Lanzamientos de Software

- 4.4.5.2
- 4.4.5.3
- 4.4.5.9
- 4.4.5.8
- 4.4.5.5
- 4.4.5.6
- 4.4.5.7
- 4.4.5.4
- 4.4.6.0
- 4.4.6.1
- 4.4.6.2
- 4.4.6.3
- 4.4.6.4
- 4.4.7.0
- 4.4.7.1
- 4.4.7.3
- 4.4.8.0
- 4.4.8.1
- 4.4.8.2
- 4.4.9.0
- 4.4.9.1
- 4.4.9.2
- 4.4.9.4
- 4.5.0.0
- 4.5.0.1
- 4.5.0.2
- 4.5.0.3
- 4.5.1.0
- 4.5.1.2
- 4.5.2.1
- 4.5.2.2
- 4.5.3.0
- 4.5.3.1

Agente de Endpoint

Índice de versiones del agente de endpoint

- 4.4.5.7
- 4.4.5.8
- 4.4.5.9
- 4.4.6.0
- 4.4.6.1
- 4.4.6.2
- 4.4.6.3
- 4.4.6.4
- 4.4.7.0
- 4.4.7.1
- 4.4.7.3
- 4.4.8.0
- 4.4.8.1
- 4.4.8.2
- 4.4.9.0
- 4.4.9.1
- 4.4.9.2
- 4.4.9.4
- 4.5.0.0
- 4.5.0.1
- 4.5.0.2
- 4.5.0.3
- 4.5.1.0
- 4.5.1.2
- 4.5.2.1
- 4.5.2.2
- 4.5.3.0

Agente de Endpoint

4.4.0.9

Funciones

- Para los grupos con telemetría habilitada, se agregaron datos de Active Directory a la lista de vigilancia de robo de credenciales

Correcciones

- Se eliminaron entradas duplicadas de volúmenes locales y recursos compartidos de red en algunos entornos.
- Se refinó el comportamiento para algunas reconstrucciones de bases de datos de miniaturas que causaban incidentes
- Se corrigió un error de validación de licencia que podía aumentar el tiempo de inicio
- Se refinó el comportamiento para el acceso a archivos en medios de escritura única, como CD y unidades de cinta WORM

Estado de validación WHCP/WHQL

Validado

Hashes MD5

```
service.exe   = c32c54381666cbd075fba2b1078b518b
assistant.exe = 2e4266bf1527f384665f57dc979c4c79
CCRRSecMon.sys (Windows10)       = 35472ab324221af5fb459badb937f899
CCRRSecMon.sys (Windows8)        = 04132be3deb9dff52166f2dd39488874
CCRRSecMon.sys (Windows7)        = fc7f480d417d0bf650bef3e5770f49c2
```

Agente de Endpoint

4.4.0.9.1

Funciones

Ninguna - actualización de mantenimiento.

Correcciones

- Se corrigió el problema por el cual algunos recursos compartidos de red conectados por un usuario eran inicialmente ignorados en los análisis.
- Se refinó el comportamiento de falsos positivos asociado con recursos compartidos que aparecen durante las sesiones de usuario, seguidos rápidamente por un cuadro de diálogo Guardar como.

Estado de validación WHCP/WHQL

Validado.

Hashes MD5

```
service.exe   = 52e03ed57dab0fac936364899140af59
assistant.exe = a90ad6f6544c2c3b2fb44bb57b70180b
CCRRSecMon.sys (Windows10)       = 6201b1a056d85c7576e4357e4ec9494e
CCRRSecMon.sys (Windows8)        = bd86ede6922503890f6d9b69871660e4
CCRRSecMon.sys (Windows7)        = ffcfbdda88faac6743b2de00c2cc4530
```

Agente de Endpoint

4.4.1.0

Funciones

- Soporte ampliado para el análisis de inyección de procesos, con el fin de aumentar drásticamente la precisión en la detección de intención maliciosa frente a benigna en aplicaciones.
  - Esto se volvió especialmente importante debido a que un pequeño número (<0.02%) de máquinas en la telemetría de Cyber Crucible generaba alertas por comportamientos agresivos de inyección de procesos en procesos del sistema.
- Mayor capacidad de monitoreo de procesos del sistema sin firmar.
  - Esto fue en parte una respuesta a que los atacantes se enfocan intensamente en involucrar esos procesos durante operaciones de movimiento lateral (dentro de un sistema y entre sistemas).

Correcciones

- Se modificó un comportamiento de modificación de archivos para reducir los falsos positivos, dejando de activarse ante ciertas acciones benignas, mediante contexto adicional a nivel de kernel sobre los comportamientos de acceso a archivos de un proceso.

Estado de validación WHCP/WHQL

Validado.

Hashes MD5

```
service.exe   = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe = 98f013fd4fdb7325f903d07c87b999ac
```

```
CCRRSecMon.sys (Windows10)       = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)        = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)        = 6a0f2e55d6a7b66bd9bbe318d5dbbebf
```

Agente de Endpoint

4.4.1.1

Funciones

- Procesamiento analítico mejorado para relaciones padre-hijo, cuando el proceso padre finaliza rápidamente antes de que Cyber Crucible complete el procesamiento (milisegundos).
  - El escenario extremadamente común aquí es que los atacantes (y los programas legítimos) frecuentemente abren múltiples programas, a veces en una “cadena” de varios pasos. Esto puede ser intencional, o debido al comportamiento de Windows u otras aplicaciones “por debajo”.
  - Los modelos de comportamiento de Cyber Crucible aprovechan las variables de actividad y estado para todos los procesos en una cadena de ejecuciones para lograr la máxima precisión y contexto.

Correcciones

- Cyber Crucible tuvo una pérdida en la precisión de la toma de decisiones del modelo de comportamiento, debido a la pérdida de telemetría cuando múltiples programas se llaman entre sí, pero uno de los programas finalizó en milisegundos.
  - En una cadena donde el Programa A ejecuta el Programa B. El Programa B inicia el Programa C, pero el Programa B finaliza en milisegundos (generalmente un fallo silencioso, pero no siempre). El análisis de comportamiento de Cyber Crucible tiene las variables del Programa A y del Programa C, pero no tuvo tiempo de analizar completamente el Programa B, ya que esperaba que estuviera en ejecución.
  - Esto se ha corregido, lo que resulta en una toma de decisiones más precisa por parte del motor de toma de decisiones hiperautomatizado de Cyber Crucible.

Estado de Validación WHCP/WHQL

Validado.

Hashes MD5

```
service.exe   = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe = a5bac35d839d7a57fcccfceb011083c1
CCRRSecMon.sys (Windows10)       = 935e43368fa95ae740a3f04defcc390d
CCRRSecMon.sys (Windows8)        = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)        = a6a5073c6565361b443651ef29e49490
```

Agente de Endpoint

4.4.1.2

Características

- Mayor especificidad disponible para listas blancas, como la ruta y los argumentos del proceso principal.
- Soporte ampliado para análisis de acceso de identidad a más bases de datos de credenciales.
  - El acceso de identidad ahora también se supervisa para Slack, Opera, Thunderbird, Discord y Vivaldi.
- Soporte de lista blanca ampliado para incluir el acceso de identidad.

Correcciones

- Se redujo el ancho de banda utilizado entre los agentes y la API REST.
- Se corrigió un problema por el cual algunas ediciones más antiguas de Windows Server mostraban señuelos (canaries) en el Explorador.
- Se corrigió un problema por el cual algunos registros de acceso de identidad no incluían indicadores de confianza de certificado.

Estado de validación WHCP/WHQL

Validado

Hashes MD5

```
service.exe   = e289ef44c5a1bca39d57861ff9d05bee
assistant.exe = d8e83309372b43ffc70feaf2bd538f36
CCRRSecMon.sys (Windows10)       = db736330f5a690a2e828472a357ee6b6
CCRRSecMon.sys (Windows8)        = b9d644930fc52495229dc7f96ffea299
```

```
CCRRSecMon.sys (Windows7)        = 7b1ece332986dadfcc6463574fd16616
```

Agente de Endpoint

4.4.1.3

Funciones

- El monitoreo de credenciales/identidad ahora incluye varias VPN, billeteras de criptomonedas y otras aplicaciones.
- En una cadena (esto es común) de procesos afectados durante un ataque (el atacante se mueve del programa en ejecución A, a B, a C, y D se utiliza para el robo de datos), el programa "paciente 0" A queda suspendido, pero el paciente D se reporta como el proceso que realiza el comportamiento de robo.
  - El estado de la memoria se preserva y se reporta a lo largo de las cadenas de procesos, para un futuro análisis forense.
- En caso de una respuesta automatizada en la que se haya modificado la memoria de un proceso en ejecución, dicha modificación de memoria se sube de forma configurable a Cyber Crucible para su ingeniería inversa y análisis adicional.
- En caso de un error de modificación de memoria no malicioso en una aplicación, las excepciones de comportamiento ("listas blancas") ahora tienen la capacidad de marcar ciertos eventos de corrupción de memoria como benignos. Esto no evitará que el propio programa se bloquee o pierda datos debido al error, pero Cyber Crucible sabrá ignorar el error mientras busca la inyección maliciosa de código en procesos en ejecución (inyección de procesos/hollowing).

Correcciones

- Se eliminó una vulnerabilidad por la cual los binarios podían ser eliminados por un proceso con privilegios mientras los binarios de CC se estaban actualizando.
- Se eliminó una vulnerabilidad por la cual las claves de registro podían ser eliminadas o alteradas por un proceso con privilegios mientras los binarios de CC se estaban actualizando.
- Se corrigió el seguimiento del estado de la memoria cuando un proceso se parchea en memoria durante la evaluación de la memoria por parte de Cyber Crucible.
- Se corrigió el seguimiento del estado de la memoria en determinadas condiciones en las que la memoria se reasigna entre páginas de memoria.
- Actualizaciones menores de eficiencia de la CPU, probablemente demasiado pequeñas para registrarse en el Administrador de tareas, ya que el uso normalmente es <1%

Estado de validación WHCP/WHQL

Validado

Hashes MD5

```
service.exe   = 90a6ca2f5b7a76b847052f3d420f0c9b
assistant.exe = b62ee623f74171f4a3f34ff129188174
CCRRSecMon.sys (Windows10)       = dfdce4016f6920e844615b3d506ec2e2
CCRRSecMon.sys (Windows8)        = 59bbd41c883ca0205fd3adbfdbb5dbb6
CCRRSecMon.sys (Windows7)        = 88e6f047f7fa26e717a24f5fd7b33dc5
```

4.4.1.3.1

Se obtuvo visibilidad sobre algunos procesos del sistema que se inicializan antes de que se cargue el controlador de Cyber Crucible.

