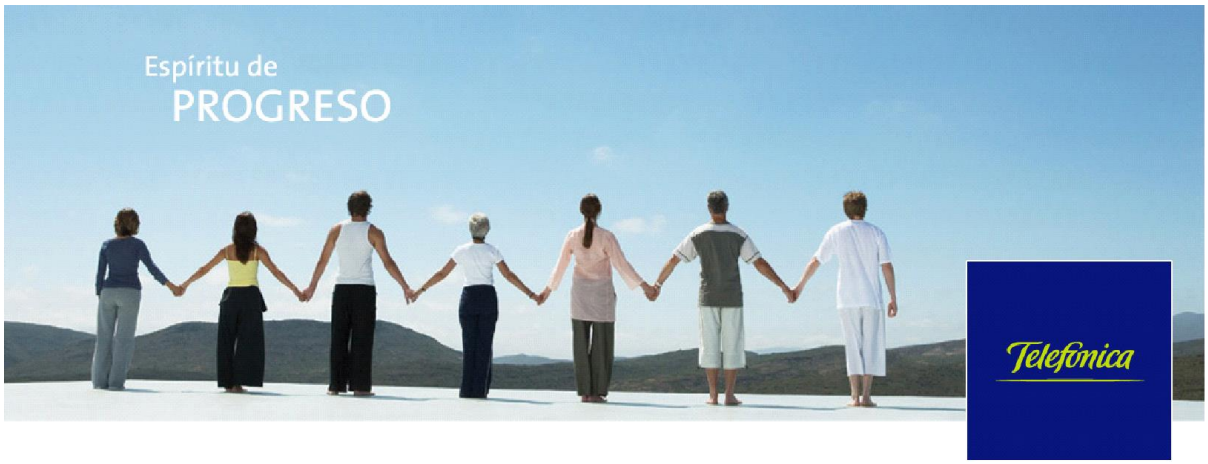
INFORME FINAL DE LA
PLATAFORMA DE AUTOMATIZACIÓN Y ORQUESTACIÓN DE SEGURIDAD



CONCURSO PÚBLICO N° 01-2020-DIRECFIN PNP

CONTRATACIÓN DEL SERVICIO DE CONECTIVIDAD DE DATOS EN BANDA ANCHA, PLATAFORMA DIGITAL INTERCONECTADA PARA SERVICIOS DE RED DE DATOS E INTEGRACIÓN TECNOLÓGICA Y SEGURIDAD INFORMÁTICA GESTIONADA PARA LAS UNIDADES POLICIALES A NIVEL NACIONAL.

DECLARACIÓN DE CONFIDENCIALIDAD

ÍNDICE

TABLAS

ILUSTRACIONES

1. OBJETIVO

Telefónica del Perú S.A.A. (en adelante Telefónica) extiende el presente documento como Informe Final del Proyecto "*Contratación del servicio de conectividad de datos en banda ancha, plataforma digital interconectada para servicios de red de datos e integración tecnológica y seguridad informática gestionada para las unidades policiales a nivel nacional*" en relación al Concurso Público N° 01-2020-DIRECFIN PNP.

El presente documento tiene como objetivo brindar la información correspondiente a los distintos servicios y actividades ejecutadas durante la implementación del Servicio "*Plataforma digital de servicios para la PNP, a nivel nacional*" del Componente Nro. 2 "*Servicio de seguridad de la información y seguridad informática gestionada.*" que se ha brindado a la Policía Nacional del Perú (PNP), con la finalidad de cumplir lo solicitado en las Bases Integradas, asegurando el cumplimiento del compromiso adquirido por Telefónica según el contrato N° 41-2020-DIRECFIN PNP, dejando operativo en óptimas condiciones..

2. ALCANCE DE LA IMPLEMENTACION

De acuerdo a lo solicitado por la Policía Nacional de Perú se adjunta y describe la información requerida respecto a los entregables según bases integradas del servicio proporcionado en referencia al Servicio N°2 del Componente N°2.

2.1. PLATAFORMA DE AUTOMATIZACIÓN Y ORQUESTACION DE SEGURIDAD

Las actividades que se realizaron fueron las siguientes:

ACTIVIDADES	ESTADO
Se definieron los tipos de incidentes	OPERATIVO
Se crearon diseños de incidentes	OPERATIVO
Se definieron cantidad, tipo y número de tareas por playbook	OPERATIVO
Se validó el licenciamiento	OPERATIVO
Se realizó la configuración e instalación	OPERATIVO
Se validó la disponibilidad del servicio	OPERATIVO
Se organizó usuarios y roles	OPERATIVO
Se crearon reportes personalizados	OPERATIVO

Tabla N°. 1: Tabla de actividades para la plataforma de automatización y orquestación

2.2. RELACIÓN DE CUMPLIMIENTO DE LOS REQUERIMIENTOS DE LAS BASES INTEGRADAS

A continuación, se lista los requerimientos de las Bases Integradas con el fin de validar su cumplimiento:

