta de atención.
    - Brindar precios competitivos.
    - Contar con acceso a capacitaciones especializadas en las diferentes tecnologías.
    - Obtener asesoría técnica oportuna si así se requiere.

Todas estas son solo algunas de las capacidades que han posicionado a Scitum como uno de los proveedores líderes en Seguridad de la información en México y Latinoamérica.

7.2. Interacción con otras áreas del cliente

En Scitum hemos desarrollado un modelo de referencia denominado **Visión Holística de la Ciberseguridad**, el cual parte del reconocimiento de los impulsores/motivadores del negocio para alinear la estrategia de ciberseguridad y tener claro cómo esta genera valor y cómo ayuda a preservar el valor que hoy ya tiene el negocio.

Los principales motivadores de esta Visión Holística de la Ciberseguridad son:

- Atender a requerimientos del negocio, esto es, que la ciberseguridad entienda las necesidades del negocio, las estrategias y objetivos establecidos para acompañar y habilitar su cumplimiento o evitar que por un tema de seguridad no se logren.
- Soportar al negocio en nuevas oportunidades, es decir, ayudar a analizar y tratar los riesgos que surjan de las iniciativas que la alta dirección decida arrancar para tomar nuevas oportunidades de negocio.
- Enfrentar las ciber-amenazas, entender el contexto de riesgos y de amenazas para evitar que la materialización de un ciber-riesgo afecte las metas del negocio.

- Dar cumplimiento a las regulaciones del sector/ país, conocer qué leyes, regulaciones y normativas son relevantes y aplicables al negocio para definir una estrategia de cumplimiento y así contribuir a que se logren las metas estratégicas planteadas.
- Proteger los activos de información críticos para el negocio, poder identificar cuáles son los activos más importantes para la organización y tener claramente definida una estrategia de protección para ellos.
- Elevar el nivel de resiliencia del negocio, contribuir a que la organización se pueda recuperar rápidamente de eventos no planeados que afecten su continuidad, desde el diagnóstico y la identificación de la causa raíz hasta la ejecución de acciones de corrección.

Posteriormente, esta visión nos lleva a entender el contexto de amenazas que tiene la organización y los escenarios de riesgos a los que nos enfrentamos. Con base en lo anterior debemos establecer la estrategia, el modelo de gobierno, la arquitectura de seguridad y el programa de ciberseguridad.

La estrategia debe estar centrada en proteger los datos donde sea que estos se encuentren, debemos identificar cuáles son los datos más críticos y valiosos para la organización, qué aplicaciones los acceden, qué usuarios y a través de qué dispositivos los utilizan, en qué infraestructura digital se procesan y almacenan, así como los medios/canales por los cuales viajan dichos datos.

Por último, se deben considerar todos los elementos del factor humano en la ciberseguridad pues este es el eslabón más débil en la cadena y nos debemos orientar a garantizar que el personal esté listo, contemplando al menos 4 grupos:

1. Los usuarios
2. La alta dirección
3. El área de sistemas
4. La propia área de seguridad

En el siguiente diagrama se puede observar el modelo de Visión Holística de la Ciberseguridad de Scitum:

Visión Holística Scitum

7.3. Colaboración con fabricantes y organizaciones del sector

Nuestra experiencia como firma de servicios y soluciones en TI, solidez financiera y capacidad de innovar, nos permiten hacer frente exitosamente a cualquier tipo de proyecto de seguridad de la información y servicios administrados.
Nuestro equipo de consultores y profesionales cuenta con más de 450 certificaciones de diversos fabricantes y entidades certificadoras, por ejemplo:

- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CHFI (Computer Hacking Forensic Investigator)
- GCFA (GIAC Certified Forensic Analyst)
- GCIH (GIAC Certified Incident Handler)
- CCNA (Cisco Certified)
- NS (Fortinet)
- PCNSE (Palo Alto)
- Network Associate, BS7799/ISO27001/ISO2000-1/ISO37001

De igual forma, somos colaboradores, de los principales fabricantes del sector: