RESOURCE CENTER

Bitwarden-Ereignisse mit Splunk für SIEM Management überwachen

Erfahren Sie, wie Bitwarden und Splunk zusammenarbeiten, um Sicherheitsinformationen und Event Management (SIEM) zur Abwehr von böswilligen Angriffen und Netzwerkverletzungen bereitzustellen.

Get the full interactive view at https://bitwarden.com/de-de/resources/monitor-bitwarden-events-using-splunk-for-siem-management/

bitwarden

Splunk ist ein Sicherheits- und Beobachtbarkeitstool, das verwendet wird, um Transparenz über große Datenmengen für Multi-Cloud- und On-Premise-Bereitstellungen bereitzustellen. Die Lösung liefert Einblicke in kritische Kennzahlen wie Betriebszeit, Anomalien, Ausfälle, verdächtige Aktivitäten und mehr. Mit diesen Erkenntnissen zur Cloud-Beobachtbarkeit kann Splunk bösartige Aktivitäten erkennen und IT-, DevOps- und SRE-Teams benachrichtigen, wenn ein Datensicherheitsereignis eintritt.

Bitwarden und Splunk arbeiten zusammen, um Sicherheitsinformationen und Event Management (SIEM) zur Abwehr von böswilligen Angriffen und Netzwerkverletzungen bereitzustellen. Die SIEM-Technologie identifiziert potenzielle Bedrohungen für Online-Anwendungen und bietet gleichzeitig Compliance- und Sicherheitsmanagement für Cloud-Infrastrukturdaten in nahezu Echtzeit. Dies wird erreicht, indem eine Sammlung detaillierter Ereignisse protokolliert wird, die über verschiedene Datenquellen hinweg auftreten.

Mit Bitwarden und Splunk können detaillierte Informationen über die Aktivitäten der Passwortverwaltung gesammelt und in visuellen Dashboards zur einfachen Überwachung angezeigt werden. Zusammen bieten die beiden wertvolle Einblicke in eine bestimmte Bitwarden-Organisation, einschließlich Informationen wie Benutzeraktivitäten, Passwortänderungen, gemeinsame Passwörter und mehr. In Kombination mit der Überwachung anderer Infrastrukturen, Apps und Netzwerke bietet Splunk eine ganzheitliche Sicht auf die Unternehmenssicherheit.

Inhaltsverzeichnis

Die Vorteile von Bitwarden und Splunk zusammen umfassen

- Warnungen bei verdächtigen Aktivitäten und detaillierte Berichte aus Bitwarden-Protokollen
- Erweitert die SIEM-Überwachung auf Website- und Anwendungsanmeldeinformationen
- Visuelle Dashboards und Makros für die Ereignissuche zur einfachen Überwachung
- Aufzeichnungen über den Zugriff auf bestimmte Anmeldeinformationen durch Benutzer
- Einblicke in die Benutzerakzeptanz von Unternehmenssicherheitstools
- Offboarding-Berichte, die Anmeldeinformationen auflisten, auf die ein ehemaliger Mitarbeiter Zugriff hatte, um eine strengere Sicherheit und Zugriffskontrolle zu gewährleisten

Wussten Sie schon?

Bitwarden zeichnet mehr als 60 Arten von Ereignissen auf, die auf Dauer protokolliert werden und zur Analyse und Integration

in bestehende Sicherheitssysteme an Splunk übergeben werden können.

Integrationsdetails: Die offizielle Bitwarden Splunk App

Bitwarden lässt sich über die offizielle Bitwarden Event Logs-App, die in der Benutzeroberfläche verfügbar ist, problemlos in selbst gehostete Splunk Enterprise-, Splunk Cloud Classic- und Splunk Cloud Victoria-Installationen integrieren. Der App-Eintrag ist auch auf Splunkbase zu finden**.** Befolgen Sie die Schritte in der Splunk Siem-Integrationsdokumentation des Bitwarden-Hilfecenters. Sobald Ihre Bitwarden-Organisation mit Splunk verbunden ist, werden drei vorgefertigte Dashboards ausgefüllt: Authentifizierungsereignisse, Tresorartikelereignisse und Organisationsereignisse. Andere benutzerdefinierte Dashboards können erstellt werden, um diese Daten zu nutzen.

Alternativ können Sie die Bitwarden-API-Integration verwenden, um die SIEM-Funktionalität einzurichten, indem Sie Ereignisdaten aus Ihrer Organisation exportieren. Die öffentliche API kann Informationen über Ihre Organisation und Benutzer bereitstellen. Die Vault Management API bietet Zugriff auf Informationen über verschlüsselte Daten und wird innerhalb des Bitwarden CLI-Clients mithilfe des Befehls `serve` auf einem eigenen Endpunkt gehostet. In Kombination bieten diese beiden APIs einen vollständigen Überblick über Ihr Unternehmen und Ihren Tresor.

Zusätzliche Ressourcen

- Verwendung von Splunk mit Bitwarden
- Ereignisprotokolle
- Ereignisprotokolle in Onboarding und Nachfolge
- Splunk SIEM
- Öffentliche Bitwarden-API
- Bitwarden-Tresor-Management-API