CONSOLE ADMIN > COMPTE RENDU

Microsoft Sentinel SIEM

Afficher dans le centre d'aide: https://bitwarden.com/help/microsoft-sentinel-siem/

Microsoft Sentinel SIEM

Microsoft Sentinel is a security information and event management (SIEM) platform that can be used to monitor Bitwarden organizations. Organizations can monitor event activity with the Bitwarden Event Logs app on Microsoft Sentinel.

Setup

To setup the Bitwarden integration, an active Azure account with access to a Microsoft Sentinel Workspace is required. Additionally, a Bitwarden API key, which can only be retrieved by organization owners.

Install the Bitwarden app to your Microsoft Sentinel dashboard

The Bitwarden Event Logs application can be located in the Microsoft Azure Marketplace. To add the new application to your Workspace:

1. Choose the Bitwarden Event Logs plan from the dropdown menu and select Create.

Microsoft Azure

Home > Marketplace >

Bitwarden Event Logs >> ...

Bitwarden Inc.

Bitwarden Inc. | Azure Application

Plan

Bitwarden Event Logs >> (Create)

2. Complete the required fields and select the Workspace that will be monitoring Bitwarden organization data.

3. Once complete, select Review + create.

Connect your Bitwarden Organization

Once the Bitwarden Event Logs app has been added to your Microsoft Sentinel Workspace, you can connect your Bitwarden organization using your Bitwarden API key.

1. Return to the **Data connectors** screen and select the Bitwarden Event Logs app. Select **Open connector page**. If the Bitwarden Event Logs app is not visible, you may be required to select \bigcirc **Refresh.**

Microsoft Sentinel Selected workspace: "bw-event-logs"	Data con	nectors				×
	🕐 Refresh	<section-header> Guides & Feedback</section-header>				
✓ General	1	••• 0	- More content at			
Overview (Preview)	Connectors	s Connected	Content hub			
₽ Logs						3
📤 News & guides	Search I	by name or provider	Providers : Bitwarden Inc Data Types : All Status	Bitwarde	n Event Logs	
	y- search	by name of provider				
arsigma Threat management	Status	Connector name 1		- Status	Sitwarden Inc Provider	Contraction Contractico Con
Incidents	Status					
2 Workbooks		Bitwarden Event Logs		 Description This connector prov	vides insight into activ	vity of your
Hunting		bitwarden nic		Bitwarden organiza	tion such as user's act	tivity (logged in,
Notebooks				updated, deleted, s	hared, etc.), collection	activity,
Entity behavior				organization activit	y, and more.	
Threat intelligence				Last data received		
MITRE ATT&CK					Manalaa	
(Preview)				Bitwarden	1.0.0	
SOC optimization				Author	Supported	l hu
✓ Content management				Bitwarden	Bitwarden	Inc Email
Content hub				Related content		
 Repositories (Preview) 					10 A	
s Community				Workbooks	Queries Analy	rtics rules templates
\vee Configuration						
Workspace manager (Preview)				Data received		Go to log analytics
Data connectors				3-		
Analytics				2-		
Summary rules (Preview)						
S Watchlist				Open connecto	r page	
		M	icrosoft Sontinal Pitwardon Evant Lags ann			

Microsoft Sentinel Bitwarden Event Logs app

2. Keep this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:

D Password Manager	All vaults			New 🗸	BW BW
🗇 Vaults	FILTERS 📀		Name	Owner	:
🖉 Send					
\ll Tools $\qquad \qquad \bigvee$	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	:
፰ Reports	✓ All vaults				
🕸 Settings 🛛 🗸 🗸	A My vault My Organiz	0 3	Personal Login myusername	Me	:
	→ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ۞ Login □ Card Identity □ Secure note 	0 Ø	Shared Login sharedusername	My Organiz	:
 Password Manager Secrets Manager <i>∰</i> Admin Console <i>∰</i> Toggle Width 	 Folders No folder Collections Default colle Default colle Trash 				

commutateur-de-produit

3. Navigate to your organization's **Settings** → **Organization info** screen and select the **View API key** button. You will be asked to re-enter your master password in order to access your API key information.

Secure and trusted open source password manager for business

D bit warden



Informations sur l'API de l'organisation

4. Return to the Microsoft Sentinel tab. On the **Configuration** page, complete the following fields:

Field	Value
Bitwarden Identity URL	For Bitwarden cloud users, the default URL will be https://identity.bitwarden.com or https://identity.bitwarden.eu. For self-hosted Bitwarden users, input your self-hosted URL. For example, https:// <self-hosted-url>/i dentity. Be sure that the URL does not include any trailing forward slashes at the end of the URL "/".</self-hosted-url>
Bitwarden API URL	For Bitwarden cloud users, the default URL will be https://api.bitwarden.com or https://api.bitwarden.eu. For self-hosted Bitwarden users, input your self-hosted URL. For example, https:// <self-hosted-url>/a pi. Be sure that the URL does not include any trailing forward slashes at the end of the URL "/".</self-hosted-url>
Client ID	Input the value for client_id from the Bitwarden organization API key window.
Client Secret	Input the value for client_secret from the Bitwarden organization API key window.