Ítem	Requerimiento según BI para el XSOAR	Comentario
1	AUTOMATIZACIÓN	Cumple
2	DETECTAR Y RESPONDER ANTE INCIDENTES	Cumple
3	INSTALACIÓN Y CONFIGURACIÓN	Cumple
4	PUESTA FUNCIONAMIENTO	Cumple

Tabla N°. 2: Requerimiento para la plataforma de automatización y orquestación según contrato

3. ALCANCE EN LA OPERACIÓN

De acuerdo a lo solicitado por la Policía Nacional del Perú (PNP), se adjunta información sobre la operación realizada:

3.1. ARQUITECTURA

3.1.1. TOPOLOGÍA GENERAL DEL SERVICIO

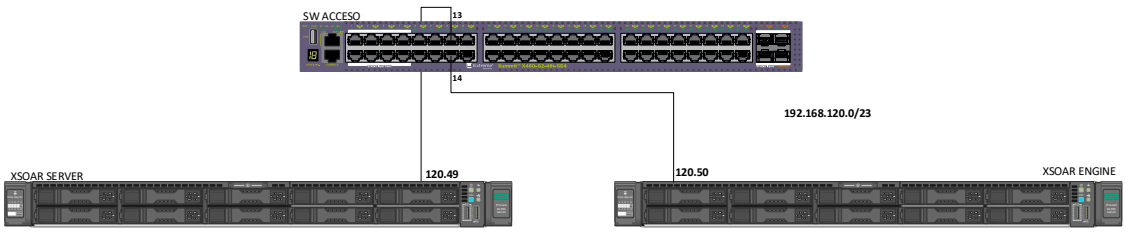


Ilustración N°. 1: Topología Física y Lógica

3.1.2. DETALLES DE HARDWARE Y SOFTWARE DE LOS EQUIPOS INSTALADOS EN LA SEDE PRINCIPAL

3.1.2.1. DETALLES DE HARDWARE

Ítem	Descripción	Detalle
1	MARCA	HP
2	MODELO	ProLiant DL360 Gen10
3	NRO. DE EQUIPOS	2
4	SERIE	MXQ0490DBF (XSOAR ENGINE) MXQ0490DBC (XSOAR SERVER)
5	RU	01
6	VOLTAJE	100-240
7	FUENTE REDUNDANTE	SI
8	DIMENSIONES	4.29x43.46x70.7cm
9	GABINETE NRO.	5
10	NRO. DE RU ASIGNADO	28 (XSOAR SERVER) 29 (XSOAR ENGINE)

Ilustración N°. 2: Detalles de hardware

3.1.2.2. DETALLES DE SOFTWARE

Ítem	Descripción	Detalle
1	VERSION	6.1.0
2	IP	192.168.120.49 (XSOAR SERVER) 192.168.120.50 (XSOAR ENGINE)
3	GATEWAY	192.168.120.1
4	MASCARA	255.255.254.0
5	DNS	172.31.1.7 & 172.31.1.10