Hashes MD5:

```
service.exe: a03b91df83f86ffe322f7b16960f503c
assistant.exe: e22641924d3a1811b86a0f4357f74720
win7/CCRRSecMon.sys: b64b63c04f00afd1020a7a43fc0bb67d
win8/CCRRSecMon.sys: c50aacb4aac6ac9f1e95e4ffa749cb2a
win10/CCRRSecMon.sys: 77dd029b8e4b2cf5a2354787402ecc17
```

4.4.1.3.2

Se agregó telemetría adicional para los procesos del sistema ahora visibles debido a 4.4.1.3.1.

Hashes MD5:

```
service.exe: 47f408d6102eb06a94f2244cf139a0a5
assistant.exe: 86733da51ee703f93dcda9346231cca6
```

```
win7/CCRRSecMon.sys: b01e8933fa9ac9f0a049527b20d9f679
win8/CCRRSecMon.sys: 4467124cf7e8b5ab5652169f9eb41663
win10/CCRRSecMon.sys: 8f06de95303eeac038002ec27c297811
```

4.4.1.3.3

Se corrigieron algunos reportes de incidentes que incluían datos del proceso incorrecto, cuando un proceso finaliza a mitad de un cálculo.

Hashes MD5:

```
service.exe: f2a341ca4856ab3f8a15b7cf725cd0cc
assistant.exe: 5d5d2213e276bc066f4d42ab751c7317
win7/CCRRSecMon.sys: 13da73b66751d12f5f3e65cde0602266
win8/CCRRSecMon.sys: 08fe8cb3391c9215bc37a997ec59b0a2
win10/CCRRSecMon.sys: 4c8a1707839f0d28c386f17ce2dbc8ed
```

4.4.1.3.4

Optimización de los cálculos de memoria, en preparación para la 4.4.1.4.

Hashes MD5:

```
service.exe   = 4a5bd9822ea28c10f399afe437837a2a
assistant.exe = 7070e61862bc2ede3205c4bfdc6805d2
CCRRSecMon.sys (Windows10)       = 4e9b790522fe61e9206140e15e37b7fe
CCRRSecMon.sys (Windows8)        = 7b477503840f882028ff8bdbbfc72121
CCRRSecMon.sys (Windows7)        = 65e95b4dd58cb1c9a5dab398155e2113
```

Agente de Endpoint

4.4.1.4

Funciones

- Capacidades de coincidencia de patrones mejoradas en el modelo de comportamiento.
  - Esto es especialmente relevante para la cobertura adicional de ubicaciones de almacenes de identidad, como las ubicaciones de billeteras de criptomonedas.
- Funcionalidad de dependencia de software incrementada para las bibliotecas (de Cyber Crucible) en uso para la próxima protección de acceso a identidades totalmente automatizada.
- Capacidad opcional para ejecutar el agente en modo seguro

Correcciones

- Se optimizó el uso de memoria en el servicio. Esto solo se habría experimentado en servidores muy ocupados con mucho análisis de comportamiento en curso (por parte de Cyber Crucible) simultáneamente.

Hashes MD5

```
service.exe   = 1cb8e19fc9ed2788189684f23693087a
assistant.exe = c60e851d9836955b078474270e04d0c1
CCRRSecMon.sys (Windows7)        = 3b7656b24a0e2387389f0ce9db375379
CCRRSecMon.sys (Windows8)        = 204689e666bb704621ebbd5d606a1274
CCRRSecMon.sys (Windows10)       = f9839b8b2437a3a7b6a099d2598dc639
```

Agente de Endpoint

4.4.2.0

Características

- Capacidades de monitoreo y prevención mejoradas para la protección automatizada del acceso a identidades.
- Optimización del uso de la red mediante tasas de comunicación variables según el comportamiento del cliente.

Correcciones

- N/A

Hashes MD5

```
service.exe   = 408d8ae9e35ee65c8e208cfa76c67df6
assistant.exe = 8ba7fa2a201ae92f595e85e4cf52b804
CCRRSecMon.sys (Windows7)        = 359ff6e23107798fd01a3afb33716f78
CCRRSecMon.sys (Windows8)        = 2bd4267eeea697a137447d91a8b38e1c
CCRRSecMon.sys (Windows10)       = fcf979529c13eba5f93bf6c6d0096d6f
```

Agente de Endpoint

4.4.2.1

Correcciones

- Se optimizó el seguimiento de información de identidad para aplicaciones con un gran número de directorios profundamente anidados.

Hashes MD5

```
service.exe   = 9c6474e44959e8eba54876c46e13fb25
assistant.exe = 03d671ffa567ac8dc783ce905d624351
CCRRSecMon.sys (Windows7)        = 5fbd3b4a9066299c9ce3d619dc6fca17
CCRRSecMon.sys (Windows8)        = 0ee960548846da463d4c66381dea0841
CCRRSecMon.sys (Windows10)       = bda977682effcd61e6d478da750c966b
```

Agente de Endpoint

4.4.2.2

Funciones

- Ninguna

Correcciones

- Optimización del manejo de variables para un tipo de comportamiento.
  - Causa: Un producto de seguridad no especificado generó una cantidad muy grande de comportamientos en un par de servidores grandes, lo que provocó un uso excesivo de memoria por parte de Cyber Crucible.
  - Síntomas: El uso de memoria de Cyber Crucible aumenta de unos pocos MB a GB. El uso de memoria del producto de seguridad también aumentó 100 veces, hasta superar los 250 GB. Si experimenta esto, dado que podría ser independiente de Cyber Crucible, por favor abra un ticket de soporte para que podamos ayudarle. Sospechamos que esto también fue un problema del producto de seguridad, independiente de la optimización de Cyber Crucible.
  - Corrección: Este seguimiento de la variable de comportamiento se migró de un algoritmo que esperaba una población de bajo volumen a un algoritmo de alto volumen, similar al utilizado en otras partes del controlador.
  - ¿Quién se ve afectado? Solo se observó este problema en un cliente, y únicamente en una pequeña parte de sus servidores grandes. De todos modos, esta actualización se implementa para todos los clientes.

Hashes MD5

```
service.exe   = bbfb0bf47d942d30438a260b497c04cd
assistant.exe = 280d746ed3edea9b7267955a94b97a8e
CCRRSecMon.sys (Windows7)        = cded2aaa7dd0c2fe446694451bd17960
CCRRSecMon.sys (Windows8)        = a06dce5e19627fe1f982cbde632fc313
CCRRSecMon.sys (Windows10)       = 14e0c4e7f86405562701187fac93aea2
```

Agente de Endpoint

4.4.2.3

Funciones

- Ninguna

Correcciones

- Se corrigieron problemas de compatibilidad con Acronis

Hashes MD5

```
service.exe   = 4747ae6372a0f3a410c145e64314123c
assistant.exe = f7c0ac0044a3b186d2f6db2a8a1989f0
CCRRSecMon.sys (Windows10)       = f69661a61bb9364d6f25f5f4b410729c
CCRRSecMon.sys (Windows8)        = 25b496529282e6c973b53a14a94a3480
CCRRSecMon.sys (Windows7)        = ca9ee3cde474ea3b6b5b61b8bc26f170
```

Agente de Endpoint

4.4.2.4

Características

- Compatibilidad de protección de credenciales para Microsoft Teams y Signal Messenger

Correcciones

- Se suprimieron los registros relacionados con la red cuando se está en modo seguro sin redes
- Se realiza una copia de seguridad de algunos datos del agente al desinstalar, en la carpeta de almacenamiento temporal de Windows

Hashes MD5

```
service.exe   = 23735f3ca870b1d70017c433d5e24d17
assistant.exe = 57d8742b1bbc27b73dd134fb3ac6ebc2
CCRRSecMon.sys (Windows8)        = 99262ee4a93e4751adb8b4b1ef2102ce
CCRRSecMon.sys (Windows10)       = 0f2809c32a22af2eda0fe606c361d6d2
CCRRSecMon.sys (Windows7)        = 0d73a497bebfad7b85441ae981ed4be1
```

Agente de Endpoint

4.4.2.5

Características

- Ninguna

Correcciones

- Reducción del uso de red al enviar grandes cantidades de informes a la vez
- Corrección en el manejo de algunos datos de certificados

Hashes MD5

```
service.exe   = a54087913a6ddd451853ffce64112e21
assistant.exe = 14859d6c32192a073c0518b0d3e957ee
CCRRSecMon.sys (Windows8)        = 99262ee4a93e4751adb8b4b1ef2102ce
CCRRSecMon.sys (Windows10)       = 0f2809c32a22af2eda0fe606c361d6d2
CCRRSecMon.sys (Windows7)        = 0d73a497bebfad7b85441ae981ed4be1
```

Agente de Endpoint

4.4.2.6

Características

- Ninguna

Correcciones

- Reducción del uso de memoria en servidores con muchos certificados de programa únicos

Hashes MD5

```
service.exe   = c7afcb665f6849d39430df2271703cd6
assistant.exe = d6ed1b6f2d6d914e9bb08396a3d03a57
CCRRSecMon.sys (Windows8)        = 1a399a22cecdca9b5ffefe69a211fc66
CCRRSecMon.sys (Windows7)        = 57363998c02e1334f6fda931c6c194ba
CCRRSecMon.sys (Windows10)       = d15ddd4035830b80a67e9057456560c2
```

Agente de Endpoint

4.4.2.7

Características

- Ninguna

Correcciones

- Se redujo el uso de memoria durante el manejo de programas que utilizan un comportamiento indefinido al consultar directorios

Hashes MD5

```
service.exe   = 7bf08deada69a09e2c0362337554c124
assistant.exe = ced782e4c6793e4b8a2ec2d4580b90f8
CCRRSecMon.sys (Windows10)       = 1eea1da529c0251a5438a0169ace53b7
CCRRSecMon.sys (Windows7)        = f82d5fbe2b22b70158dbbfb57949e948
CCRRSecMon.sys (Windows8)        = 9ff7406c41c583337357163a8dd8aeb2
```

Agente de Endpoint

4.4.2.8

Características

- Ninguna

Correcciones

- Aumento del registro y la telemetría para estados de máquina defectuosos
- Aumento de la estabilidad de las protecciones de identidad en el momento del arranque

Hashes MD5

```
service.exe   = 5f33211e1c36f31439a9d5efb8e7b029
assistant.exe = ced782e4c6793e4b8a2ec2d4580b90f8
CCRRSecMon.sys (Windows10) = 49c474f127041672509d31f013653259
CCRRSecMon.sys (Windows7) = 411f80c24854874d81b80a7d7af03ac9
CCRRSecMon.sys (Windows8) = fac1a12c4d1bbebd1e7ed1c21bf9fc2f
```

Agente de Endpoint

4.4.3.0

Características

- Además de las protecciones de servicio existentes, el controlador en modo kernel reiniciará el servicio si este se detiene por cualquier motivo.