Select **Connect** once the required fields have been completed.

(i) Note

Les informations de votre clé API de l'organisation sont des données sensibles. Ne partagez pas ces valeurs dans des endroits non sécurisés.

Start monitoring event logs

(i) Note

Historic event data is not available for the Bitwarden Event Logs app on Microsoft Sentinel at this time. Additionally, it may take up to 1 hour for the first events to appear in Microsoft Sentinel.

Bitwarden organization event logs can be viewed in Microsoft Sentinel using the **BitwardenEventLogs** query function.

- 1. From Microsoft Sentinel, select Logs. A New Query tab will be created. On the left hand navigation, select Functions → Workspace functions → BitwardenEventLogs.
- 2. Before running the query, you may select time frame and add specific parameters to the query. To being the query, select Run.



Queries can be saved for future use.

<pre>Water definition of the set of the set</pre>	Mission & Continui										• • • • · · ·	
<pre>Multiple Set Description Set Description</pre>	Microsoft Sentinel											
	Selected workspace: 'bitwarden'	Logs										
ard arg	Search X «	- New Owen 11									Save > th Share >	1 85 0
Autor Autor	General	P New Query I										
Windows Participation Participation Participation Part	Constant (Decident)	E P Run Time range : I	ast 7 days Limit : 100	D							[KQL mod
very constraints very	Overview (Preview)	BitwardenEventLogs										
in style	Logs	{ f ₀ }										
> Janding - Janding <t< td=""><td>Rews & guides</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Rews & guides	•										
Markandandandandandandandandandandandandanda	Disearch											
in ordinal with with with with with with with with	Inreat management											
Monting Partial Cart Reinded Autorige Au	Incidents											
Maring Indicator Rendo group actingUserial devices lpdddess Type devices eventTypeAtame actingUserial devices lpdddess Type devices eventTypeAtame actingUserial devices lpddess Type devices eventTypeAtame actingUserial actingUserial devices lpddess Type devices eventTypeAtame actingUserial actingUseria actingUseria actingUseria <td>Workbooks</td> <td>Results Chart 🗵 Add b</td> <td></td>	Workbooks	Results Chart 🗵 Add b										
Notices 0 100/2020, 1413.4313 M 402 9 Biteraidenferentiage, CL Onome Browser Orea, Updated 0 Instruction 0 00/2020, 1413.4313 M 100 0 <t< td=""><td>Hunting</td><td>☐ TimeGenerated [UTC] ↑↓</td><td>eventType</td><td>itemId</td><td>groupId</td><td>actingUserId</td><td>device</td><td>ipAddress</td><td>Type</td><td>deviceName</td><td>eventTypeName</td><td>ar</td></t<>	Hunting	☐ TimeGenerated [UTC] ↑↓	eventType	itemId	groupId	actingUserId	device	ipAddress	Type	deviceName	eventTypeName	ar
Inity Entry E	Notebooks	> 10/9/2024, 1:41:34.313 PM	1402				9		BitwardenEventLogs_CL	Chrome Browser	Group_Deleted	
Intelligence > > 0007002,14112769 M 1007 0007005,0000000000000000000000000000000	Entity behavior	> 10/9/2024, 1:41:30.397 PM	1401		100 C 10	1 H H H H	9		BitwardenEventLogs_CL	Chrome Browser	Group_Updated	
MIRAC / Prefered > 100/0020, 14111468 PM 101 - 9 Binard entropy, CL, Clonose Browser Cpher, Lipdated < SOC opinizion	Threat intelligence	> 10/9/2024, 1:41:12.765 PM	1107				9	1 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A	BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
⁰ 000000000000000000000000000	MITRE ATT&CK (Preview)	D > 10/9/2024, 1:41:11.466 PM	1101				9		BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
Image:	SOC optimization	D > 10/9/2024, 1:41:08.698 PM	1107				9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
0 (mmt hu) > 100/2024, 12.58.48.8.8.1 M 101 - 9 Bitmaid/SectorgC. Othore Browser OpherLipdated A lepolibility (Precised) > 100/2024, 12.58.68.379 M 1007 100 9 Bitmaid/SectorgC. Othore Browser OpherLipdated Community > 100/2024, 12.58.68.379 M 1007 100 9 Bitmaid/SectorgC. Othore Browser OpherLipdated Community > 100/2024, 12.58.68.379 M 107 100 9 Bitmaid/SectorgC. Othore Browser OpherLipdated Community > 100/2024, 12.58.59.328 PM 107 100 9 Bitmaid/SectorgC. Othore Browser OpherLipdated Voltage manager > 100/2024, 12.58.59.328 PM 107 100 9 Bitmaid/SectorgC. Othore Browser OpherLipdated Use connectors - <	Content management	> 10/9/2024, 1:40:37.288 PM	1000				9		BitwardenEventLogs_CL	Chrome Browser	User_LoggedIn	
b polycickie (phywier) > 0 (bdyc2/24, 1258 46.87) M 107 9 Bhauddhertudga_CL Chone Browser Cyber_Clent/Veed b Community > > 0 (bdyc2/24, 1258 46.87) M 1007 9 Bhauddhertudga_CL Chone Browser Cyber_Clent/Veed b S Community > > 0 (bdyc2/24, 1258 46.87) M 1007 9 Bhauddhertudga_CL Chone Browser Cyber_Clent/Veed W property > 10 (bdyc2/24, 1258 57.232 PM 107 9 Bhauddhertudga_CL Chone Browser Cyber_Clent/Veed W property > 10 (bdyc2/24, 1258 57.232 PM 107 9 Bhauddhertudga_CL Chone Browser Cyber_Clent/Veed B Lat connectors > 10 Adormation > 10 Adormation -	Content hub	> 10/8/2024, 12:58:48.814 PM	1101				9		BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
0. mmuny	Repositories (Preview)	> 10/8/2024, 12:58:45.879 PM	1107				9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
Configuration DisplayZay, Zas Sassa / M Tot/ DisplayZay DisplayZay <thdisplayzay< th=""> <thdisplayzay< th=""> <</thdisplayzay<></thdisplayzay<>	Community	> 10/8/2024, 12:56:02.933 PM	1101			11 A A A A A A A A A A A A A A A A A A	9	-	BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
Wetersday Seminary material Seminary material Seminary material Seminary material Wetersday Automation Seminary material Seminary material Seminary material Seminary material Seminary material	Configuration	> 10/8/2024, 12:55:59:947 PM	1107	- 22.			9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	- 7
Prevent Import Analytics Summary Reprevent Machine Automation Startings	Workspace manager	0101012024, 12-00-07-202 PM	1107				ø		bitwardenEventEugs_CC	Childine browser	cipitel_citettettewed	
In Date connectors Analytics Analytics Summary July Browkew) Matchinst Andonetion Automation Settings	(Preview)											
Analysis Summary rules (Brivens) Summary rules (Brivens) Analysis Analysis Analysis	Data connectors											
Summar Julis (Preview) Watchist Automation Settings	 Analytics 											
Wachist Autoration S settings	Summary rules (Preview)											
Automation O settings	Watchlist											
Q Settings	3 Automation											
	Settings											

