Inteligencia

Dato, información e inteligencia

- https://www.jesusninoc.com/02/01/desarrollo-de-planes-de-prevencion-y-concienciacion-en-ciberseguridad-incidentes-de-ciberseguridad/#Principios_generales_en_materia_de_ciberseguridad

Tipologías de Inteligencia

La inteligencia se puede clasificar en:

- Estratégica: tendencias más amplias normalmente dirigidas a un público no técnico.
- Táctica: esquemas de las tácticas, técnicas y procedimientos de los actores de amenazas para una audiencia más técnica.
- Operacional: detalles técnicos sobre ataques y campañas específicos.

Ciclo de la Inteligencia

El ciclo o proceso de creación de inteligencia se apoya en diferentes fases, normalmente usando terminología militar para su nomenclatura. A continuación, exponemos una posible adaptación de las mismas:

- **Planificación y objetivo:** Como en todo ciclo, se debe tener una fase de inicio, cuyo primer paso sea la correcta definición del objetivo, en particular la

definición del tipo de inteligencia resultante y, en segundo lugar, los procedimientos para obtenerla. Habrá que tener claro desde el principio que la inteligencia que se quiere obtener va a estar enfocada a la mejora de la defensa de nuestro entorno industrial particular. Consumir datos que no apliquen específicamente a nuestro entorno, nuestro sector o nuestras amenazas en particular, es un error muy grave que deberá ser controlado desde esta primera fase.

- **Recolección:** Los datos, la información o la inteligencia pueden ser componentes de nuestras fuentes de datos pero, en esta fase, la clave será la forma en la que se recolectan estos datos y la manera en la que van a ser utilizados. Si recolectamos un IoC (Indicador de Compromiso) sobre un determinado fichero que reside en memoria, ¿se dispone de la capacidad para aplicar este IoC en nuestros dispositivos industriales? Si la respuesta es no, lo primero que debemos comprender es que esa pieza de inteligencia no sirve en nuestro entorno específico y lo segundo, es plantearse si se deben obtener estas capacidades para aumentar la resiliencia en el entorno.
- **Procesamiento y explotación:** El término de explotación en este contexto, está más enfocado a obtener algo valioso. En esta fase, se pretende obtener información a partir de los datos en crudo, que posteriormente puede ser analizada. Se deben procesar, establecer una correlación y explotar al máximo los datos de los que disponemos, para crear tablas o visualizaciones más concretas del entorno industrial particular que puedan ser analizadas en fases posteriores. Por ejemplo, procesar los comandos obtenidos en una captura de tráfico en crudo sobre un protocolo industrial o que nos indiquen que se ha cambiado una estrategia en un PLC. Este procesamiento nos permite saber cuándo se realiza un cambio en la programación del PLC, pudiendo ser explotados estos datos para obtener una gráfica donde se

pueda visualizar el número de veces que se cambia de programación y cuando se realizaron dichos cambios de una manera fácil.

- **Análisis y producción:** La utilidad real de toda la información procesada en las fases anteriores viene determina por el análisis de la persona encargada de este proceso. El analista es el encargado de juntar las piezas para que todo encaje, sin olvidar la tarea de discernir de nuevo, qué información es útil y cuál será descartada, basándose en su experiencia, en el entorno específico en ese momento, etc. Finalmente, el analista deberá crear un informe donde muestre toda esta información de manera correcta, orientado en cada caso al público objetivo. Esta fase no puede ser automatizada, ya que debe realizarse por una persona especializada, por lo que puede ser la más costosa.
- **Diseminación e integración:** En la última fase de este proceso, se dan a conocer los resultados a las personas indicadas, en el formato adecuado. Facilitar los descubrimientos en tiempo y forma, para que estos sean integrados de una manera rápida y acorde a la situación, debe ser el objetivo primordial. No tendría sentido que la inteligencia obtenida para detener una situación crítica llegue pasados los años. De aquí la importancia de compartir la información, mientras mantenga su valor útil para los destinatarios.
- **Evaluación y retroalimentación:** No es una fase como tal, sino más bien un marco común a todas las fases. Este marco de trabajo plantea que, en todo momento, se debe evaluar si los resultados que se han obteniendo son realmente útiles, así como contemplar y evaluar, las opiniones de mejora de cualquier persona, en cualquiera de las fases.

Inteligencia de Fuentes Abiertas (OSINT)

- https://www.jesusninoc.com/02/02/auditoria-de-incidentes-de-ciberseguridad-incidentes-de-ciberseguridad/#Controles_herramientas_y_mecanismos_de_monitorizacion_identificacion_deteccion_y_alerta_de_incidentes_a_traves_de_la_investigacion_en_fuentes_abiertas_OSINT

Surface Web

Se conoce como Internet superficial a la porción de Internet que es indexada por las arañas de los motores de búsqueda. La parte que no es indexada se conoce como Internet profunda.

Deep Web

Internet profunda, internet invisible o internet oculta es el contenido de internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores. El término se atribuye al informático Mike Bergman.

Dark Web

La dark web o internet oscura es el contenido de la World Wide Web que existe en darknets, redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder.

Dark Net

El concepto de red oscura, también conocido por su nombre original en inglés darknet, ha ido evolucionando con el tiempo

desde su definición original, dada por unos investigadores de Microsoft. A la fecha de este artículo, el término darknet no tiene una definición universalmente aceptada.