Middleware (REST-Server)

- Middleware 01.23
- Middleware 04.23
- Middleware 08.23
- Middleware 11.23
- Middleware 04.24
- Middleware 09.24
- Middleware 05.25
- Middleware 12.25

Middleware 01.23

Funktionen

- Controller für Schulungslizenzen implementiert und einen Dienst für den Ablauf von Schulungslizenzen hinzugefügt.
- Jeden Endpunkt aktualisiert, um die neue Trainingsmodus-Funktion der Webanwendung zu berücksichtigen, sowie Tests für jeden Endpunkt im Trainingsmodus hinzugefügt.
- Einen Endpunkt zum Zurücksetzen aller Schulungsdaten einer übergeordneten Gruppe auf ihren ursprünglichen Zustand hinzugefügt.
- Endpunkte für die neue Einstellung der Passwortalterungsrichtlinie für Gruppen implementiert.
- Dokumentation für die Reactive-Springboot-Endpunkte hinzugefügt.

Middleware 04.23

Funktionen

- Partnerportal-Updates:
  - Endpunkte für den neuen Register-Deal-Prozess mit Genehmigung von Deals durch Cyber Crucible implementiert
  - Das PartnerDeal-Modell aktualisiert, sodass Deals ein zugehöriger Typ zugeordnet ist, wobei jedem ein prozentualer Rabatt zugeordnet ist
    - Das PartnerDeal-Modell auch für beide Referral-Deal-Typen aktualisiert, um das Dashboard-Benutzerkonto zu speichern, das den Lizenzen für den Deal zugeordnet werden soll
  - Das PartnerDeal-Modell aktualisiert, um monatliche und jährliche Abrechnung für die Zahlung von Deals trennen zu können
    - Beinhaltet die Aktualisierung bestehender Endpunkte, um monatliche und jährliche Abrechnung für Stripe zu berücksichtigen
  - Endpunkte implementiert, um Angebote für einen Deal über Stripe versenden zu können
  - Endpunkt implementiert, um die Stripe-Rechnung für einen Deal erneut zu versenden
  - Endpunkt implementiert, um mehrere Felder für einen Deal gleichzeitig zu bearbeiten, verknüpft mit dem Bearbeiten-Deal-Modal in der Webanwendung
- Agenten-/Lizenzverwaltung:
  - Endpunkt implementiert, um Lizenzen massenweise Agenten zuzuweisen
  - Endpunkt implementiert, um die Einstellung für die automatische Neulizenzierung für einen bestimmten Agenten zu ändern
  - Endpunkt implementiert, um eine Lizenz von einem Agenten freizugeben, indem die agentId in der Anfrage übergeben wird
- Endpunkte implementiert, um die Benutzereinstellung zum Anzeigen des Installer-Skript-Konfigurationssymbols im Gruppenraster abzurufen und zu speichern
- Endpunkt implementiert, um den Wert für die Agent-Installer-Skript-Client-Authentifizierung für eine Gruppe abzurufen
- Unseren AV-Scanner-Dienst aktualisiert, um zusätzlich zur Prozesserstellungs-Collection auch in der Identitätsvorfall-Collection zu suchen
- Verschiedene Aktualisierungen unserer Liste von Standarddaten- und Identitäts-Whitelists für AVs.
- Neuen Change-Stream-Endpunkt implementiert, um auf neue Extortion-Response-Einfügungen zu horchen
- Endpunkt implementiert, um Whitelists in eine andere Gruppe zu kopieren
- Endpunkt implementiert, um die Memory-Diff-Datei für einen Vorfall herunterzuladen
- Kategorisierung von Identitätsvorfall-Programmen in Anwendungen implementiert

- Speichern von Spaltenmodi für jedes Web-Seiten-Raster sowie Speichern der Sichtbarkeitseinstellungen für Diagramme implementiert

