Simulación de Ransomware
Respuestas ante incidentes

Simulación de ataque de Ransomware

¿Está tu empresa preparada para saber hasta donde podría llegar una intrusión por ***malware/ransomware***?

Simulación de ataque de Ransomware

OBJETIVO

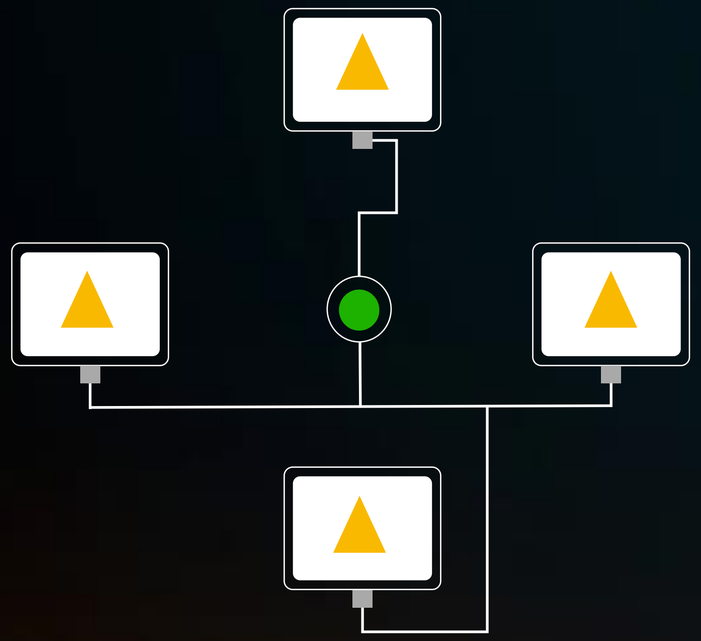
Simular un ataque de ***ransomware***, emulando solo el comportamiento de expansión y bloqueo de pantalla del equipo, sin cifrar ni alterar datos de los equipos en los cuales logre ingresar.

Simulación de ataque de Ransomware

¿CÓMO?

Utilizando un archivo .EXE diseñado por ISG, que se ejecutará desde diferentes localizaciones y además con diferentes tipos de privilegios de usuarios. Te ofrecemos diferentes escenarios para que tengas un mejor panorama de expansión del ransomware.

Simulación de ataque de Ransomware



COMPORTAMIENTO ESPERADO

El usuario descarga el archivo del sitio *https://isglatam.com/isg.exe* Luego dependiendo del escenario/privilegios el ***ransomware*** intentará esparcirse por la red interna, solo bloqueando la pantalla de aquellos equipos a los que pueda ingresar según cada escenario de ejecución.

Simulación de ataque de Ransomware

TRABAJO EN EQUIPO

TODOS, los colaboradores de la empresa deben estar informados de que se realizará el ejercicio de ciberseguridad y tanto el resultado como el proceso de ejecución del mismo debe permanecer bajo absoluta confidencialidad.

Simulación de ataque de Ransomware

ANÁLISIS DEL RESULTADO

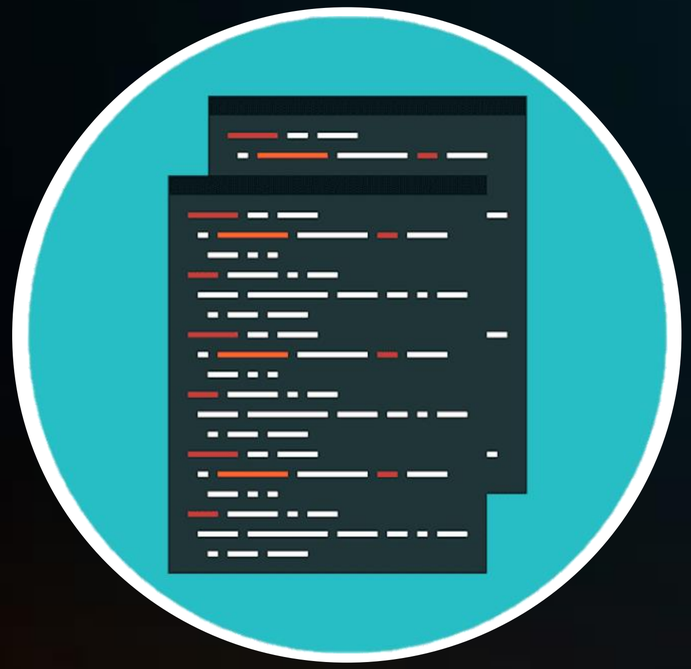
El análisis determinará que tipos de medidas se deberían llevar a cabo para aislar de la mejor manera el ***ransomware***, como así también que puntos de auditoría/eventos son necesarios activar/configurar para tener mayor cantidad de datos a la hora de realizar un procedimiento forense.

