Versions logicielles

- 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
- 4.5.3.2

- Middleware (serveurs REST)
  - Middleware 01.23

Agent de terminal

Index des versions de l'agent 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

Agent de terminal

4.4.0.9

Fonctionnalités

- Pour les groupes avec télémétrie activée, ajout des données Active Directory à la liste de surveillance du vol d'identifiants

Corrections

- Suppression des volumes locaux et des entrées de partages réseau en double dans certains environnements.
- Comportement affiné pour certaines reconstructions de bases de données de vignettes provoquant des incidents
- Correction d'un bogue de validation de licence pouvant augmenter le temps de démarrage
- Comportement affiné pour l'accès aux fichiers sur des supports à écriture unique tels que les CD et les lecteurs de bandes WORM

Statut de validation WHCP/WHQL

Validé

Hachages MD5

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

Agent de terminal

4.4.0.9.1

Fonctionnalités

Aucune - mise à jour de maintenance.

Corrections

- Correction d'un problème où certains partages réseau connectés par un utilisateur étaient initialement ignorés dans l'analytique.
- Amélioration du comportement de faux positif associé aux partages apparaissant pendant les sessions utilisateur, suivis rapidement d'une boîte de dialogue Enregistrer sous.

Statut de validation WHCP/WHQL

Validé.

Hachages MD5

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

Agent de terminal

4.4.1.0

Fonctionnalités

- Prise en charge étendue de l'analyse des injections de processus, afin d'augmenter considérablement la précision de la détection des intentions malveillantes ou bénignes pour les applications.
  - Cela est devenu particulièrement important en raison d'un petit nombre (<0,02 %) de machines dans la télémétrie de Cyber Crucible déclenchant des alertes sur des comportements agressifs d'injection de processus provenant de processus système.
- Capacité de surveillance accrue des processus système non signés.
  - Cela répond en partie à la forte concentration des attaquants sur l'implication de ces processus lors des opérations de mouvement latéral (sur un système, et entre les systèmes).

Corrections

- Modification d'un comportement de modification de fichier afin de réduire les faux positifs en ne déclenchant plus d'alerte sur certaines actions bénignes, grâce à un contexte supplémentaire au niveau du noyau concernant les comportements d'accès aux fichiers d'un processus.

Statut de validation WHCP/WHQL

Validé.

Empreintes MD5

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

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

Agent de terminal

4.4.1.1

Fonctionnalités

- Amélioration du traitement analytique des relations parent-enfant, lorsque le processus parent se termine rapidement avant que Cyber Crucible n'ait terminé son traitement (millisecondes).
  - Le scénario extrêmement courant ici est que les attaquants (et les programmes légitimes) ouvrent souvent plusieurs programmes, parfois selon une « chaîne » en plusieurs étapes. Cela peut être intentionnel, ou dû au comportement « sous le capot » de Windows ou d'autres applications.
  - Les modèles comportementaux de Cyber Crucible exploitent les variables d'activité et d'état pour tous les processus d'une chaîne d'exécutions afin d'atteindre une précision et un contexte maximaux.

Corrections

- Cyber Crucible connaissait une perte de précision dans la prise de décision des modèles comportementaux, due à la perte de télémétrie lorsque plusieurs programmes s'appellent mutuellement, mais que l'un des programmes se termine en quelques millisecondes.
  - Dans une chaîne où le programme A exécute le programme B. Le programme B démarre le programme C, mais le programme B se termine en quelques millisecondes (généralement un plantage silencieux, mais pas toujours). L'analyse comportementale de Cyber Crucible dispose des variables des programmes A et C, mais n'a pas eu le temps d'analyser complètement le programme B, puisqu'elle s'attendait à ce qu'il soit en cours d'exécution.
  - Ce problème a été corrigé, ce qui améliore la précision de la prise de décision du moteur de décision hyper-automatisé de Cyber Crucible.

Statut de validation WHCP/WHQL

Validé.

Hachages MD5

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

Agent de terminal

4.4.1.2

Fonctionnalités

- Spécificité disponible accrue pour les listes blanches, telles que le chemin et les arguments du processus parent.
- Support étendu pour l'analyse des accès d'identité à davantage de bases de données d'identifiants.
  - L'accès d'identité est désormais également surveillé pour Slack, Opera, Thunderbird, Discord et Vivaldi.
- Support de liste blanche étendu pour inclure l'accès d'identité.

Corrections

- Réduction de la bande passante utilisée entre les agents et l'API REST.
- Correction de l'affichage des canaris dans l'Explorateur sur certaines anciennes éditions de Windows Server.
- Correction de journaux d'accès d'identité auxquels manquaient des indicateurs de confiance de certificat.

Statut de validation WHCP/WHQL

Validé

Hachages MD5

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

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

Agent de terminal

4.4.1.3

Fonctionnalités

- La surveillance des identifiants/identités inclut désormais divers VPN, portefeuilles de cryptomonnaie et autres applications.
- Dans une chaîne de processus affectés lors d'une attaque (ceci est courant : l'attaquant passe du programme A en cours d'exécution, à B, à C, et D est utilisé pour le vol de données), le programme « patient 0 » A est suspendu, mais le patient D est signalé comme étant le processus effectuant le comportement de vol.
  - L'état de la mémoire est préservé et signalé tout au long des chaînes de processus, pour une analyse judiciaire future.
- En cas de réponse automatisée au cours de laquelle la mémoire d'un processus en cours d'exécution a été modifiée, cette modification de mémoire est téléchargée de manière configurable vers Cyber Crucible à des fins de rétro-ingénierie et d'analyse approfondie.
- En cas de bogue de modification de mémoire non malveillant dans une application, les exceptions comportementales (« listes blanches ») ont désormais la capacité de signaler certains événements de corruption de mémoire comme bénins. Cela n'empêchera pas le programme lui-même de planter ou de perdre des données en raison du bogue, mais Cyber Crucible saura ignorer le bogue lors de la recherche d'injection malveillante de code dans les processus en cours d'exécution (injection/évidement de processus).

Corrections

- Suppression d'une vulnérabilité permettant à des binaires d'être supprimés par un processus privilégié pendant la mise à jour des binaires CC.
- Suppression d'une vulnérabilité permettant à des clés de registre d'être supprimées ou modifiées par un processus privilégié pendant la mise à jour des binaires CC.
- Correction du suivi de l'état de la mémoire lorsqu'un processus est corrigé en mémoire pendant l'évaluation de la mémoire par Cyber Crucible.
- Correction du suivi de l'état de la mémoire dans certaines conditions où la mémoire est réallouée entre les pages mémoire.
- Mises à jour mineures d'efficacité du CPU, probablement trop minimes pour être visibles dans le Gestionnaire des tâches, car l'utilisation est normalement <1 %

Statut de validation WHCP/WHQL

Validé

Hachages MD5

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

4.4.1.3.1

Visibilité obtenue sur certains processus système qui s'initialisent avant le chargement du pilote Cyber Crucible.

Hachages MD5 :

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

4.4.1.3.2

Ajout de télémétrie supplémentaire pour les processus système désormais visibles grâce à la version 4.4.1.3.1.

Hachages MD5 :

```
service.exe: 47f408d6102eb06a94f2244cf139a0a5
assistant.exe: 86733da51ee703f93dcda9346231cca6
win7/CCRRSecMon.sys: b01e8933fa9ac9f0a049527b20d9f679
win8/CCRRSecMon.sys: 4467124cf7e8b5ab5652169f9eb41663
win10/CCRRSecMon.sys: 8f06de95303eeac038002ec27c297811
```

4.4.1.3.3

Correction de certains rapports d'incident incluant des données pour le mauvais processus, lorsqu'un processus meurt en cours de calcul.

Hachages MD5 :

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

4.4.1.3.4

Optimisation des calculs de mémoire, en préparation de la version 4.4.1.4.

