Software Releases

- Endpoint Agent
  - Endpoint Agent Version Index
  - 4.4.0.9
  - 4.4.0.9.1
  - 4.4.1.0
  - 4.4.1.1
  - 4.4.1.2
  - 4.4.1.3
  - 4.4.1.4
  - 4.4.2.0
  - 4.4.2.1
  - 4.4.2.2
  - 4.4.2.3
  - 4.4.2.4
  - 4.4.2.5
  - 4.4.2.6
  - 4.4.2.7
  - 4.4.2.8
  - 4.4.3.0
  - 4.4.3.2
  - 4.4.3.1
  - 4.4.4.0
  - 4.4.4.4
  - 4.4.5.1
  - 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
- 4.5.3.2

- Middleware (REST Servers)
  - Middleware 01.23

Endpoint Agent

Endpoint Agent Version Index

- 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

Endpoint Agent

4.4.0.9

Features

- For telementry-enabled groups, added Active Directory data to credential theft watch list

Fixes

- Remove duplicate local volumes and network share entries in some environments.
- Refined behavior for some thumbnail database rebuilds causing incidents
- Fixed license validation bug which could increase startup time
- Refined behavior for file access to write-once media such as CD’s and WORM tape drives

WHCP/WHQL Validation Status

Validated

MD5 Hashes

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

Endpoint Agent

4.4.0.9.1

Features

None - maintenance update.

Fixes

- Fixed some network shares connected by a user being initially ignored in analytics.
- Refined false positive behavior associated with shares appearing during user sessions, followed quickly by a Save As dialog box.

WHCP/WHQL Validation Status

Validated.

MD5 Hashes

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

Endpoint Agent

4.4.1.0

Features

- Expanded support for processes injection analytics, to dramatically increase the accuracy of detecting malicious vs benign intent for applications.
  - This became especially important due to a small number (<0.02%) of machines in Cyber Crucible telemetry alerting on aggressive process injection behaviors of system processes.
- Increased monitoring capability of unsigned system processes.
  - This was partially in response to attackers focusing heavily on involving those processes during lateral movement operations (on a system, and between systems).

Fixes

- Changed a file modification behavior to decrease false positives by no longer triggering on certain benign actions, through additional kernel-level context to a process' file-access behaviors.

WHCP/WHQL Validation Status

Validated.

MD5 Hashes

```
service.exe   = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)       = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)        = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)        = 6a0f2e55d6a7b66bd9bbe318d5dbbebf
```

Endpoint Agent

4.4.1.1

Features

- Improved analytical processing for parent-child relationships, when the parent process quickly dies before Cyber Crucible completes processing (milliseconds).
  - The extremely common scenario here is that attackers (and legitimate programs) will often open up multiple programs, sometimes in a muli-step “daisy-chain”. This may be on purpose, or due to Windows or other application behavior “under the hood”.
  - Cyber Crucible behavioral models leverage activity & state variables for all processes in a chain of executions to achieve maximum accuracy and context.

Fixes

- Cyber Crucible had a loss in behavioral model decision making accuracy, due to the loss of telemetry when multiple programs each call each other, but one of the programs died in milliseconds.
  - In a chain where Program A executes Program B. Program B starts Program C, but Program B dies within milliseconds (usually a silent crash, but not always). Cyber Crucible behavioral analysis has Program A and Program C variables, but did not have time to completely analyze program B, since it expected it to be running.
  - This has been correcting, resulting in more accurate decision making by the Cyber Crucible hyper-automated decision making engine.

WHCP/WHQL Validation Status

Validated.

MD5 Hashes

```
service.exe   = db76d0abc8f4bc4b2a093435bc314bde
assistant.exe = a5bac35d839d7a57fcccfceb011083c1
```

```
CCRRSecMon.sys (Windows10)       = 935e43368fa95ae740a3f04defcc390d
CCRRSecMon.sys (Windows8)        = ee555ad0f282f36dd11deada8d1ca9c7
CCRRSecMon.sys (Windows7)        = a6a5073c6565361b443651ef29e49490
```

Endpoint Agent

4.4.1.2

Features

- Increased available specificity for whitelists, such as parent process path and arguments.
- Expanded support for identity access analytics to more credential databases.
  - Identity access is now also monitored for Slack, Opera, Thunderbird, Discord, and Vivaldi.
- Expanded whitelist support to include identity access.

Fixes

- Reduced the bandwidth used between agents and the rest API.
- Fixed some older Windows Server editions displaying canaries on in Explorer.
- Fixed some identify access logs missing certificate trust indicators.

WHCP/WHQL Validation Status

Validated

MD5 Hashes

```
service.exe   = e289ef44c5a1bca39d57861ff9d05bee
assistant.exe = d8e83309372b43ffc70feaf2bd538f36
CCRRSecMon.sys (Windows10)       = db736330f5a690a2e828472a357ee6b6
CCRRSecMon.sys (Windows8)        = b9d644930fc52495229dc7f96ffea299
CCRRSecMon.sys (Windows7)        = 7b1ece332986dadfcc6463574fd16616
```

Endpoint Agent

4.4.1.3

Features

- Credential/Identity Monitoring now includes various VPN, cryptocurrency wallet, and other applications.
- In a (this is common) chain of affected processes during an attack (attacker moves from running program A, to B, to C, and D is used for data theft), the “patient 0” program A is suspended, but patient D is reported as the process performing the theft behavior.
  - Memory state is preserved and reported throughout the process chains, for future forensic analysis.
- In the event of an automated response in which a running process' memory was modified, that memory modification is configurably uploaded to Cyber Crucible for reverse engineering and further analysis.
- In the event of a non-malicious memory modification bug in an application, behavioral exceptions (“whitelists”) now have the ability to flag certain memory corruption events as benign. This will not stop the program itself from crashing or losing data due to the bug, but Cyber Crucible will know to ignore the bug while searching for malicious injection of code into running processes (process injection/hollowing).

