

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.

Revision #1

Created 2026-07-24 04:10:51 UTC by Dennis Underwood

Updated 2026-07-24 04:10:51 UTC by Dennis Underwood