Metrics Monitoring Stack

Document Name :	Metrics Monitoring Stack
Version :	1.0
Version Date :	13/07/2022
Modified By :	Marc MARTINEZ
Creation Date :	13/07/2022
Created by :	Marc MARTINEZ
Approved by :	Marc MARTINEZ
Confidentiality Level :	INTERNAL

Modification History

	Date	Author	Commentary
1.0	13/07/2022	Marc MARTINEZ	Creation of the document

Introduction

This document is here to present the tools the Security Team suggests to set up as this metrics monitoring stack.

Description

All systems described in this document could be running in docker cortainers handled.

For ease of management and deployment, the Security Team suggests to use the docker versions of those systems as well as Portainer, a simple robust docker containers management software.

The Security Team is open to suggestions from the Cloud Team as to the softwares that could be used, including the metric stack itself or the management systems, as using a kubernetes system instead of portainer.

Softwares suggested

Portainer

A management software for docker containers, making use of docker compose easier and allowing for a quick access to logs and rebooting functions. Come with a web interface.

Prometheus

Prometheus is a monitoring software than handles receiving the data from different “subsystems” and dispatching it to others.

Grafana

Grafana is a subsystem of prometheus, it takes the data from prometheus and display it in comprehensive graphs on a web interface.

Node exporter

Node exporter is a subsystem of prometheus, it gives data to prometheus for dispatching. To get data from remote VMs, you need to install a node exporter agent on said VM.

Postgres Exporter

Postgres exporter is a subsystem of prometheus, it tracks data from postgres database and give them to prometheus for dispatching.

Blackbox

Blackbox is a subsystem of prometheus. It monitores traffic on http, https, TCP and DNS connexions and send the data to prometheus for dispatching.

Alert Manager

Alert Manager is a subsystem of prometheus. It creates alerts that triggers depending on the data received by prometheus, can then send emails or others notifications depending on the configuration

Required budget

- All softwares suggested by the security team on that list are free/open source.
- A mail address to send the alerts through Alert Manager. Can be free if using solutions like Yahoo. As a note, Google Mail do not allow the use of Gmail addresses for this purpose since mid 2022.
- Three (3) days worth of man hours (2400 €).