Ilustración N°. 3: Detalles de software

4. DETALLE DE LA IMPLEMENTACIÓN

4.1. LICENCIAMIENTO

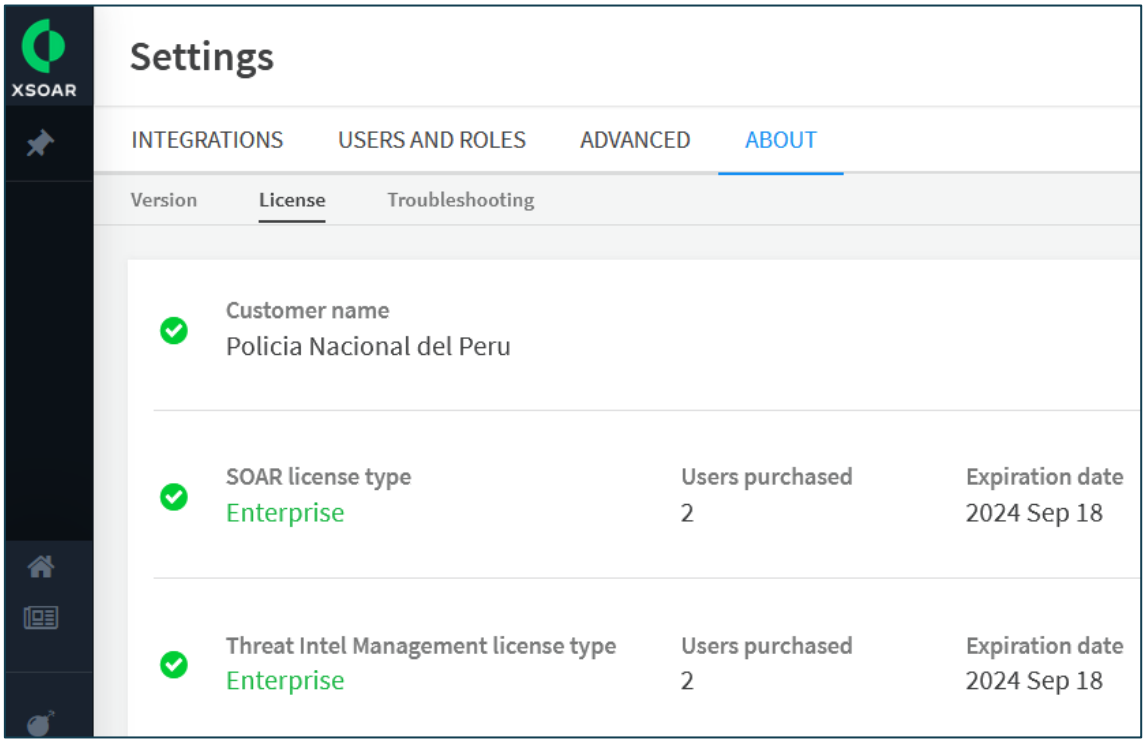


Ilustración N°. 4: Licencia XSOAR

4.2. INSTALACIÓN FÍSICA

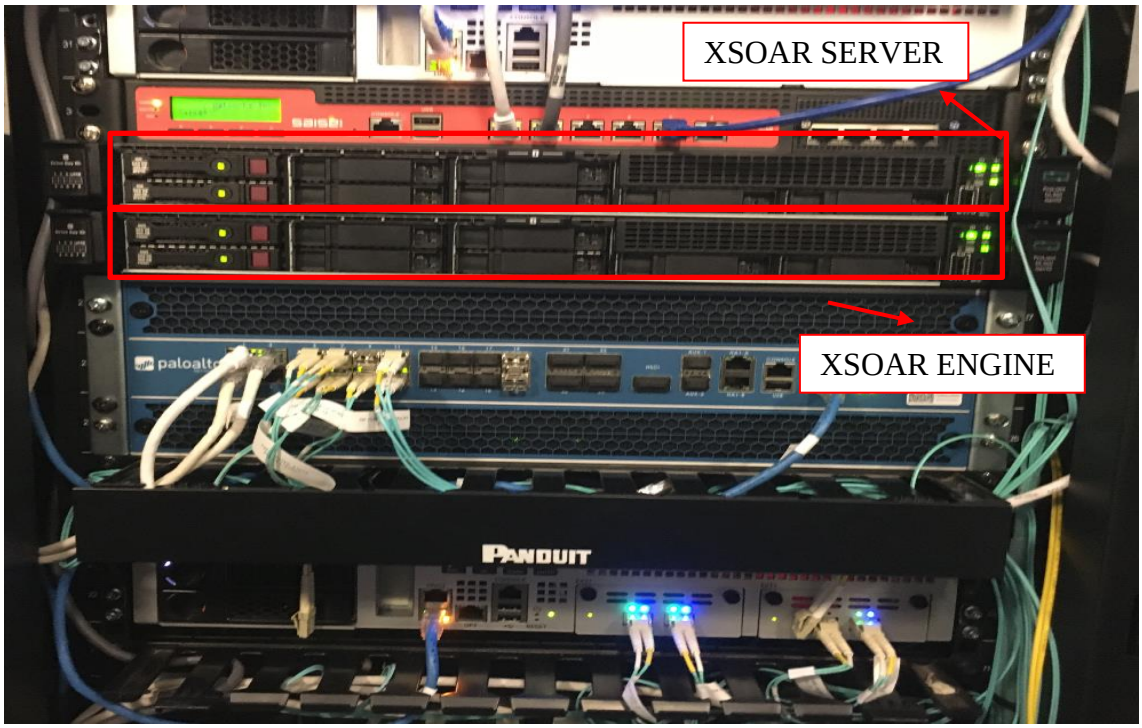


Ilustración N°. 5: Instalación Física del XSOAR Server y Engine

4.3. FUNCIONALIDADES

4.3.1. DASHBOARD DE LA SOLUCION

Se accede mediante la siguiente dirección IP, https://192.168.120.49, las credenciales de acceso serán entregadas al personal administrativo de la PNP.

