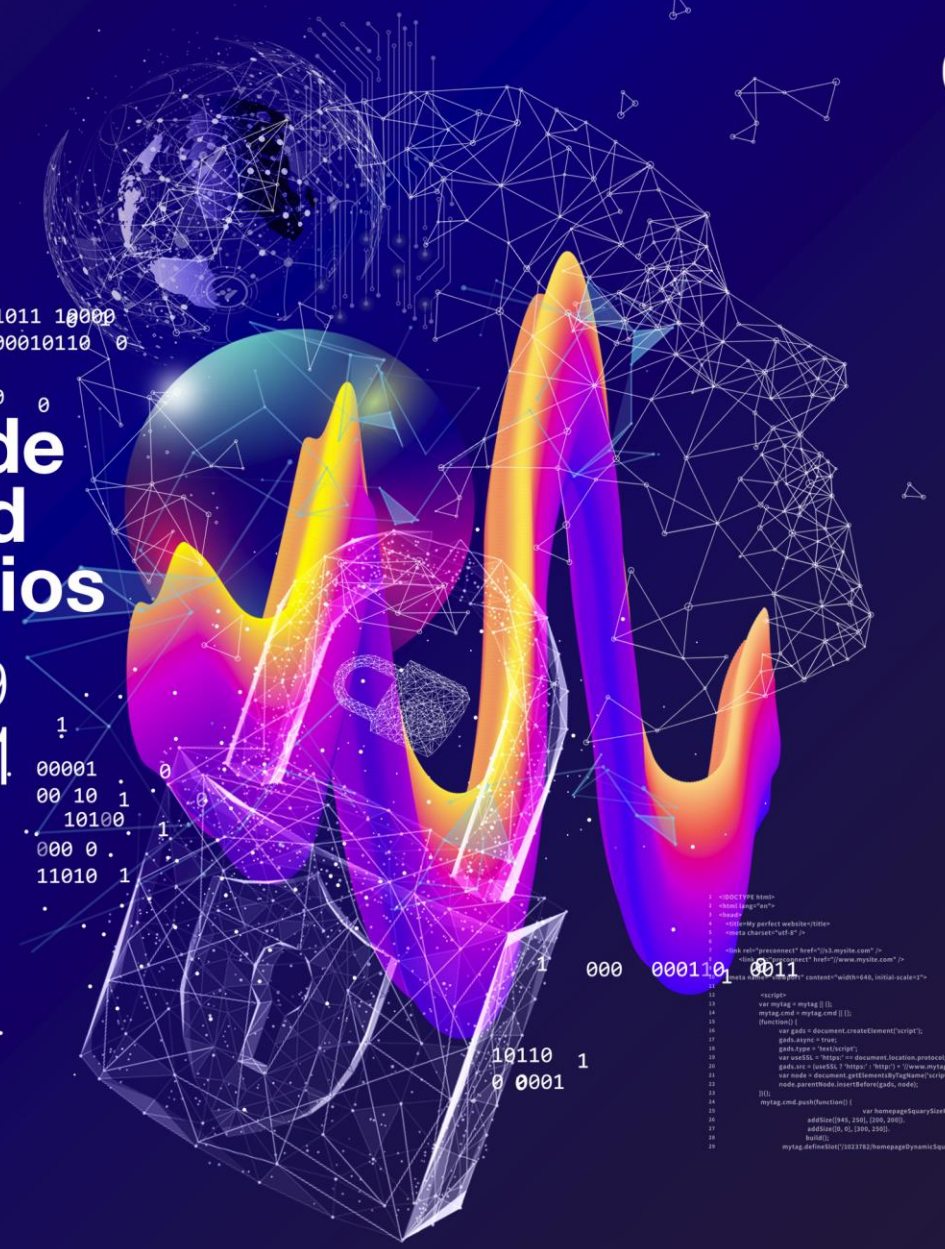
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

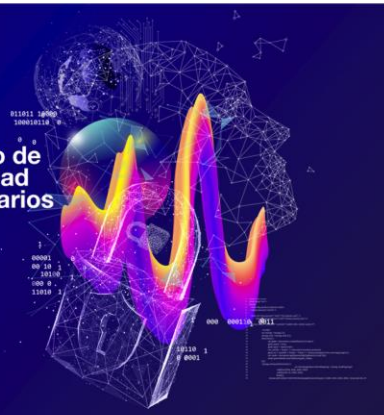
MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

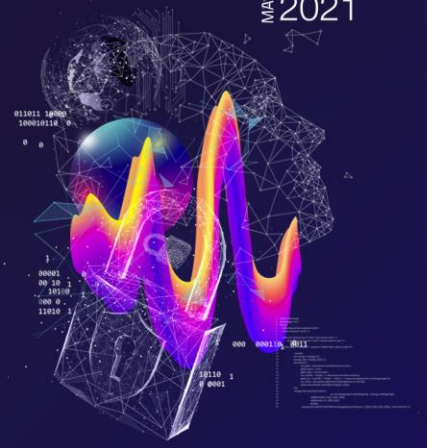
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática



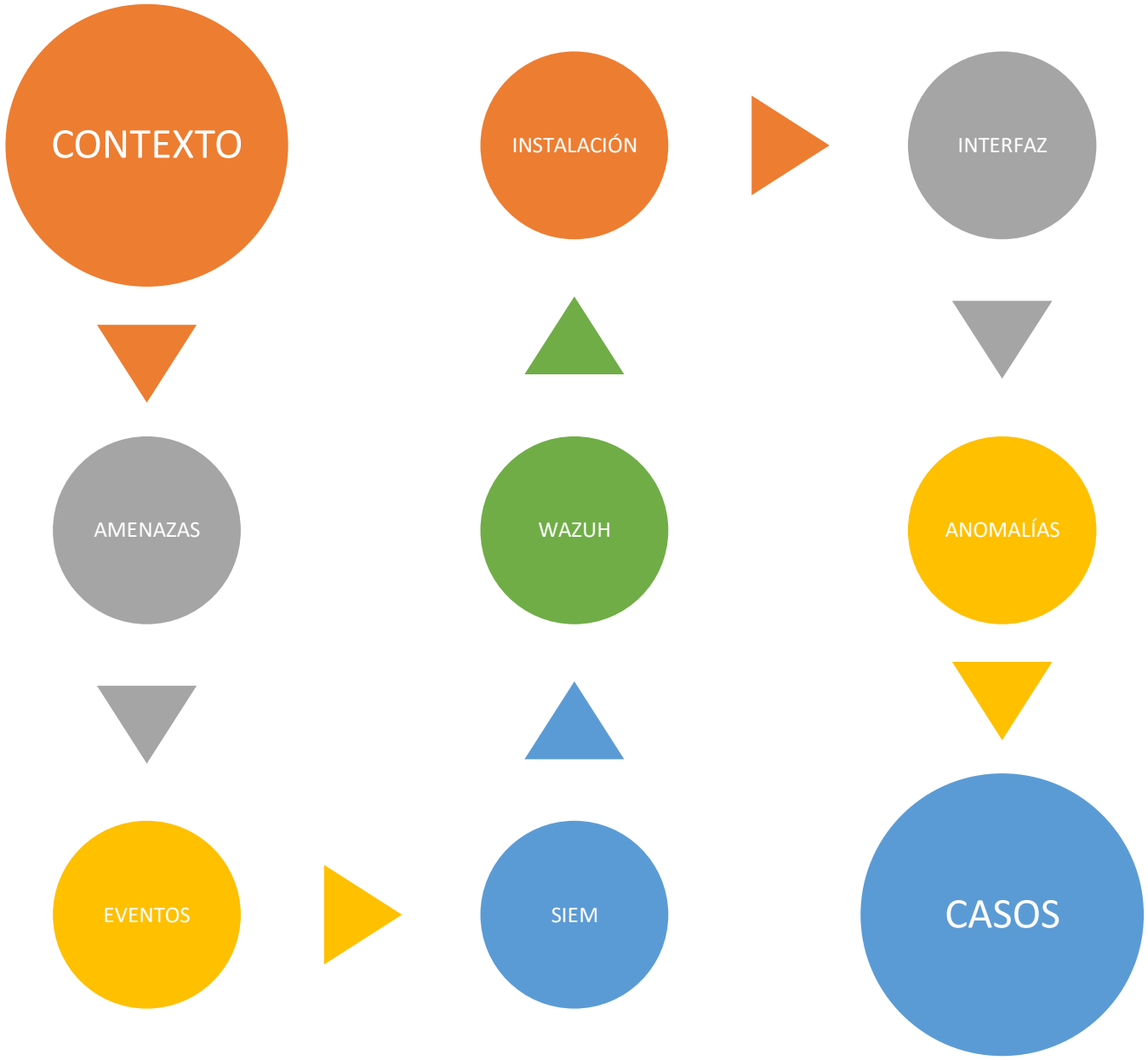
Taller:
SIEM opensource: Wazuh

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA

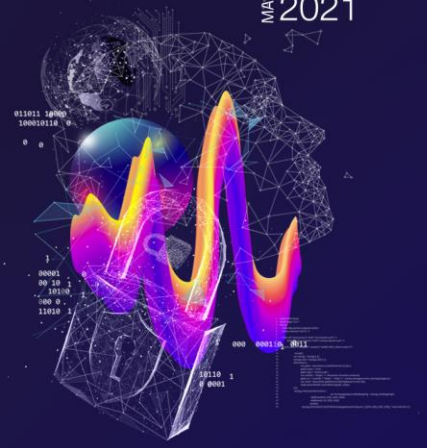


Ministerio del Interior y Seguridad Pública

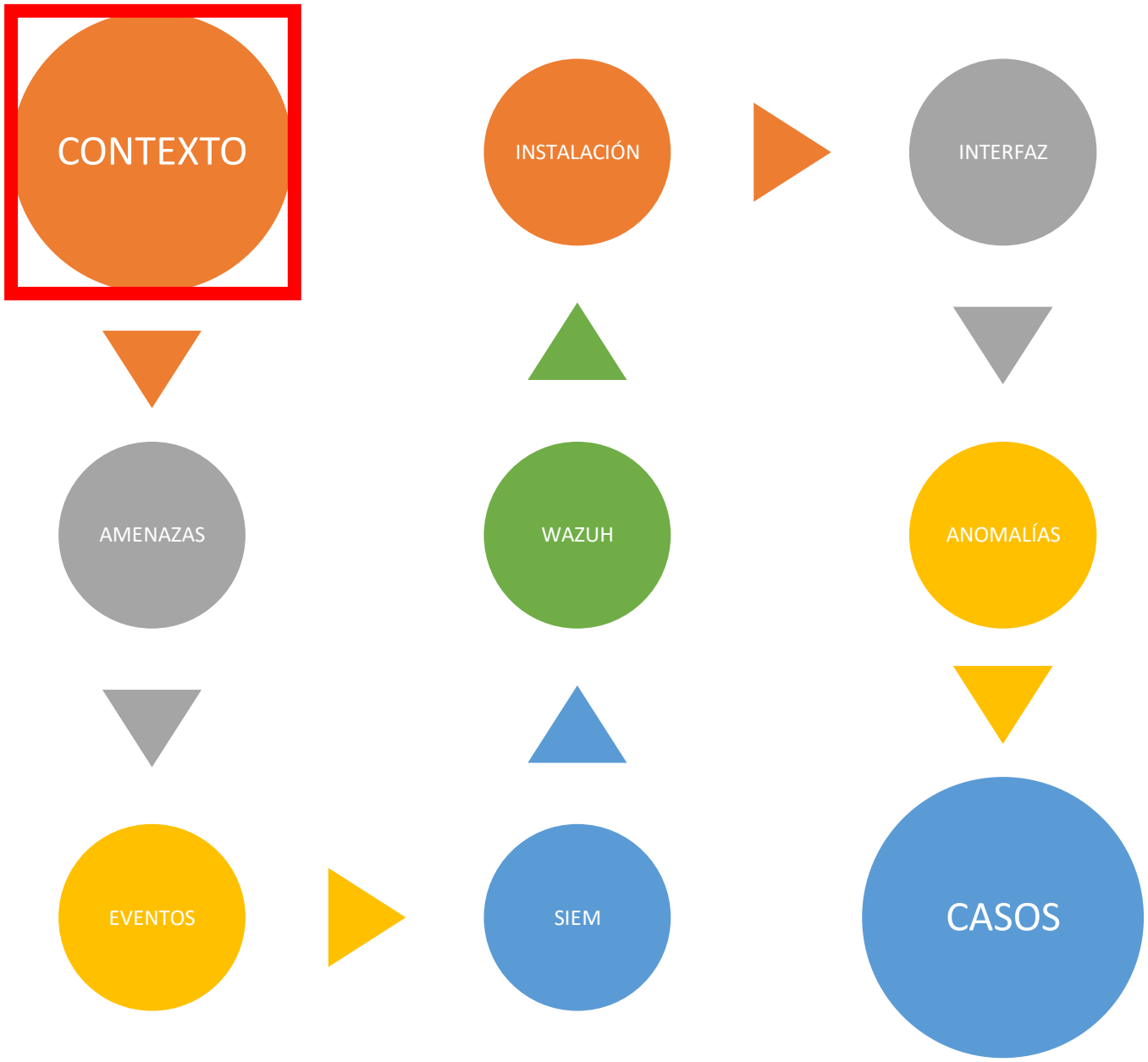
Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CONTEXTO: NORMATIVO

Instructivo Presidencial N°8

Medidas Internas de Ciberseguridad (N°3)

- Cada Jefe de Servicio, deberá presentar una evaluación de riesgo de ciberseguridad, un análisis del estado de vulnerabilidades, medidas actualmente adoptadas y un plan de acción de corto plazo.

Decretos Supremo: N°83 de 2005, N°93 de 206, N°14 de 2014, N°1 de 2015.

NOTA

El Artículo 2° de la **Resolución 1535 Exenta, Economía, publicada el 02.09.2009**, anula y reemplaza la Norma NCh2777 por la Norma NCh-ISO 27002, que el Artículo 1° de la mencionada Resolución, declara como Norma Oficial de la República de Chile, con su respectivo código y título de identificación como Tecnología de la información, Códigos de prácticas para la gestión de la seguridad de la información.

CONTEXTO: NORMATIVO

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

ISO/IEC 27002

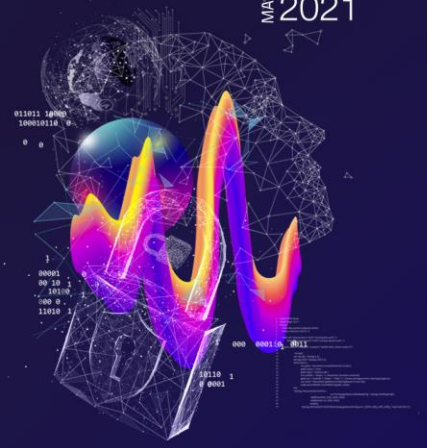
- 12.4.1 Registro de Eventos: Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

- 16.1.1 Responsabilidades y procedimientos: Establecer procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad;

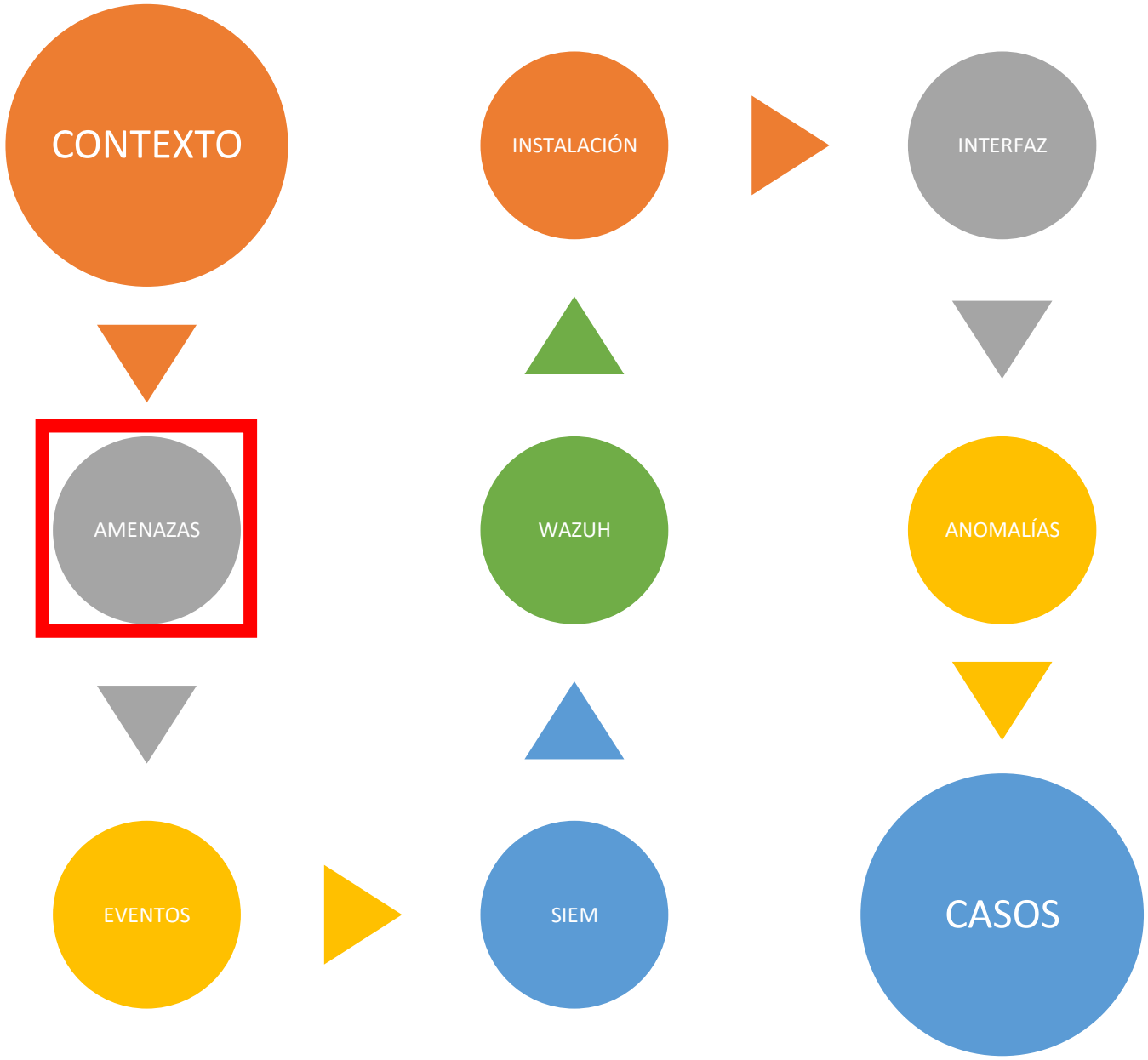
- 16.1.2 Informe de eventos de seguridad de la información: Los eventos de seguridad de la información se deberían informar a través de canales de administración adecuados lo más pronto posible.

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

AMENAZAS

¿Qué puede afectar la Confidencialidad, Integridad o Disponibilidad de mis activos de información?

- Daño físico: Fuego, agua, destrucción de equipos o medios, Polvo, corrosión, congelamiento.
- Eventos naturales: Fenómeno climático, fenómeno sísmico, fenómeno volcánico, fenómeno meteorológico, inundación.
- Pérdida de servicios esenciales: Falla de aire acondicionado o suministro de agua, pérdida de suministro de energía, falla de equipamiento de telecomunicaciones.
- Perturbación debido a radiación: Radiación electromagnética, radiación térmica, pulsos electromagnéticos .
- Compromiso de información: Señales de interferencia e interceptación que comprometen activos de información, espionaje remoto, escucha secreta, robo de medios o documentos, robo de equipos, recuperación de medios reciclados o descartados, divulgación o exfiltración, datos de fuentes poco fiables, manipulación con hardware, manipulación con software.

AMENAZAS

- Fallas técnicas: Falla de equipo, mal funcionamiento del equipo, saturación del sistema de información, mal funcionamiento del software, brecha de mantenimiento del sistema de información.

- Acciones no autorizadas: Uso no autorizado del equipo, copia fraudulenta de software, uso de software falsificado o copiado, corrupción de datos, procesamiento ilegal de datos.

- Compromiso de funciones: Error de uso, abuso de derechos, falsificación de derechos, negación de acciones, brecha de disponibilidad de personal.

- Pueden existir otras fuentes de amenazas de las siguientes vertientes a analizar según el caso:

i. Crackers
ii. Delitos informáticos
iii. Terrorismo
iv. Espionaje industrial (nacional o transnacional)
v. Internos

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

AMENAZAS:
¿CUÁNTO TIEMPO SE DEMORAN EN SER DETECTADOS LOS CIBERATAQUES?

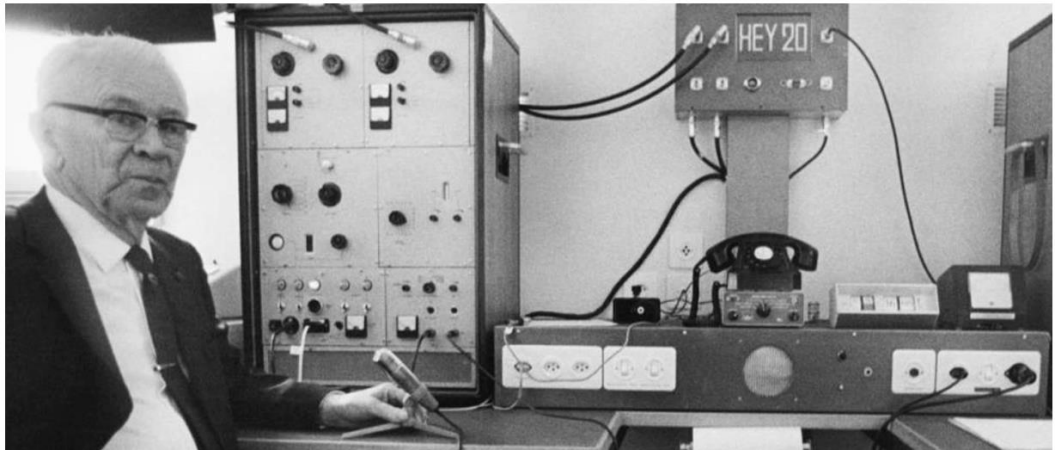
Las cifras son diversas, dependiendo del tipo de ataque y su objetivo, donde algunos ejemplos pueden ser:

- Minutos ante una denegación de servicios.
- Horas en un hackeo de sitio web. [index / flag / webshell]
- Meses en algunos tipos de exfiltración de datos.
- Años o décadas en infiltraciones de alto nivel.

ESPIONAJE >

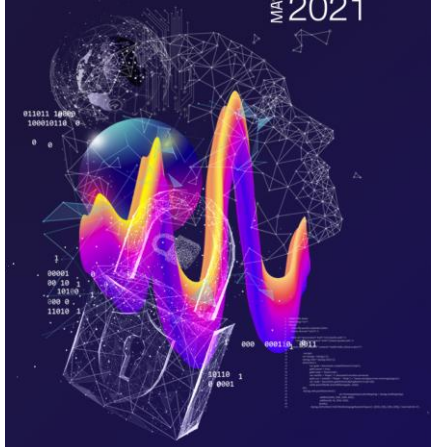
El golpe maestro de la CIA y sus socios alemanes

Una investigación de 'The Washington Post' y las cadenas ZDF y SRF destapa el espionaje de EE UU y Alemania a otros Gobiernos durante décadas



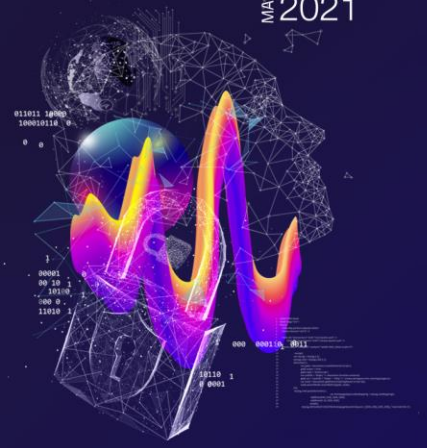
2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

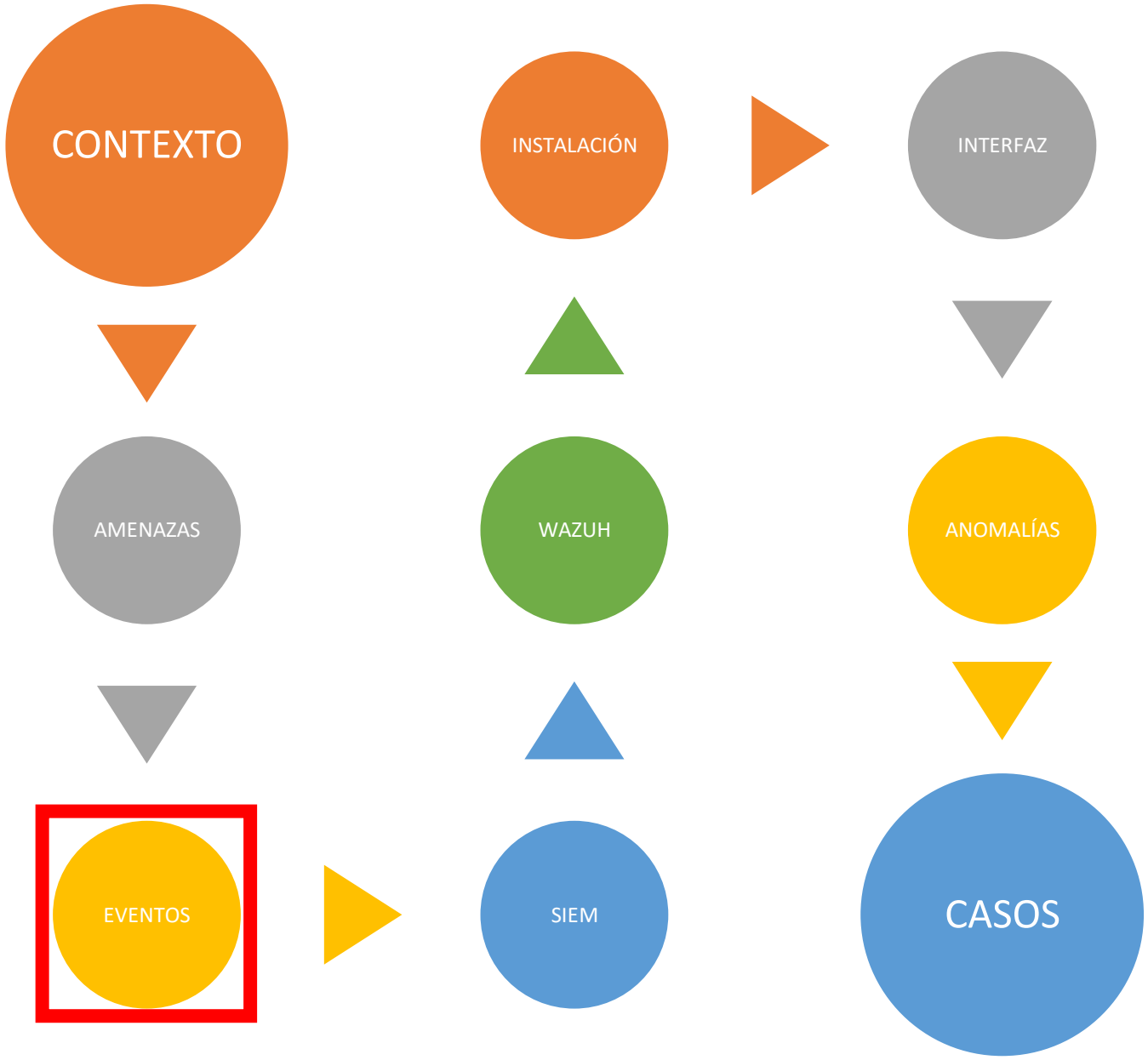


2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

EVENTOS: LOS DISPOSITIVOS, SISTEMAS Y APLICATIVOS NOS HABLAN

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Todos los equipos y sistemas bien diseñados contemplan funciones de auditoría y trazas de error.

