Dashboard & Reporting

Verwendung der Cyber Crucible Webanwendung – Agenten-Sichtbarkeit, Prozessaktivität, Speicheranalysen und Berichte für die Geschäftsführung.

- Kann Cyber Crucible auf einen Angriff still reagieren, ohne mich zu benachrichtigen/alarmieren?
- Wie kann ich die Ursache eines Ereignisses untersuchen?
- Was zeigt die Seite „Prozessinjektionen“?
- Was zeigt die Seite "Prozesserstellungen" an?
- Was sind Executive Report Summaries?
- Wie zeige ich versteckte Agenten an?
- Wie kann ich einen Agenten ausblenden oder entfernen?
- Erhalte ich weiterhin Warnungen und Benachrichtigungen, wenn ich einen Agenten ausblende?

Kann Cyber Crucible auf einen Angriff still reagieren, ohne mich zu benachrichtigen/alarmieren?

Es kann legitime Szenarien geben, in denen Sie nicht möchten, dass eine Anwendung etwas tut (wahrscheinlich auf Ihren Rechnern), Sie aber nicht bei jedem Vorfall benachrichtigt werden müssen.

Dies ist eine andere Situation als die, in der Sie etwas auf die Whitelist setzen müssen, sodass durch die Datenerpressungs-Prävention von Cyber Crucible keine Maßnahme ergriffen wird.

Die Funktion, nach der Sie suchen, sind stille automatisierte Reaktionen (silent automated responses).

Eine bestehende automatisierte Reaktion künftig still schalten:

Gehen Sie zunächst zur Seite „Vorfälle verwalten“ (Manage Incidents). Wir werden den Namen in naher Zukunft in „Reaktionen verwalten“ (Manage Responses) ändern.

Klicken Sie anschließend auf die Lautsprecher-/Lautstärke-Schaltfläche, wie unten zu sehen.

4784131.png?width=680
Durch Klicken auf diese Schaltfläche öffnet sich das Modal „Vorfall stummschalten“ bzw. „Automatische Reaktion stummschalten“ (Silence Incident / Silence Auto-Response).

Wir verfügen über Analysefunktionen, die anhand zuvor ausgewählter Programme und Argumente prüfen, ob eine Reaktion still erfolgen sollte.

In diesem Fall sehen wir, dass Adobe als Teil seiner Softwaresuite einen Webserver ausführt, und wir möchten künftig keine Warnungen mehr erhalten, dass der Webserver angehalten wurde.

(In diesem Fall haben wir bösartigen JavaScript-Code in die von Adobe ausgeführte Datei eingeschleust, und Cyber Crucible hat den Webserver von Adobe daran gehindert, Daten zu stehlen oder zu verschlüsseln.)

4784138.png

Klicken Sie auf „Zur Seite für stille Reaktionen“ (Take me to Silent Responses Page)

Es wird ein Menü zum Einfügen dieser spezifischen Stummschaltungsregel angezeigt, aber schauen wir uns zunächst die Seite an:

5013506.png?width=680
Wir sehen hier, dass die Regeln sowohl auf dem Prozess als auch auf den Prozessargumenten für eine automatisierte Reaktion basieren, die nicht in Benachrichtigungs-E-Mails oder anderen Warnungen enthalten sein soll.

Das Anhalten erfolgt weiterhin – nur ohne Benachrichtigung darüber.

Wir sehen hier, dass wir nicht möchten, dass der Microsoft-Edge-Browser oder der Chrome-Browser mit diesen Argumenten ausgeführt werden können, mit Platzhaltern davor und danach, um andere vorhandene Argumente zu berücksichtigen.

(Sicherheitshinweis zur Erklärung: Beide Browser führen ein identisches Codestück aus, das die Browser im Hintergrund ohne sichtbares Fenster lädt, um im Verborgenen Ihre Dateien zu scannen und zu lesen. Wir möchten nicht, dass unsere Webbrowser das hinter unserem Rücken tun!)