Middleware 08.23

Funktionen

- Partner-Portal-Updates:
  - Endpunkte implementiert, um ein POC für genehmigte Partner-Deals erstellen zu können
  - Endpunkte für die Seite zur Verwaltung von Distributorgruppen in der Webanwendung implementiert
  - Endpunkt implementiert, um die Daten für das Payment-Management-Raster in der Webanwendung zurückzugeben
  - Möglichkeit implementiert, den Eigentümer eines Partner-Deals zu ändern
  - Möglichkeit implementiert, ein benutzerdefiniertes Memo für Partner-Deals festzulegen, das auf Stripe-Rechnungen und -Angeboten angezeigt wird
- Endpunkt implementiert, um Einladungen zu Benutzerkonten erneut senden zu können
- Weitere Anwendungsbeschriftungsoptionen für Identity-Access-Objekte hinzugefügt
- Das Group-Modell für Partnergruppen um neue boolesche Felder für den Partnertyp aktualisiert
- Das Group-Modell um eine Liste von Canary-Erweiterungskonfigurationen aktualisiert
- Verschiedene Aktualisierungen unserer Standardliste für Daten-, Identitäts- und Zertifikats-Whitelists für Antivirenprogramme
- HTTP/2-Unterstützung aktiviert
- Unser Spring Boot auf die neueste Version sowie verschiedene weitere Abhängigkeiten aktualisiert
- Benachrichtigungswarnungen für ungewöhnliche Identity-Zugriffe implementiert
- Serverantwort-Komprimierung für Agenten aktiviert
- Filterung für die Spalte „Kein vertrauenswürdiges Zertifikat“ im Identity-Access-Raster in der Webanwendung für die Optionen „Getrennt beim Abrufen der Zertifikatsinformationen“ und „Zeitüberschreitung beim Abrufen der Zertifikatsinformationen“ implementiert
- Problem in unserem Benachrichtigungsdienst für ablaufende Partner-Deals behoben, sodass für abgeschlossene Deals keine „abgelaufen“-E-Mails mehr gesendet werden

Middleware 11.23

Funktionen

- Whitelist-Updates
  - Implementierung der Möglichkeit, eine Ausnahme mit dem übergeordneten Programmpfad und den Argumenten zu erstellen
  - Implementierung der Möglichkeit, eine Ausnahme zu erstellen, die Erpressungsantworten abgleicht, wenn nur vertrauenswürdige Zertifikate vorhanden sind, nur dann übereinstimmt, wenn keine zugehörigen Injektionen vorliegen, und nur dann übereinstimmt, wenn kein modifizierter Speicher vorhanden ist
  - Implementierung der Möglichkeit, eine Ausnahme zu erstellen, die bestimmte Dateizugriffsauslöser abgleicht
- Implementierung einer Gruppeneinstellung zur automatischen Freigabe von Lizenzen für inaktive Agenten
  - Aktualisierung des Gruppenmodells um eine Einstellung, wann Lizenzen von inaktiven Agenten in der Gruppe freigegeben werden sollen. Optionen sind 30/60/90 Tage oder die Deaktivierung dieser Einstellung
  - Aktualisierung des Agentenmodells um einen neuen Inaktivitätsstatus
  - Implementierung eines Dienstes zur automatischen Freigabe von Lizenzen inaktiver Agenten gemäß ihrer Gruppeneinstellung
- Aktualisierung des Endpunkts zum Abrufen von Erpressungsantworten, um den übergeordneten Programmpfad und die Argumente einzuschließen
  - Der übergeordnete Programmpfad und die Argumente sind nun auch in den eindeutigen Erpressungsantwort-Zählungen für die Webanwendung, die Sicherheitsbenachrichtigungen und die Executive Summaries enthalten
- Aktualisierung unserer Executive-Summary-Berichte, um die Lizenzen-Folie in separate Folien für Desktop- und Server-Lizenzen aufzuteilen
- Aktualisierung des E-Mail-Sicherheitsbenachrichtigungsmodells und des Sicherheitsbenachrichtigungsdienstes um zwei neue Alarmtypen
  - Verhaltensmodell angepasst
  - Neue Agentenversion
    - Wenn die verwalteten Update-Einstellungen einer Gruppe so geändert werden, dass automatische Updates deaktiviert sind, wird automatisch eine Benachrichtigung über eine neue Agentenversion für die Gruppe erstellt
- Aktualisierungen der Benutzerrollen/-berechtigungen
  - Aktualisierung der Berechtigungen des Rollenmodells „Incident Manager“, sodass nun nur noch Ansicht/Bearbeitung für Whitelists und stille Reaktionsregeln vorhanden sind
  - Gruppen verfügen nun über 3 Standardrollen, die von Benutzern nicht bearbeitet werden können:

