RESOURCE CENTER

Monitor Bitwarden events using Microsoft Sentinel SIEM

Discover how Bitwarden integrates with Microsoft Sentinel to deliver robust security information and event management (SIEM), helping defend against malicious attacks and network breaches

Get the full interactive view at https://bitwarden.com/resources/monitor-bitwarden-events-using-microsoft-sentinel/

bitwarden

Using Microsoft Sentinel with Bitwarden password manager for enhanced security monitoring

Monitoring security events from Bitwarden in a centralized platform is essential for organizations that manage sensitive credentials. Microsoft Sentinel, a cloud-native security information and event management (SIEM) system, provides real-time insights into security risks and enables proactive monitoring. In this quick overview, you'll learn about the benefits of integrating Bitwarden with Microsoft Sentinel to improve your organization's security posture.

Why integrate Bitwarden with Microsoft Sentinel?

Some of the key benefits of Integrating Bitwarden with Microsoft Sentinel include:

1. **Enhanced threat detection** Integrating Bitwarden with Sentinel allows for continuous monitoring of Bitwarden activities, such as password changes, unauthorized access attempts, and configuration changes. By collecting these events, Sentinel can correlate them with other security data from across your organization, enabling better detection of suspicious activity.

2. **Streamlined incident response** Security teams can set up automated alerts in Sentinel when potential threats are identified within Bitwarden. For example, Sentinel can notify your team if there's unusual login behavior, repeated failed login attempts, or changes to administrative permissions. This enables quicker responses to potential breaches or misuse of sensitive information.

3. **Centralized security management** Managing security events across multiple tools and platforms can be challenging. By bringing Bitwarden events into Sentinel's centralized dashboard, organizations can simplify their security operations and gain full visibility into credential-related activities alongside other critical security events.

4. **Compliance reporting** For organizations that need to meet stringent security standards or regulatory requirements, the integration helps ensure compliance. Sentinel can log Bitwarden activities, making it easier to track and report on access and usage of credentials, helping organizations meet audit and compliance requirements.

Key Bitwarden events to monitor

The following Bitwarden events logs can provide valuable insights into your organization's security when analyzed through Microsoft Sentinel:

- **Login attempts**: Track user login activity to detect suspicious or unauthorized access attempts.
- **Failed logins**: Monitor failed login attempts, which may indicate brute force attacks or unauthorized access attempts.
- **Collection and item access**: Analyze when users or admins access Bitwarden vaults, including specific collections or sensitive credential items.
- **Password changes**: Log password changes to detect any unusual patterns, such as mass changes across multiple accounts.
- **Admin actions**: Keep an eye on administrative activities, including account management, collection creation, and policy updates.

These events provide critical information that security teams can act upon to prevent credential-related incidents.

Did you know?

Bitwarden records more than 60 types of events that are logged in perpetuity and can be passed to Microsoft Sentinel for analysis and integration into existing security systems.

Integration details: Using Bitwarden with Microsoft Sentinel

Bitwarden integrates seamlessly into Microsoft Sentinel through its SIEM functionality, enabling organizations to track and analyze Bitwarden event logs in real-time. By using the custom logs connector in Microsoft Sentinel, Bitwarden events can be ingested and monitored directly within the platform. Follow the steps in the Bitwarden Help Center for Sentinel SIEM integration to connect your organization and start receiving event data.

Once connected, custom dashboards can be built in Sentinel to monitor critical Bitwarden events such as authentication attempts, vault access, and administrative actions. Use Sentinel's automation features and playbooks to respond to security incidents proactively.

Alternatively, the **Bitwarden public API** can be used to export event data for custom SIEM integrations. The **Public API** offers insights into your organization and users, while the Vault Management API provides encrypted vault data. Both APIs work together to provide a comprehensive view of your organization's security activities.

Additional Resources

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