Fixes

- Removed vulnerability where binaries could be deleted by a privileged process while CC binaries are updating.
- Removed vulnerability where registry keys could be deleted or altered by a privileged process while CC binaries are updating.
- Corrected memory state tracking when a process is patched in-memory during Cyber Crucible evaluation of the memory.
- Corrected memory state tracking under certain conditions where memory is re-allocated between memory pages.
- Minor CPU efficiency updates, that are likely too minor to register in Task Manager, since usage is normally <1%

WHCP/WHQL Validation Status

Validated

MD5 Hashes

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

4.4.1.3.1

Gained visibility into some system processes that initialize before the Cyber Crucible driver loads.

MD5 Hashes:

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

4.4.1.3.2

Added additional telemetry for the now-visible system processes due to 4.4.1.3.1.

MD5 Hashes:

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

4.4.1.3.3

Fixed some incident reports including data for the wrong process, when a process dies mid-calculation.

MD5 Hashes:

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

4.4.1.3.4

Optimization of memory calculations, in preparation for 4.4.1.4.

MD5 Hashes:

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

Endpoint Agent

4.4.1.4

Features

- Upgraded pattern matching capabilities in the behavioral model.
  - This is especially relevant for additional coverage of identity store locations, such as cryptocurrency wallet locations.
- Increased software dependency functionality for (Cyber Crucible) libraries in use for upcoming fully automated identity access protection.
- Opt-in capability to run the agent in safe mode

Fixes

- Optimize memory usage in the service. This would only have been experienced on very busy servers with lots of behavioral analysis occurring (by Cyber Crucible) simultaneously.

MD5 Hashes

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

Endpoint Agent

4.4.2.0

Features

- Upgraded monitoring and prevention capabilities for automated identity access protection.
- Optimize network usage through variable communication rates dependent on client behaviors.

Fixes

- N/A

MD5 Hashes

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

Endpoint Agent

4.4.2.1

Fixes

- Optimized identity information tracking for applications with large number of deeply nested directories.

MD5 Hashes

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

Endpoint Agent

4.4.2.2

Features

- None

Fixes

- Optimization of variable handling for one genre of behavior.
  - Cause: One unspecified security product produced a very large number of behaviors on a couple large servers, which cause excessive memory usage of Cyber Crucible.
  - Symptoms: Cyber Crucible’s memory usage jumps from a few MB to GB’s. The security product’s memory usage also jumped by 100 fold as well, to over 250GB. If you experience this, as that may be independent of Cyber Crucible, please open a support ticket so we may help you. We suspect this was an issue with the security product as well, independent of Cyber Crucible’s optimization.
  - Fix: This behavior variable tracking was migrated from an algorithm which expected low-volume population to a high-volume algorithm like in use elsewhere in the driver.
  - Who is affected? Only one customer was observed with this issue, and only on a small portion of their large servers. Regardless - this update is deployed to all customers.

MD5 Hashes

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

Endpoint Agent

4.4.2.3

Features

- None

Fixes

- Fixed Acronis compatibility issues

MD5 Hashes

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

Endpoint Agent

4.4.2.4

Features

- Credential protection support for Microsoft Teams and Signal Messenger

Fixes

- Suppressed network related logs when in safe mode without networking
- Backup some agent data on uninstall to the Windows temporary storage folder

MD5 Hashes

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

Endpoint Agent

4.4.2.5

Features

- None

Fixes

- Reduced network usage when sending large amounts of reports at once
- Fix handling of some certificate data

MD5 Hashes

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

Endpoint Agent

4.4.2.6

Features

- None

Fixes

- Reduced memory usage in servers with many unique program certificates

MD5 Hashes

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

Endpoint Agent

4.4.2.7

Features

- None

Fixes

- Reduced memory usage during handling of programs that use undefined behavior in querying directories

MD5 Hashes

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

Endpoint Agent

4.4.2.8

Features

- None

Fixes

- Increased logging and telemetry for bad machine states
- Stability increase for Identity protections at boot time

MD5 Hashes

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

Endpoint Agent

4.4.3.0

Features

- In addition to existing service protections, the kernel mode driver will restart the service if it terminates for any reason.

Fixes

- None

MD5 Hashes

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

Endpoint Agent

4.4.3.2

Features

- None

Fixes

- Reduced CPU usage during process starts.
- Reduced CPU usage in trust determinations during consecutive directory queries.

MD5 Hashes

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

Endpoint Agent

4.4.3.1

Features

- None

Fixes

- Fixed some machines with unusual Windows installation characteristics having visible canaries in Explorer.

MD5 Hashes

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

Endpoint Agent

4.4.4.0

Features

- Reports for incidents and telemetry are stored on disk for offline scenarios.
  - Due to tampering attempts observed against multiple EDR/XDR logging stores, Cyber Crucible enabled kernel-level protection against the disk-stored data before deploying this capability.
- Increased protection of the service process used for backend communication and updates, as part of look-ahead zero-trust hardening.
  - This was not in response to an existing threat, but proactive for one the Team sees upcoming.

