wazuh.

Google Cloud report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	wazuh_agent_ubuntu_2	172.20.0.7	Wazuh v4.9.0	wazuh-manager-4.9.0-7102	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 16, 2024 @ 15:49:19.000

Group: default

Security events related to your Google Cloud Platform services, collected directly via GCP API.
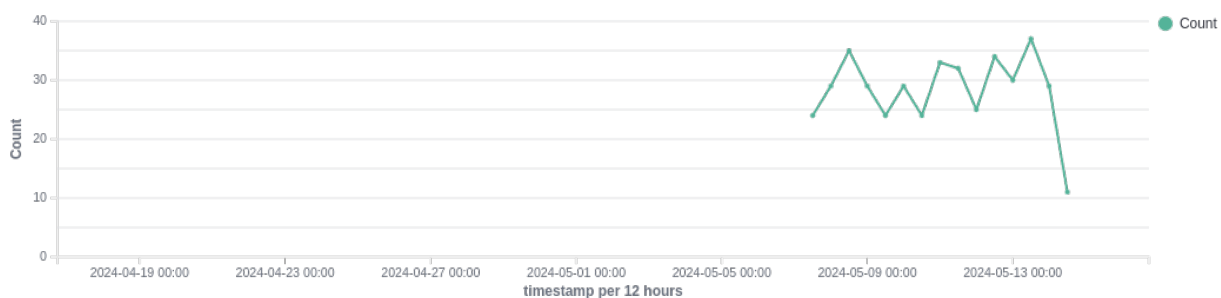
⏲ 2024-04-16T17:49:28 to 2024-05-16T17:49:28

🔍 rule.groups: gcp AND cluster.name: wazuh AND agent.id: 002

Top 5 rules

Rule ID	⌄	Event	⌄	Count	⌄
65007		Unable to process query due to a prol		64	
65032		DNS external query		57	
65010		GCP notice event with source IP 83.3		56	
65034		GCP warning event from VM 5313392		55	

‹ **1** ›

GCP alerts evolution

Auth answer count

Resource type by project id

Top query events

- 185.5.205.124.in-ad…
- 98.72.244.104.in-ad…
- mirrors.advancedhos…
- 41.212.95.203.in-ad…
- 41.212.95.203.in-ad…

Top 5 instances

- 49801139288008396…
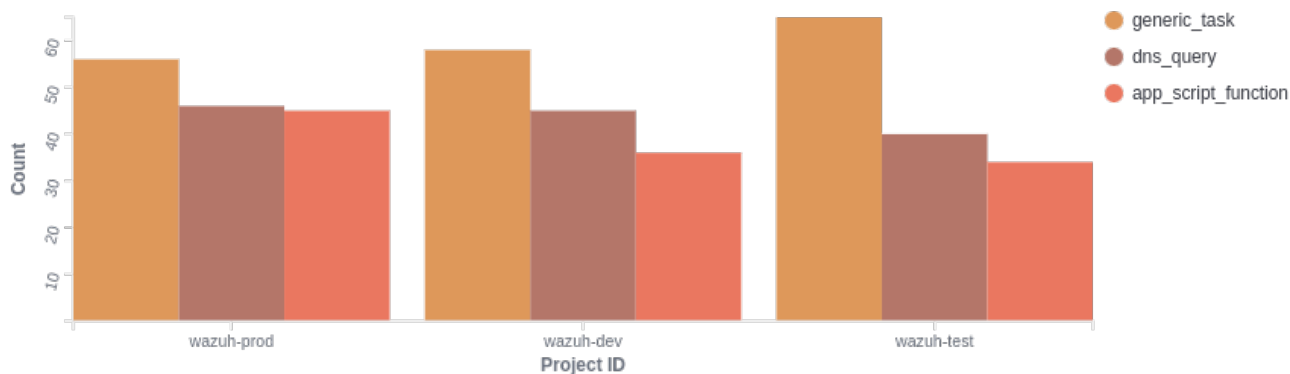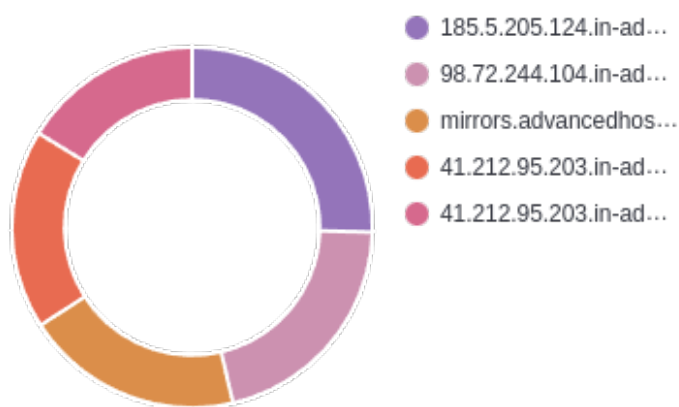
Top project id by sourcetype

- europe-west1
- australia-southeast1
- us-west2
- us-east1
- us-central1
- wazuh-prod
- wazuh-dev
- wazuh-test
- gce-vm
- internet
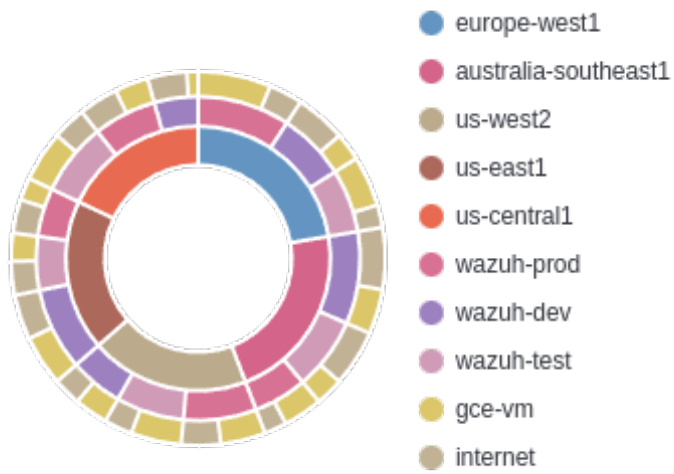
Alerts summary

Rule ID	Description	Level	Count
65007	Unable to process query due to a problem with the name server	12	64
65032	DNS external query	3	57
65010	GCP notice event with source IP 83.32.0.0 from europe-west1 with response code NXDOMAIN	5	56
65034	GCP warning event from VM 531339229531.instance-1 with source IP 83.32.0.0 from europe-west1	5	55
65036	GCP critical event from VM 531339229531.instance-1 with source IP 83.32.0.0 from europe-west1	9	51
65038	GCP emergency event from VM 531339229531.instance-1 with source IP 83.32.0.0 from europe-west1	12	50
65001	GCP notice event	5	47
65037	GCP alert event from VM 531339229531.instance-1 with source IP 83.32.0.0 from europe-west1	11	45