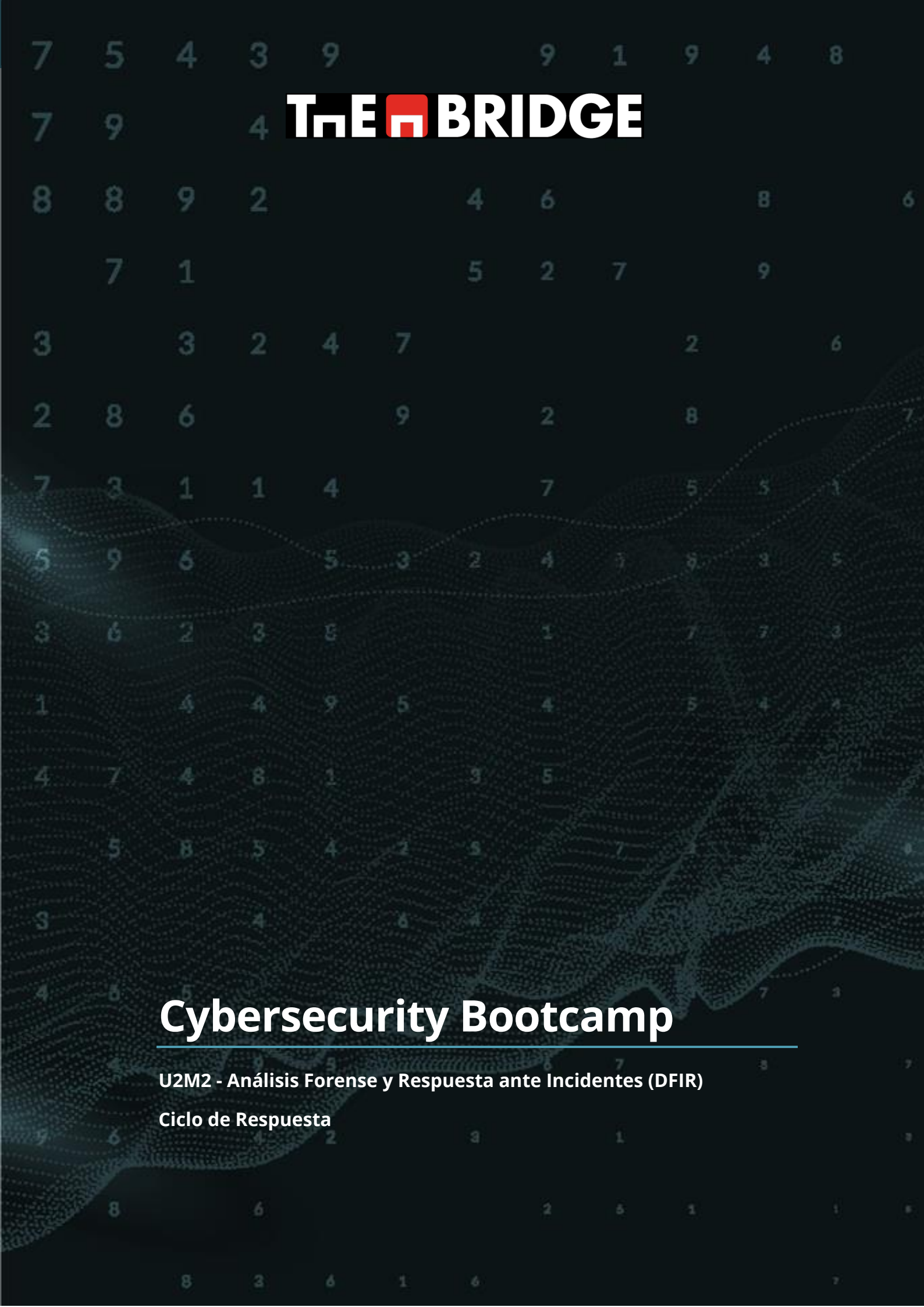

Cybersecurity Bootcamp

U2M2 - Análisis Forense y Respuesta ante Incidentes (DFIR)

Ciclo de Respuesta

Índice

Ciclo de respuesta

1.1. Clasifica los siguientes eventos en precursores o indicadores

#	Evento	Precursor	Indicador
1	Aparición de interlocutores desconocidos o que no deberían estar en la conversación (CC y CCO en hilos de email)		X
2	Identificación de un amplio número de conexiones provenientes de una misma máquina de la organización hacia otros sistemas de la misma		X
3	Amenazas por parte de terceros (internos o externos)		X
4	Recepción de correos no deseados provenientes de dominios no identificados o de escasa reputación en respuesta a hilos de conversación legítimos ya existentes		X
5	Cambios en la configuración de las máquinas que puedan permitir el acceso de *malware*, como detectar el firewall deshabilitado	X	
6	Identificación de información confidencial de la organización en medios externos (*Deep web*, redes sociales, webs públicas, medios de comunicación, etc.)		X
7	Múltiples intentos de acceso fallidos a la base de datos o servidores	X	
8	Notificación de usuarios por identificación de la misma extensión inusual en varios ficheros ya existentes previamente en el equipo		X
9	Tráfico de red elevado relacionado con servicios de mensajería electrónica o dominios de almacenamiento en la nube	X	
10	Recepción de mensajes inesperados que instan a cambiar o revelar las credenciales de plataformas corporativas	X	
11	Presencia de dispositivos y equipos no corporativos en la red		X
12	Identificación de un gran número de ficheros con fecha de última modificación simultánea y de madrugada		X
13	Degradación de la experiencia de usuario (incremento en el tiempo de respuesta de los servidores, ralentización de la navegación, etc.)		X
14	Existencia de campañas de denegación de servicios activas que afectan a otras compañías del sector	X	
15	Alerta en los sistemas de monitorización de la organización por la ejecución simultánea de un proceso con el mismo nombre en varias máquinas del mismo segmento de red y ubicado en rutas temporales (como C:\Users\Administrador\AppData\Local\Temp)		X

1. Usuarios ya creados (Indicador).
2. Conexión establecida (Indicador).
3. Amenaza existente (Indicador).
4. Correos no deseados en espera en la carpeta de spam (Indicador).
5. Malware activo tras desactivar el firewall (Precursor).
6. Información identificada de otras ocasiones (Indicador).
7. Intento sin éxito (Precursor).

