RESOURCE CENTER

Monitoriza los eventos de Bitwarden usando Splunk para la gestión SIEM

Aprenda cómo Bitwarden y Splunk se integran para proporcionar información de seguridad y gestión de eventos (SIEM) para la defensa contra ataques maliciosos y brechas en la red.

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

bitwarden

Splunk es una herramienta de seguridad y observabilidad que se utiliza para proporcionar visibilidad sobre grandes cantidades de datos para despliegues en múltiples nubes y en las instalaciones. La solución ofrece información sobre parámetros críticos como el tiempo de actividad, anomalías, interrupciones, actividades sospechosas, etc. Con estas perspectivas de observabilidad de la nube, Splunk puede detectar actividad maliciosa y notificar a los equipos de TI, DevOps y SRE cuando se produce un evento de seguridad de datos.

Bitwarden y Splunk se integran para proporcionar información de seguridad y gestión de eventos (SIEM) para la defensa contra ataques maliciosos y brechas en la red. La tecnología SIEM identifica las amenazas potenciales para las aplicaciones en línea, al tiempo que proporciona una gestión de la conformidad y la seguridad de los datos de la infraestructura en la nube prácticamente en tiempo real. Esto se consigue registrando una colección de eventos detallados que se producen en varias fuentes de datos.

Con Bitwarden y Splunk, se puede recopilar información detallada sobre la actividad de gestión de contraseñas y mostrarla en paneles visuales para facilitar la supervisión. Juntos, los dos se integran para proporcionar información valiosa sobre una organización Bitwarden determinada, incluida información como la actividad de los usuarios, los cambios de contraseña, las contraseñas compartidas, etc. Combinado con la supervisión de otras infraestructuras, aplicaciones y redes, Splunk proporciona una visión holística de la seguridad de la empresa.

Índice

Los beneficios de Bitwarden y Splunk juntos

Detalles de la integración: La aplicación oficial de Bitwarden para Splunk

Los beneficios de Bitwarden y Splunk juntos incluyen

- Alertas de actividad sospechosa e informes detallados de los registros de Bitwarden
- Amplía la supervisión SIEM a las credenciales de sitios web y aplicaciones
- Cuadros de mando visuales y macros de búsqueda de eventos para facilitar la supervisión
- Registros de acceso a credenciales específicas por parte de los usuarios
- Información sobre la adopción de las herramientas de seguridad de la empresa por parte de los usuarios
- Informes de baja que enumeran las credenciales a las que ha tenido acceso un antiguo empleado, lo que garantiza una seguridad y un control de acceso más estrictos.

¿Lo sabías?

Bitwarden registra más de 60 tipos de eventos que quedan registrados a perpetuidad y pueden pasarse a Splunk para su

análisis e integración en los sistemas de seguridad existentes.

Detalles de la integración: La aplicación oficial de Bitwarden para Splunk

Bitwarden se integra fácilmente en las instalaciones Splunk Enterprise self-hosted, Splunk Cloud Classic y Splunk Cloud Victoria a través de la app oficial Bitwarden Event Logs disponible en la interfaz de usuario. La entrada de la aplicación también se puede encontrar en Splunkbase**.** Siga los pasos de la documentación de integración Splunk SIEM del Centro de Ayuda de Bitwarden. Una vez que su organización Bitwarden esté conectada a Splunk, aparecerán tres paneles pre-construidos: Eventos de autenticación, Eventos de elementos de bóveda y Eventos de organización. Se pueden crear otros cuadros de mando personalizados para utilizar estos datos.

Alternativamente, utilice la integración API de Bitwarden para configurar la funcionalidad SIEM mediante la exportación de datos de eventos de su organización. La API pública puede proporcionar información sobre su organización y sus usuarios. La API de gestión de bóvedas proporciona acceso a información sobre datos cifrados y se aloja dentro del cliente CLI de Bitwarden mediante el comando `serve` en un endpoint propio. Combinadas, estas dos API proporcionarán una visión completa de su organización y su cámara acorazada.

Recursos adicionales

- Uso de Splunk con Bitwarden
- Registros de sucesos
- Registros de sucesos en incorporación y sucesión
- Splunk SIEM
- API pública de Bitwarden
- API de gestión de bóvedas de Bitwarden