# Votiro SaaS Knowledge Base



March 2025



### **Copyright Notice**

The material herein is proprietary to Votiro CyberSec Ltd. This document is for informative purposes. Any unauthorized reproduction, use or disclosure of any part of this document is strictly prohibited.

Votiro CyberSec's name and logos are trademarks of Votiro CyberSec Ltd., its subsidiaries or affiliates. All other company or product names are the trademarks of their respective holders.

www.votiro.com

### Contents

1 H	ow to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit	4
1.	1 Prerequisites	4
1.	2 Procedure	. 4
2 H	ow to Integrate SIEM with Azure Sentinel	12
2.	1 System prerequisites	12
2.	2 Procedure	.12
	2.2.1 Manual/Offline Deployment	12
3 H	ow to Send Files to Votiro via Postman	.24
3.	1 Prerequisites	24
3.	2 Procedure	.24
	3.2.1 Generating a Service Token	24
	3.2.2 Postman Setup	28
4 H	ow to Use Kibana to Troubleshoot Votiro Incidents	.35
4.	1 Example of Votiro Incident	35
4.	2 Procedure	.35
	4.2.1 Create and Configure an Index Pattern	35
4.	3 Analyze the Data	.37
	4.3.1 Discover	38
	4.3.2 Votiro Explore Incident & File Info	42
	4.3.3 File Sanitization Analysis	.42
5 N	ISSP User Guide	.45
<b>5 №</b> 5.	ISSP User Guide	. <b>45</b> .45
<b>5 №</b> 5. 5.	ISSP User Guide 1 MSSP Tenant Management 2 Monitoring Tenant Activity	. <b>45</b> .45 .51
5 № 5. 5. 6 H	ISSP User Guide 1 MSSP Tenant Management 2 Monitoring Tenant Activity ow to Use QR Code Sanitization	. <b>45</b> .45 .51 . <b>53</b>
5 № 5. 5. 6 H 6.	ISSP User Guide 1 MSSP Tenant Management 2 Monitoring Tenant Activity ow to Use QR Code Sanitization 1 Disarm QR Codes behavior	. <b>45</b> .45 .51 . <b>53</b> .53

### 1 How to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit

In this tutorial, you'll learn how to integrate Azure AD single sign-on with Votiro using SAML Toolkit to enable users to log in to the Votiro Management console using their corporate credentials.

### **1.1 Prerequisites**

Ensure you have the following items:

- Azure AD subscription
- Azure AD SAML Toolkit enabled on the above-mentioned subscription

### **1.2 Procedure**

- 1. Sign in to the <u>Azure portal</u>.
- 2. Select Azure Active Directory.

■ Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)		D & Q & Ø &
All services			
All	Filter services		
Favorites			
Recents	I I I I I I I I I I I I I I I I I I I	<b>=</b> 💀 📀	$\leftrightarrow$
Categories	Azure Active Virtual Resource App Services	Storage SQL Cost	Virtual
General	Directory machines groups	accounts databases Management	networks
Compute	General (18)		
Networking			
Storage	All resources	( Recent	
Web	(\land) Management groups	📍 Subscriptions	
Mobile	(iii) Resource groups	💿 Cost Management + Billing	
Containers	Marketplace	B Help + support	
Databases			
Analytics	V Service Health	Templates	PREVIEW
AI + machine learning	Tags	<ol> <li>What's new</li> </ol>	
Internet of Things	🚀 Quickstart Center	Shared dashboards	
Mixed reality	Free services	Reservations	
Integration			
Identity	Resource Explorer	Preview features	PREVIEW

3. In the left pane, select **Enterprise applications**.

	𝒫 Search resources, ser	vices, and docs (G+/)				$\sum$	Ģ	Q	۲	?	ନ୍ଦି
All services >											
Votiro   Overview     Azure Active Directory											
Overview	+ Add 🗸 🛞 M	anage tenants 🛛 What's new 🛛 💀 Pre	view features	🖗 Got feedba	ick? 🗸						
Preview features	<u>Microsoft Entra</u>	has a simpler, integrated experience for manage	ging all your	Identity and Access M	anagement needs. Try the new N	licrosoft E	intra ac	lmin ce	nter! 🛛		
X Diagnose and solve problems	Overview Monit	oring Properties Recommendations	Tutoria	ls							
Manage											
L Users	Search your ten	ant									
A Groups	Basic information										
External Identities											
& Roles and administrators	Name	Votiro		Users	307						
Administrative units	Tenant ID	a66f051a-cd66-4949-bf39-a108012d45ee	D	Groups	215						
🚸 Delegated admin partners	Primary domain	votiro.com		Applications	59						
Enterprise applications	License	Azure AD Free		Devices	153						
Devices											
App registrations	Alerts										
Identity Governance	•	met t									
Application proxy	Organizati	ons that use named locations in	A	Please migrate from I	Ver deprecation MFA Server to Azure AD Multi-						
<ul> <li>Custom security attributes (Preview)</li> </ul>	Conditiona action as s impact.	I Access or Identity Protection must take oon as possible to avoid any service		Factor Authentication any service impact.	by September 2024 to avoid						
🔓 Licenses 👻		. 13		Loom more 78							

#### 4. Select **New application**:

	P Search resources, services, and docs (G+/)	0
All services > Votiro   Enterprise applic	cations > Enterprise applications	
Enterprise applicat	tions   All applications	×
Overview	< 🕂 New application 🕐 Refresh 🛓 Download (Export) 🛛 Preview info 🛛 🎫 Columns 🛛 🖼 Preview features 🛛 🖗 Got feedback?	*
0 Overview	View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.	
🗙 Diagnose and solve problems	The list of applications that are maintained by your organization are in application registrations.	
Manage	ρ Search by application name or object ID Application type == Enterprise Applications × Application ID starts with × + Add filters	
All applications	163 applications found	
Application proxy	Name ↑↓ Object ID Application ID Homepage URL Created on ↑↓ Certificate Expiry Status	
User settings	bob 0088066F-0fe0-4e53-bfb8-d2950 48199d7F-1426-4b4e-a27F-af52 https://app.hibob.com/ 4/14/2022 -	
🕮 App launchers	∑ VT SSO 02e285ab-8c85-45ca-9a58-c6a 9e947dbb-29fb-4b8b-9812-b3 https://www.virustotal.com/ 2/9/2023 -	
Custom authentication	Stack         072bca59-64d3-46e9-be72-196         da2e137b-c136-411b-85f1-be97         -	
extensions (Preview)	<b>20</b> Zoom 089fffb8-14c5-4937-9f14-9b087 fc108d3f-543d-4374-bbff-c7c5 https://zoom.us 11/25/2019 -	
Security	M         monday.com         0c2eaf5a=c75e=457c-98a25-944838fa0b1d=4df6-463a-bf67-1a6fhttps://monday.com         11/11/2021         -	
🍨 Conditional Access	AS Assembla 0d209699-faac-44bc-9782-ec71 a5edd250-fb41-453e-9912-978 https://account.activedirectory	
Consent and permissions	12/15/2022 -	
Activity	Metup 0/aa5c10-f792-4d1a-b52f-2337 a1cf9e0a-fe14-487c-beb9-dd33	
∋ Sign-in logs	Log in using Office 365 0fbb48bb-c678-4857-b38b-1b9 5cd6e32d-de3f-4cb5-a322-ea0 https://cloud-protect.net 3/17/2020 -	
🕍 Usage & insights	SL Slack 118b4f5f-f569-4291-ba64-86be 8c3b7662-a040-4180-89c1-57f https://*.slack.com/sso/sami?m 2/11/2020 -	
Audit logs	2         Cirrus Insight         135286d4-83a2-4cl3-b0bc-2618/508648-bb9e-4l57-ae86-fd6fhttp://www.cirrusinsight.com         -	

5. In the search field type **Azure AD SAML Toolkit**.

# Browse Azure AD Gallery



- 6. Lastly, select it from the results and add it. After a few moments, the app will be added to your tenant.
- 7. Navigate back to **Enterprise applications | All applications** and select the newly added app: **Azure AD SAML Toolkit**.
- 8. On the left pane, select **Single sign-on**.
- 9. On the **Basic SAML Configuration** page, click the pencil button to edit the configuration.



- 10. For Identifier (Entity ID), leave as default https://samltoolkit.azurewebsites.net.
- 11. Both Reply URL (Assertion Consumer Service URL) and Sign on URL should be in the following format: <u>https://<VOTIRO-FQDN>/assertionconsumerservice</u>.

#### Note:

If you're configuring SAML for SaaS cluster, please make sure to include the tenant id after the Reply URL and Sign on URL:

https://<VOTIRO-FQDN>/assertionconsumerservice/<TENANT\_ID>

12. Other fields are optional and will remain blank, lastly press the Save button.

 $\times$ 

Identifier (Entity ID) * 🙃		
The default identifier will be the audience of the SAML response for IDP-initiated SSO		
	Default	
https://camito.all/it.com/couchaitas.pst		T
Add identifier	✓ ∪	
Patterns: https://samltoolkit.azurewebsites.net		
Reply URL (Assertion Consumer Service URL) * 🕕		
The default reply URL will be the destination in the SAML response for IDP-initiated SSO		
	Default	
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice,	/e54e1298-78 🔽 🛈	Ĺ
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice,	/e54e1298-78	ĺ
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https://terreservice Add reply URL	Default /e54e1298-78 🗹 🛈	ĺ
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https:// <b>immenne</b> /assertionconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume	Default /e54e1298-78 🗹 🛈	ĺ
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https:// <b>termenerg</b> /assertionconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume	Default /e54e1298-78 <table-cell> 🛈</table-cell>	ĺ
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https://termenergassertionconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume Sign on URL * ①	Default /e54e1298-78 🗹 🛈	
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https://tereserviceassertionconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume Sign on URL * ① https://tereserviceassertionconsumerservice	Default /e54e1298-78 🗹 🛈	
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https://ieuteneutrationconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume Sign on URL * ① https://ieuteneutrationconsumerservice Patterns: https://samltoolkit.azurewebsites.net/	Default /e54e1298-78 <table-cell> 🕐</table-cell>	
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice https://ternerge/assertionconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume Sign on URL * () https://ternerge/assertionconsumerservice Patterns: https://samltoolkit.azurewebsites.net/	Default /e54e1298-78 <table-cell> 🕐</table-cell>	
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice, https://tensetum/assertionconsumerservice Add reply URL Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume Sign on URL * ① https://tensetum/assertionconsumerservice Patterns: https://samltoolkit.azurewebsites.net/ Relay State (Optional) ①	Default /e54e1298-78 🗹 🛈	

- 13. On the **Attributes & Claims** section, click the pencil button to edit the configuration.
- 14. Select Add a group claim on the left-hand side, choose All groups, expand Advanced options, select Customize the name of the group claim, and provide it with a name, for instance, "AzureGroup1", then press the Save button. Also create a group with that name if you choose to use "AzureGroup1" and copy it's objectID to the Votiro UI.



