Ciberseguridad: El camino recorrido por la UNQ

Autor: Fabian Ampalio

Universidad Nacional de Quilmes - Quilmes - Buenos Aires

Eje temático: Ciberseguridad desde los servidores a los usuarios

Contacto: Fabian Ampalio

Correo: fabian@unq.edu.ar

Teléfono: 1135686885

Telefono UNQ: 4365-7100 - Interno: 5443

1. Acuerdos en la terminología

Mirada Proactiva vs Mirada reactiva y Mirada resiliente

La mirada proactiva

Esta es la mirada que queremos implementar, estar atentos a lo que puede llegar a pasar, para minimizar los riesgos.

Para esto, proponemos la creación de un SOC (Security Operation Center), el mismo consta de una serie de herramientas que forman un ecosistema de trabajo del cual los administradores formamos parte.

La mirada reactiva

Este tipo de monitoreo de servicios se basa en actuar después de que el evento sucedió, de alguna manera somos como *bomberos*, estamos todo el tiempo detrás del suceso.

Es el modelo con el que estamos trabajando en este momento.

Recibimos una alerta y actuamos tratando de mitigar el problema.

Los usuarios reportan un phishing y luego enviamos un correo a todosunq@unq.edu.ar, avisando del mismo.

La mirada resiliente

En nuestro vocabulario *resiliencia* tiene que ver con el proceso de recuperación de incidentes de ciberseguridad, es el proceso por el cual vamos a restaurar la información, luego de producido el incidente.

Además de comunicar lo ocurrido sin decir que fue vulnerada nuestra seguridad para evitar que el miedo nos paralice. Muchos piensan que con tener el antivirus actualizado y un firewall de borde alcanza, la realidad nos muestra otra cosa.

Debido a esto es que pensamos la seguridad por capas desde los servicios a los usuarios. Tenemos que ver todas las capas, firewalls, los servicios y los usuarios .

2. Definición de SOC

Contexto

En un momento en el que los usuarios son cada vez más móviles y las redes periféricas están migrando a la nube, los recursos de TI están más expuestos a amenazas tales como: malware, ransomware, phishing, ataques DDOS, ataque de fuerza bruta. La UNQ necesita controles de seguridad coherentes que cubran tanto los entornos de trabajo ya sean locales o remotos. Estos controles deben tener en cuenta el contexto de trabajo para anticipar, prevenir, detectar y reaccionar mejor ante las amenazas, con el objetivo de asegurar el acceso a la información de manera segura.

Definición

El SOC está compuesto por equipos informáticos,programas y técnicos, responsables de garantizar la seguridad de la información.

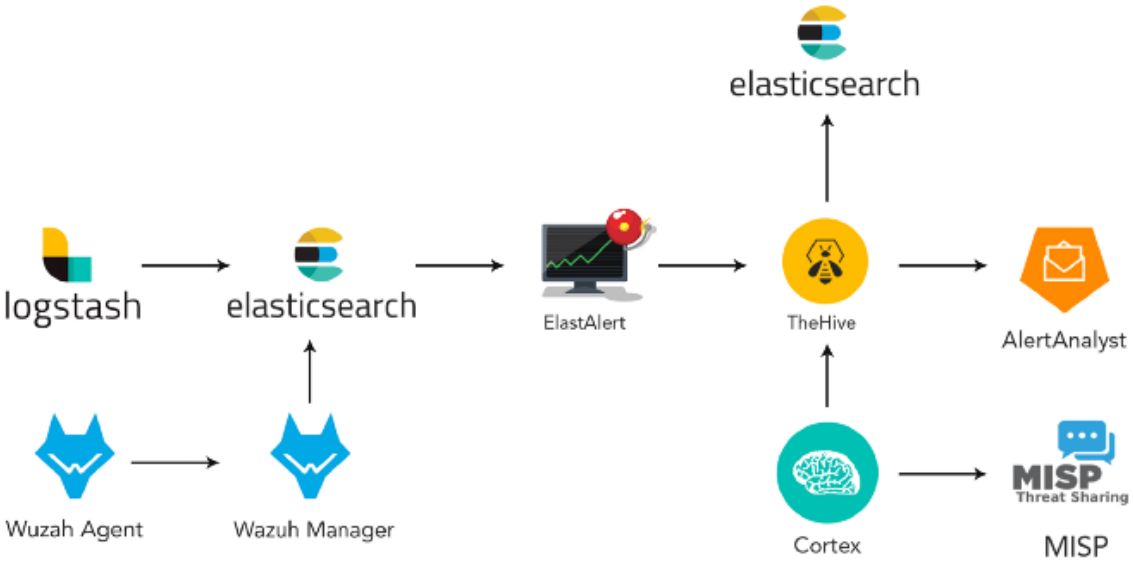
El SOC es una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recolección de datos y su correlación con eventos de intervención remota. El SIEM (Security Information Event Management) es la principal herramienta del SOC ya que permite gestionar los eventos de los Sistemas de Información.

El objetivo de un SOC es detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas y enfoques diferentes. Supervisan y analizan la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad o un compromiso. El SOC debe garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen adecuadamente. Los SOC están generalmente compuestos por analistas de seguridad y las operaciones de seguridad. Las capacidades de los SOC pueden incluir el análisis avanzado, el criptoanálisis asi como de ingeniería inversa del malware para analizar los incidentes. Los equipos de Ciberseguridad trabajan en estrecha colaboración con los equipos de Sysadmins, redes y programación para garantizar que el incidente sea abordado adecuadamente, una vez descubierto.