Hachages MD5 :

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

Agent de terminal

4.4.1.4

Fonctionnalités

- Amélioration des capacités de reconnaissance de motifs dans le modèle comportemental.
  - Ceci est particulièrement pertinent pour une couverture supplémentaire des emplacements de stockage d'identités, tels que les emplacements de portefeuilles de cryptomonnaie.
- Amélioration des fonctionnalités de dépendances logicielles pour les bibliothèques (Cyber Crucible) utilisées en vue de la future protection entièrement automatisée de l'accès aux identités.
- Possibilité d'activer l'exécution de l'agent en mode sans échec (opt-in)

Corrections

- Optimisation de l'utilisation de la mémoire dans le service. Cela n'aurait été ressenti que sur des serveurs très sollicités où de nombreuses analyses comportementales étaient effectuées (par Cyber Crucible) simultanément.

Hachages MD5

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

Agent de terminal

4.4.2.0

Fonctionnalités

- Capacités de surveillance et de prévention améliorées pour la protection automatisée de l'accès aux identités.
- Optimisation de l'utilisation du réseau grâce à des taux de communication variables en fonction du comportement des clients.

Corrections

- N/A

Hachages MD5

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

Agent de terminal

4.4.2.1

Corrections

- Optimisation du suivi des informations d'identité pour les applications comportant un grand nombre de répertoires profondément imbriqués.

Hachages MD5

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

Agent de terminal

4.4.2.2

Fonctionnalités

- Aucune

Corrections

- Optimisation de la gestion des variables pour un type de comportement.
  - Cause : Un produit de sécurité non précisé a généré un très grand nombre de comportements sur quelques serveurs de grande taille, ce qui a entraîné une utilisation excessive de la mémoire par Cyber Crucible.
  - Symptômes : L'utilisation de la mémoire de Cyber Crucible passe de quelques Mo à plusieurs Go. L'utilisation de la mémoire du produit de sécurité a également augmenté d'un facteur 100, dépassant 250 Go. Si vous rencontrez ce problème, qui peut être indépendant de Cyber Crucible, veuillez ouvrir un ticket d'assistance afin que nous puissions vous aider. Nous soupçonnons également qu'il s'agissait d'un problème lié au produit de sécurité, indépendant de l'optimisation de Cyber Crucible.
  - Correction : Ce suivi des variables de comportement a été migré d'un algorithme conçu pour une faible volumétrie vers un algorithme adapté à une volumétrie élevée, comme cela est déjà utilisé ailleurs dans le pilote.
  - Qui est concerné ? Un seul client a été observé avec ce problème, et uniquement sur une petite partie de ses serveurs de grande taille. Néanmoins, cette mise à jour est déployée pour l'ensemble des clients.

Empreintes MD5

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

Agent de terminal

4.4.2.3

Fonctionnalités

- Aucune

Corrections

- Correction des problèmes de compatibilité avec Acronis

Hachages MD5

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

Agent de terminal

4.4.2.4

Fonctionnalités

- Prise en charge de la protection des identifiants pour Microsoft Teams et Signal Messenger

Corrections

- Suppression des journaux liés au réseau en mode sans échec sans mise en réseau
- Sauvegarde de certaines données de l'agent lors de la désinstallation dans le dossier de stockage temporaire de Windows

Empreintes MD5

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

Agent de terminal

4.4.2.5

Fonctionnalités

- Aucune

Corrections

- Réduction de l'utilisation du réseau lors de l'envoi d'un grand nombre de rapports à la fois
- Correction de la gestion de certaines données de certificat

Hachages MD5

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

Agent de terminal

4.4.2.6

Fonctionnalités

- Aucune

Corrections

- Réduction de l'utilisation de la mémoire sur les serveurs comportant de nombreux certificats de programme uniques

Hachages MD5

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

Agent de terminal

4.4.2.7

Fonctionnalités

- Aucune

Corrections

- Réduction de l'utilisation de la mémoire lors du traitement des programmes qui utilisent un comportement non défini lors de l'interrogation des répertoires

Hachages MD5

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

Agent de terminal

4.4.2.8

Fonctionnalités

- Aucune

Corrections

- Augmentation de la journalisation et de la télémétrie pour les états machine défectueux
- Amélioration de la stabilité des protections d'identité au démarrage

Hachages MD5

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

Agent de terminal

4.4.3.0

Fonctionnalités

- En plus des protections de service existantes, le pilote en mode noyau redémarrera le service si celui-ci s'arrête pour une raison quelconque.

Corrections

- Aucune

Hachages MD5

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

Agent de terminal

4.4.3.2

Fonctionnalités

- Aucune

Corrections

- Réduction de l'utilisation du CPU lors du démarrage des processus.
- Réduction de l'utilisation du CPU lors des déterminations de confiance pendant les requêtes de répertoires consécutives.

Hachages MD5

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

Agent de terminal

4.4.3.1

Fonctionnalités

- Aucune

Corrections

- Correction d'un problème sur certaines machines présentant des caractéristiques d'installation Windows inhabituelles où des canaris étaient visibles dans l'Explorateur.

Hachages MD5

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

Agent de terminal

4.4.4.0

Fonctionnalités

- Les rapports d'incidents et de télémétrie sont stockés sur disque pour les scénarios hors ligne.
  - En raison de tentatives d'altération observées contre plusieurs magasins de journalisation EDR/XDR, Cyber Crucible a activé une protection au niveau du noyau pour les données stockées sur disque avant de déployer cette fonctionnalité.
- Protection renforcée du processus de service utilisé pour la communication backend et les mises à jour, dans le cadre du durcissement zero-trust anticipatif.
  - Ceci n'était pas une réponse à une menace existante, mais une mesure proactive face à une menace que l'équipe anticipe.

Corrections

- Correction des processus se chargeant au démarrage qui n'étaient pas disponibles dans le tableau de bord sous les créations de processus.
- Empêchement de l'exécution simultanée de deux programmes d'installation, ce qui aurait enregistré la même machine deux fois.

Empreintes MD5

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

Agent de terminal

4.4.4.4

Fonctionnalités

- Aucune

Corrections

- Amélioration des performances pour l'analyse des données de certificat au démarrage du système.

Hachages MD5

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

Agent de terminal

4.4.5.1

Fonctionnalités

- Réduction de l'utilisation de la bande passante :
  - Utilisation de la compression pour les données de télémétrie plus volumineuses et les réponses serveur plus importantes
  - Utilisation de HTTP/2 pour les en-têtes compressés et une meilleure efficacité des sockets
- Amélioration de la visibilité sur les opérations liées aux certificats.

Corrections

- Encodage des métadonnées de certificat dans la télémétrie brute en présence d'étiquettes non conformes à la RFC. L'infrastructure de sécurité réseau corrompait ou supprimait les charges utiles, ce qui obligeait l'agent à retransmettre jusqu'à réussite.

Hachages MD5

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

Agent de terminal

4.4.5.2

Fonctionnalités

- Nouvelle télémétrie d'accès au niveau du noyau pour les comportements réseau, afin de mieux identifier les bugs réseau possibles côté client, ou les opportunités d'optimisation
- La télémétrie sortante est désormais regroupée et envoyée ensemble, tout comme les paramètres entrants
  - Transmise avec une variance de synchronisation de 25 %, afin que chaque machine n'envoie pas de paquets simultanément sur un réseau client
- HTTP/2 est désormais pleinement utilisé de bout en bout

Corrections

- Réduction du nombre minimum de threads utilisés en espace utilisateur
- Réduction de l'utilisation du CPU pour le service en espace utilisateur
- L'authentification Agent-Serveur est désormais effectuée plus efficacement
- Remplacement de l'ancien algorithme de mise en veille/redémarrage du service lorsque les licences n'étaient pas disponibles.
  - L'ancien algorithme provoquait un « service exited unexpectedly » (service arrêté de manière inattendue) dans le gestionnaire d'événements toutes les 15 minutes.
  - Permettre au système d'exploitation d'indiquer au service de s'arrêter (une pratique exploitée par des criminels et d'autres outils de sécurité) aurait permis un redémarrage « propre » du service sans journaux dans le gestionnaire d'événements. Plutôt que de créer cette vulnérabilité, le service de Cyber Crucible s'est redémarré lui-même sans l'intervention de Windows, ce qui génère l'entrée dans le journal d'événements.

Empreintes MD5

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

Agent de terminal

4.4.5.3

Fonctionnalités

- Ajout d'un second domaine pour la communication avec le serveur (voir la liste des domaines ici).
  - En cas de problèmes de communication avec un domaine, l'agent basculera automatiquement vers l'autre.