Estos registros hablan de los que está sucediendo con ellos, los problemas, y general todo tipo de señales que nos ayudan a diagnosticar situaciones cuando hay problemas.

También ayudan estos registros a tener trazabilidad de las acciones ejecutadas por los usuarios de los sistemas, siendo por tanto una herramienta importante para auditorías.

Por tanto estos registros deben estar protegidos para evitar su pérdida por fallas del almacenamiento o modificaciones maliciosas internas o por terceras parte son autorizadas.

En general estos registros pueden llamarse eventos.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

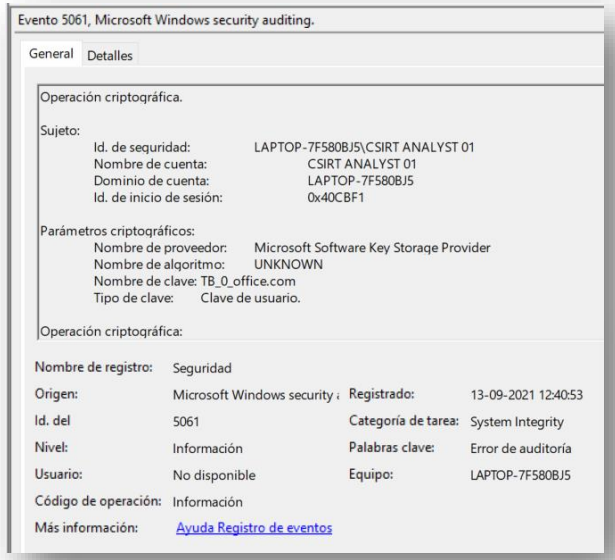
EVENTOS: ¿CÓMO SE DEFINEN?

Según la ISO 27000

Evento es la “aparición o cambio de una serie de circunstancias particulares”

Evento de seguridad de la información es:

Una ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o una falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

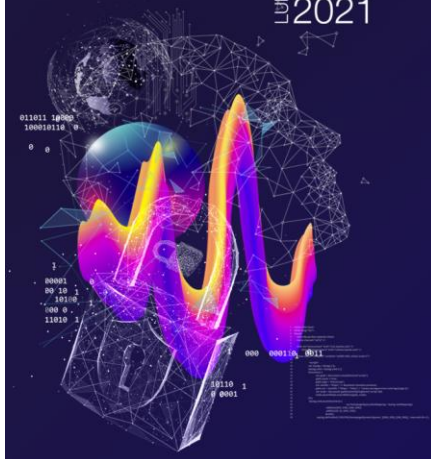


Evento de un servidor DNS:
Sep 13 11:48:16 ns2 named[32753]: 13-Sep-2021 11:48:16.060 client @0x7f0ed4090930 52.186.120.26#54558 (www.gob.cl): query: www.gob.cl IN AAAA - (163.247.70.25)

Sep 13, 2021 @ 12:36:10.708 predecoder.hostname: V predecoder.program_name: sshd predecoder.timestamp: Sep 13 12:36:10 input.type: log agent.name: V agent.id: 000 data.srcuser: squid data.srcip: 1.179.157.230 manager.name: V rule.mail: false rule.level: 5 rule.pci_dss: 10.2.4, 10.2.5, 10.6.1 rule.hipaa: 164.312.b rule.tsc: CC6.1, CC6.8, CC7.2, CC7.3 rule.description: sshd: Attempt to login using a non-existent user rule.groups: syslog, sshd, invalid_login, authentication_failed rule.nist_800_53: AU.14, AC.7, AU.6 rule.gdpr: IV_35.7.d, IV_32.2 rule.firedtimes: 35 rule.mitre.technique: Brute Force rule.mitre.id: T1110 rule.mitre.tactic: Credential Access rule.id: 5710 rule.gpg13: 7.1 location: /var/log/auth.log decoder.parent: sshd decoder.name: sshd id: 1631547370.7793193 GeoLocation.city_name: Nakhon Nayok

2do Seminario de Ciberseguridad para funcionarios públicos

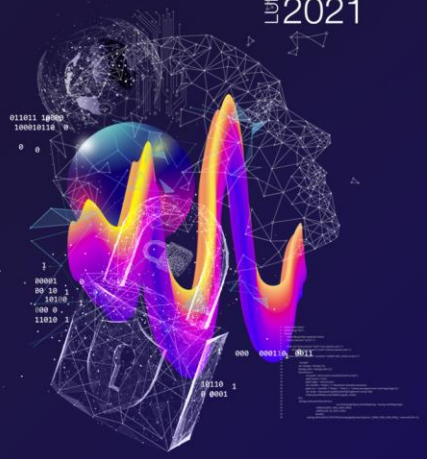
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

EVENTOS: ELEMENTOS QUE LOS COMPONEN

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Los registros de eventos deberían incluir, cuando corresponda:

a) IDs de usuarios;

b) Actividades del sistema;

c) Fechas, horas y detalles de los eventos clave, es decir el inicio y la finalización de la sesión;

d) La identidad del dispositivo y su ubicación si es posible, junto con el identificador del sistema;

e) Los registros de los intentos de acceso al sistema exitosos y rechazados;

f) Los registros de los datos exitosos y rechazados y otros intentos de acceso a los recursos;

g) Los cambios a la configuración del sistema;

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

EVENTOS : ELEMENTOS QUE LOS COMPONEN

h) El uso de privilegios;

i) El uso de utilidades y aplicaciones del sistema;

j) Los archivos y el tipo de acceso;

k) Las direcciones y protocolos de redes;

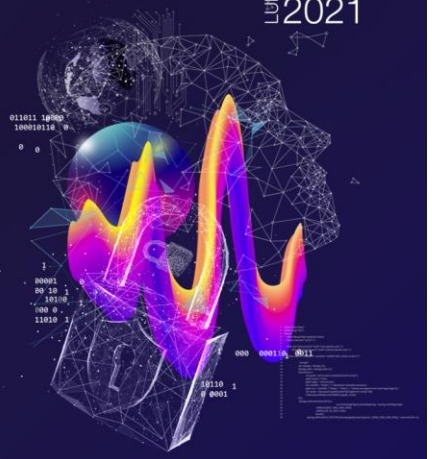
l) Las alarmas que se activaron con el sistema de control de acceso;

m) La activación y la desactivación de los sistemas de protección, como los sistemas de antivirus y los sistemas de detección de intrusos;

n) Los registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

El registro de eventos establece las bases para los sistemas de monitoreo automatizado que son capaces de generar informes y alertas consolidadas sobre la seguridad del sistema.

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

EVENTOS: EJEMPLOS DE INDICADORES BASADOS EN ÉSTOS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- Tráfico no humano (NHT): ¿está viendo una cantidad normal de tráfico en su sitio web o hay un aumento que indica un posible ataque de bot?

- Dispositivos no identificados en la red interna: sus empleados llevan dispositivos al trabajo; su organización puede estar usando dispositivos de Internet de las cosas (IoT) que no conoce. Estos dispositivos probablemente no sean seguros y pueden representar un gran riesgo para su organización. ¿Cuántos de estos dispositivos hay en su red?

- Intentos de intrusión: ¿Cuántas veces han intentado agentes malintencionados violar sus redes?

- Tiempo medio entre fallas (MTBF): ¿Cuánto tiempo existe entre fallas del sistema o del producto cuando se determina la confiabilidad?

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

EVENTOS: EJEMPLOS DE INDICADORES BASADOS EN ÉSTOS

- Tiempo medio de detección (MTTD): ¿Cuánto tiempo pasan desapercibidas las amenazas de seguridad en su organización? MTTD mide cuánto tiempo le toma a su equipo darse cuenta de un posible incidente de seguridad .

- Tiempo medio de reconocimiento (MTTA): ¿Cuál es el tiempo promedio que le toma comenzar a trabajar en un problema después de recibir una alerta?

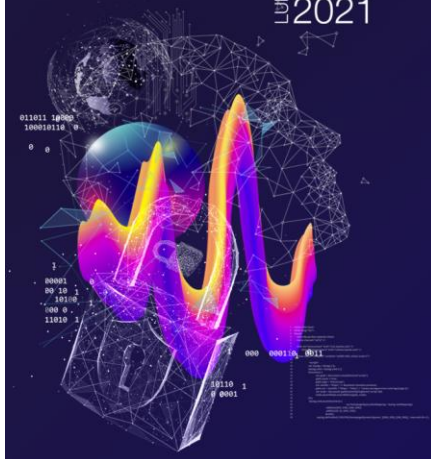
- Tiempo medio de contención (MTTC): ¿Cuánto tiempo se tarda en contener los vectores de ataque identificados?

- Tiempo medio de resolución (MTTR): ¿Cuánto tiempo le toma a su equipo responder a una amenaza una vez que se da cuenta de ella?

- Tiempo medio de recuperación (MTTR): ¿Cuánto tiempo le toma a su organización recuperarse de una falla del producto o del sistema?

2do Seminario de Ciberseguridad para funcionarios públicos

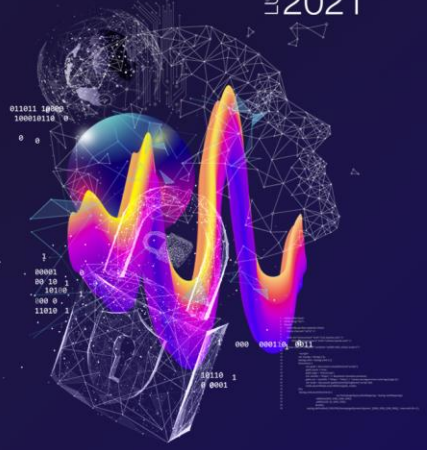
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

EVENTOS: EJEMPLOS DE INDICADORES BASADOS EN ÉSTOS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- Cumplimiento de la política de seguridad: ¿Qué tan bien realiza el seguimiento y la documentación de las excepciones, las configuraciones y los controles de cumplimiento?

- Días para parchear: los ciberdelincuentes a menudo aprovechan los retrasos entre la publicación de parches y la implementación. ¿Cuánto tiempo le toma a su equipo implementar los parches de seguridad?

- Capacitación en concientización sobre ciberseguridad : ¿Qué tan bien mantiene la documentación para la capacitación en concientización sobre ciberseguridad ? ¿Incluye a todos los miembros de su organización, incluidos los altos ejecutivos? ¿Quién ha recibido (y completado) la formación? ¿Entendieron esas personas el material?

- Número de incidentes de ciberseguridad informados: ¿Los empleados y usuarios informan sobre problemas de ciberseguridad a su equipo? Si es así, es una buena señal; los empleados y las partes interesadas reconocen los problemas descritos en su formación.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

EVENTOS: EJEMPLOS DE INDICADORES BASADOS EN ÉSTOS

- Clasificaciones de seguridad : una puntuación fácil de entender suele ser la forma más sencilla de comunicar métricas a colegas no técnicos. Un puntaje de postura de seguridad le da a su empresa una calificación en categorías de seguridad que incluyen seguridad de red, estado de DNS, cadencia de parcheo , puntaje de cubito, seguridad de punto final , reputación de IP, seguridad de aplicaciones web, charla de piratas informáticos, credenciales filtradas e ingeniería social . Según estos factores, su organización recibe una calificación general, lo que facilita ver de un vistazo qué tan segura es su empresa en relación con otras en su industria.

- Gestión de acceso: ¿Cuántos usuarios tienen acceso administrativo?

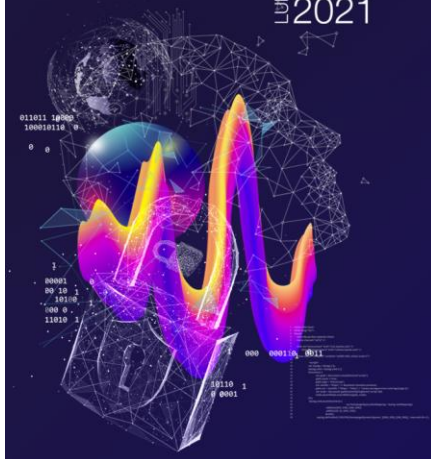
- Éxito del ataque de phishing : ¿Cuál es el porcentaje de correos electrónicos de phishing abiertos por sus empleados?

- Monitoreo de infecciones de virus: ¿Con qué frecuencia su software antivirus escanea aplicaciones comunes como clientes de correo electrónico, navegadores web y software de mensajería instantánea en busca de malware conocido ?

- Costo por incidente: ¿Cuánto cuesta responder y resolver un ataque? ¿Cuánto dinero está gastando en horas extra del personal, costos de investigación, pérdida de productividad de los empleados y comunicación con los clientes?

2do Seminario de Ciberseguridad para funcionarios públicos

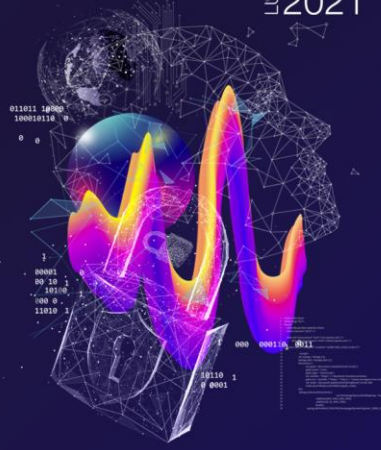
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



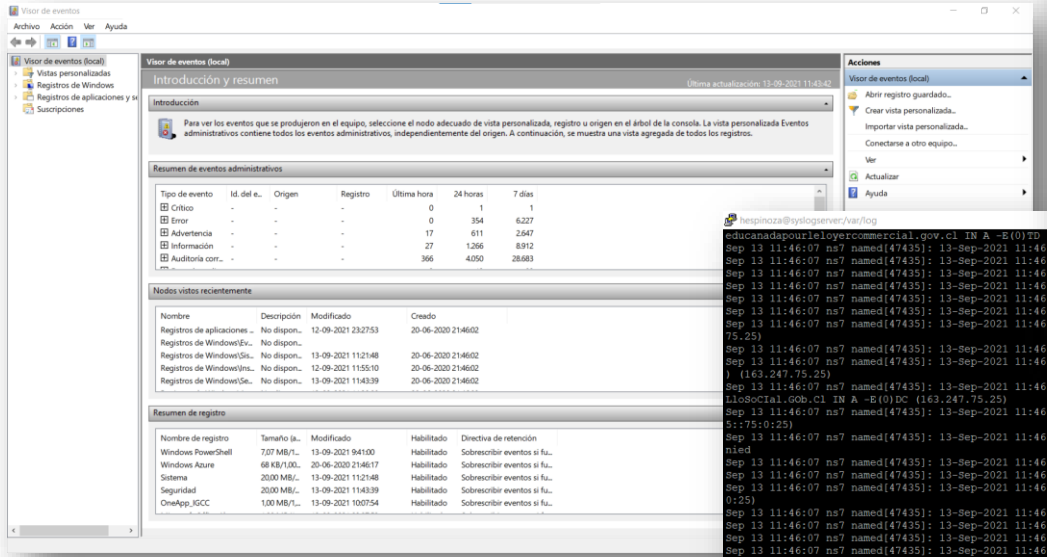
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

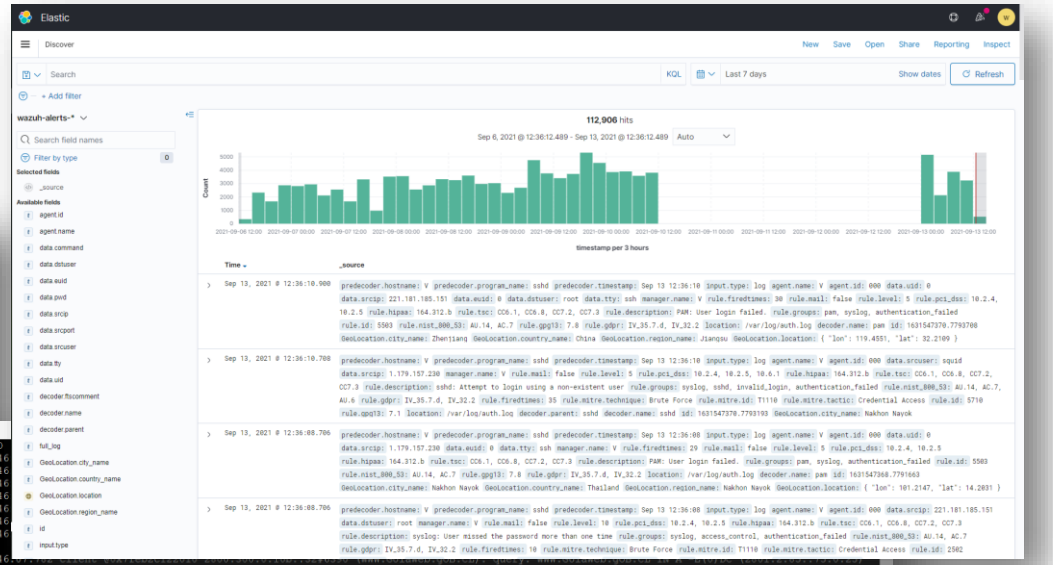
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

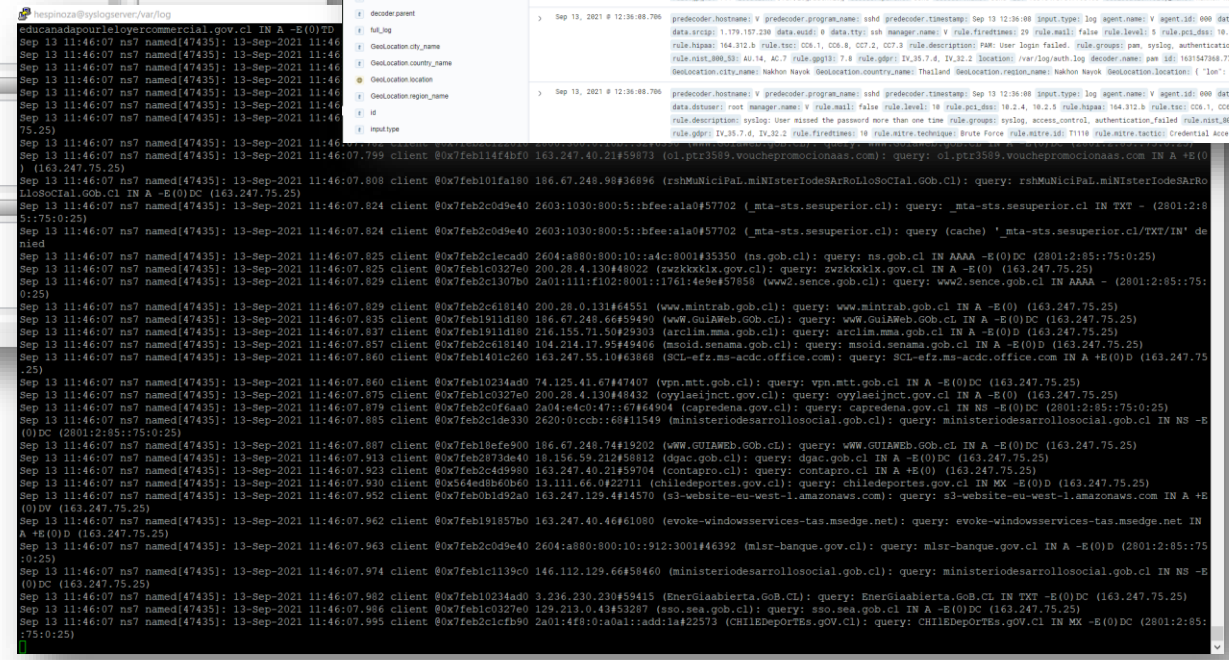
EVENTOS: ¿DÓNDE ESTAN?

En general son archivos y se encuentran archivos en texto plano o algunos en bases de datos…

Aportan información, pero son millones…







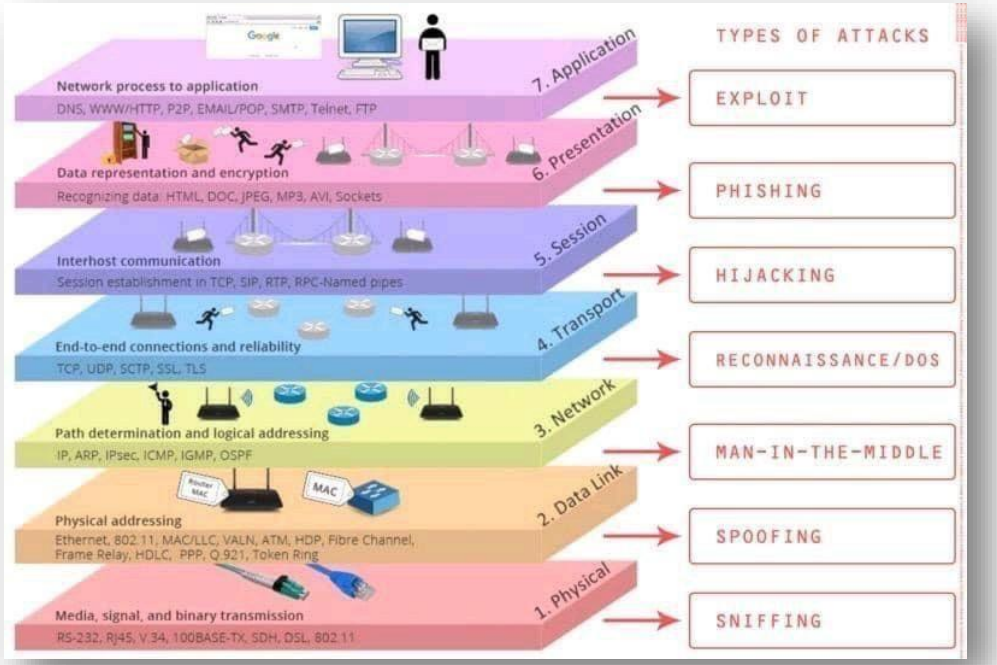
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

EVENTOS: ¿CÓMO SE RELACIONA CON INCIDENTES?

Según la ISO 27000

Incidente de seguridad de la información:

Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

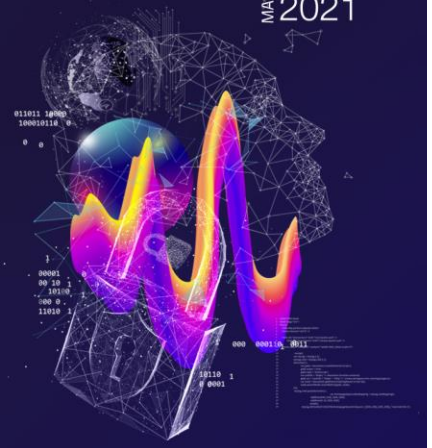


2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021

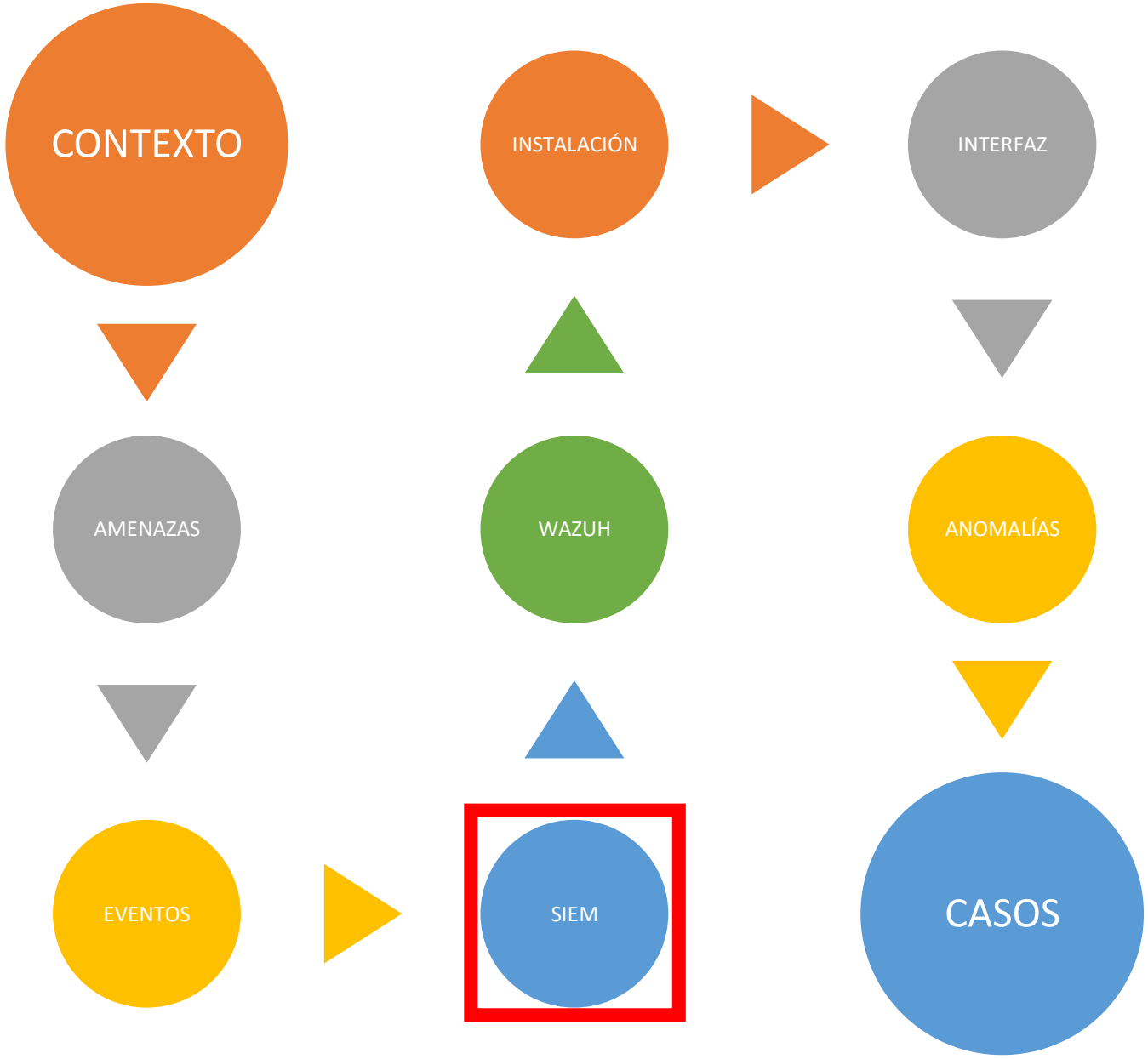
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



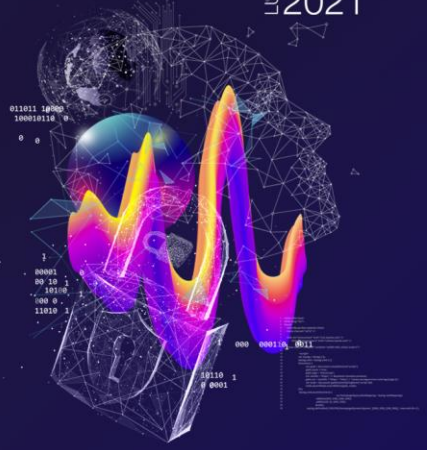
AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

SIEM: SYSLOG SERVER
(UN SIMPLE RECOLECTOR DE EVENTOS O UN SIEM ULTRA BAJO COSTO)

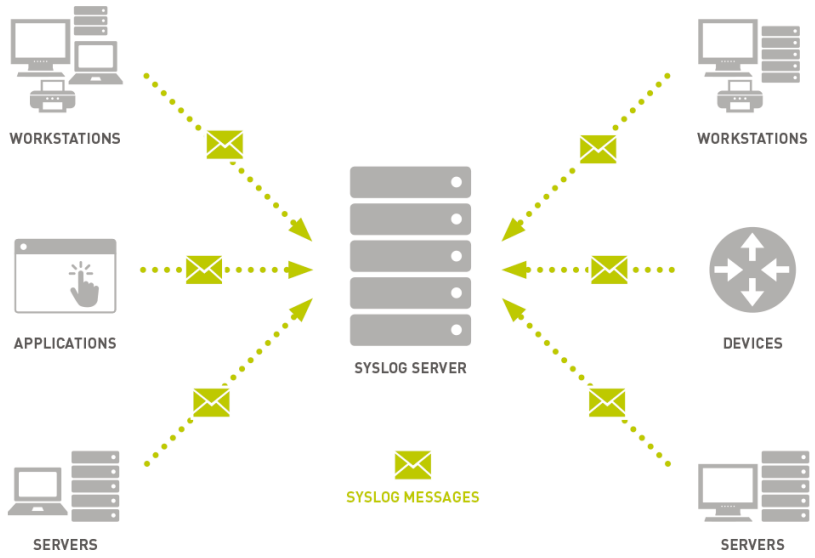
Muchos dispositivos

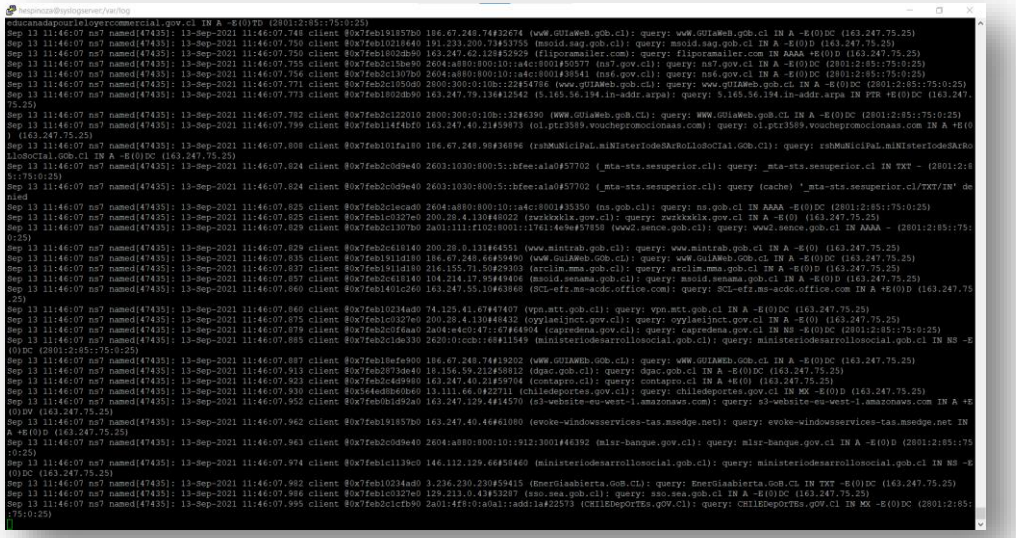
Muchos aplicativos por dispositivos

Muchos dispositivos por usuario

Muchas oficinas y redes con dispositivos

=> Log's = Dispositivos * Aplicativos * Usuarios * instalaciones* tasa => Millones de registros…





Ministerio del Interior y Seguridad Pública
Gobierno de Chile

SIEM:
¿CÓMO ENCONTRAMOS ALGO RELEVANTE EN ESE OCÉANOS DE DATOS?

