

II JORNADA STIC

CAPÍTULO COLOMBIA



Sobreviviendo a una intrusión avanzada de Ransomware: Claves del éxito

Jess Garcia
Founder & CEO of One eSecurity



\$whoami



Jess Garcia

@j3ssgarcia



Fundador y CEO de One eSecurity
25 años de experiencia



Compañía global de DFIR
15 años



Líder del proyecto DS4N6
www.ds4n6.io



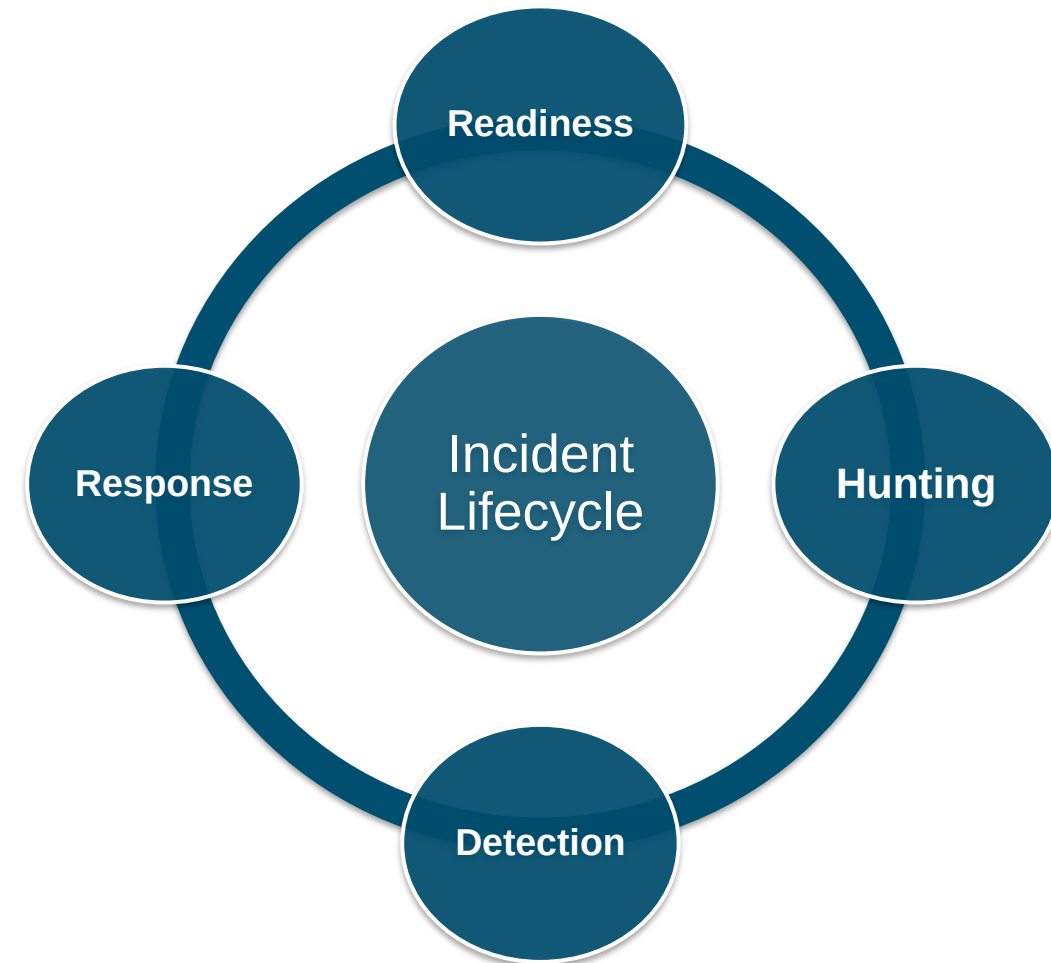
Senior Instructor en SANS Institute
20 años



Who we are

One eSecurity is a market leading specialist in **Digital Forensics and Incident Response (DFIR)** Services and Technology **since 2007**.

- **Flexibility**
- **Adaptability**
- **Deep, Specialist Expertise**
- **Forensic Vision**
- **Rapid Response**

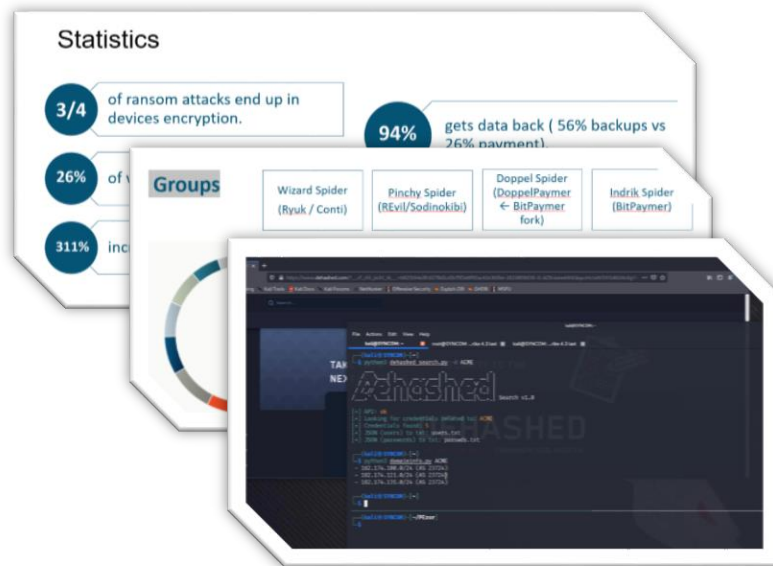


Our primary mission is to make the world a safer place.