Simulación de ataque de Ransomware

PRESENTACIÓN DE RESULTADOS

Se presentarán informes técnicos y gerenciales que detallaran el proceso/ejecución/resultado de la prueba como así también las medidas de protección adiciones para ayudar a mitigar el impacto de un ***ransomware***.

Simulación de ataque de Ransomware



CÓDIGO FUENTE

El código fuente del *ransomware* utilizado por ISG se brindará al cliente de manera cifrada. Estará cifrado con una llave asimétrica, de la cual parte quedará bajo la custodia del cliente y parte bajo la custodia de ISG, solo podrá ser descifrado en conjunto para investigaciones/auditorías puntuales.

Gestión de Respuestas ante Incidentes

¿Está tu empresa preparada responder ante un incidente de ***malware/ransomware***?

Gestión de Respuestas ante Incidentes

OBJETIVO

Capacitar al personal del cliente para identificar diferentes tipos de incidentes relacionados a ***malware/ransomware***, saber cómo proceder en cada caso, ***conteniendo el incidente***, cumpliendo con los protocolos formales de recolección de evidencias, cadena de custodia y análisis de la información recolectada.

Gestión de Respuestas ante Incidentes

EQUIPO A CAPACITAR

Se debe considerar que las personas que tomaran el curso estén desempeñando tareas en sectores como Infraestructura, Seguridad y Desarrollo con el fin de tener un equipo mixto de hasta 6 personas para tomar el curso que se dictará para la Gestión de respuestas ante incidentes.

Gestión de Respuestas ante Incidentes

TIEMPO DE DURACIÓN

El curso se imparte durante 5 días hábiles continuados, de clases de 4 horas cada día + 4 hs de examen práctico final.

MATERIALES

Se brindarán materiales en digital tanto teóricos como maquinas virtuales para los ejercicios de práctica.

REQUISITOS

Notebook con procesador i5 o superior, 8 GB RAM o +, 100 GB o + de espacio en disco. Privilegios de administrador local en la Notebook.

MODALIDAD

- Presencial, desde las oficinas del cliente (Recomendado)
- Online, a través de Zoom/meet/Teams

Gestión de Respuestas ante Incidentes

MODULO 1

- Definición y tipos de incidente:
- **ATP/Malware/Ransomware**
- Clasificación de incidentes
- Qué hacer de acuerdo al incidente
- Primera barrera de contención

MODULO 2

- El incidente esta contenido y ahora qué?
- Metodología para la adquisición de evidencia en Windows
- Herramientas / ejercicios prácticos

MODULO 3

- Artifacts de Sistema Operativo/Usuarios/Aplicación
- Análisis de los artifacts / herramientas
- Análisis de sistemas de ficheros y memoria RAM
- Ejercicios prácticos

Gestión de Respuestas ante Incidentes

MODULO 4

- Determinando el qué, quién, cuándo y cómo
- Cómo realizar el time line de los sucesos
- Cómo escribir el reporte forense y almacenar las evidencias
- Cómo presentar el caso

MODULO 5

- Examen Práctico de 4 horas, donde el alumno deberá contener un incidente, y determinar el cómo, cuándo y quién. Adicionalmente debe escribir el reporte técnico correspondiente

Tiempos de Ejecución

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Simulación Ransomware															
Capacitación Gestión de Incidentes															

Tiempos a 15 días hábiles incluyendo informes. Tiempo de re check de Ransomware estimado 4 días.

Beneficios

	Conocer el nivel real de expansión que podría tener un malware dentro de tu red interna
	Saber cómo establecer puntos de control/alertas de forma efectiva
	Estar capacitado para responder ante un incidente de manera correcta
	Mejorar la prevención de posibles infecciones de malware
	Ajustar registros/evidencias que servirán para realizar un mejor análisis de incidentes