Unabhängig davon, ob Sie eine vollständig präventive stille Reaktionsregel erstellen oder nicht, ist das gleiche Fenster unten (im nächsten Abschnitt) der nächste Schritt.

Erstellen einer stillen Reaktion

Hier sehen wir sowohl den Programmpfad als auch die Programmargumente. Platzhalter sind erlaubt, um sicherzustellen, dass beispielsweise ein Benutzername oder eine Anwendungsversionsnummer Ihre Verhaltensregel nicht daran hindert, zu funktionieren.

Ein Beispiel dafür, warum Platzhalter benötigt werden: Es könnte ein Programm auf allen Desktops Ihrer Mitarbeiter geben, die einer Gruppe angehören.

C:\Users\mary\Desktop\runme.exe
C:\Users\joe\Desktop\runme.exe

Die Lösung wäre:

C:\Users*\Desktop\runme.exe

5046277.png

Hier sehen wir, dass wir eine stille Reaktion für die gesamte Gruppe TEMPORARY GIRAFFE 2 erstellen, für einen von Adobe Creative Cloud angelegten Pfad, und wir möchten nur Reaktionen stummschalten, die ein bestimmtes Argument aufweisen (in diesem Fall einen Dateipfad zu einer bestimmten JavaScript-Datei).

Es gibt keine eindeutigen Bestandteile im Pfad, wie z. B. Benutzernamen, sodass wir die Regel so erstellen können, wie sie ist.

Reaktionen können benannt werden, wobei die Namen pro Gruppe eindeutig sind.

Die Regeln beginnen innerhalb weniger Minuten, an die Agenten verteilt zu werden.

Wie kann ich die Ursache eines Ereignisses untersuchen?

- Speicheranalyse
- Analyse von Prozess-Injektionen
- Analyse von Prozesserstellungen
- Alles zusammengeführt – eine durchgängige Untersuchung
  - Warum haben wir uns entschieden, dieses Beispiel zu zeigen?

Es gibt drei Analysebausteine, die Ihnen bei der Untersuchung eines Alarms zur Verfügung stehen.

Derzeit ist es wahrscheinlicher, dass ein Angreifer eine Vielzahl von Aktivitäten auf einem System durchführt, indem er eine Kombination aus speicherbasierten Techniken und Prozess-Hijacking (Injection oder Hollowing) nutzt, anstatt ein offensichtliches „hacker.exe“-Programm auszuführen.

Speicheranalyse

Der erste Baustein findet sich direkt auf der Response- bzw. Incident-Seite. Die Speicheranalyse verfolgt das Verhalten des Prozesses im Speicher während der kontinuierlichen Überprüfung auf mögliches Datenerpressungsverhalten (Diebstahl oder Verschlüsselung).

Ein Speicherzustand, der auf eine wahrscheinliche Manipulation hinweist, ist typischerweise ein Hinweis auf ein Problem.

Dies ist nicht immer bösartig an sich, da auch schlechte Programmierpraktiken oder Softwarefehler dazu führen können, dass der Speicherzustand eines laufenden Programms verändert wird.

63504385.png?width=680
Hier sehen wir einen Fall, in dem ein Adobe-Acrobat-Prozess nach dem Öffnen einer heruntergeladenen PDF-Datei mögliches Datenerpressungsverhalten zeigt, und wir sehen, dass der Speicher des Acrobat-Prozesses verändert wurde. Die Acrobat.exe-Datei auf der Festplatte wurde in keiner Weise beeinträchtigt.

Eine forensische Analyse des mit der angehaltenen Acrobat.exe verbundenen Speichers wird wahrscheinlich auf ein bedenkliches Problem hinweisen – möglicherweise auf einen genutzten Exploit, wenn nicht sogar auf Prozess-Injection oder Prozess-Hollowing.