Corrections

- Modification de certaines anciennes chaînes de caractères faisant référence à « Ransomware Rewind » pour désormais faire référence à « Cyber Crucible ».

Hachages MD5

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

Agent de terminal

4.4.5.9

Fonctionnalités

- Renforcement accru de certaines parties des fonctionnalités précédemment assurées par les bibliothèques de cryptographie Windows, désormais prises en charge par le pilote de noyau Cyber Crucible.
  - Il s'agit à la fois d'un renforcement général et d'une augmentation de la télémétrie indiquant d'éventuelles attaques contre les bibliothèques et API de cryptographie Windows.
- Il s'agit d'une version jalon par rapport aux versions incrémentales 4.4.5.4 à 4.4.5.8, toutes alignées sur la précédente fonctionnalité de renforcement de l'analyse cryptographique.
  - Les premières données de télémétrie indiquent que les échecs des bibliothèques de certificats et de cryptographie Windows ont été traités de manière légitime par Cyber Crucible.
  - On ignore actuellement quel pourcentage des problèmes était dû à une exploitation par rapport à un bug d'une bibliothèque système Windows. Veuillez contacter votre représentant Cyber Crucible pour en discuter plus en détail si nécessaire.

Corrections

- Correction de certains rapports de processus signalant à tort le certificat répertorié comme « non approuvé », en raison d'une perte de fonctionnalité de la bibliothèque de certificats Windows.

Hachages MD5

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

Agent de terminal

4.4.5.8

Fonctionnalités

- Renforcement accru de certaines portions de fonctionnalités auparavant assurées par les bibliothèques de cryptographie Windows, désormais gérées par le pilote de noyau Cyber Crucible.
  - Il s'agit à la fois d'un renforcement général et d'une augmentation de la télémétrie indiquant d'éventuelles attaques contre les bibliothèques et API de cryptographie Windows.

Corrections

- Correction de certains rapports de processus signalant incorrectement le certificat listé comme « non approuvé », en raison d'une perte de fonctionnalité de la bibliothèque de certificats Windows.

Hachages MD5

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

Agent de terminal

4.4.5.5

Fonctionnalités

- Renforcement accru de certaines portions de fonctionnalité auparavant assurées par les bibliothèques de cryptographie Windows, désormais prises en charge par le pilote noyau de Cyber Crucible.
  - Il s’agit à la fois d’un renforcement général et d’une augmentation de la télémétrie signalant d’éventuelles attaques contre les bibliothèques et API de cryptographie Windows.

Corrections

- Correction de certains rapports de processus indiquant à tort le certificat listé comme « non approuvé », en raison d’une perte de fonctionnalité de la bibliothèque de certificats Windows.

Hachages MD5

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

Agent de terminal

4.4.5.6

Fonctionnalités

- Renforcement accru de certaines fonctionnalités auparavant assurées par les bibliothèques de cryptographie Windows, désormais gérées par le pilote de noyau Cyber Crucible.
  - Il s'agit à la fois d'un renforcement général et d'une augmentation de la télémétrie indiquant d'éventuelles attaques contre les bibliothèques et API de cryptographie Windows.

Corrections

- Correction de certains rapports de processus signalant à tort le certificat listé comme « non approuvé », en raison d'une perte de fonctionnalité de la bibliothèque de certificats Windows.

Hachages MD5

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

Agent de terminal

4.4.5.7

Fonctionnalités

- Renforcement accru de certaines parties des fonctionnalités auparavant assurées par les bibliothèques de cryptographie Windows, désormais prises en charge par le pilote noyau de Cyber Crucible.
  - Il s'agit à la fois d'un renforcement général et d'une augmentation de la télémétrie indiquant de possibles attaques contre les bibliothèques et API de cryptographie Windows.

Corrections

- Correction de certains rapports de processus indiquant à tort que le certificat listé n'était « pas approuvé », en raison d'une perte de fonctionnalité de la bibliothèque de certificats Windows.

Hachages MD5

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

Agent de terminal

4.4.5.4

Fonctionnalités

- Renforcement accru de certaines parties de la fonctionnalité précédemment assurée par les bibliothèques de cryptographie Windows, désormais assurée par le pilote noyau de Cyber Crucible.
  - Il s’agit à la fois d’un renforcement général et d’une augmentation de la télémétrie indiquant d’éventuelles attaques contre les bibliothèques et API de cryptographie Windows.

Corrections

- Correction de certains rapports de processus signalant à tort le certificat listé comme « non fiable », en raison d’une perte de fonctionnalité de la bibliothèque de certificats Windows.

Empreintes MD5

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

Agent de terminal

4.4.6.0

Fonctionnalités

- Amélioration des performances du processeur pour certaines applications qui déclenchent un grand nombre de parcours de répertoires automatisés et simultanés dans le cadre de leur comportement applicatif.

Corrections

-

Hachages MD5

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

Agent de terminal

4.4.6.1

Fonctionnalités

- Poursuite de la migration du nom de produit « Ransomware Rewind » vers « Cyber Crucible ».
  - Le nom de service hérité `"Ransomware Rewind"` migrera vers `"CyberCrucibleAgent"`. Le nom du processus reste inchangé.
  - La clé de registre dans `HKLM\SOFTWARE` migrera de l'ancienne clé `RansomwareRewind` vers la clé actuelle `CyberCrucibleAgent.`

Corrections

- Correction de certains processus 32 bits déclenchant à tort une alerte de « mémoire modifiée » lorsque l'image du processus atteint la taille maximale autorisée pour un processus 32 bits.

Empreintes MD5

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

Agent de terminal

4.4.6.2

Fonctionnalités

- Ajout d'indicateurs optionnels de « type d'accès » exposés aux utilisateurs finaux pour une spécificité comportementale des accès.

Corrections

- Aucune.

Hachages MD5

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

Agent de terminal

4.4.6.3

Fonctionnalités

- Ajout d'une prise en charge optionnelle du proxy SOCKS5 pour faciliter le déploiement des agents.

Corrections

- Correction des réinstallations à partir d'agents plus anciens utilisant un ID d'installation incorrect.
- Correction des installations existantes provenant d'anciens installateurs présentant un chemin de service non délimité par des guillemets.

Hachages MD5

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

Agent de terminal

4.4.6.4

Fonctionnalités

- Les informations sur la mémoire du processus parent sont disponibles pour les rapports de processus lorsque des modifications ont été détectées.

Améliorations

- Modification de certaines fréquences de communication avec le serveur afin qu'elles ne nécessitent plus de redémarrage pour être ajustées.

Corrections

Aucune pour cette version.

Hachages MD5

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

Agent de terminal

4.4.7.0

Fonctionnalités

- Début du déploiement des communications HTTPS basées sur JWE.
  - Les clés de chiffrement sont uniques à chaque agent.
  - Toutes les charges utiles sont chiffrées sous HTTPS. Désactivé par défaut pendant le déploiement initial.
  - Possibilité de revenir facultativement du HTTPS chiffré par JWE au HTTPS non chiffré si les charges utiles au format JWE ne sont pas transmises avec succès.

Hachages MD5

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

Agent de terminal

4.4.7.1

Fonctionnalités

- Télémétrie enrichie pour les créations de processus et les incidents
  - SID de l'utilisateur
  - Nom de connexion de l'utilisateur (down-level logon name)
  - Indication si le processus est élevé (Exécuter en tant qu'administrateur)
- Les incidents indiquent désormais où l'accès itératif aux données s'est produit

Corrections

- Réduction de l'utilisation de la mémoire pendant les périodes de problèmes de connectivité au serveur et de télémétrie intense survenant simultanément
- Réduction de l'utilisation de la mémoire lors du signalement des incidents

Empreintes MD5

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

Agent de terminal

4.4.7.3

Fonctionnalités

- Mode DMZ
  - Configuration facultative permettant d’utiliser un ensemble d’autorités de certification (CA bundle) signé pour les communications TLS avec les serveurs d’authentification et de télémétrie. Ces ensembles d’autorités de certification sont ensuite protégés contre toute altération ou suppression grâce aux capacités propriétaires anti-altération de Cyber Crucible.
  - Les vérifications OCSP et CRL sont désactivées afin de réduire la liste des domaines à autoriser via un pare-feu.

