VirtualMetric

virtualmetric.com

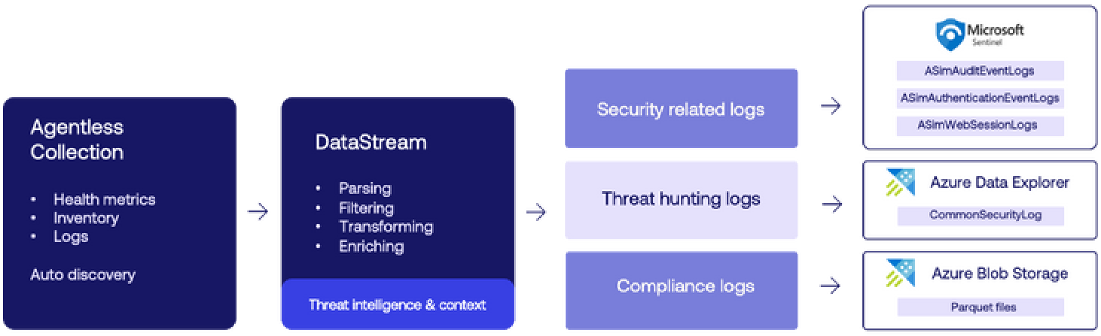
Introducing DataStream

Maximize Microsoft Sentinel ROI with VirtualMetric DataStream

The Smarter Way to Optimize Log Data for Security Operations

Transform your Sentinel Operations

VirtualMetric DataStream is your strategic ally for Microsoft Sentinel. It is designed to cut costs, optimize data processing, and supercharge your security operations. By reducing the volume of irrelevant data sent to Sentinel, we lower ingestion costs while maintaining complete security visibility. Critical logs go to Sentinel, while non-essential ones are directed to Azure Data Explorer or Azure Blob Storage for cost-effective storage and compliance.



Unparalelled Business value

DataStream optimizes Microsoft Sentinel by reducing data ingestion by up to 90% and cutting manual effort by 60% through intelligent filtering, log enrichment, and automated normalization. It streamlines log management, removes redundant data, and enhances SIEM efficiency—reducing Azure costs while freeing resources for advanced threat hunting and incident response.

Why DataStream?

Reduce Sentinel Ingestion Costs

Route high-value security logs to Sentinel and non-critical logs to cost-effective storage like Azure Data Explorer or Blob Storage, cutting ingestion costs dramatically.

Enhance Security Team Efficiency

Automated log filtering, contextual enrichment, and advanced compression eliminate the need for manual data wrangling. Analysts focus on real threats, not noise.

Ensure Compliance & Scalability

Comply with regulations by securely storing filtered logs for long-term access. As needed, push them back to Sentinel to ensure visibility for audits and investigations.

Key Features for Sentinel Optimization

1. Smart data filtering

- Automatically filter out non-actionable logs.
- Route only meaningful data to Sentinel.

2. Seamless Integration

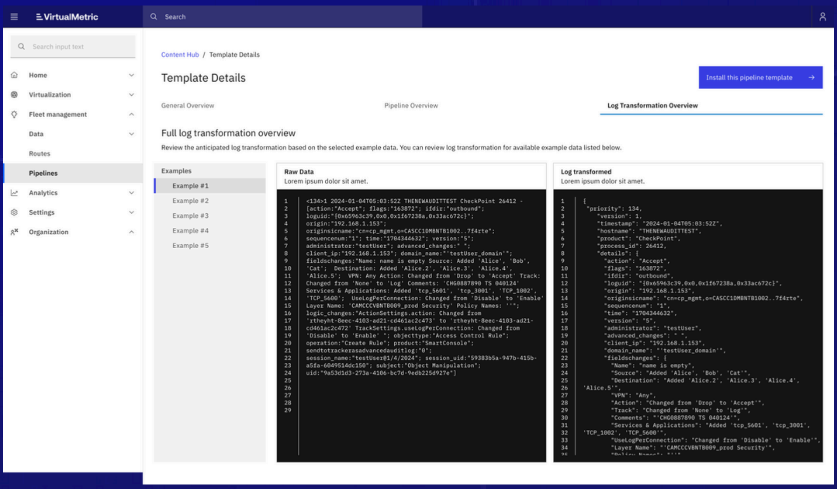
- Built-in compatibility with Microsoft Sentinel connectors.
- Easy setup with no disruption to existing pipelines.