Group Claims Manage the group claims used by Azu	ire AD to populate SAML tokens issued to your app	
🕜 This page includes previews availa	ble for your evaluation in the 'Advanced options' section.	
Which groups associated with the us	er should be returned in the claim?	
○ None		
<ul> <li>All groups</li> </ul>		
<ul> <li>Security groups</li> </ul>		
<ul> <li>Directory roles</li> </ul>		
Groups assigned to the appl	ication	
Source attribute *		
Group ID		
Filter groups (Preview) Attribute to match		
		$\sim$
Match with		
		$\sim$
String		
✓ Customize the name o	f the group claim	
Name (required)		
AzureGroup1		
Namespace (optional)		
Emit groups as re	ole claims (i)	
Apply regex repla	ace to groups claim content (Preview)	



 To avoid issues such as "User without any role", make sure the users that should have access to the environment via SAML are listed under Azure AD SAML Toolkit | Users and groups.

Microsoft Azure	ی Search	resources, services, and docs (G+/)	E 6
Home > Home > Enterprise applica	tions > Azure AD SAML Toolkit		
Azure AD SAML To	olkit   Users and groups		
«	🛛 🕂 Add user/group 🖉 Edit 🔋 Remove 🖉 Update Credentials 🛛 🎫 Columns 🗎 🧖 Got feedbac	12	
Cverview	1 The application will appear for assigned users within My Apps. Set 'visible to users' to no in properties to prevent this.	→	
Deployment Plan	•		
Manage	P First 200 shown, to search all users & groups, enter a display name.		
Properties	Display Name	Object Type	Role assigned
A Owners		User	Default Access
& Roles and administra	🗆 🥶 🚥	Uter	Default Access
A Users and groups		User	Default Access
Single sign-on	- 💿 📥	User	Default Access
Provisioning	🗆 😡 💼	User	Default Access
😔 Self-service	🗆 🤒 💼	User	Default Access
<ul> <li>Custom security attributes (preview)</li> </ul>	- 😼 🚥	User	Default Access

16. Log in to Votiro's Management console. On the left pane, click on the cogwheel, and select **SAML**. For the IDP Metadata address, copy and paste the value from the **App Federation Metadata Url** field in Azure.

≡ Microsoft Azure	≫ Search resources, services, and docs (G+/)	
Home > Enterprise applications   All ap	plications > Azure AD SAML Toolkit - AWS TEST >	
Azure AD SAML Toolkit Enterprise Application	- AWS TEST   SAML-based Sign-on	
«	<ul> <li>↑ Upload metadata file</li> <li>&gt; Change single sign-on mode</li> <li>Image: Test this application</li> <li>&gt; Read the configuration guide </li> <li>&gt; for help integrating Azure AD SAML Toolkit - AWS TEST.</li> </ul>	
Deployment Plan	Basic SAML Configuration	
III Properties	Identifier (Entity ID) https://samltoolkit.azurewebsites.net.beta Reply URL (Assertion Consumer Service URL) https://prod.us.paralus.votiro.com/assertionconsumerse	
<ul> <li>Owners</li> <li>Roles and administrators</li> </ul>	Sign on URL https://prod.us.paralus.votiro.com/assertionconsumerse rvice/ Relay State (Optional) Optional	
<ul> <li>Single sign-on</li> </ul>	Logout Url (Optional) Optional	
<ul> <li>Provisioning</li> <li>Self-centice</li> </ul>	2 Attributes & Claims	
<ul> <li>Custom security attributes (preview)</li> </ul>	givenname user.givenname sumame user.sumame emailaddress user.mail	
Security	name user.userprincipalname AzureGroup1 user.groups Unique User Identifier user.useronicriaalname	
<ul> <li>Conditional Access</li> <li>Permissions</li> <li>Token encryption</li> </ul>	SAML Certificates	
Activity	Token signing certificate Status Active	
<ul> <li>Sign-in logs</li> <li>Usage &amp; insights</li> </ul>	Thumbprint Expiration 5/2/2025, 8:25:10 AM Notification Email	
<ul> <li>Audit logs</li> <li>Provisioning logs</li> </ul>	App Federation Metadata Url     https://login.microsoftonline.com/ca604247-726       Certificate (Base64)     Download       Certificate (Raw)     Download	
Second technology + Support	Federation Metadata XML Download	
<ul> <li>Virtual assistant (Preview)</li> </ul>	Verification certificates (optional) (Preview)        Required     No       Active     0       Expired     0	

17. For the Issuer, copy and paste <u>https://samltoolkit.azurewebsites.net</u> from the **Basic SAML Configuration** you configured above.



- 18. For the SAML Username identifier, leave by default: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
- 19. The Admin role key should be the value you provided for the group above in **Group Claims**, in this case, AzureGroup1.
- 20. The Admin role value should be the Object Id of the group in which the admin's users are members.

Home > Constants Groups >			
i admins ጵ … <sub>Group</sub>			
«	📋 Delete 🛛 📯 Got feedback?		
<ul> <li>Overview</li> </ul>	a during		
🗙 Diagnose and solve problems	admins		
Manage			
Properties			Copy to clipboard
🐣 Members	Membership type	Assigned	
🚨 Owners	Source	Cloud	
🔓 Roles and administrators	Turne	Security	₽.
Administrative units	type	Security	U.
🔅 Group memberships	Object Id	1feef5b7-feinenninkersen and the second	
Applications	Creation date	7/6/2021, 5:07:22 AM	a l
🔓 Licenses			
📍 Azure role assignments	Direct members		
Activity	🕀 4 Total 🛛 🔒 4 User(s)	A Group(s) 🛛 🔤 O Device(s)	0 Other(s)
≆ Access reviews		0	<b>T</b> . 1
Audit logs	Group membersnips	Owners	Iotal members
👶 Bulk operation results	<b>™</b> 0	<b>a</b> 0	<b>(2)</b> 4
Troubleshooting + Support			
New support request			

21. Press the **Save changes** button, log out from the Management console and log in with the corporate credentials. You may continue and set up the Help Desk and SOC groups, similar to what was configured for the admins group.

### 2 How to Integrate SIEM with Azure Sentinel

In this tutorial, you'll learn how to integrate SIEM with Azure Sentinel using **Votiro Solution for Microsoft Sentinel**. **Votiro Solution for Microsoft Sentinel** is a collection of Data Connectors, Parser, Workbook and Analytic Rules that are used together to analyze data.

### 2.1 System prerequisites

Ensure you have the following:

- Linux machine with at least 4 CPU cores and 8 GB RAM
- Python 2.7 or 3 installed on the Linux machine
- Rsyslog: v8/Syslog-ng: 2.1 3.22.1
- Syslog RFC 3164/5424
- Download and unpack the file: Votiro-Offline.zip

### 2.2 Procedure

#### 2.2.1 Manual/Offline Deployment

To test the solution before publishing, follow the below steps.

#### **Deploy CEF Data Connector on Forwarder Machine**

- 1. Sign in to the <u>Azure portal</u>.
- 2. Search for Microsoft Sentinel.

	∠ Sentinel	×	≥ ¢ (	3 0 R	XXXX @votiro.co 🧶
Azure services	All Services (1) Marketplace (31)	✓ More (4)			<u>^</u>
+ 👌	Services		squ	$\rightarrow$	
Create a Microsoft	Entra Olicrosoft Sentinel		Storage SQL databases M	ore services	
resource ID	Marketplace	See more	accounts		
	🐴 Azure Sentinel	_			
Resources	🐴 Microsoft Defender for Endpoint	_			
Recent Favorite	Snowflake	_			
Name	aws IAM	_	Last Vieward		
TANTIS.	Documentation	See more	Last Frenca		
	Hybrid security monitoring with Microsoft Sentinel -	Azure Architecture Center 🛛 🖻			
	Entity pages in Microsoft Sentinel	ď			
	Create new watchlists - Microsoft Sentinel	c"			
	Visualize collected data	C <sup>1</sup>			
	Continue searching in Microsoft Entra ID				
Navigate	Searching all subscriptions.	R <sup>2</sup> Give feedback			
<b>†</b> Subscriptions	Resource groups	All resources	Zh Dashboard		

3. Select Microsoft Sentinel from Services.

Microsoft Azure			E				XXXX@votire VOTIRO (VOTIR	р.со 🧧
Home >								
Microsoft Sentinel 🖈 …								×
+ Create 🛞 Manage view 🗸 🖒 Refresh	🛓 Export to CSV 🛛 😵 Open query 📔 🖻 View incidents							
Filter for any field Subscription equ	als all Resource group equals all $ imes$ Location equals all $ imes$	+ <sub>♥</sub> Add filter						
Showing 0 to 0 of 0 records.				No gro	ouping		✓ III List view	$\sim$
Name 14	Resource group ↑↓	Location ↑↓	Subscription ↑↓			Dire	ctory ↑↓	
	<b>No Microsoft</b> See and stop threats before they cause harm, with SII birds-eye view	Sentinel to display EM reinvented for a modern world. It across the enterprise.	vlicrosoft Sentinel is your					
	Create M	licrosoft Sentinel						
		-2						

4. Press + Create or Create Microsoft Sentinel to add Microsoft Sentinel to a Workspace::

Microsoft Azure		D 0 0 R	XXXX @votiro.co Votiro (votiro.com)
Home > Microsoft Sentinel >			
Add Microsoft Sentinel to a	workspace		:
+ Create a new workspace () Refresh			
Microsoft Sentinel offers a 31-day free trial. See Micro	soft Sentinel pricing for more details.		
Plan human			
Filter by name			
	No workspaces found		
	Create a new workspace		
Add Cancel			

5. Press + Create a new workspace:

Give feedback

Home > Microsoft Sentinel > Add M	licrosoft Sentinel to a workspace >								
Create Log Analytics workspace									
Basics Tags Review + Create									
A Log Analytics workspace is the backspace	asic management unit of Azure Monitor Logs. There are specific	considerations ×							
you should take when creating a ne	ew Log Analytics workspace. Learn more								
With Azure Monitor Logs you can easily	store retain and guery data collected from your menitors	od recourses in Azure							
and other environments for valuable in	sights. A Log Analytics workspace is the logical storage unit	where your log data							
is collected and stored.									
Project details									
Select the subscription to manage depl	oyed resources and costs. Use resource groups like folders	to organize and							
manage all your resources.									
Subscription * ①	Enterprise Dev/Test	~							
Resource group * ①		~							
	Create new								
Instance details									
Name * 🕕									
Region * 🕕	East US	$\sim$							
	L								

6. Create a new **Resource Group** if it does not exist yet. Then create a new machine with the system requirements mentioned above → via Resource Group > Create > select Virtual Machine (Ubuntu 22.06 server is recommended):

Home > Microsoft Sentinel >			
Microsoft Sentinel « Votiro (votiro.com)	Sentinel-Test 🖈 🕏	ξ ···	
+ Create  🛞 Manage view 🗸 …		🕂 Create 🔞 Manage view 🗸 📋 Delete resource group 💍 Refresh 🞍 Export to CSV 😤 Op	en query   🛛
Filter for any field	Overview		
Name 14	Activity log	Subscription (move) : Votiro - CSP	
Sentinal-Tect	Access control (IAM)	Subscription ID : 240d6f29-e1ab-4c5b-b28a-e62883cb41a9	
• Senare rea	🔷 Tags	Tags (edit) : Add tags	
	🔥 Resource visualizer		
	🗲 Events	Resources Recommendations (1)	
	Settings	Filter for any field Type equals all X Location equals all X <sup>+</sup> 7 Add filter	
	Deployments	Showing 1 to 12 of 12 records.	
	Security	□ Name ↑↓	Type ↑↓
	Deployment stacks		Azure Workboo
	Policies		Azure Workboo
	Properties	Security/insights/sentinel-test)	Solution
	🔒 Locks	Sentinel-logforwarder	Virtual machine