Correlación de eventos

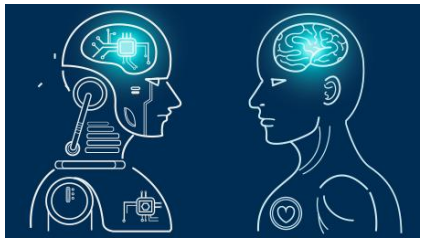
Cuando somos capaces de manejar diferentes fuentes de información, asociarlas Y entenderlas es posible obtener un nivel de información de mayor valor:

Incidentes con mayor relevancia desde el punto de vista de la ciberseguridad.

Aquí los analistas deben poner ojo y hacer el zoom pertinente para indagar que hay detrás de esa anomalía.

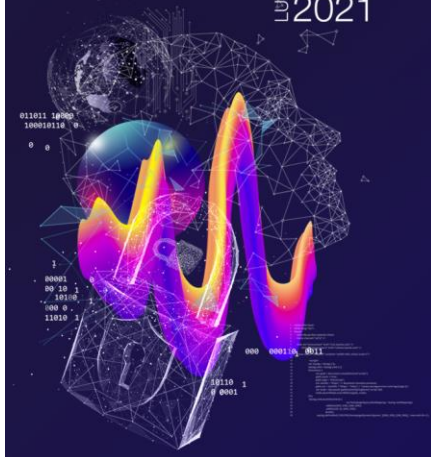
La fórmula es: Concentrador/Recolector de eventos + una Red Neuronal que establezca y aplique correlaciones.

+



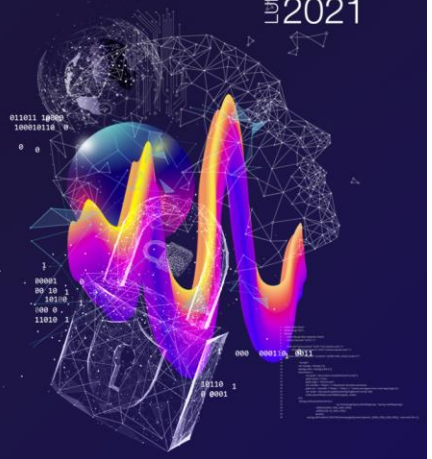
= ANÁLISIS EN BASE A CORRELACIÓN DE EVENTOS **SIEM**

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

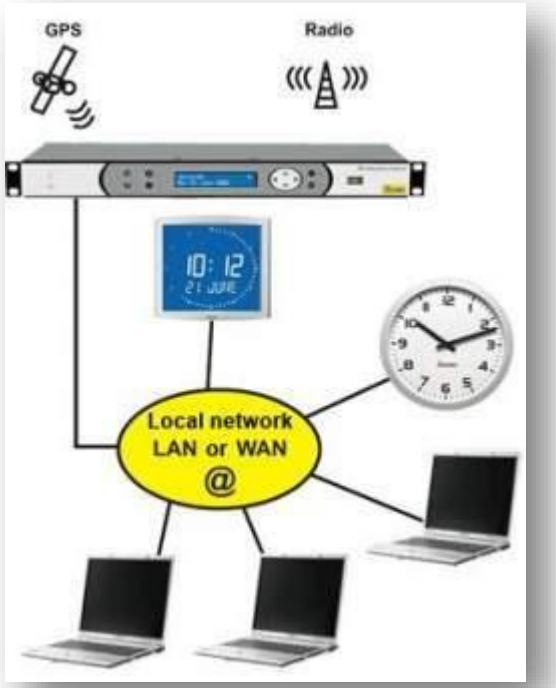
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

SIEM: NTP Y LA IMPORTANCIA DEL TIEMPO

Hay un factor que es crítico y que muchas veces es pasado por alto: El Tiempo.

Cada evento tiene un sello de tiempo.

Si los sellos de tiempo no están adecuadamente sincronizados, pues provienen de múltiples fuentes, entonces la red neuronal o el analista con alta probabilidad obtendrá conclusiones incorrectas y no encontrará el incidente relevante.



Entonces nos salta a la memoria el control normativo: A.12.4.4 [Sincronización de Relojes].
Es importante que todos los dispositivos que nos hablan y escriben sus registros lo hagan con un patrón de tiempo sincronizado a través del protocolo NTP. [ntp.shoa.cl]

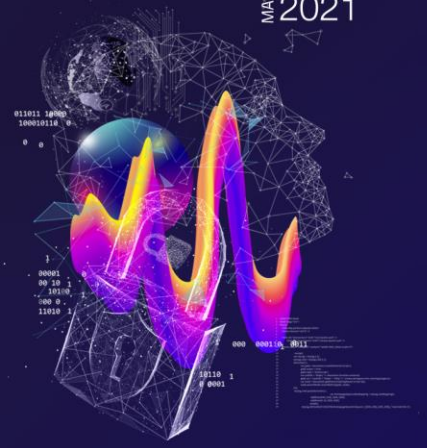
Con una adecuada regla de correlación y sincronización de los eventos, se podrán obtener análisis interesantes:

Por ejemplo, una secuencia de eventos de interés, que correlaciona conceptos:

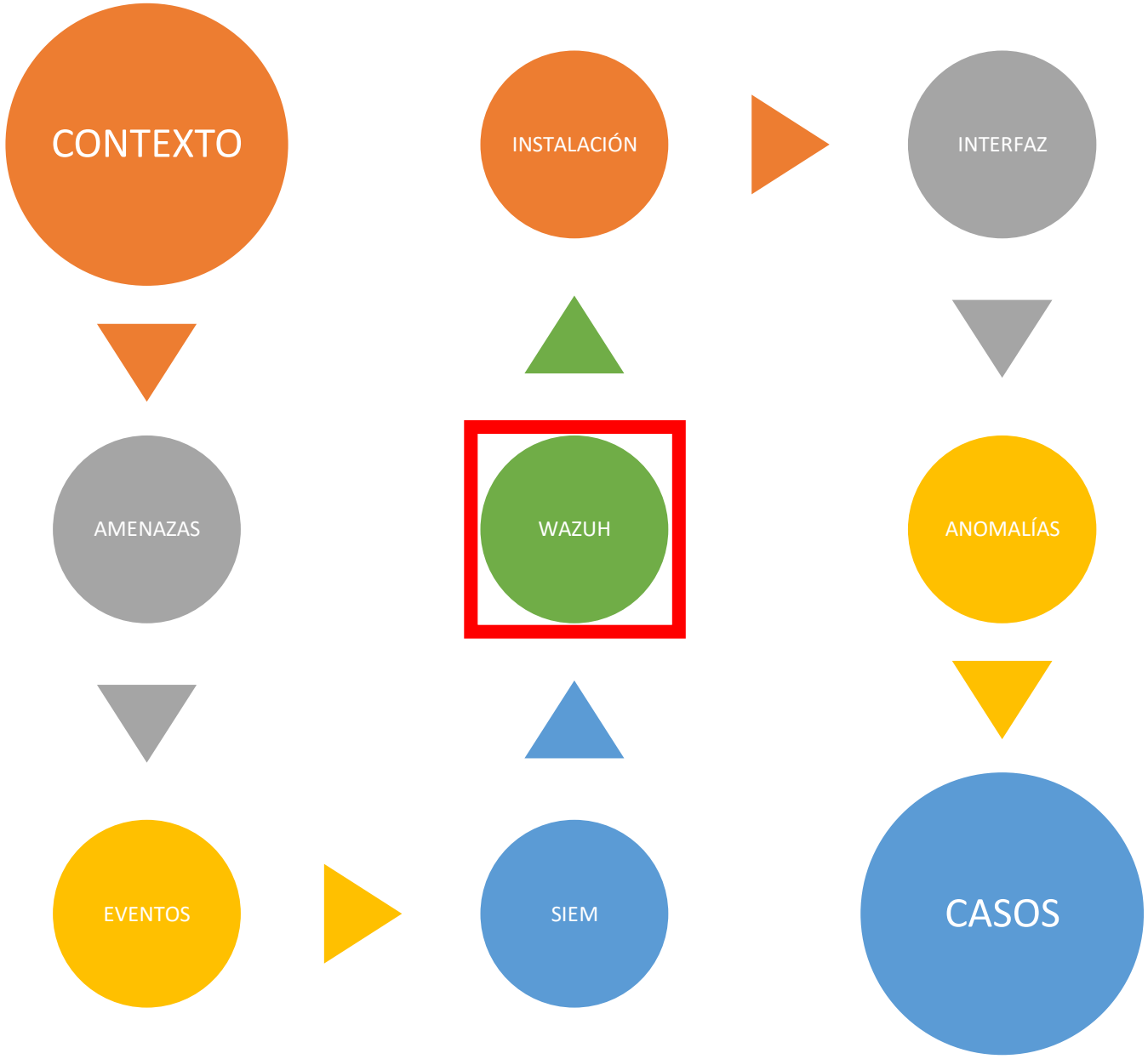
- Que se registres más de 3 intentos de logins incorrectos
- Que a continuación exista un acceso exitoso en el sistema “miPlataforma”
- Que la IP de origen sea de un país que no tiene relación con “miPlataforma”
- Que esto eventos se encuentran enmarcados en la ventana temporal de 00:00-08:00hrs

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

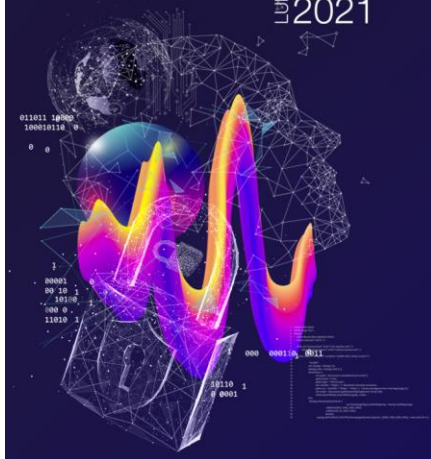
WAZUH: ¿CÓMO PUEDO IMPLEMENTAR UN CENTRO DE ANÁLISIS A BAJO COSTO?

1.- Los más simple y barato: un syslogserver + un ser humano [correlacionador] ;-)
Pro: Bajo costo y simple
Con: la correlación depende de la habilidad
De la persona

2.- Comprar un software/hardware
en el mercado hay muchos y muy buenos
Pro: con soporte, muchas funcionalidades
(xdr, cloud)
Con: costo.

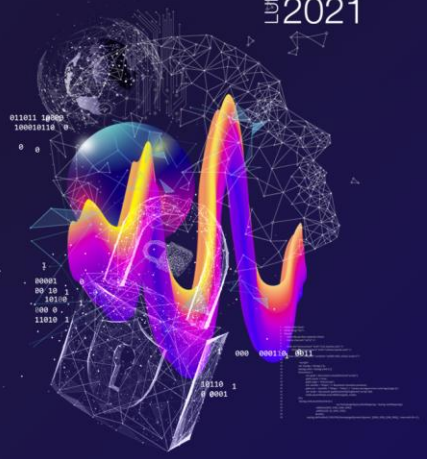
3.- Buscar un plataforma de código abierto
Que requiere conocimientos de diferentes
Paquetes que en su conjunto estructuran un
SIEM, como por ejemplo:

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

WAZUH: ¿QUÉ ES?

Wazuh es una solución de monitoreo de seguridad gratuita, de código abierto y lista para la detección de amenazas, monitoreo de integridad, respuesta a incidentes y cumplimiento.

Wazuh se utiliza para recopilar, agregar, indexar y analizar datos de seguridad, lo que ayuda a las instituciones a detectar intrusiones, amenazas y anomalías de comportamiento.

A medida que las amenazas cibernéticas se vuelven más sofisticadas, se necesitan análisis de seguridad y monitoreo en tiempo real para una rápida detección y reparación de amenazas. Es por eso que wazuh contempla un agente liviano que proporciona las capacidades necesarias de monitoreo y respuesta, mientras que el componente de servidor proporciona la inteligencia de seguridad y realiza análisis de datos.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

WAZUH: ¿QUÉ ES?

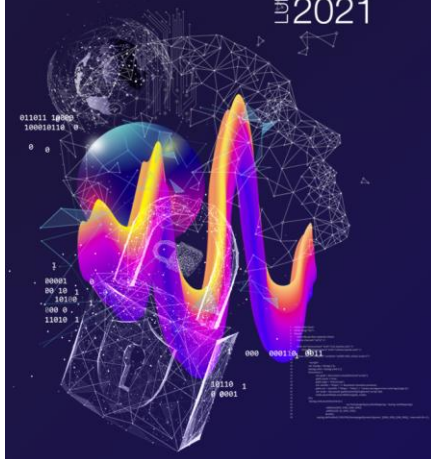
Las reglas de Wazuh le ayudan a conocer los errores de la aplicación o del sistema, las configuraciones incorrectas, las actividades maliciosas intentadas o exitosas, las violaciones de políticas y una variedad de otros problemas operativos y de seguridad.

Wazuh supervisa el sistema de archivos e identifica cambios en el contenido, los permisos, la propiedad y los atributos de los archivos que debe vigilar. Además, identifica de forma nativa a los usuarios y las aplicaciones que se utilizan para crear o modificar archivos.

Las capacidades de monitoreo de la integridad de los archivos se pueden usar en combinación con la inteligencia de amenazas para identificar amenazas o hosts comprometidos. Además, varios estándares de cumplimiento normativo, como PCI DSS, lo requieren.

2do Seminario de Ciberseguridad para funcionarios públicos

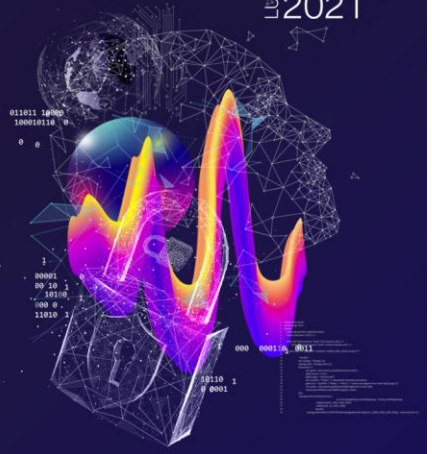
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

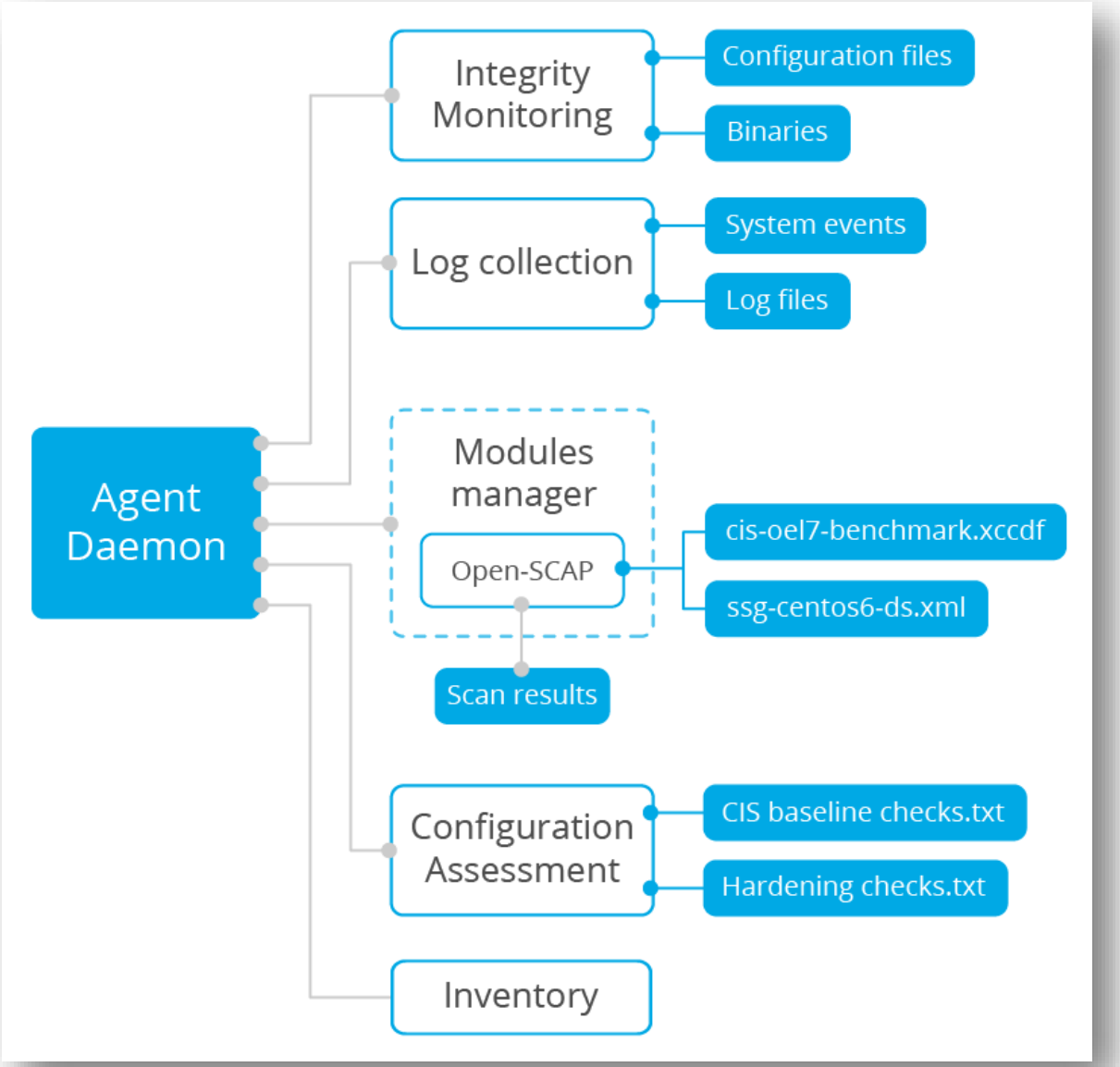
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

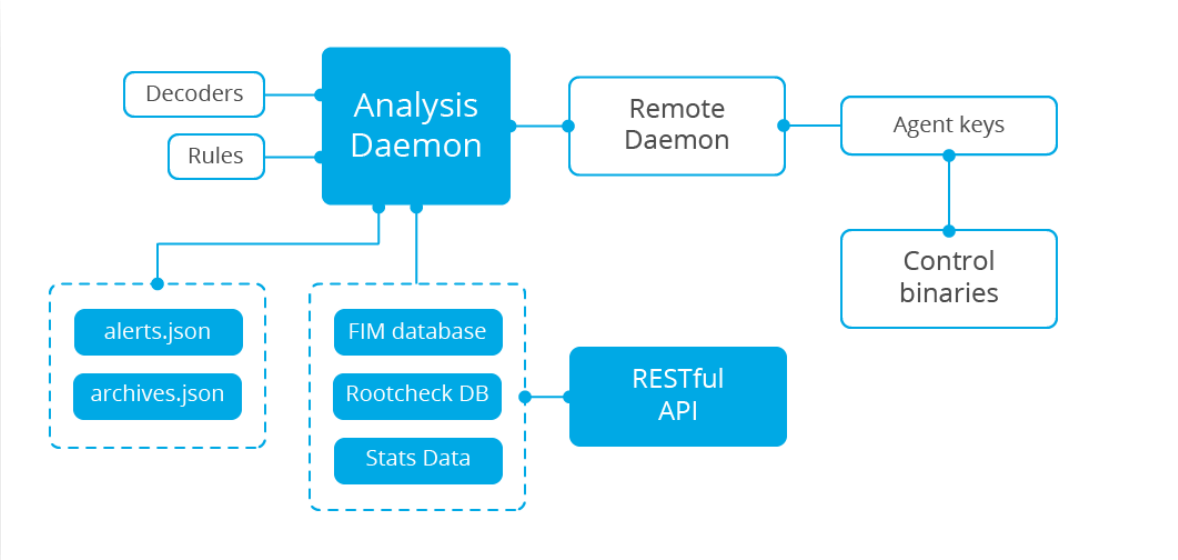
WAZUH: COMPONENTES

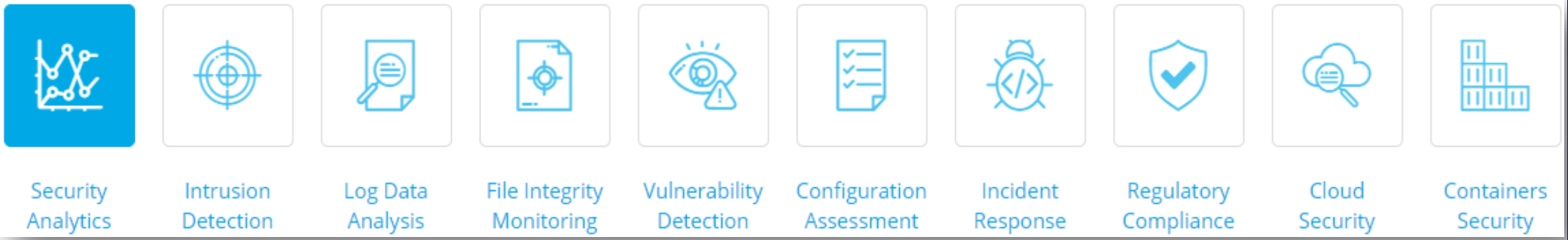


Ministerio del Interior y Seguridad Pública

Gobierno de Chile

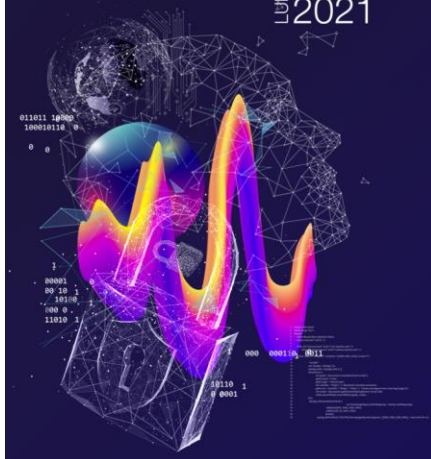
WAZUH: COMPONENTES





2do Seminario de Ciberseguridad para funcionarios públicos

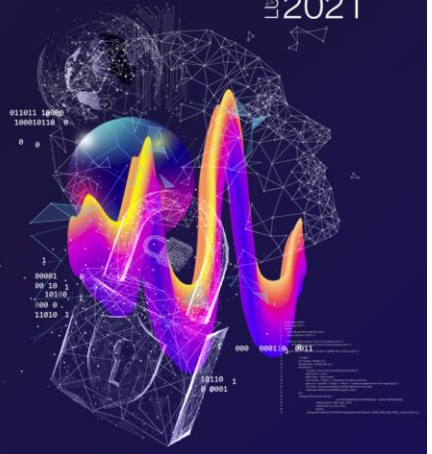
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

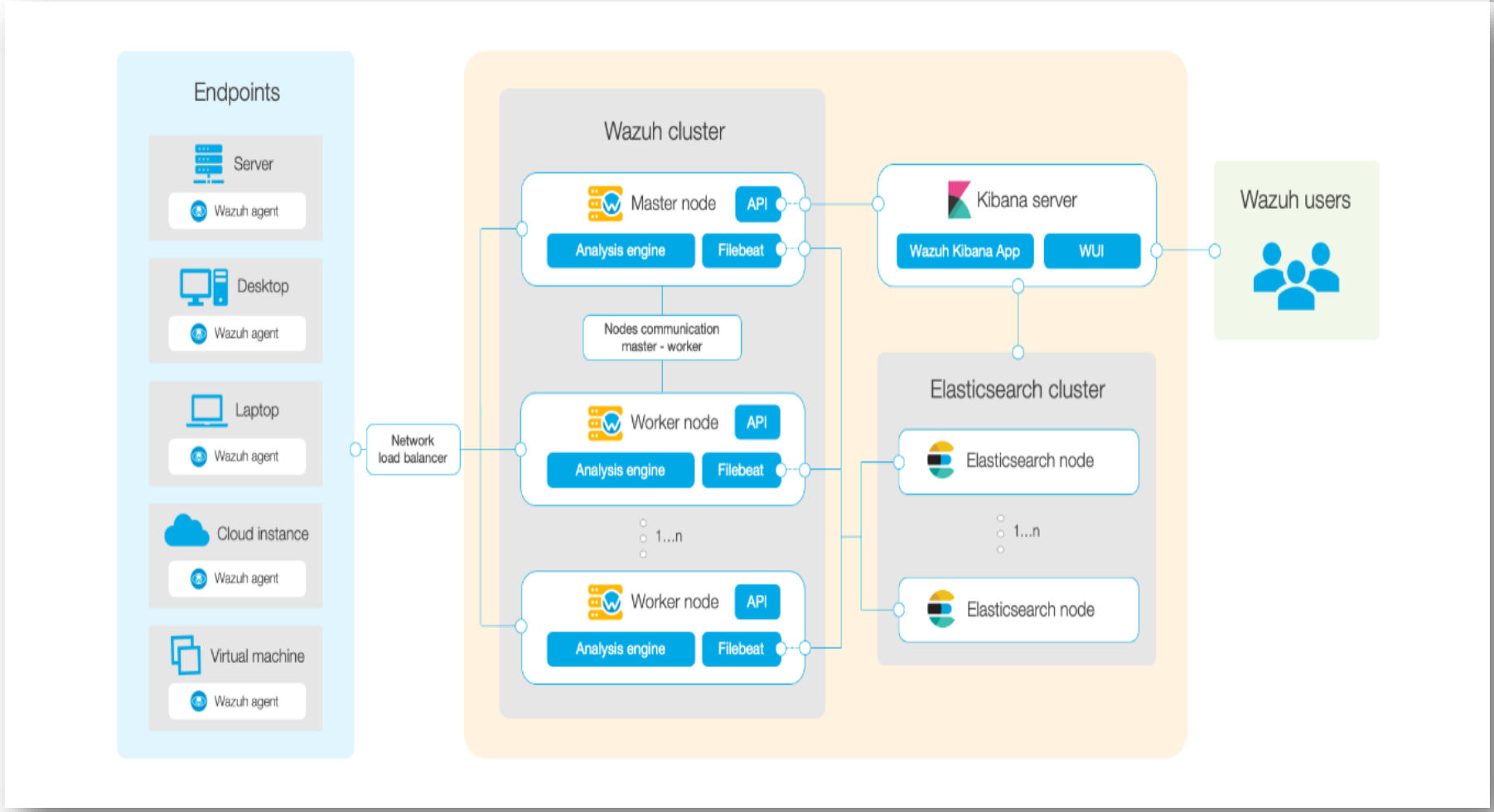
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