Anteriormente...

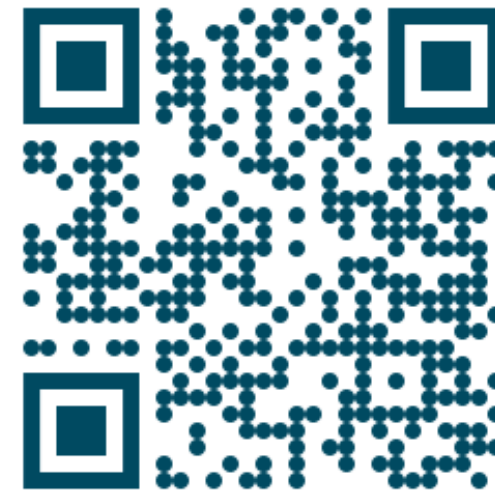
Ransomware:

Lecciones desde las trincheras



one-esecurity.com/ens21

Desde las trincheras:
Sobreviviendo a una intrusión
avanzada de Ransomware



one-esecurity.com/sticco22

Factores de éxito

Evaluar y mejorar

Modelo de Madurez IR	Planes/playbooks de IR
Forensic Readiness	Mejora de capacidades
Mapeo de detección	Mejora de infra DFIR

Investigar

Análisis profundo	Registros rastreables
Contestar preguntas	Procesos legales/admin
Cadena de custodia	

Readiness

Hunting

Detection

Response

Concientizar/evaluar

Eval. capacidades	Medir conocimiento
Medir preparación	Identificar brechas
Crear conciencia	

Ransomware

Prepararse	Detectar
Responder	

Responder

Reacción rápida	Identificar
Contener	Erradicar
Minimizar downtime	Restaurar y mejorar

Asegurarse

Suscripción	Cálculo de impacto
Coberturas y servicios	1ª respuesta

Detectar amenazas

Continua	Proactiva	Basada en inteligencia
Compromise assessment	Detección en host/red	Managed hunting

**La siguiente es una historia
basada en casos reales**

**Basada en múltiples casos de éxito y
lecciones aprendidas**

[La identidad de las víctimas ha sido cambiada]

Contexto

- Empresa global
- Presente en 5 continentes
- Headquarters regionales:
 - Londres / NY / Sídney
- SOC basado en EEUU
- One eSecurity brinda:
 - Servicios de Threat Hunting, con infra desplegada en EMEA y LATAM
 - DFIR Retainer





Cyber Consulting



- **Prepararse** ante la materialización de un incidente
- **Evaluar y mejorar** las capacidades de gestión de IR
- **Tener un guía** en los procesos de toma de decisiones
- **Aumentar la madurez**, preparación y resiliencia a incidentes de seguridad.
- **Evaluar y detectar brechas** de capacidades de detección y respuesta
- **Mejorar** la infraestructura de DFIR



Recursos

- Modelos de madurez de IR
- Desarrollo de planes/playbooks de IR
- Mapeo de detección (MITRE)
- Mejora de capacidades

Evaluar y mejorar

Modelo de Madurez IR	Planes/playbooks de IR
Forensic Readiness	Mejora de capacidades
Mapeo de detección	Mejora de infra DFIR

Ransomware

- Threat Landscapes basados en inteligencia
- Playbooks propios de Ransomware
- Manuales de decisiones de alto nivel
 - ¿Apagar sistemas?
 - ¿Pagar o no pagar?
 - ¿Hacer público?



Readiness

Hunting

Detection

Response



Cyber Exercises

Concientizar/evaluar	
Eval. capacidades	Medir conocimiento
Medir preparación	Identificar brechas
Crear conciencia	



- **Simular** eventos reales
- **Evaluar capacidades** de respuesta
- **Identificar**
 - Brechas
 - Planes incompletos/no maduros



Recursos

- Ejercicios ad-hoc / customizados
- Repositorio de ejercicios
- Workshops con expertos de One eSecurity
- Formato híbrido
 - CybEx/Workshop

- **Evaluar** el conocimiento
- **Analizar** reacciones
- **Crear conciencia** en niveles técnicos y directivos



Readiness

Hunting

Detection

Response

¿Con qué nos enfrentamos?

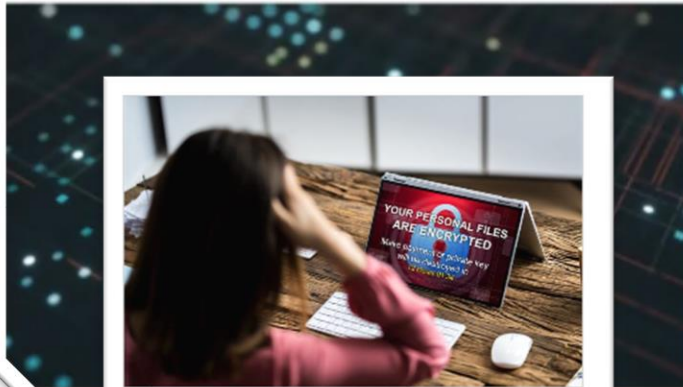
Mining technology company Gyrodata hit by ransomware attack – employee data leaked

Isabella Haverth 23 April 2021 at 14:46 UTC
Updated: 06 July 2021 at 09:28 UTC

Ransomware Cyberattacks Data Breach



Sensitive personal details possibly stolen



Conti and LockBit Make Waves with High-Profile Attacks: Ransomware in Q4 2021

January 28, 2022

This latest report features the ransomware threat landscape in the fourth quarter of 2021, and includes notable ransomware families and the types of industries and enterprises that were targeted. This report also highlights two modern ransomware families that worked overtime during this period, Conti and LockBit.

