PROJECT

Multi-tenant cybersecurity operations centre designed
as an open cloud service with machine learning elements

Dashboards – visualization of data from tools

Linked to work package KPB2 – Design of the SOCaaS service

Linked to output
V6 – Description of dashboards, the monitoring and reporting system

Funded by the European Union NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

List of figures 3
Dashboard in the Kibana tool 4
IDS dashboard 4
Login Activity Monitoring dashboard 6
System load analysis dashboard 7

List of figures

Figure 1 IDS DMZ dashboard, alerts 4
Figure 2 IDS DMZ dashboard, top signatures 5
Figure 3 IDS DMZ dashboard, top source IPs 5
Figure 4 IDS DMZ dashboard, map 5
Figure 5 Login Activity Monitoring dashboard, basic information 6
Figure 6 Login Activity Monitoring dashboard, charts 6
Figure 7 Login Activity Monitoring dashboard, tables 7
Figure 8 Stack Load dashboard, Elasticsearch 7
Figure 9 Stack Load dashboard, Kibana 8
Figure 10 Stack Load dashboard, Loghstash 8

A dashboard in the Kibana tool makes it possible to quickly create views that combine charts, maps and filters. These views serve to display a complete picture of the data stored in Elasticsearch.

IDS dashboard

This dashboard serves to display visualized data from the IDS tools that monitor the data flow. The IDS dashboard clearly shows the number of detections by the IDS sensors and also a mutual comparison of the detections of the *Suricata* IDS and the IDS module in Fortigate. The dashboard clearly shows that the IDS sensors detect different events, even though they monitor the same data flow.

When deploying the IDS, the assumption was that the sets of detections produced by IDS sensors from different vendors monitoring the same data flow would have a significant overlap. This assumption was not fulfilled.

Figure 1, Figure 2, Figure 3 and Figure 4 show the individual visualizations in the given dashboard.



Figure 1 IDS DMZ dashboard, alerts

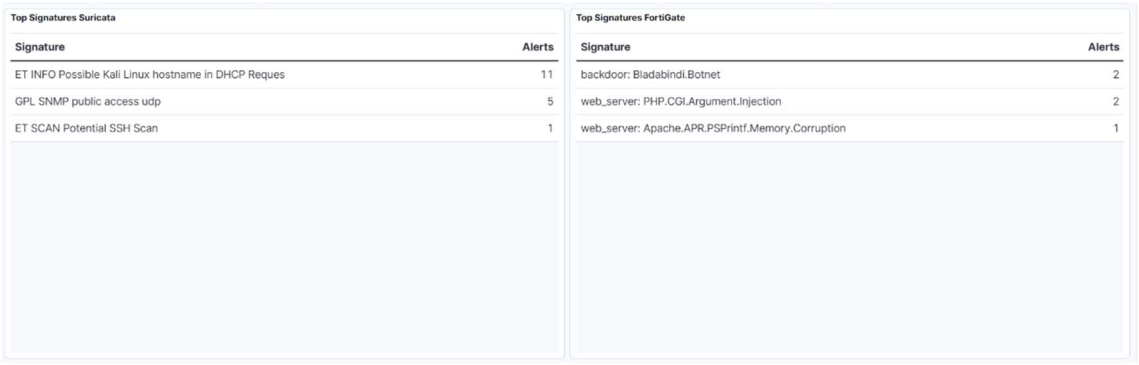


Figure 2 IDS DMZ dashboard, top signatures



Figure 3 IDS DMZ dashboard, top source IPs

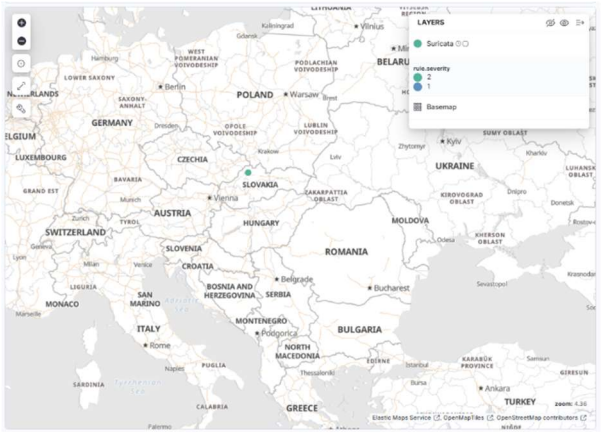


Figure 4 IDS DMZ dashboard, map

Login Activity Monitoring dashboard

We created this dashboard to visualize login events on the monitored servers. A clear visualization of successful and failed logins in combination with user names and server names can facilitate the investigation of potential security incidents recorded by means of security alerts. Figure 5, Figure 6 and Figure 7 show the individual visualizations in the given dashboard.