 Select the created workspace, then go to Content Hub > Select Common Event Format (CEF) and install it:

Home & Microsoft Section & Microsoft Section	ool.										
Microsoft Sentinel «	Microsoft Sentinel	Content hub									
🕂 Create ( Manage view 🗸 \cdots		🕐 Refresh 👃 install/Update 👔 Delete 🖉 Guides & Feedback									
	General	- 242	272	<b>0</b> 1	<u>^</u> 0						
Name 1.	Overview (Preview)	Solutions Si	andalone contents	Installed	Updates						
🔋 Sentinel-Test	🧬 Logs										
	News & guides	cet		Status : All Content	type : All	Support : All P	rovider : All Cat	egory : All Conte	ent sources : All		
	🔎 Search										
	Threat management	Content title		Status		Content source	Provider	Support	Category		
	Incidents	📃 💿 Akamai Security				Solution	Akamai	Microsoft	Security - Cloud Security		
	Workbooks	Azure Cloud NG	FW By Palo Alto Net			Solution	Palo Alto Netw	Microsoft	Security - Automation (SCAR), Securit		
	Notebooks										
	Entity behavior	Common Event	format	Installed		Solution	Microsoft	Microsoft	IT Operations		
	Threat intelligence	Cortex XDR Data	Connector			Solution	DEFEND Ltd.	DEFEND Ltd.	Security - Threat Protection		
	MITRE ATT&CK (Preview)	CyberArk Enterp	rise Password Vault (			Solution	Gyberark	Cyberark	identity		
	Content management	Defetrare				Colution	Darktraza	Davistrana	Security - Threat Protection		
	Content hub					2010/001	Carkende	Carkberre	accurry - milder Protection		
	Repositories (Preview)	📃 💧 Dev-0530 File Ext	tension Rename			Standalone		Community	Security - Others		
	Community	F5 Advanced WA	F Integration via Sy			Solution	F5 Networks		Security - Network		

8. Once installed, go to your workspace > Data Connectors > Open Connector Page:



9. Follow the instructions in 1.2 below, Install the CEF collector on the Linux machine:



10. Verify that you have Python 2.7 or Python 3 installed on the Linux machine by running:

python --version or python3 --version

11. Copy the command below:

```
sudo wget -O cef_installer.py
https://raw.githubusercontent.com/Azure/Azure-
Sentinel/master/DataConnectors/CEF/cef_installer.py&&sudo
python cef_installer.py [WorkspaceID] [Workspace Primary
Key]
```

Note: You must have the GNU Wget package installed on the Linux machine.

- 12. Paste the command into the command line on your log forwarder, and replace [WorkspaceID] and [Workspace Primary Key] with their values.
- 13. Run the command. This installs the CEF connector and Log Analytics Agent on the forwarder machine. Once done, the connector is now listening to events on TCP port 514.
- 14. Verify that the port used is indeed opened via the Virtual Machine's Network settings:

Sentinel-logforwar	r <b>der</b> ∣Network settings										
🔎 Search 🤍	This is a new experience. <u>Elease provide feedback</u>										
Overview	🖉 Attach network interface 🖉 Detach network interface 🌲 View topology 🤰 Troubleshoot 🗡 🖒 Refresh 👰 Dive feedback										
Activity log											
Access control (IAM)	Rebook interface / IP configuration										
🔹 Tags											
* Diagnose and solve problems	∧ Essentials										
Connect	Network interface : sentinel-logforwarder616_z1	Load balancers : 0 (Configure)									
Ø Connect	Virtual network / subnet : Sentinel-logforwarder-vnet / default	Application security groups : 0 (Configure)									
× Bastion	Public IP address : Sentinel-logforwarder-ip	Network security group : Sentinel-logforwarder-nsg									
Networking	Private IP address : 10.0.04	Accelerated networking : Disabled									
Network settings	Admin secunty rules : 0 (Contigure)	Effective security rules 1 0									
+ Load balancing	Rules \land Collapse all										
Application security groups											
Network manager	Vetwork security group Sentinel-logforwarder-nsg (attached to networkinterface sentinel-logforwarder616_z1)      Imports 0 schoets 1 network interfaces		+ Create port rule 🗸								
Settings	HIGHER & PRIVAL & HIGHER PHILIPLE										
Disks											
Extensions + applications	Source == an Unpersident == an Protocol == an Accor == an	Restant former Restantes									
Configuration	Phoney F Name Port	Protocol Source Destination	Action								
Advisor recommendations	Inbound port rules (5)										
tit Properties	300 🔺 SSH 22	TCP Any Any	🛛 Alow 🔋								
🔒 Locks	310 AllowAnyCustomS14Inbound 514	Any Any Any	🥥 Allow 🔋								

**Note**: In this case, we used TCP port 514 (default) and **Allow=any**, but the best practice is to use the TLS protocol with other ports used and restrict to specific IPs pointed to specific NAT gateways. For example, in prod.us:

Simp	le Queue Service 🛛 🔯 Elast	ic Kubernetes Service 🛛 🖓 VPC	🔍 Amazon Inspector 🛛 🧟	Systems Manager									
NAT	gateways (2) Info						0						
Q,	Q. Find resources by attribute or tog												
	Name 🛛	NAT gateway ID	♥ Connectivity.	v State		▼ Primary public I	▼ Primary private I						
0	ngw-prod-egress-01	nat-013cc592b4306c371	Public	⊘ Available	-	54.234.70.44	10.240.128.14						
0	ngw-prod-egress-02	nat-0f7ba826618ac4c93	Public	⊘ Available	-	34.237.77.26	10.240.129.207						

#### **Deploy Parser Function**

Follow the instructions to parse ingested data:

- Copy the function code from the downloaded package file: /Votiro-Offline/Parser/VotiroEvents.txt
- 2. On Microsoft Sentinel  $\rightarrow$  Go to your created Workspace -> Logs
- 3. Paste the content of VotiroEvents.txt in the area as shown below:

Microsoft Azure		P Search resources, services,	and docs (G+/)		×	<b>₽</b> 0	© 0 /	Zorel.Mishal@votiro.cor votiso.evotiso.cox
Home > Microsoft Sentinel > Microsoft Sentine								
Microsoft Sentinel « Votiro (votiro.com)	Microsoft Sentinel	Logs						
+ Create 💿 Manage view 🗸 …		🥐 New Query 1 🛛 🗧 🕂					💙 Feedt	ack 📰 Queries 🛛 🕲 🛄
Filter for any field	General	P Sentinel-Test	D Run Time range : Last 24 hours	la Save ∨ Le? Share ∨	+ New alert rule ~	→ Export	∨ 📌 Pint	io 🗸   📨 Format query 🚽
Name 10	Overview (Preview)	Tables Queries Functions ···· «						
Sentinel-Test	🕐 Logi							
	News & guides	₽ Search						
	🔎 Search	Fiter III Group by: Solution V						
	Threat management	F" Collapse all						
	Incidents	Favorites						,
	Workbooks	You can add favorites by clicking on the ☆ icon	Queries History					
	Hunting	▶ LogManagement						
	Notebooks	Microsoft Sentinel	CommonSecurityLog   where DeviceVendor == '	"Votiro" and DeviceProduct ==	"Votiro cloud"   parse	kv Additionall	ixtensions as (c	ompanyName:
	Entity behavior	<ul> <li>Workspace functions</li> </ul>	string, correlation/d:guid, item/d: guid, fileName	r: string, fileSize: int, password	Protected: bool, AVRes	It: string, Thre	atCount int, bi	ockedCount
	O Threat intelligence	f VotiroEvents	3/6/2024, 12:40 PM   33 results					
	MITRE ATT&CK (Preview)		CommonSecurityLog   where DeviceVendor == '	"Votiro" and DeviceProduct ==	"Votiro cloud"   parse	ky Additionall	ixtensions as (c	ompanyName:
	Content management		string, correlationid:guid, itemid: guid, fileName	r: string, fileSize: int, password	Protected: bool, AVRes	lt: string, Thre	atCount: int, bl	ockedCount Run
	Content hub		appy zoon, it zoo pain 10 results					

4. Then click on Save > Save as function. Enter the Function name as VotiroEvents and click on Save:

Function name *			
VotiroEvents			
Code			
dfgdfg			
Legacy category * VotiroEvents			
Parameters			
Туре	Name	Default value	
Select type	✓ Type name	Type default value	]
Select type	✓ Type name	Type default value	]