Correcciones

- Ninguna

Hashes MD5

```
service.exe   = 65c8d59a22f376a8918347166def50a3
assistant.exe = ced782e4c6793e4b8a2ec2d4580b90f8
CCRRSecMon.sys (Windows7)        = 3a336be46b11c5875dda0e94340eb62a
CCRRSecMon.sys (Windows8)        = 8ddef1c798f94931ef8131674ad9ebf6
CCRRSecMon.sys (Windows10)       = 9fb3336a3c1990be3a1c4c3fdd8c53e2
```

Agente de Endpoint

4.4.3.2

Características

- Ninguna

Correcciones

- Se redujo el uso de CPU durante el inicio de procesos.
- Se redujo el uso de CPU en las determinaciones de confianza durante consultas consecutivas de directorios.

Hashes MD5

```
service.exe   = a1e5c45b87f914343c772c05e18b153e
CCRRSecMon.sys (Windows7)        = c995f7efeb88ef42425cf54b0b210dc7
CCRRSecMon.sys (Windows8)        = 3135a7787076286f3e8d82ca384582e9
CCRRSecMon.sys (Windows10)       = 0f6be8ec8806d4acabb8d03904c1b148
```

Agente de Endpoint

4.4.3.1

Características

- Ninguna

Correcciones

- Se corrigió un problema en algunas máquinas con características de instalación de Windows inusuales que presentaban canarios visibles en el Explorador.

Hashes MD5

```
service.exe   = b2a62cc2285afe01a28f4859afc03511
CCRRSecMon.sys (Windows7)        = 16b9d8946189feb7d620351a4d9c6a9f
CCRRSecMon.sys (Windows8)        = 24f55af4414447ec46f450eeca35c92e
CCRRSecMon.sys (Windows10)       = 2305ebd13864355ef384099dae1bee57
```

Agente de Endpoint

4.4.4.0

Funciones

- Los informes de incidentes y telemetría se almacenan en disco para escenarios sin conexión.
  - Debido a los intentos de manipulación observados contra múltiples almacenes de registro de EDR/XDR, Cyber Crucible habilitó la protección a nivel de kernel para los datos almacenados en disco antes de implementar esta capacidad.
- Mayor protección del proceso de servicio utilizado para la comunicación y las actualizaciones de backend, como parte del endurecimiento de confianza cero anticipatorio.
  - Esto no fue en respuesta a una amenaza existente, sino de forma proactiva ante una que el Equipo prevé próximamente.

Correcciones

- Se corrigieron los procesos que se cargan al arrancar y que no estaban disponibles en el panel bajo creaciones de procesos.
- Se impidió que dos instaladores se ejecutaran al mismo tiempo, lo cual registraría el mismo equipo dos veces.

Hashes MD5

```
service.exe                    = 116dab615aab07d804667b13ecfe821a
CCRRSecMon.sys (Windows7)      = db358b3d6e784d11827ff899722e3070
CCRRSecMon.sys (Windows8)      = a95dd87d2ea9944e8643de787f11d71c
CCRRSecMon.sys (Windows10)     = 6eb017a5cb3a9dd45bc065b466fb4789
```

Agente de Endpoint

4.4.4.4

Características

- Ninguna

Correcciones

- Rendimiento mejorado para el análisis de datos de certificados durante el inicio del sistema.

Hashes MD5

```
service.exe   = 69395e14240c91bc4df73168615927d9
CCRRSecMon.sys (Windows7)        = 2dd89c52e5a2914289371d4c3fd80ef8
CCRRSecMon.sys (Windows8)        = 41f25ea44e1f1a6ba11c7e7181554467
CCRRSecMon.sys (Windows10)       = ecc7f1f0a1d63f801a3a84f7b52b850c
```

Agente de Endpoint

4.4.5.1

Características

- Reducción del uso de ancho de banda:
  - Uso de compresión para datos de telemetría más grandes y respuestas del servidor más grandes
  - Uso de HTTP/2 para encabezados comprimidos y mayor eficiencia de sockets
- Mayor visibilidad de las operaciones de certificados.

Correcciones

- Codificación de los metadatos del certificado en la telemetría sin procesar cuando existen etiquetas no conformes con RFC. La infraestructura de seguridad de red estaba corrompiendo o eliminando las cargas útiles, lo que provocaba que el agente retransmitiera hasta lograr el éxito.

Hashes MD5

```
service.exe   = 686e91ca0f1bab7a0f3b09d2052d7e4c
CCRRSecMon.sys (Windows7)        = 25c194ee5f3c4ef25ef86124303aec82
CCRRSecMon.sys (Windows8)        = 6b4b8b6cc960a718464fd3ebb89b1fe8
CCRRSecMon.sys (Windows10)       = 8c668fe57652530d77d323b8563d3f4e
```

Agente de Endpoint

4.4.5.2

Características

- Nueva telemetría de acceso a nivel de kernel para comportamientos basados en red, con el fin de identificar mejor posibles errores de red del lado del cliente, u oportunidades de optimización
- La telemetría saliente ahora se agrupa y se envía en conjunto, al igual que la configuración entrante
  - Transmitida con una variación de tiempo del 25%, para que no todas las máquinas envíen paquetes simultáneamente a través de una red de clientes
- HTTP/2 ahora se utiliza completamente de extremo a extremo

Correcciones

- Se redujo el número mínimo de subprocesos en uso en el espacio de usuario
- Se redujo el uso de CPU para el servicio de espacio de usuario
- La autenticación Agente-Servidor ahora se realiza de manera más eficiente
- Se reemplazó el algoritmo anterior de suspensión <> reinicio del servicio cuando las licencias no estaban disponibles.
  - El algoritmo anterior causaba un "el servicio finalizó inesperadamente" en el administrador de eventos cada 15 minutos.
  - Permitir que el sistema operativo indique al servicio que se apague (algo que ha sido explotado por delincuentes y otras herramientas de seguridad) habría permitido un reinicio "limpio" del servicio sin registros en el administrador de eventos. En lugar de crear esa vulnerabilidad, el servicio de Cyber Crucible se reinició por sí mismo sin la intervención de Windows, provocando el registro de eventos.

Hashes MD5

```
service.exe  = b17a2a528a4424771fdeca8559b9f56b
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Agente de Endpoint

4.4.5.3

Características

- Se agregó un segundo dominio para la comunicación con el servidor (vea la lista de dominios aquí).
  - Si hay problemas de comunicación con un dominio, el agente cambiará automáticamente al otro.

Correcciones

- Se cambiaron algunas cadenas antiguas heredadas que hacían referencia a “Ransomware Rewind” para que ahora hagan referencia a “Cyber Crucible”.

Hashes MD5

```
service.exe  = 8cf710b96d15ec9ff0b88bba12dcd142
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Agente de Endpoint

4.4.5.9

Funciones

- Se ha aumentado el endurecimiento de partes de la funcionalidad previamente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son gestionadas por el controlador del kernel de Cyber Crucible.
  - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.
- Este es un lanzamiento importante (milestone) respecto a los lanzamientos incrementales encontrados en 4.4.5.4 - 4.4.5.8, todos alineados con la funcionalidad de endurecimiento de análisis criptográfico anterior.
  - La telemetría inicial indica que los fallos en las bibliotecas de certificados y criptografía de Windows fueron respondidos legítimamente por Cyber Crucible.
  - En este momento se desconoce qué porcentaje de los problemas se debió a explotación frente a un error en la biblioteca central de Windows. Póngase en contacto con su representante de Cyber Crucible para conversar más al respecto según sea necesario.

Correcciones

- Se corrigieron algunos informes de procesos que indicaban incorrectamente el certificado listado como “no confiable”, debido a una pérdida de funcionalidad en la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe  = 79650eea0a93b8f480b4247d57ddd03b
CCRRSecMon.sys (Windows7)        = 06a647c897f9f385416482a4e899e204
CCRRSecMon.sys (Windows8)        = 72c1b462e3e8e3fa4dcf6344ce3b0acd
CCRRSecMon.sys (Windows10)       = 02b1c53268059ae38427fe43152d593c
```

Agente de Endpoint

4.4.5.8

Funciones

- Se incrementó el endurecimiento (hardening) de partes de la funcionalidad previamente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son realizadas por el controlador (driver) de kernel de Cyber Crucible.
  - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado no era “de confianza”, debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe  = d8187cf4468cba634470772fe8e7ba8b
CCRRSecMon.sys (Windows7)        = b97b6bc79529be5ccd88807892e16153
CCRRSecMon.sys (Windows8)        = 6a6b5801b5a4552a4be8477d74706198
CCRRSecMon.sys (Windows10)       = 4f3e54c2a9d348b0279767bc03420c99
```

Agente de Endpoint

4.4.5.5

Funcionalidades

- Mayor fortalecimiento de partes de la funcionalidad previamente realizadas por las bibliotecas de criptografía de Windows, ahora realizadas por el controlador del kernel de Cyber Crucible.
  - Esto constituye tanto un fortalecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió el hecho de que algunos informes de procesos indicaban incorrectamente que el certificado listado era “no confiable”, debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe  = 90525bbf61ae57bd5e61f79198ae031f
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Agente de Endpoint

4.4.5.6

Funciones

- Se ha aumentado el endurecimiento de partes de la funcionalidad previamente realizadas por las bibliotecas de criptografía de Windows, las cuales ahora son realizadas por el controlador del kernel de Cyber Crucible.
  - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado era “no confiable”, debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe  = 60c0b7b7d00dc14415334ddef590f593
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Agente de Endpoint

4.4.5.7

Funcionalidades

- Se ha incrementado el endurecimiento de partes de la funcionalidad anteriormente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son gestionadas por el controlador del núcleo de Cyber Crucible.
  - Esto representa tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado no era de confianza (“not trusted”), debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe  = c97ce96b69c0be846af70c2359671e22
CCRRSecMon.sys (Windows7)        = 475915b1881add45c6af260f82bd43b9
CCRRSecMon.sys (Windows8)        = dfc09e7504b4aa73ecfb15e62f8cde86
CCRRSecMon.sys (Windows10)       = 5581c7c11aa52488a1858fa728cfaf46
```

Agente de Endpoint

4.4.5.4

Características

- Se ha aumentado el endurecimiento de partes de la funcionalidad anteriormente realizada por las bibliotecas de criptografía de Windows, las cuales ahora son realizadas por el controlador del kernel de Cyber Crucible.
  - Esto incluye tanto un endurecimiento general como un aumento en la telemetría que indica posibles ataques contra las bibliotecas y API de criptografía de Windows.

Correcciones

- Se corrigió un problema por el cual algunos informes de procesos indicaban incorrectamente que el certificado listado no era de confianza (“not trusted”), debido a la pérdida de funcionalidad de la biblioteca de certificados de Windows.

Hashes MD5

```
service.exe  = fd2157d8dee1d07ec45406a1d323359c
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Agente de Endpoint

4.4.6.0

Funciones

- Mejora del rendimiento de la CPU para algunas aplicaciones que generan grandes cantidades de recorridos de directorios automatizados y simultáneos como parte del comportamiento de sus aplicaciones.

