Webanwendung

- Web Application 04.23
- Web Application 08.23
- Web Application 11.23
- Web Application 04.24
- Webanwendung 09.24
- Web Application 05.25
- Web Application 12.25

Web Application 04.23

Funktionen

- Partnerportal-Updates:
  - Möglichkeit, auf der Seite „Deal registrieren“ eine Demo zu planen
  - Neuen Prozess zur Deal-Registrierung mit Cyber Crucible-Genehmigung von Deals implementiert
  - Deal-Prospect-Typ bei der Registrierung von Deals hinzugefügt
  - Monatlichen und jährlichen Abrechnungszyklus für Deals hinzugefügt
  - Versand von Angeboten für von Cyber Crucible genehmigte Deals über Stripe sowie Unterzeichnung von Angeboten vor Abschluss eines Deals implementiert
  - Möglichkeit, die Stripe-Rechnung für einen abgeschlossenen Deal erneut zu senden
  - Möglichkeit, einen Deal über ein Modal zu bearbeiten, ähnlich dem Modal zur Registrierung eines neuen Deals, vorausgefüllt mit den aktuellen Informationen des Deals
- Agenten-/Lizenzverwaltung:
  - Möglichkeit, Lizenzen auf der Agenten-Seite in großer Anzahl freizugeben
  - Möglichkeit, Lizenzen auf der Agenten-Seite in großer Anzahl Agenten zuzuweisen
  - Möglichkeit, auf der Agenten-Seite die Einstellungen für die automatische Neu-Lizenzierung von Agenten anzuzeigen und zu ändern, wenn diese ohne Lizenz unseren REST-Server aufrufen
    - Benutzer können Agenten einzeln und in großer Anzahl aktualisieren
- Möglichkeit implementiert, auf der Gruppen-Seite die Id und die Client-Auth-Werte einer Gruppe anzuzeigen, die im Agent-Installationsskript verwendet werden
- Möglichkeit implementiert, Whitelists in eine andere Gruppe zu kopieren
- Auf React 18 aktualisiert
- Optionen „Spalten zurücksetzen“ und „Alle Spalten automatisch anpassen“ zum Kontextmenü der Raster bei Rechtsklick hinzugefügt
- Option zum Herunterladen der Memory-Diff-Datei zum Raster „Erpressungsantworten“ für zutreffende Antworten hinzugefügt
- Speicherung des Status für die Diagramm-Sichtbarkeit implementiert
- Neue Anwendungsspalten zum Raster „Identitätszugriff“ für die aufgerufenen, zugreifenden und übergeordneten Programme hinzugefügt.
- Umschaltung des Spaltenmodus für jedes Raster hinsichtlich der Anzahl der anzuzeigenden Spalten implementiert. Modi umfassen: Min, Mittel, Max und Benutzerdefiniert
- Such-/Autovervollständigungsfunktion in Dropdown-Auswahlelementen mit Material UI implementiert

Web Application 08.23

Funktionen

- Partner-Portal-Updates:
  - Die Seite „Demo-Videos“ wurde dem Partner-Portal hinzugefügt
  - Die Möglichkeit, ein POC für genehmigte Partner-Deals zu erstellen, wurde hinzugefügt
  - Die Seite „Distributor Group Management“ wurde dem Partner-Portal hinzugefügt, damit Distributor-Partner ihre Untergruppen erstellen und verwalten können
  - Die Seite „Zahlungsverwaltung“ wurde dem Partner-Portal hinzugefügt
  - Die Möglichkeit, den Eigentümer eines Partner-Deals zu ändern, wurde hinzugefügt
  - Ein benutzerdefiniertes Notizfeld für Partner-Deals wurde hinzugefügt, das auf Stripe-Rechnungen und -Angeboten angezeigt wird
- Eine „Angemeldet bleiben“-Funktion wurde implementiert, mit der Benutzer angemeldet bleiben können
- Ein Link zur Ansicht des Stripe-Kundenportals wurde hinzugefügt, über das Benutzer ihre Abonnements und Zahlungsmethoden verwalten können
- Die Möglichkeit, auf der Seite „Agent-Lizenzen“ die Gruppe mehrerer ausgewählter Lizenzen im Raster zu ändern, wurde hinzugefügt
- AG Grid wurde auf Version 29 aktualisiert
- Abhängigkeiten wurden auf ihre neuesten Versionen aktualisiert
- Die Schaltfläche „Automatisierung“ oberhalb der Raster, die Symbole anzeigte, wurde entfernt; stattdessen wurden die Symbole direkt oberhalb des Rasters platziert
- Die Schaltfläche „Spalten“ oberhalb der Raster, die die Rasterspalten-Statusoptionen anzeigte, wurde entfernt; stattdessen wurden die Rasterspalten-Statusoptionen direkt oberhalb des Rasters platziert
- Die Möglichkeit, Benutzerkonto-Einladungen auf der Seite „Gruppen“ erneut zu senden, wurde hinzugefügt
- Die Spalte „Canary Extension Mode“ wurde der Seite „Gruppen“ hinzugefügt
- Weitere Anwendungsbeschriftungen wurden der Seite „Identitätszugriff“ hinzugefügt
- Symbole und Filterung im Raster „Identitätszugriff“ wurden der Spalte „Kein vertrauenswürdiges Zertifikat“ für „Verbindung getrennt beim Abrufen der Zertifikatinformationen“ und „Zeitüberschreitung beim Abrufen der Zertifikatinformationen“ hinzugefügt
- Ein Problem beim Rendern von Rastern auf mobilen Geräten wurde behoben