WAZUH: ARQUITECTURA

Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Ministerio del Interior y Seguridad Pública

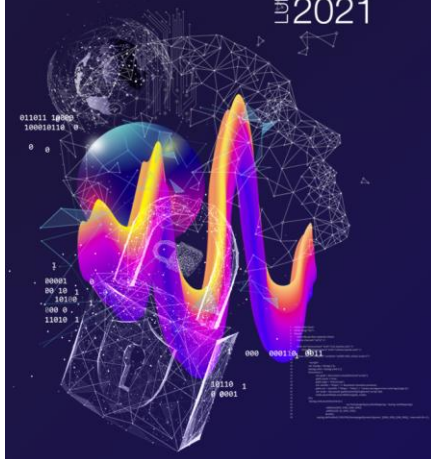
Gobierno de Chile

WAZUH: PUERTOS DE COMUNICACIÓN RELEVANTES

Componente	Software	Puerto	Protocolo	Objetivo
Servidor de Wazuh	Gestor de Wazuh	1514	TCP (predeterminado)	Servicio de conexión de agentes
		1514	UDP	Servicio de conexión de agentes
		1515	TCP	Servicio de registro de agentes
		1516	TCP	Demonio de clúster de Wazuh
		514	UDP (predeterminado)	Recopilador de syslog de Wazuh (deshabilitado de forma predeterminada)
		514	TCP	Recopilador de syslog de Wazuh (deshabilitado de forma predeterminada)
	API de Wazuh	55000	TCP	API RESTful de Wazuh
Pila elástica	Elasticsearch	9200	TCP	API RESTful de Elasticsearch
		9300-9400	TCP	Comunicación de clúster de Elasticsearch
	Kibana	443	TCP	Interfaz web de Kibana

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

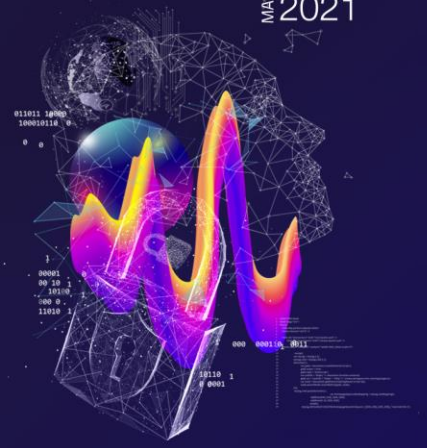


CSIRT

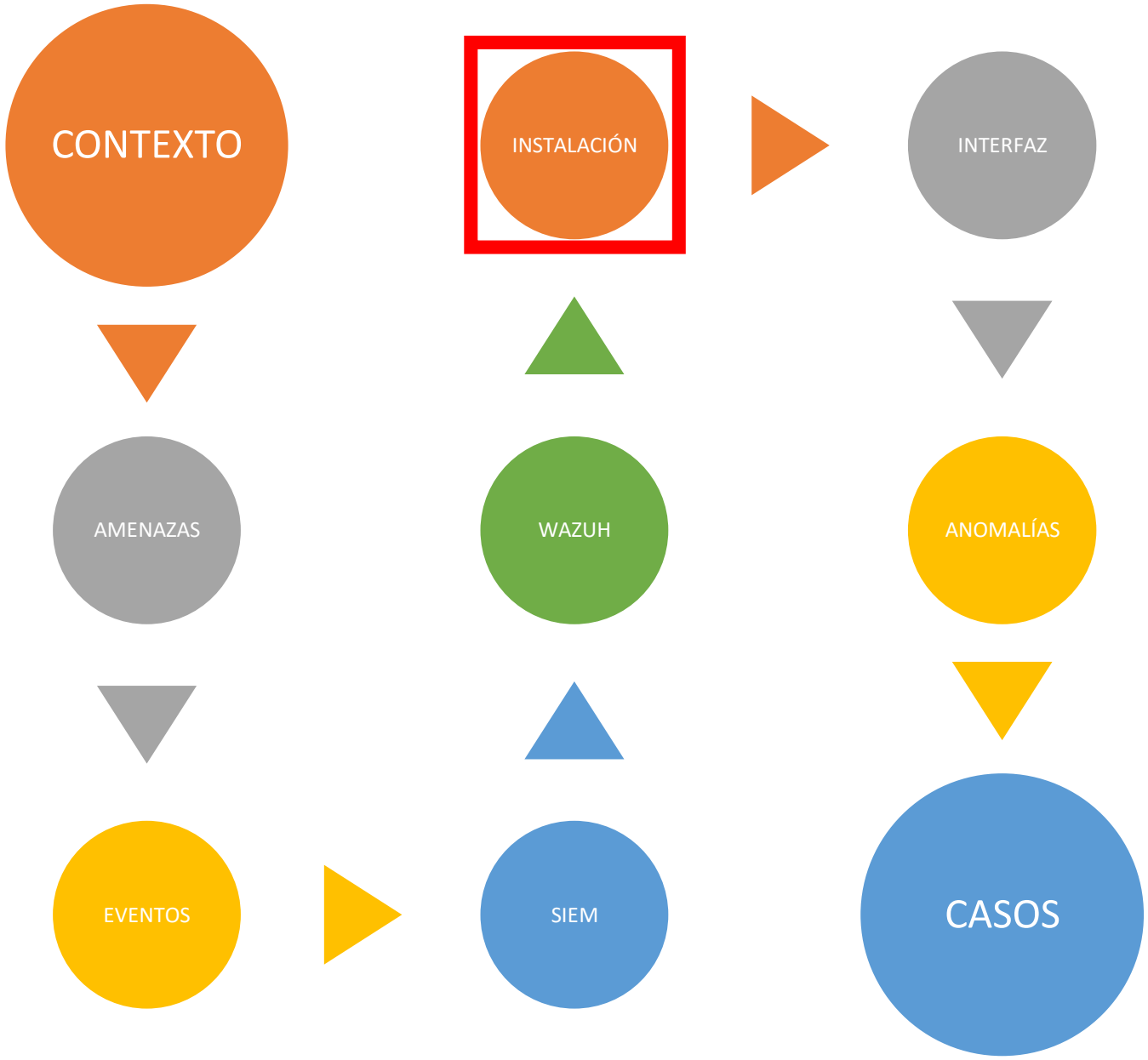
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



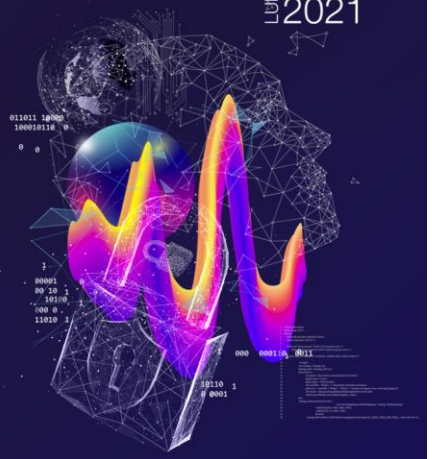
AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: REQUISITOS BÁSICOS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

El servidor Wazuh y los componentes Elastic Stack se pueden instalar en los siguientes sistemas operativos Linux, por el momento:

- Amazon Linux 1 y 2
- CentOS 6 o posterior
- Debian 7 o posterior
- Fedora 31 o posterior
- Oracle Linux 6 o posterior
- Red Hat Enterprise Linux 6 o posterior
- Ubuntu 12 o posterior

En una implementación todo en uno, tanto el servidor Wazuh como Elastic Stack se instalan en el mismo host. Un caso de uso típico para este tipo de entorno admite alrededor de 100 agentes.

- Los requisitos mínimos para este tipo de implementación son 4 GB de RAM y 2 núcleos de CPU, y los recomendados son 16 GB de RAM y 8 núcleos de CPU. Se requiere un sistema operativo de 64 bits.

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

INSTALACIÓN: REQUISITOS BÁSICOS

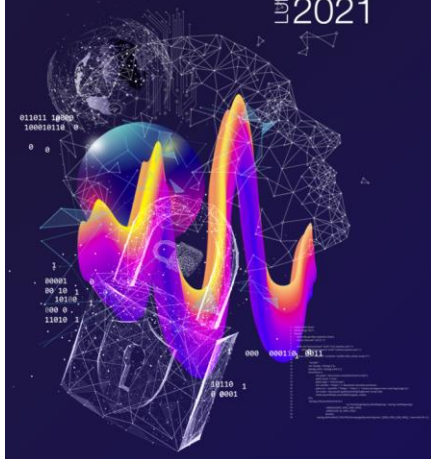
Los requisitos de **espacio en disco** dependen de las **alertas por segundo (APS)** generadas. El APS esperado varía significativamente según la cantidad y el tipo de puntos finales monitoreados.

Almacenamiento estimado por agente necesario para 90 días de alertas según el tipo de *endpoint* monitoreado

Puntos finales supervisados	APS	Almacenamiento (GB / 90 días)
Servidores	0,25	3.8
Estaciones de trabajo	0,1	1,5
Dispositivos de red	0,5	7,6

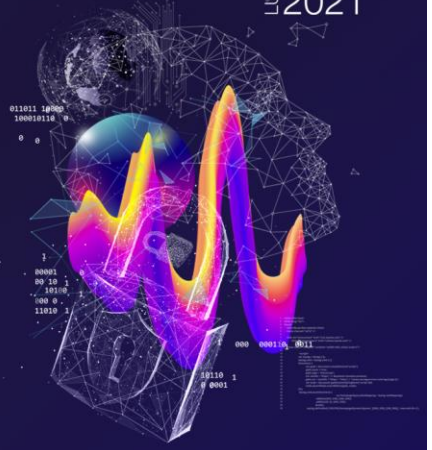
Por ejemplo, para un entorno con 80 estaciones de trabajo, 10 servidores y 10 dispositivos de red, el almacenamiento necesario para 90 días de alertas es de 236 GB aproximadamente.

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021

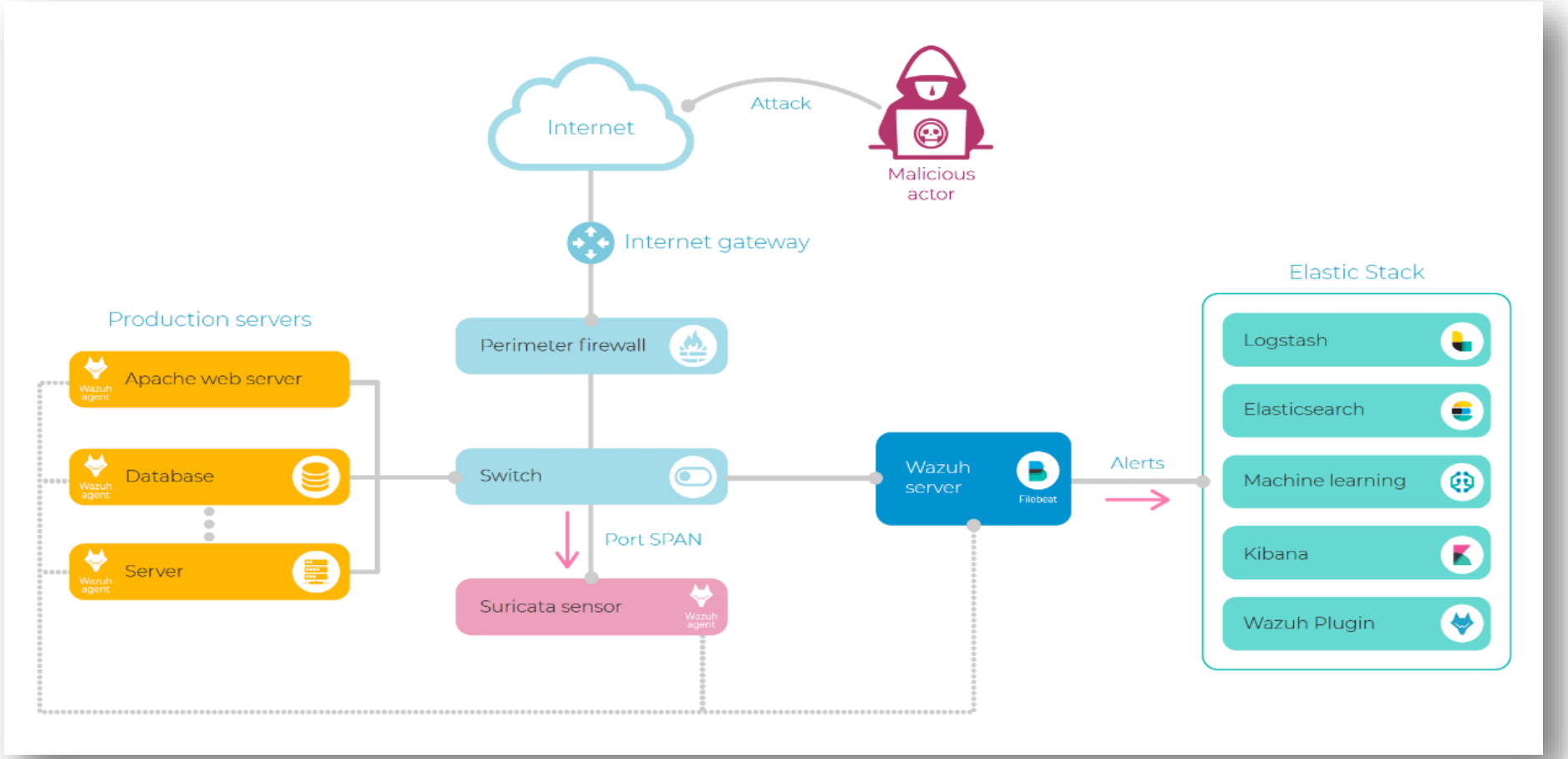


CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: ¿DONDE UBICAR WAZUH EN NUESTRA RED INTERNA?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Mediante la detección de intrusiones basada en firmas y anomalías, con tecnologías como Wazuh, Suricata y Machine Learning de Elastic, se puede facilitar la detección de amenazas y aumentar la eficiencia en la respuesta a las mismas, ayudando también en la investigación y generación de medidas para su prevención.

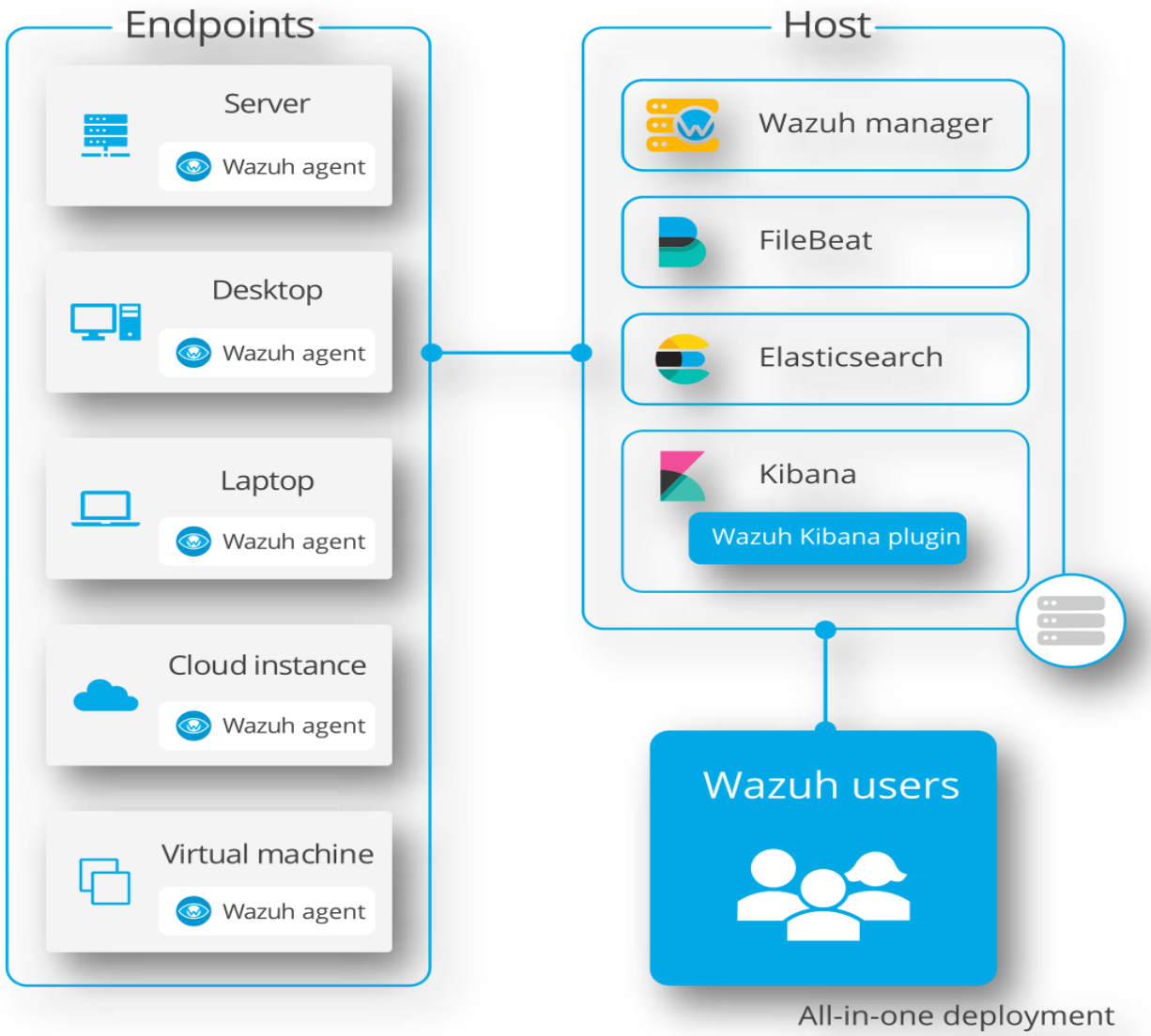


Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INSTALACIÓN: TODO EN UNO / DISTRIBUIDA

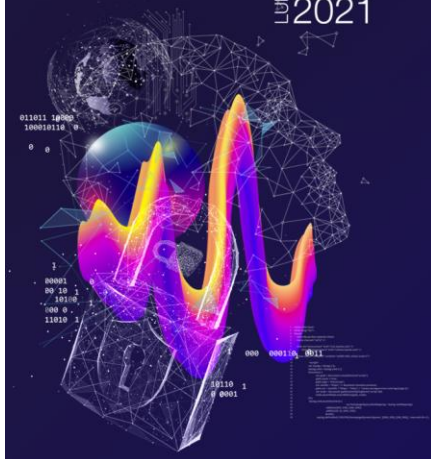
Todo en uno:



All-in-one deployment

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

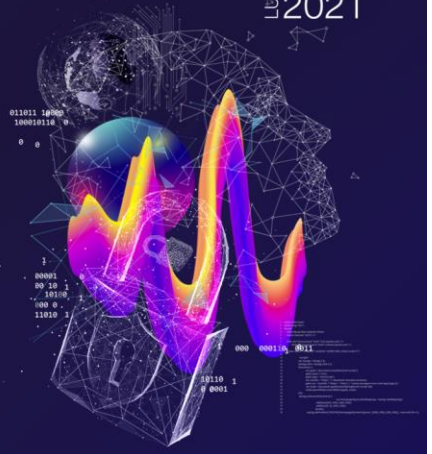


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: TODO EN UNO / DISTRIBUIDA

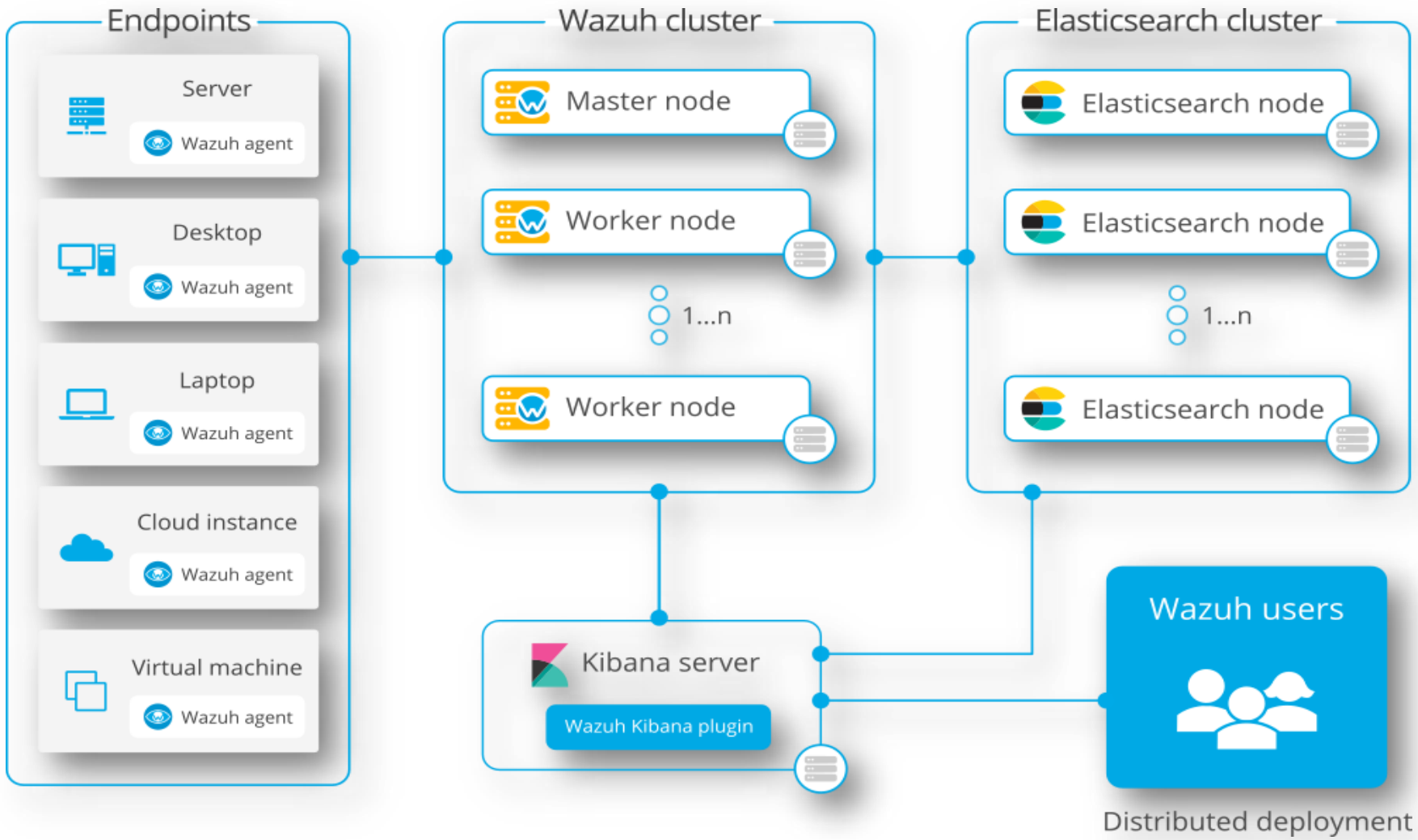
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Instalación Distribuida



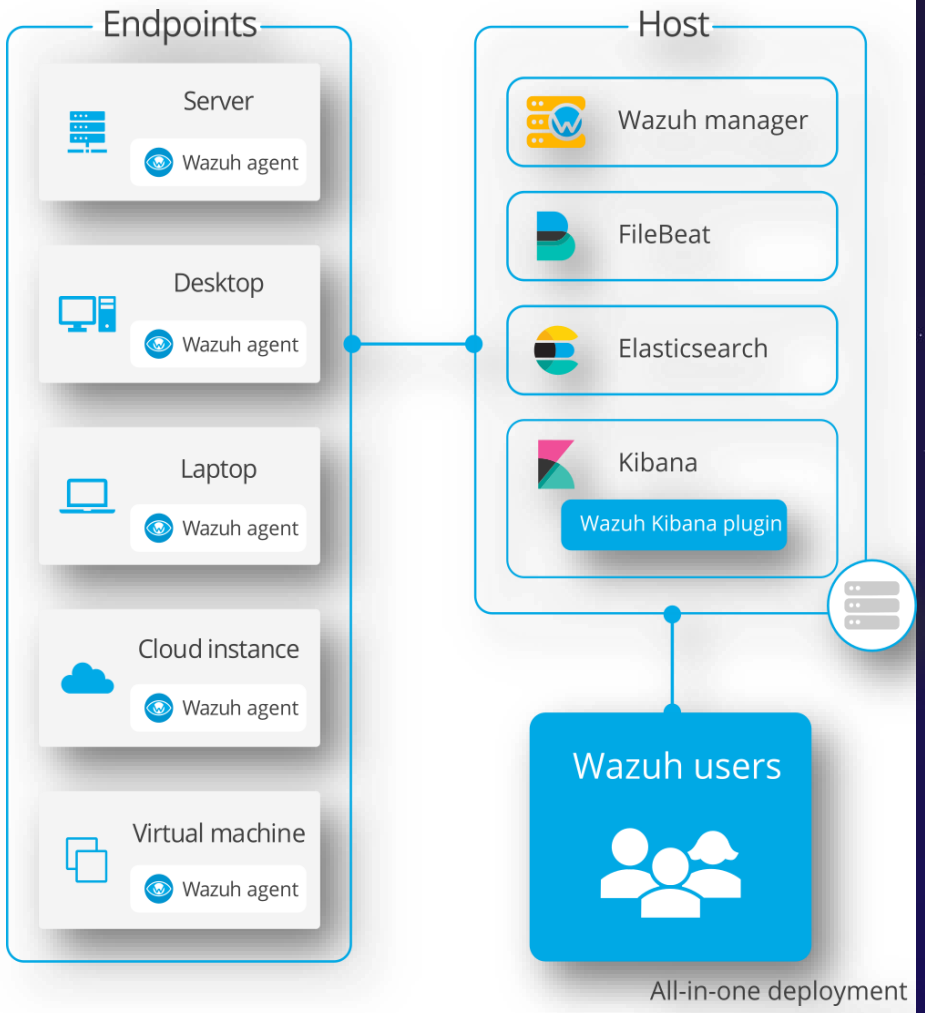
Distributed deployment

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

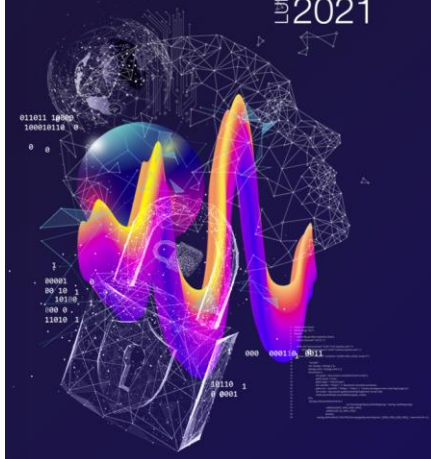
INSTALACIÓN: PROPUESTA TODO EN UNO PARA POC EN SUS INSTALACIONES

Todo en uno para avanzar en una PoC que permita obtener:

- Conocimiento de la herramienta.
- Verificación de los agentes con las diferentes plataformas institucionales.
- Instalación simple: **15-20 minutos (servidor)**
- Avanzar en aprendizaje de:
  - KQL.
  - Sintaxis de detectores.
  - Correlaciones comunes.
  - Configuración de alertas

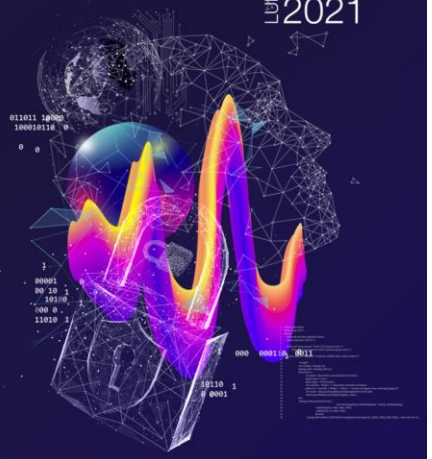


2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

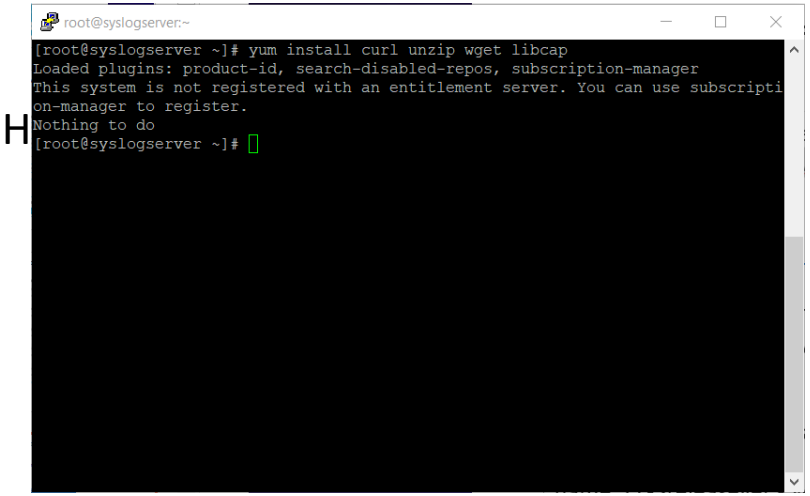
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Primero que todo accede a la consola del servidor destinado para la PoC cmo usuario "root".