Corrections

- Réduction de l’utilisation de la mémoire et du temps CPU consacré à la soumission des différences mémoire (memory diff), en particulier après de longues périodes hors ligne.

Empreintes MD5

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

Agent de terminal

4.4.8.0

Fonctionnalités

- Télémétrie Authenticode en mode noyau
  - Pour une rapidité et une fiabilité accrues, les données de certificat relatives aux créations de processus et aux incidents seront enregistrées par le pilote seul.
  - Cette mise à jour ne supprime pas les dépendances vis-à-vis des bibliothèques de cryptographie Windows, mais effectue les calculs cryptographiques en parallèle. À terme, la dépendance à Windows pourra être entièrement supprimée.

Corrections

- Réduction de l’utilisation de la mémoire et du temps CPU consacré aux tentatives de soumission d’événements en mode hors ligne, période durant laquelle la télémétrie est stockée de manière sécurisée jusqu’à ce que la machine retrouve la connectivité aux serveurs Cyber Crucible.
- Certains programmes d’installation de pilotes Nvidia estimaient à tort ne pas disposer des privilèges nécessaires pour s’installer, en raison de l’utilisation d’une fonction interne du noyau Microsoft visant à accéder aux fichiers installés par Cyber Crucible.
- Correction d’une incompatibilité entre le mode JWE et le mode DMZ

Empreintes MD5

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

Agent de terminal

4.4.8.1

Fonctionnalités

- Les métadonnées des exécutables telles que la version du produit, le nom de la société, etc. pour les processus en mémoire sont signalées par le pilote via la visibilité du noyau. Le fonctionnement normal consiste à utiliser des appels API Windows en espace utilisateur. Ce passage à l'analyse au niveau du noyau supprime la possibilité (observée) pour les attaquants de falsifier les informations relatives aux processus.
- Les informations d'authentification de l'agent sont répliquées ailleurs dans le système afin de permettre une restauration en cas de corruption du registre par un pilote malveillant.

Améliorations

- Les erreurs de connexion au serveur sont enregistrées de manière minimale par l'agent, ce qui réduit la taille des journaux sur le disque.

Corrections

- N/A

Hachages MD5

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

Agent de terminal

4.4.8.2

Fonctionnalités

- Ajout de la prise en charge d'une icône optionnelle dans la barre d'état système. Cette fonctionnalité est désactivée par défaut.

Corrections

- Ajout d'une solution de contournement pour un problème lié aux requêtes de hachage de l'API Windows du noyau. Cette solution de contournement pourra être supprimée à l'avenir si le problème Windows est corrigé, éventuellement lors de la prochaine mise à jour du noyau.

Hachages MD5

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

Agent de terminal

4.4.9.0

Fonctionnalités

- Télémétrie des DLL en mode noyau
  - Analyse des certificats et calcul de la confiance pour toutes les DLL chargées dans le pilote.

Corrections

- Aucune.

Hachages MD5

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

Agent de terminal

4.4.9.1

Fonctionnalités

- Aucune.

Corrections

- Augmentation de la quantité de télémétrie traitée simultanément par le service pour les données de création et d'injection.
- Ajustement de l'ordre des canaris pour les programmes utilisant des méthodes d'itération de fichiers inhabituelles.
- Ajustement de la liste de contrôle d'accès (ACL) sur certains canaris afin de mieux s'intégrer aux systèmes de fichiers réels.

Empreintes MD5

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

Agent de terminal

4.4.9.2

Fonctionnalités

- Suivi de la modification de la mémoire pour les DLL chargées.
- Génération de différences mémoire (diff) pour les DLL modifiées.

Corrections

- Correction du traitement de certaines DLL non conformes qui produisaient des résultats de hachage Authenticode incorrects.

Empreintes MD5

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

Agent de terminal

4.4.9.4

Corrections

- Les fichiers de vidage de service (dump) sont désormais limités à 10 par combinaison version+thread.

Empreintes MD5

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

Agent de terminal

4.5.0.0

Fonctionnalités

- Pare-feu noyau IA
- Accélérations du calcul du hachage Authenticode
- Réduction significative de l'utilisation de la mémoire pour la télémétrie des DLL
- Visibilité accrue pour les modifications de mémoire dans les DLL

Corrections

- Correction de la compatibilité de la récupération du service avec 24H2

Hachages MD5

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

Agent de terminal

4.5.0.1

Fonctionnalités

- Option permettant de migrer vers le domaine du serveur d’authentification OAuth hébergé
- Tâche permettant de configurer dynamiquement les URL des serveurs REST et OAuth

Corrections

- Aucune.

Empreintes MD5

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

Agent de terminal

4.5.0.2

Fonctionnalités

- Aucune.

Corrections

- Réduction de la mémoire utilisée pour l'AI Kernel Firewall.
- Utilisation plus rapide des nouveaux points de terminaison d'authentification.
- Suppression des appels à icanhazip.com, auparavant facultatifs mais désormais inutiles.

Empreintes MD5

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

Agent de terminal

4.5.0.3

Fonctionnalités

- L'indicateur de la barre d'état affiche désormais le statut de configuration automatique pour les nouvelles installations.

Hachages MD5

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

Agent de terminal

4.5.1.0

Fonctionnalités

- OpenSSL est désormais utilisé pour les communications TLS.
  - Cela devrait permettre de contourner les problèmes sur les anciennes versions de systèmes d'exploitation qui ne reçoivent plus de correctifs pour les nouvelles exigences TLS.

Corrections

- Amélioration de la prise en charge de l'analyse des signatures Authenticode non conformes.

Hachages MD5

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

Agent de terminal

4.5.1.2

Fonctionnalités

- Suppression de l'ancienne validation de certificat qui reposait sur des bibliothèques Windows intégrées et lentes.
- Ajout de la possibilité de conserver les journaux lors de la désinstallation.

Hachages MD5

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

Agent de terminal

4.5.2.1

Fonctionnalités

- Diffusion élargie des rapports pour l'accès à Fortress AI

Corrections

- Optimisation des opérations du noyau Cyber Crucible n'utilisant pas les API Windows afin de contrer l'augmentation de la latence dans certains environnements Windows d'environ 20 %.

Hachages MD5

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

Agent de terminal

4.5.2.2

Corrections

- Optimisation des opérations du noyau de Cyber Crucible grâce à l'évitement des fonctionnalités problématiques du bus d'événements et de données du système d'exploitation principal Windows.

Empreintes MD5

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

Agent de terminal

4.5.3.0

Fonctionnalités

- FortressAI
  - Ajout de notifications lorsqu'une violation de politique est signalée
    - Intégration avec le Centre de notifications Windows
  - Ajout d'une interface graphique pour consulter l'historique des notifications de politique
  - Ajout du mode simulation
- Cyber Crucible Core
  - Analyse DLL asynchrone configurable pour les machines disposant de ressources matérielles minimales
  - Analyse et télémétrie de la création de processus
    - utilise désormais la persistance sur disque
    - suppression des dépendances au MiniFilter Windows
  - Analyse et télémétrie des injections de processus
    - utilise désormais la persistance sur disque
    - suppression des dépendances au MiniFilter Windows
  - Suppression de dépendances supplémentaires aux ressources du noyau Windows

Corrections

- Optimisation du signalement de la télémétrie pour un reporting encore plus rapide
- Suppression d'un interblocage dû à un accès exclusif ou partagé à une ressource spécifique du noyau, exigé par Microsoft Defender lorsque celui-ci active le mode débogage du pilote

Empreintes MD5

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

Agent de terminal

4.5.3.1

Fonctionnalités

- FortressAI
  - Détecte les tentatives de contournement des contrôles de politique par l’utilisation de captures d’écran.
- Cyber Crucible Core
  - Prend en charge la réinitialisation de l’identité d’un agent sans nécessiter un redéploiement complet.
    - Cela corrige les situations où une machine sur laquelle Cyber Crucible est installé est clonée, clonant ainsi la licence et les identifiants de l’agent. Tout comme pour les adresses IP, les adresses MAC, les noms de machine et autres identifiants uniques, Cyber Crucible identifie un agent cloné et alerte les administrateurs CC de la possibilité de générer de nouveaux identifiants CC.

