Your Logo Here

info@example.com
https://example.com

Security events report

ID	Name	IP	Version	Manager	OS
029	S-DEMO-SIT01	10.101.4.38	Wazuh v3.9.5	S-DEMO-SEC01.example.com	CentOS Linux 7.6

Registration date: 2019-09-11 08:04:04.

Last keep alive: 2019-09-11 10:14:45.

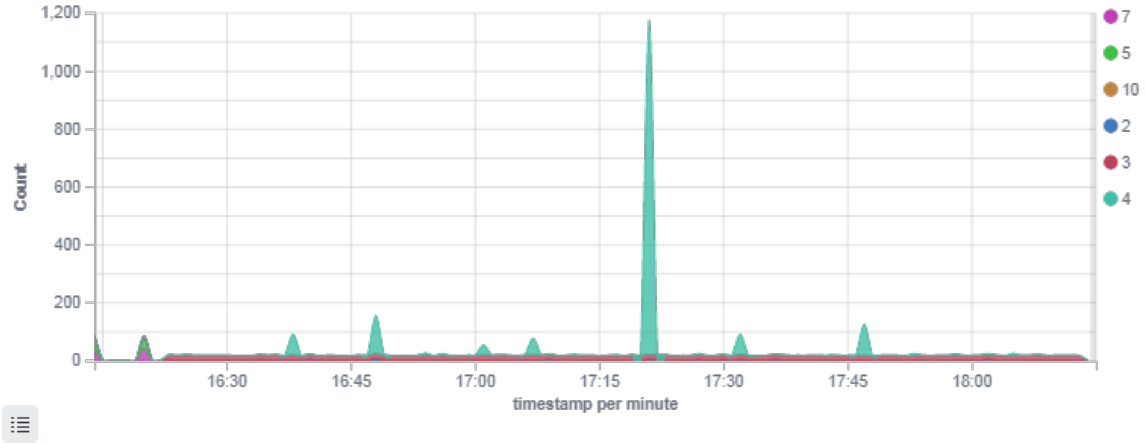
Group: default

Browse through your security alerts, identifying issues and threats in your environment.

2019-09-11T16:14:26 to 2019-09-11T18:14:26

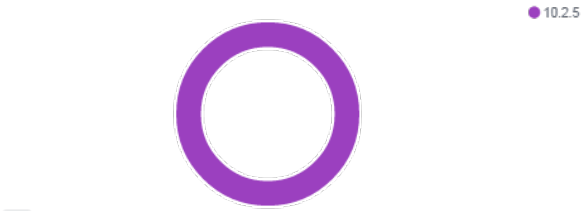
manager.name: S-DEMO-SEC01.example.com AND agent.id: 029

Alerts

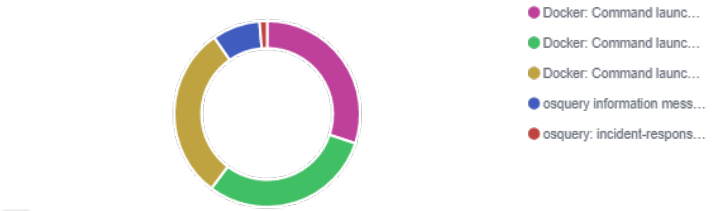


Alert groups evolution

Top 5 PCI DSS requirements



Top 5 alerts



Top 5 rule groups

Alerts summary

Rule ID	Description	Level	Count
87907	Docker: Command launched in container k8s_calico-kube-controllers_calico-kube-controllers-65b8787765-b5n5v_kube-system_b48ca686-bc9d-4cce-b6a0-9bacccca21fc_0. Action: "exec_start: /usr/bin/check-status -r"	3	666
24003	osquery information message	2	184
24050	osquery: incident-response logged_in_users: User is logged from host	4	29
24023	osquery: osquery-monitoring osquery_info: Osquery version is 3.3.2 build on ubuntu xenial	4	12
24011	osquery: System memory is under 70%	4	11
24058	osquery: incident-response listening_ports: Process 1 has opened port 0 address	4	10
24064	osquery: incident-response iptables: Iptable source ip 0.0.0.0 with policy ACCEPT and target FORWARD_direct has a packet count of 23478	4	8
1002	Unknown problem somewhere in the system.	2	5
23503	Kernel: KVM: leak of uninitialized stack contents to guest	5	2
23504	Kernel: tcp: excessive resource consumption while processing SACK blocks allows remote denial of service	7	2
23505	Kernel: page cache side channel attacks	10	2
24053	osquery: incident-response mounts: Mount point at /dev/mapper/VolGroup00-lv_root with 6909446 free blocks	4	2
24416	osquery: hardware-monitoring device_nodes: Device /dev/core, UID 0, GID 0, type regular	4	2
24021	osquery: osquery-monitoring schedule: The pack executed is high_load_average and the interval is 900	4	1
24063	osquery: incident-response disk_encryption: Device /dev/dm-0 encryption status is not encrypted	4	1
24104	osquery: it-compliance os_version: OS CentOS Linux CentOS Linux release 7.6.1810 (Core) 7.6	4	1
24131	osquery: it-compliance rpm_packages: RPM package GeoIP version 1.5.0 is installed on the system	4	1
24134	osquery: it-compliance disk_encryption: Device /dev/dm-0 encryption status is not encrypted	4	1
24302	osquery: vuln-management os_version: OS CentOS Linux CentOS Linux release 7.6.1810 (Core) with minor 6 and major 7	4	1
24317	osquery: vuln-management rpm_packages: RPM package GeoIP version 1.5.0 is installed on the system	4	1
24402	osquery: hardware-monitoring cpuid: CPU feature 3dnowprefetch and value 0	4	1
24409	osquery: hardware-monitoring hardware_events: Hardware device triggered action change	4	1

info@example.com
https://example.com

Groups summary

Group	Count
docker	1998
osquery	1853
it_compliance	591
vuln_management	578
incident_response	330
vulnerability-detector	170
osquery_monitoring	83
hardware_monitoring	76
errors	5
syslog	5