RESOURCE CENTER

Utiliser Panther avec Bitwarden pour le SIEM afin de surveiller les événements Bitwarden

Découvrez comment Panther peut surveiller les événements Bitwarden pour fournir une gestion des informations et des événements de sécurité (SIEM) afin de générer des alertes et de rationaliser les enquêtes sur les activités suspectes.

Get the full interactive view at https://bitwarden.com/fr-fr/resources/use-panther-with-bitwarden-for-siem-to-monitor-bitwarden-events/

bitwarden

Panther is a cloud-native SIEM solution that is able to process large amounts of data, allowing security teams to investigate security concerns for their infrastructure quickly and in a manner that's easily understood. Panther detects suspicious activity and generates alerts for IT, DevOps, and SRE teams when a potential threat is identified.

Bitwarden integrates with Panther to furnish event logs for security information and event management (SIEM), as a defense against malevolent attacks and intrusions into the network and other IT assets. SIEM technology aggregates events from data sources to detect possible threats in real-time, while also helping ensure compliance and security oversight for data within cloud infrastructure.

With Bitwarden and Panther, detailed information on activity within Bitwarden Password Manager and Secrets Manager can be gathered and analyzed for easy monitoring and alerts. Together, the two integrate to provide valuable insights into a given Bitwarden organization, including information such as user activity, password changes, shared passwords, and more. Panther ingests this data and combines it with the monitoring of other infrastructure, apps, and networking, to provide alerts and streamline investigation into suspicious activities.

The benefits of Bitwarden and Panther together include

- Alerts for suspicious activity and detailed reports from Bitwarden logs
- Expands SIEM oversight to website and application credentials
- Visual dashboards and event search macros for easy monitoring
- Records of specific credential access by users
- Insights into user adoption of company security tools
- Offboarding reports that list credentials a former employee had access to, ensuring tighter security and access control

Did you know?

Bitwarden records more than 50 types of events that are logged in perpetuity and can be passed to Panther for analysis and integration into existing security systems.

Integration Details

Panther connects to Bitwarden through an API key and OAuth 2.0 credentials. Panther has designed an integration within the Panther application catalog, accessible within `Log Sources` in the Panther Dashboard Overview. Once connected to the Bitwarden organization, even logs will automatically flow into Panther. Note that Panther integration is only available for Bitwarden cloud hosted organizations.

Alternatively, use Bitwarden API integration to set up SIEM functionality with any provider by exporting event data from your organization. The Public API can provide information about your organization and users. The Vault Management API provides access to information

about encrypted data and is hosted within the Bitwarden CLI client using the serve command on an owned endpoint. Combined, these two APIs will provide a full view of your organization and vault.

Additional Resources

- Panther SIEM
- Event Logs
- Event Logs in Onboarding and Succession
- Bitwarden Public API
- Bitwarden Vault Management API