8. Usuarios identificados (Indicador).
9. Tráfico elevado, no necesariamente malicioso (Precursor).
10. Falta de respuesta a mensajes para cambiar credenciales (Precursor).
11. Presencia dentro de la red (Indicador).
12. Actividad inusual en horas no habituales (Indicador).
13. Presencia en servidores ralentizando el sistema (Indicador).
14. Amenaza existente, no dirigida específicamente a la compañía (Precursor).
15. Creación de rutas temporales con acceso para todos los usuarios (Indicador).

1.2. [DDoS] Completa la siguiente tabla con eventos que permitirían identificar que se podría estar produciendo un potencial incidente de denegación de servicios.

#	Evento
1	Modificaciones en la configuración de las máquinas que podrían facilitar el acceso de malware, como la detección de desactivación del firewall
2	Numerosos intentos fallidos de acceso a la base de datos o servidores
3	Presencia de dispositivos no autorizados en la red corporativa
4	Incremento repentino en el tráfico web proveniente de una única dirección IP o un rango de direcciones IP
5	Detección de información confidencial de la organización en fuentes externas como la deep web, redes sociales, sitios web públicos o medios de comunicación
6	Recepción de correos no deseados de dominios poco reconocidos o con baja reputación en respuesta a conversaciones legítimas previas
7	Fallo completa del servicio
8	Red o servidor con bajo rendimiento

1.3. [Defacement] Completa la siguiente tabla con eventos que permitirían identificar que se podría estar produciendo un potencial incidente de *defacement*

#	Evento
1	Alteración de la apariencia de una página del sitio web
2	Presencia de mensajes de error o advertencia en el sitio web
3	Contenido inapropiado en el sitio web, ya sea mensajes o imágenes
4	Modificaciones no autorizadas en el contenido del sitio web

1.4. [Ransomware] Completa la siguiente tabla con eventos que permitirían identificar que se podría estar produciendo un potencial incidente de infección por ransomware

#	Evento
1	Archivos encriptados o renombrados con una extensión distinta a la original
2	Archivos encriptados con una extensión modificada y la aparición de un mensaje de rescate en el dispositivo comprometido
3	Archivos cifrados y mensaje de rescate en dispositivos, con nota de rescate en el servidor de correo
4	Archivos encriptados con una extensión diferente a la original
5	Solicitudes de rescate en los sistemas comprometidos

1.5. [Fraude en transferencia] Completa la siguiente tabla con eventos que permitirían identificar que se podría estar produciendo un potencial incidente de fraude en transferencia

#	Evento
1	Transacciones hacia destinos con alta probabilidad de fraude
2	Transferencias efectuadas fuera del horario laboral estándar
3	Transferencias a cuentas bancarias no reconocidas o poco usuales
4	Transferencias de cantidades significativas a cuentas bancarias de terceros
5	Transferencias a cuentas bancarias no vinculadas a la transacción original

1.6. Clasifica los siguientes eventos en la fase correspondiente de la Cyber Kill Chain

#	Evento	Fase	Medida de seguridad
1	Enlace web a un portal falso de acceso a Google en un correo de phishing	Distribución	Entrenamiento en seguridad para comprender el uso de herramientas de filtrado de correos electrónicos
2	Detección de varios procesos WMIC en equipos corporativos conectados al mismo segmento de red	Explotación	Bloquear el tráfico de red relacionado con esos procesos utilizando firewalls o herramientas de administración de red. Además, puedes finalizar o detener esos procesos para interrumpir su actividad.
3	Escaneo de todos los subdominios y direcciones IP asociadas al dominio principal de la organización	Reconocimiento	Supervisión de flujo de datos y detección de exploraciones
4	Incremento en el volumen de tráfico desde el segmento de servidores ERP y de gestión hacia direcciones IP desconocidas	Explotación	Para observar y registrar el tráfico de esos servidores, puedes usar herramientas de monitoreo de red.
5	Identificación de peticiones hacia direcciones IP calificadas como C&C en horas de madrugada durante los últimos 15 días	Distribución	Control o restricción de tráfico de red
6	Cifrado de todos los servidores en el mismo segmento de red por medio de ransomware	Comando y control	Recuperación de servidores afectados mediante copias de seguridad y análisis de la vulnerabilidad que originó la infección
7	Borrado de todos los logs de eventos (EVTX) de los servidores y equipos corporativos donde se detectó la presencia de Trickbot	Acciones sobre objetivos	Examen forense de los dispositivos comprometidos y recuperación de los registros de eventos
8	Alto número de intentos de inicio de sesión con la cuenta de administrador local de madrugada y en un rango de pocos minutos	Armamentización	Monitorear y capturar el tráfico de los servidores, podrías usar herramientas como Wireshark o TCPDump.
9	Instalación de Trickbot en todos los equipos del mismo segmento de red	Instalación	Examen forense de los dispositivos comprometidos y erradicación del software malicioso
10	Detección de una versión del malware Emotet en varios equipos, no identificado por el antivirus	Instalación	Actualización del antivirus y evaluación de vulnerabilidades del software