Fixes

- Fixed processes that load at boot not being available in the dashboard under process creations.
- Prevented two installers from running at the same time, which would use register the same machine twice.

MD5 Hashes

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

Endpoint Agent

4.4.4.4

Features

- None

Fixes

- Improved performance for parsing certificate data on system startup.

MD5 Hashes

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

Endpoint Agent

4.4.5.1

Features

- Reduced bandwidth usage:
  - Use compression for larger telemetry data and larger server responses
  - Use HTTP/2 for compressed headers and greater socket efficiency
- Increased insight into certificate operations.

Fixes

- Encode certificate metadata in raw telemetry when non-RFC-compliant labels exist. Network security infrastructure was corrupting or deleting the payloads, causing the agent to re-transmit until success.

MD5 Hashes

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

Endpoint Agent

4.4.5.2

Features

- New kernel level access telemetry for network-based behaviors, to better identify possible client-side networking bugs, or opportunities to optimize
- Outbound telemetry is now bundled and sent together, just like inbound settings
  - Transmitted with a 25% timing variance, so that every machine will not be sending packets simultaneously across a client network
- HTTP/2 is now fully utilized end to end

Fixes

- Reduced minimum threads in use in userspace
- Reduced CPU usage for userspace service
- Agent-Server authentication is now performed more efficiently
- Replaced previous service sleep <> restart algorithm when licenses were not available.
  - Previous algorithm caused a "service exited unexpectedly" in event manager every 15 minutes.
  - Allowing the Operating System to tell the service to shut off (something abused by criminals and other security tools) would have allowed a “clean” service restart without event manager logs. Instead of creating that vulnerability, Cyber Crucible’s service restarted itself without Windows involvement, causing the event log.

MD5 Hashes

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

Endpoint Agent

4.4.5.3

Features

- Added a second domain for server communication (see domain list here).
  - If there are communication issues with one domain the agent will automatically switch to the other.

Fixes

- Changed some old legacy strings that referred to “Ransomware Rewind” to now refer to “Cyber Crucible”.

MD5 Hashes

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

Endpoint Agent

4.4.5.9

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
  - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.
- This is a milestone release from incremental releases found in 4.4.5.4 - 4.4.5.8, all aligned on the previous cryptography analysis hardening functionality.
  - Early telemetry indicates the failures in Windows certificate and cryptography libraries were legitimately responded to by Cyber Crucible.
  - It is unknown at this time what percentage of issues were due to exploitation vs a Windows core library bug. Please contact your Cyber Crucible representative to discuss further as necessary.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

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

Endpoint Agent

4.4.5.8

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
  - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

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

Endpoint Agent

4.4.5.5

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
  - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

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

Endpoint Agent

4.4.5.6

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
  - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

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

Endpoint Agent

4.4.5.7

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
  - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

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

Endpoint Agent

4.4.5.4

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
  - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

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

Endpoint Agent

4.4.6.0

Features

- CPU performance enhancement for some applications which burst large numbers of automated & simultaneous directory traversals as part of their application behaviors.

Fixes

-

MD5 Hashes

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

Endpoint Agent

4.4.6.1

Features

- Further migration from the “Ransomware Rewind” product name to “Cyber Crucible”.
  - Legacy service name `"Ransomware Rewind"` will migrate to `"CyberCrucibleAgent"`. Process name stays the same.
  - Registry key in `HKLM\SOFTWARE` will migrate from legacy `RansomwareRewind` to current `CyberCrucibleAgent.`

Fixes

- Fixed some 32bit processes triggering as having “modified memory” when the process image is at the maximum allowable size of a 32 bit process.

MD5 Hashes

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

Endpoint Agent

4.4.6.2

Features

- Added optional “access type” flags exposed to end users for behavioral access specificity.

Fixes

- None.

MD5 Hashes

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

Endpoint Agent

4.4.6.3

Features

- Added optional SOCKS5 proxy support to assist agent deployment.

Fixes

- Fixed reinstallations from older agents using the incorrect installation ID.
- Fixed existing installations from older installers having an unquoted service path.

MD5 Hashes

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

Endpoint Agent

4.4.6.4

Features

- Parent process memory information is available for process reports when modifications were detected.

Enhancements

- Changed some server communication frequencies to no longer require reboot for adjustment.

Fixes

None this release.

MD5 Hashes

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

Endpoint Agent

4.4.7.0

Features

- Beginning rollout of JWE-based HTTPS communications.
  - Encryption keys are unique to every agent.
  - All payloads encrypted under the HTTPS. Disabled by default during the initial rollout.
  - Ability to optionally revert from JWE-encrypted HTTPS to unencrypted HTTPS if JWE formatted payloads are not transmitting successfully.

MD5 Hashes

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

Endpoint Agent

4.4.7.1

Features

- More telemetry for process creations and incidents
  - User SID
  - User down-level logon name
  - Whether or not the process is elevated (Run As Administrator)
- Incidents now report where iterative data access occurred

Fixes

- Reduced memory usage during periods of server connectivity issues and heavy telemetry occurring at once
- Reduced memory usage during incident reporting

MD5 Hashes

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

Endpoint Agent

4.4.7.3

Features

- DMZ Mode
  - Optional configuration to use a signed CA bundle for TLS communication with authentication and telemetry servers. These CA bundles are then protected from tampering or deletion by Cyber Crucible’s proprietary anti-tampering capabilities.
  - OCSP and CRL checks are disabled to reduce the list of domains to allow through a firewall.