Microsoft Sentinel query result

Monitor using Workbooks

Workbooks can be used to review event logs and visualize data. Additionally, templates are included in the Bitwarden Event Logs Workbook for a pre-configured overview of available data.

To access Workbooks, select **Workbooks** from the navigation and then **Templates**.

Home > Microsoft Sentinel

♀ Search × «	🖒 Refresh 🕂 Add	Workbook 🛛 🛜 Guid	es & Feedback				
✓ General	A O	<i>a</i> 2	0	More content at			
Overview	My workbooks	Templates	Updates	Content hub			
₽ Logs							
🜰 News & guides	My workbooks Ter	nplates				🧹 Bitwarden Orga	nization Events
🔎 Search	🔎 Search		√ Add filter			<u> </u>	
 Threat management 	Name			Status	Source name		
Incidents				Status	Source nume	Description This workbook provides	insights on Bitwarden Organizations
🞽 Workbooks	Bitwarden Authen	tication Events			Bitwarden	Event Logs.	
🔶 Hunting	Bitwarden Organiz	ation Events			Bitwarden	Content source (i) Bitwarden	Template version
Notebooks	Bitwarden Vault Ite	ems Events			Bitwarden	bitwarden	1.0.0
🧬 Entity behavior						Author Bitwarden	Supported by Bitwarden Inc Email
Threat intelligence							
MITRE ATT&CK (Preview)							
SOC optimization (Preview)							
✓ Content management							

Workbook templates

The Bitwarden Event Logs app will have three templates included by default. Select one of the templates and choose **View Template** to begin monitoring data.

My workbo	oks Templates			
🔎 Search		√ Add filter		
Name			Status	Source name
Bitwar	den Authentication Events			Bitwarden
Bitwar	den Organization Events			Bitwarden
Bitwar	den Vault Items Events			Bitwarden

Included templates

The dashboards include visualized data:



Time: Last 14 days ∨ Successful Log In Attempts by Country



Polan 2 1



Microsoft Sentinel dashboard view

Continue scrolling the overview page for additional event log data:

Top Users By: User Name ∨





Latest Authentication Events

3

TimeGenerated	↑↓ eventType↑↓	itemId ↑↓ collectionId	↑↓ groupld ↑↓	policyId ↑↓	memberld↑↓	actingUserId	↑↓ installationId	↑↓ device↑↓	ipA ↑↓	Tenantid	i -
5/19/2024, 11:36:30.951 PM	1006	5				A REPORT OF A R		2		10.0	
5/19/2024, 11:36:16.556 PM	1006	5						2		10.0	
5/16/2024, 2:03:05.447 PM	1000)						9		10.0	
5/16/2024, 2:03:55.748 PM	1005	5						9		10.0	
5/16/2024, 6:00:29.614 PM	1000)				A REAL PROPERTY.		9		10.0	1.10
5/17/2024, 9:11:59.709 PM	1005	5				The second second		1		10.0	1.10
5/21/2024, 9:34:05.581 PM	1000)				The second second		2			

Bitwarden even log view