## Para lograr el intercambio de información es necesario encontrar una representación de la información que sea común a las organizaciones, dicha representación debe ser legible por un analista y parseable por una máquina. Una representación adecuada de la información ayuda a

## La motivación para una herramienta como la que se desea desarrollar es facilitar la operativa de los CSIRTs ayudando a solucionar problemas que se presentan en el intercambio de información. Dichos problemas

## La herramienta que se pretende desarrollar busca ayudar a las organizaciones con las problemáticas que se les presentan a la hora de intercambiar información de seguridad.

Se pretende

## Modelo utilizado

La herramienta que se desea desarrollar busca solucionar las problemáticas que se presentan en el intercambio de información de seguridad entre organizaciones. Dichas problemáticas afectan la reputación, seguridad y la capacidad de trabajo de la organización. Se pretende desarrollar una herramienta que solucione las problemáticas existentes y que a su vez pueda ser extendida en un futuro con nuevas funcionalidades.

Para la selección del modelo se estudiaron las características de la organización, se concluyó que el CSIRT-Tilsor es una organización de investigación que busca tener contacto directo con otros CSIRTs. Además no es una organización gubernamental ni de coordinación de esfuerzos. Otra de las características que afectan en el modelo del CSIRT es en la capacidad limitada que tiene la organización de producir y consumir información. Por dichas razones se decidió la utilización de un modelo “Peer to Peer” que permita el establecimiento de acuerdos mutuos para compartir información entre las organizaciones.

## Análisis

La herramienta que se desea desarrollar busca integrarse con RTIR para realizar un seguimiento de incidentes de seguridad. Esta herramienta debe permitir el intercambio de indicadores entre dos organizaciones, el cual debe ser realizado por medio de TAXII con la información representada por medio de STIX.

Se debería dar la posibilidad de interactuar por medio de RTIR con otros CSIRTs. En dicha interacción se podría realizar el manejo de incidentes intercambiando información referente a éstos entre los CSIRTs. En dichos intercambios se podría dar información sobre la identificación , solución, atacantes, etc. Cabe recordar que dichos intercambios hoy en día se realizan principalmente por medio de foros, email o comunicaciones telefónicas. Se puede ver que la creación de una herramienta de estas características permitiría el manejo centralizado de la información facilitando el trabajo de los analistas.

Si bien el intercambio de información no es un problema estrictamente técnico, hay procedimientos y consideraciones legales y de confianza que podrían afectar el intercambio de información. TAXII y STIX no pretenden solucionar dichos problemas sino que deben ser tomados en cuenta en los sistemas desarrollados. Por ello es necesario definir políticas de intercambio de información que especifiquen qué puede ser compartido y qué no.

Con la finalidad de aplicar dichas políticas se puede sanitizar y anonimizar la información con el fin de remover datos confidenciales o sensibles antes de que sean compartidos. Para resolver el problema planteado se debe evaluar la protección que se le quiere dar a la información y de que tanta utilidad es la información luego de ser sanitizada.

Del análisis anterior se desprende la necesidad de contar con un módulo que permita a la aplicación sanitizar la información. Es deseado que dicha sanitización se alimente de políticas definidas por la organización. La finalidad del módulo es analizar la información y filtrar datos que pudieran ser sensibles y que pusieran en riesgo los intereses de la organización.

Otro problema que se presenta en el intercambio de grandes volúmenes de datos es la correlación de información. Si se tiene información proveniente de diversas fuentes, con datos específicos y referente a distintos tipos de objetos es deseado correlacionar y vincular dicha información con la finalidad de manejar pocos datos los cuales sean más significativos que los originales.

Un sistema que use correlación busca reducir la carga de trabajo de los analistas y a su vez bajar el periodo de tiempo entre la detección del problema y su solución.

Con la correlación es posible vincular eventos generados de distintas fuentes para decidir si se tratan de falsos positivos o hechos reales. A su vez, permite detectar ataques que pudieran pasar desapercibidos en volúmenes muy grandes de información.

Si bien la información correlacionada es de utilidad para los analistas, puede ser necesario contar con toda la información recibida para poder hacer un análisis mas profundo de la situación. Por ello es necesario que toda la información que ingrese al sistema sea almacenada de forma independiente a los datos correlacionados.

Con los datos almacenados, el módulo de correlación aplica las estrategias necesarias para agrupar los datos de forma adecuada.

Además de recibir información proveniente de socios de la organización es deseable que se pueda ingresar nueva información al sistema. Se identifican dos posibles métodos de entrada al sistema.

El primero de los métodos identificados es por medio de RTIR, en este un analista ingresa información referente a un incidente por medio del RTIR. La información es dada de alta en el cliente TAXII y luego es compartida con otros CSIRTs. El otro método identificado es por medio de sensores dentro de la organización que registren los eventos de la red. Dichos eventos pueden ser dados de alta en el sistema y compartidos con otros CSIRTs.

De lo anterior podemos resumir los siguientes requerimientos funcionales:

|  |
| --- |
| Requerimientos funcionales |
| * La herramienta de implementar un modelo peer-to-peer jde intercambio de información entre CSIRTs. * Se debe dar la psobilidad de sanitizar la información intercambiada por medio de políticas definidas por el administrador. * Es deseable contar con un modulo para correlacionar la información de los incidentes. * Dar la posibilidad de ingresar nueva información de seguridad en el sistema. * Agregar políticas de sanitización de la información. * Aplicación de las políticas de sanitización para la información intercambiada * Tener la posibilidad de crear información de incidentes de seguridad en el sistema por medio de RTIR y sensores existentes en la organización. * Realizar un seguimiento y manejo de incidentes de seguridad. * La herramienta debe implementar un modelo peer-to-peer de intercambio de información para la interacción con otros CSIRTs. El intercambio se da por medio de STIX. * Tener un módulo de correlación de cyber observables. * Se debe dar la posibilidad de hacer un alta, baja y modificación de servicios TAXII en otras organizaciones. * Se debe dar la posibilidad de dar alta, baja y modificación a TAXII Data Feeds de otras organizaciones. |

También se pueden ver los siguientes requerimientos no funcionales:

|  |
| --- |
| Requerimientos no funcionales |
| * Extensibilidad: Debe ser posible extender la herramienta con nuevos módulos que implementen nuevas funcionalidades. * La herramienta debe mantener información en una base de datos independiente a la de RTIR. Dicha base de datos debe poder representar objetos STIX. Estos objetos podrían ser intercambiados o no. * Independencia de RTIR |