Correcciones

-

Hashes MD5

```
service.exe  = 3e443b55efdf1c1fd10a2b2931aa1bfd
CCRRSecMon.sys (Windows7)        = eb992a496b88874e59d71f8ad83ba917
CCRRSecMon.sys (Windows8)        = 2e9786c84a55911e1b94aec38b4a90ff
CCRRSecMon.sys (Windows10)       = c68c4d4ba3f2e42953e6550b5e7c0b47
```

Agente de Endpoint

4.4.6.1

Funcionalidades

- Continuación de la migración del nombre de producto “Ransomware Rewind” a “Cyber Crucible”.
  - El nombre del servicio heredado `"Ransomware Rewind"` migrará a `"CyberCrucibleAgent"`. El nombre del proceso permanece igual.
  - La clave de registro en `HKLM\SOFTWARE` migrará de la heredada `RansomwareRewind` a la actual `CyberCrucibleAgent.`

Correcciones

- Se corrigió que algunos procesos de 32 bits se activaran como si tuvieran “memoria modificada” cuando la imagen del proceso alcanza el tamaño máximo permitido para un proceso de 32 bits.

Hashes MD5

```
service.exe  = 51ff73ab3caac8d269d1fad823de9f60
CCRRSecMon.sys (Windows7)        = 6014b3fa07cec7e39753f7eaea4d1ea7
CCRRSecMon.sys (Windows8)        = 26756d6394a70482952519c104730676
CCRRSecMon.sys (Windows10)       = 8665c9f7b99b385acaecc11d42fda468
```

Agente de Endpoint

4.4.6.2

Funciones

- Se agregaron indicadores opcionales de “tipo de acceso” expuestos a los usuarios finales para mayor especificidad de acceso conductual.

Correcciones

- Ninguna.

Hashes MD5

```
service.exe  = 07a709d672f38ea466de675b8c8f1b76
CCRRSecMon.sys (Windows7)        = 4d9195aeda4ae5dafb6f27405b541d9a
CCRRSecMon.sys (Windows8)        = 12deea5a512128e62aba173c2f786387
CCRRSecMon.sys (Windows10)       = 39daf75dd7678ae2b83a5f79aeab3b68
```

Agente de Endpoint

4.4.6.3

Características

- Se agregó compatibilidad opcional con proxy SOCKS5 para ayudar en la implementación del agente.

Correcciones

- Se corrigieron las reinstalaciones desde agentes anteriores que utilizaban un ID de instalación incorrecto.
- Se corrigió que las instalaciones existentes provenientes de instaladores anteriores tuvieran una ruta de servicio sin comillas.

Hashes MD5

```
service.exe  = 610b75a1a4fc7460138f545751cc7606
CCRRSecMon.sys (Windows7)        = 4d9195aeda4ae5dafb6f27405b541d9a
CCRRSecMon.sys (Windows8)        = 12deea5a512128e62aba173c2f786387
CCRRSecMon.sys (Windows10)       = 39daf75dd7678ae2b83a5f79aeab3b68
```

Agente de Endpoint

4.4.6.4

Características

- La información de memoria del proceso principal está disponible para los informes de procesos cuando se detectaron modificaciones.

Mejoras

- Se modificaron algunas frecuencias de comunicación con el servidor para que ya no requieran reinicio para su ajuste.

Correcciones

Ninguna en esta versión.

Hashes MD5

```
service.exe  = 608ab69e92f5592a3da66801edaafd0e
CCRRSecMon.sys (Windows7)        = 090b0b8decd4634797de4acf3aef05ae
CCRRSecMon.sys (Windows8)        = d993e733702bc810de9139965850e210
CCRRSecMon.sys (Windows10)       = 65a48c062156b4723894783fa9115204
```

Agente de Endpoint

4.4.7.0

Características

- Inicio de la implementación de comunicaciones HTTPS basadas en JWE.
  - Las claves de cifrado son únicas para cada agente.
  - Todas las cargas útiles cifradas bajo el HTTPS. Deshabilitado de forma predeterminada durante la implementación inicial.
  - Capacidad de revertir opcionalmente de HTTPS cifrado con JWE a HTTPS no cifrado si las cargas útiles con formato JWE no se transmiten correctamente.

Hashes MD5

```
service.exe  = 581a528318644c55d9dc6d552fb295c0
CCRRSecMon.sys (Windows7)        = 629e77591a672915021842a9f5271157
CCRRSecMon.sys (Windows8)        = 3f499538502e0b7c4fe956eb7b4bd0ab
CCRRSecMon.sys (Windows10)       = 0f7db98f84a6f67aac02dd4eb2dbd547
```

Agente de Endpoint

4.4.7.1

Características

- Más telemetría para creaciones de procesos e incidentes
  - SID de usuario
  - Nombre de inicio de sesión de nivel inferior del usuario
  - Si el proceso está elevado o no (Ejecutar como administrador)
- Los incidentes ahora informan dónde ocurrió el acceso iterativo a datos

Correcciones

- Reducción del uso de memoria durante períodos de problemas de conectividad con el servidor y de gran volumen de telemetría simultánea
- Reducción del uso de memoria durante la generación de informes de incidentes

Hashes MD5

```
service.exe  = 0df0b7d76abd0978734ac961cd4cddaf
CCRRSecMon.sys (Windows7)        = dced5933e7b3e720a72160eb32cd83cb
CCRRSecMon.sys (Windows8)        = e14aa1324a9a42958cd955b9fffd4f79
CCRRSecMon.sys (Windows10)       = 9d2edcf2288e7563892dac6300517102
```

Agente de Endpoint

4.4.7.3

Características

- Modo DMZ
  - Configuración opcional para utilizar un paquete de CA firmado para la comunicación TLS con los servidores de autenticación y telemetría. Estos paquetes de CA quedan protegidos contra manipulación o eliminación mediante las capacidades antimanipulación propietarias de Cyber Crucible.
  - Las comprobaciones OCSP y CRL están deshabilitadas para reducir la lista de dominios que deben permitirse a través de un firewall.

Correcciones

- Se redujo el uso de memoria y el tiempo de CPU dedicado al envío de diferencias de memoria (memory diff), especialmente después de períodos prolongados sin conexión.

Hashes MD5

```
service.exe  = 536adc06bd5ac3d4caca53dd5b780759
CCRRSecMon.sys (Windows7)        = dc446d663e8c865b039de0eb585de1fb
CCRRSecMon.sys (Windows8)        = ea96fdf4b097ac9afb646e6a766431aa
CCRRSecMon.sys (Windows10)       = 434c9061390804e4e61f5299158aaa00
```

Agente de Endpoint

4.4.8.0

Características

- Telemetría de Authenticode en modo kernel
  - Para aumentar la velocidad y la fiabilidad, los datos de certificados para las creaciones de procesos e incidentes serán registrados únicamente por el controlador.
  - Esta actualización no elimina las dependencias de las bibliotecas de criptografía de Windows, pero realiza los cálculos criptográficos en paralelo. Eventualmente, la dependencia de Windows podría eliminarse por completo.

Correcciones

- Reducción del uso de memoria y del tiempo de CPU dedicado a los intentos de envío de eventos cuando se está sin conexión, durante los cuales la telemetría se almacena de forma segura hasta que el equipo recupera la conectividad con los servidores de Cyber Crucible.
- Algunos instaladores de controladores de Nvidia consideraban que no tenían privilegios para instalarse debido al uso de una función interna del kernel de Microsoft para intentar acceder a los archivos instalados de Cyber Crucible.
- Se corrigió una incompatibilidad entre el modo JWE y el modo DMZ

Hashes MD5

```
service.exe  = 5189fe49a1bfade50766fce2a1980eef
CCRRSecMon.sys (Windows7)        = 342dd1bbe5f5dfcffe7752b74b34a9e8
CCRRSecMon.sys (Windows8)        = a20c9cca59be651db7ae69f9f1f64cf2
CCRRSecMon.sys (Windows10)       = a3cf6860d3f059a1ab38ee7b2d82b097
```

Agente de Endpoint

4.4.8.1

Características

- Los metadatos ejecutables, como la versión del producto, el nombre de la empresa, etc., para los procesos en memoria son informados por el controlador mediante visibilidad a nivel de kernel. La funcionalidad normal es utilizar llamadas a la API de Windows en espacio de usuario. Este cambio hacia el análisis en el kernel elimina la oportunidad (observada) de que los atacantes manipulen la información del proceso.
- La información de autenticación del agente se replica en otra parte del sistema para poder restaurarla en caso de que el registro sea corrompido por un controlador malicioso.

Mejoras

- Los errores de conexión al servidor son registrados de forma mínima por el agente, reduciendo el tamaño del registro en disco.

Correcciones

- N/A

Hashes MD5

```
service.exe  = 8c1f6999ccd176193e493686216f14c6
CCRRSecMon.sys (Windows7)        = 3b032d0e43674509126c6cb1c9efd688
CCRRSecMon.sys (Windows8)        = d3131131c83c2cf833ebc2157149c364
CCRRSecMon.sys (Windows10)       = eac8a8b38a8743a13dd7130509de9907
```

Agente de Endpoint

4.4.8.2

Funciones

- Se agregó soporte para un icono opcional en la bandeja del sistema. Esta función está deshabilitada de forma predeterminada.

Correcciones

- Se agregó una solución alternativa para un problema relacionado con las solicitudes de hashing de la API de Windows del kernel. Esta solución alternativa podría eliminarse en algún momento en el futuro si se corrige el problema de Windows, posiblemente en la próxima actualización del kernel.

Hashes MD5

```
service.exe  = 6e21b0a7c41b156f2001c93bbcd142de
CCRRSecMon.sys (Windows7)        = 43cce21323465eac015fc7c90b88ac87
CCRRSecMon.sys (Windows8)        = c7b2d8d130f8c3e768891ad0b20931a5
CCRRSecMon.sys (Windows10)       = d95d162bc7f87f3eaef46d58eb543364
```

Agente de Endpoint

4.4.9.0

Características

- Telemetría de DLL en modo kernel
  - Análisis de certificados y cálculo de confianza para todas las DLL cargadas en el controlador.

Correcciones

- Ninguna.

