RESOURCE CENTER

Surveiller les événements Bitwarden à l'aide de Splunk pour la gestion SIEM

Découvrez comment Bitwarden et Splunk s'intègrent pour fournir une gestion des informations et des événements de sécurité (SIEM) afin de se défendre contre les attaques malveillantes et les brèches dans le réseau.

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

bitwarden

Splunk est un outil de sécurité et d'observabilité utilisé pour fournir une visibilité sur de grandes quantités de données pour des déploiements multi-cloud et sur site. La solution fournit des informations sur les mesures critiques telles que le temps de fonctionnement, les anomalies, les pannes, les activités suspectes, etc. Grâce à ces informations sur l'observabilité du cloud, Splunk peut détecter les activités malveillantes et avertir les équipes informatiques, DevOps et SRE lorsqu'un événement de sécurité des données se produit.

Bitwarden et Splunk s'intègrent ensemble pour fournir une gestion des informations et des événements de sécurité (SIEM) pour la défense contre les attaques malveillantes et les violations de réseau. La technologie SIEM identifie les menaces potentielles pour les applications en ligne, tout en assurant la gestion de la conformité et de la sécurité des données de l'infrastructure en nuage en temps quasi réel. Pour ce faire, on enregistre une série d'événements détaillés qui se produisent dans diverses sources de données.

Avec Bitwarden et Splunk, des informations détaillées sur l'activité de gestion des mots de passe peuvent être collectées et affichées dans des tableaux de bord visuels pour un contrôle facile. Ensemble, les deux s'intègrent pour fournir des informations précieuses sur une organisation Bitwarden donnée, y compris des informations telles que l'activité des utilisateurs, les changements de mot de passe, les mots de passe partagés, et plus encore. Associé à la surveillance d'autres infrastructures, applications et réseaux, Splunk offre une vision holistique de la sécurité de l'entreprise.

Table des matières

Les avantages de l'association de Bitwarden et de Splunk sont les suivants

- Alertes en cas d'activité suspecte et rapports détaillés à partir des journaux Bitwarden
- Extension de la surveillance SIEM aux informations d'identification des sites web et des applications
- Tableaux de bord visuels et macros de recherche d'événements pour un contrôle aisé
- Enregistrements de l'accès des utilisateurs à des informations d'identification spécifiques
- Aperçu de l'adoption par les utilisateurs des outils de sécurité de l'entreprise
- Les rapports d'abandon de poste qui répertorient les informations d'identification auxquelles un ancien employé a eu accès, garantissant ainsi une sécurité et un contrôle d'accès plus stricts.

Le saviez-vous ?

Bitwarden enregistre plus de 60 types d'événements qui sont consignés à perpétuité et peuvent être transmis à Splunk à des

fins d'analyse et d'intégration dans les systèmes de sécurité existants.

Détails de l'intégration : L'application officielle Bitwarden Splunk

Bitwarden s'intègre facilement dans les installations Splunk Enterprise auto-hébergées, Splunk Cloud Classic et Splunk Cloud Victoria grâce à l'application officielle Bitwarden Event Logs disponible dans l'interface utilisateur. L'entrée de l'application peut également être trouvée sur Splunkbase**.** Suivez les étapes de la documentation sur l'intégration de Splunk SIEM à partir du Centre d'aide Bitwarden. Une fois que votre organisation Bitwarden est connectée à Splunk, trois tableaux de bord préconstruits s'affichent : Événements d'authentification, Événements de l'espace de stockage et Événements de l'organisation. D'autres tableaux de bord personnalisés peuvent être élaborés pour exploiter ces données.

Vous pouvez également utiliser l'intégration API de Bitwarden pour mettre en place une fonctionnalité SIEM en exportant les données d'événements de votre organisation. L'API publique peut fournir des informations sur votre organisation et vos utilisateurs. L'API de gestion des chambres fortes permet d'accéder à des informations sur les données chiffrées et est hébergée dans le client CLI de Bitwarden à l'aide de la commande `serve` sur un point de terminaison appartenant à Bitwarden. Combinées, ces deux API fourniront une vue complète de votre organisation et de votre coffre-fort.

Ressources complémentaires

- Utiliser Splunk avec Bitwarden
- Journaux d'événements
- Les journaux d'événements dans le cadre de l'intégration et de la succession
- Splunk SIEM
- API publique Bitwarden
- API de gestion des chambres fortes Bitwarden