Instale los paquetes necesarios para agregar el repositorio de wazuh:
yum install curl unzip wget libcap

Importe la clave GPG:
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH

Agregue el repositorio en sus definiciones locales:
cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF



Ministerio del Interior y Seguridad Pública

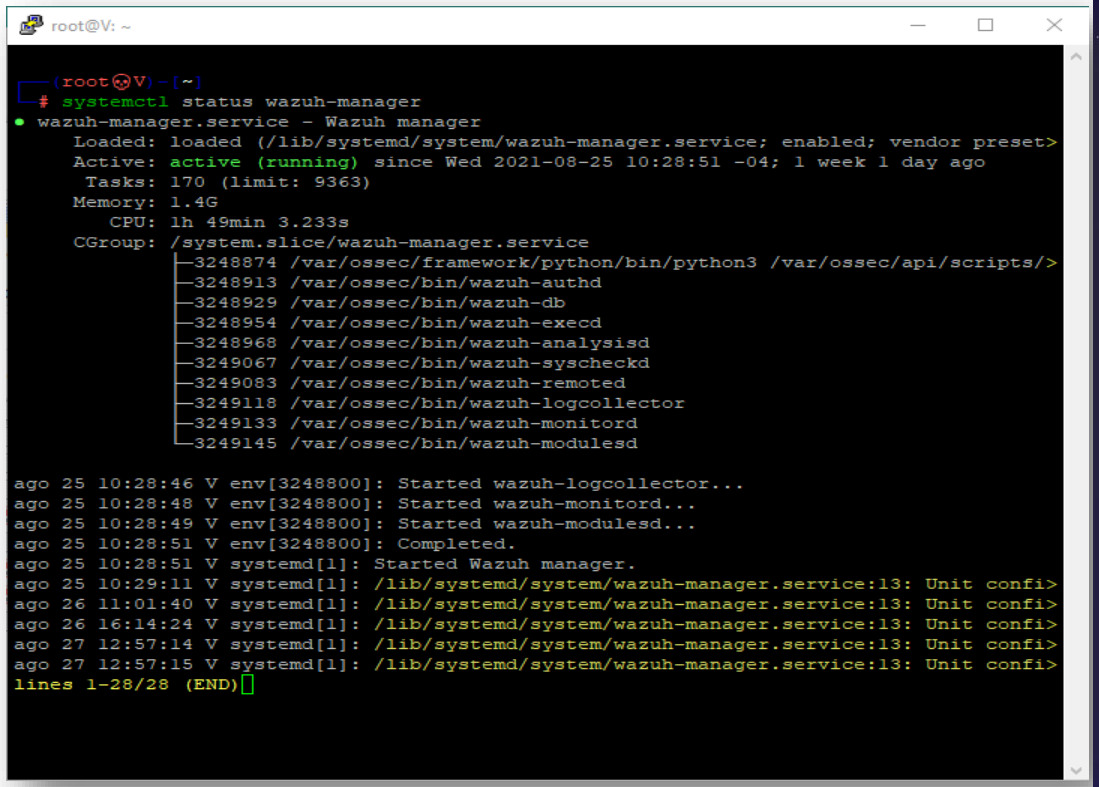
Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

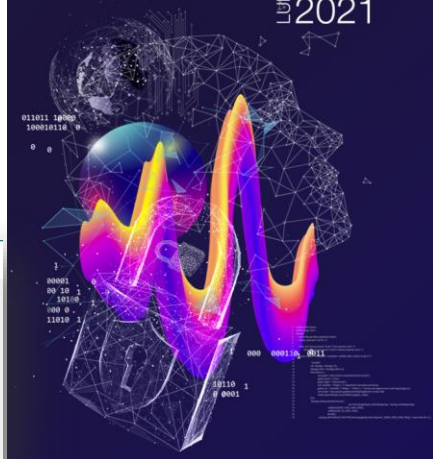
Instale el paquete del administrador de Wazuh:
yum install wazuh-manager

Habilite e inicie el servicio de administrador de Wazuh:
systemctl daemon-reload
systemctl enable wazuh-manager
systemctl start wazuh-manager

Ejecute el siguiente comando para verificar si el administrador de Wazuh está activo:
systemctl status wazuh-manager

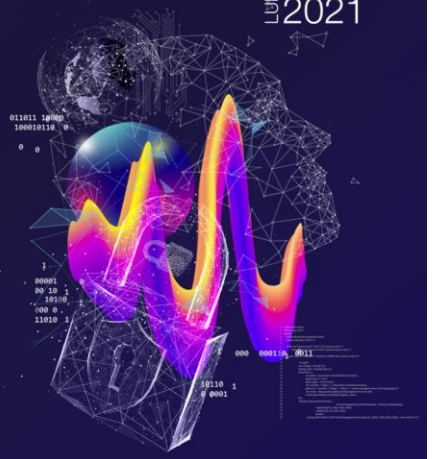


2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Instale Open Distro para Elasticsearch:
yum install opendistroforelasticsearch

Ejecute el siguiente comando para descargar el archivo de configuración /etc/elasticsearch/elasticsearch.yml:
curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/7.x/elasticsearch_all_in_one.yml

Necesita agregar usuarios y roles para usar Wazuh Kibana correctamente. Ejecute los siguientes comandos para agregar los usuarios de Wazuh y roles adicionales en Kibana:

curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles.yml
curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles_mapping.yml
curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/internal_users.yml

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Elimine los certificados de demostración:

rm /etc/elasticsearch/esnode-key.pem /etc/elasticsearch/esnode.pem /etc/elasticsearch/kirk-key.pem /etc/elasticsearch/kirk.pem /etc/elasticsearch/root-ca.pem -f

Genere e implemente los certificados:

curl -so ~/wazuh-cert-tool.sh https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/wazuh-cert-tool.sh

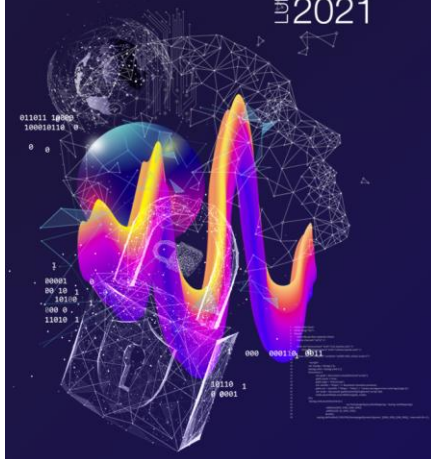
curl -so ~/instances.yml https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/instances_aio.yml

bash ~/wazuh-cert-tool.sh

mkdir /etc/elasticsearch/certs/
mv ~/certs/elasticsearch* /etc/elasticsearch/certs/
mv ~/certs/admin* /etc/elasticsearch/certs/
cp ~/certs/root-ca* /etc/elasticsearch/certs/

2do Seminario de Ciberseguridad para funcionarios públicos

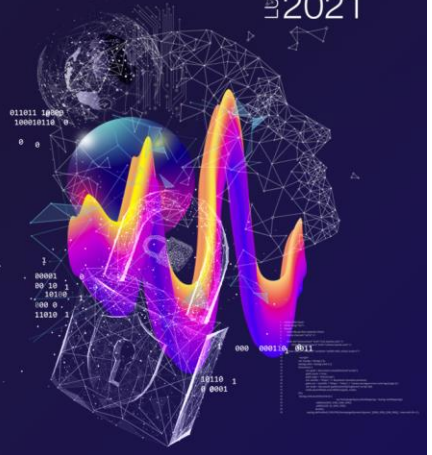
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



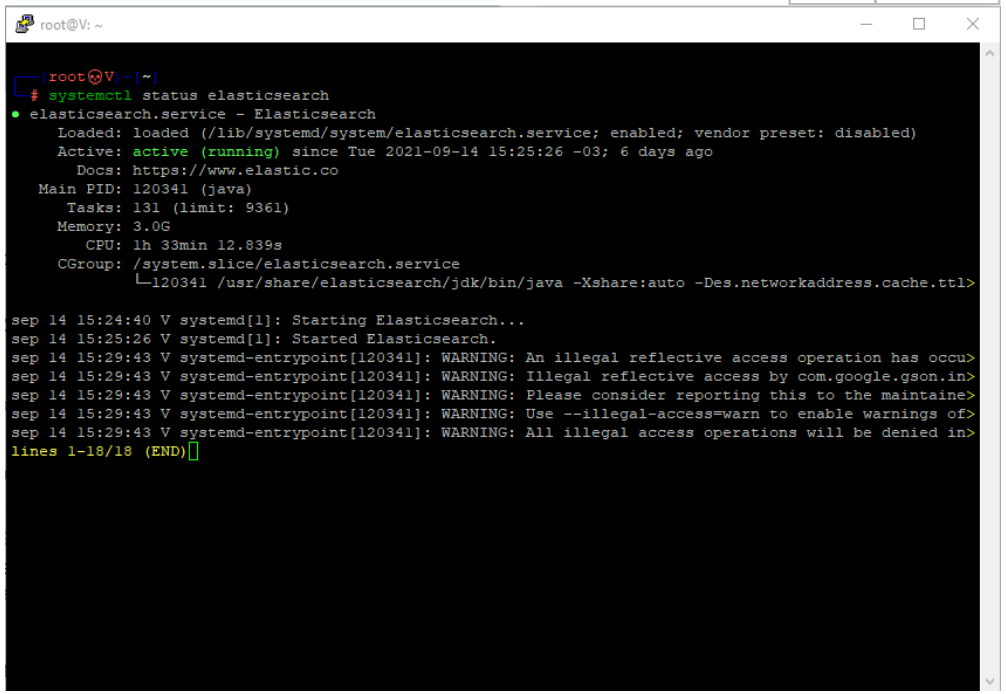
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Habilite e inicie el servicio Elasticsearch:
systemctl daemon-reload
systemctl enable elasticsearch
systemctl start elasticsearch

systemctl status elasticsearch
(verificar que haya partido sin errores)



Ejecute el securityadminscript Elasticsearch para cargar la información de los nuevos certificados e iniciar el clúster:
export JAVA_HOME=/usr/share/elasticsearch/jdk/ && /usr/share/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/ -nhnv -cacert /etc/elasticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key /etc/elasticsearch/certs/admin-key.pem

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

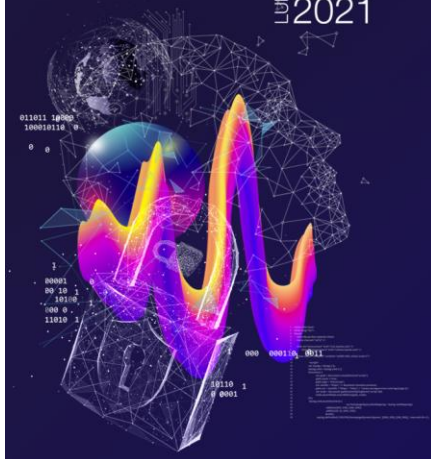
Verifique la instalación con el siguiente comando:
curl -XGET https://localhost:9200 -u admin:admin –k

Debiera observar un OUTPUT como el siguiente:


```
{
 "name" : "node-1",
 "cluster_name" : "elasticsearch",
 "cluster_uuid" : "tWYgqpgdRz6fGN8gH11flw",
 "version" : {
  "number" : "7.10.2",
  "build_flavor" : "oss",
  "build_type" : "rpm",
  "build_hash" : "747e1cc71def077253878a59143c1f785afa92b9",
  "build_date" : "2021-01-13T00:42:12.435326Z",
  "build_snapshot" : false,
  "lucene_version" : "8.7.0",
  "minimum_wire_compatibility_version" : "6.8.0",
  "minimum_index_compatibility_version" : "6.0.0-beta1"
 },
 "tagline" : "You Know, for Search"
}
```


2do Seminario de Ciberseguridad para funcionarios públicos

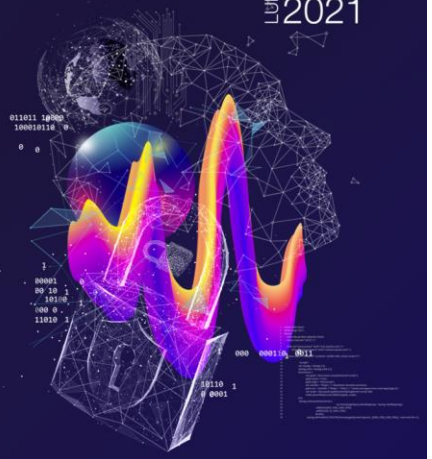
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Instale el paquete Filebeat:
yum install filebeat

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/resources/4.2/open-distro/filebeat/7.x/filebeat_all_in_one.yml

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.json
chmod go+r /etc/filebeat/wazuh-template.json

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.1.tar.gz | tar -xvz -C /usr/share/filebeat/module

mkdir /etc/filebeat/certs
cp ~/certs/root-ca.pem /etc/filebeat/certs/
mv ~/certs/filebeat* /etc/filebeat/certs/

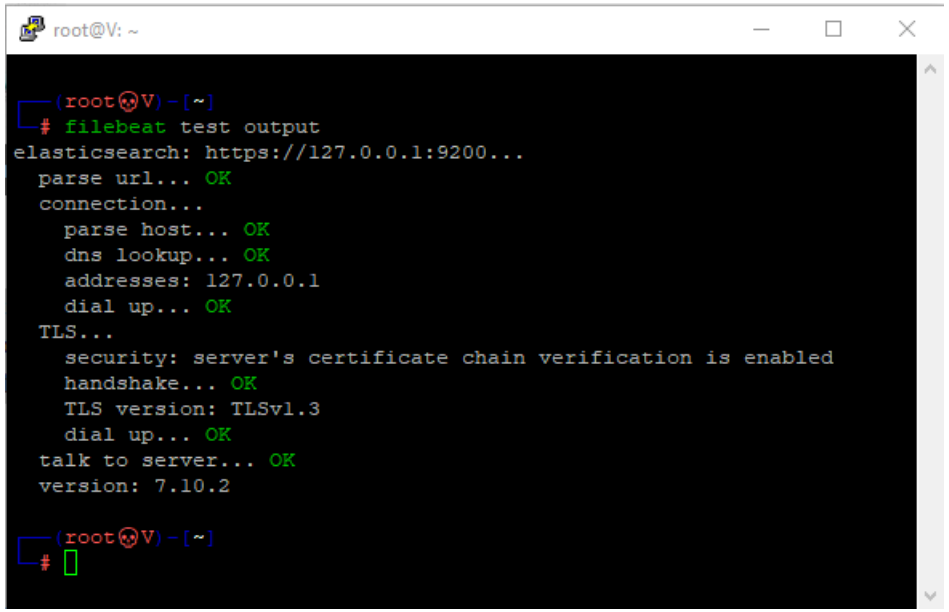
Nota: Filebeat es un cargador ligero para reenviar y centralizar datos de registro. Instalado como un agente en sus servidores, Filebeat monitorea los archivos de registro o las ubicaciones que usted especifica, recopila eventos de registro y los reenvía a Elasticsearch o Logstash para su indexación

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

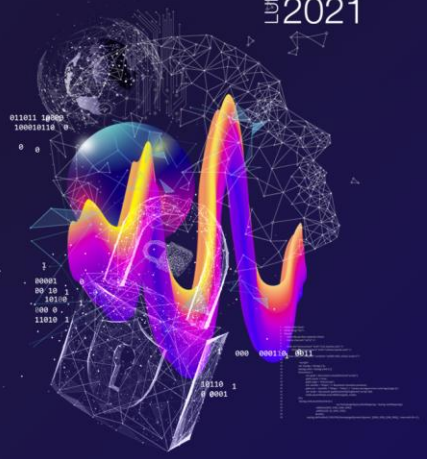
Asegúrese de que se instaló correctamente:
filebeat test output

Y observe un output como el siguiente:



elasticsearch: https://127.0.0.1:9200...
parse url... OK
connection...
parse host... OK
dns lookup... OK
addresses: 127.0.0.1
dial up... OK
TLS...
security: server's certificate chain verification is enabled
handshake... OK
TLS version: TLSv1.3
dial up... OK
talk to server... OK
version: 7.10.2

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Instale Kibana: es una interfaz de usuario gratuita y abierta que te permite visualizar los datos de Elasticsearch y navegar en el Elastic Stack.

```
# yum install opendistroforelasticsearch-kibana

# curl -so /etc/kibana/kibana.yml https://packages.wazuh.com/resources/4.2/open-distro/kibana/7.x/kibana_all_in_one.yml

# mkdir /usr/share/kibana/data
# chown -R kibana:kibana /usr/share/kibana/data

# cd /usr/share/kibana
# sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.2.0_7.10.2-1.zip

# setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node

# systemctl daemon-reload
# systemctl enable kibana
# systemctl start kibana
```

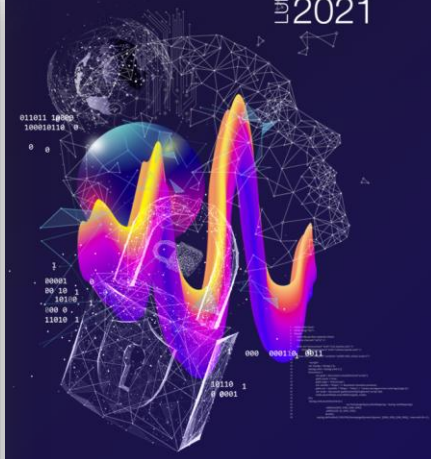
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

systemctl status kibana

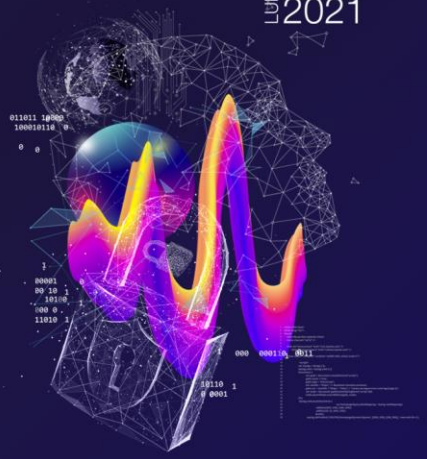
```
root@V: ~

┌──(root㉿V)-[~]
└─# systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: disab>
     Active: active (running) since Wed 2021-08-11 10:59:35 -04; 3 weeks 0 days ago
   Main PID: 212617 (node)
      Tasks: 11 (limit: 9363)
     Memory: 144.1M
        CPU: 47min 56.974s
     CGroup: /system.slice/kibana.service
             └─212617 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../>

sep 02 08:33:18 V kibana[212617]: {"type":"response","@timestamp":"2021-09-02T12:33:18>
sep 02 08:33:20 V kibana[212617]: {"type":"response","@timestamp":"2021-09-02T12:33:20>
sep 02 08:33:22 V kibana[212617]: {"type":"response","@timestamp":"2021-09-02T12:33:22>
sep 02 08:33:23 V kibana[212617]: {"type":"response","@timestamp":"2021-09-02T12:33:23>
sep 02 08:33:26 V kibana[212617]: {"type":"response","@timestamp":"2021-09-02T12:33:26>
sep 02 08:39:14 V kibana[212617]: {"type":"error","@timestamp":"2021-09-02T12:39:14Z",>
sep 02 09:45:03 V kibana[212617]: {"type":"error","@timestamp":"2021-09-02T13:45:03Z",>
sep 02 09:45:09 V kibana[212617]: {"type":"response","@timestamp":"2021-09-02T13:45:09>
sep 02 10:27:41 V kibana[212617]: {"type":"error","@timestamp":"2021-09-02T14:27:41Z",>
sep 02 10:31:15 V kibana[212617]: {"type":"error","@timestamp":"2021-09-02T14:31:15Z",>
lines 1-20/20 (END)
```

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021

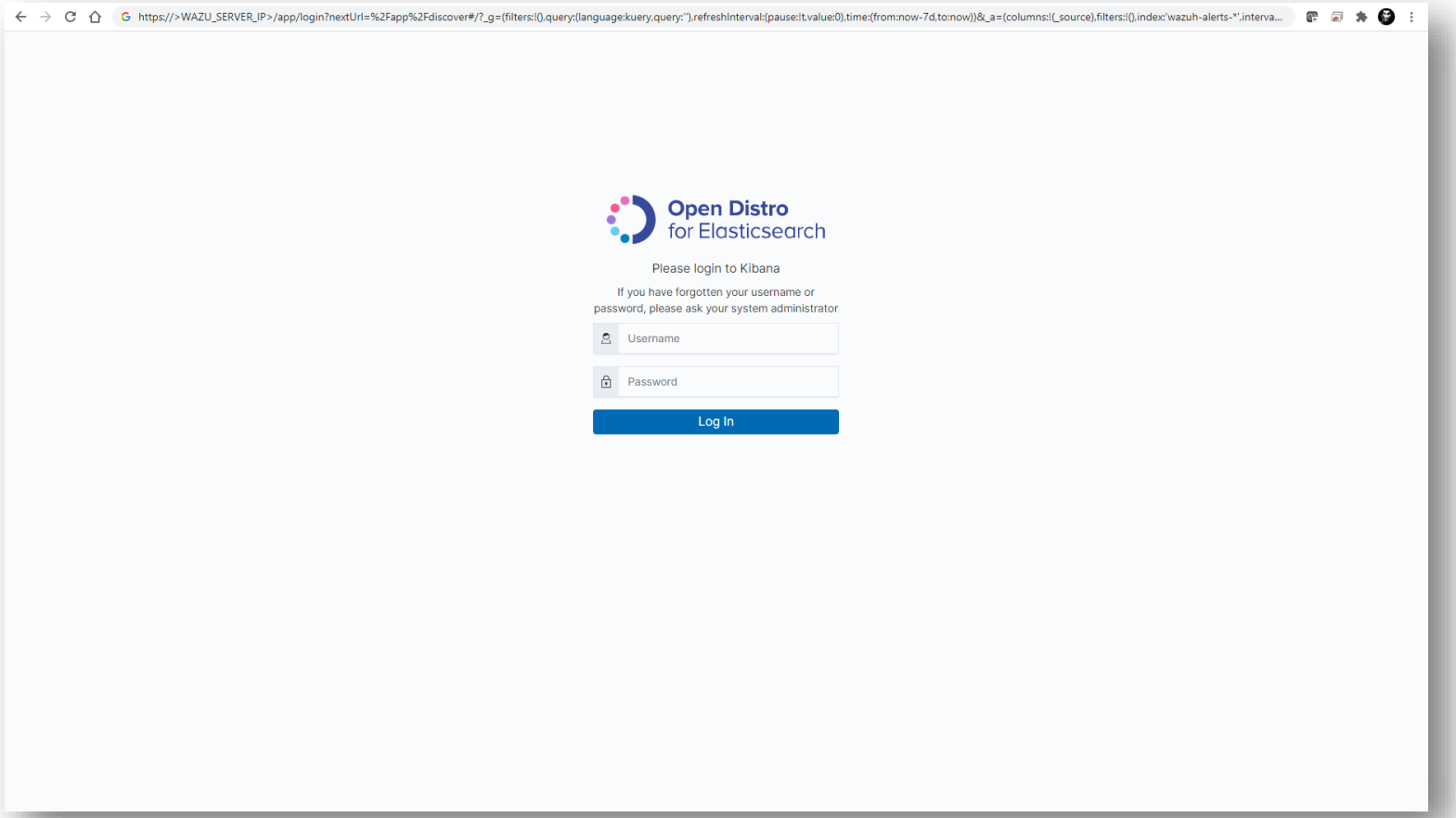


CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Acceda a la interfaz web:
URL: https://<wazuh_server_ip>
user: admin
password: *



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INSTALACIÓN: MODO DESATENDIDO (TIPO REDHAT)

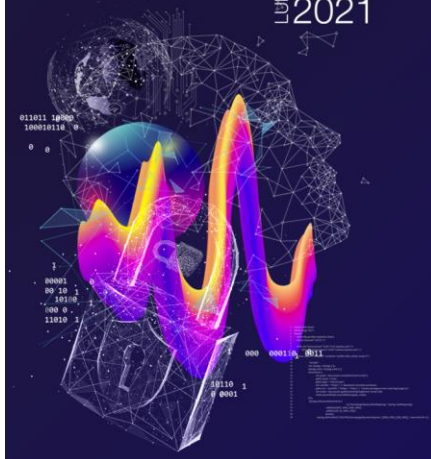
La PoC que desarrollamos para ejemplificar esta implementación usamos el modo desatendido de una instalación “todo en uno” y a continuación ilustramos la salida de la instalación en nuestro servidor:

curl -so ~/unattended-installation.sh https://packages.wazuh.com/resources/4.2/open-distro/unattended-installation/unattended-installation.sh && bash ~/unattended-installation.sh

Luego de 15 a 30 minutos dependiendo del hardware….queda instalado “Todo en Uno” y listo para empezar a gestionar tus LOGS de eventos e integrarle agentes.