Hashes MD5

```
service.exe  = f4e017fab1f1117859bcfcd4733cc439
CCRRSecMon.sys (Windows7)        = 976f8826ebd5bacb1803fcf6d274a6d0
CCRRSecMon.sys (Windows8)        = 90f02751eca65f6286b3676ea8b2bb2c
CCRRSecMon.sys (Windows10)       = af9c0469fb05a0104579d8fb1694719e
```

Agente de Endpoint

4.4.9.1

Funciones

- Ninguna.

Correcciones

- Se aumentó la cantidad de telemetría gestionada a la vez por el servicio para los datos de creación e inyección.
- Se ajustó el orden de los canarios para programas que utilizan métodos inusuales de iteración de archivos.
- Se ajustó la ACL en algunos canarios para adaptarse mejor a los sistemas de archivos reales.

Hashes MD5

```
service.exe  = 5728b771c4b89d47942043fece634be9
CCRRSecMon.sys (Windows7)        = fd1b9163edfcfa66370a0510286de6bf
CCRRSecMon.sys (Windows8)        = c7bf417fdd2f2f0fdec9a9011913b672
CCRRSecMon.sys (Windows10)       = 22066d3fcf90b3a0e672a41d8fe787d8
```

Agente de Endpoint

4.4.9.2

Funciones

- Seguimiento de modificaciones de memoria para DLL cargadas.
- Generación de diferencias de memoria (memory diff) para DLL modificadas.

Correcciones

- Se solucionó un problema por el cual algunas DLL no conformes generaban resultados incorrectos de hash de authenticode.

Hashes MD5

```
service.exe  = 7b76a84809347d1caa4f46217d7c02ad
CCRRSecMon.sys (Windows7)        = 27cc77a22706f1f007f0c8f433910efd
CCRRSecMon.sys (Windows8)        = d94978e73452be5869b194fe234fc125
CCRRSecMon.sys (Windows10)       = c321cf4abafbd8f2b6d3ef1917904d57
```

Agente de Endpoint

4.4.9.4

Correcciones

- Los archivos de volcado del servicio ahora están limitados a 10 por combinación de versión + subproceso.

Hashes MD5

```
service.exe  = TBD
CCRRSecMon.sys (Windows7)        = 27cc77a22706f1f007f0c8f433910efd
CCRRSecMon.sys (Windows8)        = d94978e73452be5869b194fe234fc125
CCRRSecMon.sys (Windows10)       = c321cf4abafbd8f2b6d3ef1917904d57
```

Agente de Endpoint

4.5.0.0

Características

- Firewall de Kernel con IA
- Mejoras de velocidad en el cálculo de hash Authenticode
- Uso de memoria significativamente reducido para la telemetría de DLL
- Mayor visibilidad de las modificaciones de memoria en las DLL

Correcciones

- Corrección de la compatibilidad de recuperación del servicio con 24H2

Hashes MD5

```
service.exe  = 2a01dc8267e6bbae3c42c0f0d873286f
CCRRSecMon.sys (Windows7)        = 502b85e17a7103a35d5b6eb50ce0eea7
CCRRSecMon.sys (Windows8)        = 65c315313330c83f602d19e031d99f67
CCRRSecMon.sys (Windows10)       = d17ba3cde6c2051d85dea395891caff9
```

Agente de Endpoint

4.5.0.1

Características

- Opción para migrar al dominio del servidor de autenticación OAuth alojado
- Tarea para configurar dinámicamente las URL de los servidores REST y OAuth

Correcciones

- Ninguna.

Hashes MD5

```
service.exe  = 171e15eb5bf2a8c2d5f13ef6711d09d0
CCRRSecMon.sys (Windows7)        = 502b85e17a7103a35d5b6eb50ce0eea7
CCRRSecMon.sys (Windows8)        = 65c315313330c83f602d19e031d99f67
CCRRSecMon.sys (Windows10)       = d17ba3cde6c2051d85dea395891caff9
```

Agente de Endpoint

4.5.0.2

Funciones

- Ninguna.

Correcciones

- Se redujo la memoria utilizada para AI Kernel Firewall.
- Uso más rápido de los nuevos puntos de conexión de autenticación.
- Se eliminaron las llamadas a icanhazip.com, previamente opcionales pero ya no necesarias.

Hashes MD5

```
service.exe  = 716d0a77b44e612342007d64cb1b54aa
CCRRSecMon.sys (Windows7)        = 754908e2775c1e88e2ca693e8fc4f71b
CCRRSecMon.sys (Windows8)        = 50c180de6862f4741fa6569736b61c97
CCRRSecMon.sys (Windows10)       = b3a32b9d639f481aa14a36bfe2f37092
```

Agente de Endpoint

4.5.0.3

Funciones

- El indicador de la bandeja de estado ahora muestra el estado de autoconfiguración para nuevas instalaciones.

Hashes MD5

```
service.exe  = 517b27279ea728223d6dd32ecb90f2e5
CCRRSecMon.sys (Windows7)        = 754908e2775c1e88e2ca693e8fc4f71b
CCRRSecMon.sys (Windows8)        = 50c180de6862f4741fa6569736b61c97
CCRRSecMon.sys (Windows10)       = b3a32b9d639f481aa14a36bfe2f37092
```

Agente de Endpoint

4.5.1.0

Características

- Ahora se utiliza OpenSSL para la comunicación TLS.
  - Esto debería evitar problemas en versiones de sistemas operativos más antiguos que ya no reciben parches para los nuevos requisitos de TLS.

Correcciones

- Se mejoró la compatibilidad de análisis para firmas Authenticode no conformes.

Hashes MD5

```
service.exe  = b19823fcc66eef583fa4dc3e2f16a6d6
CCRRSecMon.sys (Windows10)       = 0f27455b5ca7c7e028e1a4ce6a7d7f68
CCRRSecMon.sys (Windows8)        = 0ac88365a3585ae79928a337900ae16b
CCRRSecMon.sys (Windows7)        = 041f03d5e37154f183deb5af7b89bc6b
```

Agente de Endpoint

4.5.1.2

Características

- Se eliminó la validación de certificados heredada que dependía de bibliotecas de Windows integradas y lentas.
- Se agregó la capacidad de conservar los registros al desinstalar.

Hashes MD5

```
service.exe  = fe8a70286926dba3b6277a9cdf446c38
CCRRSecMon.sys (Windows10)       = d4e458f3960a7b1c4b6d06ce4d062f1e
CCRRSecMon.sys (Windows8)        = 1f090bc190b80c9c08b03a1017381e6c
CCRRSecMon.sys (Windows7)        = 592020ee1f145357c3b77c681ebb3bac
```

Agente de Endpoint

4.5.2.1

Funcionalidades

- Lanzamiento amplio de informes para el acceso a Fortress AI

Correcciones

- Optimización de las operaciones del núcleo de Cyber Crucible que no utilizan las API de Windows para contrarrestar el aumento de latencia en algunos entornos Windows en aproximadamente un 20%.

Hashes MD5

```
service.exe  = 6ddad1f20f43e8ba799b562235363ceb
CCRRSecMon.sys (Windows10)       = d9c81609fafd99957063b2b6574b4a3c
CCRRSecMon.sys (Windows8)        = 429dd8f9e39fe8e3bad6b5592dea91f9
CCRRSecMon.sys (Windows7)        = 1f6aa2cf085e710c01a0347d6f4489d2
```

Agente de Endpoint

4.5.2.2

Correcciones

- Optimización de las operaciones del kernel de Cyber Crucible mediante la evitación de capacidades problemáticas del núcleo del sistema operativo relacionadas con eventos de Windows y el bus de datos.

Hashes MD5

```
service.exe  = a4bfeca13496d47c8b91121a5da2b3b8
CCRRSecMon.sys (Windows10)       = 042d39305b91caff229605c3a043a24b
CCRRSecMon.sys (Windows8)        = 429dd8f9e39fe8e3bad6b5592dea91f9
CCRRSecMon.sys (Windows7)        = 1f6aa2cf085e710c01a0347d6f4489d2
```

Agente de Endpoint

4.5.3.0

Funciones

- FortressAI
  - Se agregaron notificaciones cuando se informa una infracción de política
    - Integración con el Centro de notificaciones de Windows
  - Se agregó una interfaz gráfica para ver el historial de notificaciones de políticas
  - Se agregó el modo de simulación
- Cyber Crucible Core
  - Análisis asíncrono configurable de DLL para equipos con recursos de hardware mínimos
  - Análisis y telemetría de creación de procesos
    - ahora utiliza persistencia en disco
    - se eliminaron las dependencias de Windows MiniFilter
  - Análisis y telemetría de inyecciones de procesos
    - ahora utiliza persistencia en disco
    - se eliminaron las dependencias de Windows MiniFilter
  - Se eliminaron dependencias adicionales de recursos del kernel de Windows

Correcciones

- Optimización de los informes de telemetría para lograr informes aún más rápidos
- Se eliminó un bloqueo mutuo (deadlock) debido al acceso exclusivo frente al acceso compartido a un recurso específico del kernel requerido por Microsoft Defender cuando Defender habilita el modo de depuración del controlador

Hashes MD5

```
service.exe  = 37ba9005bb7dc8a8e5b86670dd02f5dd
CCRRSecMon.sys (Windows10)       = aabc6d7299e2c5da21784f12b8836647
CCRRSecMon.sys (Windows8)        = 678bb0459a74030dcaab19646141fde7
CCRRSecMon.sys (Windows7)        = 07d4c04a12da5979dd8f2d7347669887
```

Agente de Endpoint

4.5.3.1

Funciones

- FortressAI
  - Detecta intentos de eludir los controles de política mediante el uso de capturas de pantalla.
- Cyber Crucible Core
  - Admite la reinicialización de la identidad de un agente sin necesidad de una reimplementación completa.
    - Esto soluciona situaciones en las que una máquina con Cyber Crucible instalado se clona, clonando así la licencia y los identificadores del agente. Al igual que con las direcciones IP, las direcciones MAC, los nombres de máquina y otros identificadores únicos, Cyber Crucible identifica un agente clonado y alerta a los administradores de CC sobre la posibilidad de generar nuevos identificadores de CC.