Hachages MD5

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

Agent de terminal

4.5.3.2

Fonctionnalités

- FortressAI
  - Aucune
- Cyber Crucible Core
  - Amélioration du fonctionnement du tampon du noyau
    - Le pilote exploite des tampons pour stocker temporairement la télémétrie qui est finalement envoyée au tableau de bord client. Cette activité est distincte de l'alimentation ou du fonctionnement du modèle comportemental.
    - Si un tampon du noyau est surchargé, la charge CPU du système augmente.
      - Cela ne se produirait qu'en raison d'un bug majeur du système d'exploitation ou d'une attaque sur les systèmes.
      - Notification automatisée du client en cas d'utilisation très élevée du tampon disponible le 1 JUIN 2026.
    - Presque toutes les opérations de tampon du noyau pour CC impliquent trois tampons principaux.
    - Le pourcentage d'utilisation des trois tampons principaux est désormais transmis à l'infrastructure CC pour la collecte de métriques et l'identification de l'utilisation des tampons par agent.
    - Les trois tampons principaux peuvent voir leur taille ajustée à distance, et leur statut est suivi par les utilisateurs.

Corrections

- Une mise à jour récente impliquant les bibliothèques redistribuables DotNet et MSVC a submergé les tampons de Cyber Crucible avec des événements d'opérations de processus et de DLL très élevés et soutenus (500 % et plus), affectant certains clients. Bien que l'utilisation des tampons soit revenue au niveau normal de 1 à 5 %, y compris pour les clients concernés, tous les tampons ont vu leur taille doublée pour anticiper tout problème futur. Ceci vient s'ajouter aux capacités de configuration mentionnées ci-dessus.

Hachages Sha-256

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

Middleware (serveurs REST)

Middleware 01.23

Fonctionnalités

- Mise en œuvre d’un contrôleur pour les licences de formation et ajout d’un service d’expiration des licences de formation.
- Mise à jour de chaque point de terminaison pour prendre en compte la nouvelle fonctionnalité de mode formation de l’application web, ainsi que des tests pour chaque point de terminaison relatifs au mode formation.
- Ajout d’un point de terminaison permettant de réinitialiser toutes les données de formation d’un groupe parent à leur état d’origine.
- Mise en œuvre des points de terminaison pour le nouveau paramètre de politique de vieillissement des mots de passe pour les groupes.
- Ajout de la documentation pour les points de terminaison Reactive Springboot.

Middleware 04.23

Fonctionnalités

- Mises à jour du Portail Partenaire :
  - Mise en œuvre des points de terminaison pour le nouveau processus d'enregistrement de transaction (Register Deal) avec approbation des transactions par Cyber Crucible
  - Mise à jour du modèle PartnerDeal pour associer un type aux transactions, chacun ayant un pourcentage de remise associé
    - Mise à jour également du modèle PartnerDeal pour les transactions de type Référence (Referral) afin de stocker le compte utilisateur du Tableau de bord à associer aux licences de la transaction
  - Mise à jour du modèle PartnerDeal pour pouvoir distinguer la facturation mensuelle de la facturation annuelle pour le paiement des transactions
    - Comprend la mise à jour des points de terminaison existants pour prendre en compte la facturation mensuelle par rapport à la facturation annuelle pour Stripe
  - Mise en œuvre des points de terminaison permettant d'envoyer des devis via Stripe pour une transaction
  - Mise en œuvre d'un point de terminaison pour renvoyer la facture Stripe d'une transaction
  - Mise en œuvre d'un point de terminaison pour modifier plusieurs champs d'une transaction simultanément, associé à la fenêtre modale de modification de transaction dans l'application Web
- Gestion des agents/licences :
  - Mise en œuvre d'un point de terminaison pour attribuer des licences en masse aux agents
  - Mise en œuvre d'un point de terminaison pour modifier le paramètre de réattribution automatique de licence pour un agent donné
  - Mise en œuvre d'un point de terminaison pour libérer une licence d'un agent en transmettant l'agentId dans la requête
- Mise en œuvre des points de terminaison pour récupérer et enregistrer le paramètre utilisateur permettant d'afficher l'icône de configuration du script d'installation sur la grille des Groupes
- Mise en œuvre d'un point de terminaison pour récupérer la valeur d'authentification client du script d'installation d'agent pour un groupe
- Mise à jour de notre service de scanner antivirus pour effectuer des recherches dans la collection des incidents d'identité en plus de la collection de création de processus

- Diverses mises à jour de notre liste de données par défaut et de listes blanches d'identité pour les antivirus.
- Mise en œuvre d'un nouveau point de terminaison de flux de modifications (change stream) pour détecter les nouvelles insertions de réponses à l'extorsion (Extortion Response)
- Mise en œuvre d'un point de terminaison pour copier les listes blanches vers un autre groupe
- Mise en œuvre d'un point de terminaison pour télécharger le fichier de différence mémoire (Memory Diff File) d'un incident
- Mise en œuvre de la catégorisation des programmes d'incidents d'identité en applications
- Mise en œuvre de l'enregistrement des modes de colonnes pour chaque grille de page Web ainsi que des paramètres de visibilité des graphiques

Middleware 08.23

Fonctionnalités

- Mises à jour du portail partenaire :
  - Implémentation de points de terminaison permettant de créer un POC pour les accords partenaires approuvés
  - Implémentation de points de terminaison pour la page de gestion des groupes de distributeurs dans l'application Web
  - Implémentation d'un point de terminaison pour renvoyer les données de la grille de gestion des paiements dans l'application Web
  - Implémentation de la possibilité de changer le propriétaire d'un accord partenaire
  - Implémentation de la possibilité de définir un mémo personnalisé pour les accords partenaires apparaissant sur les factures et devis Stripe
- Implémentation d'un point de terminaison permettant de renvoyer les invitations de compte utilisateur
- Ajout d'options d'étiquetage d'application supplémentaires pour les objets d'accès à l'identité
- Mise à jour du modèle de groupe pour les groupes partenaires afin d'y ajouter de nouveaux champs booléens indiquant le type de partenaire
- Mise à jour du modèle de groupe afin d'y inclure une liste de configurations d'extensions canari
- Diverses mises à jour de notre liste par défaut de listes blanches de données, d'identités et de certificats pour les antivirus
- Activation de la prise en charge de HTTP/2
- Mise à niveau de notre Spring Boot vers la dernière version, ainsi que diverses autres dépendances
- Implémentation d'alertes de notification pour les accès à l'identité anormaux
- Activation de la compression des réponses du serveur pour les agents
- Implémentation du filtrage pour la colonne « Aucun certificat de confiance » de la grille d'accès à l'identité dans l'application Web pour les options « Récupération des informations de certificat déconnectée » et « Récupération des informations de certificat expirée »
- Correction d'un problème dans notre service de notification d'expiration des accords partenaires afin de ne pas envoyer d'e-mails d'expiration pour les accords terminés

Middleware 11.23

Fonctionnalités

- Mises à jour de la liste blanche
  - Mise en œuvre de la possibilité de créer une exception avec le chemin et les arguments du programme parent
  - Mise en œuvre de la possibilité de créer une exception pour faire correspondre les réponses d'extorsion lorsqu'il n'y a que des certificats de confiance, ne faire correspondre que lorsqu'il n'y a pas d'injections associées, et ne faire correspondre que lorsqu'il n'y a pas de mémoire modifiée
  - Mise en œuvre de la possibilité de créer une exception pour faire correspondre des déclencheurs d'accès à des fichiers spécifiques
- Mise en œuvre du paramètre de groupe pour libérer automatiquement les licences des agents inactifs
  - Mise à jour du modèle de groupe pour disposer d'un paramètre déterminant quand libérer les licences des agents inactifs du groupe. Les options sont 30/60/90 jours, ou la désactivation de ce paramètre
  - Mise à jour du modèle d'agent pour ajouter un nouveau statut inactif
  - Mise en œuvre d'un service permettant de libérer automatiquement les licences des agents inactifs selon le paramètre de leur groupe
- Mise à jour du point de terminaison pour la récupération des réponses d'extorsion afin d'inclure le chemin et les arguments du programme parent
  - Le chemin et les arguments du programme parent sont désormais également inclus dans le décompte des réponses d'extorsion uniques pour l'application Web, les alertes de notification de sécurité et les résumés exécutifs
- Mise à jour de nos rapports de résumé exécutif afin de séparer la diapositive des licences en diapositives distinctes pour les licences de bureau et de serveur
- Mise à jour du modèle de notification par e-mail de sécurité et du service de notification de sécurité afin d'inclure deux nouveaux types d'alerte
  - Modèle comportemental ajusté
  - Nouvelle version de l'agent
    - Lorsque les paramètres de mise à jour gérée d'un groupe sont modifiés pour désactiver la mise à jour automatique, une notification « Nouvelle version de l'agent » est automatiquement créée pour le groupe
- Mises à jour des rôles/permissions utilisateur
  - Mise à jour des permissions du modèle de rôle Gestionnaire d'incident pour n'avoir désormais que la visualisation/l'édition des listes blanches et des règles de réponse silencieuse