The Destructive Rise Of Ransomware-As-A-Service

Barbara Kay Brand Contributor
ServiceNow BRANDVOICE | Paid Program
Innovation

Businesses need to confront the growing threat from targeted ransomware before it's too late.

2021 has seen a surge of ransomware attacks against targets ranging from international meat producers, oil pipelines, and global technology companies to regional victims like the ferries between Martha's Vineyard and Nantucket.



Ransomware Isn't Back. It Never Left

A recent wave of attacks belies an apparent lull toward the end of the summer.



The attack on the New Cooperative grain co-op is part of a resurgence in high-profile incidents. PHOTOGRAPH: GETTY IMAGES

A Ransomware Attack Hit Up To 1,500 Businesses. A Cybersecurity Expert On What's Next

Updated: July 8, 2021 8:28 PM ET
Heard on Morning Edition



5-Minute Listen

PLAYLIST

Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers

The payment clears risks emboldening companies hostage

HSE hackers were in health service's computer system for eight weeks before cyber attack

The detonation of the ransomware attack took place on May 14th

Fri 12:01 PM 28,580 Views 83 Comments

Updated Fri 1:20 PM

A NEW REPORT into the HSE cyber attack in May shows that the hackers were in the health service's computer systems for eight weeks before they initiated the attack.

The report, which was launched this afternoon, gives details on how the HSE were unprepared for a cyber attack, due to the weakness of their IT system and a lack of cybersecurity detection and monitoring.



¿Qué pasaría si se despliega un Ransomware?

Colonial Pipeline

- Rescate: 5M USD
- Impacto al negocio: No revelado
- **Downtime: ~2 semanas**
- El pago se hizo **horas** después del ataque
- Nunca se recibieron las **claves de descifrado**

Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers

The payment clears risks emboldening companies hostage

HSE hackers were in health service's computer system for eight weeks before cyber attack

The detonation of the ransomware attack took place on May 14th

Updated Fri 1:20 PM

A NEW REPORT into the HSE cyber attack in May shows that the hackers were in the health service's computer systems for eight weeks before they initiated the attack.

The report, which was launched this afternoon, gives details on how the HSE were unprepared for a cyber



Servicios de Salud de Irlanda (HSE)

- Ataque a **servicios de salud** en plena pandemia
- Impacto al negocio: 100M€
- ~6 meses de recuperación
- Impacto en vidas humanas

Ireland's Health System Forced To Shut Computer Systems After Being Hit By 'Significant' Ransomware Attack



Siladitya Ray Forbes Staff
Business

Covering breaking news and tech policy stories at Forbes.



Listen to article 4 minutes



Updated May 14, 2021, 09:11am EDT



Cyber Insurance

Asegurarse	
Suscripción	Cálculo de impacto
Coberturas y servicios	1ª respuesta

Antes

- **Conocer** el sector de ciberseguros
- **Alcanzar** los niveles de cobertura requeridos
- **Ejecutar** servicios de preparación
- **Calcular el impacto** de un incidente
- **Contar con un 1st responder** ante un incidente o investigación forense



Durante

- **Comunicación** asegurado/aseguradora



Después

- **Optimizar** límites/cobertura
- Lecciones aprendidas y mejoras propuestas



Otros

- Nuevos requerimientos/coberturas por Ransomware



Readiness

Hunting

Detection

Response

Día 0



Alerta del SOC



Herramientas de
Pre-Ransomware
encontradas



5 máquinas
infectadas



Posible propagación
a otras regiones

Estrategia global

KEEP
CALM
AND
CALL
(one)
esecurity

Respuesta a incidentes

Preparación > Identificación > Contención > Erradicación > Recuperación > Lecciones aprendidas

Evitar la catástrofe

Impacto de. Negocio / Aislamiento de la red / Aislamiento de DCs

Protección de backups

Protección / Aislamiento / Restauración

Threat Hunting

Basado en inteligencia / Monitorización avanzada / 24x7 / Nivel crítico

Investigación

Quién / Qué / Dónde / Cómo / Cuándo – Análisis forense

CTI

Análisis de amenazas / TTPs / IOCs / Atribución de actores

Alcance del ataque

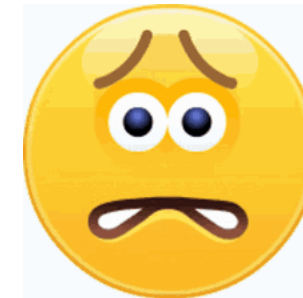


Estados Unidos

Servidores	5,000
DC	350
Workstations/laptops	12,000



Riesgo de propagación mundial



Impacto al negocio



Paro de actividades



Robo de datos

Extorsión



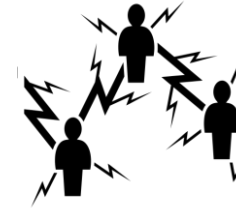
Pago de rescate

Millones de dólares



Costos de recuperación

Millones/Billones

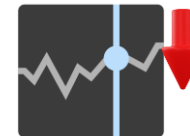


Impacto a terceros

Daño a relaciones comerciales



Daño reputacional



Impacto en la bolsa



Otros daños
desconocidos/no previstos

Comienza el incidente

Día 1



Misiones

El despliegue de Ransomware es inminente

Medidas agresivas
para evitar el cifrado masivo

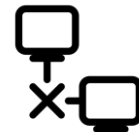
Preparación



Proteger backups



SOC alerta máxima



Aislar de redes



Apoyo C-level



Desconectar DCs



Impacto al negocio



Emergency Incident Response

Responder	
Reacción rápida	Identificar
Contener	Erradicar
Minimizar downtime	Restaurar y mejorar