Fixes

- Reduced memory usage and CPU time spent on memory diff submission, especially after long offline periods.

MD5 Hashes

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

Endpoint Agent

4.4.8.0

Features

- Kernel-mode Authenticode telemetry
  - For increased speed and reliability, certificate data for process creations and incidents will be recorded by the driver alone.
  - This update does not remove dependencies on Windows cryptography libraries, but conducts cryptographic calculations in parallel. Eventually the dependency on Windows may be entirely removed.

Fixes

- Reduced memory usage and CPU time spent on attempted event submission when offline, during which telemetry is securely stored until the machine regains connectivity to Cyber Crucible servers.
- Some Nvidia driver installers believed they didn’t have privilege to install due to use of an internal Microsoft kernel function to attempt to access Cyber Crucible installed files.
- Fixed incompatibility with JWE mode and DMZ mode

MD5 Hashes

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

Endpoint Agent

4.4.8.1

Features

- Executable metadata such as product version, company name, etc. for in-memory processes are reported by the driver via kernel visibility. Normal functionality is to use user-space Windows API calls. This move to parsing in the kernel removing the (observed) opportunity for attackers to tamper with the process information.
- Agent authentication information is replicated elsewhere in the system to restore in the event the registry is corrupted by a malicious driver.

Enhancements

- Server connection errors are minimally logged by the agent, reducing log size on disk.

Fixes

- N/A

MD5 Hashes

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

Endpoint Agent

4.4.8.2

Features

- Added support for an optional system tray icon. This feature is disabled by default.

Fixes

- Added workaround for issue requesting kernel Windows API hashing requests. Workaround may be removed at some point in the future if Windows issue is corrected, possibly at next kernel update.

MD5 Hashes

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

Endpoint Agent

4.4.9.0

Features

- Kernel-mode DLL telemetry
  - Certificate parsing and trust calculation for all loaded DLLs in the driver.

Fixes

- None.

MD5 Hashes

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

Endpoint Agent

4.4.9.1

Features

- None.

Fixes

- Increased amount of telemetry handled at once by the service for creation and injection data.
- Adjusted ordering of canaries for programs using unusual file iteration methods.
- Adjusted ACL on some canaries to better fit in with real filesystems.

MD5 Hashes

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

Endpoint Agent

4.4.9.2

Features

- Memory modification tracking for loaded DLLs.
- Memory diff generation for modified DLLs.

Fixes

- Handle some non-conforming DLLs from yielding incorrect authenticode hash results.

MD5 Hashes

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

Endpoint Agent

4.4.9.4

Fixes

- Service dump files are now limited to 10 per version+thread combination.

MD5 Hashes

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

Endpoint Agent

4.5.0.0

Features

- AI Kernel Firewall
- Authenticode hash calculation speedups
- Significantly reduced memory usage for DLL telemetry
- Increased visibility for memory modifications in DLLs

Fixes

- Fix service recovery compatibility with 24H2

MD5 Hashes

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

Endpoint Agent

4.5.0.1

Features

- Option to migrate to hosted OAuth authentication server domain
- Task to dynamically configure REST and OAuth server URLs

Fixes

- None.

MD5 Hashes

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

Endpoint Agent

4.5.0.2

Features

- None.

Fixes

- Reduced memory used for AI Kernel Firewall.
- Quicker usage of new authentication endpoints.
- Removed icanhazip.com calls, previously optional but no longer necessary.

MD5 Hashes

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

Endpoint Agent

4.5.0.3

Features

- Status tray indicator now displays self configuration status for new installations.

MD5 Hashes

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

Endpoint Agent

4.5.1.0

Features

- OpenSSL is now used for TLS communication.
  - This should sidestep issues on older OS versions that are no longer being patched for newer TLS requirements.

Fixes

- Improved parsing support for non compliant Authenticode signatures.

MD5 Hashes

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

Endpoint Agent

4.5.1.2

Features

- Dropped legacy certificate validating that relied on builtin, slow Windows libraries.
- Added ability to keep logs on uninstall.

MD5 Hashes

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

Endpoint Agent

4.5.2.1

Features

- Broad release of reports for Fortress AI access

Fixes

- Optimization of Cyber Crucible kernel operations not using Windows APIs to counteract increased latency in some Windows environments by approximately 20%.

MD5 Hashes

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

Endpoint Agent

4.5.2.2

Fixes

- Optimization of Cyber Crucible kernel operations via avoidance of problematic windows event and data bus core OS capabilities.

MD5 Hashes

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

Endpoint Agent

4.5.3.0

Features

- FortressAI
  - Added notifications when a policy violation is reported
    - Integration with Windows Notification Center
  - Added a GUI to view policy notification history
  - Added simulate mode
- Cyber Crucible Core
  - Configurable asynchronous DLL analytics for machines with minimal hardware resources
  - Process creation analytics and telemetry
    - now uses disk persistence
    - removed Windows MiniFilter dependencies
  - Process injections analytics and telemetry
    - now uses disk persistence
    - removed Windows MiniFilter dependencies
  - Removed additional Windows kernel resource dependencies

Fixes

- Optimization of telemetry reporting for even faster reporting
- Removed deadlock due to exclusive vs shared kernel resource access for a specific kernel resource demanded by Microsoft Defender when Defender enables driver debug mode

MD5 Hashes

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

Endpoint Agent

4.5.3.1

Features

- FortressAI
  - Detects attempts to bypass policy controls through the use of screenshots.
- Cyber Crucible Core
  - Supports reinitializing an agent’s identity without requiring a full redeployment.
    - This fixes situations where a machine with Cyber Crucible installed is cloned, thus cloning the license and agent identifiers. Just like with IP addresses, MAC addresses, machine names, and other unique identifiers, Cyber Crucible identifies a cloned agent and alerts the CC administrators to the opportunity to generate new CC identifiers.