5. Try running the query to see the following type of results (adjust the time range according to data ingested):

Sentinel-Test    Sentinel-Test   Sentinel-Test   Image: Lest 7 days   Babes   Queries   Image: Lest 7 days   Stare V   Auber Cueries   Search   Filter   Group by Solut        Results   Chart   Add bookmark        Image: Lest 7 days   Stare V   Stare V   Collapse all   Format quere   Vou can add favorites by   Claining on the \$* icon   LogManagement   Microsoft Sentinel   VotiroEvents                    Prove Classification summary   VotiroEvents               VotiroEvents							V recuback		⇔ ∎
bits       Outries       I       VotiroEvents         Fibre:       Group by Solut         Form:       Group by Solut         Form:       Group by Solut         Fouries       Nou can add favorites by cicking on the % icon         Vou can add favorites by cicking on the % icon       Device/Vendor	st	Time rang	e: Last 7 days	🛛 🔚 Save 🗸 📝	Share $\vee$ + N	ew alert rule 🗸 🛛 🛏 Eq	port 🗸 📝 Pin to 🗸	📔 😇 Format qu	ery
Search     Firer     Group by Solid     For Group by Solid     Collapse all     For Start     Collapse all     For Start     Collapse all     Collapse all	es <b>«</b> 1	VotiroEvents							
File     File     For outp by Solut     For outp by Solut     Collapse all     Favorites     You can add favorites by     dicking on the % i con     LogManagement Microsoft Sentinel Workspace functions     / VotiroEvents     // VotiroEvent     //									
Prece         Output dy, sould           Collapse all Favorites         Results         Chart         Add bookmark:           Collapse all Globing on the 's' con LogManagement Microsoft Sentinel Workspace functions / VotiroEvents         DeviceVendor         DeviceVe	Group his Solut								
Collapse all         Favorites           Fororites         Nou can add favorites by clicking on the 'k's icon CogManagement Microsoft Sentinel Workspace functions         Results         Chart         Reductore         Device/Pendant         Device/Pendant         Device/Vension         Device/Vension         Device/Vension         Metivity         LogSeverity           \u00ed Stanitization summary         3/2/024, 2043/0713 PM         Vetrico         Vetrico Coud         1.0.0.0         500         Sanitization summary         1           \u00ed > 2/29/2024, 100312.774 AM         Vetrico         Vetrico Coud         1.0.0.0         500         Sanitization summary         1           \u00ed > 2/29/2024, 10114/07.88 AM         Vetrico         Vetrico cloud         1.0.0.0         500         Sanitization summary         1           \u00ed > 2/29/2024, 10114/07.88 AM         Vetrico         Vetrico cloud         1.0.0.0         500         Sanitization summary         1           \u00ed > 2/29/2024, 1014/07.384 AM         Vetrico         Vetrico cloud         1.0.0.0         500         Sanitization summary         1           \u00ed > 2/29/2024, 1014/07.384 AM         Vetrico         Vetrico cloud         1.0.0.0         500         Sanitization summary         1           \u00ed > 2/29/2024, 1014/07.384 AM         Vetrico         Vet	croup by, solur								
Favorites         Results         Chart         Results         Device/Vendor         Device/Vendor <thdevice th="" vendor<="">         Device/Vendor         <thdev< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></thdev<></thdevice>									
Nou can dol fivorities by clicking on the fri con LogManagement Microsoft Stanlard Workspace functions         Results         Chart         Device/Workspace         Device/Workspace <thdevice th="" workspace<="">         Device/Workspace<td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></thdevice>									
Calculary on the X room         TimeGenerated [UTC]         DeviceProduct         DeviceProduct <thdeviceproduct< th="">         DeviceProduct</thdeviceproduct<>	favorites by	Results Chart   🕅 Add b							
Lognal ageneric         > 3/2/2024, 20430/T3 PM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           Workspace functions         > 2/29/2024, 1033:12.724 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > Vorkspace functions         > 2/29/2024, 10190:12.724 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10119;147 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10119;147 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10119;147 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10119;17;88 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10119;72;82 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 1011;42;92 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary		TimeGenerated [UTC]	DeviceVendor	DeviceProduct	DeviceVersion	DeviceEventClassID	Activity	LogSeverity	FileHa
Image: Second Sections         > 2/29/2024, 10.03312.734 AM         Votiro         Votiro cloud         1.0.00         500         Sanitization summary         1           VotiroEvents         > 2/29/2024, 10.01.0376 AM         Votiro         Votiro cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.11.0376 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.11.0377 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.11.0377 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.11.0377 33 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.13477 33 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.13477 33 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10.13477 34 AM         Votiro         Votiro Cloud         1.0.00         500         Sanitization summary         1     <		> 3/3/2024, 2:04:30.713 PM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		fa274
Image: Name of the second se		> 2/29/2024, 10:03:12.734 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		fa274
> Votrockvents         > 2/29/2024, 1011:19.147 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 1011:19.147 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 1011:17.398 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 1011:47.398 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 1011:47.398 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 101:454.742 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 101:454.742 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 101:454.742 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 101:454.742 AM         Votro         Votro cloud         10.00         Solo         Sanitization summary         1           > 2/29/2024, 1024.1028.0124 A		> 2/29/2024, 10:10:40.876 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980d
> 2/29/2024, 10:11:47.788 AM       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:31:37.393 AM       Votiro       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:31:47.293 AM       Votiro       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:34:026 AM       Votiro       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:18:40:26 AM       Votiro       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:19:03:04 AM       Votiro       Votiro       Votiro       500       Sanitization summary       1         > 2/29/2024, 10:19:03:02 AM       Votiro       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:29:07 JAM       Votiro       Votiro       Votiro       10.00       500       Sanitization summary       1         > 2/29/2024, 10:24:10	vents	> 2/29/2024, 10:11:19.147 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980d
>         2/29/2024, 10.13/17.393 AM         Votiro         Votiro         10.00         500         Sanitization summary         1           >         2/29/2024, 10.13/47.393 AM         Votiro         Votiro         Votiro         500         Sanitization summary         1           >         2/29/2024, 10.13/47.393 AM         Votiro         Votiro         Votiro         500         Sanitization summary         1           >         2/29/2024, 10.13/40.266 AM         Votiro         Votiro         Votiro         10.00         500         Sanitization summary         1           >         2/29/2024, 10.18/40.066 AM         Votiro         Votiro         Votiro         10.00         500         Sanitization summary         1           >         2/29/2024, 10.18/40.066 AM         Votiro         Votiro         Votiro         10.00         500         Sanitization summary         1           >         2/29/2024, 10.19/20.211 AM         Votiro         Votiro         Votiro         Votiro         500         Sanitization summary         1           >         2/29/2024, 10.23/10.279 AM         Votiro         Votiro         10.00         500         Sanitization summary         1           >         2/29/2024, 10.24/10.24/10.24/10.24/10.24/10.24/10.24/10.2		> 2/29/2024, 10:11:47.788 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980d8
>         2/29/2024, 10:1545.742 AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:1849.026 AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:1849.026 AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:1903.034 AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:20:11 AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:23:10:279 AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:24:10:48 1AM         Votiro         Votiro cloud         1.0.0.0         500         Sanitization summary         1           >         2/29/2024, 10:24:10:2		> 2/29/2024, 10:13:17.393 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980d
> 2/29/2024, 10:18:49.026 AM         Votiro         Votiro         10.00         500         Sanitization summary         1           > 2/29/2024, 10:19:03.034 AM         Votiro         Votiro         Votiro         500         Sanitization summary         1           > 2/29/2024, 10:19:03.034 AM         Votiro         Votiro         Votiro         500         Sanitization summary         1           > 2/29/2024, 10:20:211 AM         Votiro         Votiro         Votiro         500         Sanitization summary         1           > 2/29/2024, 10:220:211 AM         Votiro         Votiro         Votiro         1.0.00         500         Sanitization summary         1           > 2/29/2024, 10:240:229:AM         Votiro         Votiro         Votiro         0.0.0         500         Sanitization summary         1           > 2/29/2024, 10:240:729:AM         Votiro         Votiro         Votiro         Sanitization summary         1           > 2/29/2024, 10:240:729:728 AM         Votiro         Votiro         Votiro         Votiro         Sanitization summary         1		> 2/29/2024, 10:15:45.742 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df79
>         2/29/2024, 10:1903.034 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           >         2/29/2024, 10:1903.034 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           >         2/29/2024, 10:1903.0279 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           >         2/29/2024, 10:24.1024 MM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           >         2/29/2024, 10:24.1024 MM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           >         2/29/2024, 10:257.792 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1		> 2/29/2024, 10:18:49.026 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df79
> 2/29/2024, 10:19:20:211 AM         Votiro         Votiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10:23:10:279 AM         Vetiro         Vetiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10:23:10:269 AM         Vetiro         Vetiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10:26:179 AM         Vetiro         Vetiro cloud         1.0.0         500         Sanitization summary         1           > 2/29/2024, 10:26:179 AM         Vetiro         Vetiro cloud         1.0.0         500         Sanitization summary         1		> 2/29/2024, 10:19:03.034 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df79
→         2/29/2024, 10:23:10:279 AM         Votiro         Votiro         Votiro         10.00         500         Sanitization summary         1           →         > 2/29/2024, 10:24:10:481 AM         Vetiro         Vetiro         Vetiro         500         Sanitization summary         1           →         > 2/29/2024, 10:24:10:481 AM         Vetiro         Vetiro         Vetiro         500         Sanitization summary         1           →         > 2/29/2024, 10:25:07.792 AM         Vetiro         Vetiro         Vetiro         500         Sanitization summary         1		> 2/29/2024, 10:19:20.211 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df79
→         2/29/2024, 10:24:10:481 AM         Votiro         Votiro         Local         500         Sanitization summary         1           →         > 2/29/2024 10:25:97.792 AM         Vetiro         Votiro doud         1.0.0.0         500         Sanitization summary         1		> 2/29/2024, 10:23:10.279 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df79
→ 2/29/2024.10:25:07.792 AM Votiro Votiro Cloud 1.0.0. 500 Sanitization summary 1		> 2/29/2024, 10:24:10.481 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df79
		> 2/29/2024, 10:25:07.792 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		38c97
2/29/2024, 10/26:14.751 AM Votiro Votiro doud 1.0.0.0 500 Sanitization summary 1		> 2/29/2024, 10:26:14.751 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		38c97
> 2/29/2024, 10:28:03:185 AM Votiro Votiro cloud 1.0.0.0 500 Sanitization summary 1		> 2/29/2024, 10:28:03.185 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		38c97

	3/3/2024, 2:04:30.713 PM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		fa2742
	Tenantid	6c0fa6d8-ec71-4593-8e	5f-45b4f7770685					
	TimeGenerated [UTC]	2024-03-03T14:04:30.71	3Z					
	DeviceVendor	Votiro						
	DeviceProduct	Votiro cloud						
	DeviceVersion	1.0.0.0						
	DeviceEventClassID	500						
	Activity	Sanitization summary						
	LogSeverity							
	FileHash	fa2742aec57ae5a21e80a	a0cf7767af566ba48e0	b035fa5546fc34e28	98a31ad6			
	FileType	Word (2007-2010)						
	Computer	ec2-54-234-70-44.comp	ute-1.amazonaws.con	n				
	SourceSystem	OpsManager						
	Туре	CommonSecurityLog						
	_ResourceId	/subscriptions/240d6f29	l-e1ab-4c5b-b28a-e62	2883cb41a9/resour	cegroups/sentinel-test/p	providers/microsoft.compute/virtualm	achines/sentinel-	logforward
	companyName	securityjoes						
	correlationId	6965cf87-045f-4a6b-bd	a5-f0321c75a43f					
	itemId	6965cf87-045f-4a6b-bd	a5-f0321c75a43f					
	SrcFileName	saddsaDSA.docx						

6. Results can be viewed in **Local Time** zone by changing the option in the bottom bar:



### **Deploy the Workbook**

- Copy the contents of the file: /Votiro-Offline/Workbooks/Votiro Monitoring Dashboard.json
- 2. On Microsoft Sentinel, go to your WorkSpace > Workbooks > Add Workbook":



3. On the New Workbook page, click on Edit > Advanced Editor icon:



4. Replace the Gallery template contents with the copied contents, and click on **Apply**:

$\equiv$ Microsoft Azure	♀ Search resources, ser
Home > Microsoft Sentinel   Workbooks >	
New workbook ∞ … sentinel-test	
$\square$ Done Editing $\square$ Open $\square$ $\square$ $\square$ $\square$ $\square$ $\checkmark$ $\checkmark$ $\bigcirc$ $\square$ $\checkmark$ $\checkmark$ $\bigcirc$ $?$ Help	
Shown below is a JSON representation of the current item. Any changes you make here will be reflected when you press 'Apply'.	
Template Type ①	
Gallery Template ARM Template	
l l	
"version": "Notebook/1.0",	
"items": [	
{   "two": 1	
"content": {	
"ison": "## This Workbook is used to analyse file sanitization data from Votir	o's endpoints."
"customWidth": "90",	
"name": "text - 5",	
"styleSettings": {	
"maxWidth": "90"	
"content": {	
"version": "KqlParameterItem/1.0",	
"parameters": [	
"id": "8b8cd15e-bd0d-4cb9-aef6-07e117e2cf5a",	
"version": "KqlParameterItem/1.0",	
"name": "TimeRange",	
type: 4,	
Iskequireu : true,	
"durationMs": 60480000	
}.	
"typeSettings": {	
"selectableValues": [	
"durationMs": 300000	