Web Application 11.23

Funktionen

- Die Möglichkeit hinzugefügt, Lizenzen für inaktive Agenten automatisch freizugeben.
  - Diese Funktion ist eine Gruppeneinstellung und bietet die Optionen, Lizenzen für inaktive Agenten in der Gruppe nach 30/60/90 Tagen automatisch freizugeben, sowie die Möglichkeit, diese Einstellung zu deaktivieren
- Aktualisierungen der Whitelist
  - Die Möglichkeit hinzugefügt, eine Ausnahme mit dem übergeordneten Programmpfad und den Argumenten zu erstellen
  - Die Möglichkeit hinzugefügt, eine Ausnahme zu erstellen, die Erpressungsreaktionen zuordnet, wenn nur vertrauenswürdige Zertifikate vorhanden sind, nur dann übereinstimmt, wenn keine zugehörigen Injektionen vorliegen, und nur dann übereinstimmt, wenn kein veränderter Speicher vorliegt
  - Die Möglichkeit hinzugefügt, eine Ausnahme zu erstellen, die bestimmten Dateizugriffsauslösern entspricht
- Den übergeordneten Programmpfad und die Argumente zum Raster der Erpressungsreaktionen hinzugefügt
- Dateihashes zum Modal für Erpressungsreaktionsdetails hinzugefügt
- Neue Warnungstypen für Sicherheitsbenachrichtigungen hinzugefügt:
  - Verhaltensmodell abgestimmt
  - Neue Agent-Version
- Die E-Mails für Ransomware-Aktivitätswarnungen aktualisiert, sodass sie einen Link enthalten, der Benutzer automatisch zur Seite „Erpressungsreaktionen“ mit einem Filter weiterleitet, der die Reaktionen anzeigt, auf die sich die Warnung bezog
- Option zum Diagramm der Agenten-Seite hinzugefügt, um im Diagramm nur Zählungen für Agenten einzubeziehen, die sich in den letzten 30/60/90 Tagen gemeldet haben, sowie die Option, die Zählungen nicht zu begrenzen
- Beispiele auf der Seite der REST-Integration für den Aufruf des AWS-/token-Endpunkts hinzugefügt. Die Beispiele umfassen den Aufruf des Endpunkts mit Bash, PowerShell und der Eingabeaufforderung
- Die Berechtigungen für den Incident Manager auf der Seite „Rollen“ aktualisiert, sodass nur Ansichts-/Bearbeitungsrechte für Whitelists und stille Reaktionsregeln bestehen
- Der veraltete Response Automation Manager wurde von der Seite „Rollen“ entfernt
- Das Modal für die Abstimmung von Browser-Hilfsprozessen wurde zu den Seiten „Whitelists“, „Stille Reaktionsregeln“ und „Erpressungsreaktionen“ hinzugefügt
  - Enthält die Option auszuwählen, wie Agenten in Gruppen auf Chrome-Hilfsprozesse reagieren sollen
- Option hinzugefügt, den Agenten mithilfe eines PowerShell-Skripts herunterzuladen

- Die Gruppeneinstellung hinzugefügt, damit Agenten in der Gruppe im abgesicherten Modus ausgeführt werden
- Die Spalte „Betriebssystemname“ zum Agenten-Raster hinzugefügt
- Ein Problem behoben, bei dem sich bei bestimmten Rastern die Spaltenbreiten und die Reihenfolge bei Klicks auf Symbole/Schaltflächen auf der Seite zurücksetzten