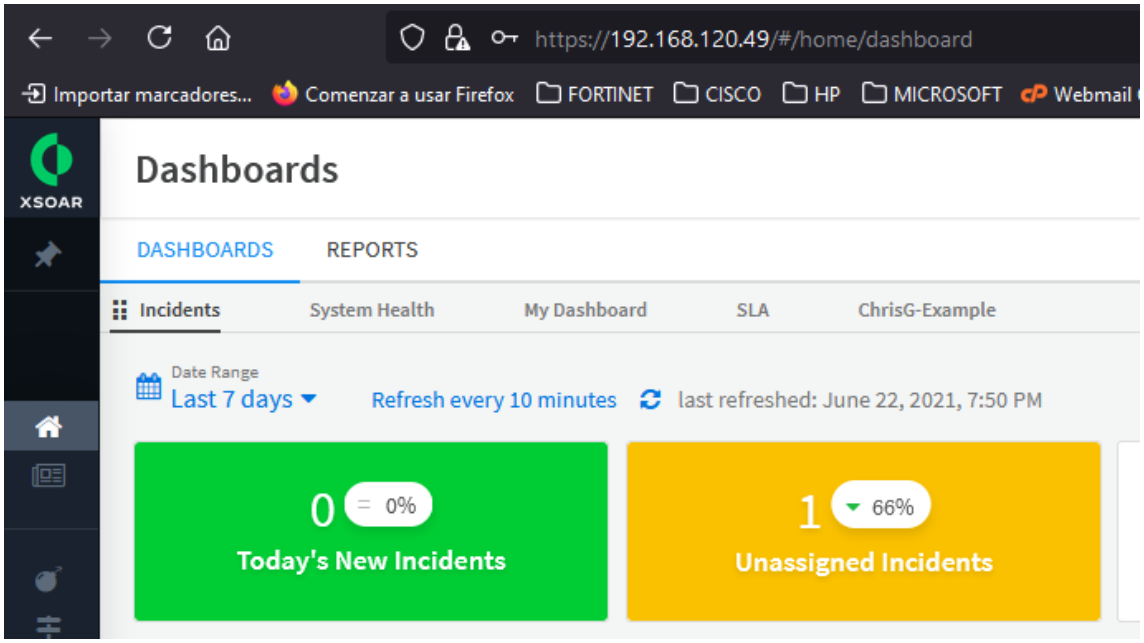


Ilustración N°. 6: Dashboards de la solución

4.3.2. CREACIÓN DE USUARIOS

En la ruta Settings > USERS AND ROLES, se pueden crear los usuarios con niveles de administración

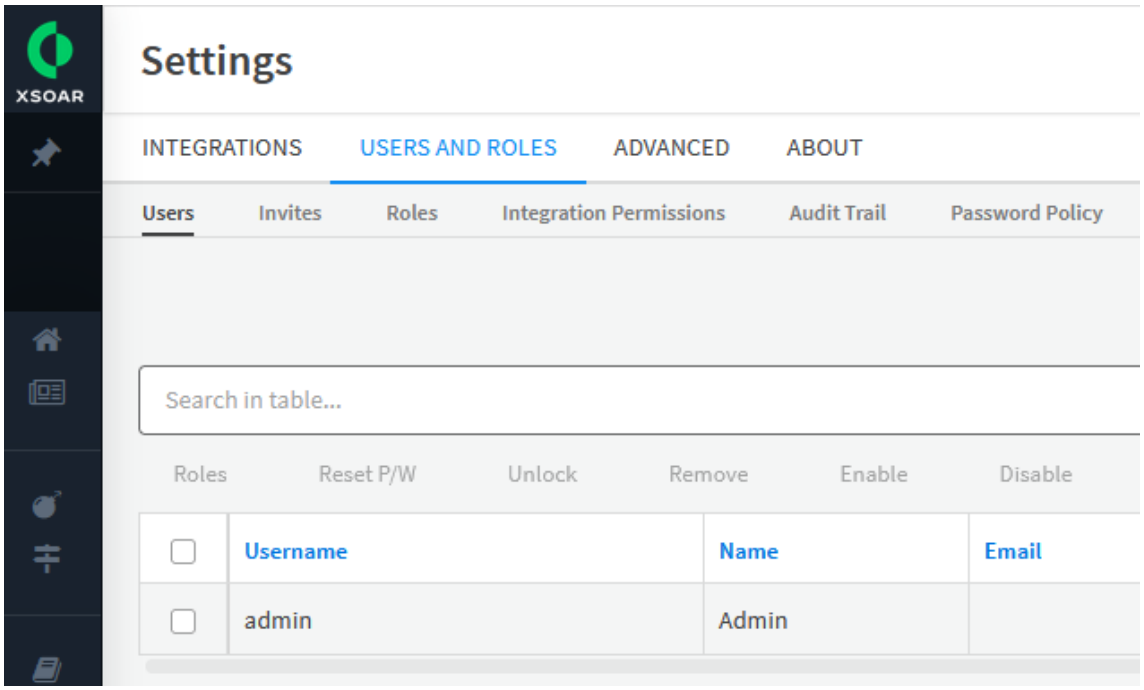


Ilustración N°. 7: Creación de Usuarios y Roles

4.3.3. INCIDENTES

En la ruta > Incidents > Search in incidents, tienes la opción de buscar el incidente por tiempos