5. The Following Workbook must be visible: After a scroll

### **Set Alert Queries for Incidents**

- 1. Go to /Votiro-Offline/Analytic Rules. Keep both Votiro File Blocked FromConnector.json and Votiro File Blocked in Email.json files ready.
- 2. On Microsoft Sentinel > Workspace, select Analytics.
- 3. Click **Import** (from the bar at the top of the screen) in the resulting dialog box, navigate to and select the JSON files one by one, and select **Open**:

Microsoft Sentinel   Selected workspace: Sentinel -	Analytics									
🔎 Search	+ Create 🗸 🜔 Refresh	🗠 Analytics workbooks 🛩 😋 Rule		B Delete ← Import → Export ■	Columns 🛛 🔗 Guide	s & Feedback				
General	1.5	(ii). Many control of	Rules by severity							
Overview	o J Active rules	Content hub	High (1) Medium (0) Low (2)	Informational (0)						
🕈 Logs										
News & guides	Active rules Rule templ	ates Anomalies								
🔎 Search	Search by ID, name, tact	tic or technique 🛛 🖓 Add filter								
Threat management	Severity	Name		Rule type	Status	Tactics	Techniques	Source name	Last modified 4	
Incidents	Low	Votiro File Blocked in Email		Scheduled	C Enabled			Custom Content	2/26/2024, 2:02	
Workbooks	Low	Votiro File Blocked From Connector		Scheduled	C Enabled			Custom Content	2/26/2024, 2:02	
Hunting     Hotelseels	High	Advanced Multistage Attack Detecti	on .	C Fusion	C Enabled	ѐ Col +11 ()		Gallery Content	1/28/2024, 12:1	
Notebooks     Entity behavior										
<ul> <li>Threat intelligence</li> </ul>										
MITRE ATT&CK (Preview)										
Content management										
Content hub										
Repositories (Preview)										
Community										
Configuration										
A Workspace manager (Preview)										
III Data connectors										
🍐 Analytics										
Watchlist										
Automation										
Settings										

4. Make sure that the status of each active rule is enabled:

+ Create	e 🗸 💍 Refresh 占	🗠 Analytics workbooks 🗠 🤇 Rule r	uns (Preview)	🖒 Enable	O Disable	🗊 Delete \leftrightarrow	Import I Export	III Columns	🔗 Guides	& Feedback	
<b>4</b> 3		More content at	Rules by se	werity							
Active rule	Active rules		High (1)	Medium (0)	Low (2)	Informational (0)					
Active rule	Active rules         Rule templates         Anomalies           P         Search by ID, name, tactic or technique         V         Add filter										
s	everity	Name				Rule	type	Statu	5	Tactics	Techniques
	Low	Votiro File Blocked in Email				٩	Scheduled		Enabled		
	Low	Votiro File Blocked From Connector				9	Scheduled		Enabled		
	High	Advanced Multistage Attack Detection					Fusion		Enabled	<mark>è</mark> Col +11 🛈	

5. Check for recent alerts or incidents on the **Overview** page. Incidents are also available on the **Microsoft Sentinel** > **Incidents** page.

the second designed												
Home > Microsoft Sentinel												
Microsoft Sentinel	Incider	ts …										
₽ Search «	+ Creat	incident (Preview)	🕐 Refresh 🕓 Cust	om range: 2/6/2023 - 3/7/2024 <		iete 🔣 Security efficiency w	orkbook III Columns 🔗	Guides & Feedback				
General				~-	Open incidents by sev	rity						
Overview	Open inci	lents	New incidents	Active incidents	High (D)	Medium (I)	Leve (b)	Informational (	-			
🧬 Logs												
News & guides	P Search	by ID, title, tags, o	wher or product	Severity : All Sta	itus : 2 selected in	cident Provider name : All	Alert product name : All	Owner : All				
🔎 Search	- ,	uto-refresh incider	ts									
Threat management		dev 11	Incident ID 11	Title 11	Alerts	locidant providar name	Alast product name	Created time 11	Last undata time 11.	Owner 1	Status 11	Taras
Incidents				free of the second second		Annual Contract	A formula formula			there is a second		
Workbooks		-		google_satebrowsing_samp		Azure Sentinel	Morosoft Sensinel	02/20/24, 07:12 PM	02/20/24, 07:12 PM	Unassigned	New	
Hunting		-		google_saterowsing_samp		Azure sentinel	Microsoft Sensinel	02/20/24, 07:12 PM	02/20/24, 07:12 PM	Unassigned	New	
Notebooks		-		google_satecrowsing_samp		Azure Senther	Microsoft Sentinel	02/20/24, 07/12 PM	02/20/24, 07:12 PM	Unasigned	New Street	
Entity behavior		*		[claimd.conf was blocked		Azure sentinel	Microsoft sensitiel	02/20/24, 02:22 PM	02/26/24, 02:22 PM	Unassigned	New	
Threat intelligence		*	4	hyslog.txt was blocked		Azure Sentinel	Microsoft Sentinel	02/26/24, 02:12 PM	02/26/24, 02:12 PM	Unassigned	New	
MITRE ATTRICK (Preview)		*		[clamd.conf was blocked		Azure Sentinel	Microsoft Sentinel	02/26/24, 02:12 PM	02/26/24, 02:12 PM	Unassigned	New	
Content management		iolum.		Newtest		Azure Senthel		01/28/24, 02:55 PM	01/28/24, 02:55 PM	20rel Mishal	New	
Content hub												
Repositories (Preview)												
Community												

Select the security efficiency workbook for a better view.

- 6. Alerts Logic:
- Votiro File Blocked From Connector: If the syslog message includes "blocked" under -Sanitization result- field and "false" under -password protected- field and "null" under -from- field create an alert with the following message: [file name] with hash [file hash] that was sent from connector [connector name] was blocked by Votiro due to Policy [policy name], see more detail in the following link [incident url]
- Votiro File Blocked in Email: If the syslog message includes "blocked" under -Sanitization result- field and "false" under -password protected- field and not "null" under -from- field create an alert with the following message: Attachment [file name] with the hash [file hash] was blocked in an email that was sent from user [from] to the following recipients [Recipients] by Votiro due to Policy [policy name], see more detail in the following link [incident URL]

### **3 How to Send Files to Votiro via Postman**

Postman is an API platform for developers to design, build, test and iterate their APIs. It is an HTTP client that tests HTTP requests, utilizing a graphical user interface, through which different types of responses are returned that need to be subsequently validated. This article describes how to use Postman with Votiro.

### 3.1 Prerequisites

Install Postman by downloading one of the following:

- The Postman app from <u>Download Postman</u>.
- The Postman portable app from Postman<sup>™</sup> portable.

### 3.2 Procedure

#### 3.2.1 Generating a Service Token

1. Generate a Service Token. Go to Settings > Service Tokens > Create New :

Settings

Service To A list of service	kens to tokens which allows other services to communicat	e with Votiro produ	cts + Create N
ID	bd7b56a2-2692-4686-9df2-ea61165a0bf9	ID	6c96ea87-4fa9-409e-b882-e55470aeeb7
Issued To	King Browser Plugin	Issued To	King Dem
Created At	20/08/2024 22:24	Created At	25/09/2024 10:3
Expiration	13/02/2026	Expiration	13/02/202
Туре	Connector	Туре	Develope
	Revoke		Revok

- 2. Select the token **Type**:
  - a. **Connector** Basic integration. Allows authentication for uploading files procedure.
  - b. **Developer** Advanced integration. For all available APIs. Handle it with caution.
- 3. Enter a name for the new token under **Issued To**.
- 4. Set Expiration Time
- 5. Press **CREATE**:

.....



#### Create New Service Token

.

#### Set Expiration Time

<	Fel	o 🛊	; 2	027	\$	>
Su	Мо	Ти	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28						
	EL				CF	REAT

6. Copy and save the token string that appears on this page.



WARNING!



#### Save the token string. This page will only appear once.

#### Please Save Your Token, You Won't Be Able To See It Again

ID	ff5e09af-0867-4514-bfed-4186e86ef2fe
Issued To	Test-Token
Expiration	15/03/2023

#### Token

eyJhbGciOiJSUzI1NiIsImtpZCI6IjI0OTMxRUM5QzA4NTIGOEV GNkMONUY0MDExQTU0MTAzNzhGMTY5REEiLCJ0eXAiOiJK V1QifQ.eyJ1bmlxdWVfbmFtZSI6IIRIc3QtVG9rZW4iLCJncm91c HNpZCI6IIZvdGlyb0ludGVybmFsU2VydmljZXMiLCJyb2xIljoiQ WRtaW5pc3RyYXRvciIsImp0aSI6ImZmNWUwOWFmLTA4Njct NDUxNC1iZmVkLTQx0DZI0DZIZjJmZSIsIm5iZiI6MTY0NzgzN DQxMCwiZXhwIjoxNjc40DA5NjAwLCJpYXQi0jE2NDc4MzQ0 MTB9.EYm24-

YcS6RnXSCh7LiYDFAMA5d\_U7Z6nBW670FOgiA6AH3tG14am RWc6wjo2LpKxNAVLbrnMUbrVUTCRToAWABPvT47gJslBdafP 9R0sPOh0voAdbh\_hjt-

J9jspYuF8hu7NfukUxUVhDd3oKRnGDmWizBANbqCbXXw2fE GLgWpn0VuR88y\_o7vxoBp5mqlqRWvQ1p3mGTEAem6sI1U8 HhYgvOvKMYY9TH9cxnuRbnpA-

xVwGCQ8OFQuA6ITJw9ehwl34vUA22qri65-xNvWoakgXVAtiHSpWxdgWrmeLK88wKum7dUyFfDu4rrEadvvmLFZK3eEZ1K pZOv1DcDg

ОК

7. Press **OK** to close the Token window.

### 3.2.2 Postman Setup

1. In the Postman app, go to **Workspaces** > **My Workspace** and press **New**:



2. The Create New window opens. Select HTTP Request:

Create New	r					$\times$
Building Bl	ocks					
GET	HTTP Request	<u>মি</u>	WebSocket Request BETA Test and debug your WebSocket connections	¢g	<b>gRPC Request BETA</b> Test and debug your gRPC request	
	Collection Save your requests in a collection for reuse and sharing		Environment Save values you frequently use in an environment		Workspace Create a workspace to build independently or in collaboration	I
Advanced						
	API Documentation Create and publish beautiful documentation for your APIs		Mock Server Create a mock server for your in- development APIs	<b>^</b>	Monitor Schedule automated tests and check performance of your APIs	
00	API Manage all aspects of API design, development, and testing	어 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다	Flows BETA Create API workflows by connecting series of requests through a drag-and-drop UI.			
Not sure w	here to start? Explore featured APIs, o	collections	, and workspaces published by the Po	ostman coi	mmunity.	
					Learn more on Postman Do	ocs
Press the	e Settings icon:					

🤣 Postman File Edit View Help					- a ×
🥖 Home 🛛 Workspaces 🗸	API Network V Reports Explore		Q Search Postman	A Invite ୪ <sup>3</sup> to a G	Upgrade ~
A My Workspace	New Import 🛞 Overview	GET Untitled Request	+ ***	Settings pent	~ ©

4. The **Settings** window opens. To ensure that http requests will go through even if your VA is using a self-signed certificate, toggle **SSL certificate verification** to **OFF**:

3.