Bei Erpressungs-Responses mit dem Wert „True“ für „Modified Memory“ gibt es in der Spalte „Root Cause Analysis“ ein Download-Symbol, um die Memory-Diff-Datei für die Response herunterzuladen:

63602693.png?width=680
Die Memory-Diff-Datei ist der kompilierte Quellcode dessen, was in das Programm injiziert wurde. Sie enthält wahrscheinlich Malware und/oder Exploit-Code, den ein Malware- oder Sicherheitsanalyst untersuchen kann. Beachten Sie, dass diese Datei nicht das gesamte Programm enthält, sondern nur den Teil, der durch einen Exploit oder eine Angriffstechnik wie Prozess-Injection verändert wurde. Erfahren Sie mehr über diese Datei hier.

Analyse von Prozess-Injektionen

Der erste Hinweis darauf, dass ein Prozess-Injection-Ereignis für eine automatisierte Response relevant sein könnte, ist die Spalte „Untrusted Remote Threads“ für einen Incident/Response. Dies zeigt an, dass die Verhaltensanalyse auf Kernel-Ebene einen nicht vertrauenswürdigen Remote-Thread festgestellt hat, der bei einem Prozess mit Datendiebstahl- oder Ransomware-ähnlichem Verhalten beobachtet wurde.

63471635.png?width=680
Eine weitergehende Untersuchung kann auf der Seite „Process Injection“ durchgeführt werden. Der Wert „True“ bei „Untrusted Remote Threads“ ist ein guter Hinweis darauf, ob man dorthin gehen sollte.

Die Spalte „Root Cause Analysis“ verfügt außerdem über ein Symbol, mit dem Sie automatisch zur Seite „Injections“ weitergeleitet werden, um nur die zu der Response gehörenden Prozess-Injektionen anzuzeigen.

63602703.png?width=680
Nach dem Klicken auf das Injections-Symbol werden Sie zur Seite „Process Injections“ weitergeleitet, auf der Sie nur die zu der Response gehörenden Prozess-Injektionen sehen:

63569930.png?width=680
Hier auf der Seite „Process Injection Events“ sehen wir den Pfad und die Argumente des Injektor-Prozesses sowie den Pfad und die Argumente des injizierten Prozesses (Injectee). Die Argumente spielen in der Regel eine sehr wichtige Rolle bei der Speicheranalyse oder zeigen beispielsweise an, welche PowerShell-Befehle ausgeführt werden sollen. Auch die Prozess-IDs sind vorhanden, um iterative Injektionen zu verfolgen, während ein Angreifer von Prozess zu Prozess wechselt, oder um die Ursachenanalyse auf der Seite „Process Creation“ nachzuschlagen.

63438879.png?width=680
Wie wussten wir, dass rundll32.exe in Wirklichkeit ein Antivirenanbieter war? Lesen Sie weiter!

Analyse von Prozesserstellungen

Es ist sehr selten, dass ein Angreifer bei seinem Angriff nur einen einzigen Prozess verwendet. Möglicherweise weiß er nicht einmal, dass die von ihm verwendeten Tools neue Prozesse erzeugen und verschiedene Verwaltungstools auf dem infizierten System nutzen.

Die Seite „Process Creation“ verfolgt alle Prozesse, die andere Prozesse (oder sich selbst) öffnen, die dabei verwendeten Argumente sowie die Prozess-IDs (Pids) für jede Quelle und jedes Ziel.

Dies erfolgt auf Kernel-Ebene, sodass nichts übersehen wird.

Hinweis: Die Microsoft-Telemetrie enthält einige dieser Daten, jedoch nicht alle. Wir verzichten bewusst auf diese Datenquelle, da wir festgestellt haben, dass diese Telemetriequelle wichtige Ereignisse übersehen oder von Angreifern während eines Angriffs deaktiviert werden kann.

Wie gut ist unsere Sichtbarkeit?