    - Les groupes disposent désormais de 3 rôles par défaut non modifiables par l'utilisateur :
        - Admin
        - Lecture seule
        - Invité
    - Les utilisateurs ajoutés à un groupe se voient attribuer par défaut le rôle Invité
- Mise en œuvre de points de terminaison pour la fenêtre modale de réglage des processus utilitaires du navigateur de l'application Web afin de gérer facilement la manière dont les agents d'un groupe doivent répondre aux processus utilitaires de Chrome
- Mise à jour du point de terminaison du graphique de la page Agents afin de pouvoir limiter les décomptes aux agents ayant contacté le serveur au cours des 30/60/90 derniers jours
- Mise à jour de l'alerte e-mail de notification de sécurité relative à l'activité de rançongiciel afin d'inclure un lien redirigeant automatiquement les utilisateurs vers la page des réponses d'extorsion avec un filtre affichant les réponses concernées par l'alerte
- Mise en œuvre d'un paramètre de groupe permettant de définir si les agents d'un groupe s'exécutent ou non en mode sans échec
- Mise en œuvre d'une option de script PowerShell pour l'installation des agents
- Mise à niveau de notre Spring Boot vers la dernière version
- Diverses mises à jour de notre liste de données par défaut + identités + listes blanches de certificats pour les antivirus

Middleware 04.24

Fonctionnalités

- Mise en œuvre du paramètre de groupe et des points de terminaison associés pour la configuration et la gestion des configurations de proxy afin de faciliter le déploiement des agents
- Mise à jour de nos points de terminaison de données de télémétrie afin de pouvoir afficher toutes les données de télémétrie ou uniquement les données directement liées à une réponse à une extorsion
- Mise en œuvre du paramètre de groupe permettant de masquer automatiquement les agents dans les groupes lorsqu'une licence est libérée d'un agent, qu'un agent est marqué comme inactif, ou qu'un agent termine une désinstallation
- Mise à jour des liens vers notre tableau de bord dans nos e-mails de notification afin d'inclure un paramètre d'URL utilisé pour filtrer automatiquement les données sur la grille frontend associée, afin d'afficher ce qui a déclenché la notification
- Mise à jour du point de terminaison utilisé pour le graphique des licences d'agents frontend afin d'inclure les décomptes pour les licences Desktop et Server
- Mise en œuvre des points de terminaison pour la nouvelle page frontend « Customer Deployment Health »
- Mise à jour de notre réglage des processus afin de tenir compte de Microsoft Edge WebView

Middleware 09.24

Fonctionnalités

- Implémentation des points de terminaison pour le nouveau paramètre de Mode DMZ de groupe
- Mise à jour des points de terminaison d’enregistrement des offres afin de permettre l’enregistrement d’offres pluriannuelles avec la possibilité de payer d’avance ou annuellement pour les offres pluriannuelles
- Ajout de la possibilité de visualiser l’analyse des causes profondes pour les accès d’identité
- Implémentation des comportements adaptés temporaires
- Mise à jour du modèle Utilisateur afin d’enregistrer le paramètre permettant de masquer ou d’afficher par défaut les licences d’agent expirées dans la grille des licences d’agent
- Mise à jour du modèle de notification de sécurité et des points de terminaison/services associés pour les nouvelles options d’alerte d’agent hors ligne « Partiellement » et « Entièrement » hors ligne
- Mises à jour des points de terminaison liés à l’ajout des nouvelles colonnes côté interface dans la grille des agents, afin d’afficher la date d’expiration de la licence attribuée et la date d’attribution de la licence à l’agent
- Ajout d’un paramètre au modèle de groupe permettant aux agents du groupe d’afficher l’icône de l’agent dans la barre d’état système de la machine agent correspondante
- Mise à jour des requêtes de grille côté serveur afin de pouvoir prendre en charge des filtres à conditions multiples pour une même clé/colonne

Middleware 05.25

Fonctionnalités

- Mise à jour du modèle de notification des ventes avec de nouveaux types :
  - Les partenaires distributeurs peuvent recevoir des alertes lorsque leurs sous-groupes de revendeurs créent un nouvel enregistrement de transaction (Deal Registration)
  - Activité des points de contact (POC) des transactions partenaires
- Mise à jour du processus d'authentification pour permettre l'intégration SSO avec Microsoft Entra ID (Azure Active Directory)
- Mise à jour du point de terminaison de l'installateur d'agent pour permettre un nouveau type d'installateur pour Native Cli
- Mise à jour des points de terminaison pour les nouvelles mises à jour des partenaires distributeurs
  - Ajout d'un nouveau modèle Partner in Motion
  - Mise à jour du modèle d'enregistrement des transactions partenaires afin de permettre aux distributeurs d'approuver les transactions de leurs sous-groupes de revendeurs
  - Ajout de la possibilité pour les partenaires distributeurs de modifier les remises pluriannuelles pour leurs sous-groupes de revendeurs
  - Ajout de la possibilité pour les distributeurs de s'envoyer des devis avec leur tarification de distributeur pour une transaction d'un sous-groupe de revendeurs
  - Ajout d'une exigence selon laquelle, lorsqu'un sous-groupe de revendeurs enregistre une transaction, l'accord de sous-groupe revendeur (Subgroup Reseller Agreement) doit être téléversé par son distributeur parent sur la page de gestion des groupes de distributeurs
- Mise à jour du modèle de rôle avec un nouveau rôle de Gestionnaire des transactions partenaires (Partner Deal Manager) pour les opérations d'enregistrement des transactions, et mise à jour de chaque point de terminaison associé afin de vérifier les autorisations
- Ajout du point de terminaison permettant de modifier les paramètres d'un groupe en masse
- Mise à niveau de notre Spring Boot vers la dernière version
- Amélioration des requêtes utilisées pour la génération des rapports de direction afin de réduire le temps nécessaire à leur génération
- Migration de nos collections de télémétrie dans la base de données vers l'utilisation du sharding
- Mise à jour de la requête des agents utilisée pour la grille du tableau de bord afin d'indiquer si l'agent est un serveur ou non

- Mise à jour du point de terminaison /updateGroupAutomaticallyHideAgentsReactive afin d’appliquer rétroactivement la mise à jour aux agents existants
- Mises à jour majeures de l’authentification pour permettre aux agents d’appeler nos serveurs REST avec la nouvelle authentification OAuth hébergée
- Ajout de nouveaux points de terminaison pour la soumission de télémétrie DLL par les agents

Middleware 12.25

Fonctionnalités

- Ajout de nouveaux points de terminaison pour la visualisation des DLL sur le tableau de bord, permettant de consulter les chargements de modules non fiables associés aux Réponses à l'extorsion, aux Créations de processus, aux Injections de processus et aux Accès d'identité
- Mise à jour des points de terminaison des requêtes du tableau de bord pour les Réponses à l'extorsion et les Accès d'identité afin de retourner des champs supplémentaires pour la visualisation des DLL, notamment la mémoire de module modifiée, le chemin de module modifié, etc.
- Mise à jour du modèle Agent avec de nouveaux champs indiquant si l'agent est entièrement configuré et la date à laquelle l'agent a été entièrement configuré pour la première fois
- Ajout de nouveaux points de terminaison et d'un contrôleur pour la page de gestion du pare-feu IA
- Mise à jour du point de terminaison retournant la liste des agents pour le tableau de bord afin d'inclure de nouveaux champs indiquant vers quel serveur REST et serveur OAuth l'agent effectue ses appels, ainsi que les adresses IPv4 et IPv6 WAN de l'agent
- Ajout d'un nouveau point de terminaison pour la page des Réponses à l'extorsion, permettant aux utilisateurs de consulter tous les champs d'une Réponse à l'extorsion dans ce point de terminaison, plutôt que d'utiliser le point de terminaison existant qui propose une vue condensée des champs et nécessite un appel API supplémentaire pour obtenir plus de détails.
  - Les utilisateurs du tableau de bord peuvent utiliser le bouton bascule sur la page des Réponses à l'extorsion pour choisir entre l'option de grille précédente et la nouvelle option de grille qui retourne tous les champs dans une seule grille
- Ajout d'une nouvelle option dans les Notifications de sécurité permettant d'inclure un fichier CSV dans l'alerte par e-mail pour les alertes de Rançongiciel et d'Accès d'identité, contenant des informations sur la raison du déclenchement de l'alerte.

