RESOURCE CENTER

Bitwarden-gebeurtenissen bewaken met Splunk voor SIEM-beheer

Leer hoe Bitwarden en Splunk samenwerken om beveiligingsinformatie en -gebeurtenissenbeheer (SIEM) te bieden voor verdediging tegen kwaadwillige aanvallen en netwerkinbreuken.

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

bitwarden

Splunk is een beveiligings- en observatietool die wordt gebruikt om inzicht te bieden in grote hoeveelheden gegevens voor multi-cloud en on-premise implementaties. De oplossing biedt inzicht in kritieke meetgegevens zoals uptime, anomalieën, uitval, verdachte activiteiten en meer. Met deze inzichten in cloudobservabiliteit kan Splunk schadelijke activiteiten detecteren en IT-, DevOps- en SRE-teams op de hoogte stellen wanneer zich een gebeurtenis voordoet op het gebied van gegevensbeveiliging.

Bitwarden en Splunk integreren samen om beveiligingsinformatie en gebeurtenisbeheer (SIEM) te bieden voor verdediging tegen kwaadwillige aanvallen en netwerkinbreuken. SIEM-technologie identificeert potentiële bedreigingen voor onlinetoepassingen en biedt tegelijkertijd compliance- en beveiligingsbeheer voor cloudinfrastructuurgegevens in bijna realtime. Dit wordt bereikt door het loggen van een verzameling gedetailleerde gebeurtenissen die plaatsvinden in verschillende gegevensbronnen.

Met Bitwarden en Splunk kan gedetailleerde informatie over activiteiten op het gebied van wachtwoordbeheer worden verzameld en weergegeven in visuele dashboards voor eenvoudige monitoring. Samen bieden de twee samen waardevolle inzichten in een bepaalde Bitwarden-organisatie, waaronder informatie over gebruikersactiviteiten, wachtwoordwijzigingen, gedeelde wachtwoorden en meer. In combinatie met monitoring van andere infrastructuur, apps en netwerken biedt Splunk een holistisch beeld van de bedrijfsbeveiliging.

Inhoudsopgave

De voordelen van Bitwarden en Splunk samen zijn onder andere

- Waarschuwingen voor verdachte activiteiten en gedetailleerde rapporten uit Bitwarden-logboeken
- Breidt SIEM-toezicht uit naar website- en applicatiegegevens
- Visuele dashboards en zoekmacro's voor gebeurtenissen voor eenvoudige monitoring
- Registratie van specifieke credentialtoegang door gebruikers
- Inzicht in de gebruikersadoptie van beveiligingsprogramma's van het bedrijf
- Offboarding-rapporten met een lijst van referenties waartoe een voormalige werknemer toegang had, voor een betere beveiliging en toegangscontrole

Wist je dat?

Bitwarden registreert meer dan 60 soorten gebeurtenissen die permanent worden gelogd en kunnen worden doorgegeven aan

Splunk voor analyse en integratie in bestaande beveiligingssystemen.

Integratiedetails: De officiële Bitwarden Splunk-app

Bitwarden integreert eenvoudig in Splunk Enterprise self-hosted, Splunk Cloud Classic en Splunk Cloud Victoria installaties via de officiële Bitwarden Event Logs app die beschikbaar is in de gebruikersinterface. De app kan ook worden gevonden op Splunkbase**.** Volg de stappen in de Splunk SIEM integratiedocumentatie van het Bitwarden Helpcentrum. Zodra uw Bitwarden-organisatie is verbonden met Splunk, worden drie vooraf gedefinieerde dashboards weergegeven: Authenticatiegebeurtenissen, Vault-itemgebeurtenissen en Organisatiegebeurtenissen. Er kunnen andere aangepaste dashboards worden gebouwd om gebruik te maken van deze gegevens.

U kunt ook de Bitwarden API-integratie gebruiken om SIEM-functionaliteit in te stellen door gebeurtenisgegevens uit uw organisatie te exporteren. De Openbare API kan informatie verschaffen over je organisatie en gebruikers. De Vault Management API biedt toegang tot informatie over versleutelde gegevens en wordt gehost in de Bitwarden CLI-client met behulp van de opdracht `serve` op een eigen eindpunt. Gecombineerd geven deze twee API's een volledig beeld van je organisatie en kluis.

Aanvullende bronnen

- Splunk gebruiken met Bitwarden
- Gebeurtenislogboeken
- Gebeurtenislogboeken bij onboarding en opvolging
- Splunk SIEM
- Openbare API van Bitwarden
- Bitwarden Kluisbeheer API