Alles zusammengeführt – eine durchgängige Untersuchung

Wie gut ist unsere Sichtbarkeit, und wie schnell können Sie eine Ursachenanalyse (Root Cause Analysis) durchführen? Sehen Sie sich dieses Beispiel an – ein Antivirenprogramm mit möglicherweise einigen der höchsten Berechtigungen auf einem System wurde dabei beobachtet, wie es versuchte, Code in unsere Cyber Crucible-Software zu injizieren. Wir hoffen, dass dies zur Untersuchung unserer Software geschah, aber wir wechseln trotzdem in den Selbstschutzmodus (das führte also dazu, dass unsere Software die Manipulation durch das Antivirenprogramm zurückwies … es gibt keine Hintertüren, die es externen Parteien ermöglichen, unsere Software zu bearbeiten oder zu nutzen).

Beginnen wir also hier mit einer automatisierten Response:

63569937.png?width=680
Offensichtlich ist Cyber Crucible keine Ransomware. Wir sehen hier, dass ein Prozess-Injection-Versuch mit verdächtigem Remote-Thread-Verhalten in Verbindung mit datenerpressungsähnlichem Verhalten auftrat.

OK – schauen wir uns an, was in den Process Injection Events passiert, indem wir auf das Injections-Symbol klicken. 5 Sekunden später haben wir unsere Antwort!

63471644.png?width=56463438879.png?width=680

Aber Moment – rundll? Das ist doch kein Hacker, oder? Das ist sicherlich kein hacker.exe-Programm. Lassen Sie uns etwas filtern, um unsere Antwort auf der Seite „Process Creation“ zu erhalten. Wir haben hier keinen Screenshot, aber Prozess-IDs sind für alle Responses und Prozess-Injektionen verfügbar. Gehen wir zurück zur Seite „Responses“ und klicken auf das Process-Creations-Symbol, um zur Seite „Process Creations“ zu gelangen und das Raster automatisch so zu filtern, dass die zu dieser Response gehörenden Prozesserstellungen angezeigt werden.

63537184.png63438886.png?width=680

Schnell und einfach sehen wir nun, dass die „Wurzel“ (kein Wortspiel beabsichtigt) WebRoot war, ein Antivirenanbieter, der einen rundll32.exe-Prozess erzeugte, um eine der DLLs von WebRoot zu laden, die dann versuchte, *irgendetwas* mit der Software von Cyber Crucible zu tun, um sie zu zwingen, Dateien wie ein Datendiebstahl-Tool zu durchlaufen.

Warum haben wir uns entschieden, dieses Beispiel zu zeigen?

Wir verfügen über zahlreiche Beispiele für Angreifer-Taktiken mit unterschiedlichem Kompetenzniveau der Angreifer. Antivirenprogramme erreichen ein Berechtigungsniveau auf einem System, das ein sehr hohes Maß an Fähigkeiten, Technologie und Vorbereitung von Seiten der Angreifer erfordert. Dass Cyber Crucible „hackerähnliches“ Verhalten von einem etablierten Sicherheitstool erkennt und es dann automatisch stoppt, zeigt einige der höchsten Ebenen technischer und sicherheitstechnischer Exzellenz unsererseits, ohne sich in einzelnen Exploits oder Angreifer-Taktiken zu verlieren.

Was zeigt die Seite „Prozessinjektionen“?

Prozessinjektionen sind eine softwaretechnische Fähigkeit, die in nicht-bösartigem Kontext auftreten kann oder direkt von einem Angreifer genutzt wird. Tatsächlich gehören Prozessinjektionen und die damit verbundenen Techniken zu den bevorzugten Methoden von Angreifern, aus einer Vielzahl von Gründen, die den Rahmen dieses Artikels sprengen würden (aber wenn Sie interessiert sind, können wir Sie auf entsprechende Schulungen verweisen).

Cyber Crucible macht Prozessinjektions-Ereignisse auf Kernel-Ebene sichtbar. Das bedeutet, Sie erhalten vollständige Transparenz über alle Prozesse und deren Informationen, unabhängig von den Berechtigungen dieses Prozesses. Wir haben festgestellt, dass viele der klassischen Telemetriequellen für Sicherheitstools verstummen, sobald Angreifer oder Software ein bestimmtes Berechtigungsniveau erreichen. Niemals wichtige Daten zu verpassen und niemals „stumm“ zu werden, ist ein wesentlicher Bestandteil unseres Zero-Trust-Produktdesigns.