2do Seminario de Ciberseguridad para funcionarios públicos

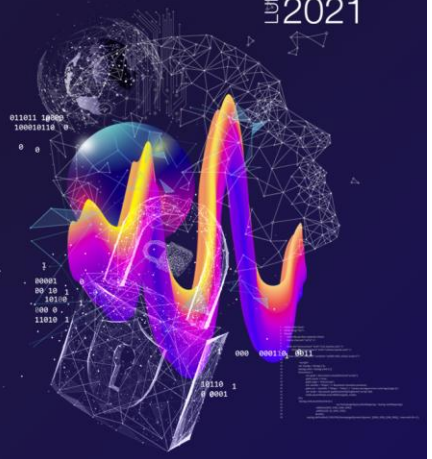
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: PASO POR PASO (TIPO REDHAT)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Starting the installation...
Installing all necessary utilities for the installation...
Done
Adding the Wazuh repository...
Done
Installing the Wazuh manager...
Done
Wazuh-manager started
Installing Open Distro for Elasticsearch...
Done
Configuring Elasticsearch...
Configuration file found. Creating certificates...
Creating the Elasticsearch certificates...
Creating Wazuh server certificates...
Creating Kibana certificate...
Certificates creation finished. They can be found in ~/certs.
Certificates created
Elasticsearch started
Initializing Elasticsearch...
Done
Installing Filebeat...
Filebeat started
Done
Installing Open Distro for Kibana...
Kibana started
Done
Generating random passwords
Done
Creating backup...

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INSTALACIÓN: MODO DESATENDIDO (TIPO REDHAT)

Backup created
Generating hashes
Hashes generated
Filebeat started
Kibana started
Loading changes...
Done

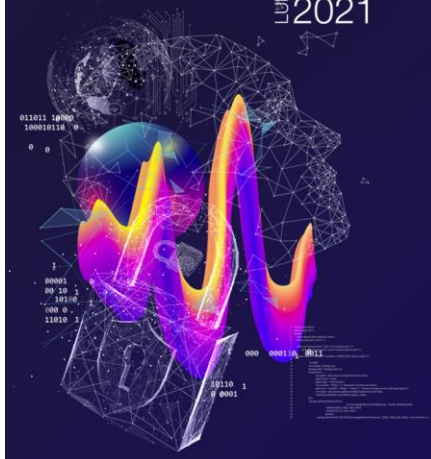
The password for wazuh is gi6bufRyojrxxDGck9f95EoJBki9axCHPl
The password for admin is Uk1HioqlNUhgX5mopOuiASjAZB7YojTMjO
The password for kibanaserver is mcy1Tv4Do-lYFd3Xp60MsNerjjdboDyU_p
The password for kibanaro is v2o2agrAoGEI6H9V-n73thgoL4GJCAHQzO
The password for logstash is nL5JoIM0KmtMczloSQoDXY1aSvrN_M1tPO
The password for readall is TcMKL_4pYaSAI0oQDe4NI99vnc3AoouLRV
The password for snapshotrestore is l3cAfoGrR7nLj3TB2qyhvuN3A3YL9ujyk
The password for wazuh_admin is v2zOY_NjjCPHAroYhi1BInqt3CW7okroGS
The password for wazuh_user is 1ihfWCOfoNroaYkUnxJ2oD_c6gvprmo8oSr1

Passwords changed. Remember to update the password in /etc/filebeat/filebeat.yml and /etc/kibana/kibana.yml if necessary and restart the services.

Checking the installation...
Elasticsearch installation succeeded.
Filebeat installation succeeded.
Initializing Kibana (this may take a while)
.
Installation finished

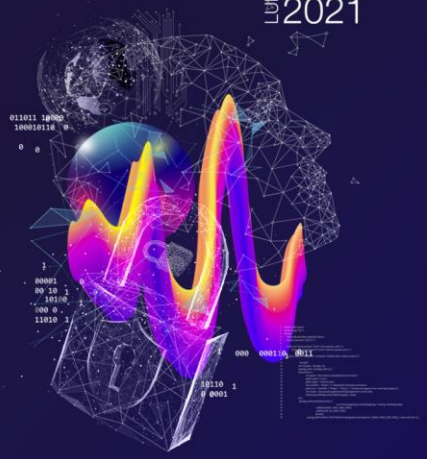
You can access the web interface https://<kibana_ip>.
The credentials are wazuh:Cgi6bufRyojrxxDGck9f95EoJBki9aoCHPl

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

INSTALACIÓN: AGENTE - PASO POR PASO (TIPO REDHAT)

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Importe la clave GPG:
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH

Agregue el repositorio:
cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF

Para implementar el agente de Wazuh en su sistema, seleccione su administrador de paquetes y edite la WAZUH_MANAGERvariable para que contenga la dirección IP o el nombre de host de su administrador de Wazuh.

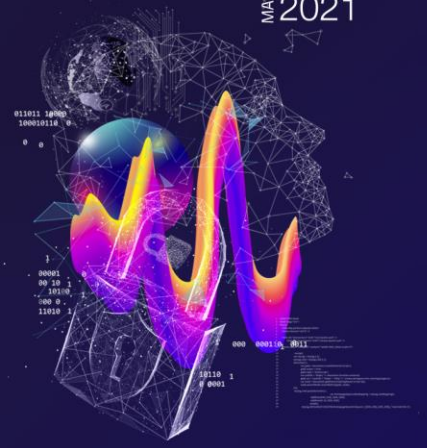
WAZUH_MANAGER="10.0.0.2" yum install wazuh-agent

Habilite e inicie el servicio de agente de Wazuh.

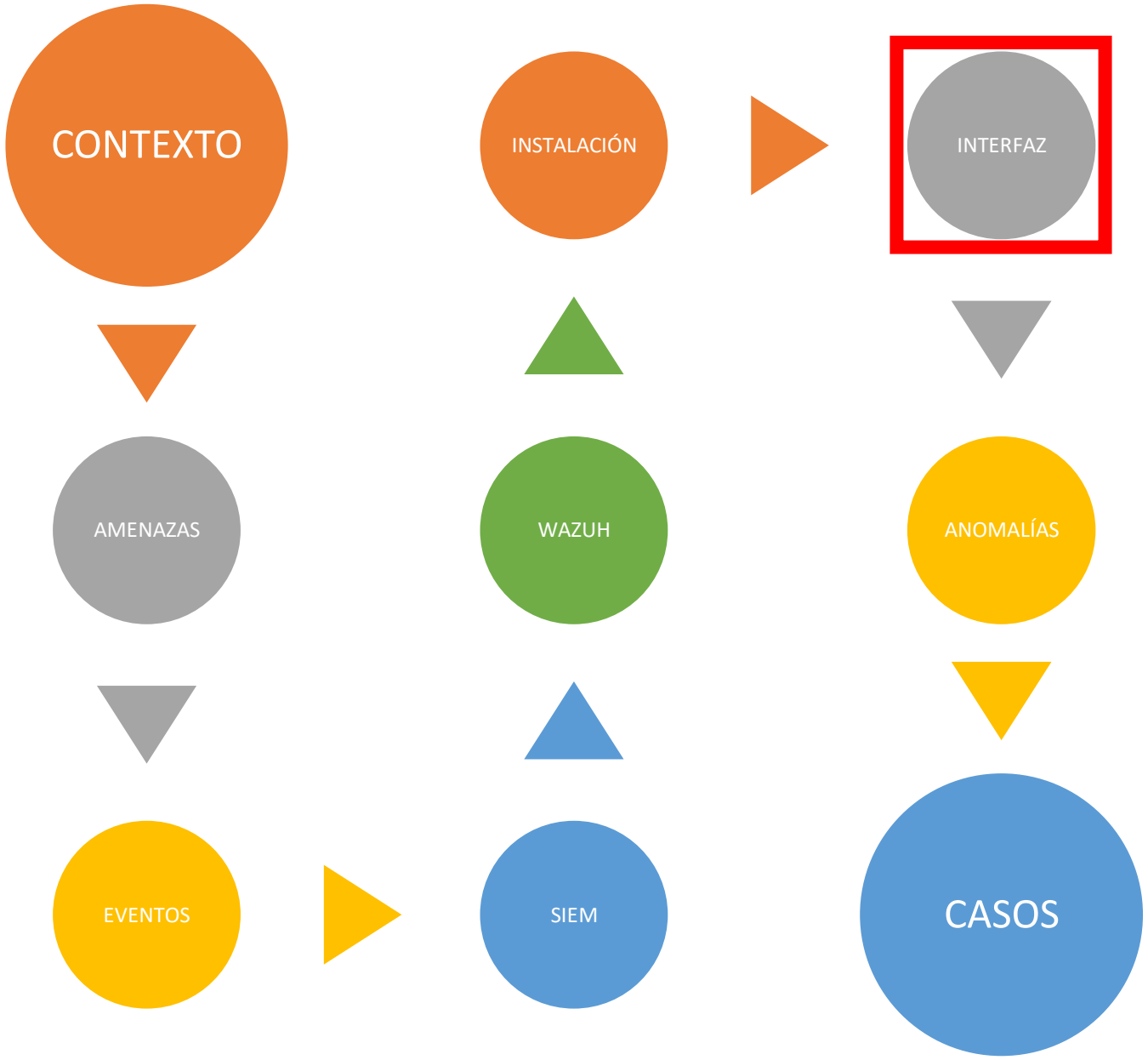
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Ministerio del Interior y Seguridad Pública

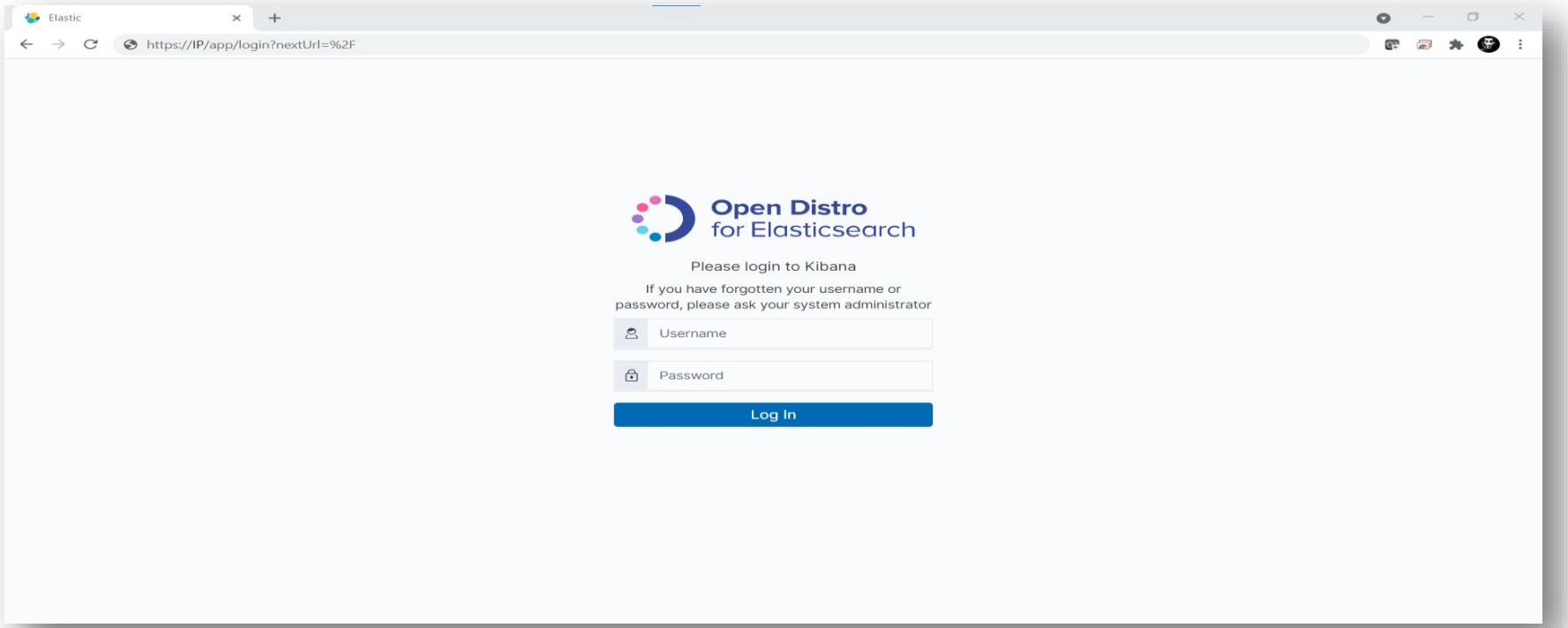
Gobierno de Chile

INTERFAZ: USANDO WAZUH

Puede acceder a la interfaz:

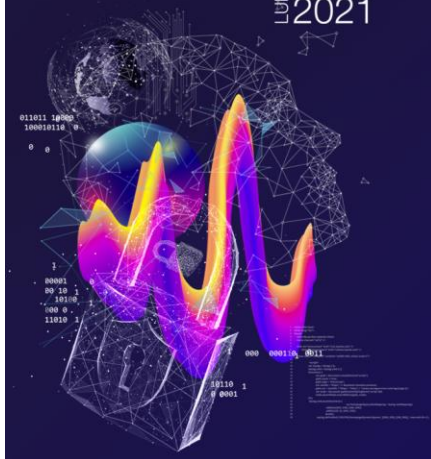
Acceda a la URL: https://<wazuh_server_ip> e ingrese las credenciales asociadas al usuario "wazuh".

- URL: https://<wazuh_server_ip>
- user: wazuh
- password: <wazuh_user_password>



2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

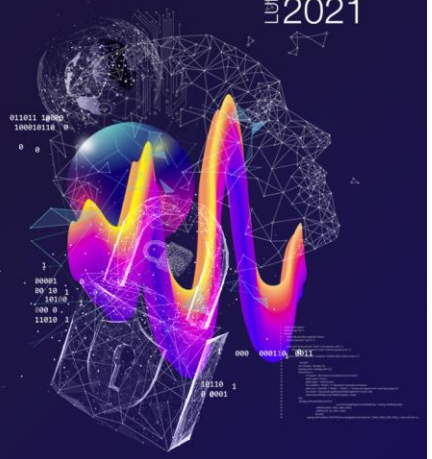


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

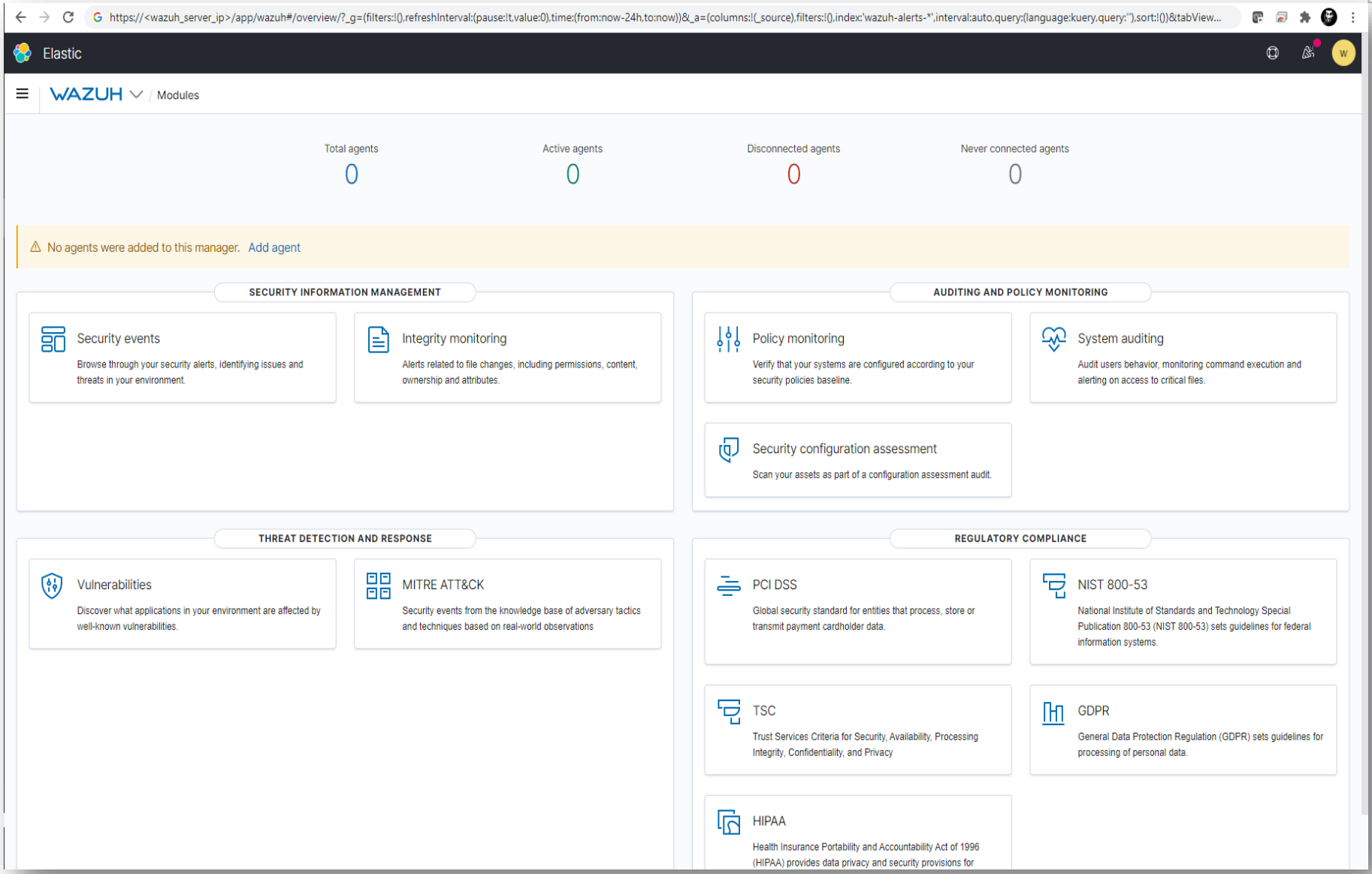
INTERFAZ: USANDO WAZUH

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

INTERFAZ: FUENTES DE INFORMACIÓN

Wazuh desde su instalación ya comienza a recopilar información del servir en el que se encuentra, pero la potencia está en poder ir incorporando agentes desplegados en diferentes puntos relevantes de la red interna o externa.

¿Cuáles son puntos relevantes?

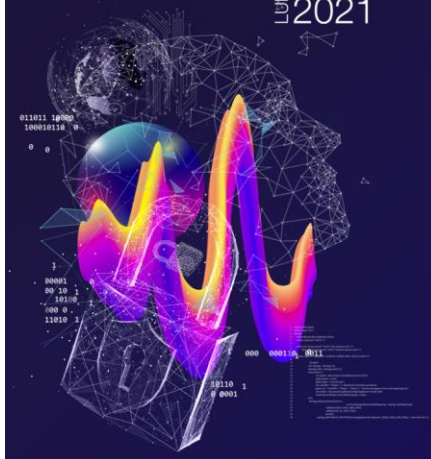
- Un firewall puede enviar información a wazuh mediante syslog
- Un IPS fuede enviar información a wazuh mediante syslog
- Un switch central puede enviar información a wazuh mediante syslog

Podemos instalar un agente en servidores estratégicos para que se reporten a wazuh, como por ejemplo:

- Nuestros DNS
- Nuestros Webserver
- Nuestros servidores de base de datos
- Nuestros servidores de correo
- Nuestros Active Directory

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

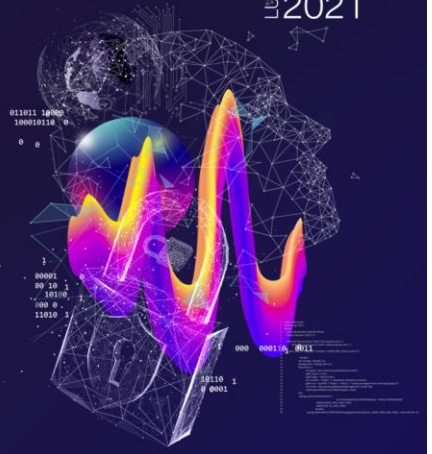


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

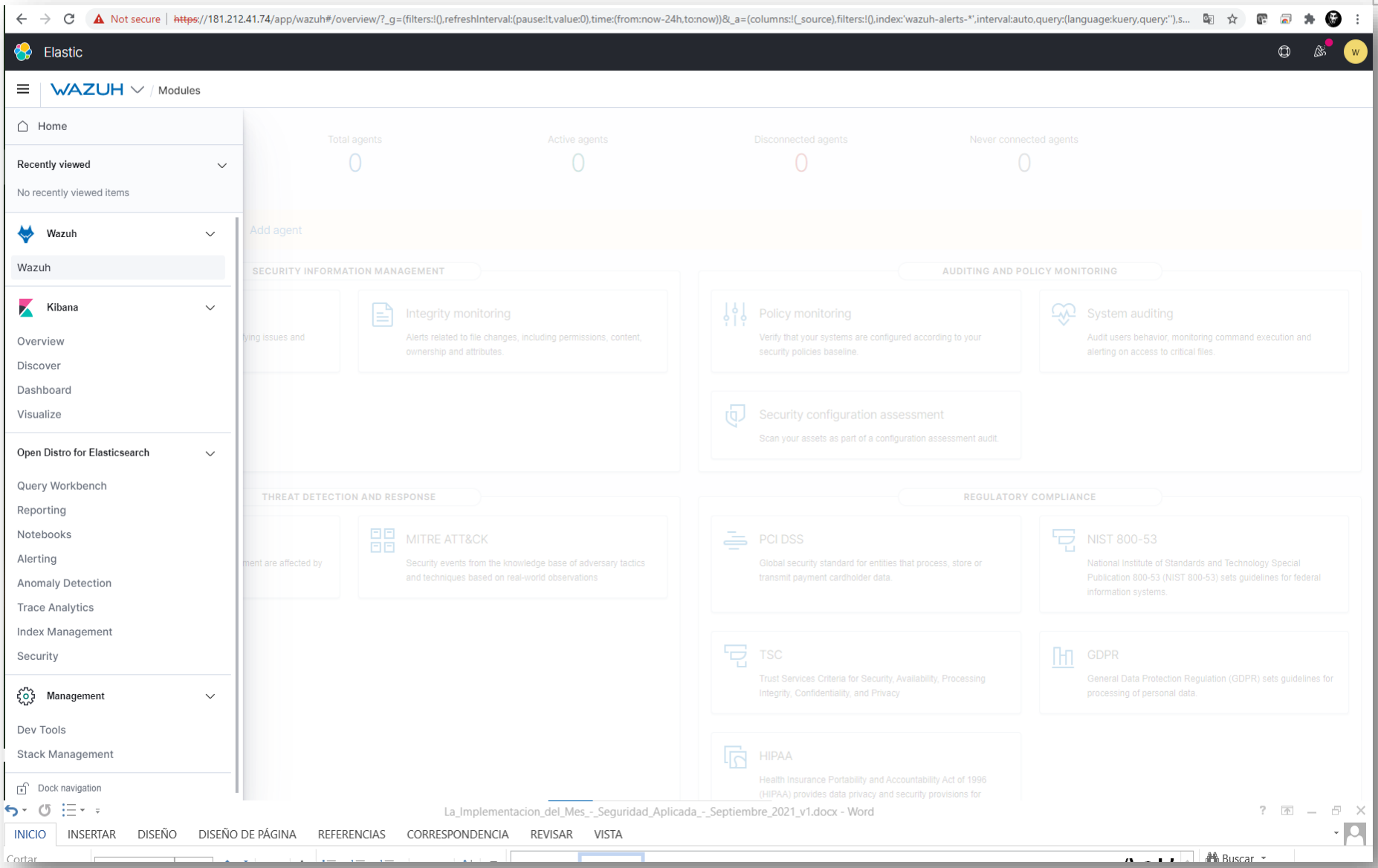
INTERFAZ: MENU LATERAL IZQUIERDO

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

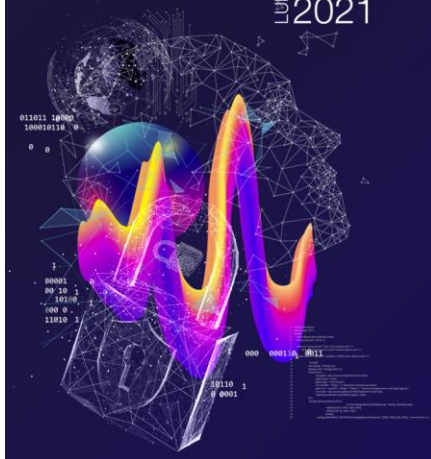
INTERFAZ:

Vía este menú se puede acceder directamente a:

- Administración de wazuh.
- Administración de kibana y sus diferentes dashboards y visualizaciones. [Overview, Discover, Dashboard, Visualize].
- Administración y análisis de elasticsearch. [Query Workbench, Reporting, Notebooks, Alerting, Anomaly Detection, Trace Analytics, Index Management, Security]
- Administración de herramientas de desarrollo y gestión de índices y otros temas operativos del sistema mismo. [Dev Tools, Stack Management]

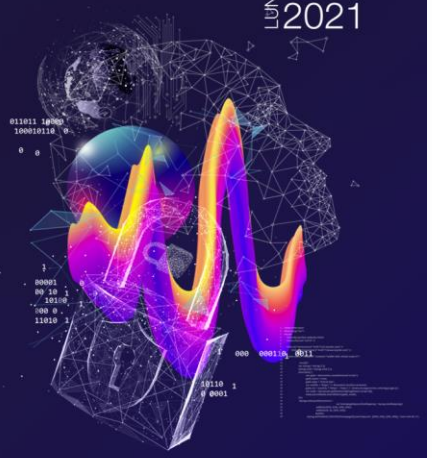
El módulo wazuh permite acceder a distintas vistas preconfiguradas con información sobre:

- Security information management
- Threat detection and response
- Auditing and policy monitoring
- Regulatory compliance



