# 介绍

保存searches将保留一个Discover视图，以供以后检索和重用。您可以将保存的searches重新加载到Discover视图中，将其添加到dashboard中，并将其用作visualization的基础。

保存的searches包括查询文本，过滤器以及时间过滤器（可选）。保存的searches还包括记录表中的选定列，排序顺序和当前索引模式。

Kibana visualizations基于Elasticsearch查询从Elasticsearch索引创建数据的可视化展示效果。通过使用一系列Elasticsearch聚合来提取和处理数据，并通过各种图表展示数据。

dashboard 通常是实时显示的visualizations, searches和maps的集合。

使用dashboard，可以做到：

1）添加visualizations，保存的searches和maps以进行并排分析。

2）排列dashboard元素以准确显示所需要的数据。

3）自定义时间范围以仅显示所需的数据。

4）检查和编辑dashboard元素，以准确找出要显示的数据类型。

创建dashboard时，必须有索引到Elasticsearch中的数据，从Elasticsearch获取数据的索引模式，visualizations，已保存的searches或maps。 如果不存在这些内容，则会在创建dashboard时提示您添加它们。

查看visualization的数据源的步骤：点击该visualization右上角🡪Inspect🡪View: Data🡪选择Requests🡪 查看index pattern 即为数据源

下文中一级标题代表 dashboard， 二级标题代表该dashboard下的一个visualization。

# ALL-MITRE-ATTACK

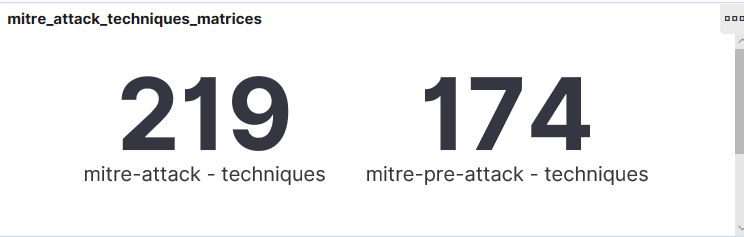
## mitre\_attack\_select

该visualization的类型为Controls,其作用是指定Matrix或者Platform为某个特定的值来为整个ALL-MITRE-ATTACK dashboard过滤数据。其界面如下图所示：



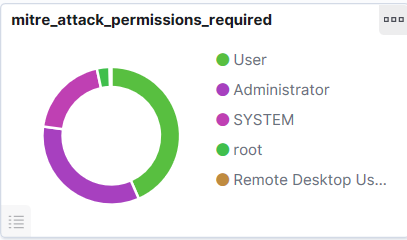
## mitre\_attack\_techniques\_matrices

该visualization的类型为Metric,其作用是按照matrix分组，统计每个matrix有多少个不同的technique。其界面如下图所示：



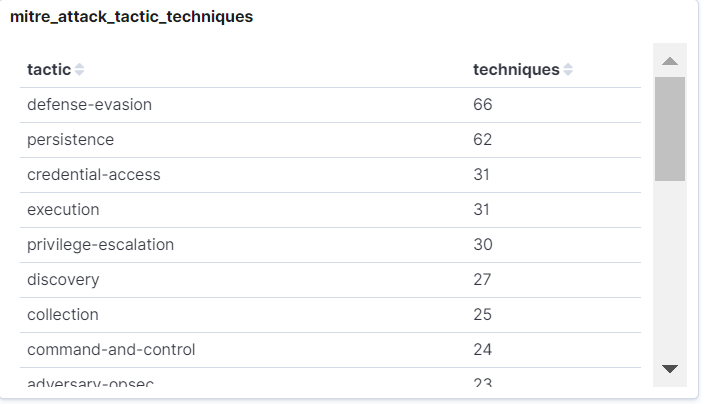
## mitre\_attack\_permissions\_required

该visualization的类型为Pie,其作用是按照permissions\_required分组，以饼图形式展现每个permissions\_required有多少个不同的technique以及所占百分比。其界面如下图所示：



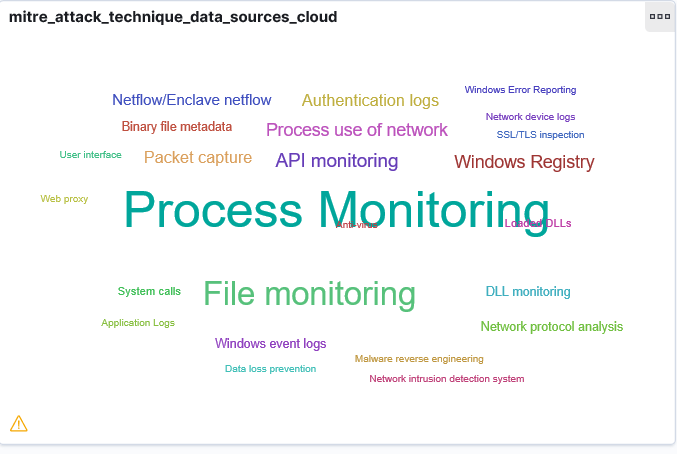
## mitre\_attack\_tactic\_techniques

该visualization的类型为Data Table,其作用是按照tactic分组，统计每个tactic有多少个不同的technique。其界面如下图所示：



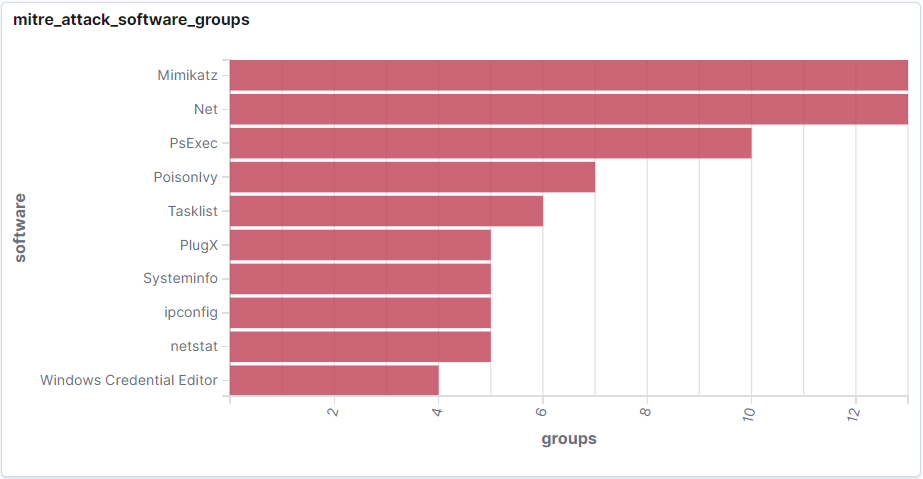
## mitre\_attack\_technique\_data\_sources\_cloud

该visualization的类型为Tag Cloud,其作用是按照data\_sources分组，统计每个data\_sources有多少个不同的technique，将technique数量多的data\_sources突出显示。其界面如下图所示：



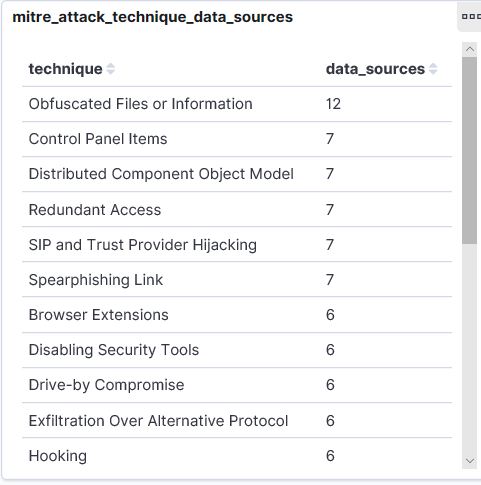
## mitre\_attack\_software\_groups

该visualization的类型为Horizontal Bar,其作用是按照software分组，统计每个software有多少个不同的group。其界面如下图所示：



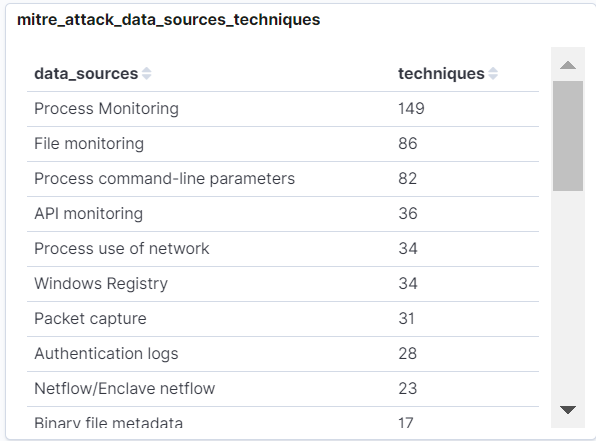
## mitre\_attack\_technique\_data\_sources

该visualization的类型为Data Table,其作用是按照technique分组，统计每个technique有多少个不同的data\_sources。其界面如下图所示：



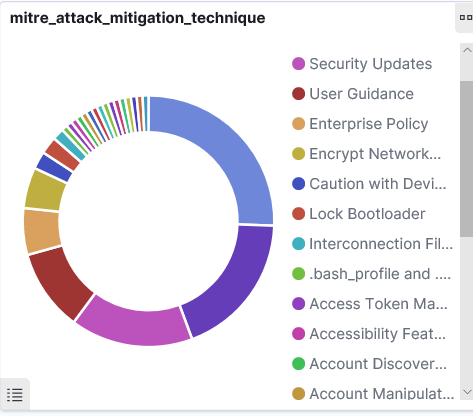
## mitre\_attack\_data\_sources\_techniques

该visualization的类型为Data Table,其作用是按照data\_sources分组，统计每个data\_sources有多少个不同的technique。其界面如下图所示：



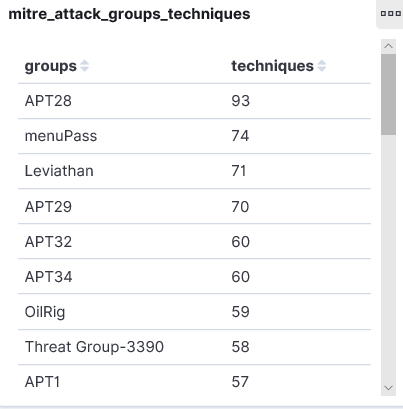
## mitre\_attack\_mitigation\_technique

该visualization的类型为Pie,其作用是按照mitigation分组，以饼图形式展现每个mitigation有多少个不同的technique以及所占百分比。其界面如下图所示：



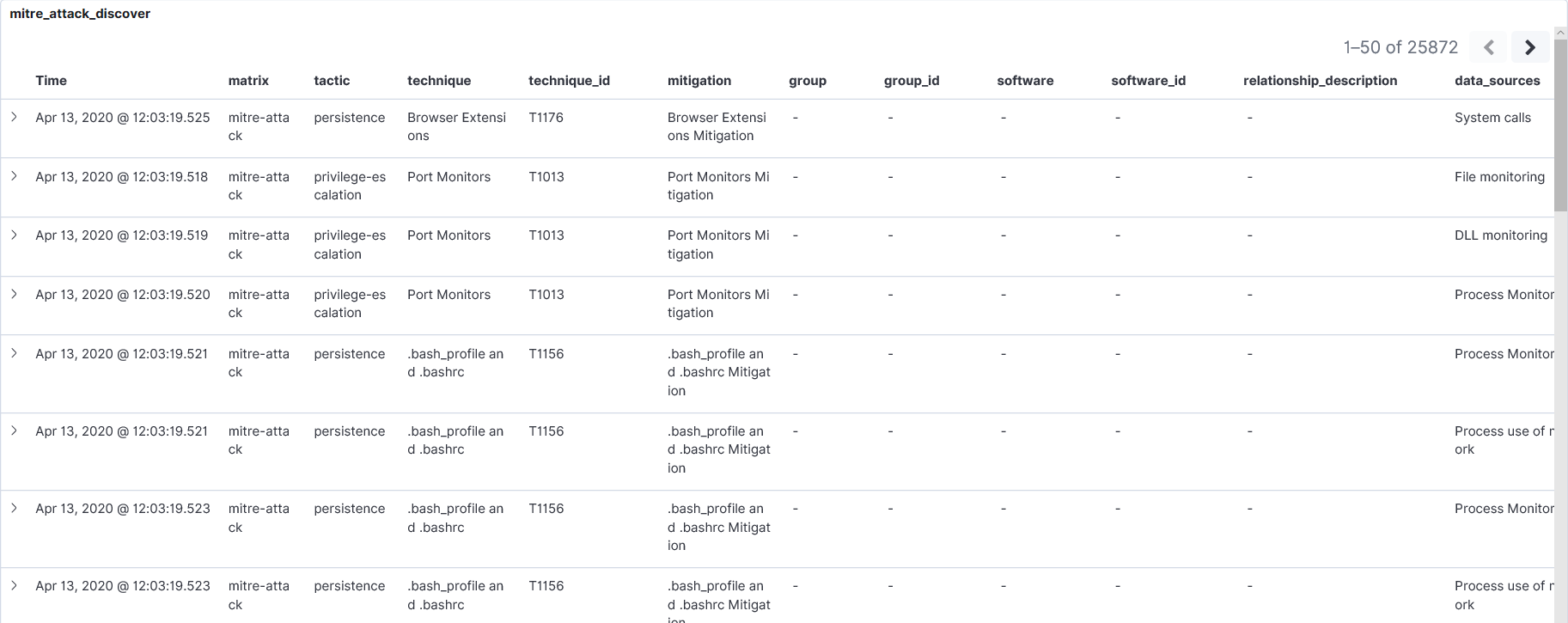
## mitre\_attack\_groups\_techniques

该visualization的类型为Data Table,其作用是按照group分组，统计每个group有多少个不同的technique。其界面如下图所示：



## mitre\_attack\_discover

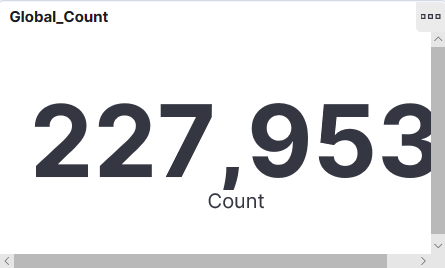
该visualization的类型为Search,其作用是从索引模式mitre-attack-\*中所有索引检索指定时间范围内的数据。其界面如下图所示：