- **Actuar rápido**

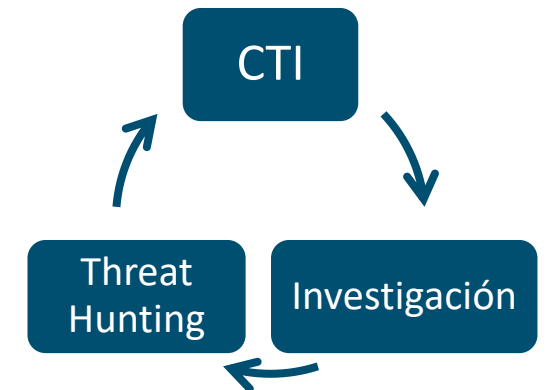


- **Tener** un Retainer +
- **Prepararse** para responder:
 - **Tener** canales de comunicación
 - **Tener** mecanismos de acceso/despliegue
 - **Integrar** recursos humanos/tecnológicos
- **Desplegar** en menos de **4 hrs**
- **Comenzar análisis** en menos de **12 hrs**

- **Contar con apoyo** en la gestión táctica/estratégica
- **Asegurar apoyo** de la organización (dirección, TI, SOC, etc.)
- **Operaciones 24x7**
(Ambas partes)
- Equipo de IR **global**



- **Capacidad** de análisis masivo
Hunting de 4000+ máquinas
- **Utilizar Ciberinteligencia** para contención/remediación:



Readiness

Hunting

Detection

Response

Día 1



Misiones

El despliegue de Ransomware es inminente

Medidas agresivas
para evitar el cifrado masivo

Frenar al actor (*tarpping*)