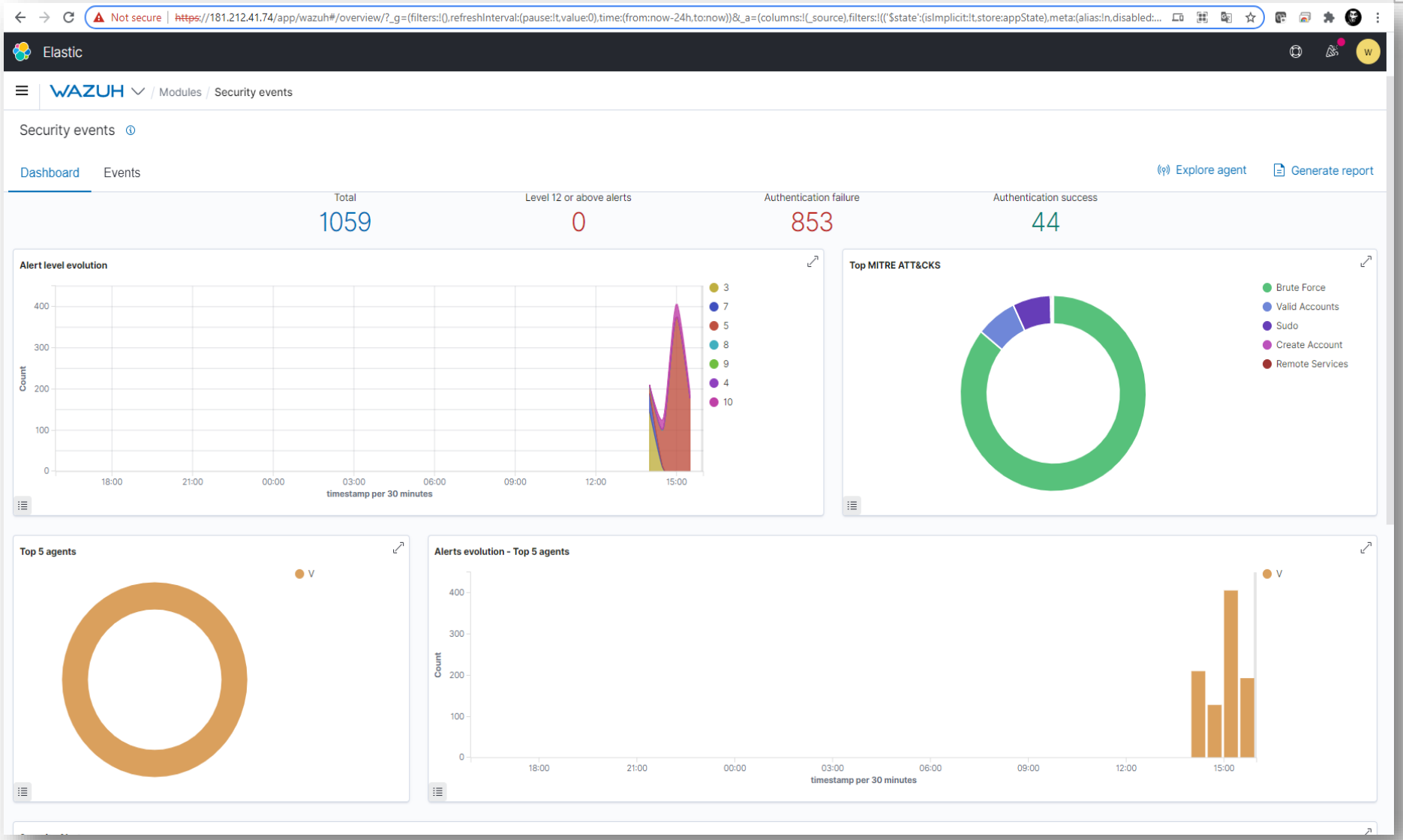
INTERFAZ – ALGUNAS VISTAS

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

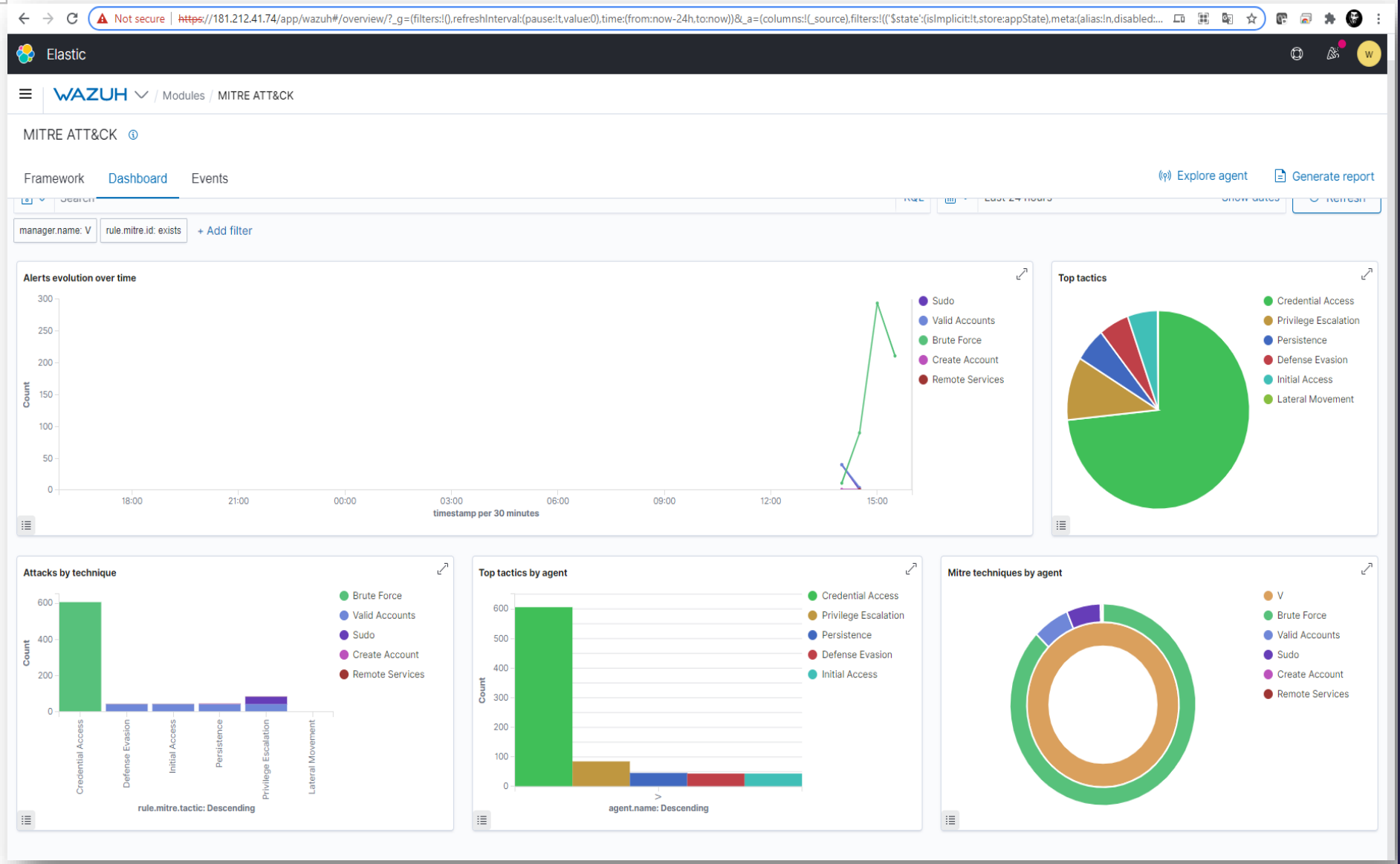
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Ministerio del Interior y Seguridad Pública

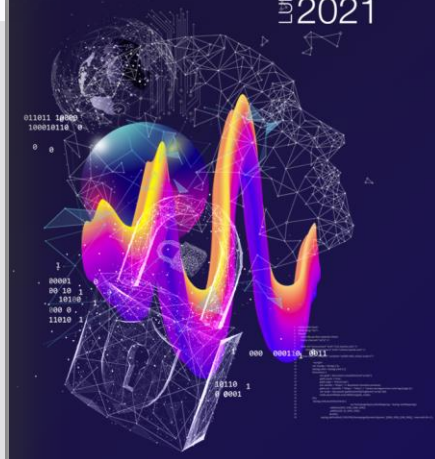
Gobierno de Chile

INTERFAZ: ALGUNAS VISTAS



2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

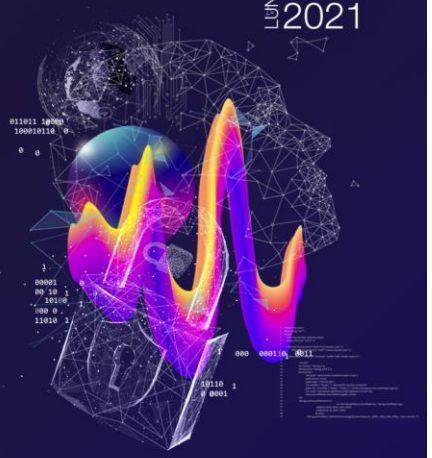


CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

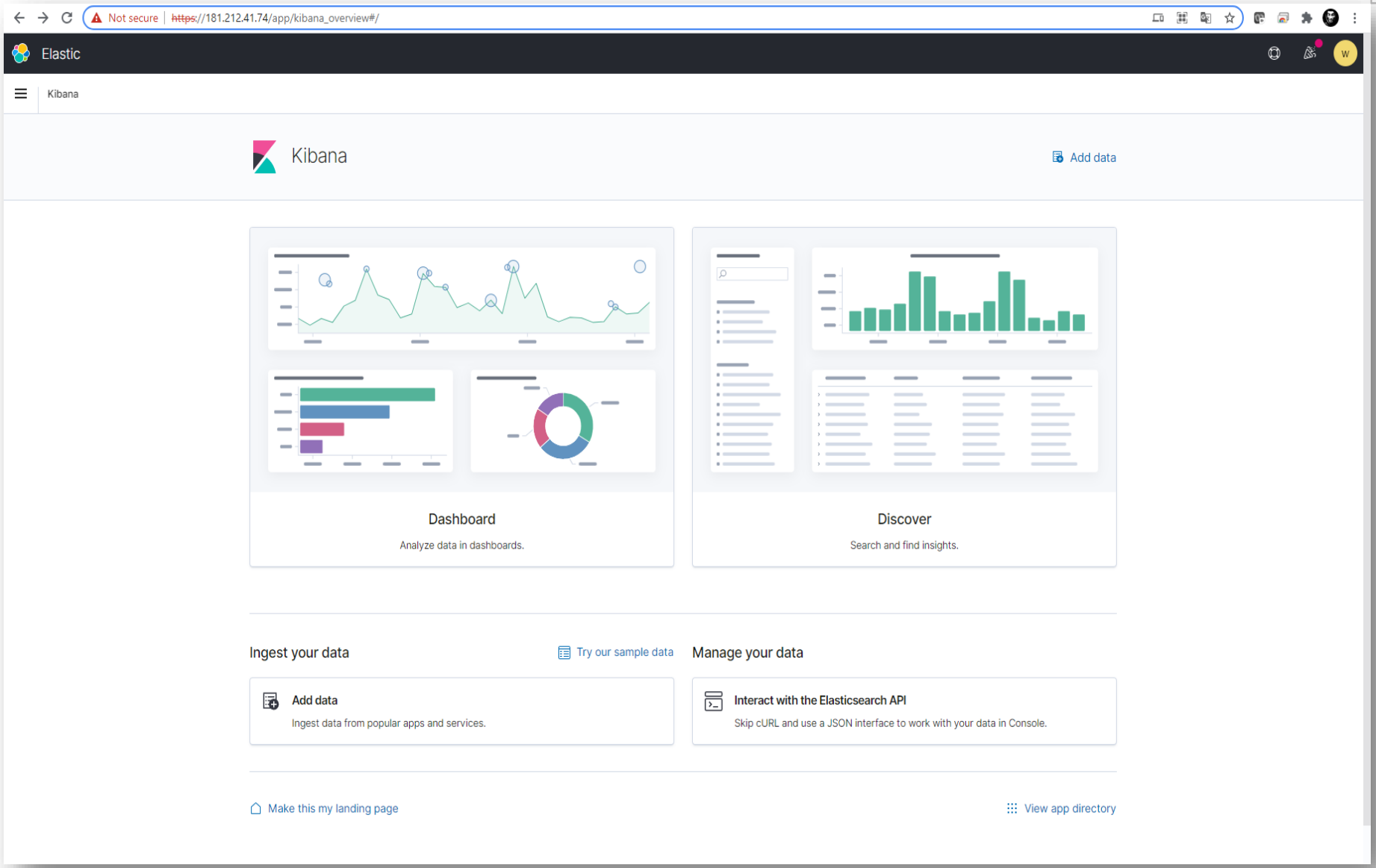
INTERFAZ – ALGUNAS VISTAS

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

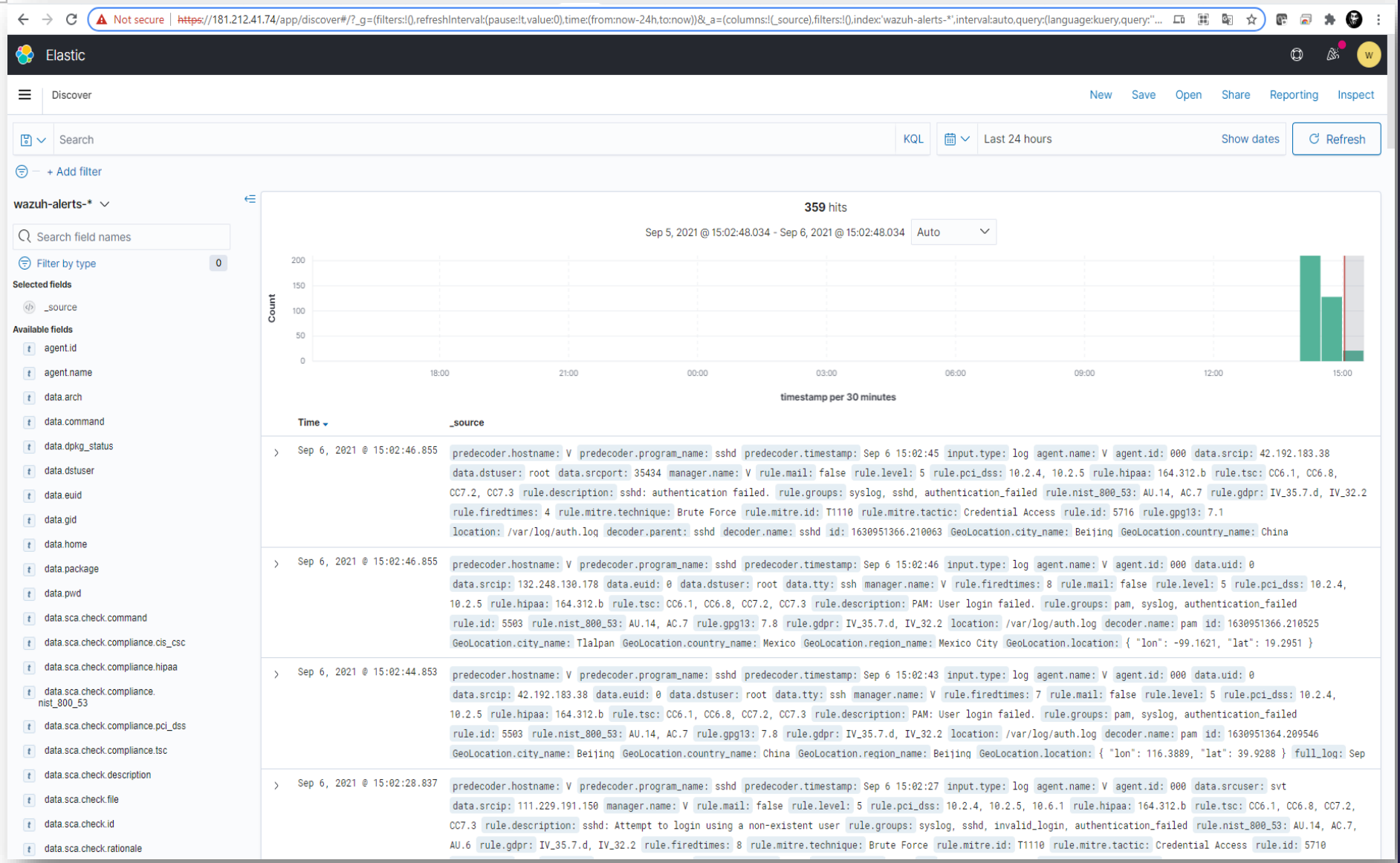
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Ministerio del Interior y Seguridad Pública

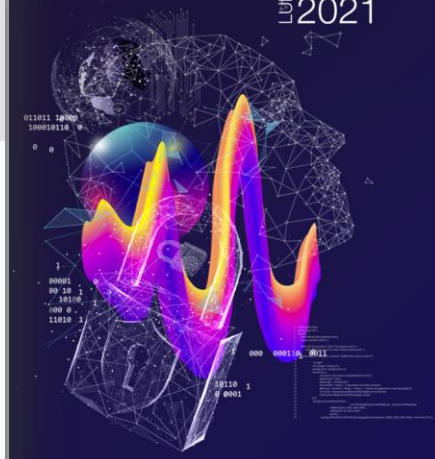
Gobierno de Chile

INTERFAZ: ALGUNAS VISTAS



2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021

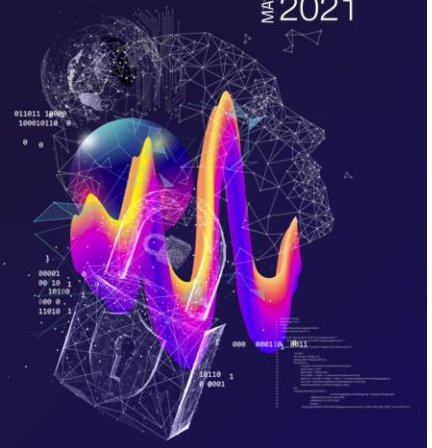


CSIRT

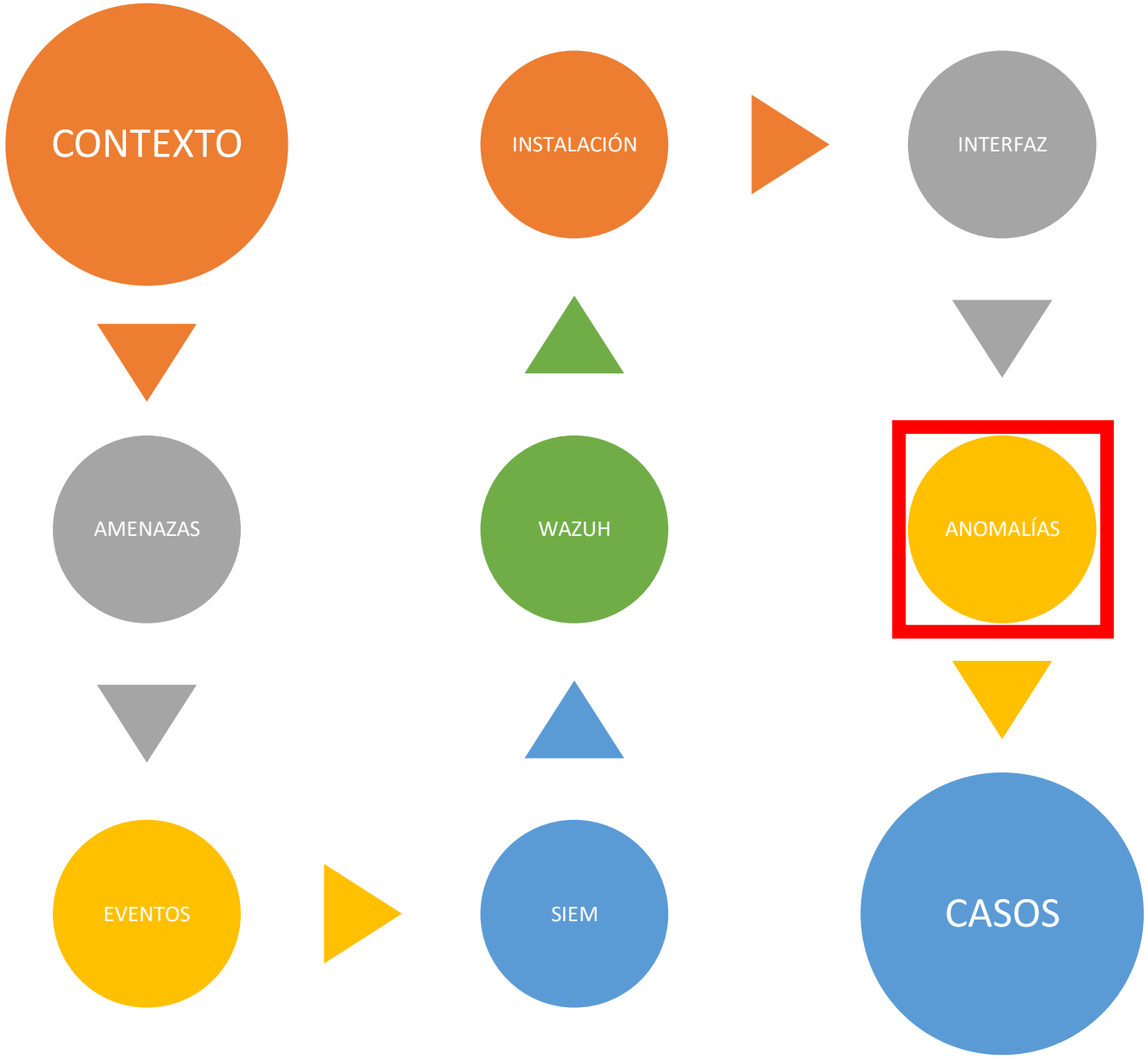
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA

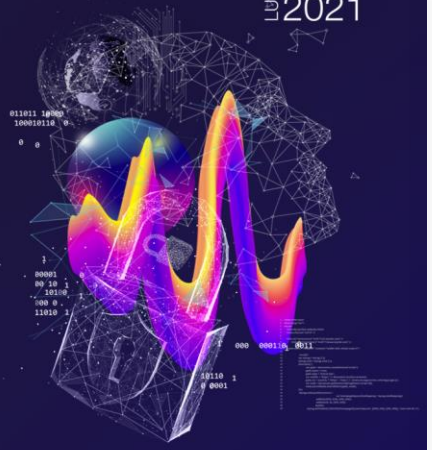


Ministerio del Interior y Seguridad Pública

Gobierno de Chile

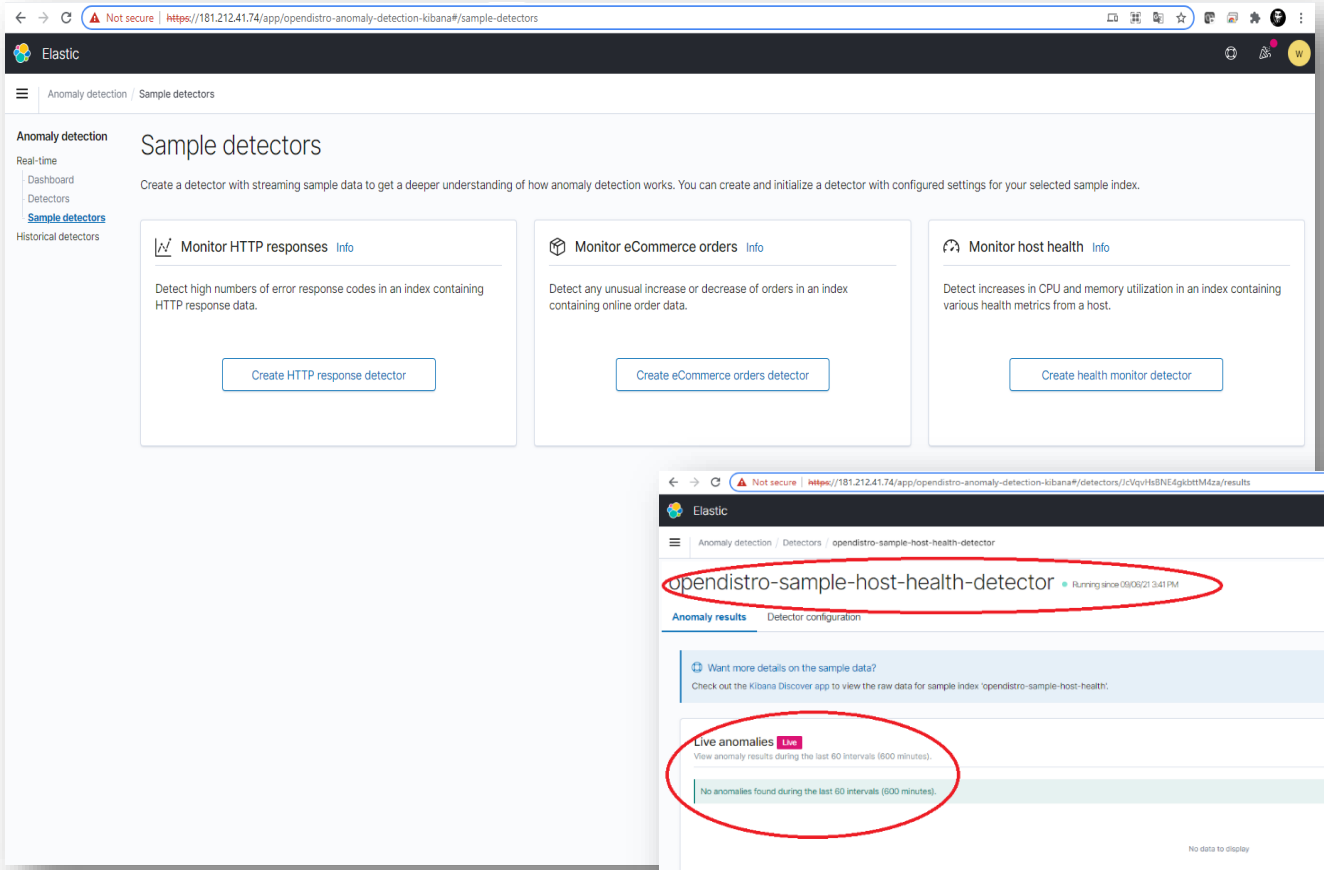
ANOMALÍAS – ALGUNAS VISTAS

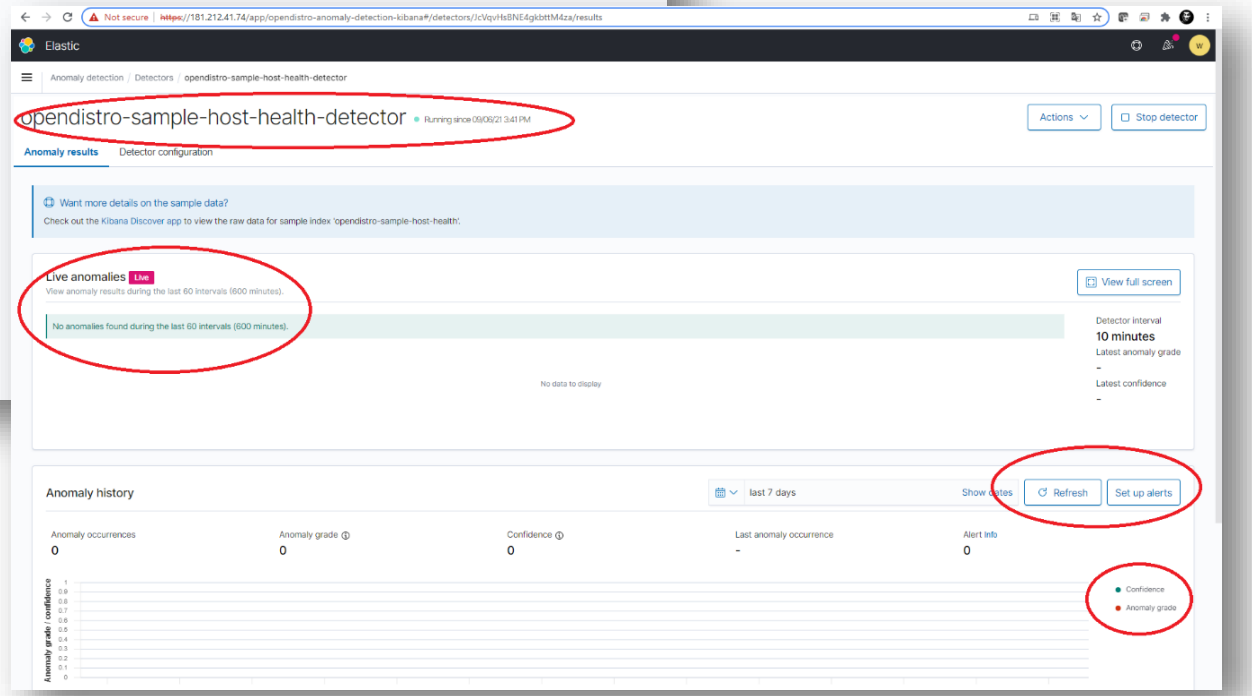
2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

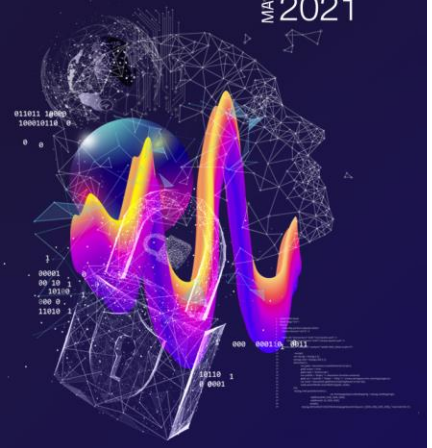
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