# Global\_Dashboard

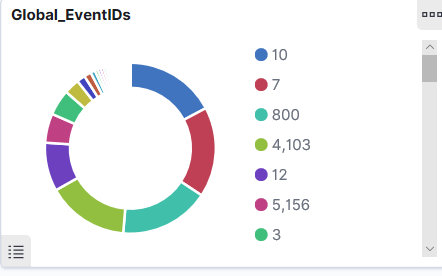
## Global\_Count

该visualization的类型为Metric,其作用是统计索引模式logs-\*中所有索引共多少条记录。其界面如下图所示：



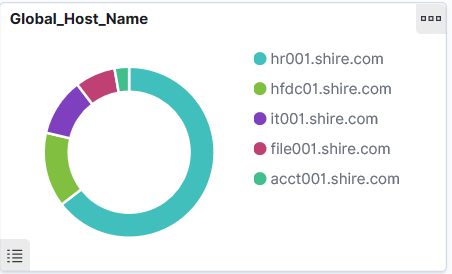
## Global\_EventIDs

该visualization的类型为Pie,其作用是按照event\_id分组，以饼图形式展现每个event\_id有多少条记录以及所占百分比。其界面如下图所示：



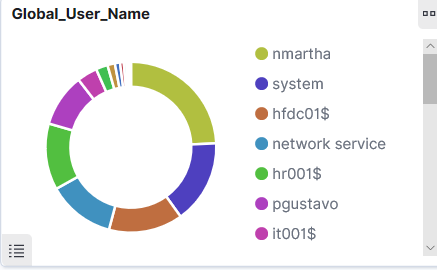
## Global\_Host\_Name

该visualization的类型为Pie,其作用是按照host\_name分组，以饼图形式展现每个host\_name有多少条记录以及所占百分比。其界面如下图所示：



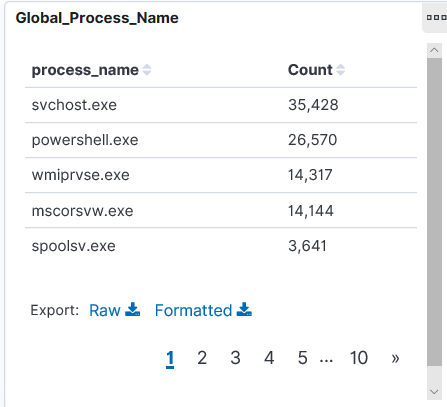
## Global\_User\_Name

该visualization的类型为Pie,其作用是按照user\_name分组，以饼图形式展现每个user\_name有多少条记录以及所占百分比 。其界面如下图所示：



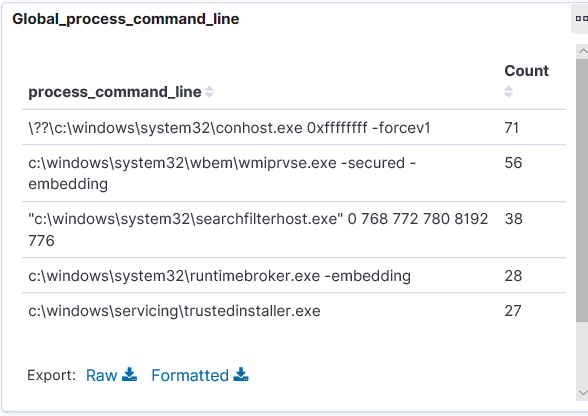
## Global\_Process\_Name

该visualization的类型为Data Table,其作用是按照process\_name分组，统计每个process\_name有多少条记录。其界面如下图所示：



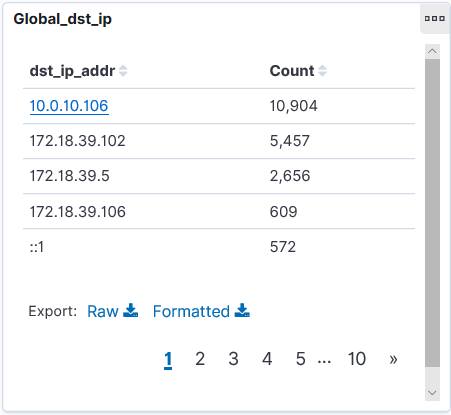
## Global\_process\_command\_line

该visualization的类型为Data Table,其作用是按照process\_command\_line分组，统计每个process\_command\_line有多少条记录。其界面如下图所示：



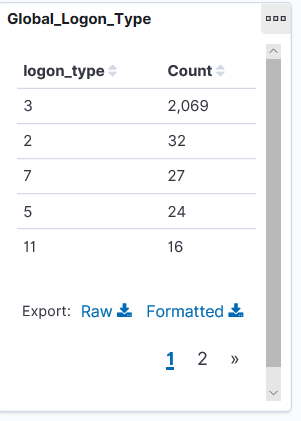
## Global\_dst\_ip

该visualization的类型为Data Table,其作用是按照dst\_ip\_addr分组，统计每个dst\_ip\_addr有多少条记录。其界面如下图所示：



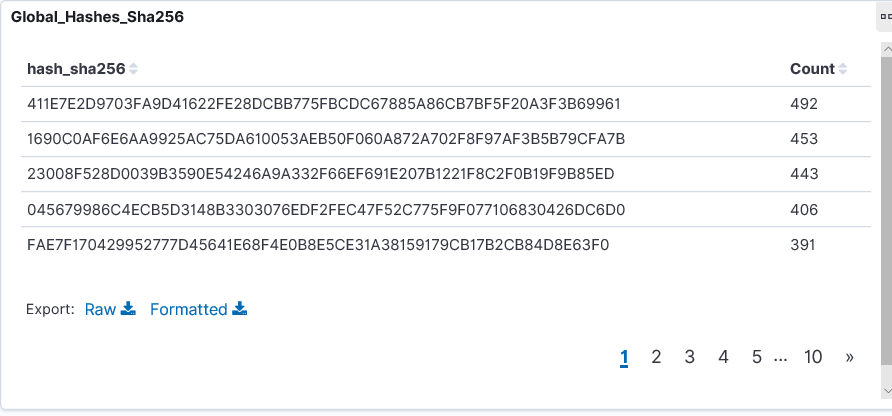
## Global\_Logon\_Type

该visualization的类型为Data Table,其作用是按照logon\_type分组，统计每个logon\_type有多少条记录。其界面如下图所示：



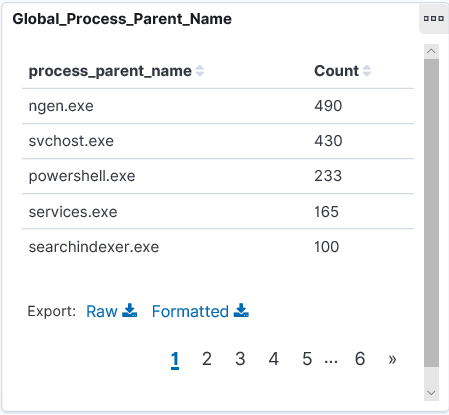
## Global\_Hashes\_Sha256

该visualization的类型为Data Table,其作用是按照hash\_sha256分组，统计每个hash\_sha256有多少条记录。其界面如下图所示：



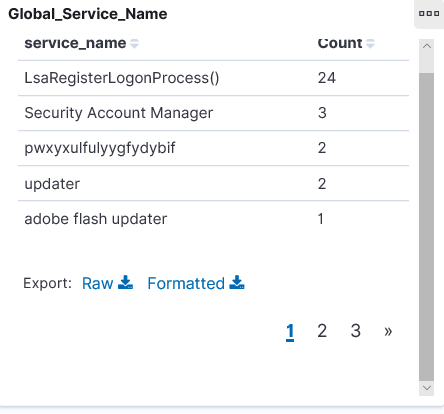
## Global\_Process\_Parent\_Name

该visualization的类型为Data Table,其作用是按照process\_parent\_name 分组，统计每个process\_parent\_name 有多少条记录。其界面如下图所示：



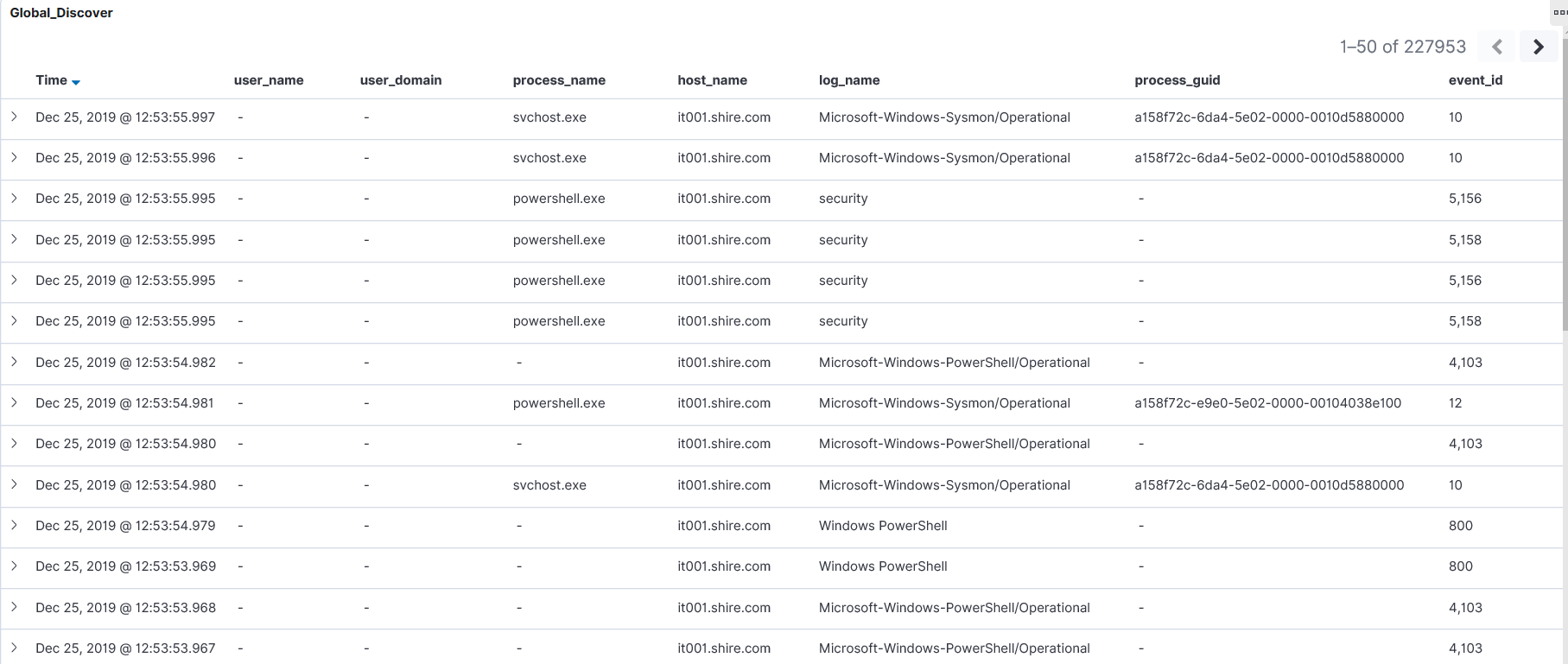
## Global\_Service\_Name

该visualization的类型为Data Table,其作用是按照service\_name分组，统计每个service\_name有多少条记录。其界面如下图所示：