MD5 Hashes

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

Endpoint Agent

4.5.3.2

Features

- FortressAI
  - None
- Cyber Crucible Core
  - Kernel Buffer Operation Enhancement
    - The driver leverages buffers to temporarily store telemetry that is ultimately sent to the customer dashboard. This activity is distinct from behavioral model population or operations.
    - If a kernel buffer overloads, system CPU load increases.
      - This would only happen due to a large OS bug or an attack on the systems.
      - Automated customer notification of very high buffer usage available 1 JUN 2026.
    - Almost all of the kernel buffer operations for CC are with three primary buffers.
    - All three primary buffers' usage percentage is now transmitted to the CC infrastructure for metrics gathering and identification of buffer usage on a per-agent basis.
    - All three primary buffers are able to be adjusted in size remotely, and their status tracked by users.

Fixes

- A recent update involving DotNet and MSVC Redistributable libraries overwhelmed Cyber Crucible buffers with sustained very high (500%+) process and DLL operations events, affecting some customers. Though buffer usage is back down to the normal 1-5% usage, including the impacted customers, all buffers were doubled in size to account for any future issues. This is in addition to the configuration capabilities listed above.

Sha-256 Hashes

```
service.exe  = 2f46657af8809339d16546f1e6f2b58975bbf4d5c10fde3510363d628b129492
fai-alert.exe  = 890ccca7e0ce14a0e2ff7f90bae75a7ef12ad6c8cd43ffb52093c8431e65770b
```

```
CCRRSecMon.sys    = d0e941bc25d31e38cbebbe9ce3918f82d0b9c7b433efed318cb34e36a50acf94
CCRRSecMon.inf    = db54d8077afdfef81286868f7bda1e8df17dbd812178ddac989127550a904a8c
ccrrsecmon.cat    = a01c31db7231fed3852c9e559eb2c3f7496a016982207c102b88d8b36dcb0486
```

Middleware (REST Servers)

Middleware 01.23

Features

- Implemented controller for training licenses and added a training license expiration service.
- Updated each endpoint to account for the web application’s new training mode feature along with tests to each endpoint for training mode.
- Added an endpoint for resetting all of a parent group’s training data to its original state.
- Implemented endpoints for the new password aging policy setting for groups.
- Adding documentation for the Reactive Springboot endpoints.

Middleware 04.23

Features

- Partner Portal Updates:
  - Implemented endpoints for the new Register Deal process with Cyber Crucible approval of deals
  - Updated the PartnerDeal model to have a type associated with deals, each having a percentage discount associated with them
    - Also updated the PartnerDeal model for both Referral type deals to store the Dashboard User Account to associate with the licenses for the deal
  - Updated the PartnerDeal model to be able to separate Monthly vs Annual billing for payment of deals
    - Includes updating existing endpoints to account for Monthly vs Annual billing for Stripe
  - Implemented endpoints to be able to send quotes through Stripe for a deal
  - Implemented endpoint to resend the Stripe invoice for a deal
  - Implemented endpoint to edit multiple fields for a deal at the same time, associated with the edit deal modal in the Web Application
- Agent/License Management:
  - Implemented endpoint to bulk assign licenses to agents
  - Implemented endpoint to change the automatic re-licensing setting for a given agent
  - Implemented endpoint to release a license from an agent by passing the agentId in the request
- Implemented endpoints to retrieve and save the user setting to show the installer script config icon on the Groups grid
- Implemented endpoint to retrieve the Agent Installer Script Client Auth value for a group
- Updated our AV Scanner Service to search in the identity incident collection in addition to the process creation collection
- Various updates to our list of default data + identity whitelists for AVs.
- Implemented new change stream endpoint to listen for new Extortion Response insertions
- Implemented endpoint to copy whitelists to another group
- Implemented endpoint to download the Memory Diff File for an incident
- Implemented categorizing identity incident programs into applications
- Implemented saving column modes for each web page grid and saving chart visibility settings

Middleware 08.23

Features

- Partner Portal Updates:
  - Implemented endpoints to be able to create a POC for approved partner deals
  - Implemented endpoints for the Distributor Group Management page in the Web Application
  - Implemented endpoint to return the data for the Payment Management grid in the Web Application
  - Implemented the ability to change a partner deal’s owner
  - Implemented the ability to set a custom memo for partner deals that appear on the Stripe invoices and quotes
- Implemented endpoint to be able to resend user account invitations
- Added more application labeling options for Identity Access objects
- Updating the Group model for partner groups to have new boolean fields for the type of partner
- Updating the Group model to have a list of canary extension configs
- Various updates to our list of default data + identity + cert whitelists for AVs
- Enabling HTTP/2 support
- Upgrading our Spring Boot to the latest version along with various other dependencies
- Implemented notification alerts for Abnormal Identity Accesses
- Enabled server response compression for agents
- Implementing filtering for the Identity Access grid’s No Trusted Cert column in the Web Application for the “Disconnected Retrieving Cert Info” and “Timed Out Retrieving Cert Info” options
- Fixed issue in our partner deal expiration notification service to not send expired emails for completed deals