SETTINGS			×	
General Themes Shortcuts Data	Add-ons	Certificates Proxy Update Abou	t	
Request		Headers		
Trim keys and values in request body	OFF	Send no-cache header	ON ON	
SSL certificate verification	OFF	Send Postman Token header	ON	
Always open requests in new tab	OFF OFF	Retain headers when clicking on links	OFF	
Always ask when closing unsaved tabs	ON ON	Automatically follow redirects	ON	
Language detection	Auto 🗸	Send anonymous usage data to ON Postman		
Request timeout in ms	0			
Set how long a request should wait for		User interface		
a response before timing out. To never time out, set to 0.		Two-pane view	OFF	
Max response size in MB	50	Show icons with tab names	ON	
Set the maximum size of a response to download. To download a response of		Variable autocomplete	ON ON	

#### 5. Close the **Settings** window.

#### 6. Under the **Untitled Request** dropdown box, select **POST**:

### **Untitled Request**

GET	$\times$ $^{\sim}$	Enter rec
GET		I
POST	]	
PUT		
PATCH		
DELETE	Ē	
COPY		
HEAD		
OPTION	٩S	
LINK		
UNLINK	< Comparison of the second sec	
PURGE		
LOCK		
UNLOC	к	
PROPFI	IND	
VIEW		

7. In the Enter request URL box, enter your VA FQDN in the following format: https://<VA-FQDN>/disarmer/api/disarmer/v4/upload

#### For example:

Votiro / e	mdbs-va	3	🖺 Save	$\sim$	000
POST	~	https://emdbs-va.mytestwon40.com/disarmer/api/disarmer/v4/upload			

8. Select the Authorization tab and under the Type dropdown, select Bearer Token:

Params Authorization	<ul> <li>Headers (8) Body</li> </ul>
Туре	Bearer Token ^
The authorization header generated when you senc Learn more about authori:	Inherit auth from parent No Auth API Key
	Bearer Token Basic Auth
	Digest Auth
Response	OAuth 1.0 OAuth 2.0
	Hawk Authentication
	AWS Signature NTLM Authentication
	Akamai EdgeGrid

#### 9. Select the **Headers** tab.

10. In the first row of the **Key** column, start to type **Content** until a dropdown list appears. Then select **Content-Type** from the dropdown list:

Head	ders 💿 8 hidden	
	KEY	
	Content	
	Content-MD5	
	Content-Length	
	Content-Transfer-Encoding	
	Content-Type	

11. In first row of the **Value** column, start to type **multipart** until a dropdown list appears. Then select **multipart/form-data** from the dropdown list:

mul multipart/mixed multipart/alternative multipart/related
multipart/mixed multipart/alternative multipart/related
multipart/alternative multipart/related
multipart/related
multipart/form-data
multipart/signed
multipart/encrypted

12. Select the **Body** tab and then select **form-type**:

Params	Authorization	n 🔴	Headers (9)	Body 🔵	Pre	-request Scrip	ot Tests	Settings
none	🖲 form-data	• x	-www-form-urle	encoded	rav	v 🔵 binary	GraphQL	

13. In the first row of the **KEY** column, type **File**, and select **File** from the hidden dropdown list:

	KEY	
$\checkmark$	File	File $\vee$
	Кеу	Text
		File

- 14. In the first row of the **VALUE** column, press **Select Files** and select the desired file from the browser window that opens.
- 15. In the second row of the **KEY** column, type **Properties**.
- 16. In the second row of the VALUE column, enter the following:

```
{"PolicyName":"Default
Policy","ChannelType":"FileConnector",
"ChannelId":"827b50a3-d585-4ba5-a5ca-
100b09068123","ChannelName":"API Up-Sync"}
```

17. After completing steps 13-16, the **KEY** and **VALUE** table should be identical to the below screenshot, with the exception of the file name:

Params	s Authorization  Headers (10)	Body  Pre-request Script Tests Set
none	e 🦲 form-data 🌑 x-www-form-urlen	coded 🔵 raw 🔵 binary 🔵 GraphQL
ŀ	KEY	VALUE
	File	Pptx-ActiveX.pptx ×
	Properties	{"PolicyName":"Default Policy","ChannelT
ł	Кеу	Value

18. Press the Send button:

POST	~	https://emdbs-va.mytest140.com/disarmer/api/disarmer/v4/upload	Send ~	
				_

19. You should get a HTTP/200 response and a GUID string in the body. This will be the Correlation ID of the file that you have submitted.

#### For example:

Test	File Collection / emdbs-va Copy		🖺 Save 🗸 👓	0	1 E
POS	T v https://emdbs-va.mytestwon40.co	m/disarmer/api/disarmer/v4/upload		Sen	nd ~
Parar	ms Authorization • Headers (11) Body •	Pre-request Script Tests Settings     raw      binary      GraphQL			Cookies
	KEY	VALUE	DESCRIPTION	000	Bulk Edit
$\checkmark$	File	Pptx-ActiveX.pptx ×			
≑ 🗹	Properties Text ~	{"PolicyName": "Default Policy", "ChannelType": "			×
	Кеу	Value	Description		
Body	Cookies Headers (4) Test Results tty Raw Preview Visualize Text	Status: 200 0	DK Time: 34 ms Size: 170 B S	ave Res	sponse ~
1	4d41873a-7e5a-4a1a-a879-ccb9b7d71620				T

20. On the Incidents page, you will be able to see the exact string:

ជ		4d41873a-7e5a-4a1a-a879-ccb9b7d71620	
88	Files File actions 🗸	File Info	Sanitization Log
6	Exptx-ActiveX.pptx		Data Processing
٥	[Content_Types].xml     .rels	= ×	File Pptx-ActiveX.pptx upload for sanitization started. Item Id: 4d41873a-7e5a-4a1a-a879-ccb9b7d71620     File Pptx-ActiveX.pptx recognized as [17] Power Point
<ul> <li>□</li> <li>□</li> </ul>	presentation.xml  presProps.xml	4	(2007-2010) (Microsoft Office).  Office Relation Types Removed  ActiveX Removed
	👊 tableStyles.xml	Pptx-ActiveX.pptx	New child created for item 4d41873a-7e5a-4a1a-a879- cch9b747820, Child ID: 68150756-68058-498c-bh9f.
	viewProps.xml	Premier rome rome rome rome rome rome rome ro	d20142040648.     Max.comm.comm.comm.comm.comm.comm.comm.com
	III_ app.xml	Connector Name API Up-Sync	Total Sanitization Time
	a core.xml	Connector Type File Connector	
	Bilde2.xml		
	III_ slide1.xml		

### 4 How to Use Kibana to Troubleshoot Votiro Incidents

This page describes how to use Kibana to view and troubleshoot Votiro Incidents.

### 4.1 Example of Votiro Incident

The following screenshot displays the Votiro Item/Incident sanitization information for a file that has undergone sanitization:



This screen shows the results of Votiro On-prem processing a file named KeePass-2.49-Setup.exe. The **File Info** pane displays some of the file properties and the **Sanitization Log** pane displays highlights of the file **Data Processing**.

### 4.2 **Procedure**

#### 4.2.1 Create and Configure an Index Pattern

To begin, you must define a Kibana index pattern.

- 1. Login to the Kibana Discover interface with the credentials provided to you by Votiro Support.
- 2. Select Create index pattern. Step 1 of 2 Define index pattern appears.
- 3. Type **votiro-logs\*** (or similar) as the Index pattern. Kibana displays a list matching the index pattern:

Elasticsearch		
Index Management	Create index pattern	
Index Lifecycle Policies Polium Jobs	Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.	X Include system indi
Transforms		
Remote Clusters	Step 1 of 2: Define index pattern	
Snapshot and Restore	Index pattern	
8.0 Upgrade Assistant	votiro-logs*	
	You can use a * as a wildcard in your index pattern.	> Next sten
📕 Kibana	You can't use spaces or the characters  /, ?, *, <, >,  .	, How dop
Index Patterns	Success! Your index pattern matches 100 indices.	
Saved Objects	votiro-logs-000001	
Reporting	votiro-logs-000002	
Advanced Settings	votiro-logs-000003	
	votiro-logs-000004	
	votiro-logs-000005	
	votiro-logs-000006	
	votiro-logs-000007	
	votiro-logs-000008	
	votiro-logs-000009	
	votiro-logs-000010	
	Rows per page: 10 $$ $$ $$	< 1 2 3 4 5 10 >

#### 4. Click on Next step. Step 2 of 2 Configure settings appears.

K	Management / Index patterns / Create index	k pattern		
	Elasticsearch			
۲	Index Management	Create index pattern		
ŝ	Rollup Jobs	Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.		X Include system indices
50	Transforms Remote Clusters	Step 2 of 2: Configure settings		
â	Snapshot and Restore	Xou've defined votice-logs* as your index pattern. Now you can specify some settings before we create it		
8	License Management 8.0 Upgrade Assistant	Time Filter field name Refresh		
2		~		
6	Kibana	Gt		
ę	Saved Objects	@timestamp key.ReceivedTime		
1	Spaces Reporting	query.Filter.Value query.From		
<sup>d</sup>	Advanced Settings	I don't want to use the Time Filter	Back	Create index pattern
Ŷ				
ŵ				
۲				

5. Select a **Time Filter field name** from the list. For example, **@t**:

	Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.	X Include system indice
Rolley Jobs Transforms Remote Clusters Snugabol and Restore License Management & Di Upgrate Assistant & Citoana Index Paterns Saved Objects Saved Objects Spaces Reporting	Step 2 of 2: Configure settings         You've defined vatiro-logs* as your index pattern. Now you can specify some settings before we create it.         The Filed rank Failersh         Image: The File values this field to they your data by time.         You can choose not thave a time field, but you will not be able to non-odd by a time image.         > Show advanced options	
Advanced Settings	< Ba	Create index pattern

6. Click on **Create index pattern**. Kibana displays every field and field type in the selected index (in this example, votiro-logs\*):

Elasticsearch Index Lifecycle Policies Rollup Jobs Transforms Remote Clusters Snapshot and Restore	★ VOTIFO-IO Time Filter field name: This page lists eve Elasticsearch Mag	gS <sup>★</sup> ⊚t Default ery field in the <b>votiro-logs*</b> ping API <b>%</b>	index and the field's assoc	ciated core type a	s recorded by Elast	icsearch. To chang	* C
License Management	Fields (181)	Scripted fields (0)	Source filters (0)				
8.0 Upgrade Assistant	Q Filter						All field type
Kibana	Name		Туре	Format	Searchable	Aggregatable	Excluded
Saved Objects	Filter		string	Þ	•		
Spaces Reporting	Filter.keyword		string	NJ.	•	•	
Advanced Settings	0		string				
	0.keyword		string		•	•	
	1		string		•		
	1.keyword		string		•	•	
	2		string		•		
	2.keyword		string		•		
	3		string				
	3.keyword		string		•	•	
	Rows per page: 10	~				< 1	2 3 4 5

### 4.3 Analyze the Data

After the index pattern is created and configured, apply it to the data in Kibana's Discover mode to yield useful results by additional filtering of the data.