## Global\_Discover

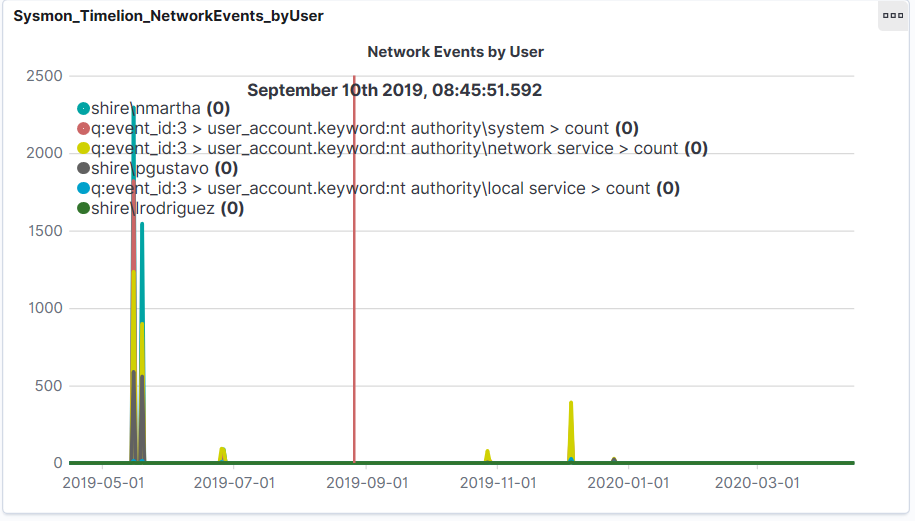
该visualization的类型为Search,其作用是从索引模式logs-\*中所有索引检索指定时间范围内的数据。其界面如下图所示：



# Host Investigation Dashboard

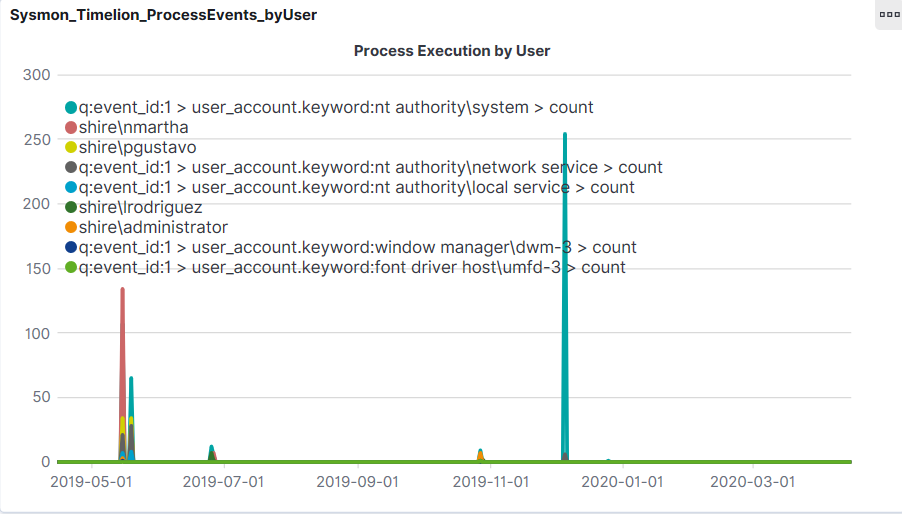
## Sysmon\_Timelion\_NetworkEvents\_byUser

该visualization的类型为Timelion,其作用是对索引logs-endpoint-winevent-sysmon\*中event\_id=3的事件，按照user\_account分组，并对每一个user\_account按照时间序列来显示其记录条数。其界面如下图所示：



## Sysmon\_Timelion\_ProcessEvents\_byUser

该visualization的类型为Timelion,其作用是对索引logs-endpoint-winevent-sysmon\*中event\_id=1的事件，按照user\_account分组，并对每一个user\_account按照时间序列来显示其记录条数。其界面如下图所示：



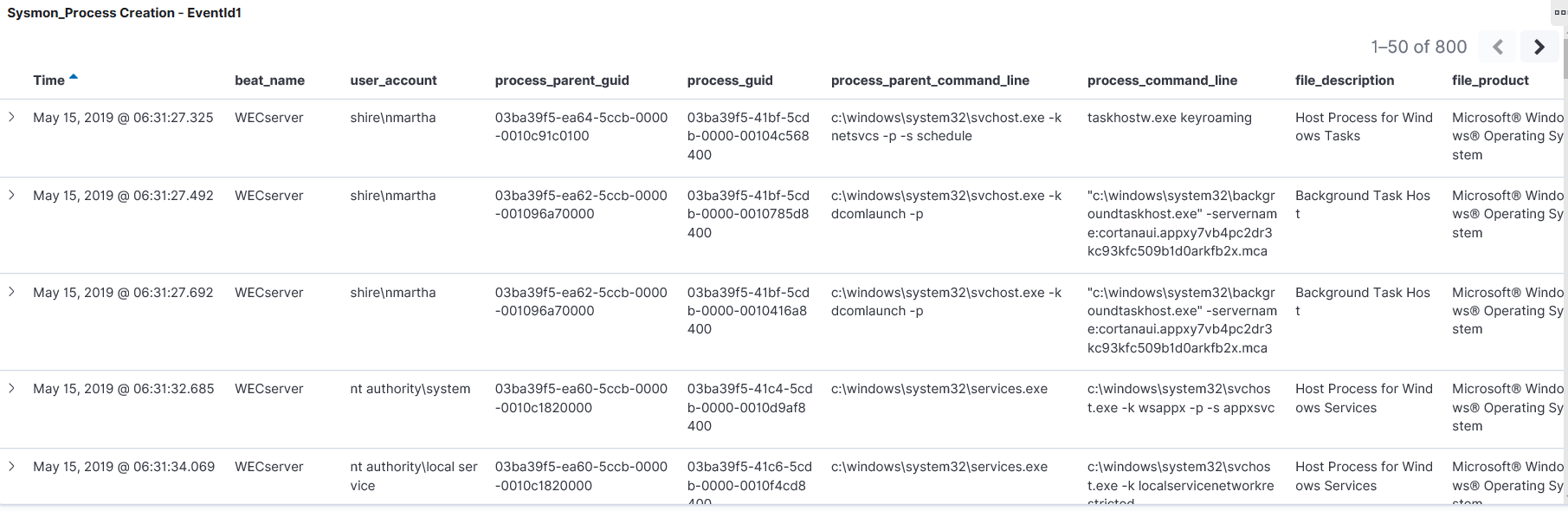
## Sysmon\_ExecutedCommands

该visualization的类型为Search,其作用是检索执行命令的事件，查询语句为：event\_id:1 AND (process\_parent\_name:\"CmD.exe\" OR process\_parent\_name:\"powershell.exe\" OR process\_parent\_name:\"wscript.exe\" OR process\_parent\_name:\"cscript.exe\")。其界面如下图所示：



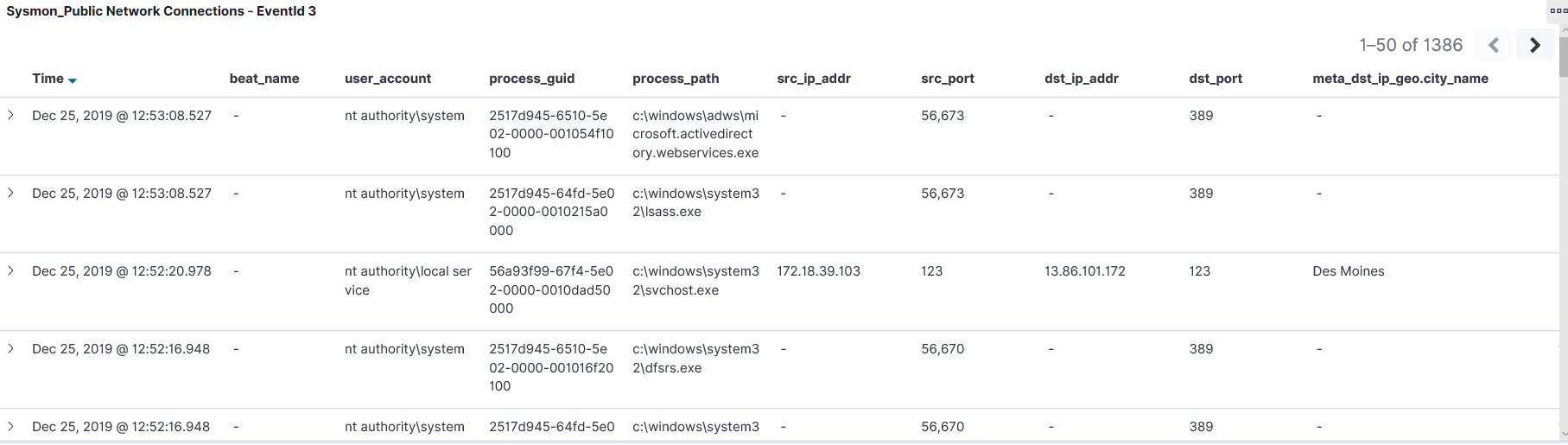
## Sysmon\_Process Creation - EventId1

该visualization的类型为Search,其作用是检索进程创建事件，查询语句为：event\_id:1。其界面如下图所示：



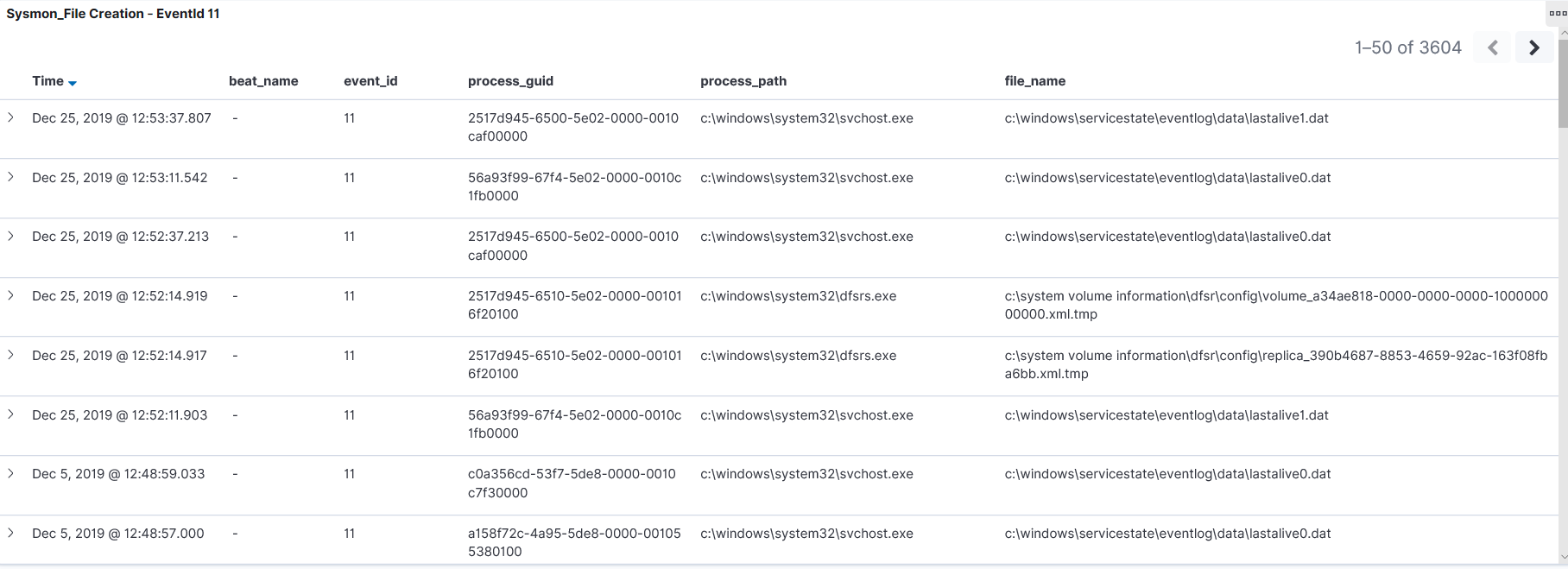
## Sysmon\_Public Network Connections - EventId 3

该visualization的类型为Search,其作用是检索连接外部网络事件，查询语句为：event\_id:3 AND (NOT dst\_ip\_addr: \"127.0.0.1\" AND NOT dst\_ip\_addr:[10.0.0.0 TO 10.255.255.255] AND NOT dst\_ip\_addr:[192.168.0.0 TO 192.168.255.255] AND NOT dst\_ip\_addr:[172.16.0.0 TO 172.31.255.255])。其界面如下图所示：



## Sysmon\_File Creation - EventId 11

该visualization的类型为Search,其作用是检索文件创建事件，查询语句为：event\_id:11。其界面如下图所示：



## Sysmon\_Downloads-EventId 15

该visualization的类型为Search,其作用是检索文件下载事件，查询语句为：source\_name: \"Microsoft-Windows-Sysmon\" AND event\_id:15。其界面如下图所示：



## Sysmon\_Registry Events

该visualization的类型为Search,其作用是检索注册表事件，查询语句为：event\_id:12 OR event\_id:13 OR event\_id:14。其界面如下图所示：