Web Application 04.24

Funktionen

- Die Möglichkeit zum Einrichten und Verwalten von Proxy-Konfigurationen wurde hinzugefügt, um die Agenten-Bereitstellung zu unterstützen. Weitere Informationen zu Proxy-Konfigurationen finden Sie hier
- Das Problem wurde behoben, bei dem die horizontale Bildlaufleiste am unteren Rand unserer Datenraster nicht sichtbar war, da das Raster über die sichtbare Bildschirmhöhe hinausging
- Auf unseren Telemetrie-Seiten wurde die Möglichkeit hinzugefügt, zwischen der Anzeige aller Telemetriedaten oder nur der Daten, die direkt mit einer Erpressungsreaktion in Zusammenhang standen, umzuschalten
- Die Gruppeneinstellung zum automatischen Ausblenden von Agenten in der Gruppe wurde hinzugefügt, wenn eine Lizenz von einem Agenten freigegeben wird, ein Agent als inaktiv markiert wird oder ein Agent eine Deinstallation abschließt
- Beim Klicken auf einen Link aus einer unserer Benachrichtigungs-E-Mails wurde die Möglichkeit hinzugefügt, die Daten im entsprechenden Raster automatisch so zu filtern, dass angezeigt wird, was die Benachrichtigung ausgelöst hat
- Das Diagramm „Agenten-Lizenzen“ wurde aktualisiert, um die Anzahl sowohl für Desktop- als auch für Server-Lizenzen anzuzeigen
- AG Grid wurde auf Version 31 aktualisiert
- Ag Charts wurde auf Version 9 aktualisiert
- Weitere Textfilteroptionen wurden zu unseren Datenrastern hinzugefügt
- Die Seite „Kunden-Bereitstellungsstatus“ wurde hinzugefügt (zu finden unter der Registerkarte „Betrieb“)

Webanwendung 09.24

Features

- Auf der Seite „Agent-Lizenzen“ wurde die Möglichkeit hinzugefügt, abgelaufene Lizenzen standardmäßig aus dem Raster und der Grafik herauszufiltern. Diese Einstellung kann über den Schalter oberhalb des Agent-Lizenzen-Rasters aktualisiert werden
- Mehrbedingungsfilter für eine einzelne Spalte in den serverseitigen Rastern implementiert. Die serverseitigen Raster sind die Raster, bei denen aufgrund der großen Zeilenanzahl nicht alle Zeilen beim ersten Laden in das Raster geladen werden: Extortion Response, Prozesserstellungen, Prozessinjektionen und Identitätszugriffe
- Die Mehrjahresoption für Deal-Registrierungen wurde hinzugefügt. Deals können bis zu 3 Jahre lang sein, und Nutzer haben bei mehrjährigen Deals die Wahl, im Voraus oder jährlich zu bezahlen
- Temporäre Tailored Behaviors implementiert. Weitere Informationen hier
- Neue Spalte im Identitätszugriffs-Raster für die Ursachenanalyse (Root Cause Analysis) hinzugefügt
- Sicherheitsbenachrichtigungen um zwei verschiedene Optionen für Offline-Agent-Warnungen aktualisiert: Teilweise und vollständig offline befindliche Agent-Warnungen
- Neue Spalten im Agenten-Raster für das Ablaufdatum der Lizenz und das Datum der Lizenzzuweisung zum Agenten hinzugefügt
- Neue Gruppeneinstellung für den DMZ-Modus hinzugefügt, die von Agenten in der Gruppe befolgt wird. Der DMZ-Modus ist für Umgebungen gedacht, in denen keine Online-Zertifikatsprüfung verfügbar ist. Durch Aktivieren des DMZ-Modus werden CA-Root-Zertifikate lokal auf den Agenten der Gruppe eingebettet und OSCP wird deaktiviert
- Neue Gruppeneinstellung hinzugefügt, damit Agenten in der Gruppe ein Agenten-Symbol im Infobereich (System-Tray) des zugehörigen Agenten-Rechners anzeigen; nur Agenten ab Version 4.4.8.2 verfügen über diese Funktion
- Eine Seitenleiste zu unseren Datenrastern hinzugefügt, um Spaltensichtbarkeit und -reihenfolge einfach zu ändern