Deshabilitar cuentas comprometidas



Desplegar de Firewalls/Proxies



Cambio de credenciales masivo



Limitar opciones de entrada

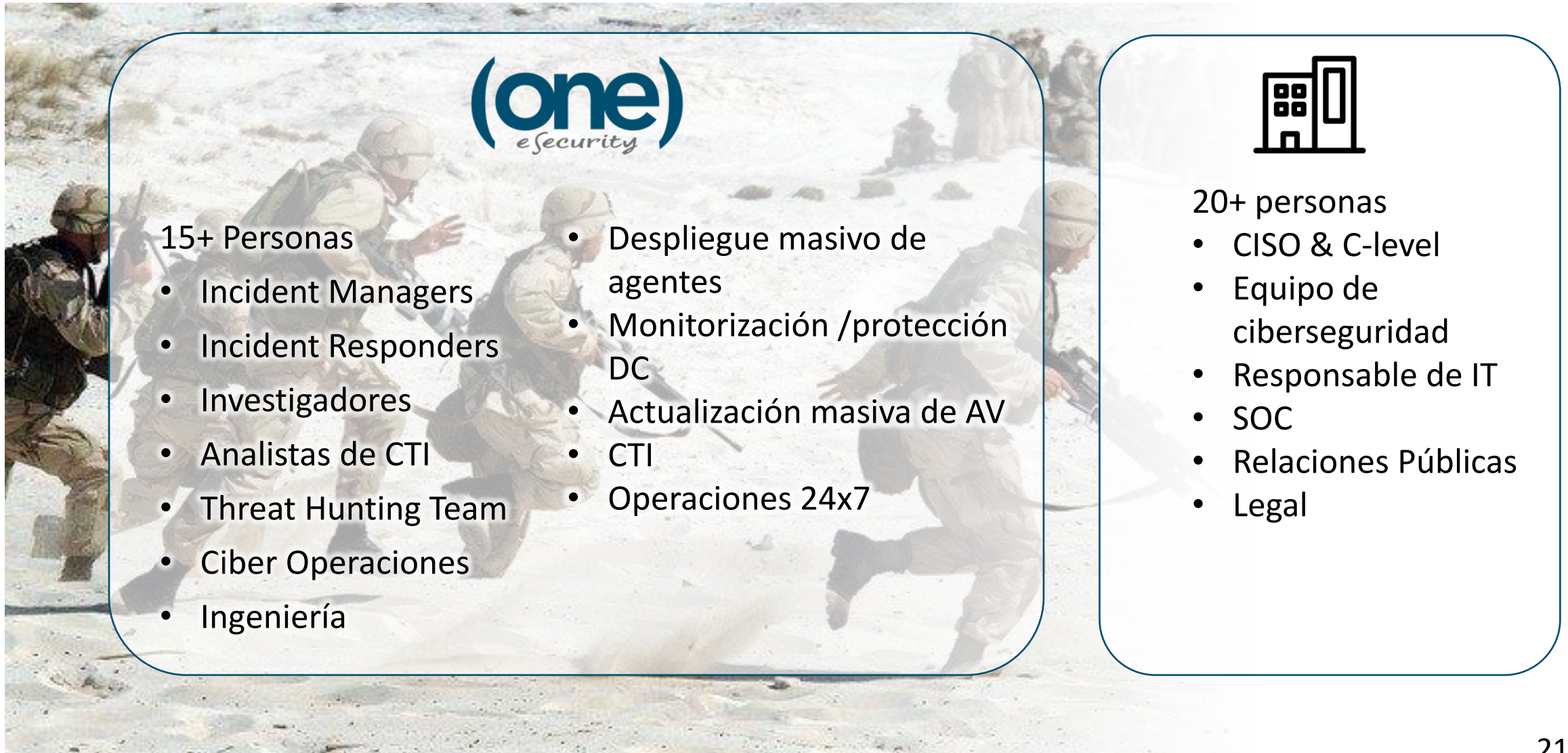


Bloquear IPs/dominios maliciosos



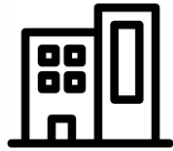
Actualizar AV

Despliegue de fuerzas





- 15+ Personas
 - Incident Managers
 - Incident Responders
 - Investigadores
 - Analistas de CTI
 - Threat Hunting Team
 - Ciber Operaciones
 - Ingeniería
- Despliegue masivo de agentes
- Monitorización /protección DC
- Actualización masiva de AV
- CTI
- Operaciones 24x7



20+ personas

- CISO & C-level
- Equipo de ciberseguridad
- Responsable de IT
- SOC
- Relaciones Públicas
- Legal

Día 1 - AM



Análisis de
artefactos



Bloqueo de
herramientas



Bloqueo de
C2



Threat
Actor



Shda.txt

Día 1 - PM



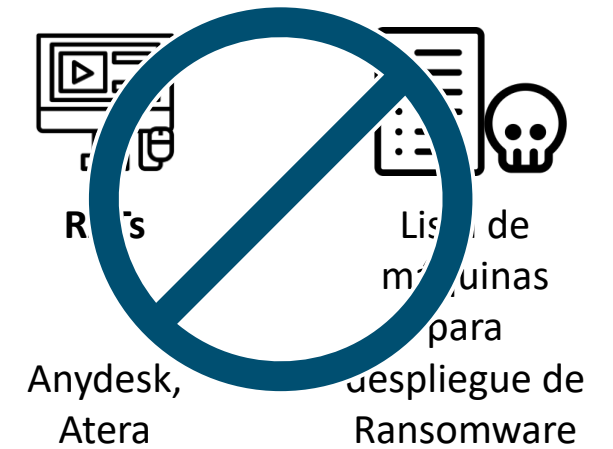
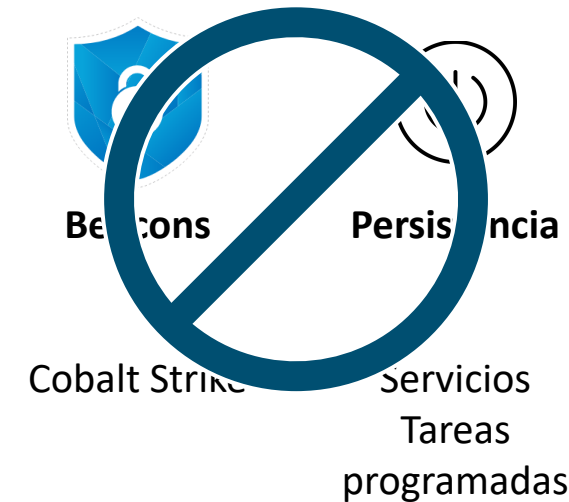
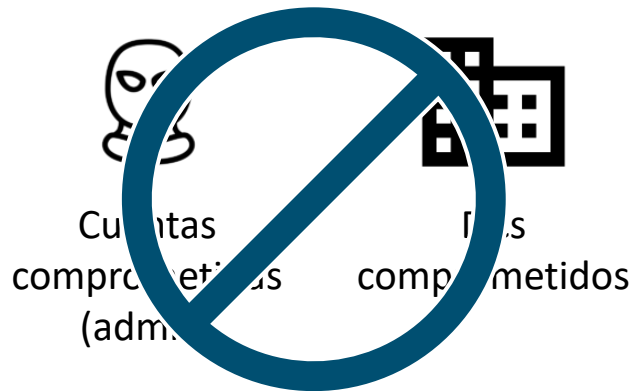
Bloqueo de cuentas



Bloqueo de herramientas



Threat Actor



Día 1 - PM

Se identifica al actor:



CONTI

- Actor ruso
- **TOP Threat Actor**
- Ransomware as a Service (RaaS)
- Especializado en doble extorsión
(Robo de datos + Ransomware)