3. Unmatched Compression

- Up to 99% compression, significantly lowering storage and bandwidth costs

4. Long-Term Storage

- Non-critical logs are stored in Azure Blob Storage with a push-back mechanism, ensuring accessibility without bloating Sentinel.



Template Details

Full log transformation overview

Review the anticipated log transformation based on the selected example data. You can review log transformation for available example data listed below.

Raw Data

Lorem ipsum dolor sit amet.

```
<134>1 2024-01-04T05:03:52Z THENEWAUDITTEST CheckPoint 26412 -
[action:"Accept"; flags:"163872"; ifdir:"outbound";
loguid:"{0x65963c39,0x0,0x1f67238a,0x33ac672c}";
origin:"192.168.1.153";
originsicname:"cn=cp_mgmt,o=CASCC1DMBNTB1002..7f4rte";
sequencenum:"1"; time:"1704344632"; version:"5";
administrator:"testUser"; advanced_changes:" ";
client_ip:"192.168.1.153"; domain_name:"'testUser_domain'";
fieldschanges:"Name: name is empty Source: Added 'Alice', 'Bob',
'Cat';  Destination: Added 'Alice.2', 'Alice.3', 'Alice.4',
'Alice.5';  VPN: Any Action: Changed from 'Drop' to 'Accept' Track:
Changed from 'None' to 'Log' Comments: 'CHG0887890 TS 040124'
Services & Applications: Added 'tcp_5601', 'tcp_3001', 'TCP_1002',
'TCP_5600';  UseLogPerConnection: Changed from 'Disable' to 'Enable'
Layer Name: 'CAMCCCVBNTB009_prod Security' Policy Names: ''";
logic_changes:"ActionSettings.action: Changed from
'rtheyht-8eec-4103-ad21-cd461ac2c473' to 'rtheyht-8eec-4103-ad21-
cd461ac2c472' TrackSettings.useLogPerConnection: Changed from
'Disable' to 'Enable' "; objecttype:"Access Control Rule";
operation:"Create Rule"; product:"SmartConsole";
sendtotrackerasadvancedauditlog:"0";
session_name:"testUser@1/4/2024"; session_uid:"59383b5a-947b-415b-
a5fa-6049514dc150"; subject:"Object Manipulation";
uid:"9a53d1d3-273a-4106-bc7d-9edb225d927e"]
```

Log transformed

Lorem ipsum dolor sit amet.

```
{
 "priority": 134,
    "version": 1,
    "timestamp": "2024-01-04T05:03:52Z",
    "hostname": "THENEWAUDITTEST",
    "product": "CheckPoint",
    "process_id": 26412,
    "details": {
      "action": "Accept",
      "flags": "163872",
      "ifdir": "outbound",
      "loguid": "{0x65963c39,0x0,0x1f67238a,0x33ac672c}",
      "origin": "192.168.1.153",
      "originsicname": "cn=cp_mgmt,o=CASCC1DMBNTB1002..7f4rte",
      "sequencenum": "1",
      "time": "1704344632",
      "version": "5",
      "administrator": "testUser",
      "advanced_changes": " ",
      "client_ip": "192.168.1.153",
      "domain_name": "'testUser_domain'",
      "fieldschanges": {
        "Name": "name is empty",
        "Source": "Added 'Alice', 'Bob', 'Cat'",
        "Destination": "Added 'Alice.2', 'Alice.3', 'Alice.4',
'Alice.5'",
        "VPN": "Any",
        "Action": "Changed from 'Drop' to 'Accept'",
        "Track": "Changed from 'None' to 'Log'",
        "Comments": "'CHG0887890 TS 040124'",
        "Services & Applications": "Added 'tcp_5601', 'tcp_3001',
'TCP_1002', 'TCP_5600'",
        "UseLogPerConnection": "Changed from 'Disable' to 'Enable'",
        "Layer Name": "'CAMCCCVBNTB009_prod Security'",
```

Achieve more with less

By partnering with VirtualMetric DataStream, you gain a cost-effective solution tailored to enhance Microsoft Sentinel. Save resources, boost security team efficiency, and maintain operational resilience.

Contact us today

Start reducing your log ingestion costs and unlocking the full potential of Microsoft Sentinel with VirtualMetric DataStream

michiel@virtualmetric.com
www.virtualmetric.com