Middleware 11.23

Features

- Whitelist Updates
  - Implemented the ability to create an exception with the parent program path and arguments
  - Implemented the ability to create an exception to match extortion responses when there are only trusted certs, match only when there are no related injections, and match only when there is no modified memory
  - Implemented the ability to create an exception to match specific file access triggers
- Implemented group setting for automatically freeing licenses for inactive agents
  - Updated Group model to have setting for when to free licenses from inactive agents in the group. Options are 30/60/90 days, or have this setting turned off
  - Updated Agent model to have new inactive status
  - Implemented service to automatically free inactive agents' licenses according to their group setting
- Updated the endpoint for the retrieving extortion responses to include the parent program path and arguments
  - The parent program path and arguments are now also included in the unique extortion response counts for the Web Application, Security Notification alerts, and Executive Summaries
- Updated our Executive Summary Reports to separate out the Licenses slide to individual Desktop and Server Licenses slides
- Updated Security Email Notification model and the Security Notification service to include two new alert types
  - Behavioral Model Tuned
  - New Agent Version
    - When a group’s managed update settings are changed to have auto update turned off, a New Agent Version notification is automatically created for the group
- User Role/Permission Updates
  - Updated the Role model Incident Manager permissions to now only have view/edit for whitelists and silent response rules
  - Groups now have 3 default roles that are not user editable:
    - Admin
    - Read Only
    - Guest
  - Users added to a group by default are assigned the Guest Role

- Implemented endpoints for the Web Application Browser Utility Process Tuning Modal to easily manage how agents in groups should respond to chrome utility processes
- Updated the endpoint for the Agents page chart to be able to limit counts to agents that have called in over the past 30/60/90 days
- Updated the Security Notification Ransomware Activity email alert to include a link that will automatically redirect users to the Extortion Responses page with the a filter to show the responses the alert was for
- Implemented group setting for agents in a group to run in safe mode or not
- Implemented a powershell script option for installing agents
- Upgrading our Spring Boot to the latest version
- Various updates to our list of default data + identity + cert whitelists for AVs

Middleware 04.24

Features

- Implemented the group setting and related endpoints for the setup and management of proxy configurations to assist in agent deployment
- Updated our telemetry data endpoints to be able to view all telemetry data or only data directly related to an extortion response
- Implemented the group setting for automatically hiding agents in groups when a license is released from an agent, an agent is marked as inactive, or an agent completes an uninstall
- Updated the links to our dashboard in our notification emails to contain a URL Parameter used to automatically filter data on the related frontend grid to show what triggered the notification
- Updated the endpoint used for the frontend Agent Licenses chart to include counts for both Desktop and Server licenses
- Implemented endpoints for the new Customer Deployment Health frontend page
- Updated our process tuning to account for Microsoft Edge WebView

Middleware 09.24

Features

- Implemented the endpoints for the new Group DMZ Mode setting
- Updated the Deal Registration endpoints to be able to register multi-year deals with the ability to pay up front or pay yearly for multi-year deals
- Added the ability to view the root cause analysis for Identity Accesses
- Implemented Temporary Tailored Behaviors
- Updated the User model to save the setting for hiding or showing expired Agent Licenses by default on the Agent Licenses grid
- Updated the Security Notification model and related endpoints/services for the new offline agent alert options of Partially and Fully Offline agents
- Updates to the endpoints related to adding the new columns on the frontend on the Agents grid to show when the assigned license expires, and when the license was assigned to the agent
- Added setting to the Group Model for agents in the group to show the agent icon in the related agent machine’s system tray
- Updated the server side grid queries to be able to take in multi condition filters for the same key/column

Middleware 05.25

Features

- Updated the Sales Notification model with new types:
  - Distributor Partners can receive alerts when their reseller subgroups create a new Deal Registration
  - Partner Deal POC activity
- Updated the authentication process to allow for SSO integration with Microsoft Entra ID (Azure Active Directory)
- Updated the agent installer endpoint to allow for a new installer type for Native Cli
- Updated the endpoints for the Distributor Partner new updates
  - Added a new Partner in Motion model
  - Updated the Partner Deal Registration model to add the ability for distributors to approve their reseller subgroup’s deals
  - Added ability for Distributor Partners to edit the multi year discounts for their reseller subgroups
  - Added ability for distributors to send themselves quotes with their distributor pricing for a reseller subgroup’s deal
  - Added requirement for when a reseller subgroup registers a deal to require the Subgroup Reseller Agreement to be uploaded by their parent distributor on the Distributor Group Management page
- Updated the Role model with a new Partner Deal Manager for deal registration operations and updated each related endpoint to check for permission
- Added the endpoint for editing a group setting’s in bulk
- Upgraded our Spring Boot to the latest version
- Improved the queries used for generating executive reports to reduce the time it takes to generate the report
- Moved our telemetry collections in the database to use sharding
- Updated the agents query used for the dashboard grid to include if the agent is a server or not
- Updated the /updateGroupAutomaticallyHideAgentsReactive endpoint to retroactively apply the update to existing agents
- Major authentication updates to allow agents to call into our REST Servers with the new hosted OAuth authentication
- Added new endpoints for DLL telemetry submission by agents