### 4.3.1 Discover

1. Click on the Discover icon on the left side of the screen:



2. Kibana displays all hits that match the time filter criteria within the time range indicated (in this example, for the last 15 minutes):

New Save Open Share In	spect		
🗓 🗸 Search			KQL 🛗 🗸 Last 15 minutes Show dates O' R
- + Add filter			
votiro-logs* Ju	0		121 hits
Q Search field names			Nov 8, 2021 (@ 10:58:03.404 - Nov 8, 2021 (@ 11:13:03.404 — Auto 🗸
Filter by type	0		
Selected fields	7		
.source	ð	300	
Available fields			
t Filter		10:59:00	1100.00 1101.00 11.02.00 11.02.00 11.04.00 11.05.00 11.08.00 11.07.00 11.08.00 11.08.00 11.08.00 11.08.00
			@t per 30 seconds
r 1		Time 🗸	_source
1 2	>	Nov 8, 2021 @ 11:12:46.871	Øtimestamp: Nov 8, 2021 0 11:12:46.871 Podkame: mmg-service-release-deployment-84b4877655-22/2v Host: t-n2.prod.votiro.com ContainerHame: mmg-service-release dt: Nov 8, 20
1 3			11122-06-071 WHIL CONTIGUTION RANGE OF ALL INFORMATION BOARDWARKS, INCLEMENTED, FORTH REALIZEMENTE, INGUESTION POLICY LEADER OF ALL AND ALL
1 01			
t Omt	,	Nov 8, 2821 0 11:12:46.871	<pre>@timestamp: Nov 8, 2021 0 11:12:46.871 PodName: mng-service-release-deployment-84b4877d55-2xv2v Host: t-n2.prod.votire.com ContainerName: mng-service-release 6t: Nov 8, 26 11:12:46.871 Empt Use confin key 'RELEASE MATLITEMPLATE's Resources/BeleaseMailTemplate http://dlinet.com/formation/SourceContext/ReleaseMarline/SourceContext</pre>
0 ot			release-deployment-&bb4877d55-2x2v [temId: no itemid CorrelationId: no correlationid ServiceId: release-service _id: 34r5_neBxsy31r55t00 _type: _doc _index: votiro-logs
Ctimestamp			900195 _score: -
t ©×	>	Nov 8, 2821 @ 11:12:46.871	@timestamp: Nov 8, 2021 @ 11:12:46.871 Podkame: mg-service-release-deployment-84b4877d55-22v2v Most: t-n2.prod.votiro.com ContainerName: mg-service-release @t: Nov 8, 20
t ActionId			11:12:46.871 dmt: Use config key 'username's'' 01: Information SourceContext: ReleaseService.Program MachineName: mg-service-release-deployment-8404877d55-2zv2v ItemId: n
# ActionName			itemid CorrelationId: no correlationid ServiceId: release-service _id: 30fS_meExsyV31r5St90 _type: _doc _index: votiro-logs-000195 _score: -
	>	Nov 8, 2021 0 11:12:46.871	Dtimestamp: Nov 8, 2021 0 11:12:46.871 PodName: mng-service-release-deployment-8404877d55-2zv2v Host: t-n2.prod.votiro.com ContainerName: mng-service-release @t: Nov 8, 20
Connectionid			11:12:46.871 dmt: Use config key 'RELEASE_MAIL_SUBJECT's' 41: Information SourceContext: ReleaseService.Program Machinekame: mg-service-release-deployment-84b4877695-22:
e Containerimage			
ContainerImage     ContainerImage     ContainerName			ItemId: no itemId CorrelationId: no correlationId ServiceId: release-service _1d: 4ETS_nw&xxyY31rSS190 _type: _doc _index: votiro-logs-000195 _score: -

3. To further filter the results, click on  $\vee$  next to the index pattern (votiro-logs\* by default) in the left side of the screen. The **CHANGE INDEX PATTERN** window opens:



4. Move the cursor down the list of **Available fields** to select fields to filter. Then click on the **add** button to add the field to the filter:



- 5. In the example below, the following fields are added:
  - @I level
  - @mt message template
  - @x exception
  - ContainerName
  - CorrelationId
- 6. The display of hits is now updated to show only the selected fields:

-									
New Save Open Share In	nspect								_
🖸 🗸 Search						KQL 🛱 🗸 Last 15 min	nutes	Show dates	C Refre
otiro-logs* ∨	0	•			121 hits				
Q Search field names					Nov 8, 2021 @ 10:58:03.404 - Nov 8, 2021 @ 11:13:03.4	404 — Auto 🗸			
Filter by type	0								
elected fields		ti	60						
1 01		S	20						
e gint			•						
©x.			10.59100	11:00:00	11.01.00 11.02.00 11.03.00 11.04.00 11.05.00 11.08.00	11.07.00 11.08.00	11:09:00 11:10:00	11.11.00 11	12:00
t ContainerName				01	Er her an addense			ContainerName	
t CorrelationId			Time 🗸		@mt		@×		CorrelationId
vailable fields		>	Nov 8, 2021 0 11:12:46.871	Info rmat	Configuration has been reloaded		-	mng-service-rele ase	no correlati
t Filter				100					
		>	Nov 8, 2021 0 11:12:46.871	Info	Use config key 'RELEASE_MAIL_TEMPLATE'='Resources/ReleaseMailTemplate.html'			mng-service-rele ase	no correlati
				100					
1 2		>	Nov 8, 2021 0 11:12:46.871	Info	Use config key 'username'=''		-	mng-service-rele	no correlati
13				ion					
		>	Nov 8, 2021 0 11:12:46.871	Info	Use config key 'RELEASE_MAIL_SUBJECT'=' '	Q	Q -	mng-service-rele	no correlati
Articold				ion				ase	
t ActionName		>	Nov 8, 2021 0 11:12:46.871	Info	Use config key 'VOTIRO_BLOB_SERVICE_ADDRESS'='http://blob-service:5000'			mng-service-rele	no correlati
t Connectionid				ion				834	
t Containerimage		>	Nov 8, 2021 0 11:12:46.871	Info	Use config key 'VOTIRO_ITEM_SERVICE_ADDRESS'='http://item-service:5000'		-	mng-service-rele	no correlati
f Host				100				924	

### 4.3.2 Votiro Explore Incident & File Info

To examine a specific file that was processed by Votiro On-prem, the threat ID is obtained from the Votiro Item/Incident sanitization information.

1. Open the Votiro Explore Incident:

C		4864f52e-5021-4280-b66c-a336a975b379	
88	Files File actions 🗸	File Info	Sanitization Log
8 () () () ()	Files File File V	File Info	Data Processing  Data Processing  A first Annual 2-49 -Setta, area spatial for samitation started, first AddAttaba 2-49 -Setta, area spatial for samitation started, first AddAttaba 2-49 -Setta, area spatial (2002) Executable (Any Brary Fies).  B Executable Rearies 2-49 -Setta, exe, pack-case, pdf tocked due to puot opparatation policy, volution (The binary file was backed in the samitation process.  Find Parise 2-49 -Setta, exe, pack-case, pdf tocked due to puot opparatation process.  Find Parise 2-49 -Setta, exe, pack-case, pdf tocked as a result.  of the samitation process.  Find Parise 2-49 -Setta, exe, pack-case, pdf tocked as a result.  of the samitation process.
		Connector Yape None	Total Sontization Time

2. Copy to the clipboard the file ID at the top of the screen, in this example:

4864f52e-5021-4280-b66c-a336a975b379

#### 4.3.3 File Sanitization Analysis

- 1. Return to the Kibana Discover screen.
- 2. In the left side of the Kibana Discover screen, click on **Add filter**. The **EDIT FILTER** window opens.
- 3. From the **Field** list, select **CorrelationId**.
- 4. From the **Operator** list, select **is**.

5. In the **Value** field, paste the file ID from the clipboard .



6. Click on **Save**. The list of hits displayed is updated to show only those hits for the relevant file, according to the CorrelationId (= Votiro item).

ew Save Open Share In	nspect									
🖞 🗸 Search						KQL	🛗 🗸 🛛 Last 15 mini	utes	Show dates	C Refr
CorrelationId: 4864152e-5021	-4280-b66c-a33	3a975b379 ×	+ Add filter							
otiro-logs* ~	0				61 hits					
C Search field names					Nov 8, 2021 @ 10:59:15.233 - Nov 8, 2021 @ 11:14:15.233	3 — A	ito 🗸			
Filter by type	0	60								
lected fields		¥ 40								
0		30 20								
gent		10								
e ex			11:00:00	11:01:00	11:02:00 11:03:00 11:04:00 11:05:00 11:06:00 11:07:00	11.08.00	11.09:00	11:10:00 11:11:00	11:12:00 11:13:0	
ContainerName					@t per 30 seconds					
CorrelationId		Time -		©I	Ømt			Ø×	ContainerName	Correlation
railable fields		> Nov 8,	2021 0 11:09:34.03	Warn	n Failed to create /votirocache/files folder for large files			System.UnauthorizedAcc	sds-service-repor	4864f52e-
Filter				103				essException: Access t o the path '/votirocac	ter	88-556c-a 5379
0								ne/files is denied. > System.IO.IOExce		
1.1								ed		
1 2		> Nov 8,	2021 0 11:09:34.03	Warn	Files-Cache folder '/votirocache/files' is not exists, will created now				sds-service-repor	4864f52e-
13				ing					Cer .	b379
B Ot		> Nov 8,	2021 0 11:09:34.03	10 Warn	n Failed to create /votirocache/files folder for large files		0, 6	System.UnauthorizedAcc	sds-service-repor	4864f52e-
8 @timestamp				ing				o the path '/votirocac	Cer	b379
ActionId								> System.IO.IOExce		
ActionName					R			ed		
					Classics only have for comparty, 'spectra, ton, the here any orthogo'					1011670-0

7. To change the time frame of the display, click on the time icon  $\stackrel{\text{def}}{=}$   $\checkmark$ . Then select the desired time interval:

Quick select			L.		6.5
Last 🗸	15		minutes	~	Apply
Commonly used					
Today		L	ast 24 hours		
This week		L	ast 7 days		
Last 15 minutes		L	ast 30 days		
Last 30 minutes		L	ast 90 days		
Last 1 hour		L	ast 1 year		
Recently used date	ranges				
Today					
This week					
Last 30 minutes					
Refresh every					
				10	

8. To view the file processing history in Votiro, scroll down the list of hits. The selected fields displayed in the columns provide more information as to what occurred during the processing. Using the *@l* (message level), *@mt* (message template) and *@x* (exceptions) columns provides you with detailed information that can help you to troubleshoot the incident.