Hashes MD5

```
service.exe  = 5db5b2dfe65b9908c93d04a136123c98
CCRRSecMon.sys (Windows10)       = e4a27842cc4352cffaea780116e5ae00
CCRRSecMon.sys (Windows8)        = 060170a2cfff082c2092dc99a8330717
CCRRSecMon.sys (Windows7)        = 63a39eb153298766a3ff7034eaafa5af
```

Agente de Endpoint

4.5.3.2

Características

- FortressAI
  - Ninguna
- Cyber Crucible Core
  - Mejora de la operación del búfer del kernel
    - El controlador utiliza búferes para almacenar temporalmente la telemetría que finalmente se envía al panel del cliente. Esta actividad es distinta de la población o las operaciones del modelo de comportamiento.
    - Si un búfer del kernel se sobrecarga, la carga de CPU del sistema aumenta.
      - Esto solo ocurriría debido a un gran error del sistema operativo o a un ataque a los sistemas.
      - La notificación automática al cliente sobre un uso de búfer muy alto estará disponible el 1 de junio de 2026.
    - Casi todas las operaciones del búfer del kernel de CC corresponden a tres búferes principales.
    - El porcentaje de uso de los tres búferes principales ahora se transmite a la infraestructura de CC para la recopilación de métricas y la identificación del uso de búfer por agente.
    - Los tres búferes principales pueden ajustarse en tamaño de forma remota, y los usuarios pueden hacer seguimiento de su estado.

Correcciones

- Una actualización reciente relacionada con las bibliotecas redistribuibles de DotNet y MSVC saturó los búferes de Cyber Crucible con eventos sostenidos y muy altos (500%+) de operaciones de procesos y DLL, lo que afectó a algunos clientes. Aunque el uso del búfer ha vuelto al nivel normal del 1-5%, incluidos los clientes afectados, se duplicó el tamaño de todos los búferes para prevenir posibles problemas futuros. Esto se suma a las capacidades de configuración mencionadas anteriormente.

Hashes Sha-256

```
service.exe  = 2f46657af8809339d16546f1e6f2b58975bbf4d5c10fde3510363d628b129492
fai-alert.exe  = 890ccca7e0ce14a0e2ff7f90bae75a7ef12ad6c8cd43ffb52093c8431e65770b
CCRRSecMon.sys   = d0e941bc25d31e38cbebbe9ce3918f82d0b9c7b433efed318cb34e36a50acf94
CCRRSecMon.inf   = db54d8077afdfef81286868f7bda1e8df17dbd812178ddac989127550a904a8c
ccrrsecmon.cat   = a01c31db7231fed3852c9e559eb2c3f7496a016982207c102b88d8b36dcb0486
```

Middleware (servidores REST)

Middleware 01.23

Funcionalidades

- Se implementó el controlador para las licencias de formación y se agregó un servicio de vencimiento de licencias de formación.
- Se actualizó cada endpoint para tener en cuenta la nueva funcionalidad de modo de formación de la aplicación web, junto con pruebas para cada endpoint en el modo de formación.
- Se agregó un endpoint para restablecer todos los datos de formación de un grupo principal a su estado original.
- Se implementaron los endpoints para la nueva configuración de política de vencimiento de contraseñas para grupos.
- Se está agregando documentación para los endpoints de Reactive Springboot.

Middleware 04.23

Características

- Actualizaciones del Portal de Socios:
  - Se implementaron los endpoints para el nuevo proceso de Registro de Acuerdos (Register Deal) con aprobación de acuerdos por parte de Cyber Crucible
  - Se actualizó el modelo PartnerDeal para que tenga un tipo asociado a los acuerdos, cada uno con un porcentaje de descuento asociado
    - También se actualizó el modelo PartnerDeal para los acuerdos de tipo Referido, a fin de almacenar la Cuenta de Usuario del Dashboard que se asociará con las licencias del acuerdo
  - Se actualizó el modelo PartnerDeal para poder separar la facturación Mensual frente a la Anual en el pago de los acuerdos
    - Incluye la actualización de los endpoints existentes para tener en cuenta la facturación Mensual frente a la Anual en Stripe
  - Se implementaron endpoints para poder enviar cotizaciones a través de Stripe para un acuerdo
  - Se implementó un endpoint para reenviar la factura de Stripe de un acuerdo
  - Se implementó un endpoint para editar múltiples campos de un acuerdo al mismo tiempo, asociado con el modal de edición de acuerdos en la Aplicación Web
- Gestión de Agentes/Licencias:
  - Se implementó un endpoint para asignar licencias de forma masiva a los agentes
  - Se implementó un endpoint para cambiar la configuración de re-licenciamiento automático para un agente determinado
  - Se implementó un endpoint para liberar una licencia de un agente pasando el agentId en la solicitud
- Se implementaron endpoints para recuperar y guardar la configuración de usuario que muestra el ícono de configuración del script del instalador en la cuadrícula de Grupos
- Se implementó un endpoint para recuperar el valor de Autenticación de Cliente del Script del Instalador del Agente para un grupo
- Se actualizó nuestro Servicio de Escaneo de AV para buscar también en la colección de incidentes de identidad, además de la colección de creación de procesos
- Varias actualizaciones a nuestra lista de datos predeterminados + listas blancas de identidad para los AV.
- Se implementó un nuevo endpoint de flujo de cambios (change stream) para detectar nuevas inserciones de Respuesta a Extorsión
- Se implementó un endpoint para copiar listas blancas a otro grupo
- Se implementó un endpoint para descargar el Archivo de Diferencia de Memoria (Memory Diff File) de un incidente

- Se implementó la categorización de los programas de incidentes de identidad en aplicaciones
- Se implementó el guardado de los modos de columna para cada cuadrícula de página web y el guardado de la configuración de visibilidad de los gráficos

Middleware 08.23

Características

- Actualizaciones del Portal de Socios:
  - Se implementaron endpoints para poder crear un POC para acuerdos de socios aprobados
  - Se implementaron endpoints para la página de Gestión de Grupos de Distribuidores en la Aplicación Web
  - Se implementó un endpoint para devolver los datos de la cuadrícula de Gestión de Pagos en la Aplicación Web
  - Se implementó la capacidad de cambiar el propietario de un acuerdo de socio
  - Se implementó la capacidad de establecer una nota personalizada para los acuerdos de socios que aparecen en las facturas y cotizaciones de Stripe
- Se implementó un endpoint para poder reenviar invitaciones de cuentas de usuario
- Se agregaron más opciones de etiquetado de aplicaciones para objetos de Acceso de Identidad
- Se actualizó el modelo de Grupo para grupos de socios para tener nuevos campos booleanos según el tipo de socio
- Se actualizó el modelo de Grupo para tener una lista de configuraciones de extensión canary
- Diversas actualizaciones a nuestra lista de listas blancas predeterminadas de datos + identidad + certificados para antivirus
- Habilitación del soporte HTTP/2
- Actualización de nuestro Spring Boot a la última versión, junto con otras diversas dependencias
- Se implementaron alertas de notificación para Accesos de Identidad Anómalos
- Se habilitó la compresión de respuestas del servidor para los agentes
- Se implementó el filtrado para la columna Sin Certificado Confiable de la cuadrícula de Acceso de Identidad en la Aplicación Web para las opciones "Desconectado al Recuperar Información del Certificado" y "Tiempo de Espera Agotado al Recuperar Información del Certificado"
- Se corrigió un problema en nuestro servicio de notificación de vencimiento de acuerdos de socios para no enviar correos de vencimiento para acuerdos completados

Middleware 11.23

Funciones

- Actualizaciones de la lista blanca
  - Se implementó la capacidad de crear una excepción con la ruta y los argumentos del programa principal
  - Se implementó la capacidad de crear una excepción para coincidir con respuestas de extorsión cuando solo hay certificados de confianza, coincidir solo cuando no hay inyecciones relacionadas, y coincidir solo cuando no hay memoria modificada
  - Se implementó la capacidad de crear una excepción para coincidir con desencadenantes de acceso a archivos específicos
- Se implementó la configuración de grupo para liberar automáticamente las licencias de los agentes inactivos
  - Se actualizó el modelo de Grupo para tener una configuración sobre cuándo liberar las licencias de los agentes inactivos en el grupo. Las opciones son 30/60/90 días, o desactivar esta configuración
  - Se actualizó el modelo de Agente para tener un nuevo estado inactivo
  - Se implementó un servicio para liberar automáticamente las licencias de los agentes inactivos según la configuración de su grupo
- Se actualizó el endpoint para la recuperación de respuestas de extorsión para incluir la ruta y los argumentos del programa principal
  - La ruta y los argumentos del programa principal ahora también se incluyen en los recuentos de respuestas de extorsión únicas para la Aplicación Web, las alertas de Notificación de Seguridad y los Resúmenes Ejecutivos
- Se actualizaron nuestros Informes de Resumen Ejecutivo para separar la diapositiva de Licencias en diapositivas individuales de Licencias de Escritorio y de Servidor
- Se actualizó el modelo de Notificación de Seguridad por Correo Electrónico y el servicio de Notificación de Seguridad para incluir dos nuevos tipos de alerta
  - Modelo de Comportamiento Ajustado
  - Nueva Versión del Agente
    - Cuando se cambia la configuración de actualizaciones administradas de un grupo para desactivar la actualización automática, se crea automáticamente una notificación de Nueva Versión del Agente para el grupo
- Actualizaciones de Roles/Permisos de Usuario
  - Se actualizaron los permisos del modelo de Rol de Gestor de Incidentes para que ahora solo tenga visualización/edición para listas blancas y reglas de respuesta silenciosa
  - Los grupos ahora tienen 3 roles predeterminados que no son editables por el usuario:

    - Administrador
    - Solo lectura
    - Invitado
  - Los usuarios agregados a un grupo se asignan por defecto al Rol de Invitado
- Se implementaron endpoints para el Modal de Ajuste del Proceso de Utilidad del Navegador de la Aplicación Web para gestionar fácilmente cómo deben responder los agentes en los grupos a los procesos de utilidad de chrome
- Se actualizó el endpoint para el gráfico de la página de Agentes para poder limitar los recuentos a los agentes que se han conectado en los últimos 30/60/90 días
- Se actualizó la alerta por correo electrónico de Notificación de Seguridad de Actividad de Ransomware para incluir un enlace que redirigirá automáticamente a los usuarios a la página de Respuestas de Extorsión con un filtro para mostrar las respuestas a las que se refería la alerta
- Se implementó la configuración de grupo para que los agentes de un grupo se ejecuten o no en modo seguro
- Se implementó una opción de script de powershell para la instalación de agentes
- Actualización de nuestro Spring Boot a la última versión
- Diversas actualizaciones a nuestra lista de listas blancas predeterminadas de datos + identidad + certificados para los antivirus