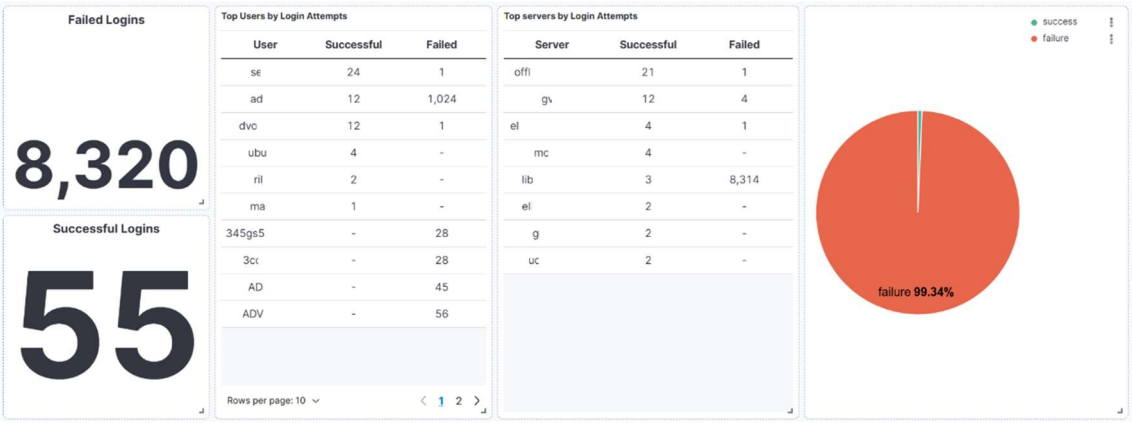


Figure 5 Login Activity Monitoring dashboard, basic information

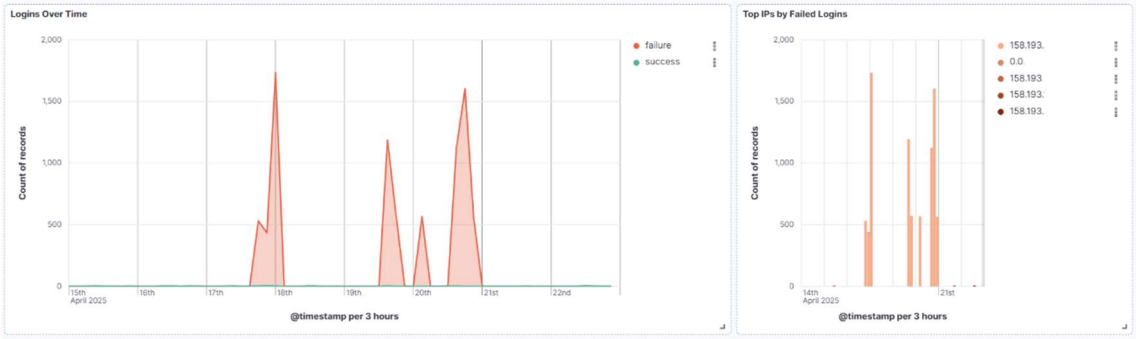


Figure 6 Login Activity Monitoring dashboard, charts

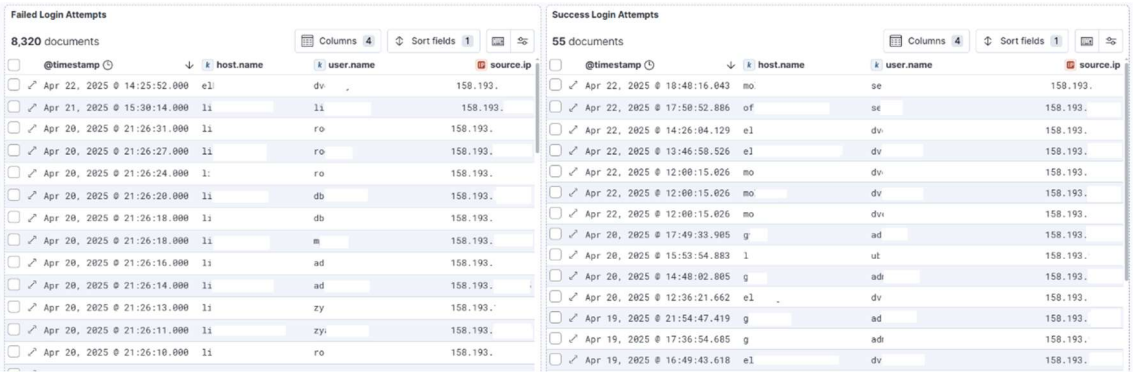


Figure 7 Login Activity Monitoring dashboard, tables

System load analysis dashboard

In the system load analysis section, we primarily focused on the utilization of the RAM allocated to the individual parts of the ELK stack: the Elasticsearch nodes, Logstash and Kibana. For effective monitoring of RAM load, data collected using the metricbeat tool were used. The default part of the Kibana application for monitoring Elastic Stack components, so-called stack monitoring, works precisely with these metrics. However, in the ELK component monitoring view, we can only see the load at a particular point in time. For the purpose of displaying the average load, we created a clear dashboard, which we named Stack Load. Figure 8, Figure 9 and Figure 10 show the average load over a period of six days.