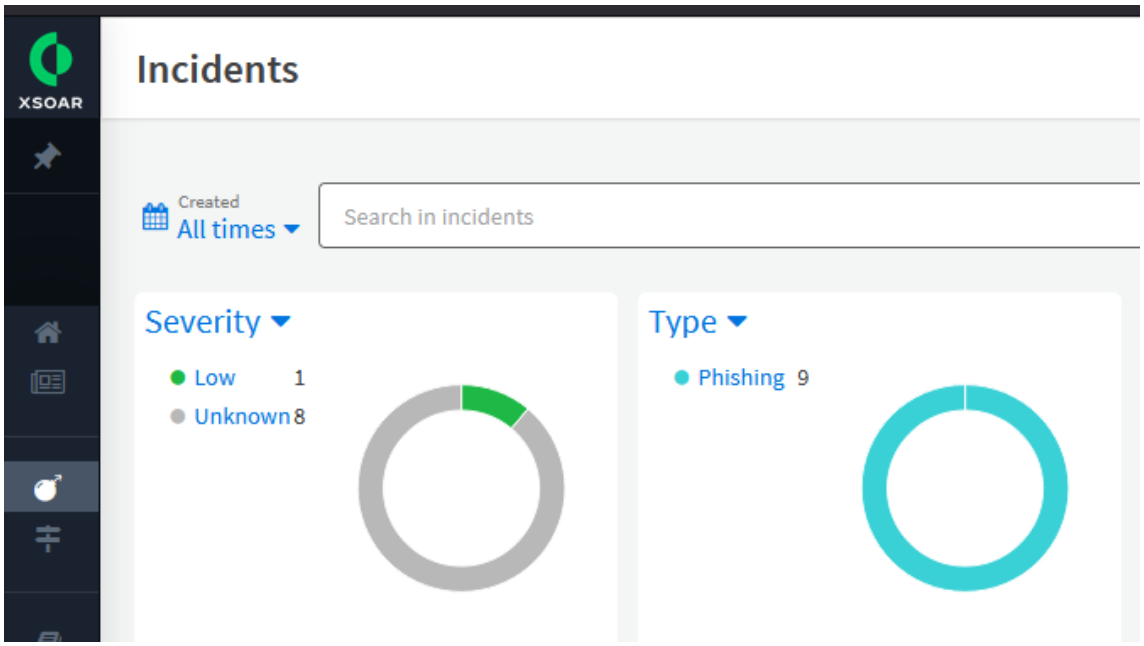


Ilustración N°. 8: Incidentes

Podemos colocar un incidente como favorito para acceder rápidamente:

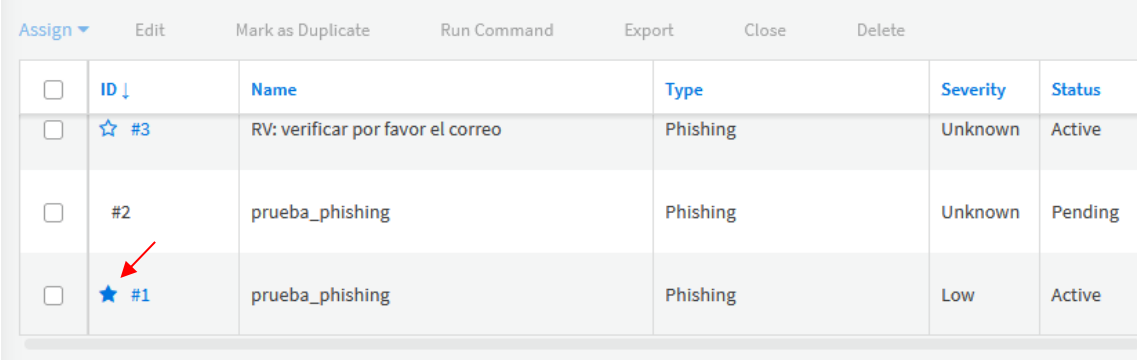


Ilustración N°.8.1: Incidentes

El incidente automáticamente se traslada al lado izquierdo de la consola:

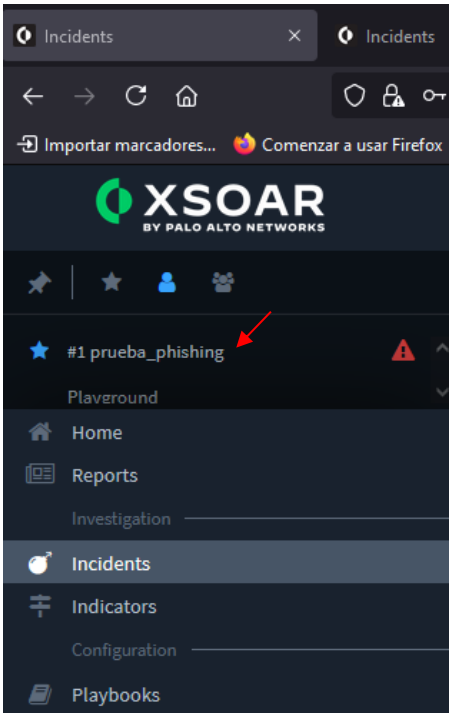


Ilustración N°.8.2: Incidentes

4.3.4. INTEGRACIÓN

En la ruta settings > INTEGRATIONS, se llevó a cabo la integración con el servidor de correos para la elaboración del primer caso de uso llamado phishing.