Auf der Seite „Prozessinjektionen“ sehen Sie pro Ereignis die folgenden Angaben, wobei Filter zur Verfeinerung Ihrer Abfragen zur Verfügung stehen:

CC_Showing_All_Process_Injection_Columns.mp4
Im Rahmen einer Untersuchung werden Sie normalerweise feststellen, dass es zusätzliche Aktivitäten auf der Seite „Prozesserstellung“ gibt.

Was zeigt die Seite "Prozesserstellungen" an?

Es kommt sehr selten vor, möglicherweise sogar nie, dass ein Angreifer einen gesamten Angriff innerhalb eines einzigen Prozesses durchführt.

Die Tatsache, dass ein Angriffswerkzeug oder eine Windows-Bibliothek mehrere Prozesse und Windows-Programme nutzt, ist für die Nutzer der Malware (also die Kriminellen) manchmal unsichtbar.

Prozessverhalten stellt eine wichtige Quelle von Variablen bei der Entscheidungsfindung von Cyber Crucible dar, die verhaltensbasierte Indikatoren aus einer Vielzahl von Quellen einbezieht.

Manchmal führen diese Prozessverhalten letztlich zu einer Prozessunterbrechung aufgrund von Datendiebstahl oder Ransomware-Verschlüsselung und können vom Einstiegspunkt des Angreifers durch das System bis hin zur endgültigen Ausführung der Erpressersoftware zurückverfolgt werden.

In anderen Fällen kann die Prozessverfolgung unbefugten Fernzugriff, Betrug, Insider-Bedrohungen oder unerwartete Software identifizieren, jedoch keine Datenerpressung. Es handelt sich also nicht um etwas, das die Software von Cyber Crucible zur Verhinderung von Datenerpressung automatisch unterbindet, aber dennoch um etwas, worüber Sie informiert sein sollten.

Unabhängig davon, ob die Prozessdaten Teil eines Datenerpressungsangriffs sind, auf etwas anderes Bemerkenswertes hinweisen oder lediglich normales Programmverhalten darstellen, werden die Quell- und Zielinformationen der Programme, einschließlich der Programmargumente, zur Verfügung gestellt. Dies liefert einen umfangreichen Datensatz zur Verfolgung von Angreifern, einschließlich solcher, die Taktiken des „living off the land“ nutzen.

Nachfolgend finden Sie einen Screenshot der Art von Daten, die aus Prozesserstellungen erfasst werden können.

CC_process_creation_demo.mp4

Was sind Executive Report Summaries?

- Einführung
- Wie man den Empfang von Berichten aktiviert und deaktiviert
- Beispielhafter Berichtsinhalt

Einführung

Executive Report Summaries sind Berichte, die per E-Mail an Benutzer gesendet werden und Informationen über die Lizenzen, Agenten und Maschinenverhalten der Benutzer enthalten. Die Berichte enthalten eine Zusammenfassung über alle Gruppen, denen der Benutzer angehört, gefolgt von einer Zusammenfassung für jede einzelne Gruppe.

Benutzer haben die Möglichkeit, wöchentliche und monatliche Berichte zu erhalten sowie das Format des per E-Mail gesendeten Berichts auszuwählen (HTML, ZIP usw.).

Wie man den Empfang von Berichten aktiviert und deaktiviert

Nach der Anmeldung auf unserer Website und dem Navigieren zur Seite Account Settings sehen Benutzer die Optionen, um ihre Präferenzen für den Empfang wöchentlicher und monatlicher Berichte festzulegen, sowie das Format des per E-Mail gesendeten Berichts einzustellen.

24051723.png?width=442

Beispielhafter Berichtsinhalt

23887914.png?width=44224084489.png?width=44223855156.png?width=442

Wie zeige ich versteckte Agenten an?