Application Web

Application Web 04.23

Fonctionnalités

- Mises à jour du Portail Partenaire :
  - Possibilité de planifier une démonstration sur la page Enregistrer une Affaire
  - Mise en œuvre du nouveau processus d'Enregistrement d'Affaire avec Approbation des Affaires par Cyber Crucible
  - Ajout d'un Type de Prospect d'Affaire lors de l'enregistrement des affaires
  - Ajout des Cycles de Facturation Mensuel et Annuel pour les affaires
  - Mise en œuvre de l'envoi de devis pour les affaires approuvées par Cyber Crucible via Stripe et de la signature des devis avant de finaliser une affaire
  - Possibilité de renvoyer la facture Stripe pour une affaire finalisée
  - Possibilité de modifier une affaire via une fenêtre modale, similaire à la fenêtre modale d'enregistrement de nouvelle affaire, pré-remplie avec les informations actuelles de l'affaire
- Gestion des Agents/Licences :
  - Possibilité de libérer des licences depuis la page Agents en masse
  - Possibilité d'attribuer des licences aux agents en masse sur la page Agents
  - Possibilité, sur la page Agents, de consulter et de modifier les paramètres de relicenciement automatique des agents lorsqu'ils se connectent à notre serveur REST sans licence
    - Les utilisateurs peuvent mettre à jour les agents individuellement ou en masse
- Mise en œuvre, sur la page Groupes, de la possibilité de consulter l'Id d'un groupe et les valeurs d'Authentification Client utilisées dans le Script d'Installation de l'Agent
- Mise en œuvre de la possibilité de copier des listes blanches vers un autre groupe
- Mise à niveau vers React 18
- Ajout des options de réinitialisation des colonnes et de redimensionnement automatique de toutes les colonnes dans le menu contextuel des grilles lors d'un clic droit
- Ajout de l'option de téléchargement du fichier de différence mémoire (Memory Diff File) dans la grille des Réponses à l'Extorsion pour les réponses applicables
- Mise en œuvre de l'enregistrement de l'état de visibilité des graphiques
- Ajout de nouvelles colonnes Application dans la grille Accès à l'Identité pour les programmes accédés, accédants et parents.
- Mise en œuvre du basculement du mode d'affichage des colonnes sur chaque grille pour le nombre de colonnes à afficher. Les modes incluent : Min, Moyen, Max et Personnalisé
- Mise en œuvre de la fonctionnalité de recherche/autocomplétion dans les éléments de sélection déroulante (Dropdown Select) avec Material UI

Application Web 08.23

Fonctionnalités

- Mises à jour du Portail Partenaire :
  - Ajout de la page Vidéos de démonstration au Portail Partenaire
  - Ajout de la possibilité de créer un POC pour les accords partenaires approuvés
  - Ajout de la page Gestion des groupes de distributeurs au Portail Partenaire permettant aux partenaires distributeurs de créer et de gérer leurs sous-groupes
  - Ajout de la page Gestion des paiements au Portail Partenaire
  - Ajout de la possibilité de modifier le propriétaire d'un accord partenaire
  - Ajout d'un champ de note personnalisé pour les accords partenaires, affiché sur les factures et devis Stripe
- Mise en œuvre d'une fonctionnalité Se souvenir de moi permettant aux utilisateurs de rester connectés
- Ajout d'un lien permettant d'accéder au Portail Client Stripe où les utilisateurs peuvent gérer leurs abonnements et leurs modes de paiement
- Ajout, sur la page Licences des Agents, de la possibilité de modifier le groupe de plusieurs licences sélectionnées dans la grille
- Mise à niveau d'AG Grid vers la version 29
- Mise à jour des dépendances vers leurs dernières versions
- Suppression du bouton Automatisation au-dessus des grilles qui affichait des icônes, et placement des icônes directement au-dessus de la grille
- Suppression du bouton Colonnes au-dessus des grilles qui affichait les Options d'état des colonnes de la grille, et placement des Options d'état des colonnes de la grille directement au-dessus de la grille
- Ajout de la possibilité de renvoyer les invitations de compte utilisateur sur la page Groupes
- Ajout de la colonne Mode Extension Canary à la page Groupes
- Ajout d'un étiquetage d'application supplémentaire à la page Accès Identité
- Ajout d'icônes et de filtres sur la grille Accès Identité pour la colonne Aucun certificat de confiance, pour les statuts « Déconnecté lors de la récupération des informations de certificat » et « Délai dépassé lors de la récupération des informations de certificat »
- Correction d'un problème d'affichage des grilles sur les appareils mobiles

Application Web 11.23

Fonctionnalités

- Ajout de la possibilité de libérer automatiquement les licences des agents inactifs.
  - Cette fonctionnalité est un paramètre de groupe et les options permettent de libérer automatiquement les licences des agents inactifs du groupe après 30/60/90 jours, ainsi que de désactiver ce paramètre
- Mises à jour de la liste blanche
  - Ajout de la possibilité de créer une exception avec le chemin du programme parent et les arguments
  - Ajout de la possibilité de créer une exception pour faire correspondre les réponses d'extorsion lorsqu'il n'y a que des certificats de confiance, correspondre uniquement lorsqu'il n'y a pas d'injections associées, et correspondre uniquement lorsqu'il n'y a pas de mémoire modifiée
  - Ajout de la possibilité de créer une exception pour faire correspondre des déclencheurs d'accès à des fichiers spécifiques
- Ajout du chemin du programme parent et des arguments à la grille des réponses d'extorsion
- Ajout des empreintes de fichiers (hashes) à la fenêtre modale des détails de la réponse d'extorsion
- Ajout de nouveaux types d'alertes de notification de sécurité :
  - Modèle comportemental ajusté
  - Nouvelle version d'agent
- Mise à jour des e-mails d'alerte d'activité de rançongiciel pour inclure un lien qui redirigera automatiquement les utilisateurs vers la page des réponses d'extorsion avec un filtre affichant les réponses concernées par l'alerte
- Ajout d'une option sur le graphique de la page Agents pour n'inclure dans le graphique que le nombre d'agents ayant communiqué au cours des 30/60/90 derniers jours, ainsi que l'option pour ne pas limiter le décompte
- Ajout d'exemples sur la page Intégration REST concernant l'appel au point de terminaison aws /token. Les exemples incluent l'appel au point de terminaison avec bash, powershell et l'invite de commandes
- Mise à jour des autorisations du Gestionnaire d'incidents sur la page Rôles afin de ne disposer que des droits de visualisation/modification pour les listes blanches et les règles de réponse silencieuse
- Le Gestionnaire d'automatisation des réponses, obsolète, a été supprimé de la page Rôles
- Ajout de la fenêtre modale de réglage des processus utilitaires du navigateur aux pages Listes blanches, Règles de réponse silencieuse et Réponses d'extorsion

    - Comprend l'option permettant de sélectionner la manière dont les agents des groupes doivent répondre aux processus utilitaires de chrome
- Ajout de l'option pour télécharger l'agent à l'aide d'un script powershell
- Ajout du paramètre de groupe permettant aux agents du groupe de s'exécuter en mode sans échec
- Ajout de la colonne Nom du système d'exploitation à la grille des agents
- Correction d'un problème sur certaines grilles où la largeur et l'ordre des colonnes se réinitialisaient lors de clics sur les icônes/boutons de la page