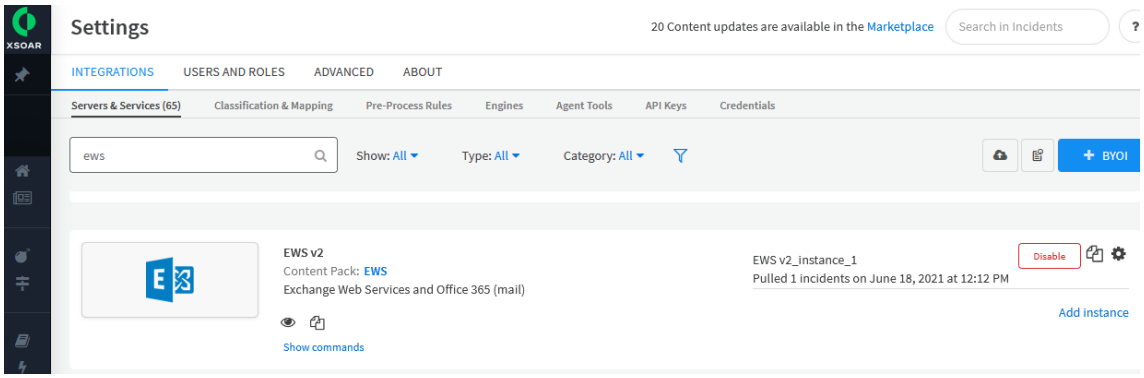


Ilustración N°. 9: Integración

También se realizó la integración con el servidor de correos para que el XSOAR envíe correos electrónicos:

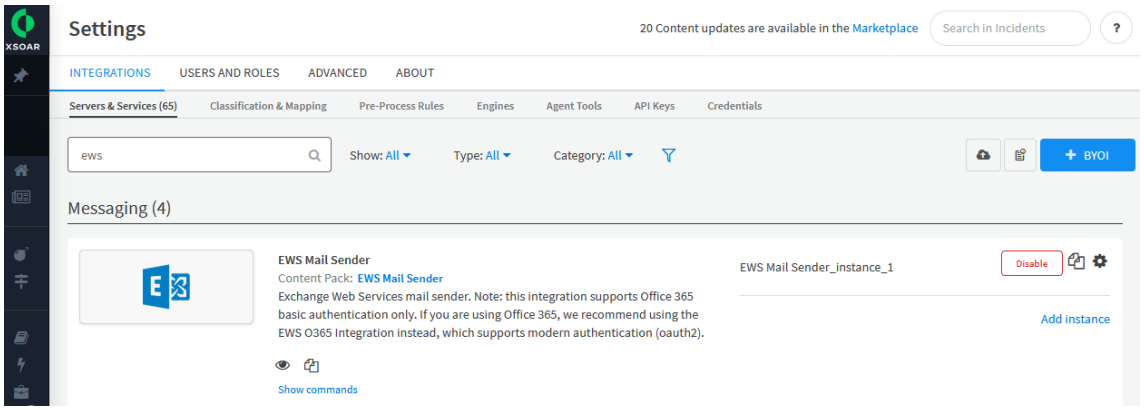


Ilustración N°. 9.1: Integración

4.3.5. INVESTIGACIÓN DEL INCIDENTE

Le damos clic al incidente como favorito, nos llevara a múltiples secciones de la página de investigación.

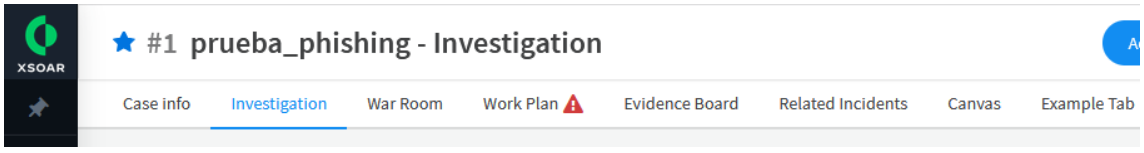


Ilustración N°. 10: Investigación de incidentes

Cada tipo de incidente de seguridad tiene un conjunto único de datos que es más relevante para la evaluación de un analista y el manejo del tipo de incidente específico.

Prácticamente todos los aspectos de los diseños de página por defecto para la información de casos y datos de investigación se pueden personalizar.