3.- Llegamos a implementar el SOC utilizando herramientas libres.

La creación del SOC está pensada para que el analista tenga su atención puesta en un solo punto, en el cual va a recibir los incidentes. A partir de haberlos recibido puede transformarlos en alertas o simplemente descartarlos. Si la alerta es crítica se genera un

reporte el cual puede distribuirse entre los distintos actores del ecosistema de red, también puede compartirlo con otros actores externos, unidos en un anillo de confianza.



4.- Trabajo con usuarios

Permanentemente surgen nuevas amenazas y formas de engaño, lo que hace que debamos estar alertas en todo momento. Por ello la única forma de estar atentos es mediante la capacitación y concientización. Entre otras acciones esta realidad exige capacitación continua a usuarios.

Para lograr esta concientización, trabajamos los conceptos de *espacios* y *entornos*. El espacio de trabajo es además de lo presencial, el espacio virtual, a distancia o remoto, por lo que es imprescindible concientizar de tener todos los cuidados cualquiera sean los espacios de trabajo en el que se estén desarrollando las tareas.

El trabajo con el personal de la UNQ

1. Creamos el sitio: https://protege.unq.edu.ar
2. Creamos la cuenta de correo **protege@unq.edu.ar**, para la recepción de consultas.
3. Realizamos capacitaciones en pandemia.
4. Trabajamos en el *glosario de informática* junto con UNQradio

- Estamos en las novedades de UNQ:
- Estamos en Instagram
- El glosario esta en Spotify

5. El camino hacia la política de ciberseguridad

Este camino comenzó hace dos años, durante el aislamiento provocado por el covid-19, en un curso de ciberseguridad para CISOs de Universidades de Latinoamérica, organizado por MetaRed. En este contexto se crea un grupo inicial de interesados en la temática conformado por representantes de varias universidades nacionales del país, entre ellas UNLP, UNC, UNGS, UTN, UNS y UNQ. En forma paralela se estaba trabajando el tema de ciberseguridad en una subcomisión del CIN. Como resultante de varios meses de trabajo conjunto y apoyados en esta subcomisión, se elabora un documento que fue aprobado en un plenario del CIN para que se instale el tema en los Consejos Superiores de cada Universidad.

El grupo original sigue reuniéndose actualmente los miércoles para diagramar los siguientes pasos, y mantenernos en contacto permanente, aportando ideas para mejorar nuestros lugares de trabajo. Se discuten nuevas acciones, pasos a seguir, herramientas que facilitan las tarea de monitoreo, incidentes, alertas, etc

Esto conforma una Comunidad de Conocimiento, con la firme convicción de que tenemos que compartir experiencias y aprender del camino que vamos recorriendo cada uno de los miembros de esta Comunidad. También se nutre de los valiosos aportes que brinda la subcomisión de Ciberseguridad del CIN.

Nuestro horizonte es pensar la seguridad de manera proactiva, trabajando con herramientas libres. Establecer vínculos con otras universidades, para que entre todas podamos ir armando un anillo colaborativo. Este horizonte nos plantea muchos desafíos técnicos, entre ellos, internet 3.0, blockchains, firma digital, sistemas de archivo encriptados, monitoreo constante de servicios, entre tantos otros temas. Lo que seguro podemos afirmar es que no existe un punto fijo donde llegar, debemos movernos al ritmo de la transformación.

6. Consideraciones Finales

Quisiera en el final retomar algo que dibujó alguno de nuestros abuelos en alguna roca antes que existiera la tecnología y los programas de manipulación de imagen.

Lo que vemos en esta imagen es que desde ese entonces hasta ahora cuando tenían hambre y querían comer se unían y planifican estrategias, de igual manera se unían para protegerse de las amenazas.

Hace muchos años quizás eran elefantes gigantes u otras criaturas que no se el nombre, desde esa época hasta ahora las amenazas siguen estando ya no son lanzas ni piedras las que necesitamos para protegernos…

Cuando nos preguntan ¿Necesitamos estar protegidos?, ¿Tenemos que invertir en ciberseguridad? la respuesta cae por sí sola, o les podemos mostrar la imagen de la roca. Es nuestro mundo tecnológico el que está en una constante transformación, los cibercriminales lo saben, y por eso trabajan todo el día para mejorar sus métodos de ataque y vulneración.

Del otro lado estamos nosotros y por eso tenemos que mantenernos despiertos e inquietos para desarrollar nuevas metodologías de análisis y monitoreo, aunque parezca mentira lo más fácil es lo más difícil: unirnos y compartir .

El software libre nos brinda posibilidades infinitas, para tomar lo que hicieron otros y mejorarlo o crear nuestras propias soluciones y distribuirlas.

Formamos parte de un ecosistema donde las redes nos conectan, instantáneamente con otras personas, a través de equipos los cuales administramos y formamos parte de ellos.

Hacer que las universidades sean seguras es nuestra responsabilidad y la aceptamos para seguir formando parte de este ecosistema híbrido humano-máquina, tanto si creemos o no somos parte de esta transformación.