## Sysmon\_WMI Subscription Events

该visualization的类型为Search,其作用是检索WMI订阅事件，查询语句为：source\_name: \"Microsoft-Windows-Sysmon\" AND (event\_id:19 OR event\_id:20 OR event\_id:21)。其界面如下图所示：



## windows\_login\_events

该visualization的类型为Search,其作用是检索登录事件，查询语句为：source\_name: \"Microsoft-Windows-Security-Auditing\" AND (event\_id:[4624 TO 4625] OR event\_id:4634)。其界面如下图所示：



## Sysmon\_Invalid Drivers

该visualization的类型为Search,其作用是检索驱动程序加载事件，查询语句为：event\_id: 6

## Sysmon\_Private Network Connections - EventId 3

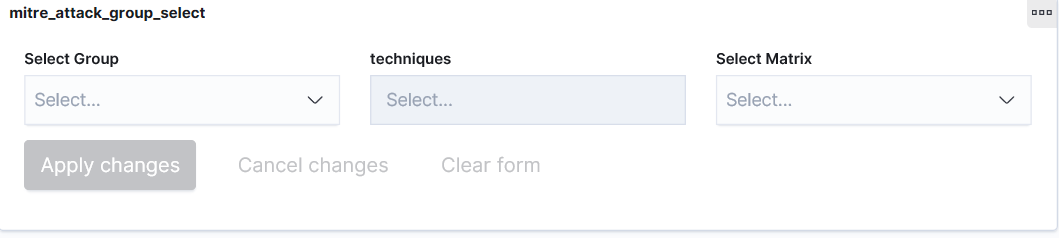
该visualization的类型为Search,其作用是检索连接局域网事件，查询语句为：event\_id:3 AND (dst\_ip\_addr:[10.0.0.0 TO 10.255.255.255] OR dst\_ip\_addr:[192.168.0.0 TO 192.168.255.255] OR dst\_ip\_addr:[172.16.0.0 TO 172.31.255.255])。其界面如下图所示：



# MITRE-ATTACK-GROUPS

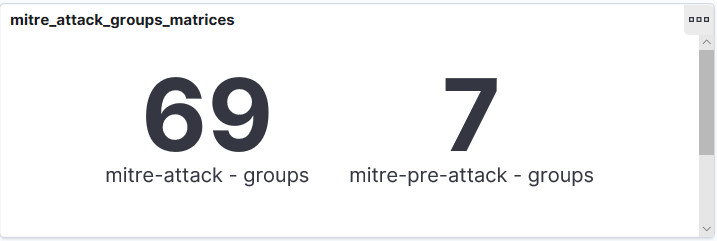
## mitre\_attack\_group\_select

该visualization的类型为Controls,其作用是指定group、techniques或者Matrix为某个特定的值来为整个MITRE-ATTACK-GROUPS dashboard过滤数据。其界面如下图所示：



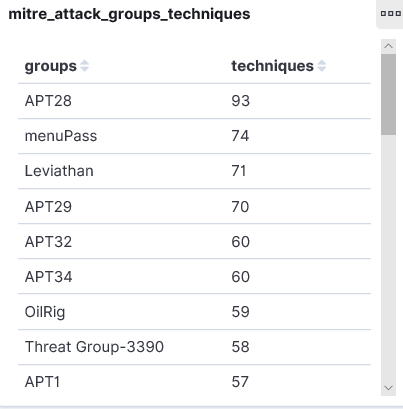
## mitre\_attack\_groups\_matrices

该visualization的类型为Metric,其作用是按照matrix分组，统计每个matrix有多少个不同的group。其界面如下图所示：



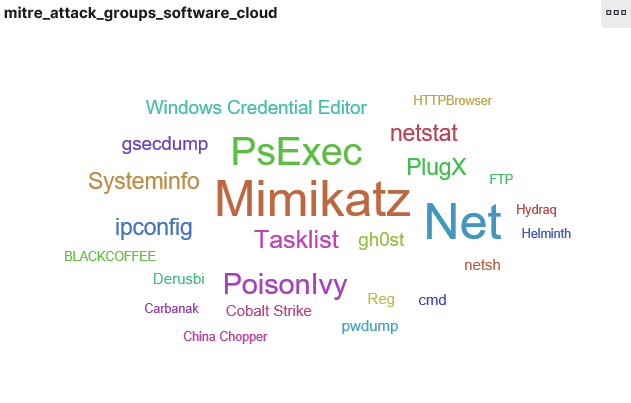
## mitre\_attack\_groups\_techniques

该visualization的类型为Data Table,其作用是按照group分组，统计每个group有多少个不同的technique。其界面如下图所示：



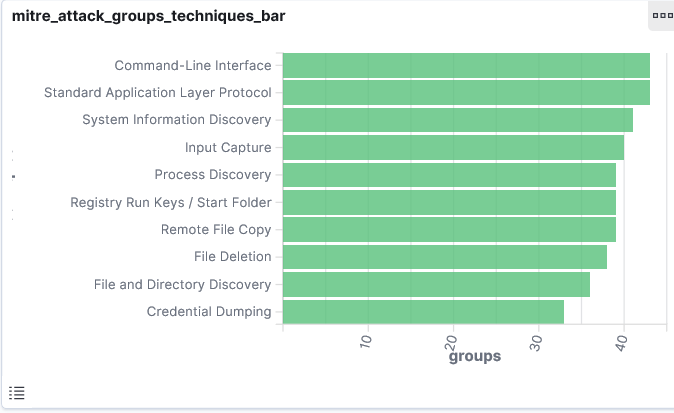
## mitre\_attack\_groups\_software\_cloud

该visualization的类型为Tag Cloud,其作用是按照software分组，统计每个software有多少个不同的group，将group数量多的software突出显示。其界面如下图所示：



## mitre\_attack\_groups\_techniques\_bar

该visualization的类型为Horizontal Bar,其作用是按照techniques分组，统计每个techniques有多少个不同的group。其界面如下图所示：



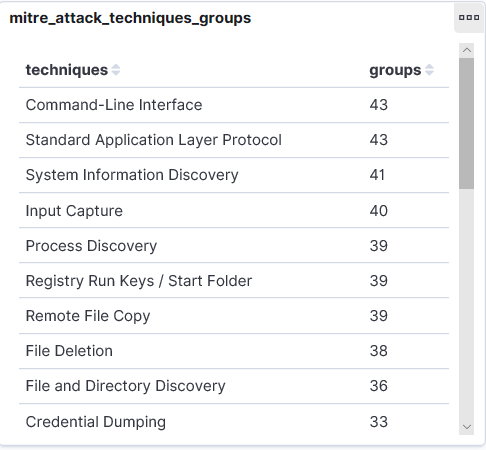
## mitre\_attack\_groups\_tactics

该visualization的类型为Data Table,其作用是按照tactic分组，统计每个tactic有多少个不同的group。其界面如下图所示：



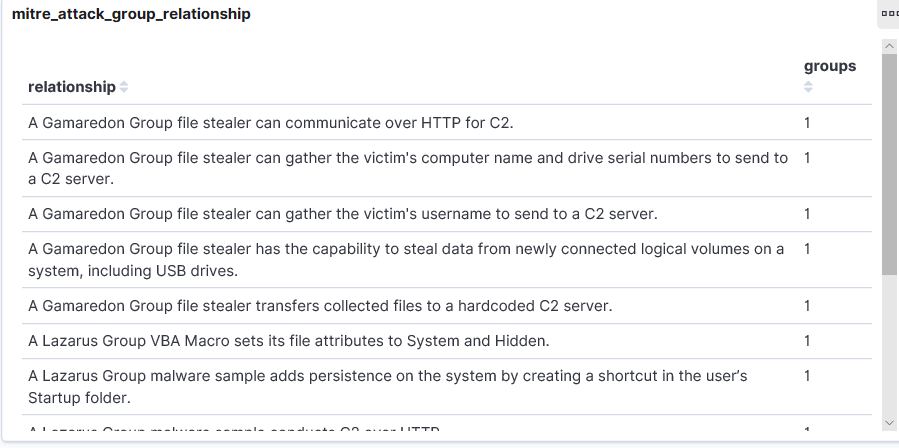
## mitre\_attack\_techniques\_groups

该visualization的类型为Data Table,其作用是按照technique分组，统计每个technique有多少个不同的group。其界面如下图所示：



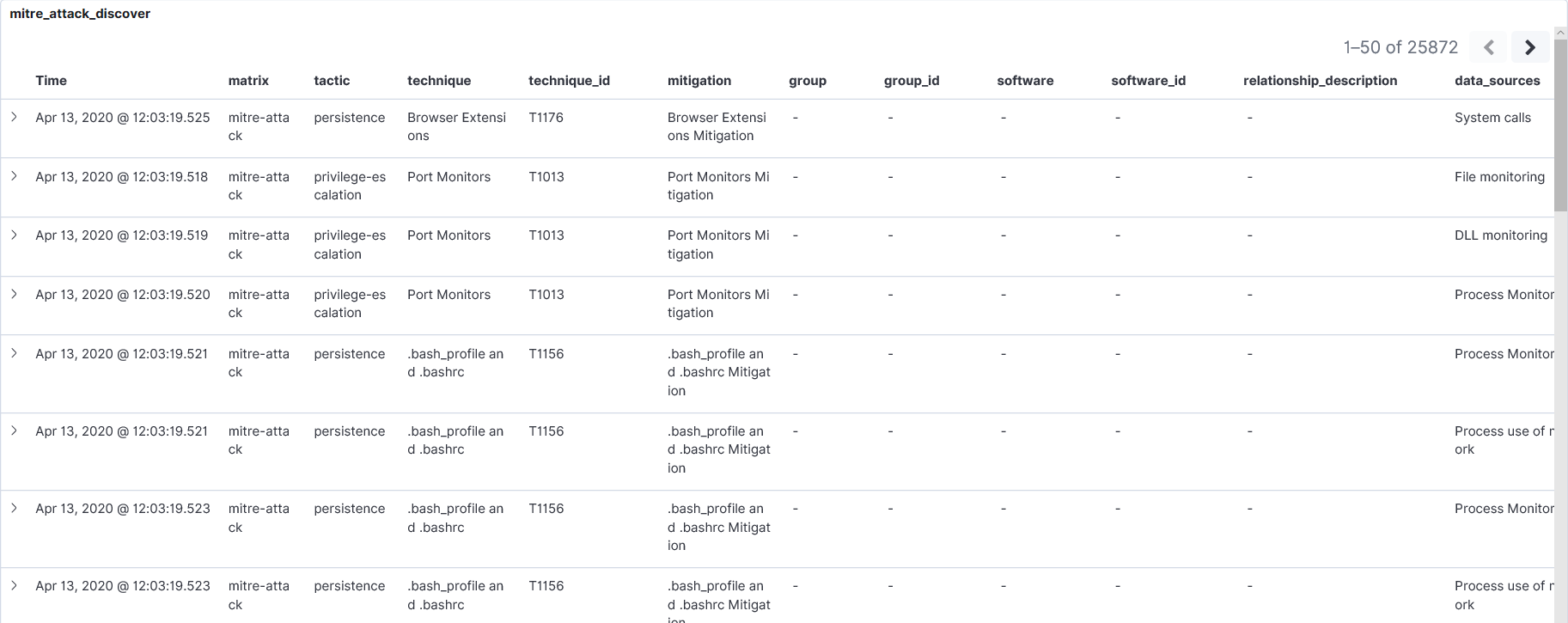
## mitre\_attack\_group\_relationship

该visualization的类型为Data Table,其作用是按照relationship分组，统计每个relationship有多少个不同的group。其界面如下图所示：