### 5 MSSP User Guide

A Managed Security Service Provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

Examples of MSSP use cases supported by Votiro include:

- Creating new customers and assigning licenses by the MSSP admin
- Viewing/filtering all the MSSP customer's data on the MSSP dashboard
- Using the MSSP incidents to see/filter all the MSSP customer's incidents data
- Creating reports on each MSSP customer's data

### 5.1 MSSP Tenant Management

1. Login

To login to MSSP Tenant Management, use the following URL address:

"https://{clusterName}/portal/#/votiro/login"

A login page will be displayed. Contact Votiro support to get the admin user credentials.

Email		
	LOG IN	
	200111	

After successful login, the Votiro MSSP Tenant Management screen is displayed:

ADD TENANT							
Name	ID	Domains	License Type	License Quota	License Expiration	License Features	
test-tomer	2a167928-deeman 200867d18/8	tomer.com	Consumption	0Bytes / 4TB	05-06-2024 (352 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
votiroapj-mssp	3aa2940a+do15-4103-000-0cc5490da997	votiroapj-mssp.com	Consumption	224.8KB / 10TB	15-06-2024 (361 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
demo-mssp	7aa33a <b>3b-6100 100 ad</b> 810423410c	demo-mssp.com	Consumption	25.8MB / 46TB	05-06-2024 (352 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
king	93d29 <b>e2140.0 10000000057</b> 72786984	king.com					ACTIONS
demotenant1	96d257cb-Shift 07c0219c2b25	demotenant1.com	Consumption	3.1MB / 10TB	05-06-2024 (352 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
votiro-dev	be9d9b4b4b4b20000000000000000000000000000000	votiro-dev.com	Requests	0 / 10,000,000,000	15-06-2024 (362 days remaining)		ACTIONS

The MSSP admin can use the Tenant Management screen to:

Add a customer tenant

- View the list of customer tenants
- View customer traffic information
- Manage each customer tenant's license
- View total actual usage compared to total license quota
- Delete customer tenants

#### 2. Add a customer tenant

To add a new customer tenant, press the **ADD TENANT** button.

	Tenant nar	ne		
O server a server to did server in the t				
Comma separated domain list	Comma se	parated do	omain list	
		A	DD TENANT	

#### Enter:

- Tenant name for example, King Demo
- Comma separated domain list for example, kingdemo.com. If there are multiple domains, separate the domains by a comma. For example, kingdemo.com, rontest.com

After adding a new customer tenant, a default admin user will be created. Contact Votiro support to get the admin user credentials.

#### 3. View the customer's tenant list

The following information is displayed on the Tenant Management screen for each tenant:

- Name Tenant name as configured in creation
- ID Tenant ID generated in UUID format
- Domains As configured in creation
- License Type The possible options are:
  - **Consumption** count by volume usage
  - Requests count by files

- License Quota Actual usage / License quota, as configured in the license import. The system will display up to date tenant usage.
- License expiration Expiration date and days remaining
- License features Currently, the possible options are:
  - menlo
  - aws s3
    - chrome
- 4. Import a license

To import a license for a customer tenant, press the corresponding **ACTIONS** button and select **IMPORT LICENSE**.

License type		
REQUESTS	CONSUMPTION	OBSOLETE
License Usa	ge: 110TB/50TB	
0		
GB TB		
Start date		
12/06/2023		
End date		
19/06/2024		
Feature flags		
Menlo		
AWS S3		
Chrome		
URL Reput	ation Coming soon	
	ADD LICENSE	
ter or select:		
License type		

- License Usage
- Start date
- End date
- Feature flags (if needed)

After creating a license, the system will display the imported license in:

- Votiro MSSP Tenant Management screen
- Customer tenant Management console license page
- 5. **Download Analytics Report**

To download an analytics report for any of the customer's tenants, press the corresponding **ACTIONS** button and select **DOWNLOAD REPORT**.

01/05/2023	
nd date	
nd date 19/06/2023	

Enter the **Start date** and **End date** to select the report's time interval, and press **GENERATE REPORT**. The report will be downloaded in CSV format.

¢	🛾 AutoSave 🖲 Off) 📙 🍤 🗸 🖓 🗸	⊽ Votiro_Summary_Exten	nded_Report_For_Tenant_7aa33a	3b-6194-4	81-9027-ad8f	0423410c	_01_05_2023_20	_06_202 ~	r
	File Home Insert Page Layout	Formulas Data Revie	w View Automate H	elp Acr	obat				
	Calibri	~ 11 ~ A^ A`	≡ ≡ 🔿 🗸 🖓 •	ab ce Wra	ap Text	G	eneral	~	B
	Paste La Copy → B I U ✓ ✓ Format Painter	• 🖽 • 🔷 • 🔺 •	= = = = =	🔁 Me	rge & Center	~ E	<b>ĕ</b> ~ % ୨	00. 0. <b>→</b> 0 <b>←</b> 00.	Con Form
	Clipboard 😼	Font 5	Alignme	nt		r <sub>2</sub>	Number	ľ2	
В	24 $\checkmark$ : $\times \checkmark f_x$								
	A		В	С	D	E	F	G	н
1	Customer name	Ron company							
2	Report dates	01/05/2023 - 20/06/2023							
3	Total Files processed		16						
4	Total Files sanitized		15						
5	Total Files blocked		1						
6	Total PPF files detected		0						
7	Number of emails	1							
8	Number of threats detected		2						
9	Average file size	1672870 bytes							
10	Average processing time	6.3325 seconds							
11									
12	License mode files	Consumption							
13	License permitted files		5.05775E+13						
14	Number of Files used so far		16						
15	License permitted consumption quota		5.05775E+13						
16	License consumption used so far		27024047						
17	License usage		0.00%						
18	Expiration date		05/06/2024 15:13						
19									
20									
2.4									

#### 6. **Delete a customer tenant**

To delete a customer tenant, press the corresponding **ACTIONS** button and select **DELETE TENANT**.

### 5.2 Monitoring Tenant Activity

#### 1. MSSP Dashboard

The MSSP user can view and filter Dashboard data by customers tenant selection.

G	Monitor Tenants ·	60 Minutes 24 Hours 7 Days 30 Days 12 Months Custom	Uve Status
88	Checkal Orectual		
0	₩ test-tomer ₩ demo-moso	<b>=</b>	
۲	Wing-seat	-	
	Incoming	Secure File	Protection &
0	Traffic	Gateway	Business Productivity
	Data Sources	Threats	Outputs
		① 1 Threats cleaned	279 Safe files
		1 incidents to inspect	
	↑ Test File		
-			

#### 2. MSSP Incidents

The MSSP user can view and filter incidents data by customer tenant selection in the **Tenants** column.

G	Incidents						٩
88	Date time 👻 Status 👻 Release	status 👻 Connectors 👻 Tenants 🛩 🕱					C
6	Date & Time 👻 Tenant na	ame File name Check all	From To	Cc	Connector type	Connector name	Blocked files
۲	11/06/2023 12:51 demo-ms	ssp D Votiro_Auditi			None	Self-sanitization	
 @	11/06/2023 12:51 demo-ms	ssp 🛞 Votiro-MSTe 📝 demoterant1			None	Self-sanitization	
	11/06/2023 12:48 demo-ms	ssp D Votiro_AuditReport_03,			None	Self-sanitization	
	07/06/2023 12:26 demotent	ant1 D Votiro_AuditReport_16_1			None	Self-sanitization	
	07/06/2023 12:25 demo-ms	ssp 🖲 Ripg			None	Self-sanitization	
	07/06/2023 12:25 demo-ms	ssp 🔳 11248-close-up-portrai			None	Self-sanitization	
	07/06/2023 12:24 demo-ms	ssp 🐻 Ripg			None	Self-sanitization	
	07/06/2023 10:48 demo-ms	ssp 🖪 11248-close-up-portrai			None	Self-sanitization	
	06/06/2023 12:06 demotion	ant1 D Votiro_AuditReport_16_1			None	Self-sanitization	
MS	06/06/2023 12:05 demoters	ant1 D Votiro_AuditReport_16_1			None	Self-sanitization	
			1 2 > >>				1/2

#### 3. MSSP Customer's Dashboard



An MSSP customer's user can view data only from their own tenant.

#### 4. MSSP Customer's Incidents

An MSSP customer's user can view data only from their own tenant.

ď	Incidents									٩
88	Date time 👻 Status 👻	Release status 👻 Co	onnectors 👻 🏋							С
۵	Date & Time 💌	File name	Subject	From	To	Co	Connector type	Connector name	Blocked files	
٢	19/06/2023 13:44	ChromeSetup.exe					None	Self-sanitization	$\oslash$	
2	19/06/2023 13:43	SMTP Connector Use	er Guic				None	Self-sanitization		
<b>(</b>					_1					1/1

### 6 How to Use QR Code Sanitization

Votiro supports QR Code sanitization. This is relevant for PDFs and emails containing QR codes.

There are four options when dealing with QR codes:

- Ignore the QR Code is ignored. The file or email is passed on as-is.
- Detect QR Codes detect if there is a QR Code in the file.
- Disarm QR Codes the original QR code is rewritten with the Votiro QR Code.
- Block QR Codes Votiro blocks the QR Code.

### 6.1 Disarm QR Codes behavior

- 1. The user scans the QR Code.

2. There will be an indication that the original QR Code was replaced with a Votiro QR Code pointing to the Votiro portal.



3. The user opens the link and is redirected to the Votiro portal. Votiro analyzes the URL for suspicious activity.



- 4. When the analysis completes:
  - If the URL was determined to be benign, the user will be redirected to the URL.
  - If the URL was determined as suspicious, the user will receive an indication that a threat was detected.



### 6.2 Votiro Administrator view

The file event will indicate if a:

- QR Code was detected and was rewritten by Votiro.
- Suspicious URL was detected.

#### For example:

Oct 8, 2024 10:43 AM Using policy "King"	Return to All Events	3 Sanitized	Files     Blocked	O Detected	1 Detected	4.7 Seconds		
Related Files Hierarchy	Privacy Risks		File Details		Data Processing			
✓ QR code sample.pdf Image0.png Image1.png	யி No Pil was	found	File name Image0.png ID 929f6769-eb62-4e43- File type	-aea1-0db2ad7387f9 6	rrae vae type File Imaged prig recognized as (56) PNO (Raster Image Files). OR Code deuteted OR Code deuteten Infel ImageD prig.code: http://malware.testing.googie.test/hesting/Imalware/*.			
	Suspicious Object List		PNG File size 1.59KiB	PNG 5		Suspicious URL detected Suspicious URL detected in file Image0.png. URL: http://maiware.testing.google.test/hesting/maiware/*		
	Suspicious URL detected Detected in (Image0.png)		Original item hash 8046380d58d7628191 Connector name Self-sanitization	1916f848e181117b42096113be5 6	QR Code Rewritten QR Code has been rewritten in file Image0.png. Code: https://ca.sg.paralax.votro.com/portal/#/uri/reputation/UC04b44 -673a-4600-bcbca-cef6617122a7/92916769-eb62-4e43-aea1- 0db2ad7387197			
			Users -	ň	uri+http:%;s4%;zF%;zFmaiware.testing.google.test%;2Ftesting% malware%;2F%;zA.			
Related Files by File Type			Subject	~	From			
PDF PNG				o o	<u>.</u>			
0 0.2 0.4 0.6 0.8	1 1.2 1.4 1.6	1.8 2	2.2					