Web Application 05.25

Funktionen

- SSO-Integration für unseren Dashboard-Login mit Microsoft Entra ID (Azure Active Directory) hinzugefügt
  - Benutzer müssen sich an Cyber Crucible wenden und einige Schritte durchführen, die hier zu finden sind, um die Entra ID SSO-Integration für ihre Organisation mit unserem Dashboard-Login einzurichten
- Distributor-Partner-Updates
  - Verbesserungen am Prozess der Zuordnung von Reseller-Untergruppen durch Distributoren sowie an der Registrierung und Abwicklung von Deals durch diese Reseller-Untergruppen. Eine detailliertere Erklärung des verbesserten Distributor Group Management-Prozesses finden Sie hier
  - Neuen Sales-Benachrichtigungstyp für Distributor-Partner hinzugefügt, um Benachrichtigungen zu erhalten, wenn ihre Reseller-Untergruppen eine neue Deal-Registrierung erstellen
  - Möglichkeit für Distributor-Partner hinzugefügt, die Mehrjahresrabatte für ihre Reseller-Untergruppen zu bearbeiten. Dies ist auf der Distributor Group Management-Seite zu finden
  - Spalte „Distributor Approval“ zur Deal-Registrierung hinzugefügt, damit Distributoren die Deals ihrer Reseller-Untergruppen verwalten können
  - Die Seite „Partner in Motion“ unter dem Tab „Partners“ hinzugefügt, damit Distributor-Partner in Vorbereitung befindliche Reseller-Untergruppen-Partner registrieren können
- Den „Partner Deal Manager“ zu den Rollen für Vorgänge im Zusammenhang mit der Deal-Registrierung hinzugefügt
- Neuen Sales-Benachrichtigungstyp für Partner Deal POC-Aktivitäten hinzugefügt. Diese Benachrichtigung gilt für die neue POC-Gruppe, die erstellt wird, wenn ein Partner einen POC für einen Deal anlegt. Benachrichtigungen dieses Typs werden bei Agent-Installationen/-Deinstallationen sowie beim Ablauf der POC-Lizenzen in der POC-Gruppe gesendet
- Neuen Agent-Installationstyp „Native CLI“ hinzugefügt
- Das Modal „Edit Group“ auf der Seite „Group Management“ hinzugefügt, mit dem Sie die Gruppeneinstellungen im großen Umfang bearbeiten können
- AG Grid auf Version 32 aktualisiert
- Umschalter/Schaltfläche zur Anzeige des Passworts beim Login hinzugefügt

Web Application 12.25

Funktionen

- Die neue Seite „AI Firewall Management“ im Tab „Operations“ wurde hinzugefügt
- DLL-Visualisierung
  - Möglichkeit zur Anzeige zugehöriger Modul-Ladevorgänge für Extortion Responses, Process Creations, Process Injections und Identity Accesses hinzugefügt
  - Diesen Seiten wurde eine neue Spalte hinzugefügt, die anzeigt, ob zugehörige nicht vertrauenswürdige Modul-Ladevorgänge gefunden wurden. Wird ein nicht vertrauenswürdiger Modul-Ladevorgang gefunden, zeigt die Zelle in dieser Spalte ein Symbol an, über das Benutzer zu einer neuen Seite gelangen, auf der alle zugehörigen nicht vertrauenswürdigen Modul-Ladevorgänge angezeigt werden
- Neue Spalten zu den Grids „Extortion Responses“ und „Identity Access“ hinzugefügt:
  - 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
- Dem Grid „Extortion Responses“ wurde die Spalte „Data Access Attempted“ hinzugefügt, die den Pfad auf dem Rechner anzeigt, an dem der Datenzugriffsversuch erfolgte
- Die Seite „Extortion Responses“ wurde aktualisiert und bietet nun 2 verschiedene Grid-Optionen. Die bisherige Grid-Option für eine kompaktere Ansicht der Extortion Responses mit übergeordnetem und untergeordnetem Grid ist weiterhin vorhanden; zusätzlich gibt es nun eine neue Option, die das übergeordnete/untergeordnete Grid entfernt und alle Daten und Spalten in einem einzigen Grid anzeigt
- Dem Grid „Agents“ wurden Spalten hinzugefügt, die anzeigen, ob der Agent vollständig konfiguriert ist, sowie das Datum, an dem der Agent erstmals vollständig konfiguriert wurde
- Dem Grid „Agents“ wurden zusätzliche Spalten hinzugefügt, die anzeigen, welchen OAuth-Server und REST-Server der Agent aufruft, sowie die WAN-IPv4- und IPv6-Adresse des Agents
- Im Tab „Partners“ wurden Co-Branding-Materialien hinzugefügt, mit denen Partner eine .zip-Datei mit allen Co-Branding-Materialien herunterladen können
- AG Grid wurde auf Version 34 aktualisiert
- Der Seite „Agent Licenses“ und der Seite „Agents“ wurde die Anzahl der Tage bis zum Ablauf einer Lizenz hinzugefügt. Diese ist auf der Seite „Agent Licenses“ als Symbol in der Spalte „Renews“ und auf der Seite „Agents“ in der Spalte „License Expiration Date“ zu finden

- Den Security Notifications wurde eine neue Option hinzugefügt, um in der E-Mail-Benachrichtigung für Ransomware- und Identity-Access-Alarme eine CSV-Datei mit Informationen darüber, warum der Alarm ausgelöst wurde, einzuschließen. Diese Option wurde hinzugefügt, damit Benutzer direkt in der E-Mail einsehen können, warum ein Alarm aufgetreten ist, ohne sich im Dashboard anmelden zu müssen