## mitre\_attack\_discover

该visualization的类型为Search,其作用是从索引模式mitre-attack-\*中所有索引检索指定时间范围内的数据。其界面如下图所示：



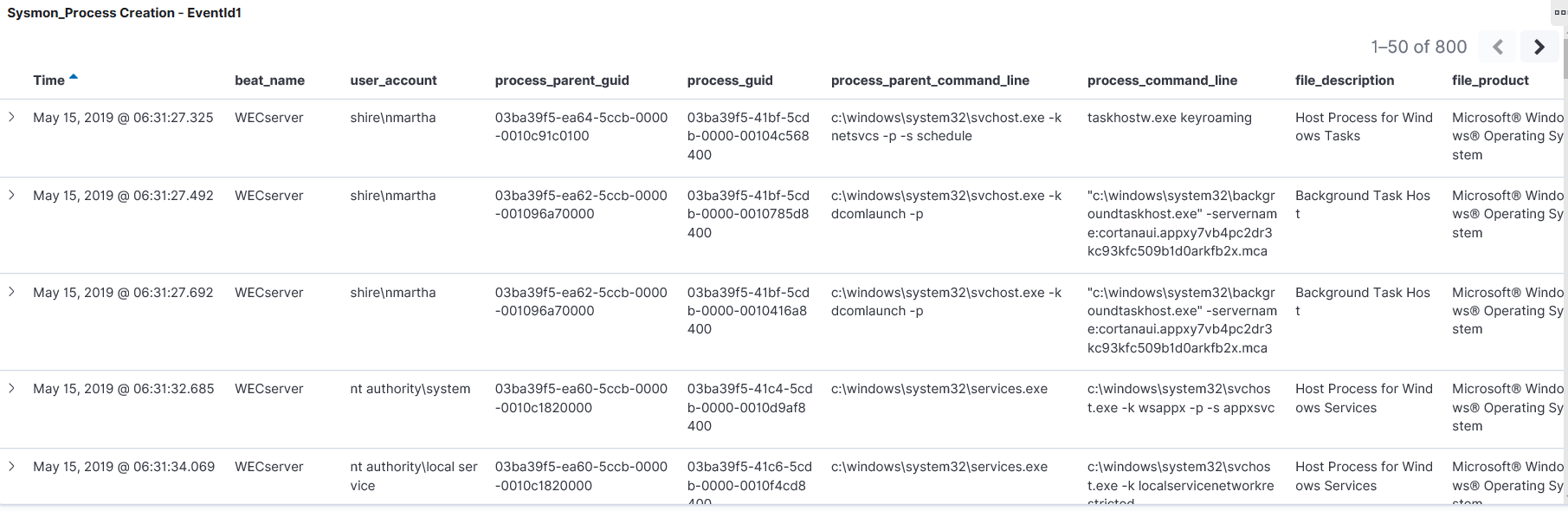
# Process Investigation

## Sysmon\_Timelion\_ProcessEvents\_byProcessGuid

该visualization的类型为Timelion,其作用是对索引logs-endpoint-winevent-sysmon\*中的事件，按照process\_guid分组，并对每一个process\_guid按照时间序列来显示其记录条数

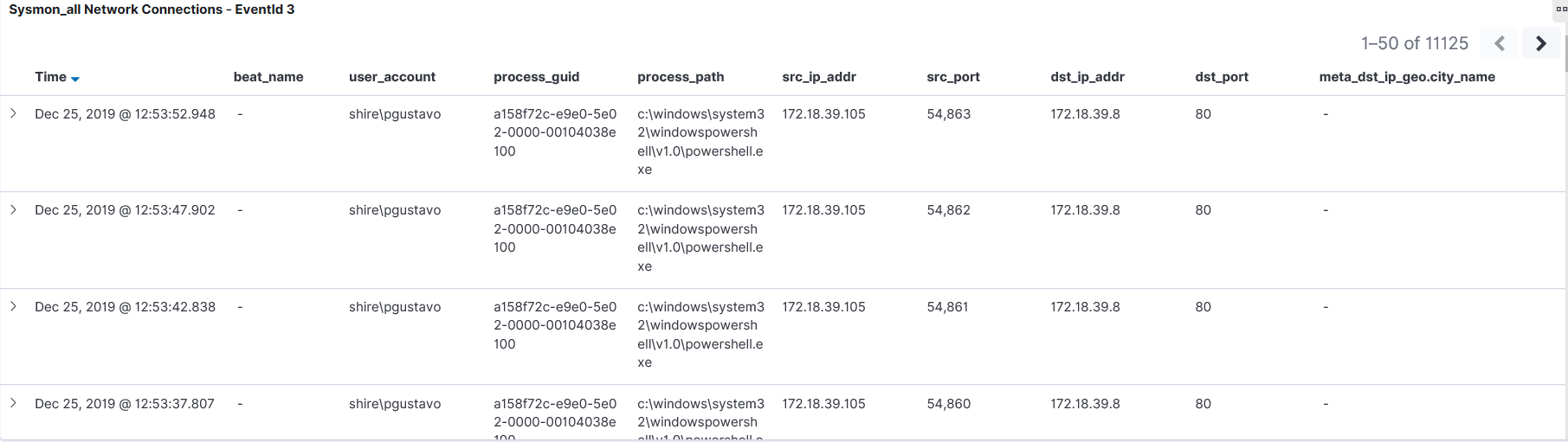
## Sysmon\_Process Creation - EventId1

该visualization的类型为Search,其作用是检索进程创建事件，查询语句为：event\_id:1。其界面如下图所示：



## Sysmon\_all Network Connections - EventId 3

该visualization的类型为Search,其作用是检索网络连接事件，查询语句为：event\_id:3。其界面如下图所示：



## Sysmon\_Downloads-EventId 15

该visualization的类型为Search,其作用是检索文件下载事件，查询语句为：source\_name: \"Microsoft-Windows-Sysmon\" AND event\_id:15。其界面如下图所示：



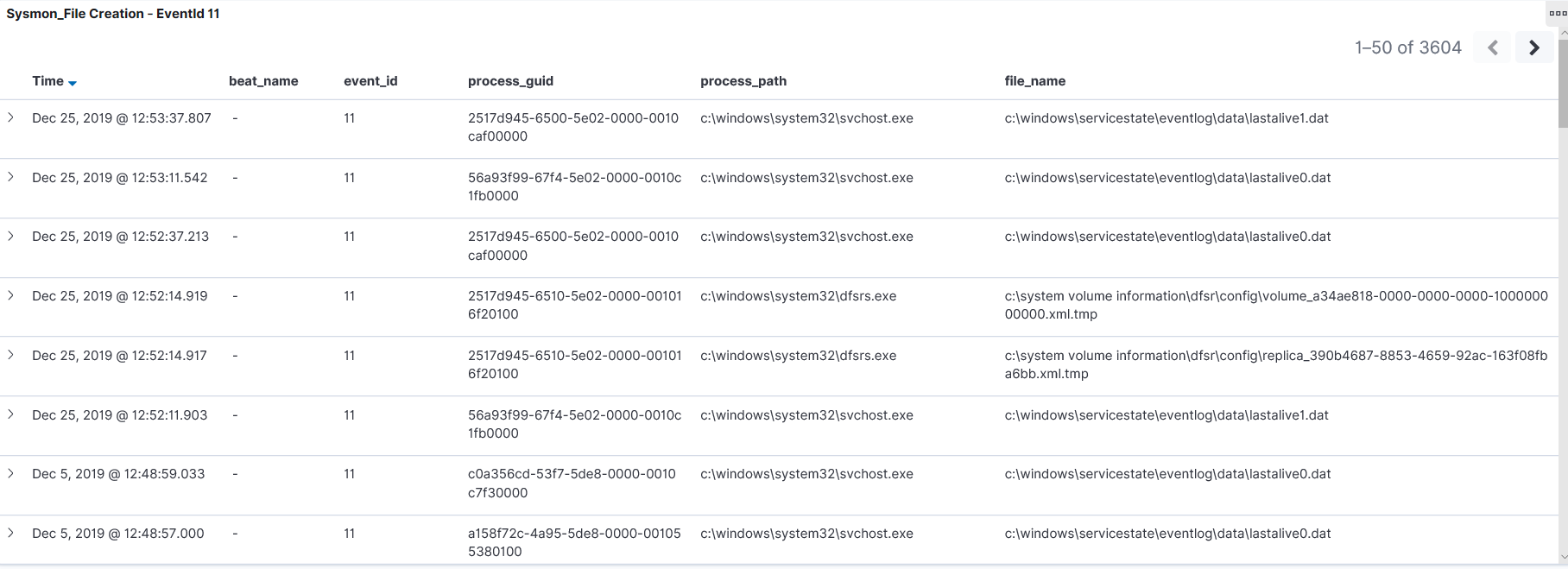
## Sysmon\_Registry Events

该visualization的类型为Search,其作用是检索注册表事件，查询语句为：event\_id:12 OR event\_id:13 OR event\_id:14。其界面如下图所示：



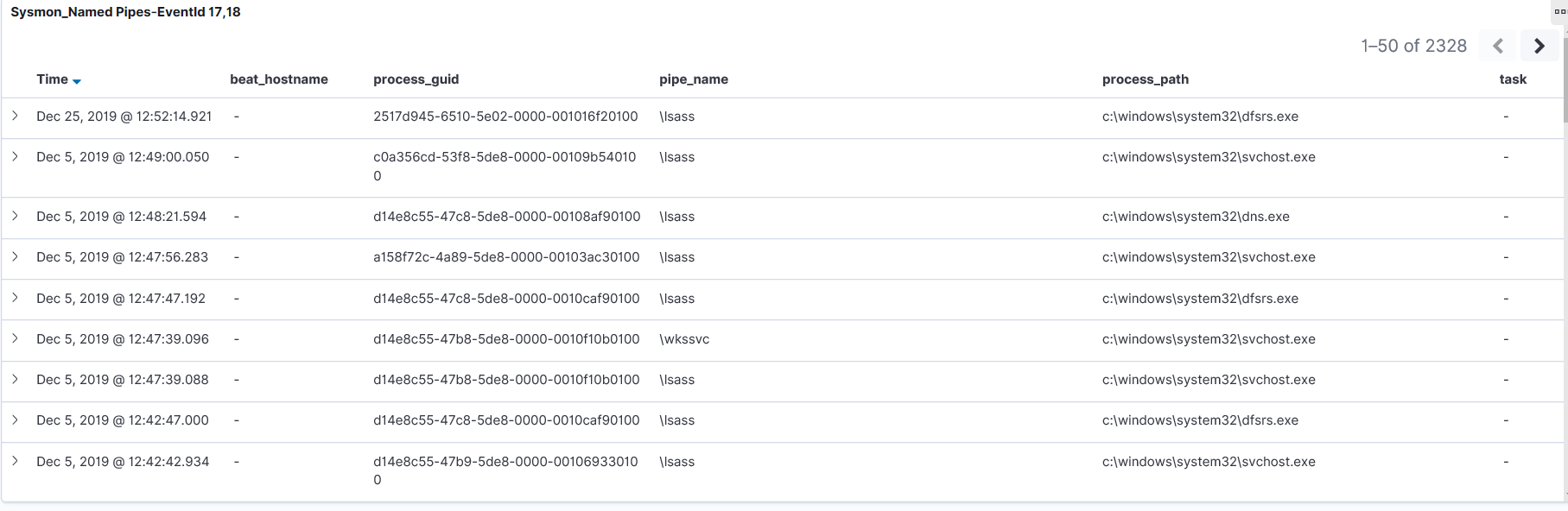
## Sysmon\_File Creation - EventId 11

该visualization的类型为Search,其作用是检索文件创建事件，查询语句为：event\_id:11。其界面如下图所示：



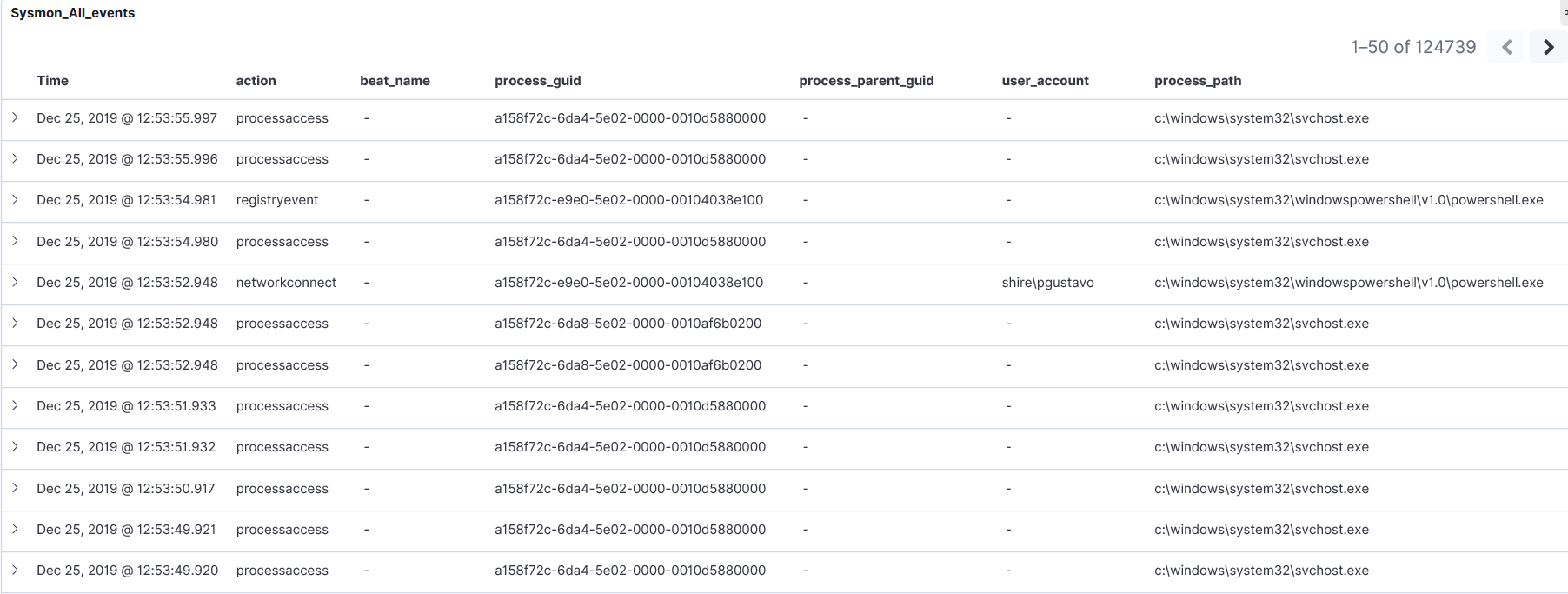
## Sysmon\_Named Pipes-EventId 17,18

该visualization的类型为Search,其作用是检索命名管道创建或者连接事件，查询语句为：event\_id:17 OR event\_id:18。其界面如下图所示：



## Sysmon\_All\_events

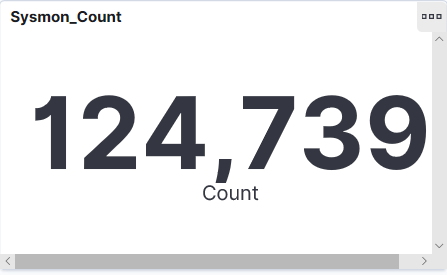
该visualization的类型为Search,其作用是检索索引模式logs-endpoint-winevent-sysmon-\*中所有索引的数据。其界面如下图所示：



# Sysmon\_Dashboard

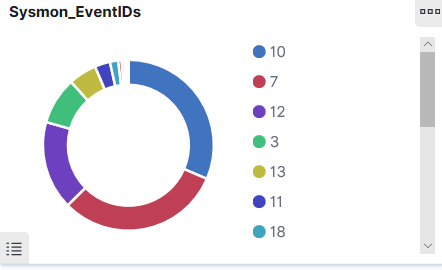
## Sysmon\_Count

该visualization的类型为Metric,其作用是统计索引模式logs-endpoint-winevent-sysmon-\*中所有索引共有多少条记录。其界面如下图所示：



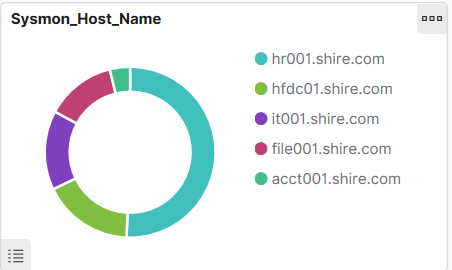
## Sysmon\_EventIDs

该visualization的类型为Pie,其作用是按照event\_id分组，以饼图形式展现每个event\_id有多少条记录以及所占百分比。其界面如下图所示：



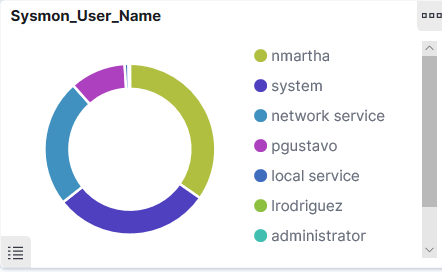
## Sysmon\_Host\_Name

该visualization的类型为Pie,其作用是按照host\_name分组，以饼图形式展现每个host\_name有多少条记录以及所占百分比。其界面如下图所示：



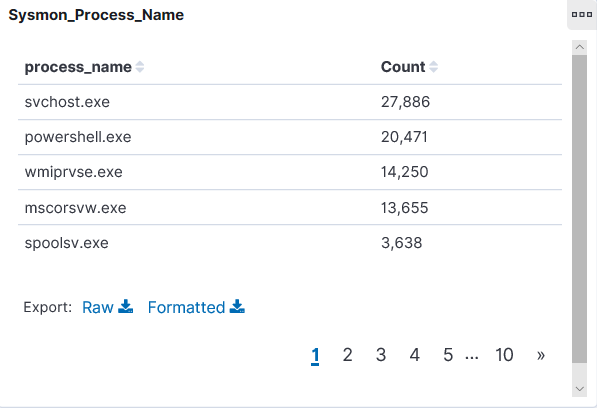
## Sysmon\_User\_Name

该visualization的类型为Pie,其作用是按照user\_name分组，以饼图形式展现每个user\_name有多少条记录以及所占百分比。其界面如下图所示：



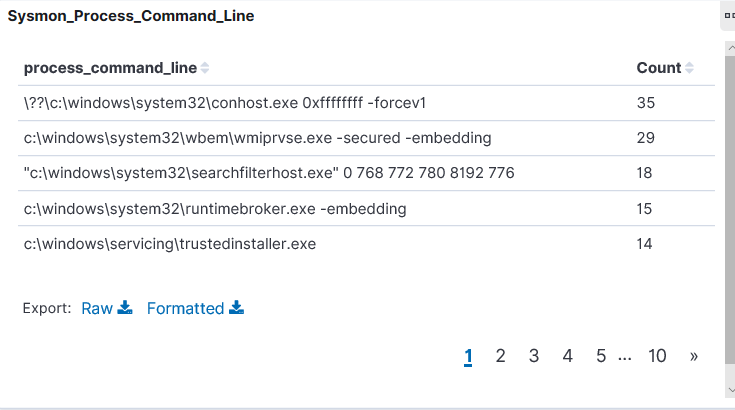
## Sysmon\_Process\_Name

该visualization的类型为Data Table,其作用是按照process\_name分组，统计每个process\_name有多少条记录。其界面如下图所示：



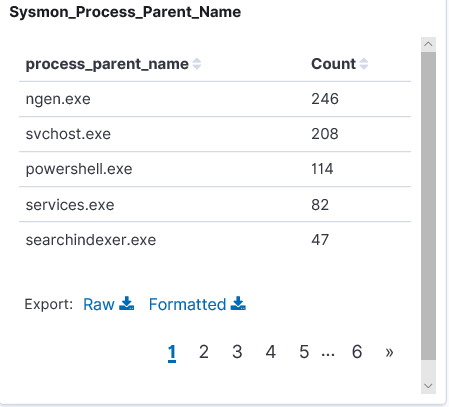
## Sysmon\_Process\_Command\_Line

该visualization的类型为Data Table,其作用是按照process\_command\_line分组，统计每个process\_command\_line有多少条记录。其界面如下图所示：



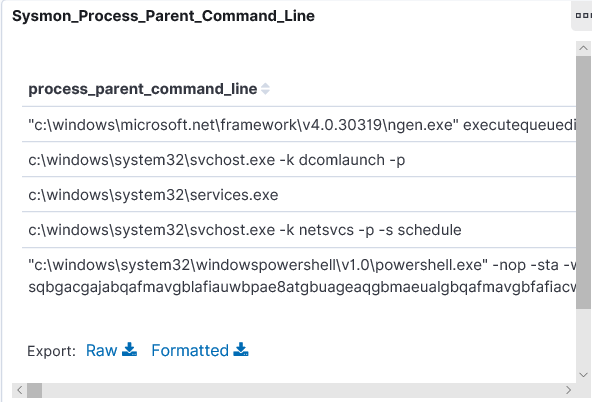
## Sysmon\_Process\_Parent\_Name

该visualization的类型为Data Table,其作用是按照process\_parent\_name分组，统计每个process\_parent\_name有多少条记录。其界面如下图所示：



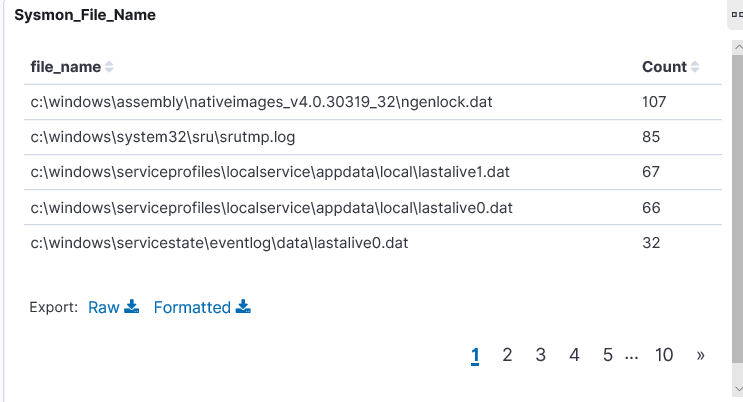
## Sysmon\_Process\_Parent\_Command\_Line

该visualization的类型为Data Table,其作用是按照process\_parent\_command\_line 分组，统计每个process\_parent\_command\_line 有多少条记录。其界面如下图所示：



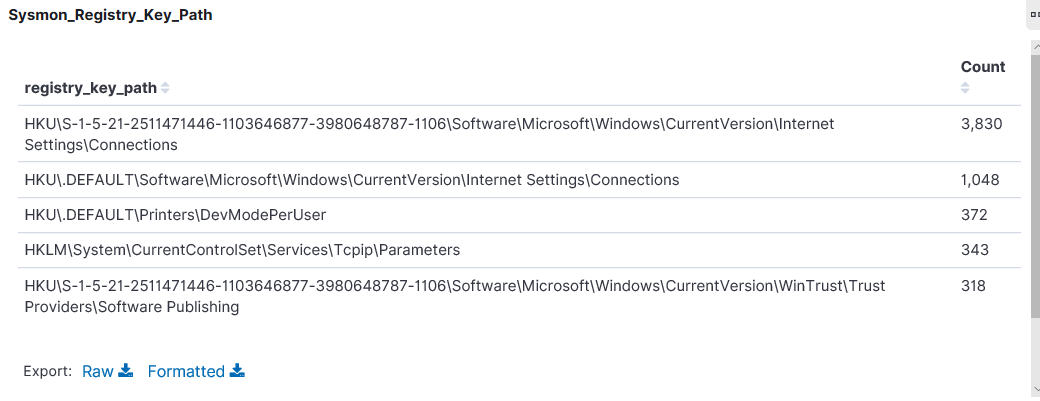
## Sysmon\_File\_Name

该visualization的类型为Data Table,其作用是按照file\_name分组，统计每个file\_name有多少条记录。其界面如下图所示：



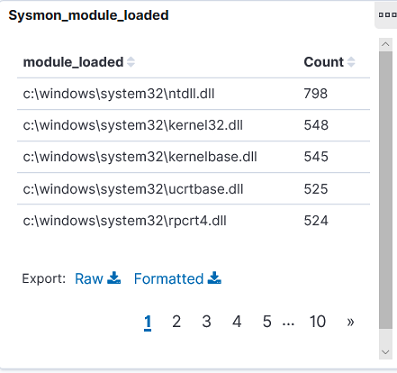
## Sysmon\_Registry\_Key\_Path

该visualization的类型为Data Table,其作用是按照registry\_key\_path分组，统计每个registry\_key\_path有多少条记录。其界面如下图所示：



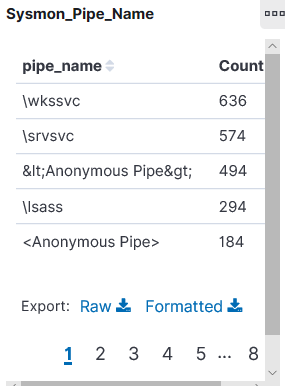
## Sysmon\_module\_loaded

该visualization的类型为Data Table,其作用是按照module\_loaded分组，统计每个module\_loaded有多少条记录。其界面如下图所示：



## Sysmon\_Pipe\_Name

该visualization的类型为Data Table,其作用是按照pipe\_name分组，统计每个pipe\_name有多少条记录。其界面如下图所示：



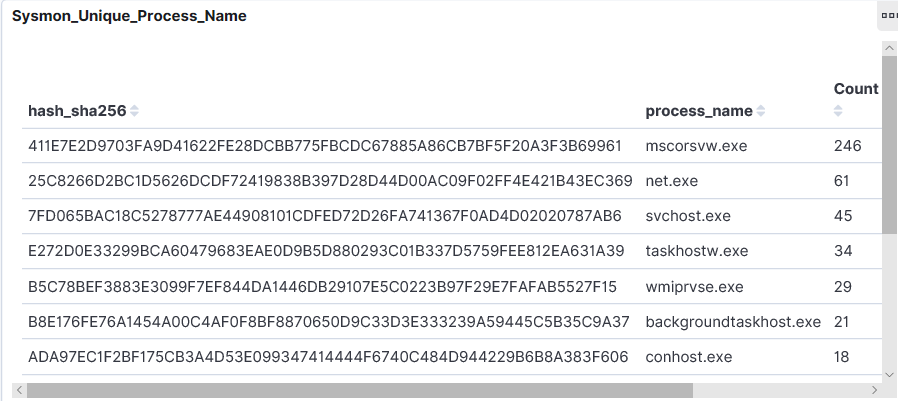
## Sysmon\_Unique\_module\_loaded

该visualization的类型为Data Table,其作用是按照hash\_sha256, module\_loaded分组， 计算每个分组有多少条记录、多少个不同的module\_loaded、多少个不同的host\_name。其界面如下图所示：



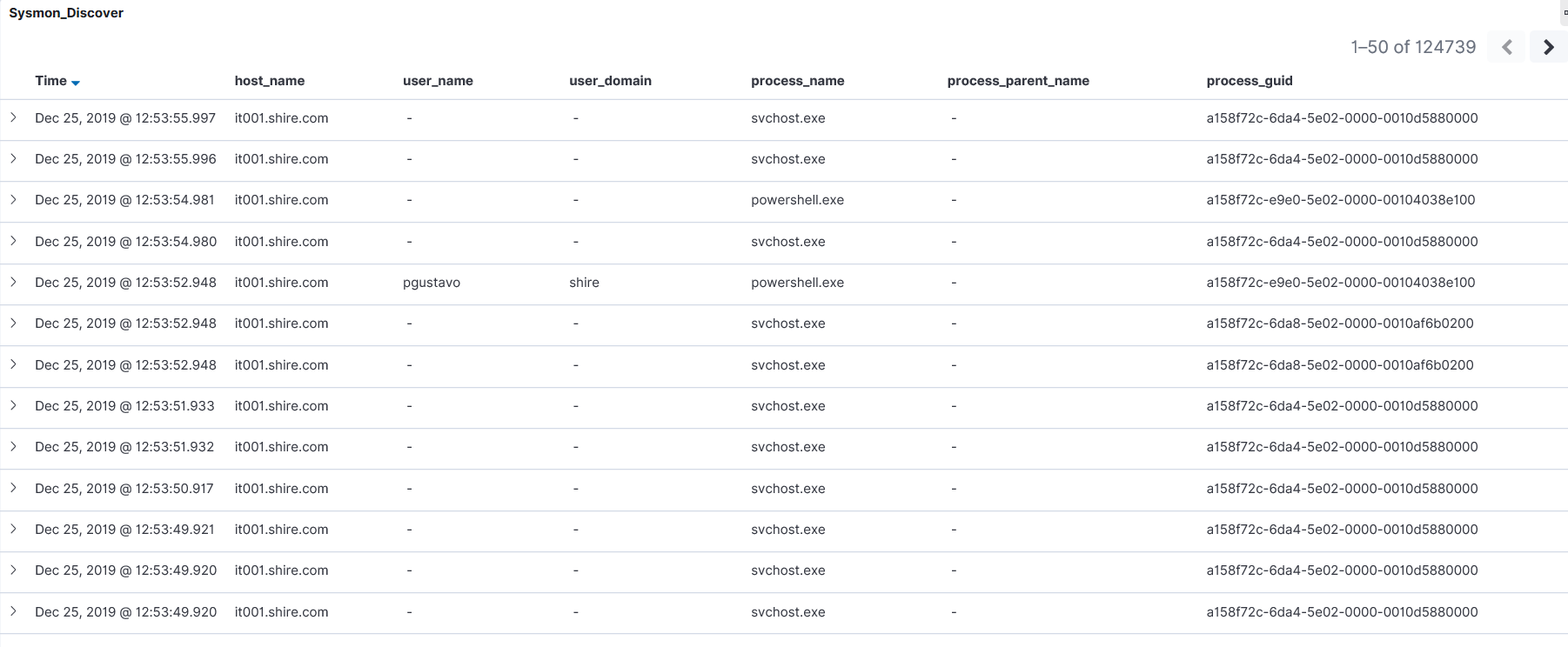
## Sysmon\_Unique\_Process\_Name

该visualization的类型为Data Table,其作用是按照hash\_sha256, process\_name分组， 计算每个分组有多少条记录、多少个不同的process\_name、多少个不同的host\_name。其界面如下图所示：



## Sysmon\_Discover

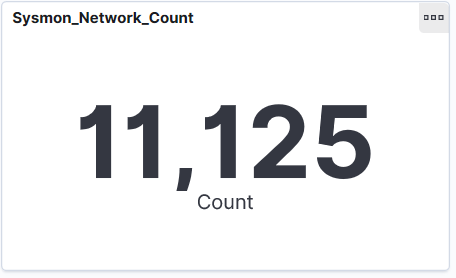
该visualization的类型为Data Table,其作用是检索索引模式logs-endpoint-winevent-sysmon-\*中所有索引的记录。其界面如下图所示：



# Sysmon\_Network\_Dashboard

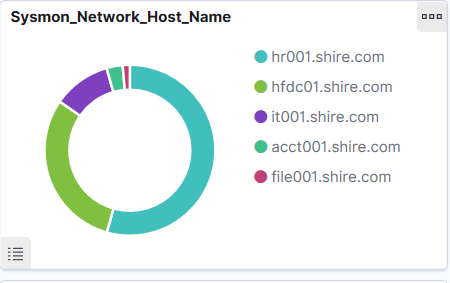
## Sysmon\_Network\_Count

该visualization的类型为Metric,其作用是统计索引模式logs-endpoint-winevent-sysmon-\*中所有索引的event\_id=3的记录的数量。其界面如下图所示：



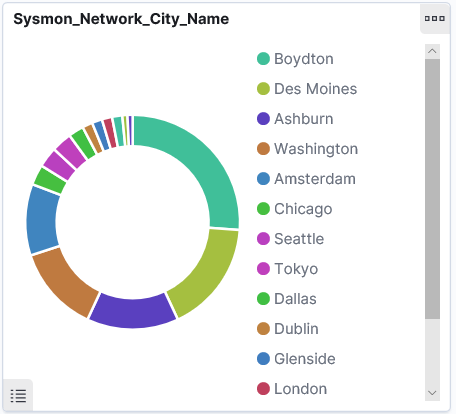
## Sysmon\_Network\_Host\_Name

该visualization的类型为Pie,其作用是对event\_id=3的记录，按照host\_name分组，以饼图形式展现每个host\_name有多少条记录以及所占百分比。其界面如下图所示：



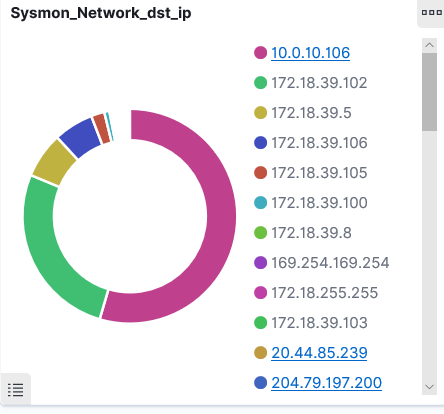
## Sysmon\_Network\_City\_Name

该visualization的类型为Pie,其作用是对event\_id=3的记录，按照meta\_dst\_ip\_geo分组， 以饼图形式展现每个meta\_dst\_ip\_geo有多少条记录以及所占百分比。其界面如下图所示：



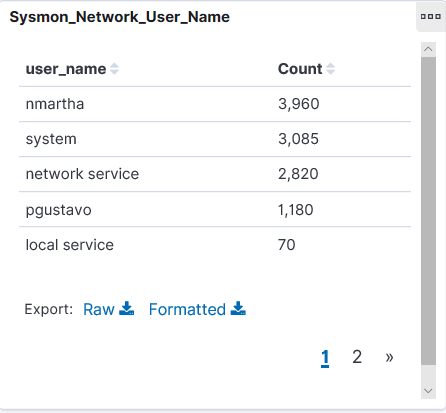
## Sysmon\_Network\_dst\_ip

该visualization的类型为Pie,其作用是对event\_id=3的记录，按照dst\_ip\_addr分组， 以饼图形式展现每个dst\_ip\_addr有多少条记录以及所占百分比。其界面如下图所示：



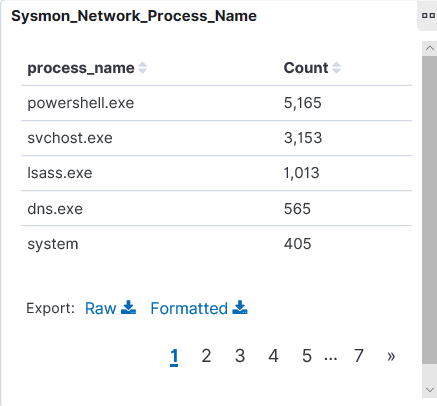
## Sysmon\_Network\_User\_Name

该visualization的类型为Data Table,其作用是对event\_id=3的记录，按照user\_name分组， 统计每个user\_name有多少条记录。其界面如下图所示：



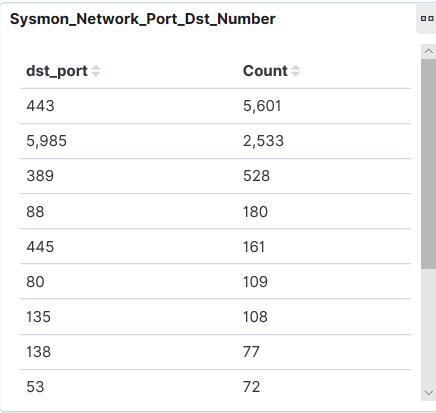
## Sysmon\_Network\_Process\_Name

该visualization的类型为Data Table,其作用是对event\_id=3的记录，按照process\_name分组， 统计每个process\_name有多少条记录。其界面如下图所示：



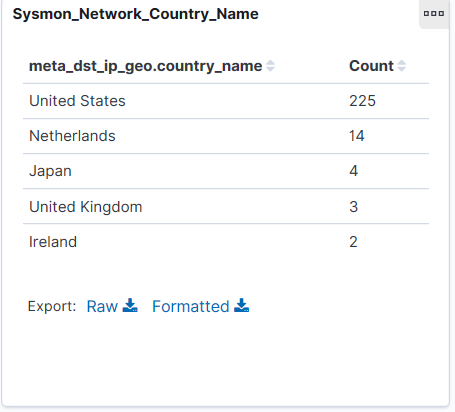
## Sysmon\_Network\_Port\_Dst\_Number

该visualization的类型为Data Table,其作用是对event\_id=3的记录，按照dst\_port分组， 统计每个dst\_port有多少条记录。其界面如下图所示：



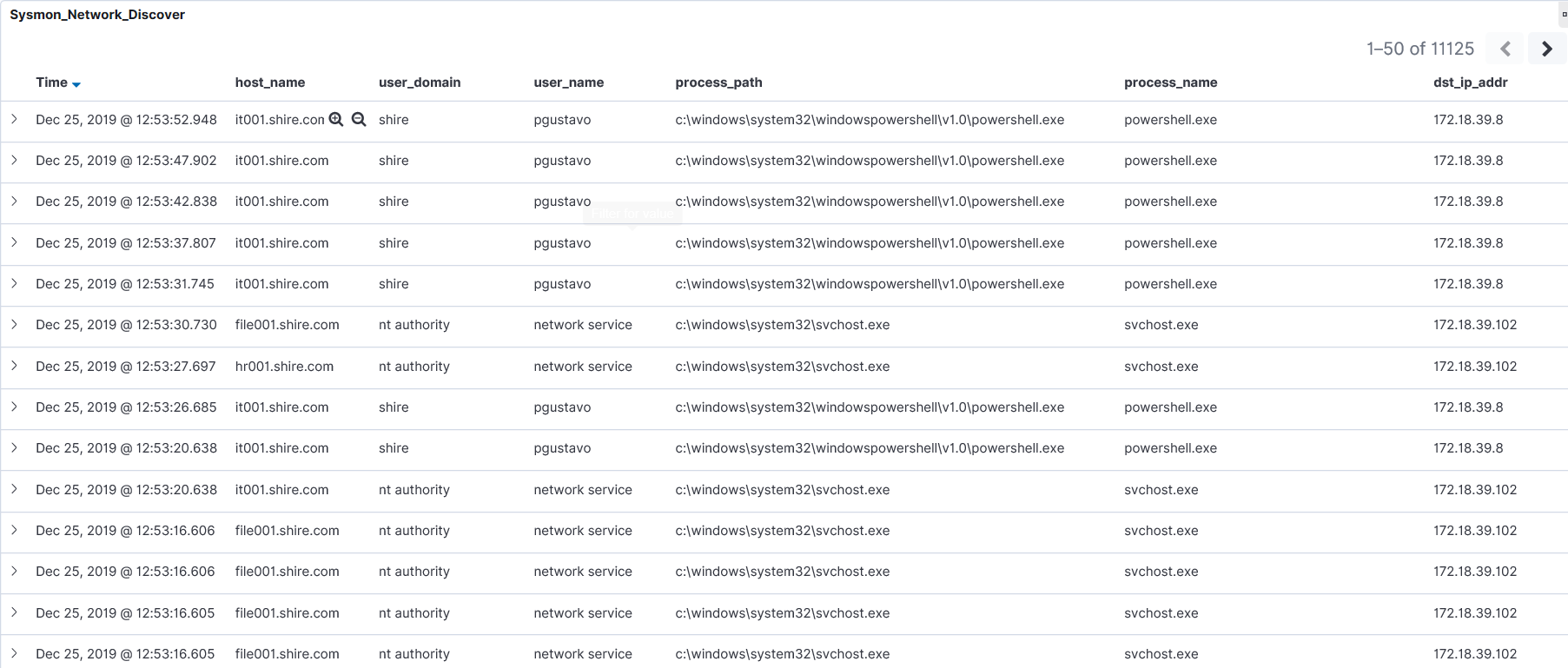
## Sysmon\_Network\_Country\_Name

该visualization的类型为Data Table,其作用是对event\_id=3的记录，按照meta\_dst\_ip\_geo.country\_name分组， 统计每个meta\_dst\_ip\_geo.country\_name有多少条记录。其界面如下图所示：



## Sysmon\_Network\_Discover

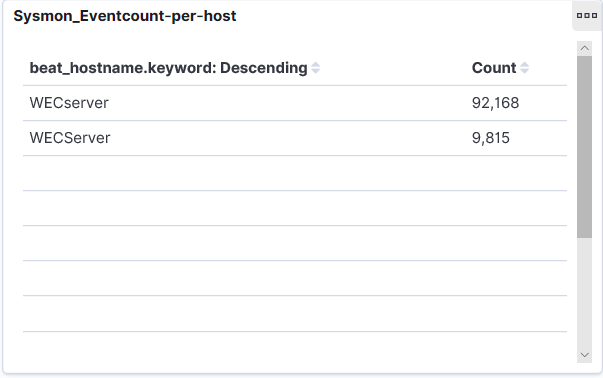
该visualization的类型为Search,其作用是检索索引模式logs-endpoint-winevent-sysmon-\*中所有索引的event\_id=3的记录。其界面如下图所示：



# User Investigation Dashboard

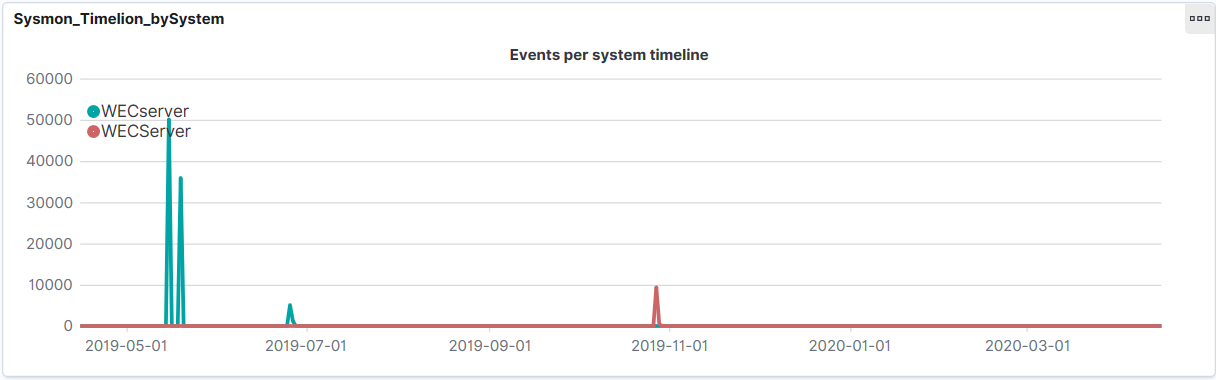
## Sysmon\_Eventcount-per-host

该visualization的类型为Data Table,其作用是按照beat\_hostname分组，统计每个beat\_hostname有多少条记录。其界面如下图所示：



## Sysmon\_Timelion\_bySystem

该visualization的类型为Timelion,其作用是对索引logs-endpoint-winevent-sysmon\*中的事件，按照beat\_hostname分组，并对每一个beat\_hostname按照时间序列来显示其记录条数。其界面如下图所示：



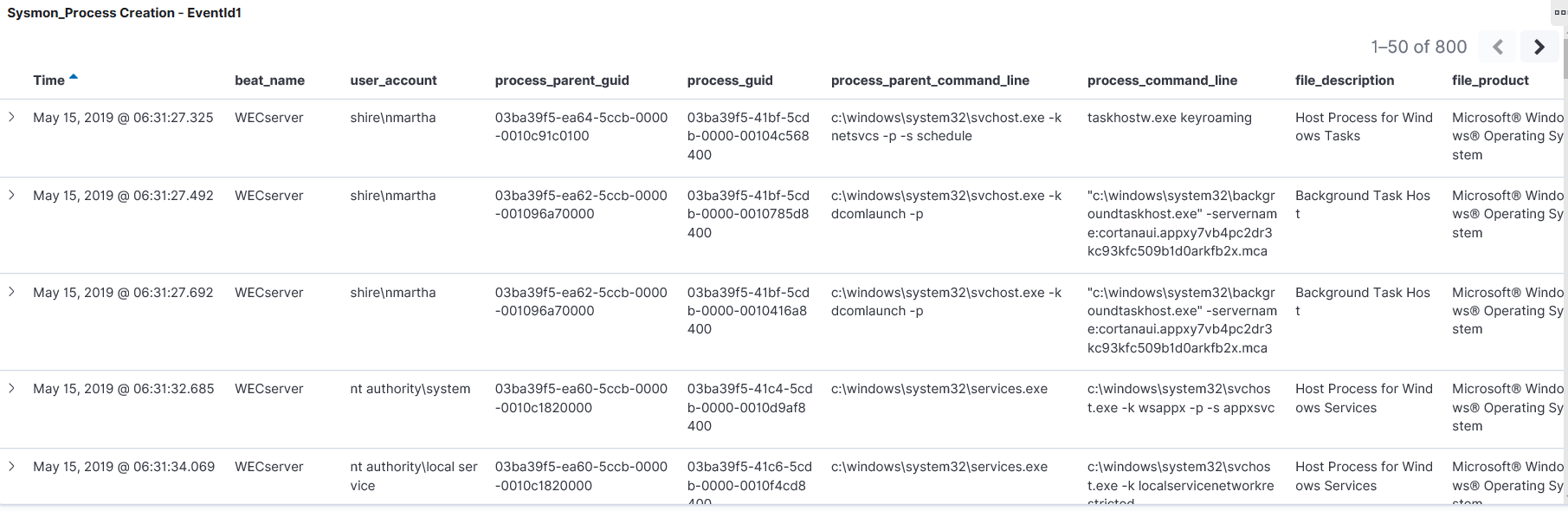
## Sysmon\_ExecutedCommands

该visualization的类型为Search,其作用是检索执行命令的事件，查询语句为：event\_id:1 AND (process\_parent\_name:\"CmD.exe\" OR process\_parent\_name:\"powershell.exe\" OR process\_parent\_name:\"wscript.exe\" OR process\_parent\_name:\"cscript.exe\")。其界面如下图所示：



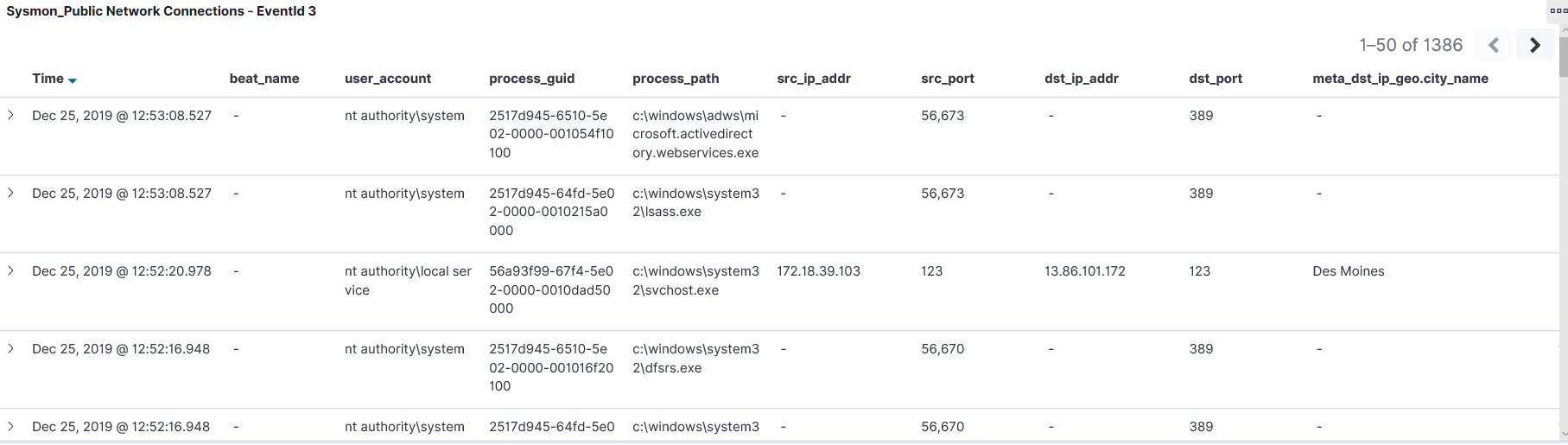
## Sysmon\_Process Creation - EventId1

该visualization的类型为Search,其作用是检索进程创建事件，查询语句为：event\_id:1。其界面如下图所示：



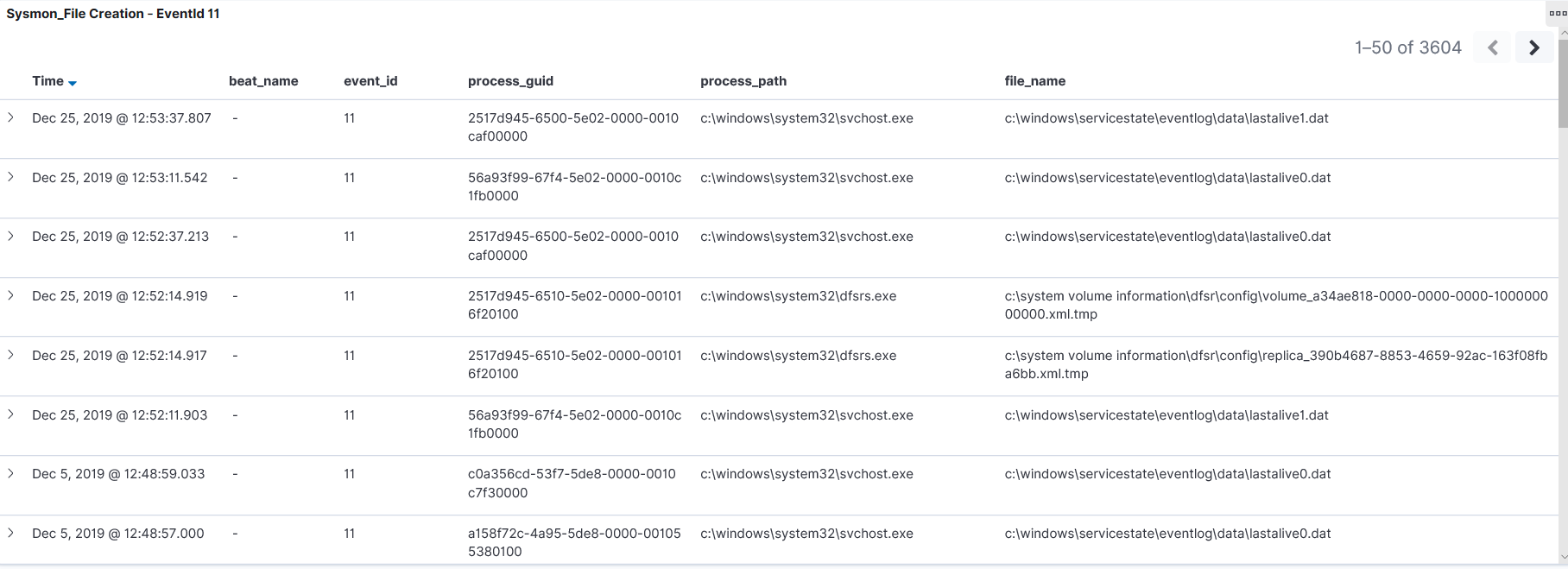
## Sysmon\_Public Network Connections - EventId 3

该visualization的类型为Search,其作用是检索连接外部网络事件，该查询语句为：event\_id:3 AND (NOT dst\_ip\_addr: \"127.0.0.1\" AND NOT dst\_ip\_addr:[10.0.0.0 TO 10.255.255.255] AND NOT dst\_ip\_addr:[192.168.0.0 TO 192.168.255.255] AND NOT dst\_ip\_addr:[172.16.0.0 TO 172.31.255.255])。其界面如下图所示：



## Sysmon\_File Creation - EventId 11

该visualization的类型为Search, 其作用是检索文件创建事件，该查询语句为：event\_id:11。其界面如下图所示：



## Sysmon\_Downloads-EventId 15

该visualization的类型为Search,其作用是检索文件下载事件， 查询语句为：source\_name: \"Microsoft-Windows-Sysmon\" AND event\_id:15。其界面如下图所示：



## Sysmon\_Registry Events

该visualization的类型为Search,其作用是检索注册表事件，查询语句为：event\_id:12 OR event\_id:13 OR event\_id:14。其界面如下图所示：



## windows\_login\_events

该visualization的类型为Search,其作用是检索登录事件，查询语句为：source\_name: \"Microsoft-Windows-Security-Auditing\" AND (event\_id:[4624 TO 4625] OR event\_id:4634)。其界面如下图所示：