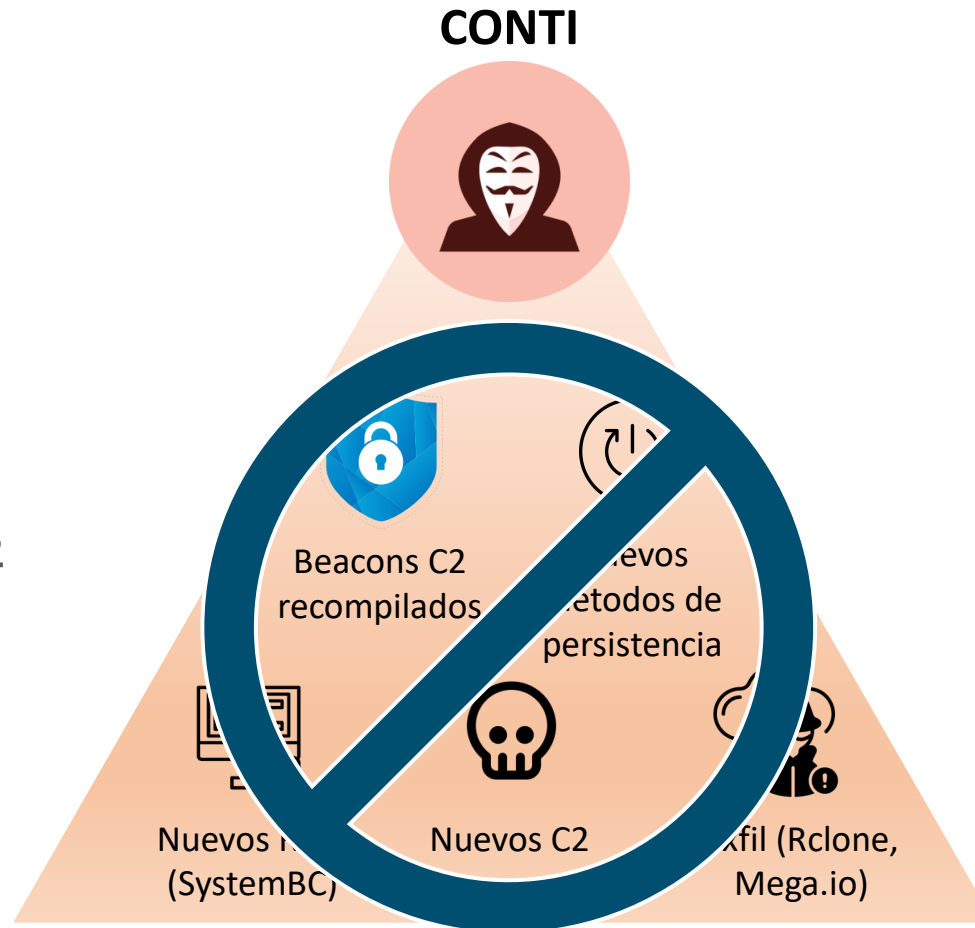
Manual filtrado
de CONTI



Día 2

El actor sabe que
está siendo
contenido

Cambia su modus
operandi

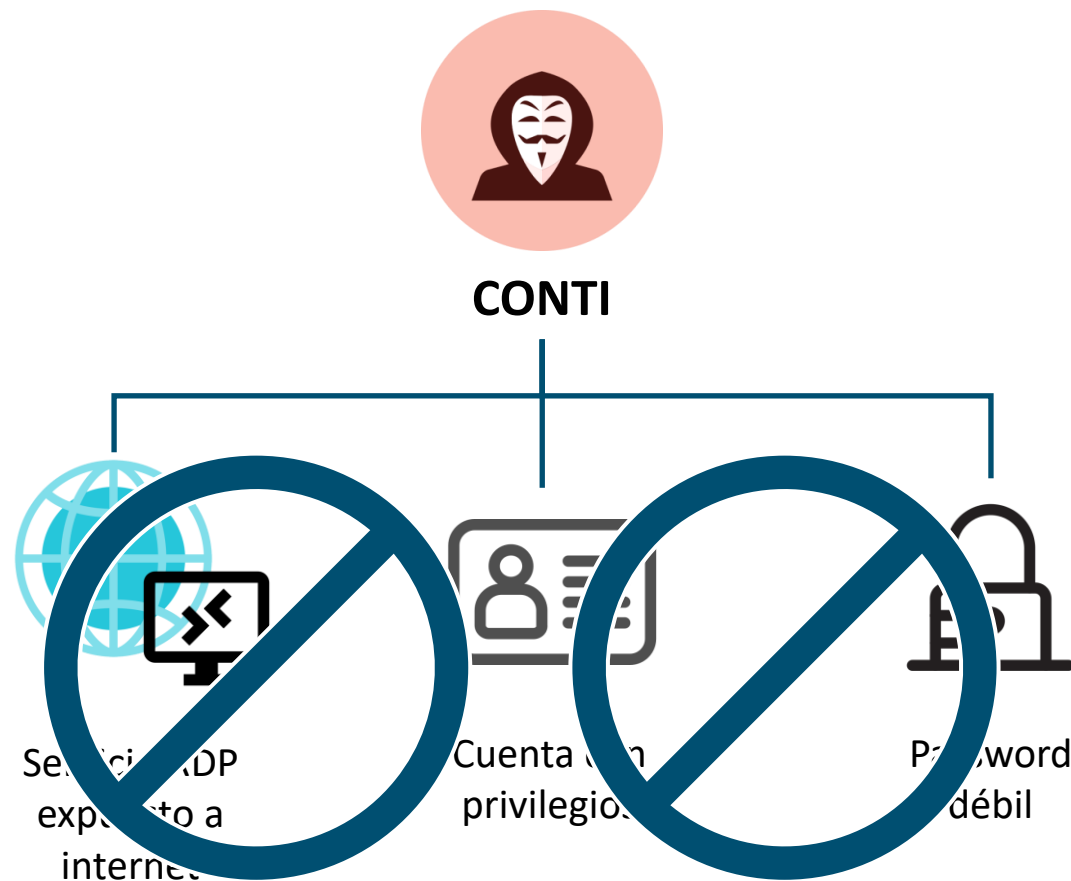


Día 3

Se confirma el
punto de entrada

Se continúa el
bloqueo de IOCs

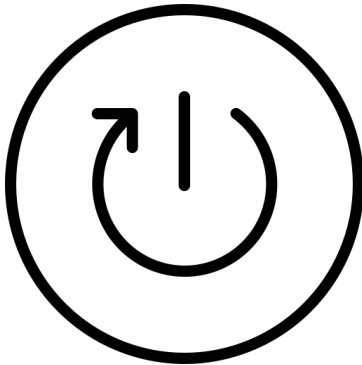
**Último día de
actividad del actor**





Emergency Incident Response

Responder	
Reacción rápida	Identificar
Contener	Erradicar
Minimizar downtime	Restaurar y mejorar