4.3.6. WAR ROOM

Le damos click en War Room,

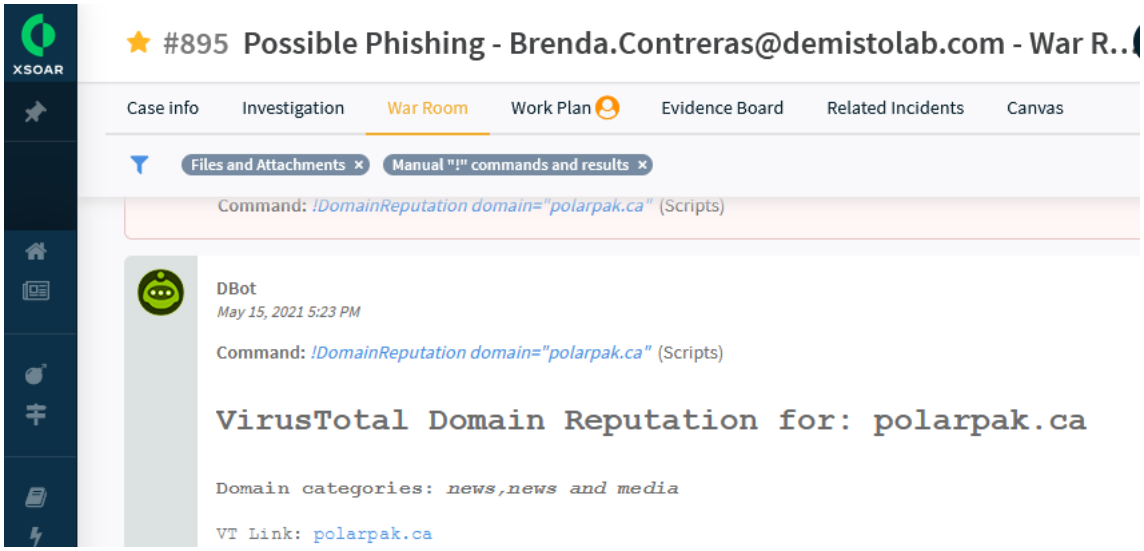


Ilustración N°. 11: War Room

Tenemos toda una colección completa de todas las acciones de investigación, entradas y colaboración. Puede pensar en War room como un diario cronológico de la investigación del incidente. Cada incidente tiene un War room. En el war room, puedes ver información, colaborar con otros y ejecutar programas.

4.3.7. RELATED INCIDENTS

Le damos click en Related incidents,

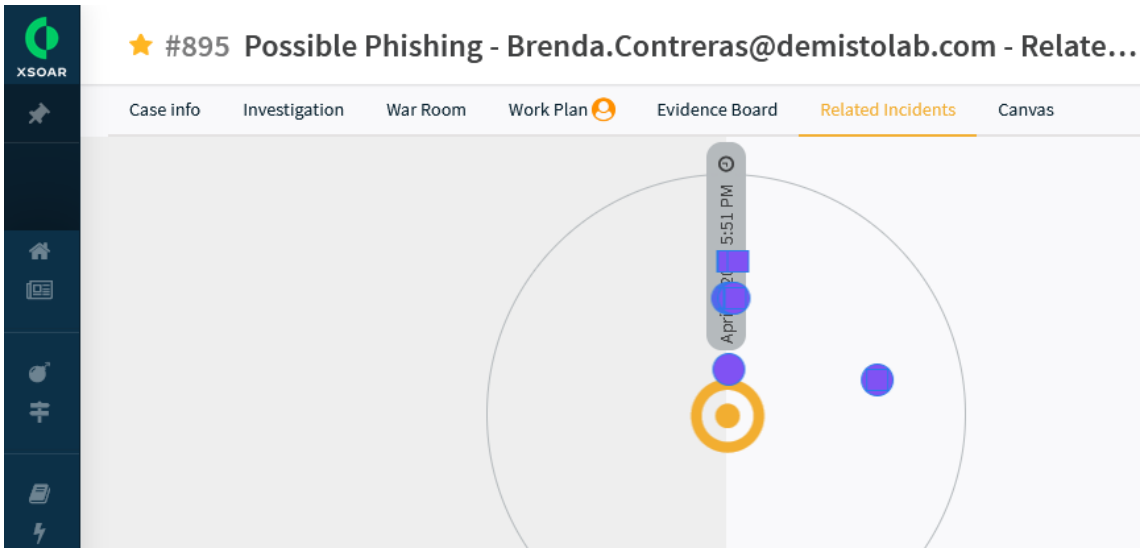


Ilustración N°. 12: Incidentes relacionados

La página Incidentes Relacionados está orientada al descubrimiento y exploración de incidentes que comparten características similares. Una visualización del volumen y el progreso a través del tiempo de las actividades coordinadas, como las campañas de phishing, puede proporcionar información importante.

4.3.8. EVIDENCE BOARD

Le damos click en Evidence Board,

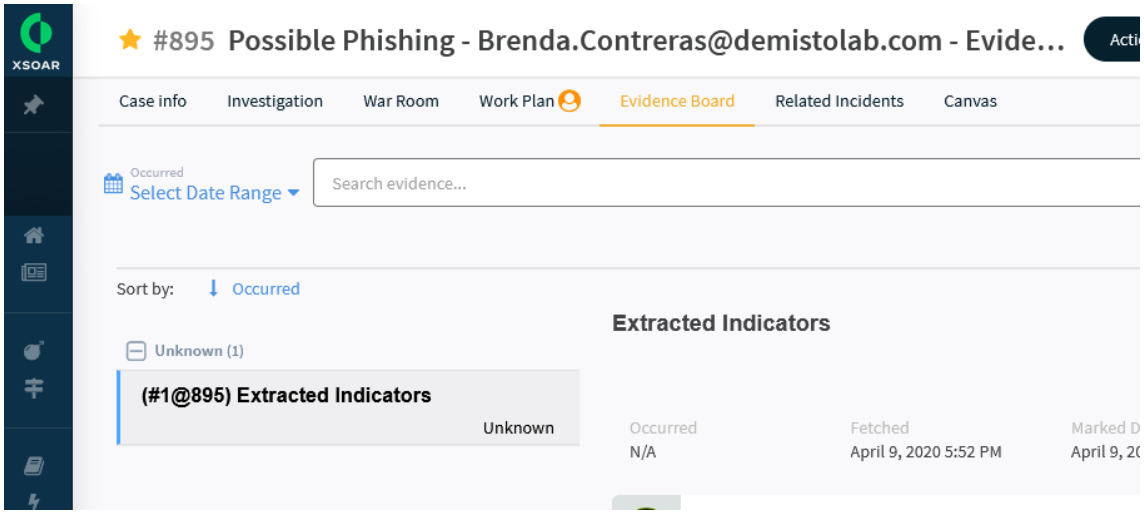


Ilustración N°. 13: Evidencias

Puede agregar y eliminar elementos de Evident Board para mantener la atención en elementos clave de interés y para curar el apoyo probatorio para hallazgos clave, análisis de causa raíz, informes de escalada y otras actividades forenses.