Middleware 04.24

Funciones

- Se implementó la configuración de grupo y los endpoints relacionados para la configuración y gestión de configuraciones de proxy, con el fin de facilitar la implementación de agentes
- Se actualizaron nuestros endpoints de datos de telemetría para poder visualizar todos los datos de telemetría o solo los datos directamente relacionados con una respuesta a extorsión
- Se implementó la configuración de grupo para ocultar automáticamente los agentes en grupos cuando se libera una licencia de un agente, un agente se marca como inactivo o un agente completa una desinstalación
- Se actualizaron los enlaces a nuestro panel en nuestros correos electrónicos de notificación para incluir un parámetro de URL utilizado para filtrar automáticamente los datos en la cuadrícula del frontend relacionada, mostrando lo que activó la notificación
- Se actualizó el endpoint utilizado para el gráfico de Licencias de Agentes del frontend para incluir los recuentos tanto de licencias de Escritorio como de Servidor
- Se implementaron endpoints para la nueva página del frontend de Estado de Implementación del Cliente
- Se actualizó nuestro ajuste de procesos para tener en cuenta Microsoft Edge WebView

Middleware 09.24

Funcionalidades

- Se implementaron los endpoints para la nueva configuración del Modo DMZ de Grupo
- Se actualizaron los endpoints de Registro de Operaciones para poder registrar acuerdos plurianuales con la posibilidad de pagar por adelantado o pagar anualmente para acuerdos plurianuales
- Se agregó la capacidad de ver el análisis de causa raíz para los Accesos de Identidad
- Se implementaron Comportamientos Personalizados Temporales
- Se actualizó el modelo de Usuario para guardar la configuración de ocultar o mostrar las Licencias de Agente vencidas de forma predeterminada en la cuadrícula de Licencias de Agente
- Se actualizaron el modelo de Notificación de Seguridad y los endpoints/servicios relacionados para las nuevas opciones de alerta de agente sin conexión de agentes Parcialmente y Totalmente sin conexión
- Actualizaciones a los endpoints relacionados con la incorporación de las nuevas columnas en el frontend en la cuadrícula de Agentes para mostrar cuándo vence la licencia asignada y cuándo se asignó la licencia al agente
- Se agregó una configuración al Modelo de Grupo para que los agentes del grupo muestren el ícono del agente en la bandeja del sistema de la máquina del agente correspondiente
- Se actualizaron las consultas de cuadrícula del lado del servidor para poder aceptar filtros de múltiples condiciones para la misma clave/columna

Middleware 05.25

Características

- Se actualizó el modelo de Notificación de Ventas con nuevos tipos:
  - Los Distributor Partners pueden recibir alertas cuando sus subgrupos de revendedores crean un nuevo Registro de Oportunidad (Deal Registration)
  - Actividad del POC de Oportunidad del Partner (Partner Deal POC)
- Se actualizó el proceso de autenticación para permitir la integración de SSO con Microsoft Entra ID (Azure Active Directory)
- Se actualizó el endpoint del instalador del agente para permitir un nuevo tipo de instalador para Native Cli
- Se actualizaron los endpoints para las nuevas actualizaciones de Distributor Partner
  - Se agregó un nuevo modelo de Partner in Motion
  - Se actualizó el modelo de Registro de Oportunidad del Partner (Partner Deal Registration) para agregar la capacidad de que los distribuidores aprueben las oportunidades de sus subgrupos de revendedores
  - Se agregó la capacidad de que los Distributor Partners editen los descuentos multianuales de sus subgrupos de revendedores
  - Se agregó la capacidad de que los distribuidores se envíen a sí mismos cotizaciones con sus precios de distribuidor para la oportunidad de un subgrupo de revendedores
  - Se agregó el requisito de que, cuando un subgrupo de revendedores registre una oportunidad, se requiera que el Acuerdo de Subgrupo de Revendedores (Subgroup Reseller Agreement) sea cargado por su distribuidor principal en la página de Gestión de Grupos de Distribuidores
- Se actualizó el modelo de Roles con un nuevo rol de Partner Deal Manager para las operaciones de registro de oportunidades, y se actualizó cada endpoint relacionado para verificar el permiso correspondiente
- Se agregó el endpoint para editar la configuración de un grupo de forma masiva
- Se actualizó nuestro Spring Boot a la última versión
- Se mejoraron las consultas utilizadas para generar informes ejecutivos, reduciendo el tiempo necesario para generar el informe
- Se migraron nuestras colecciones de telemetría en la base de datos para utilizar sharding
- Se actualizó la consulta de agentes utilizada para la cuadrícula del panel de control (dashboard grid) para incluir si el agente es un servidor o no
- Se actualizó el endpoint /updateGroupAutomaticallyHideAgentsReactive para aplicar retroactivamente la actualización a los agentes existentes
- Actualizaciones importantes de autenticación para permitir que los agentes se comuniquen con nuestros servidores REST mediante la nueva autenticación OAuth alojada

- Se agregaron nuevos endpoints para el envío de telemetría de DLL por parte de los agentes

Middleware 12.25

Funciones

- Se agregaron nuevos endpoints para la Visualización de DLL en el panel para ver las cargas de módulos no confiables relacionadas con Respuestas de Extorsión, Creaciones de Procesos, Inyecciones de Procesos y Accesos de Identidad
- Se actualizaron los endpoints de Respuesta de Extorsión y Acceso de Identidad para las consultas del panel a fin de devolver campos adicionales para la Visualización de DLL, incluyendo memoria de módulo modificada, ruta de módulo modificada, etc.
- Se actualizó el modelo de Agente para incluir nuevos campos que indican si el agente está completamente configurado y la fecha en que el agente fue completamente configurado por primera vez
- Se agregaron nuevos endpoints y un controlador para la página de Administración del Firewall de IA
- Se actualizó el endpoint que devuelve la lista de agentes para el panel a fin de incluir nuevos campos que indican a qué servidor REST y servidor OAuth está llamando el agente, así como la IPv4 y la IPv6 WAN del agente
- Se agregó un nuevo endpoint para la página de Respuestas de Extorsión que permite a los usuarios ver todos los campos de una Respuesta de Extorsión en este endpoint, en lugar de usar el endpoint existente que ofrece una vista condensada de los campos y requiere una llamada adicional a la API para obtener más detalles.
  - Los usuarios del panel pueden usar el interruptor en la página de Respuestas de Extorsión para alternar entre la opción de cuadrícula anterior y la nueva opción de cuadrícula que devuelve todos los campos en una sola cuadrícula
- Se agregó una nueva opción en Notificaciones de Seguridad para incluir un archivo CSV en la alerta por correo electrónico para Alertas de Ransomware y Acceso de Identidad, que contiene información sobre el motivo por el cual se activó la alerta.

Aplicación Web

Aplicación web 04.23

Funciones

- Actualizaciones del Portal de Socios:
  - Posibilidad de programar una demostración en la página de Registro de Negocios (Register Deal)
  - Se implementó un nuevo proceso de Registro de Negocios con Aprobación de Negocios de Cyber Crucible
  - Se añadió un Tipo de Prospecto de Negocio al registrar negocios
  - Se añadió Ciclo de Facturación Mensual y Anual para los negocios
  - Se implementó el envío de cotizaciones para negocios aprobados por Cyber Crucible a través de Stripe, así como la firma de cotizaciones antes de completar un negocio
  - Posibilidad de reenviar la factura de Stripe para un negocio completado
  - Posibilidad de editar un negocio a través de una ventana modal, similar a la ventana modal de registro de nuevo negocio, prellenada con la información actual del negocio
- Gestión de Agentes/Licencias:
  - Posibilidad de liberar licencias desde la página de Agentes de forma masiva
  - Posibilidad de asignar licencias a agentes de forma masiva en la página de Agentes
  - Posibilidad, en la página de Agentes, de ver y modificar la configuración de renovación automática de licencias para los agentes cuando se conectan a nuestro servidor REST sin una licencia
    - Los usuarios pueden actualizar los agentes de forma individual o masiva
- Se implementó la posibilidad, en la página de Grupos, de ver el Id de un grupo y los valores de Client Auth utilizados en el Script de Instalación del Agente
- Se implementó la posibilidad de copiar listas blancas a otro grupo
- Se actualizó a React 18
- Se añadieron las opciones de restablecer columnas y ajustar automáticamente el tamaño de todas las columnas al menú contextual de las cuadrículas al hacer clic derecho
- Se añadió la opción de descargar el Archivo de Diferencias de Memoria (Memory Diff File) a la cuadrícula de Respuestas de Extorsión para las respuestas aplicables
- Se implementó el guardado del estado de visibilidad de los gráficos
- Se añadieron nuevas columnas de Aplicación a la cuadrícula de Acceso de Identidad para los programas accedidos, que acceden y los programas principales.
- Se implementó la alternancia de modo de columnas en cada cuadrícula para la cantidad de columnas a mostrar. Los modos incluyen: Mínimo, Medio, Máximo y Personalizado
- Se implementó la capacidad de búsqueda/autocompletado en los elementos de Selección Desplegable (Dropdown Select) con Material UI

Web Application 08.23

Características

- Actualizaciones del Portal de Socios:
  - Se agregó la página de Videos de Demostración al Portal de Socios
  - Se agregó la capacidad de crear una POC para acuerdos de socios aprobados
  - Se agregó la página de Administración de Grupos de Distribuidores al Portal de Socios para que los socios Distribuidores creen y administren sus subgrupos
  - Se agregó la página de Administración de Pagos al Portal de Socios
  - Se agregó la capacidad de cambiar el propietario de un acuerdo de socio
  - Se agregó un campo de nota personalizado para los acuerdos de socios que se muestra en las facturas y cotizaciones de Stripe
- Se implementó una funcionalidad de Recordarme que permite a los usuarios permanecer conectados
- Se agregó un enlace para ver el Portal de Clientes de Stripe donde los usuarios pueden administrar sus suscripciones y métodos de pago
- Se agregó la capacidad, en la página de Licencias de Agente, de cambiar el grupo de varias licencias seleccionadas en la cuadrícula
- Se actualizó AG Grid a la versión 29
- Se actualizaron las dependencias a sus versiones más recientes
- Se eliminó el botón de Automatización sobre las cuadrículas que revelaba íconos y, en su lugar, se colocaron los íconos directamente encima de la cuadrícula
- Se eliminó el botón de Columnas sobre las cuadrículas que revelaba las Opciones de Estado de Columnas de la Cuadrícula y, en su lugar, se colocaron dichas opciones directamente encima de la cuadrícula
- Se agregó la capacidad de reenviar invitaciones de cuenta de usuario en la página de Grupos
- Se agregó la columna de Modo de Extensión Canary a la página de Grupos
- Se agregó más etiquetado de aplicaciones a la página de Acceso de Identidad
- Se agregaron íconos y filtrado en la cuadrícula de Acceso de Identidad a la columna de Sin Certificado de Confianza para “Desconectado al Recuperar Información de Certificado” y “Tiempo Agotado al Recuperar Información de Certificado”
- Se corrigió un problema en dispositivos móviles con la renderización de cuadrículas