Actividades post-incidente

- Documentar y dar seguimiento de lecciones aprendidas
- Utilizar Threat Hunting en la detección post incidente
- Asistir en acciones de limpieza y recuperación
- Asegurar compromiso de TI/tecnología/SOC

Readiness

Hunting

Detection

Response

Siguientes 4 semanas



DCs
comprometidos



Posibilidad de
volver



¡Siguiente víctima!



Ciclo de TH continuo 24x7



Continúa la limpieza y la
recuperación



Mejoras de seguridad



Hacerle la vida imposible
al atacante



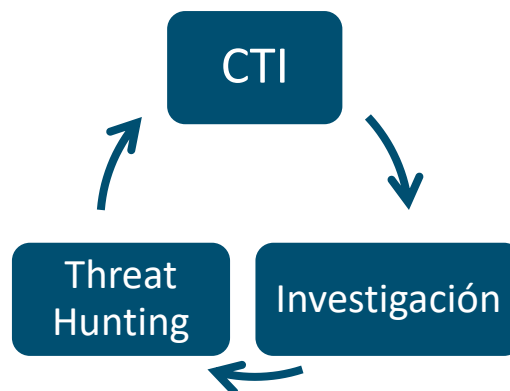
Threat Hunting

Detectar amenazas		
Continua	Proactiva	Basada en inteligencia
Compromise assessment	Detección en host/red	Managed hunting

- **Detectar** amenazas
 - Contínuamente
 - Proactivamente
- **En hosts y redes**
- **Combinar** análisis manual y automático
- **Contar** con un equipo de analistas especializados



- **Poder desplegar** en miles de equipos
- **Basarse en inteligencia** y resultados de investigación



- **Aumentar** las capacidades de detección
- **Adaptarse** a las necesidades y capacidades del cliente



Managed Threat Hunting

- Servicio gestionado
- Con las herramientas propias del cliente



Compromise assessment

- **Evaluar** objetivamente un ambiente
- **Identificar** actividad maliciosa
- Metodología DFIR

Readiness

Hunting

Detection

Response



Threat Hunting

TRINITY

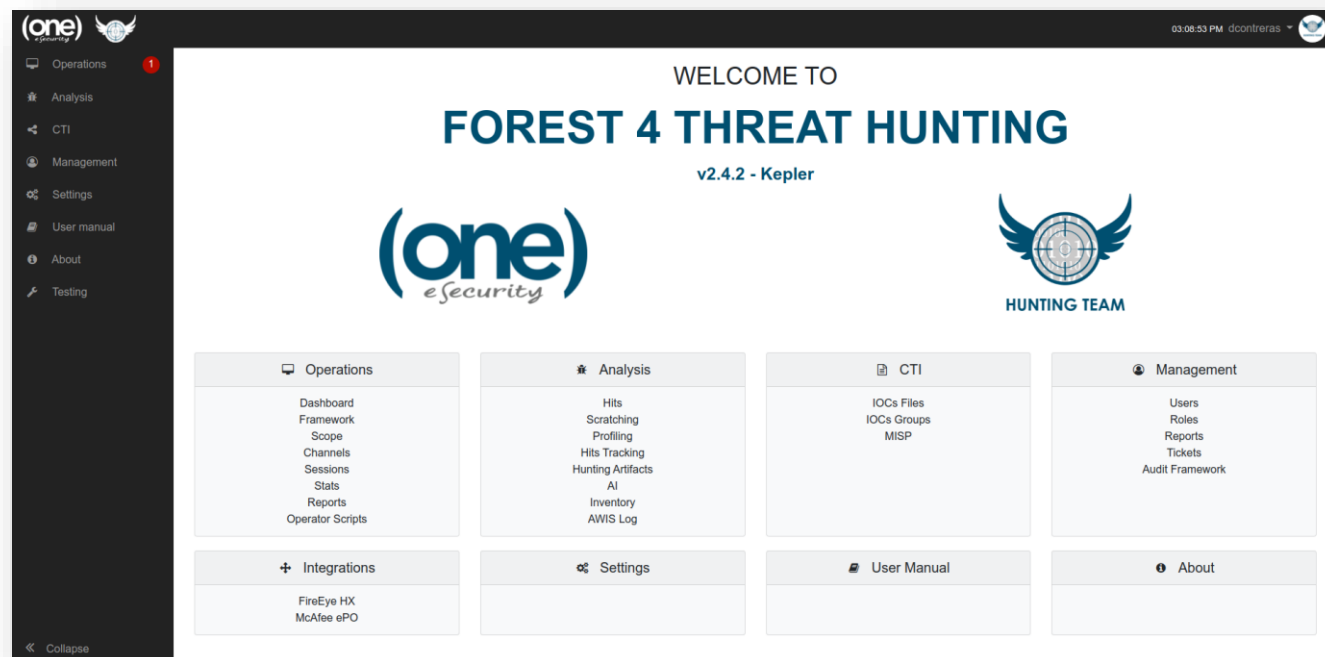
A NEW WAY TO DETECT THREATS

Trinity es la plataforma de Threat Hunting de One eSecurity.