4.3.9. CANVAS

Le damos click en Evidence Board,

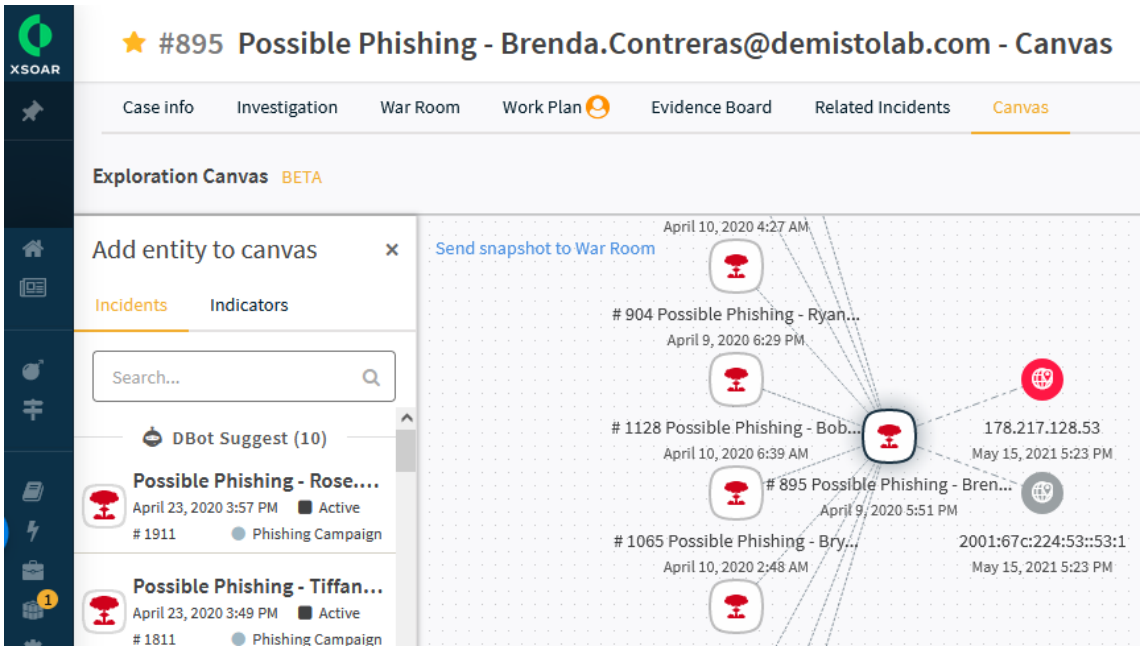


Ilustración N°. 14: Canvas

El canvas mapea las relaciones entre un incidente, sus elementos, indicadores correlacionados y otros incidentes. El Canvas proporciona aprendizaje automático para automatizar la asignación inicial del incidente actual. El Lienzo le permite decidir qué guardar, qué añadir y cómo colocar los diversos elementos.

5. RECOMENDACIONES

- Los incidentes detectados por los usuarios finales deben ser reportados al área de T.I a un correo en específico.
- Capacitaciones programadas donde se les enseñe a los usuarios a detectar eventos maliciosos en los principales servicios digitales y las buenas prácticas de seguridad en utilizar los dispositivos finales que involucren la información de la institución.
- Notificar al usuario que hemos recibido el correo electrónico del supuesto Malware para que el analista realice la investigación.
- Se debe planear como serán distribuidas las incidencias a los analistas.
- Integrar con servicios que se encuentran en el Marketplace que permiten enriquecer de información las incidencias para un mejor análisis.

6. CONCLUSIONES

- El XSOAR va gestionar un repositorio de tickets centralizado para todas las alertas de seguridad, incluidas las de phishing, las generadas por el sistema SIEM (LogRhythm), las procedentes de los endpoint y la nube.

- La respuesta a cada alerta recibida se basa en playbooks (libros de estrategias) automatizados de los que pueden beneficiarse todos los equipos y herramientas ante un ataque cibernético.
- Organizar la información sobre los incidentes permitirá mejorar la rapidez a las respuestas.
- Las nuevas amenazas serán investigadas en tiempo real con las funciones de colaboración, ejecución remota de comandos de terceros y documentación automática que ofrece el centro de mando virtual de Cortex XSOAR.
- La información obtenida con el aprendizaje automático debe mejorar la eficiencia del iSOC y la productividad del personal.