Navigieren Sie zur Seite „Agents“ und suchen Sie die Spalte „Dashboard Visibility“.

86048770.png?width=680
Der Standardfilter für diese Spalte sorgt dafür, dass versteckte Agenten nicht angezeigt werden.

Um versteckte Agenten anzuzeigen, öffnen Sie den Filter für diese Spalte, aktivieren Sie das Kontrollkästchen für „Hidden“ und deaktivieren Sie das Kontrollkästchen für „Visible“. Klicken Sie anschließend auf „Apply“.

Dadurch werden nur die versteckten Agenten angezeigt. Von dort aus können Sie die üblichen Verwaltungsvorgänge für Agenten durchführen, einschließlich der Änderung der Sichtbarkeit.

86016006.png?width=45386016013.png?width=680

Wie kann ich einen Agenten ausblenden oder entfernen?

Es ist wichtig zu verstehen, dass das Entfernen eines Agenten auch alle über diesen Agenten gesammelten Daten löschen würde. Diese Informationen könnten eines Tages für eine zukünftige Untersuchung nützlich sein.

Stattdessen ist das Ausblenden des Agenten aus der Ansicht, den Benachrichtigungen oder Warnmeldungen wahrscheinlich die gewünschte Maßnahme.

Es gibt zwei Möglichkeiten, dies zu tun.

Massenaktualisierung von Agenten

Die erste Methode ist am einfachsten, wenn mehrere Agenten aus der Web-App ausgeblendet werden müssen.

Wählen Sie zunächst auf der Seite Agenten die Agenten aus, die Sie ausblenden möchten.

Normalerweise verwenden Benutzer zunächst Filter basierend auf Installationsstatus, Rechnername oder IP-Adresse.

Wählen Sie zweitens das Symbol „Bulk Set Agent Default Visibility“ aus.

86048779.png?width=680
Es erscheint ein modales Fenster, in dem Sie auswählen können, ob die Standardsichtbarkeit der ausgewählten Agenten verborgen oder sichtbar sein soll. Klicken Sie anschließend auf die Schaltfläche „Update Selected Agents“.

86081547.png?width=448
Die Standardeinstellung für Sicherheitsbenachrichtigungen sieht vor, dass für ausgeblendete Agenten Offline-Agenten-Warnmeldungen gesendet werden. Weitere Informationen zu Sicherheitsbenachrichtigungen finden Sie hier.