Application Web 04.24

Fonctionnalités

- Ajout de la possibilité de configurer et de gérer des configurations de proxy afin de faciliter le déploiement des agents. Découvrez-en plus sur les configurations de proxy ici
- Correction du problème où la barre de défilement horizontale en bas de nos grilles de données n'était pas visible en raison du fait que la grille s'étendait au-delà de la hauteur d'écran visible
- Ajout de la possibilité, sur nos pages de télémétrie, de basculer entre l'affichage de toutes les données de télémétrie ou uniquement des données directement liées à une réponse à une extorsion
- Ajout du paramètre de groupe permettant de masquer automatiquement les agents du groupe lorsqu'une licence est libérée d'un agent, qu'un agent est marqué comme inactif, ou qu'un agent termine une désinstallation
- Ajout de la possibilité, lors d'un clic sur un lien provenant de l'un de nos e-mails de notification, de filtrer automatiquement les données de la grille correspondante afin d'afficher ce qui a déclenché la notification
- Mise à jour du graphique des licences d'agents afin d'afficher le nombre de licences Desktop et Serveur
- Mise à niveau d'AG Grid vers la version 31
- Mise à niveau d'Ag Charts vers la version 9
- Ajout d'options de filtrage de texte supplémentaires à nos grilles de données
- Ajout de la page Customer Deployment Health (accessible sous l'onglet Opérations)

Application Web 09.24

Fonctionnalités

- Ajout, sur la page des licences des agents, de la possibilité de filtrer par défaut les licences expirées de la grille et du graphique. Ce paramètre peut être modifié via le bouton situé au-dessus de la grille des licences des agents
- Mise en œuvre de filtres à conditions multiples pour une seule colonne sur les grilles côté serveur. Les grilles côté serveur sont celles où toutes les lignes ne sont pas chargées dans la grille lors du chargement initial en raison du grand nombre de lignes : Réponse à l'extorsion, Créations de processus, Injections de processus et Accès aux identités
- Ajout de l'option pluriannuelle pour les enregistrements d'opérations (Deal Registrations). Les opérations peuvent durer jusqu'à 3 ans, et les utilisateurs ont la possibilité de payer d'avance ou de payer annuellement pour les opérations pluriannuelles
- Mise en œuvre des comportements adaptés temporaires (Temporary Tailored Behaviors).

  Pour en savoir plus, cliquez ici
- Ajout d'une nouvelle colonne dans la grille des accès aux identités pour l'analyse des causes profondes (Root Cause Analysis)
- Mise à jour des notifications de sécurité avec deux options distinctes pour les alertes d'agents hors ligne : alertes d'agents partiellement hors ligne et entièrement hors ligne
- Ajout de nouvelles colonnes dans la grille des agents pour la date d'expiration de la licence et la date d'attribution de la licence à l'agent
- Ajout du nouveau paramètre de groupe pour le mode DMZ à suivre par les agents du groupe. Le mode DMZ est destiné aux environnements où la vérification en ligne des certificats n'est pas disponible. L'activation du mode DMZ intègre localement les racines d'autorité de certification (CA) sur les agents du groupe et désactive l'OSCP
- Ajout du nouveau paramètre de groupe permettant aux agents du groupe d'afficher une icône d'agent dans la barre d'état système de la machine agent concernée ; seuls les agents en version 4.4.8.2 et supérieure disposent de cette fonctionnalité
- Ajout d'une barre latérale à nos grilles de données pour modifier facilement la visibilité et l'ordre des colonnes

Application Web 05.25

Fonctionnalités

- Ajout de l'intégration SSO pour la connexion à notre tableau de bord avec Microsoft Entra ID (Azure Active Directory)
  - Les utilisateurs doivent contacter Cyber Crucible et effectuer quelques étapes disponibles ici pour intégrer le SSO Entra ID pour leur organisation avec la connexion à notre tableau de bord
- Mises à jour pour les partenaires distributeurs
  - Améliorations du processus permettant aux distributeurs d'associer des sous-groupes de revendeurs et à ces sous-groupes de revendeurs de s'enregistrer et de finaliser des transactions. Une explication plus détaillée du processus amélioré de gestion des groupes de distributeurs est disponible ici
  - Ajout d'un nouveau type de notification de vente pour les partenaires distributeurs afin de recevoir des alertes lorsque leurs sous-groupes de revendeurs créent un nouvel enregistrement de transaction
  - Ajout de la possibilité pour les partenaires distributeurs de modifier les remises pluriannuelles pour leurs sous-groupes de revendeurs. Cette fonctionnalité se trouve sur la page de gestion des groupes de distributeurs
  - Ajout de la colonne Approbation du distributeur dans l'enregistrement des transactions permettant aux distributeurs de gérer les transactions de leurs sous-groupes de revendeurs
  - Ajout de la page Partenaire en préparation, disponible sous l'onglet Partenaires, permettant aux partenaires distributeurs d'enregistrer les partenaires sous-groupes de revendeurs en cours de développement
- Ajout du rôle Gestionnaire de transactions partenaires pour les opérations liées à l'enregistrement des transactions
- Ajout d'un nouveau type de notification de vente pour l'activité des POC de transactions partenaires. Cette alerte s'applique au nouveau groupe POC créé lorsqu'un partenaire crée un POC pour une transaction. Des alertes de ce type sont envoyées lors de l'installation/désinstallation d'agents et lorsque les licences POC expirent dans le groupe POC
- Ajout du nouveau type d'installateur d'agent « Native CLI »
- Ajout de la fenêtre modale de modification de groupe sur la page de gestion des groupes, permettant de modifier en masse les paramètres du groupe
- Mise à niveau d'AG Grid vers la version 32
- Ajout d'un bouton/bascule de visibilité du mot de passe pour la connexion

Web Application 12.25

Fonctionnalités

- Ajout de la nouvelle page de gestion du pare-feu IA, disponible dans l'onglet Operations
- Visualisation des DLL
  - Ajout de la possibilité de consulter les chargements de modules associés pour les Extortion Responses, Process Creations, Process Injections et Identity Accesses
  - Une nouvelle colonne a été ajoutée à ces pages, indiquant si des chargements de modules non fiables associés ont été détectés. Lorsqu'un chargement de module non fiable est détecté, la cellule de cette colonne affiche une icône sur laquelle les utilisateurs peuvent cliquer pour accéder à une nouvelle page présentant tous les chargements de modules non fiables associés
- Ajout de nouvelles colonnes aux grilles Extortion Responses et 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
- Ajout à la grille Extortion Responses de la colonne « Data Access Attempted », qui indique le chemin sur la machine où la tentative d'accès aux données a eu lieu
- Mise à jour de la page Extortion Responses, qui propose désormais 2 options d'affichage différentes. L'option de grille précédente, offrant une vue plus condensée des extortion responses avec la grille parent/enfant, existe toujours ; une nouvelle option permettant de supprimer la grille parent/enfant et d'afficher toutes les données et colonnes sur une seule grille est désormais disponible
- Ajout de colonnes à la grille Agents indiquant si l'agent est entièrement configuré et la date à laquelle l'agent a été entièrement configuré pour la première fois
- Ajout de colonnes supplémentaires à la grille Agents indiquant le serveur OAuth et le serveur REST auxquels l'agent fait appel, ainsi que les adresses IPv4 et IPv6 WAN de l'agent
- Ajout des supports co-marqués (Co-branded Collateral) dans l'onglet Partners, permettant aux partenaires de télécharger un fichier .zip contenant tous les supports co-marqués
- Mise à niveau d'AG Grid vers la version 34
- Ajout du nombre de jours restants avant l'expiration d'une licence sur la page Agent Licenses et sur la page Agents. Cette information apparaît sous forme d'icône dans la colonne Renews de la page Agent Licenses, et dans la colonne License Expiration Date de

la page Agents

- Ajout d'une nouvelle option dans les Security Notifications permettant d'inclure un fichier CSV dans l'e-mail d'alerte pour les alertes Ransomware et Identity Access, contenant des informations sur la raison du déclenchement de l'alerte. Cette option a été ajoutée afin que les utilisateurs puissent consulter la raison d'une alerte directement dans l'e-mail, sans avoir à se connecter au tableau de bord