    - Admin
    - Nur Lesen
    - Gast
  - Benutzer, die einer Gruppe hinzugefügt werden, erhalten standardmäßig die Rolle „Gast“
- Implementierung von Endpunkten für das Modal zur Abstimmung von Browser-Hilfsprozessen der Webanwendung, um einfach verwalten zu können, wie Agenten in Gruppen auf Chrome-Hilfsprozesse reagieren sollen
- Aktualisierung des Endpunkts für das Diagramm der Agenten-Seite, um Zählungen auf Agenten beschränken zu können, die sich in den letzten 30/60/90 Tagen gemeldet haben
- Aktualisierung der E-Mail-Benachrichtigung „Ransomware-Aktivität“ der Sicherheitsbenachrichtigung, um einen Link einzuschließen, der Benutzer automatisch zur Seite „Erpressungsantworten“ weiterleitet, mit einem Filter, der die Antworten anzeigt, auf die sich die Benachrichtigung bezog
- Implementierung einer Gruppeneinstellung, ob Agenten in einer Gruppe im abgesicherten Modus ausgeführt werden oder nicht
- Implementierung einer PowerShell-Skriptoption zur Installation von Agenten
- Aktualisierung unseres Spring Boot auf die neueste Version
- Verschiedene Aktualisierungen unserer Liste von Standarddaten-, Identitäts- und Zertifikats-Whitelists für Antivirenprogramme

Middleware 04.24

Funktionen

- Die Gruppeneinstellung und zugehörige Endpunkte für die Einrichtung und Verwaltung von Proxy-Konfigurationen zur Unterstützung der Agenten-Bereitstellung wurden implementiert
- Unsere Telemetriedaten-Endpunkte wurden aktualisiert, sodass entweder alle Telemetriedaten oder nur die direkt mit einer Erpressungsreaktion zusammenhängenden Daten angezeigt werden können
- Die Gruppeneinstellung zum automatischen Ausblenden von Agenten in Gruppen wurde implementiert, wenn eine Lizenz von einem Agenten freigegeben wird, ein Agent als inaktiv markiert wird oder ein Agent eine Deinstallation abschließt
- Die Links zu unserem Dashboard in unseren Benachrichtigungs-E-Mails wurden aktualisiert, sodass sie einen URL-Parameter enthalten, der verwendet wird, um die Daten im zugehörigen Frontend-Raster automatisch zu filtern und anzuzeigen, wodurch die Benachrichtigung ausgelöst wurde
- Der für das Frontend-Diagramm „Agent Licenses“ verwendete Endpunkt wurde aktualisiert, sodass er sowohl Zählungen für Desktop- als auch für Server-Lizenzen enthält
- Endpunkte für die neue Frontend-Seite „Customer Deployment Health“ wurden implementiert
- Unsere Prozessoptimierung wurde aktualisiert, um Microsoft Edge WebView zu berücksichtigen

Middleware 09.24

Funktionen

- Endpunkte für die neue Einstellung „Group DMZ Mode“ implementiert
- Endpunkte zur Deal-Registrierung aktualisiert, sodass Mehrjahresverträge registriert werden können, mit der Möglichkeit, für Mehrjahresverträge im Voraus oder jährlich zu bezahlen
- Möglichkeit hinzugefügt, die Ursachenanalyse (Root Cause Analysis) für Identity Accesses einzusehen
- Temporary Tailored Behaviors implementiert
- Das User-Modell aktualisiert, um die Einstellung zum standardmäßigen Ein-/Ausblenden abgelaufener Agent-Lizenzen im Agent-Lizenzen-Raster zu speichern
- Das Security-Notification-Modell sowie zugehörige Endpunkte/Dienste für die neuen Offline-Agent-Warnoptionen „Teilweise offline“ und „Vollständig offline“ aktualisiert
- Aktualisierungen der Endpunkte im Zusammenhang mit den neuen Spalten im Frontend des Agents-Rasters, um anzuzeigen, wann die zugewiesene Lizenz abläuft und wann die Lizenz dem Agenten zugewiesen wurde
- Einstellung im Group-Modell hinzugefügt, damit Agenten in der Gruppe das Agent-Symbol im Systemtray des jeweiligen Agent-Rechners anzeigen
- Die serverseitigen Raster-Abfragen aktualisiert, sodass sie Filter mit mehreren Bedingungen für denselben Schlüssel/dieselbe Spalte verarbeiten können