Figure 8 Stack Load dashboard, Elasticsearch

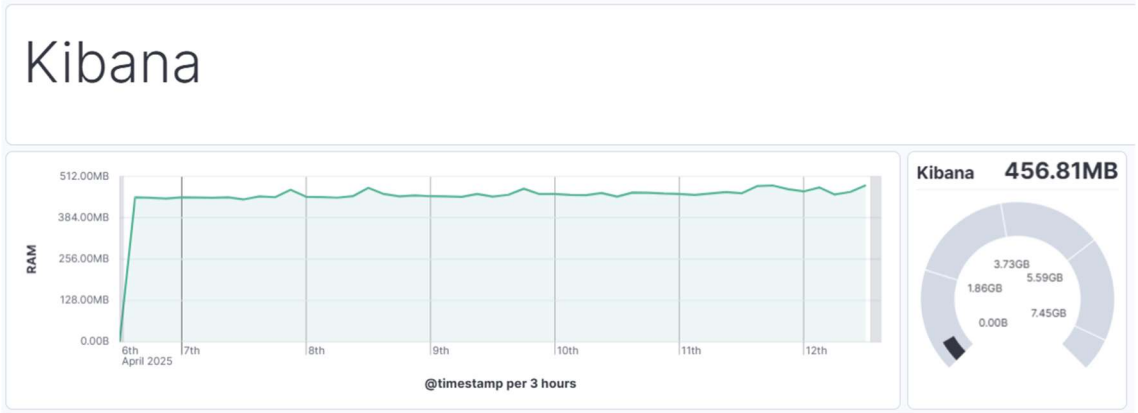


Figure 9 Stack Load dashboard, Kibana

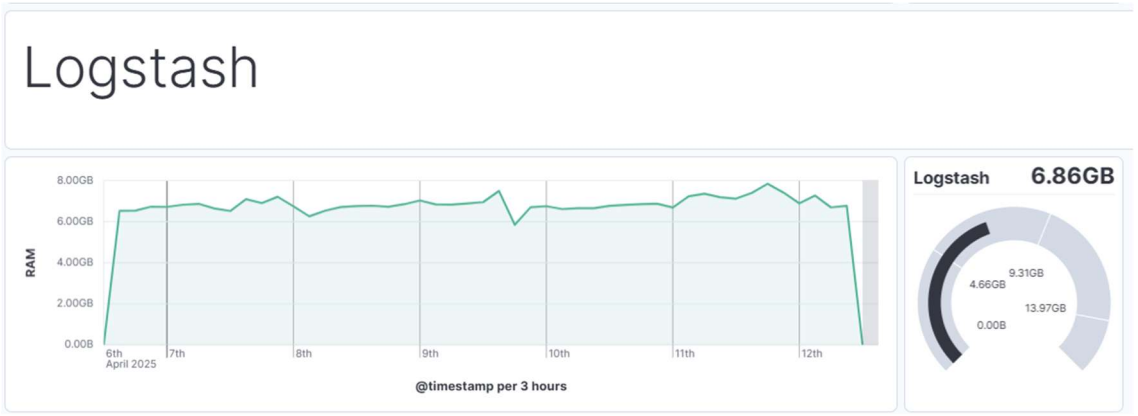


Figure 10 Stack Load dashboard, Loghstash

As can be observed from the figures above, the solution utilizes the allocated RAM effectively and no overload occurs. Moreover, the allocated RAM provides room for future expansion, possibly a transition to a 10 GB infrastructure. The transition could result in an increase in the volume of data over a given time, the processing of which would require greater hardware resources.

If we focus on the individual nodes according to their type, we can see that *Elasticsearch* places the greatest load on the data nodes labelled hot. These are followed by the nodes labelled warm and, lastly, the nodes labelled cold.

Table 1 shows the average memory utilization of the individual systems within the ELK stack.

System	RAM utilization [GB]	Allocated RAM [GB]

master1	6.3	16
hot1	9.98	31
hot2	11.44	31
hot3	10.98	31
warm1	8.80	31
warm2	4.50	31
cold1	2.91	16
kibana	0.457	8
logstash	6.86	16

Table 1, Actual RAM utilization