Middleware 12.25

Features

- Added new endpoints for DLL Visualization on the dashboard for viewing related untrusted module loads for Extortion Responses, Process Creations, Process Injections, and Identity Accesses
- Updated the Extortion Response and Identity Access endpoints for the dashboard queries to return additional fields for DLL Visualization including modified module memory, modified module path, etc
- Updated the Agent model to have new fields for if the agent is fully configured and the date the agent was first fully configured
- Added new endpoints and controller for the AI Firewall Management page
- Updated the endpoint that returns the list of agents for the dashboard to include new fields for which rest server and OAuth server the agent is calling to, and the WAN IPv4 and IPv6 of the agent
- Added new endpoint for the Extortion Responses page that allows users to view all fields for an Extortion Response in this endpoint rather than using the existing endpoint that offers a condensed view of the fields and requires an additional api call to get more details.
  - Users on the dashboard can use the toggle on the Extortion Responses page to use the previous grid option and the new grid option that returns all fields in one grid
- Added a new option to Security Notifications to include a CSV file in the email alert for Ransomware and Identity Access Alerts containing information on why the alert was triggered.

Web Application

Web Application 01.23

Features

- Implemented a cross-link on the extortion responses child grid to view the related process creations and injections.
- Implemented user password aging policy for groups.
- Added training mode and the ability to reset a parent group’s training data to its original state on the settings page.
- Added the Training License page.
- Implemented Amazon Cognito Security.
- Added the Automation button above grids that reveal operations to perform after clicking the button.

Web Application 04.23

Features

- Partner Portal Updates:
  - Ability to schedule a demo on the Register Deal page
  - Implemented new Register Deal process with Cyber Crucible Approval of Deals
  - Added a Deal Prospect Type when registering deals
  - Added Monthly and Annual Billing Cycle for deals
  - Implemented sending quotes for Cyber Crucible approved deals through Stripe and signing quotes before completing a deal
  - Ability to re-send the Stripe invoice for a completed deal
  - Ability to edit a deal through a modal, similar to the register new deal modal, pre-filled with the deal’s current information
- Agent/License Management:
  - Ability to release licenses from the Agents page in bulk
  - Ability to assign licenses to agents in bulk on the Agents page
  - Ability on the Agents page to view and change the automatic re-licensing settings for agents when they call into our rest server without a license
    - Users can update agents individually and in bulk
- Implemented the ability on the Groups page to view a group’s Id and Client Auth values used in the Agent Installer Script
- Implemented the ability to copy whitelists to another group
- Upgraded to React 18
- Added the reset columns and auto-size all columns options to the context menu on grids when right clicking
- Added the download Memory Diff File option to the Extortion Responses grid for applicable responses
- Implemented state saving for chart visibility
- Added new Application columns to the Identity Access grid for the accessed, accessing, and parent programs.
- Implemented column mode toggling on each grid for the amount of columns to show. Modes include: Min, Medium, Max, and Custom
- Implemented searching/autocomplete ability in Dropdown Select elements with Material UI

Web Application 08.23

Features

- Partner Portal Updates:
  - Added the Demo Videos page to the Partner Portal
  - Added the ability to create a POC for approved partner deals
  - Added the Distributor Group Management page to the Partner Portal for Distributor partners to create and manage their subgroups
  - Added the Payment Management page to the Partner Portal
  - Added the ability to change a partner deal’s owner
  - Added a custom memo field for partner deals to show on the Stripe invoices and quotes
- Implemented a Remember Me functionality that allows users to stayed logged in
- Added a link to view the Stripe Customer Portal where users can manage their subscriptions and payment methods
- Added the ability on the Agent Licenses page to change the group of multiple selected licenses on the grid
- Upgraded AG Grid to version 29
- Updating dependencies to their latest versions
- Removed the Automation button above grids that revealed icons and instead placed the icons directly above the grid
- Removed the Columns button above grids that revealed the Grid Column State Options and instead placed the Grid Column State Options directly above the grid
- Added the ability to resend user account invitations on the Groups page
- Added the Canary Extension Mode column to the Groups page
- Added more application labeling to the Identity Access page
- Added icons and filtering on Identity Access grid to the No Trusted Cert column for “Disconnected Retrieving Cert Info” and “Timed Out Retrieving Cert Info”
- Fixed issue on mobile devices with rendering grids

Web Application 11.23

Features

- Added the ability to automatically free licenses for inactive agents.
  - This feature is a group setting and options are to automatically free licenses for inactive agents in the group after 30/60/90 days, as well as turning this setting off
- Whitelist Updates
  - Added the ability to create an exception with the parent program path and arguments
  - Added the ability to create an exception to match extortion responses when there are only trusted certs, match only when there are no related injections, and match only when there is no modified memory
  - Added the ability to create an exception to match specific file access triggers
- Added the parent program path and arguments to the extortion responses grid
- Added file hashes to the Extortion Response Details Modal
- Added new Security Notification alert types:
  - Behavioral Model Tuned
  - New Agent Version
- Updated the Ransomware Activity alert emails to include a link that will automatically redirect users to the Extortion Responses page with the a filter to show the responses the alert was for
- Added option to the Agents page chart to only include counts on the chart for agents that have called in over the past 30/60/90 days, and also the option to not limit the counts
- Added examples on the Rest Integration page of calling to the aws /token endpoint. Examples include calling the endpoint with bash, powershell, and command prompt
- Updated the permissions for the Incident Manager on the Roles page to only have view/edit for whitelists and silent response rules
- The deprecated Response Automation Manager was removed from the Roles page
- Added the Browser Utility Process Tuning Modal to the Whitelists, Silent Response Rules, and Extortion Responses pages
  - Includes the option to select how agents in groups should respond to chrome utility processes
- Added option to download the agent using a powershell script
- Added the group setting for agents in the group to run in safe mode
- Added the OS Name column to the agents grid
- Fixed issue on certain grids where column widths and order would reset on icon/button clicks on the page