Aplicación web 11.23

Funciones

- Se agregó la capacidad de liberar automáticamente las licencias de agentes inactivos.
  - Esta función es una configuración de grupo y las opciones son liberar automáticamente las licencias de los agentes inactivos en el grupo después de 30/60/90 días, así como desactivar esta configuración
- Actualizaciones de la lista blanca
  - Se agregó la capacidad de crear una excepción con la ruta del programa principal y los argumentos
  - Se agregó la capacidad de crear una excepción para hacer coincidir las respuestas de extorsión cuando solo hay certificados de confianza, coincidir solo cuando no hay inyecciones relacionadas, y coincidir solo cuando no hay memoria modificada
  - Se agregó la capacidad de crear una excepción para hacer coincidir desencadenadores específicos de acceso a archivos
- Se agregó la ruta del programa principal y los argumentos a la cuadrícula de respuestas de extorsión
- Se agregaron los hashes de archivo al modal de detalles de respuesta de extorsión
- Se agregaron nuevos tipos de alertas de notificación de seguridad:
  - Modelo de comportamiento ajustado
  - Nueva versión de agente
- Se actualizaron los correos electrónicos de alerta de actividad de ransomware para incluir un enlace que redirigirá automáticamente a los usuarios a la página de respuestas de extorsión con un filtro para mostrar las respuestas a las que correspondía la alerta
- Se agregó una opción en el gráfico de la página de agentes para incluir en el gráfico únicamente el recuento de los agentes que se han comunicado durante los últimos 30/60/90 días, además de la opción de no limitar el recuento
- Se agregaron ejemplos en la página de integración REST sobre cómo llamar al endpoint aws /token. Los ejemplos incluyen llamar al endpoint con bash, powershell y el símbolo del sistema
- Se actualizaron los permisos del Incident Manager en la página de roles para que solo tenga permisos de visualización/edición de listas blancas y reglas de respuesta silenciosa
- Se eliminó de la página de roles el obsoleto Response Automation Manager
- Se agregó el modal de ajuste de procesos de utilidad del navegador a las páginas de listas blancas, reglas de respuesta silenciosa y respuestas de extorsión
  - Incluye la opción de seleccionar cómo deben responder los agentes de los grupos a los procesos de utilidad de chrome
- Se agregó la opción de descargar el agente mediante un script de powershell

- Se agregó la configuración de grupo para que los agentes del grupo se ejecuten en modo seguro
- Se agregó la columna de nombre del sistema operativo a la cuadrícula de agentes
- Se corrigió un problema en determinadas cuadrículas por el cual el ancho y el orden de las columnas se restablecían al hacer clic en íconos/botones de la página

Web Application 04.24

Funciones

- Se agregó la capacidad de configurar y administrar configuraciones de proxy para ayudar en la implementación de agentes. Consulte más información sobre las configuraciones de proxy aquí
- Se corrigió el problema por el cual la barra de desplazamiento horizontal en la parte inferior de nuestras cuadrículas de datos no era visible debido a que la cuadrícula se extendía más allá de la altura visible de la pantalla
- Se agregó la capacidad, en nuestras páginas de Telemetría, de alternar entre ver todos los datos de telemetría o ver únicamente los datos relacionados directamente con una respuesta a extorsión
- Se agregó la configuración de grupo para ocultar automáticamente los agentes del grupo cuando se libera una licencia de un agente, un agente se marca como inactivo, o un agente completa una desinstalación
- Se agregó la capacidad, al hacer clic en un enlace de uno de nuestros correos electrónicos de notificación, de filtrar automáticamente los datos en la cuadrícula relacionada para mostrar lo que activó la notificación
- Se actualizó el gráfico de Licencias de Agentes para mostrar los recuentos tanto de Licencias de Escritorio como de Servidor
- Se actualizó AG Grid a la versión 31
- Se actualizó Ag Charts a la versión 9
- Se agregaron más opciones de filtro de texto a nuestras cuadrículas de datos
- Se agregó la página de Estado de Implementación del Cliente (que se encuentra en la pestaña de operaciones)

Aplicación web 09.24

Funciones

- Se agregó a la página de licencias de agentes la capacidad de filtrar las licencias vencidas de la cuadrícula y el gráfico de forma predeterminada. Esta configuración se puede actualizar en el conmutador ubicado encima de la cuadrícula de licencias de agentes
- Se implementaron filtros de múltiples condiciones para una sola columna en las cuadrículas del lado del servidor. Las cuadrículas del lado del servidor son aquellas en las que no se cargan todas las filas en la cuadrícula durante la carga inicial debido a la gran cantidad de filas en estas cuadrículas: Respuesta a Extorsión, Creaciones de Procesos, Inyecciones de Procesos y Accesos de Identidad
- Se agregó la opción de varios años para los Registros de Acuerdos. Los acuerdos pueden tener una duración de hasta 3 años, y los usuarios tienen la opción de pagar por adelantado o pagar anualmente para los acuerdos de varios años
- Se implementaron los Comportamientos Personalizados Temporales. Vea más aquí
- Se agregó una nueva columna en la cuadrícula de Accesos de Identidad para el Análisis de Causa Raíz
- Se actualizaron las Notificaciones de Seguridad con dos opciones diferentes para alertas de agentes sin conexión: alertas de agente Parcialmente y Totalmente Sin Conexión
- Se agregaron nuevas columnas a la cuadrícula de agentes para la fecha de vencimiento de la licencia y la fecha en que se asignó la licencia al agente
- Se agregó la nueva configuración de Grupo para el Modo DMZ para que la sigan los agentes del grupo. El Modo DMZ es para entornos donde la verificación de certificados en línea no está disponible. Habilitar el Modo DMZ incorporará las raíces de CA localmente en los agentes del grupo y deshabilitará OSCP
- Se agregó la nueva configuración de Grupo para que los agentes del grupo muestren un ícono de agente en la máquina del agente correspondiente en la bandeja del sistema; solo los agentes con la versión 4.4.8.2 y superior tienen esta capacidad
- Se agregó una barra lateral a nuestras cuadrículas de datos para cambiar fácilmente la visibilidad y el orden de las columnas

Aplicación web 05.25

Funciones

- Se agregó la integración de SSO para el inicio de sesión de nuestro panel con Microsoft Entra ID (Azure Active Directory)
  - Los usuarios deben ponerse en contacto con Cyber Crucible y completar algunos pasos que se encuentran aquí para integrar el SSO de Entra ID de su organización con el inicio de sesión de nuestro panel
- Actualizaciones para Socios Distribuidores
  - Mejoras en el proceso mediante el cual los distribuidores asocian subgrupos de revendedores y dichos subgrupos de revendedores registran y completan negocios. Se puede encontrar una explicación más detallada del proceso mejorado de Gestión de Grupos de Distribuidores aquí
  - Se agregó un nuevo tipo de Notificación de Ventas para que los Socios Distribuidores reciban alertas cuando sus subgrupos de revendedores creen un nuevo Registro de Negocio
  - Se agregó la capacidad para que los Socios Distribuidores editen los descuentos plurianuales de sus subgrupos de revendedores. Esto se puede encontrar en la página de Gestión de Grupos de Distribuidores
  - Se agregó la columna de Aprobación del Distribuidor al Registro de Negocio para que los Distribuidores gestionen los negocios de sus subgrupos de revendedores
  - Se agregó la página Partner in Motion, ubicada en la pestaña Partners, para que los socios distribuidores registren a los socios de subgrupos de revendedores que están en proceso
- Se agregó el rol de Partner Deal Manager para operaciones relacionadas con el registro de negocios
- Se agregó un nuevo tipo de notificación de ventas para la actividad de POC de negocios de socios. Esta alerta se aplica al nuevo grupo de POC que se crea cuando un socio crea un POC para un negocio. Las alertas de este tipo se envían para las instalaciones/desinstalaciones de agentes y cuando las licencias de POC expiran en el grupo de POC
- Se agregó el nuevo tipo de instalador de Agente “Native CLI”
- Se agregó el modal de Edición de Grupo en la página de Gestión de Grupos, que permite editar la configuración de los grupos de forma masiva
- Se actualizó AG Grid a la versión 32
- Se agregó un botón/interruptor de visibilidad de contraseña para el inicio de sesión

Web Application 12.25

Funciones

- Se agregó la nueva página de Administración de AI Firewall, que se encuentra en la pestaña Operations
- Visualización de DLL
  - Se agregó la capacidad de ver las cargas de módulos relacionadas para Extortion Responses, Process Creations, Process Injections e Identity Accesses
  - Se agregó una nueva columna a estas páginas que muestra si se encontraron cargas de módulos no confiables relacionadas. Cuando se encuentra una carga de módulo no confiable, la celda de esta columna mostrará un ícono en el que, al hacer clic, se llevará a los usuarios a una nueva página para ver todas las cargas de módulos no confiables relacionadas
- Se agregaron nuevas columnas a las cuadrículas de Extortion Responses e Identity Access:
  - Modified Module Memory
  - Modified Module Path
  - Modified Module Original Memory Hash
  - Modified Module Current Memory Hash
  - Modified Module Identifier
  - Process Execution GUID
  - Pid
  - Pid Reuse Number
- Se agregó a la cuadrícula de Extortion Responses la columna “Data Access Attempted”, que muestra la ruta en la máquina donde se intentó el acceso a los datos
- Se actualizó la página de Extortion Responses para que ahora tenga 2 opciones de cuadrícula diferentes. La opción de cuadrícula anterior, con una vista más condensada de las respuestas de extorsión con la cuadrícula principal y secundaria, sigue existiendo; ahora existe una nueva opción para eliminar la cuadrícula principal/secundaria y mostrar todos los datos y columnas en una sola cuadrícula
- Se agregaron columnas a la cuadrícula de Agents que muestran si el agente está completamente configurado y la fecha en que se configuró completamente por primera vez
- Se agregaron columnas adicionales a la cuadrícula de Agents para indicar a qué servidor OAuth Server y REST Server está llamando el agente, así como la dirección WAN IPv4 e IPv6 del agente
- Se agregó Co-branded Collateral en la pestaña Partners, lo que permite a los socios descargar un archivo .zip que contiene todo el material de colateral de marca compartida
- Se actualizó AG Grid a la versión 34

- Se agregó el número de días hasta el vencimiento de una licencia en la página de Agent Licenses y en la página de Agents. Esto se puede encontrar como un ícono en la columna Renews de la página de Agent Licenses, y en la columna License Expiration Date de la página de Agents
- Se agregó una nueva opción en Security Notifications para incluir un archivo CSV en la alerta por correo electrónico para las alertas de Ransomware e Identity Access, que contiene información sobre por qué se activó la alerta. Esta opción se agregó para que los usuarios puedan ver por qué ocurrió una alerta directamente en el correo electrónico sin tener que iniciar sesión en el panel