Desarrollada por nuestros expertos para detectar amenazas antes de que impacten tu organización



Multivendor Threat Intelligence **Escalable Automation**
Endpoints / Network **Powered with AI**



Readiness

Hunting

Detection

Response



Digital Forensics



- **Analizar** a fondo
- **Obtener evidencia** de actividad
- **Contestar** preguntas investigativas



- **Tener una metodología**
 - Procedimientos
 - Técnicas
 - **Preservar** cadena de custodia



- **Garantizar** validez de la evidencia digital
 - Procesos legales
 - Procesos administrativos

Investigar	
Análisis profundo	Registros rastreables
Contestar preguntas	Procesos legales/admin
Cadena de custodia	

Readiness

Hunting

Detection

Response

Resultados de investigación

Entrada inicial:



RDP
expuesto



Cuenta con
privilegios



Password
débil



2500+ máquinas
escaneo/reconocimiento



6 días dentro
antes de ser detectado



60+ servidores comprometidos
Incl. Controladores de Dominio



Movimiento lateral inicial
en red de BBDD

30+ usuarios utilizados (20 admin)

Timeline global



Alerta

Respuesta a incidentes

Evitar la catástrofe

Protección de backups

Threat Hunting

Investigación

CTI

1er drop de malware



Compromiso de DC



Despliegue masivo de malware



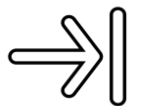
Drop de Ransomware



Prep. exfil



Nuevo malware
Nuevos C2



Última actividad

-6

-5

-4

-3

-2

-1

0

1

2

3

Acceso inicial

Reconocimiento

Mov. Lateral

Credential dumping

Comunicación C2

Lecciones aprendidas

¿Por qué se materializa un ataque?

Acceso inicial



Phishing -
Adjuntos
maliciosos



Accesos remotos/VPN
expuestos/vulnerables



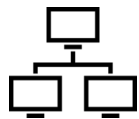
Contraseñas
débiles, No 2FA

Comunicación con C2/Exfil



Acceso a internet no controlado
Falta de controles en FW/Proxy
Herramientas de transferencia/
acceso remoto

Reconocimiento/mov. lateral

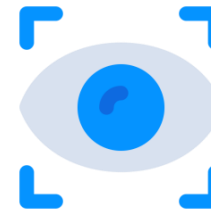


Redes no segmentadas



Mala implementación/gestión de credenciales
Cuentas de admin/servicio
Cuentas de terceros
Métodos de autenticación deprecados/vulnerables
Cambio de contraseñas

SOC/Monitorización



Visibilidad no adecuada
Alertas no refinadas
Protocolos de escalación insuficientes
Capacidad rebasada

Lecciones aprendidas

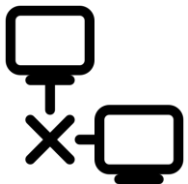
Factores clave de éxito



Compromiso de la capa
directiva (C-level)



Buena estrategia de *tarpitting*



Procedimientos de
aislamiento/shutdown



Despliegue ágil de EIR

< 4h para unirse

< 12h para iniciar análisis



Threat Hunting

Alcance

Detección



CTI

Definir la investigación

Estrategias de contención

“Conoce a tu enemigo”

Factores de éxito



Cyber Consulting

Evaluar y mejorar



Digital Forensics

Investigar



Cyber Exercises

Concientizar/evaluar



Emergency Incident Response

Responder



Cyber Insurance

Asegurarse



R3

Ransomware Resilience & Response



Threat Hunting

Detectar amenazas



Retainer

Readiness

Hunting

Detection

Response

Diferenciadores



Cyber Threat Intelligence

- Experiencia propia liderando y respondiendo a incidentes
- A través de los años y alrededor del mundo



Data Science/ Artificial Intelligence

- Comunidad de analistas forenses, data scientists y desarrolladores
- Evolucionar e innovar los métodos tradicionales de DFIR



Next Generation Forensic Lab: SKY

- Plataforma para automatizar tareas de DF/IR/CTI
- Integradora de herramientas
- Automatización de tareas complejas de análisis forense



Cyber Operations 24x7

- Equipo de operaciones
- Mantiene los servicios funcionando continuamente
- Follow-the-sun

¿Por qué nuestros clientes eligen a One eSecurity?



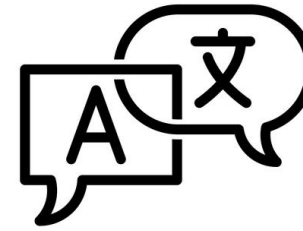
Somos Especialistas



Respuesta rápida



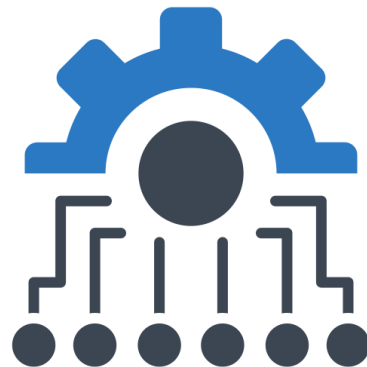
Flexibles



Multilingües



Vendor-neutral



One-stop DFIR service company

Retainer:

- Servicios continuos / EIR
- Cualquier otro servicio de nuestro catálogo DFIR



Jess Garcia
@j3ssgarcia

¡Gracias!

one-esecurity.com/sticco22

Con la colaboración de
Javier Campos