Einen einzelnen Agenten aktualisieren

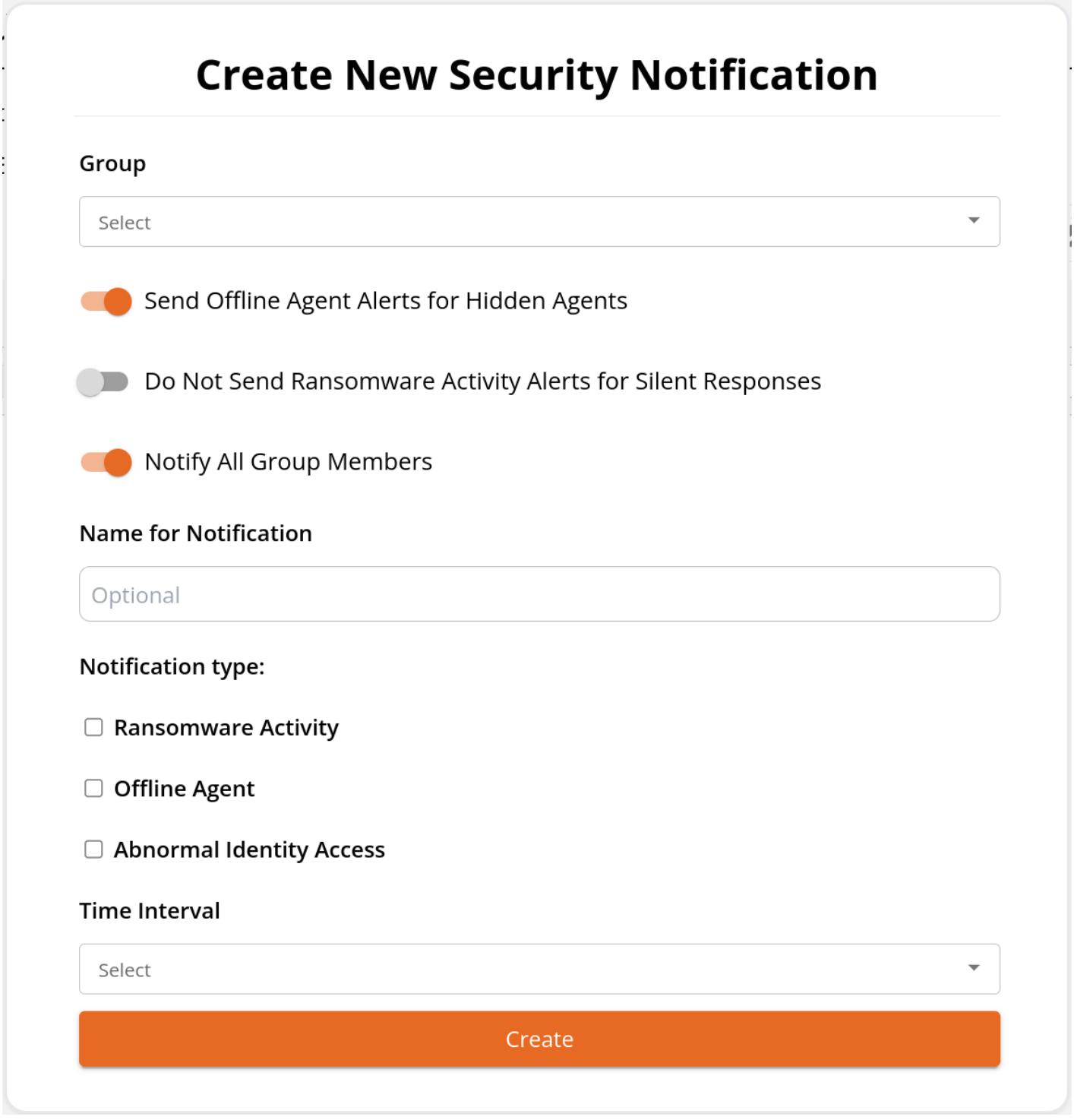
Suchen Sie auf der Seite Agenten die Spalte Dashboard-Sichtbarkeit und schalten Sie den Schieberegler „Sichtbar“ für den gewünschten Agenten um, um die Sichtbarkeit zu ändern.

86016024.png?width=680

Erhalte ich weiterhin Warnungen und Benachrichtigungen, wenn ich einen Agenten ausblende?

Die Standardeinstellung für Benachrichtigungen sieht vor, dass Offline-Agent-Warnungen für ausgeblendete Agenten gesendet werden.

Nachfolgend sehen wir die Standardeinstellung während der Erstellung einer Benachrichtigung:



Benutzer legen in der Regel eine separate Benachrichtigungskategorie für Benachrichtigungen zu ausgeblendeten Agenten an, für die seltenen Fälle, in denen dies gewünscht ist. Wir empfehlen, dass diese Benachrichtigungen unterschiedliche Ziel-E-Mail-Aliasnamen und gegebenenfalls ein anderes Benachrichtigungsintervall verwenden.

Wenn bei einer bestehenden Benachrichtigung eine Aktualisierung dieses Feldes erforderlich ist, rufen Sie die Seite Sicherheitsbenachrichtigungen auf.

Scrollen Sie in der Tabelle nach rechts, bis Sie die Spalte „Offline-Warnungen für ausgeblendete Agenten senden“ sehen, und stellen Sie den Schieberegler wie gewünscht ein.

Die Änderung wird sofort wirksam.