Web Application 04.24

Features

- Added the ability to setup and manage proxy configurations to assist in agent deployment. View more about proxy configurations here
- Fixed the issue where the horizontal scrollbar at the bottom of our data grids was not visible due to the grid extending beyond the visible screen height
- Added the ability on our Telemetry pages to toggle between viewing all telemetry data or only viewing data that was directly related to an extortion response
- Added the group setting for automatically hiding agents in the group when a license is released from an agent, an agent is marked as inactive, or an agent completes an uninstall
- Added the ability when clicking a link from one of our notification emails to automatically filter data on the related grid to show what triggered the notification
- Updated the Agent Licenses chart to show the counts for both Desktop and Server Licenses
- Upgraded AG Grid to version 31
- Upgraded Ag Charts to version 9
- Added more text filter options to our data grids
- Added the Customer Deployment Health page (found under the operations tab)

Web Application 09.24

Features

- Added to the Agent licenses page the ability to filter expired licenses from the grid and chart by default. This setting can be updated on the toggle above the agent licenses grid
- Implemented multi condition filters for a single column on the server side grids. The server side grids are the grids where all the rows are not loaded into the grid on the initial load due to the large amount of rows on these grids: Extortion Response, Process Creations, Process Injections, and Identity Accesses
- Added the multi-year option for Deal Registrations. Deals can be up to 3 years in length, and users have the option to pay up front or pay yearly for multi-year deals
- Implemented Temporary Tailored Behaviors. View more here
- Added new column on the Identity Access grid for Root Cause Analysis
- Updating Security Notifications with two different options for offline agent alerts: Partially and Fully Offline agent alerts
- Added new columns to the agents grid for the license expiration date and date license assigned to agent
- Added the new Group setting for DMZ Mode for agents in the group to follow. DMZ Mode is for environments where online certificate checking is unavailable. Enabling DMZ Mode will embed CA roots locally on agents in the group and disable OSCP
- Added the new Group setting for agents in the group to have an agent icon shown on the related agent machine in the system tray, only agents on version 4.4.8.2 and higher have this capability
- Added a sidebar to our data grids to easily change column visibility and order

Web Application 05.25

Features

- Added SSO integration for our dashboard login with Microsoft Entra ID (Azure Active Directory)
  - Users must contact Cyber Crucible and complete a few steps found here to integrate Entra ID SSO for their organization with our dashboard login
- Distributor Partner Updates
  - Improvements to the process of distributors associating reseller subgroups and those reseller subgroups registering and completing deals. A more detailed explanation of the improved Distributor Group Management process can be found here
  - Added a new Sales Notification type for Distributor Partners to receive alerts when their reseller subgroups create a new Deal Registration
  - Added ability for Distributor Partners to edit the multi year discounts for their reseller subgroups. This can be found on the Distributor Group Management Page
  - Added the Distributor Approval column to the Deal Registration for Distributors to manage their reseller subgroup deals
  - Added the Partner in Motion page found under the Partners tab for distributors partners to register reseller subgroup partners that are in the works
- Added the Partner Deal Manager to roles for deal registration related operations
- Added new sales notification type for Partner Deal POC activity. This alert applies to the new POC group that is created when a partner creates a POC for a deal. Alerts for this type are sent for agent installs/uninstalls and when the POC licenses expire in the POC group
- Added the new Agent installer type “Native CLI”
- Added the Edit Group Modal on the Group Management page that allows you to edit the group settings in bulk
- Upgraded AG Grid to version 32
- Adding password visibility toggle/button for login

Web Application 12.25

Features

- Added the new AI Firewall Management page found in the Operations tab
- DLL Visualization
  - Added ability to view related module loads for Extortion Responses, Process Creations, Process Injections, and Identity Accesses
  - A new column was added to these pages that shows if related untrusted module loads were found. When an untrusted module load is found, the cell in this column will show an icon where clicking it will take users to a new page to view all the related untrusted module loads
- Added new columns to Extortion Responses and Identity Access grids:
  - 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
- Added to the Extortion Responses grid the “Data Access Attempted” column, which shows the path on the machine where the data access was attempted at
- Updated the Extortion Responses page to now have 2 different grid options. The previous grid option for a more condensed view of the extortion responses with the parent and child grid still exists, a new option for removing the parent/child grid and showing all the data and columns on a single grid now exists
- Added columns to the Agents grid showing if the agent is fully configured and the date the agent was first fully configured
- Added additional columns to the Agents grid for which OAuth Server and REST Server the agent is calling too, and the WAN IPv4 and IPv6 of the agent
- Added Co-branded Collateral to the Partners tab that allows partners to download a .zip file containing all the co-branded collateral material
- Upgraded AG Grid to version 34
- Added the number of days until a license expires to the Agent Licenses page and Agents page. This can be found as an icon in the Renews column on the Agent Licenses page, and the License Expiration Date column on the Agents page
- Added a new option to Security Notifications to include a CSV file in the email alert for Ransomware and Identity Access Alerts containing information on why the alert was triggered. This option was added so users can view why an alert happened right in the

email without having to login to the dashboard