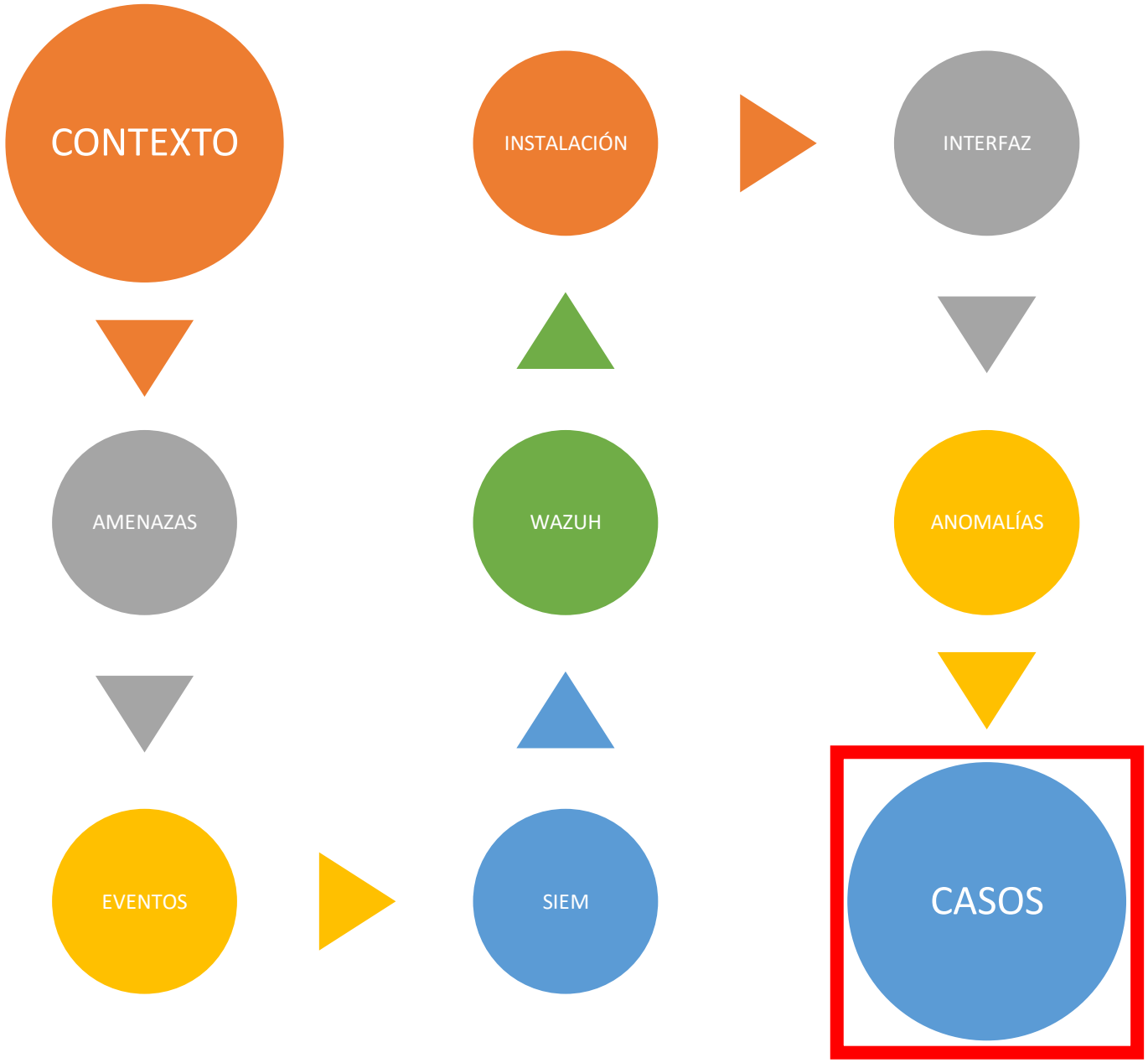


2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



AGENDA



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

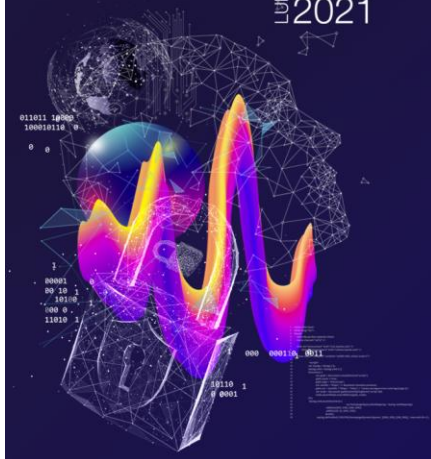
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

ALGUNOS CASOS DE USO: AWS

2do Seminario de Ciberseguridad para funcionarios públicos

LUNES 23/09 2021



Uso de Wazuh para monitorear AWS

Wazuh ayuda a aumentar la seguridad de una infraestructura de AWS de dos formas diferentes y complementarias:

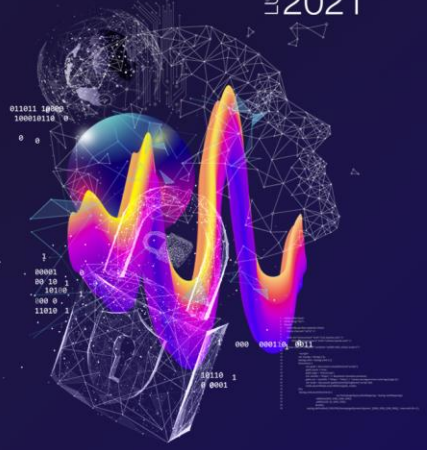
Instalar el agente de Wazuh en las instancias para monitorear la actividad dentro de ellas. Recopila diferentes tipos de datos de aplicaciones y sistemas y los reenvía al administrador de Wazuh. Se utilizan diferentes tareas o procesos del agente para monitorear el sistema de diferentes maneras (por ejemplo, monitoreando la integridad de los archivos, leyendo los mensajes de registro del sistema y escaneando las configuraciones del sistema).

Supervisión de los servicios de AWS para recopilar y analizar datos de registro sobre la infraestructura. Gracias al módulo para AWS, Wazuh puede activar alertas basadas en los eventos obtenidos de estos servicios, que brindan información rica y completa sobre la infraestructura, como la configuración de instancias, comportamiento no autorizado, datos almacenados en S3 y más.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

ALGUNOS CASOS DE USO: AWS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

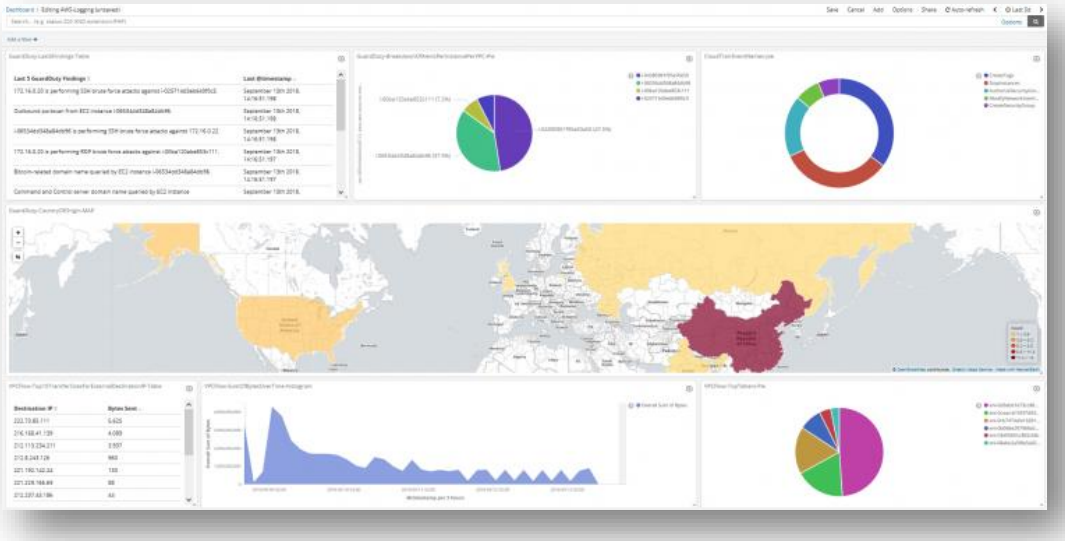
Supervisión de instancias de AWS

La instalación del agente de Wazuh en las instancias de AWS EC2 proporciona información y supervisión sobre lo que sucede dentro de ellas.

El agente se ejecuta como un servicio en la instancia y recopila diferentes tipos de datos de aplicaciones y sistemas que se reenvían al administrador de Wazuh a través de un canal encriptado y autenticado.

Gracias al agente de Wazuh, hay algunas capacidades disponibles para monitorear las instancias:

- Recolección de datos de registro
- Supervisión de la integridad de los archivos
- Detección de anomalías y malware
- Supervisión de la política de seguridad
- Inventario del sistema
- Detección de vulnerabilidades



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

ALGUNOS CASOS DE USO: AWS

Supervisión de servicios basados en AWS
El módulo Wazuh para AWS (aws-s3) proporciona capacidades para monitorear los servicios basados en AWS. Cada una de las secciones siguientes contiene instrucciones detalladas para configurar y configurar todos los servicios admitidos, y también la configuración necesaria de Wazuh para recopilar los registros.

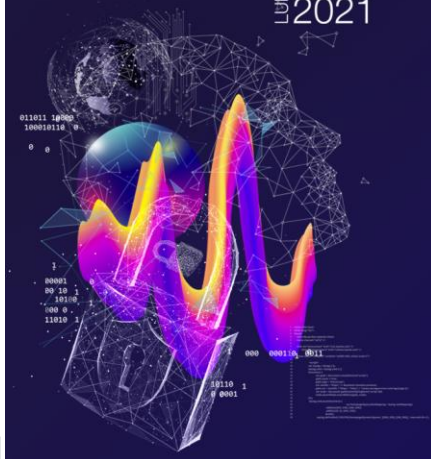
Este módulo requiere dependencias para funcionar, y también las credenciales adecuadas para acceder a los servicios. Eche un vistazo a la sección Requisitos previos antes de continuar.

Prerrequisitos: Este módulo requiere dependencias para funcionar, y también las credenciales adecuadas para acceder a los servicios.

Servicios soportados: CloudTrail, VPC, Config, etc. ->

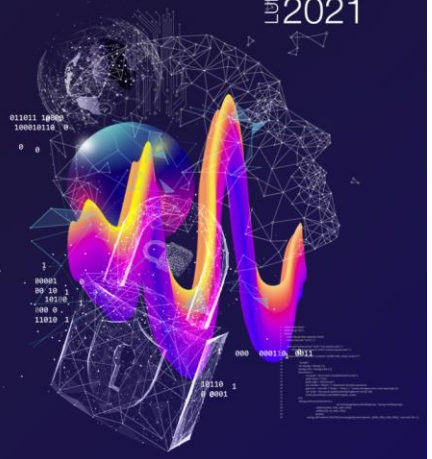
Provider	Service	Configuration tag	Type
Amazon	CloudTrail	bucket	cloudtrail
Amazon	VPC	bucket	vpcflow
Amazon	Config	bucket	config
Amazon	ALB	bucket	alb
Amazon	CLB	bucket	clb
Amazon	NLB	bucket	nlb
Amazon	KMS	bucket	custom
Amazon	Macie	bucket	custom
Amazon	Trusted Advisor	bucket	custom
Amazon	GuardDuty	bucket	guardduty
Amazon	WAF	bucket	waf
Amazon	Inspector	service	inspector
Amazon	CloudWatch Logs	service	cloudwatchlogs
Cisco	Umbrella	bucket	cisco_umbrella

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

ALGUNOS CASOS DE USO: AZURE

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Uso de Wazuh para monitorear Microsoft Azure

Permite monitorear toda la actividad que ocurre en la infraestructura, por ejemplo, cambios que ocurren en las máquinas virtuales, activación de alertas, información de datos de salud y datos de control.

Se debe instalar agentes de Wazuh para monitorear las máquinas virtuales que forman la infraestructura , las cuales enviarán eventos al gerente de Wazuh para su análisis con el fin de clasificar el evento con un rango de alertas que se pueden visualizar fácilmente.

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

ALGUNOS CASOS DE USO: AZURE

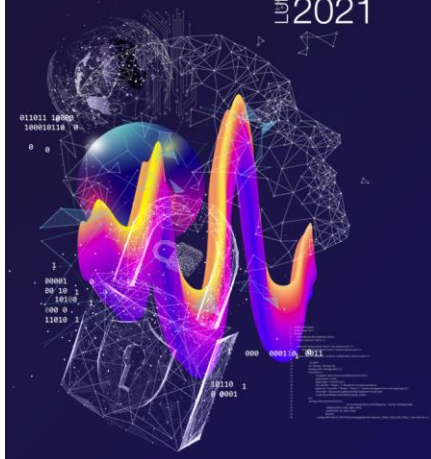
Permite monitorear servicios de la infraestructura como Azure Active Directory (AAD) .

Desde una perspectiva más amplia, los recursos de la infraestructura de Microsoft Azure se pueden dividir en dos tipos de registros, los registros de actividad y los registros de diagnóstico .

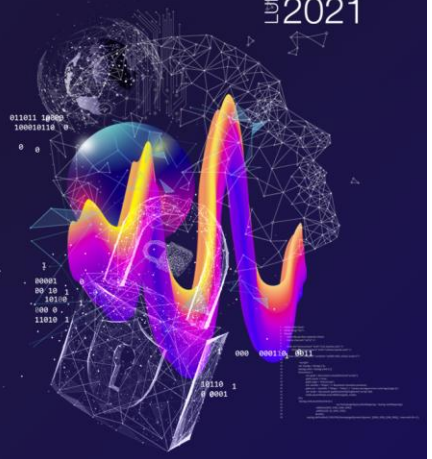
Las operaciones realizadas en un recurso fuera de la infraestructura se almacenan en los registros de actividad, proporcionando información sobre esas operaciones. Por otro lado, los datos referentes al funcionamiento de un recurso se almacenan en los registros de diagnóstico.

Wazuh tiene la capacidad de obtener y leer registros de Microsoft Azure a través de:

- Análisis de registros de Azure
- Gráfico de Azure Active Directory
- Almacenamiento de Azure



2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

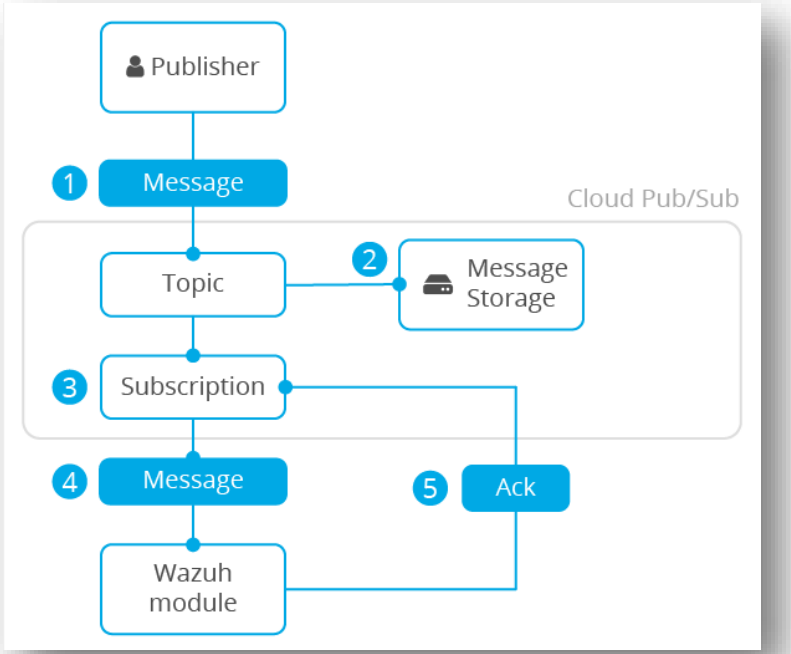
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

ALGUNOS CASOS DE USO: GOOGLE CLOUD PUB

Usar Wazuh para monitorear los servicios de GCP

Wazuh ayuda a aumentar la seguridad de una infraestructura de GCP mediante la recopilación y el análisis de datos de registro. Wazuh utiliza el servicio de transferencia y mensajería de Google Cloud Pub / Sub. Se usa ampliamente para sistemas controlados por eventos y análisis de transmisión. Permite enviar y recibir mensajes entre aplicaciones. El módulo Wazuh lo usa para obtener diferentes tipos de eventos (acceso a datos, actividad de administrador, eventos del sistema, consultas de DNS, etc.) de la infraestructura de Google Cloud. Una vez que se recopilan los eventos, Wazuh los procesa utilizando sus reglas de detección de amenazas .

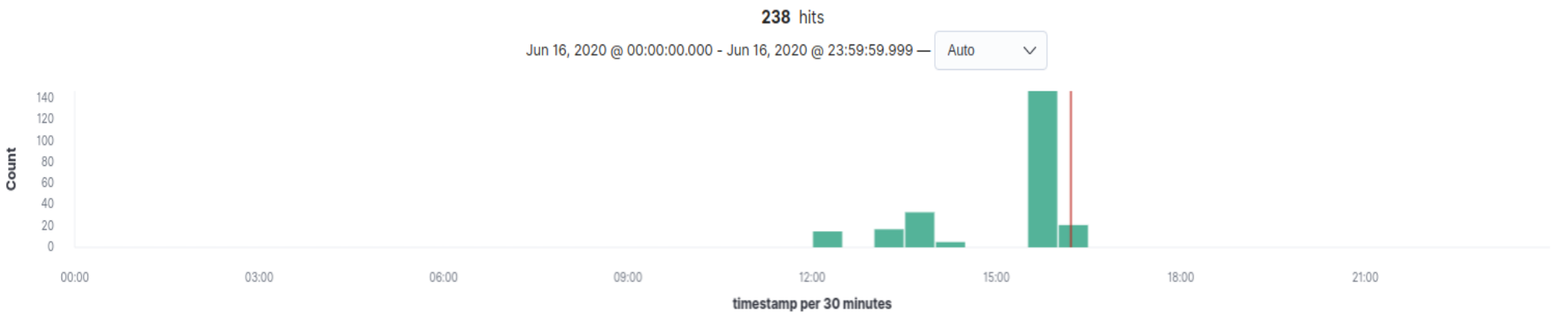
El módulo Wazuh para GCP (gcp-pubsub) proporciona la capacidad de monitorear servicios basados en GCP.



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

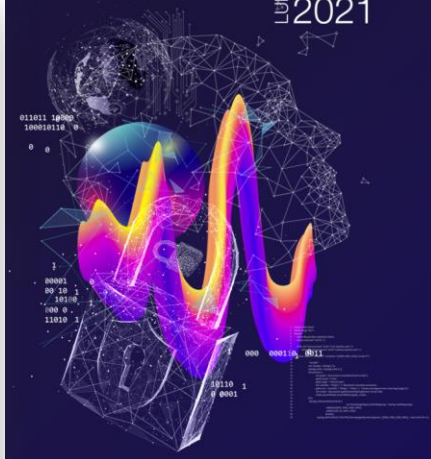
ALGUNOS CASOS DE USO: GOOGLE CLOUD PUB



Time	data.gcp.resource.labels.project_id	data.gcp.severity	data.gcp.protoPayload.request.@type	data.gcp.protoPayload.request.serviceNames	data.gcp.logName
Jun 16, 2020 @ 15:57:22.153	wazuh-dev-	INFO	type.googleapis.com/google.monitoring.v3.ListTimeSeriesRequest	-	projects/wazuh-dev- /logs/cloudaudit.googleapis.com%2Fdata_access
Jun 16, 2020 @ 15:57:22.098	wazuh-dev-	NOTICE	type.googleapis.com/google.api.servicemanagement.v1.ActivateServicesRequest	geolocation.googleapis.com	projects/wazuh-dev- /logs/cloudaudit.googleapis.com%2Factivity
Jun 16, 2020 @ 15:43:23.125	wazuh-dev-	NOTICE	type.googleapis.com/google.api.servicemanagement.v1.DeactivateServicesRequest	youtubeanalytics.googleapis.com	projects/wazuh-dev- /logs/cloudaudit.googleapis.com%2Factivity
Jun 16, 2020 @ 15:43:22.796	wazuh-dev-	INFO	type.googleapis.com/google.api.servicemanagement.v1.DeactivateServicesRequest	youtubeanalytics.googleapis.com	projects/wazuh-dev- /logs/cloudaudit.googleapis.com%2Fsystem_event
Jun 16, 2020 @ 15:42:52.917	wazuh-dev-	NOTICE	-	-	projects/wazuh-dev- /logs/cloudaudit.googleapis.com%2Factivity
Jun 16, 2020 @ 15:42:52.610	wazuh-dev-	INFO	type.googleapis.com/google.monitoring.v3.ListTimeSeriesRequest	-	projects/wazuh-dev- /logs/cloudaudit.googleapis.com%2Fdata_access

2do Seminario de Ciberseguridad para funcionarios públicos

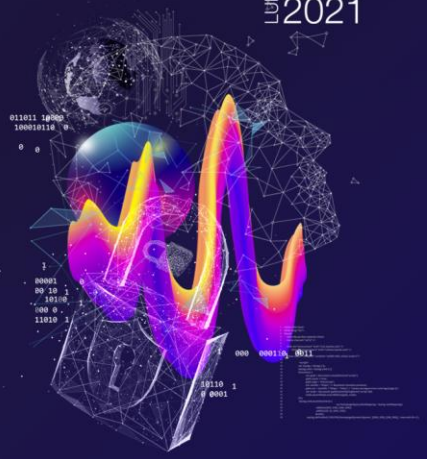
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

ALGUNOS CASOS DE USO: DETECCIÓN DE VULNERABILIDADES WINDOWS

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Configuración del detector de vulnerabilidades

El detector de vulnerabilidades funciona del lado del administrador porque almacena el inventario de los agentes conectados. Veamos cómo podemos hacer que funcione. El archivo /var/ossec/etc/ossec.conf contiene la siguiente sección:

```
<vulnerability-detector>
 <enabled>no</enabled>
 <interval>5m</interval>
 <ignore_time>6h</ignore_time>
 <run_on_start>yes</run_on_start>
 …
 <provider name="nvd">
  <enabled>no</enabled>
  <update_from_year>2010</update_from_year>
  <update_interval>1h</update_interval>
 </provider>
</vulnerability-detector>
```

Cambiar a
<enabled>yes</enabled>

Nota: NVD = https://nvd.nist.gov/

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

ALGUNOS CASOS DE USO: DETECCIÓN DE VULNERABILIDADES WINDOWS

WAZUH

Overview | Management | Agents | >_ Dev tools

wazuh

Agents / windows2012 (001) / Vulnerabilities • Active

Discover

Vulnerabilities

Search KQL | Last 24 hours | Show dates | Refresh

manager.name: wazuh | rule.groups: vulnerability-detector | agent.id: 001 | + Add filter

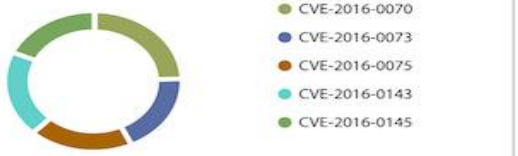
Critical severity alerts	High severity alerts	Medium severity alerts	Low severity alerts
13	350	284	11

Alerts severity

Most common rules

Rule ID	Description	Count
23504	A denial of service vulnerability exists when Windows improperty handles objects in memory, aka ``Windows Denial of Service Vulnerability``.	2
23505	A remote code execution vulnerability exists in "Microsoft COM for Windows" when it fails to properly handle serialized objects, aka "Microsoft COM for Windows Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2

Most common CVEs

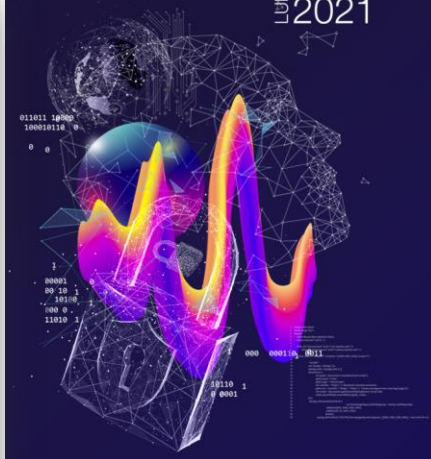


Severity distribution

Commmonly affected packages

2do Seminario de Ciberseguridad para funcionarios públicos

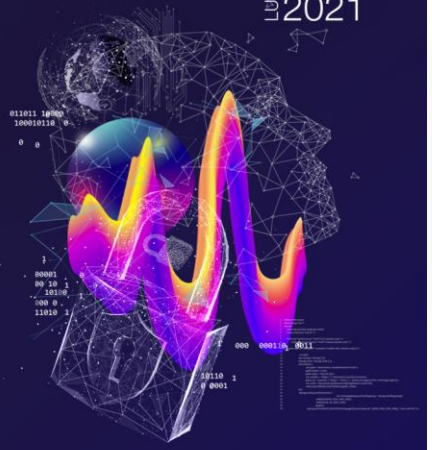
LUNES 23/09 2021



CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2do Seminario de Ciberseguridad para funcionarios públicos
LUNES 23/09 2021



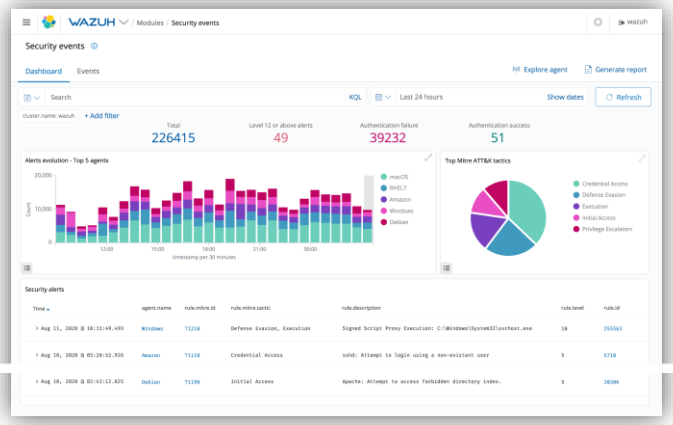
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

NO IMPRIMAN ESTE PPT, SOLO RECUERDEN ESTE COMANDO

WAZUH

Security Analytics | Intrusion Detection | Log Data Analysis | File Integrity Monitoring | Vulnerability Detection | Configuration Assessment | Incident Response | Regulatory Compliance | Cloud Security | Containers Security



curl -so ~/unattended-installation.sh https://packages.wazuh.com/resources/4.2/open-distro/unattended-installation/unattended-installation.sh && bash ~/unattended-installation.sh

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

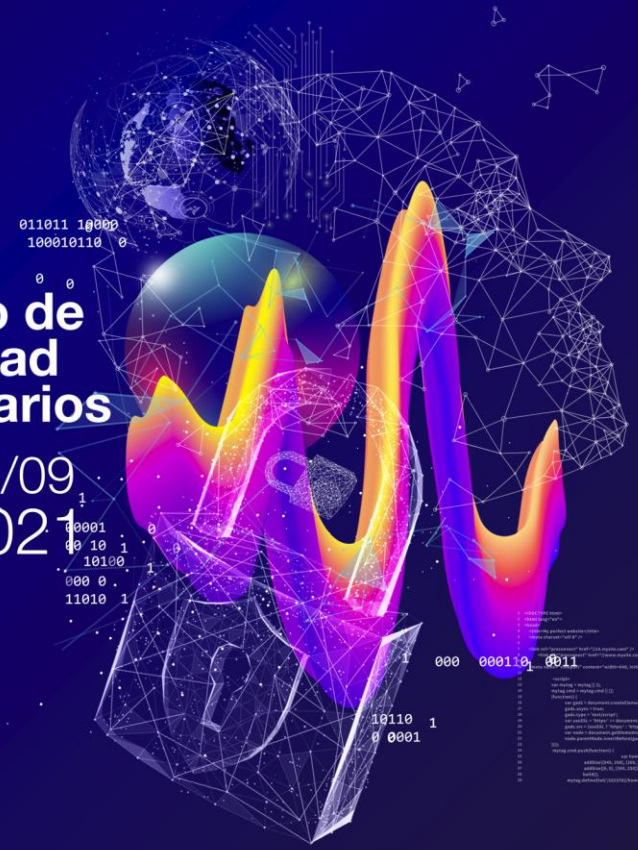
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

2do Seminario de Ciberseguridad para funcionarios públicos

MARTES 28/09 2021



Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile