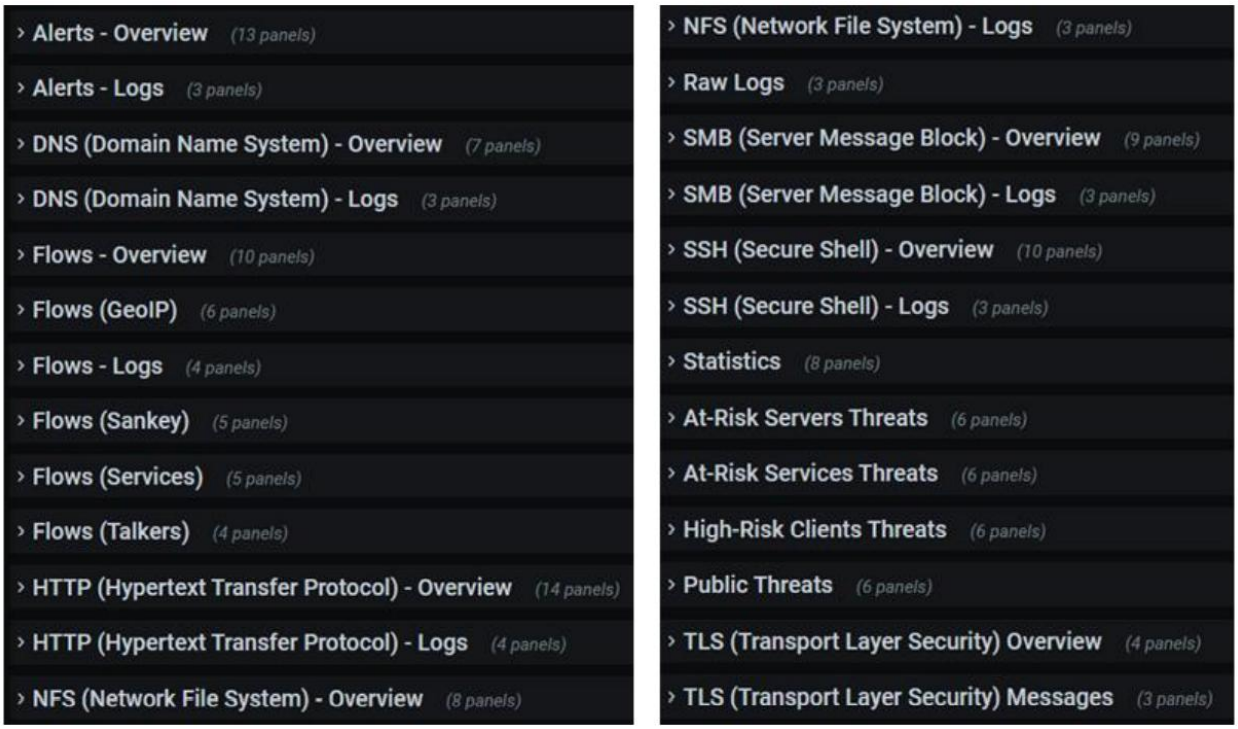
INTRODUCTION

Based on an intrusion detection system, DTM can capture and analyze the network traffic. It is responsible for the transmission of alerts to Kafka and implicitly to ID. It monitors the network traffic by applying signature‐based detection analysis and it sends traffic information, including information about connected devices.

The ID dashboard for DTM contains a wide range of graphs that are distributed in several categories like in the following figure:



All rows contain at least an overview of the system based on its event type (alert, DNS, flows, HTTP, NFS, SMB, SSH and TLS) and the logs (containing the total number of events and a table with detailed fields). Rows can also have more visualizations like pie charts, tables and different diagrams.

Every graph is filtered by the time range button from the top right corner, where the user can select its own preferred time range.

ALERTS - OVERVIEW

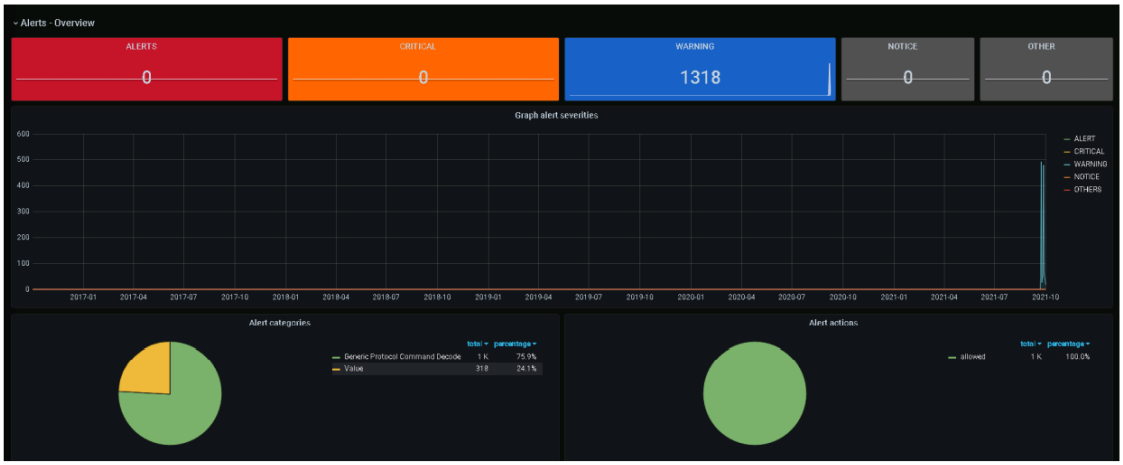
For the first two rows (**Alerts – Overview** and **Alerts – Logs**) graphs describe the alerts detected by the DTM. The first 5 graphs are of stats type, being colored according to their severity:

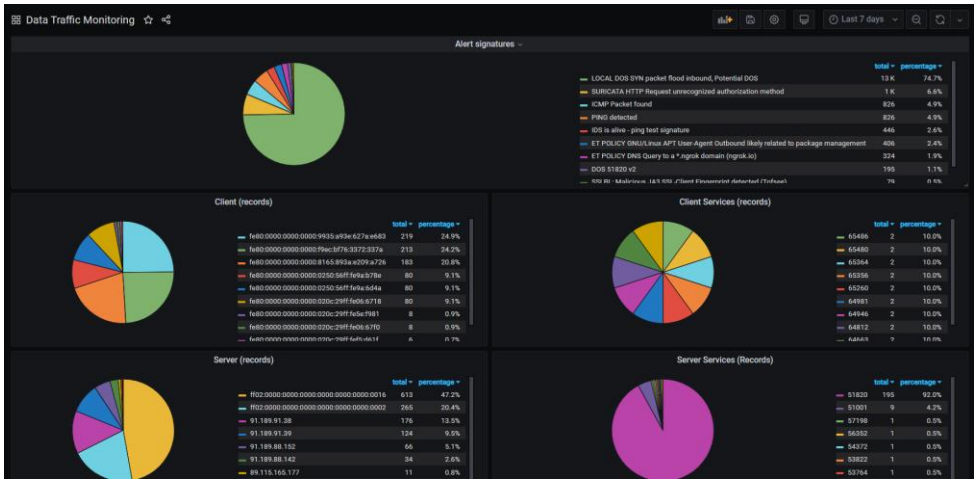
- Severity = 1 for ALERTS (red)
- Severity = 2 for CRITICAL (orange)
- Severity = 3 for Warning (blue)
- Severity = 4 for Notice (gray)
- Severity >= 5 for Others (gray)

You will meet these type of stats graphs in the **HTTP Overview** row.

Below the stats graphs, there is a combined graph for every severity type.

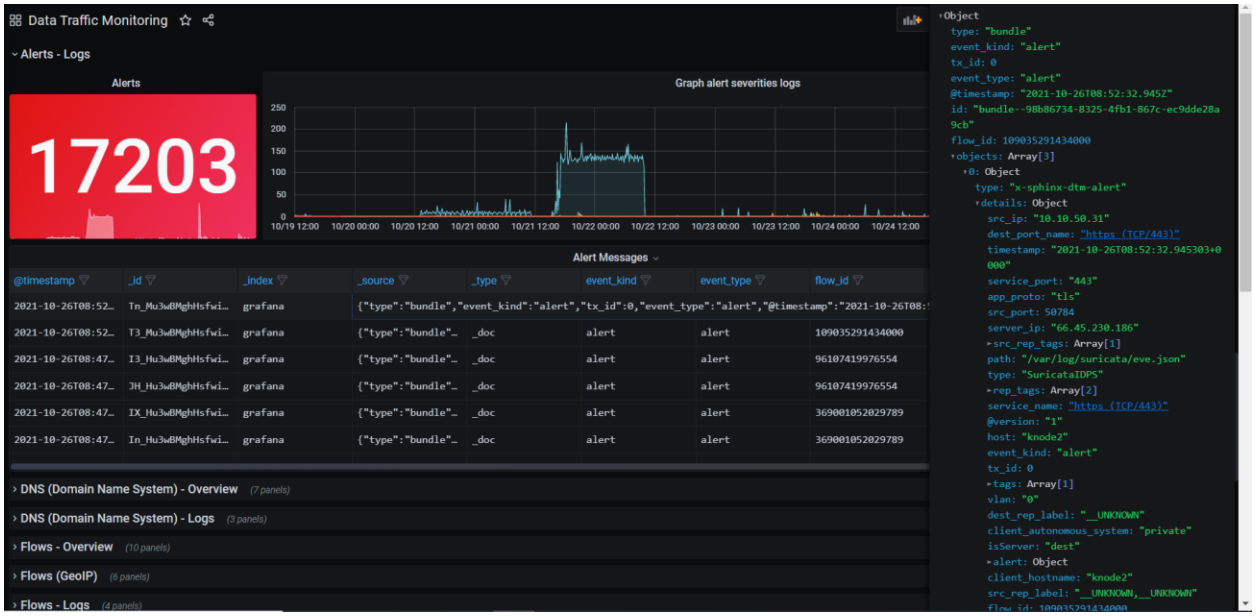
For the rest of the graphs there are pie charts for alert categories, actions, signatures, source and destination IPs detected.





ALERTS - Logs

The second row (Alerts – Logs) contains the number of alert events in the top left corner, a graph containing the number of alerts per day and a table with all JSON fields converted to columns of the alert events. The user can place the cursor over the table cells and see more details of the JSON field.



DNS - OVERVIEW

The DNS visualisations of the DTM dashboard contain details about IPs source and destination (first two pie charts) detected in the DNS events, message type (answers or requests), record type pie chart, response codes, “Top Queries” and “Top Answers”.

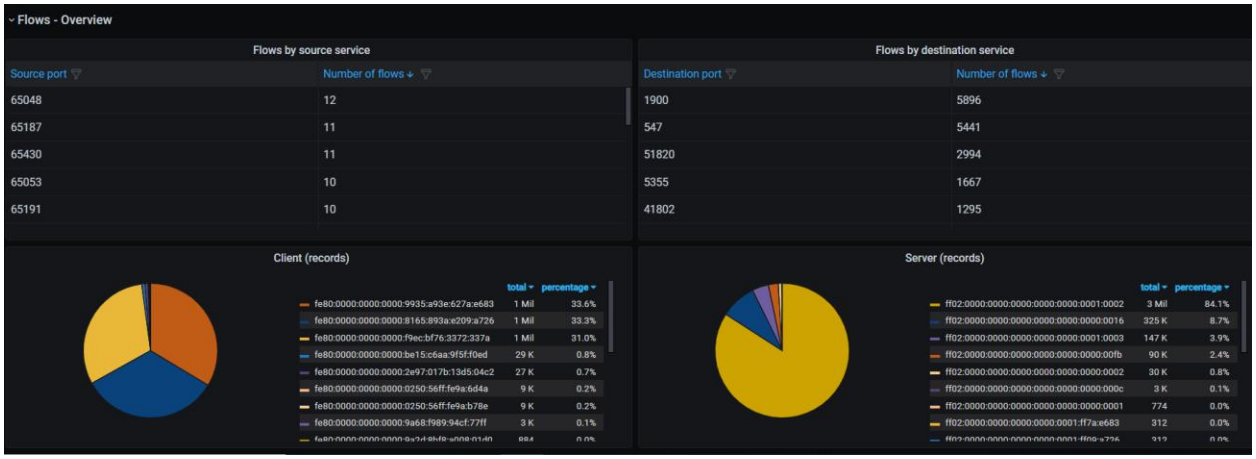
DNS - Logs

The logs contain the total number of DNS events with a graph next to it for events per day and a table with data coming from the JSON events.

Flows - Overview

Flows contain more graphs grouped in categories. The first row of Flows is “**Flows – Overview”**, which contains general statistics about flow event types grouped by source and destination ports and IPs, VLANs, IP Protocols, Flow States and TCP Flags.

You can also filter the table columns or sort them.

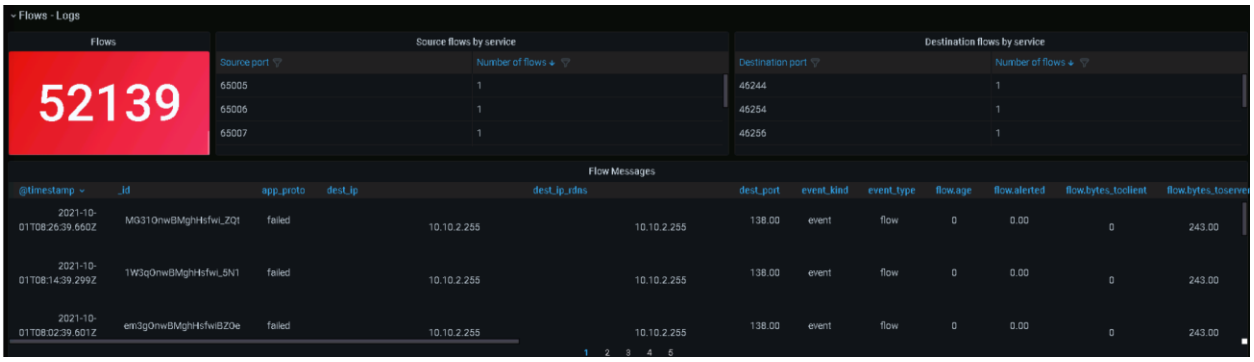


Flows - GeoIP

This row contains pie charts and world map panels regarding the geolocation (countries, cities) of the source and destination IPs.

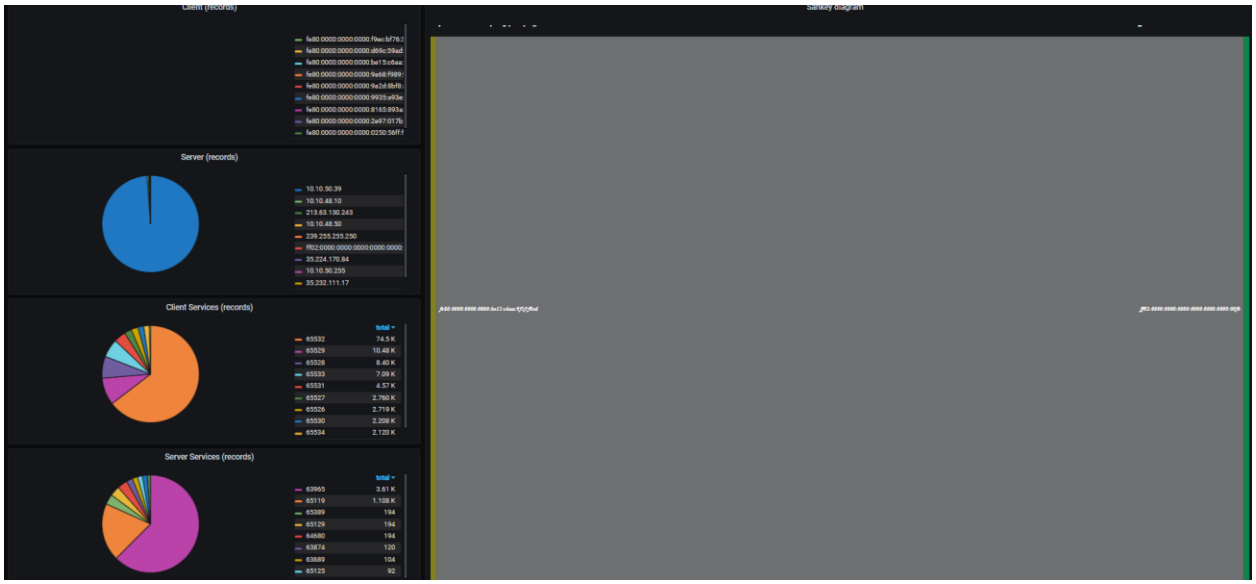
Flows - Logs

This row is for detailed statistics about the number of flow event types, with a graph of the detected events per day and a table with every JSON field.



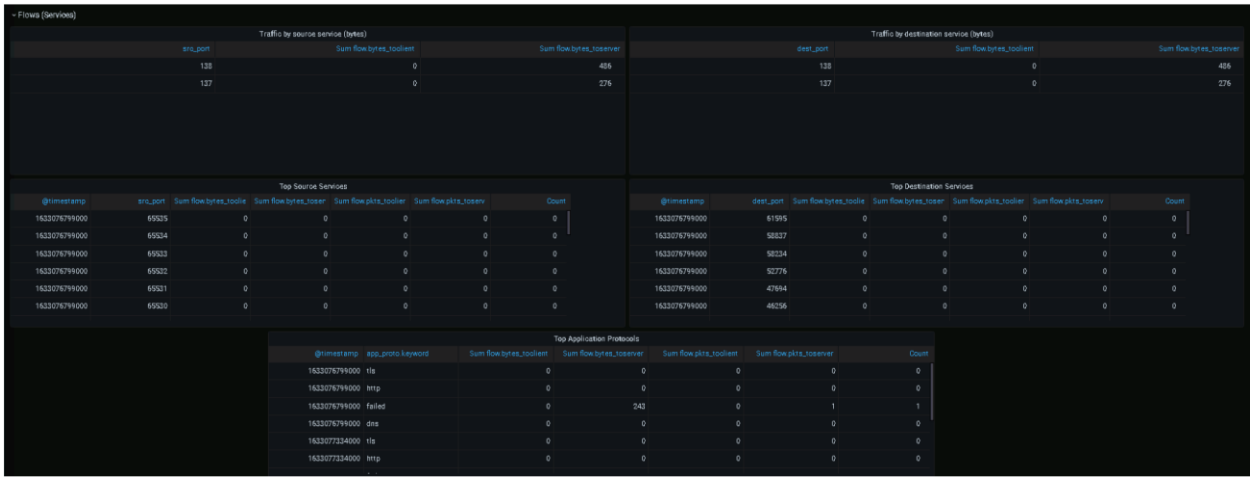
Flows - Sankey

It contains pie charts with IPs and ports by source and destination, but the most important visualization is the sankey diagram on the right, displaying the top 5 number of connections between 2 IPs.



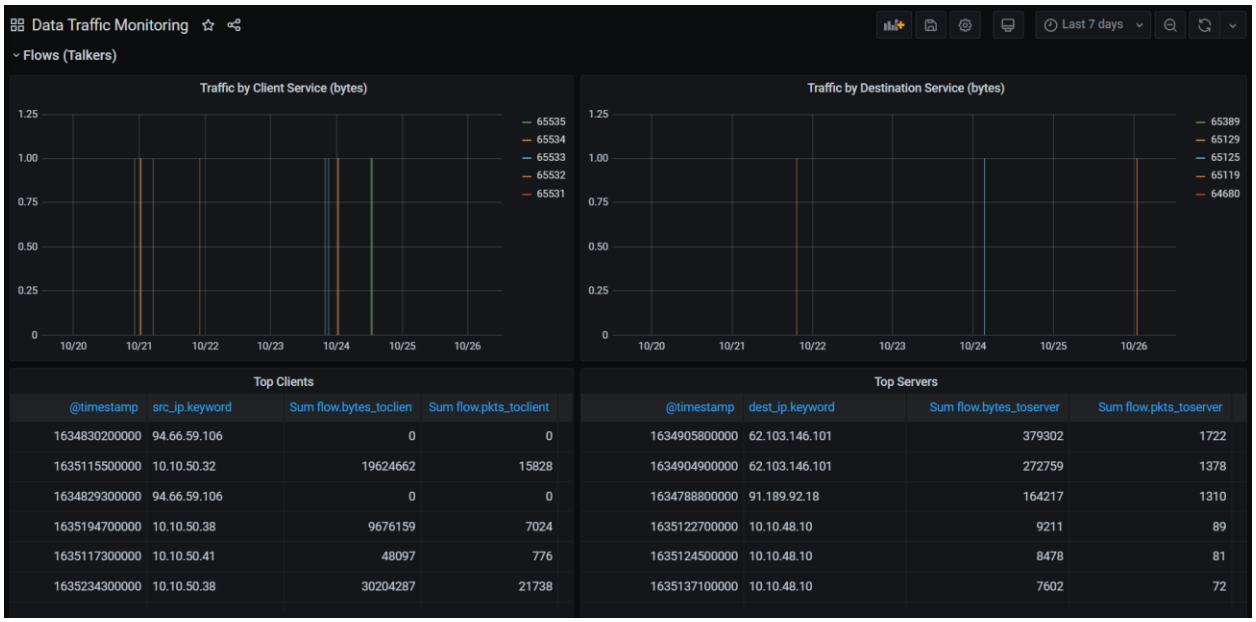
Flows - Services

It presents visualisations about traffic through client or destination ports, top application protocols (TLS, HTTP, DNS) and the number of bytes detected.



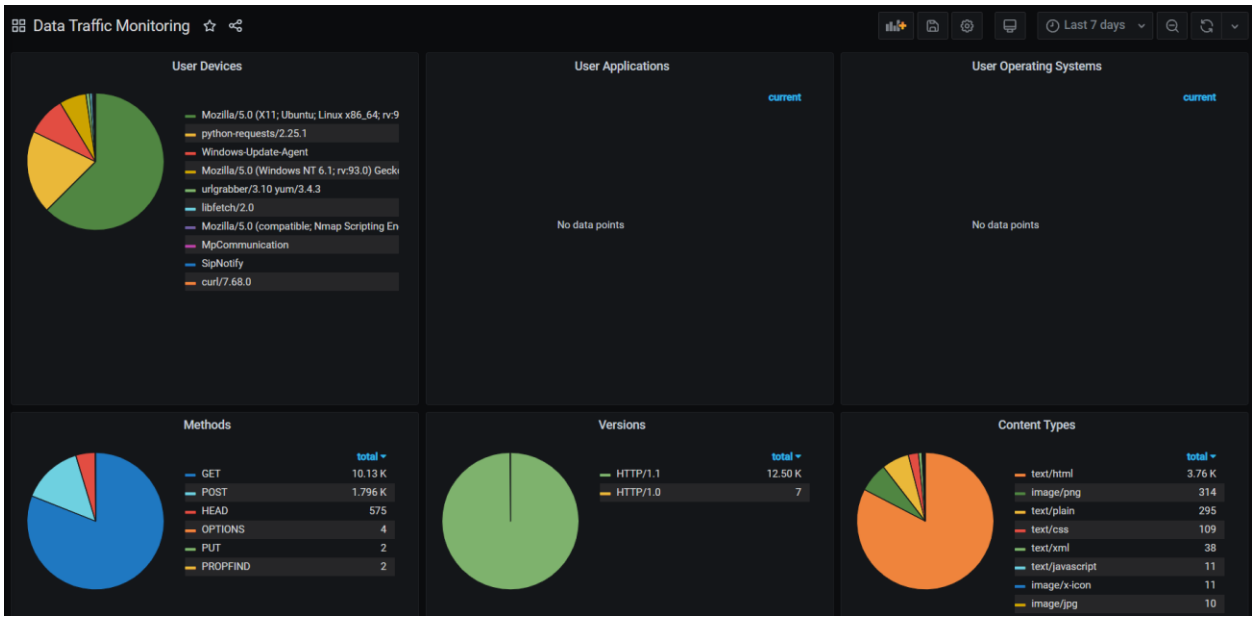
Flows - Talkers

This row displays two graphs about traffic by service and top clients/servers.



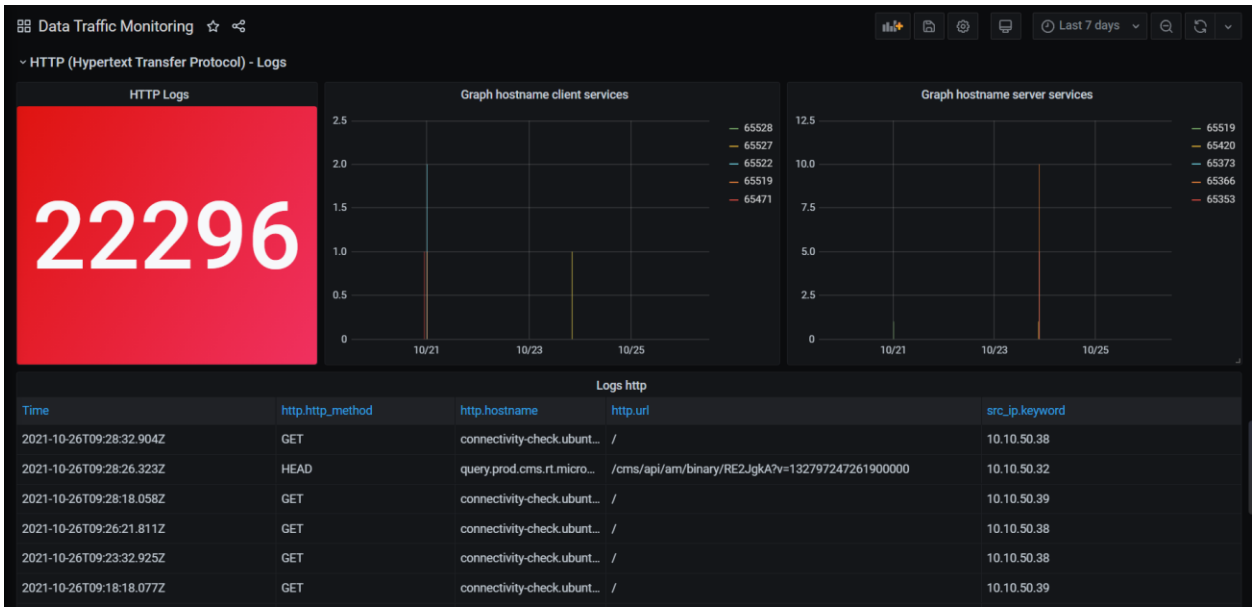
HTTP – Overview

HTTP Overview row contains in the beginning similar stats to “Alert” rows, keeping the same severity categories but it must contain the “http.hostname” field. The overview contains pie charts for source and destination IPs, referrers, user devices, user applications, operating systems, methods (GET, POST), Versions and Content Types.



HTTP – Logs

It contains the number of HTTP events detected by DTM, two graph with HTTP events categorized by source and destination port. The last table contains detailed informations about the HTTP events.



NFS - Overview & Logs

These two rows contain informations about network file system detected events, presenting pie charts for source and destination IPs, files, procedures, file transactions , number of total NFS events, number of NFS events categorized by procedures and a table with detailed informations of the NFS logs.

Raw Logs

This row contains three graphs:

- Total number of every events detected by the DTM, no matter the type;
- Raw graph logs, which is the number of events categorized by timestamp and events;
- Table with logs, containing detailed informations.

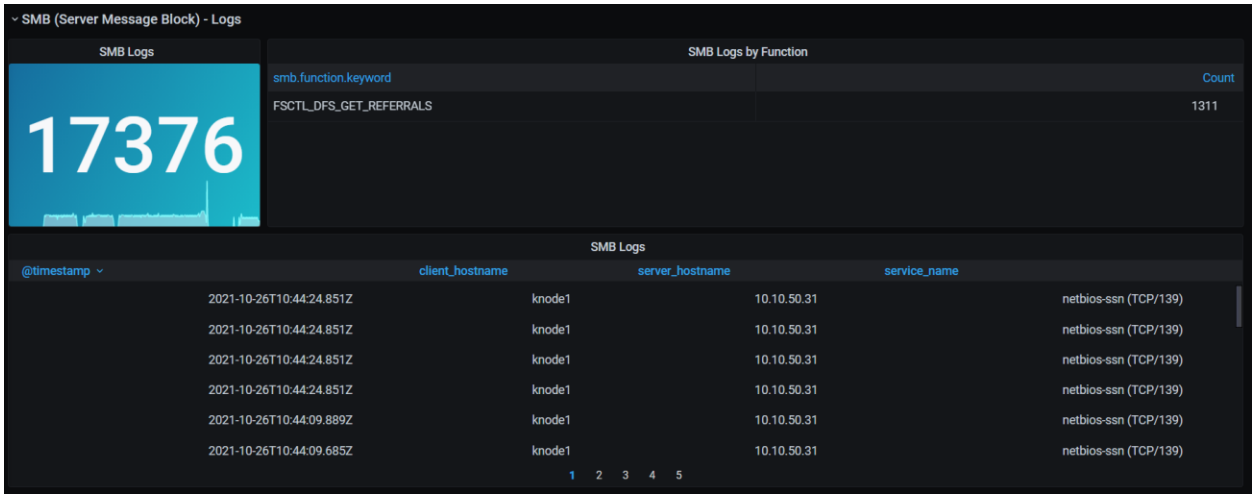
SMB - Overview

This row contains pie charts for informations regarding the “Server Message Block” events, like source and destination IPs, filenames records, commands, dispositions, status, access, dialects and functions.

SMB - Logs

The SMB logs are displayed in three types of graphs:

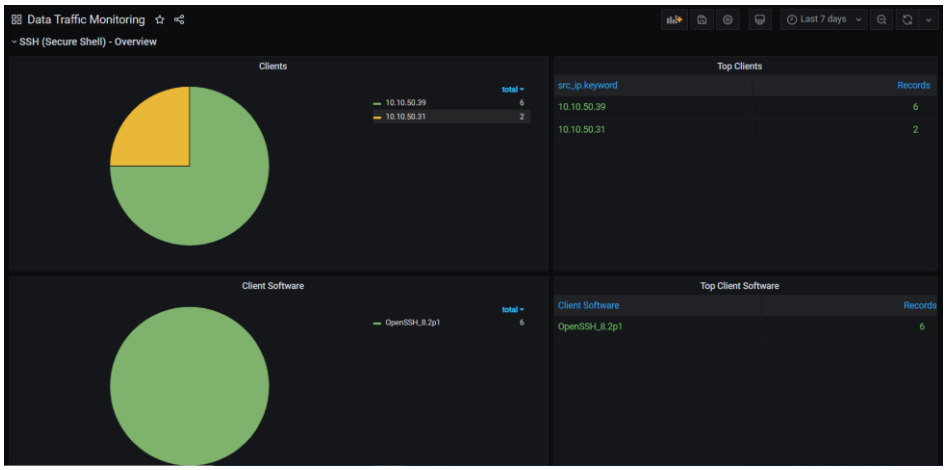
- The number of all SMB event types;
- Number of SMB logs by functions detected;
- SMB Logs containing every detail of a SMB event.

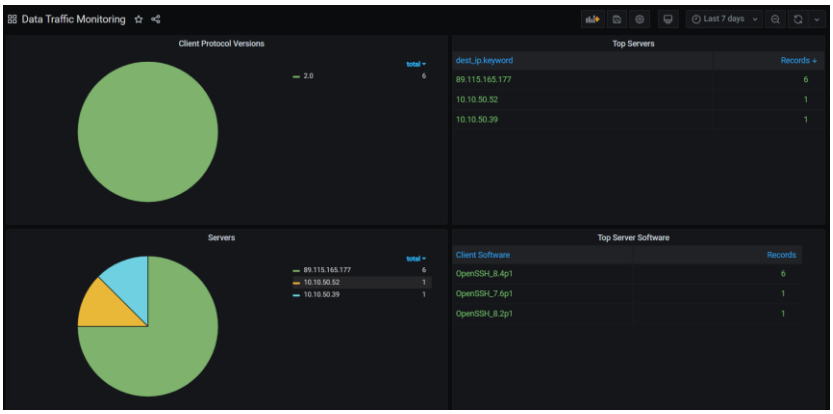


SSH - Overview

This row contains relevant details about SSH events detected by the DTM:

- Source and destination IPs
- Top source IPs
- Top destination IPs
- Client software (based on source IP)
- Client protocol versions (based on source IP)
- Top client software
- Server software (based on destination IP)
- Server protocol versions (based on destination IP)

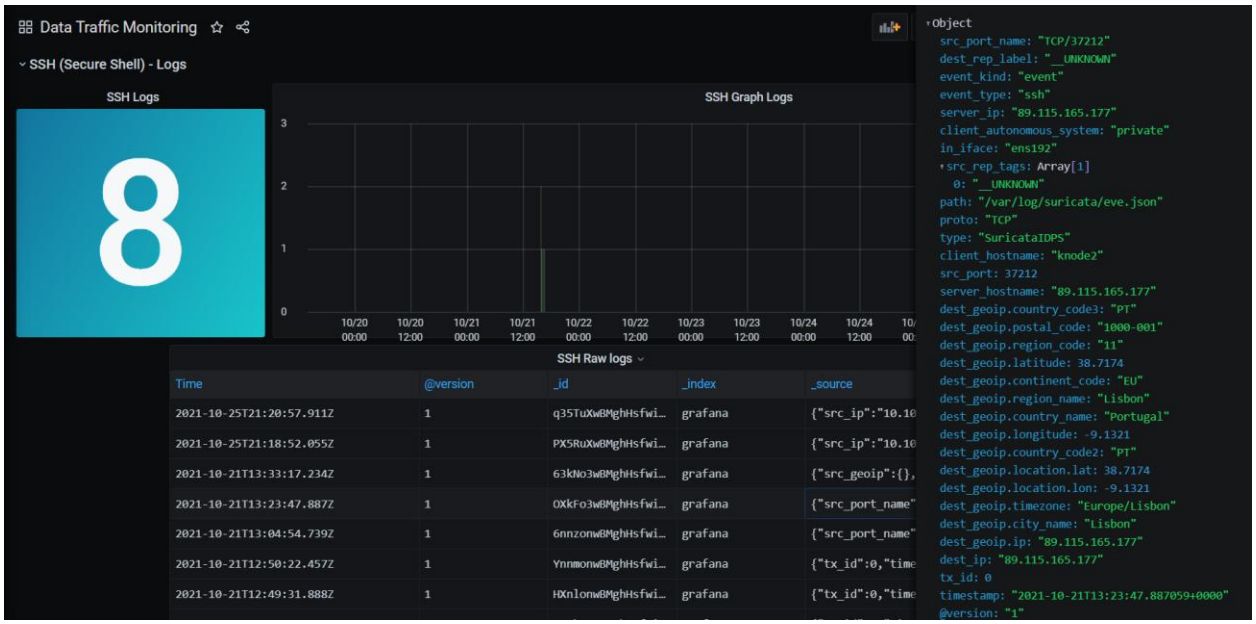




SSH - Logs

SSH logs is represented by 3 visualizations:

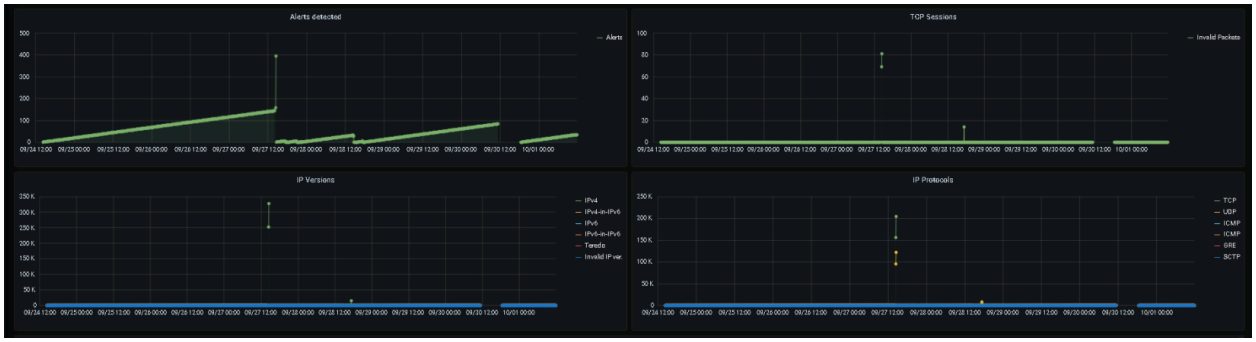
- Number of SSH events detected;
- Number of SSH events detected per timestamp;
- SSH Raw logs table where the user can move the cursor over fields and see more details regarding these events.



Statistics

Statistics row contains eight graphs with counts/timestamp. The graphs are the following:

- Decoder traffic volume (max values only);
- Memory Use (TCP, FLOW, HTTP, DNS);
- Kernel Drops;
- Invalid Packets;
- Number of Alerts Detected;
- TCP Sessions;
- Count of events by IP versions;
- IP Protocols.

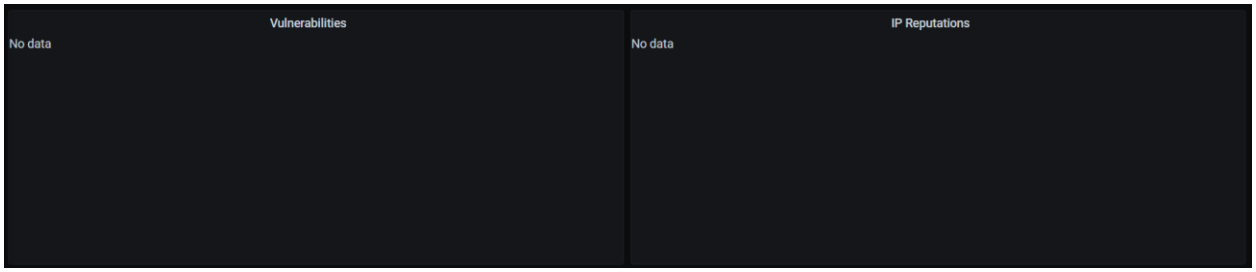


Threats

There are also four threats rows:

- At-Risk Servers (for destination IPs)
- At-Risk Services (for ports)
- High-Risk Clients (for source IPs)
- Public Threats (client_autonomous_system private)

Each row contains similar graphs. Starting with a graph with the number of threats per day, a stats visualization with the number of total threats. A table with attackers, signatures, vulnerabilities and IP reputations. Some of the rows require the IPs to be in the local network.



TLS – Overview & Messages

Transport Layer Security rows contains pie charts and tables regarding the server name indications, ports, subjects, top connections, the number of TLS events, detected events by port and TLS logs.