Middleware 05.25

Funktionen

- Das Sales-Notification-Modell wurde um neue Typen erweitert:
  - Distributor-Partner können Benachrichtigungen erhalten, wenn ihre Reseller-Untergruppen eine neue Deal-Registrierung erstellen
  - Partner Deal POC-Aktivität
- Der Authentifizierungsprozess wurde aktualisiert, um eine SSO-Integration mit Microsoft Entra ID (Azure Active Directory) zu ermöglichen
- Der Agent-Installer-Endpunkt wurde aktualisiert, um einen neuen Installer-Typ für Native Cli zu ermöglichen
- Die Endpunkte für die neuen Distributor-Partner-Updates wurden aktualisiert
  - Ein neues Partner-in-Motion-Modell wurde hinzugefügt
  - Das Partner Deal Registration-Modell wurde aktualisiert, um Distributoren die Möglichkeit zu geben, die Deals ihrer Reseller-Untergruppen zu genehmigen
  - Distributor-Partnern wurde die Möglichkeit hinzugefügt, die Mehrjahresrabatte für ihre Reseller-Untergruppen zu bearbeiten
  - Distributoren wurde die Möglichkeit hinzugefügt, sich selbst Angebote mit ihrer Distributor-Preisgestaltung für den Deal einer Reseller-Untergruppe zu senden
  - Es wurde die Anforderung hinzugefügt, dass bei der Registrierung eines Deals durch eine Reseller-Untergruppe die Subgroup Reseller Agreement von deren übergeordnetem Distributor auf der Distributor Group Management-Seite hochgeladen werden muss
- Das Role-Modell wurde um einen neuen Partner Deal Manager für Deal-Registrierungsvorgänge erweitert, und jeder zugehörige Endpunkt wurde aktualisiert, um die Berechtigung zu prüfen
- Der Endpunkt zum massenhaften Bearbeiten von Gruppeneinstellungen wurde hinzugefügt
- Unser Spring Boot wurde auf die neueste Version aktualisiert
- Die für die Erstellung von Executive Reports verwendeten Abfragen wurden verbessert, um die Zeit zur Erstellung des Reports zu verkürzen
- Unsere Telemetriesammlungen in der Datenbank wurden auf Sharding umgestellt
- Die für das Dashboard-Grid verwendete Agenten-Abfrage wurde aktualisiert, um anzugeben, ob es sich bei dem Agenten um einen Server handelt oder nicht
- Der Endpunkt /updateGroupAutomaticallyHideAgentsReactive wurde aktualisiert, um das Update rückwirkend auf bestehende Agenten anzuwenden
- Wesentliche Authentifizierungsupdates, damit Agenten unsere REST-Server mit der neuen gehosteten OAuth-Authentifizierung aufrufen können
- Neue Endpunkte für die Übermittlung von DLL-Telemetrie durch Agenten wurden hinzugefügt

Middleware 12.25

Funktionen

- Neue Endpunkte für die DLL-Visualisierung im Dashboard hinzugefügt, um zugehörige nicht vertrauenswürdige Modul-Ladevorgänge für Extortion Responses, Prozesserstellungen, Prozessinjektionen und Identitätszugriffe anzuzeigen
- Die Endpunkte für Extortion Response und Identitätszugriff für die Dashboard-Abfragen aktualisiert, sodass zusätzliche Felder für die DLL-Visualisierung zurückgegeben werden, einschließlich geänderter Modulspeicher, geänderter Modulpfad usw.
- Das Agent-Modell um neue Felder erweitert, die angeben, ob der Agent vollständig konfiguriert ist und an welchem Datum der Agent erstmals vollständig konfiguriert wurde
- Neue Endpunkte und Controller für die Seite AI Firewall Management hinzugefügt
- Den Endpunkt, der die Liste der Agenten für das Dashboard zurückgibt, aktualisiert, um neue Felder für den Rest-Server und OAuth-Server, mit dem der Agent kommuniziert, sowie die WAN-IPv4- und IPv6-Adresse des Agenten einzuschließen
- Neuen Endpunkt für die Seite Extortion Responses hinzugefügt, der es Benutzern ermöglicht, alle Felder eines Extortion Response über diesen Endpunkt einzusehen, anstatt den bestehenden Endpunkt zu verwenden, der eine verkürzte Ansicht der Felder bietet und einen zusätzlichen API-Aufruf für weitere Details erfordert.
  - Benutzer im Dashboard können über den Umschalter auf der Seite Extortion Responses zwischen der bisherigen Rasteransicht und der neuen Rasteransicht wählen, die alle Felder in einem einzigen Raster zurückgibt
- Neue Option für Sicherheitsbenachrichtigungen hinzugefügt, um dem E-Mail-Alarm für Ransomware- und Identitätszugriffswarnungen eine CSV-Datei mit Informationen darüber beizufügen, warum der Alarm ausgelöst wurde.