Security and Monitoring Tools

Day 3 – SS Track – SomNOG6

Linux security and monitoring tools

- They are software applications that can help you protect and optimize your Linux systems and networks.
- They can perform various functions, such as scanning for vulnerabilities, detecting intrusions, analyzing traffic, auditing configurations, enforcing policies

Some of the best tools

- Vuls: This is an open-source vulnerability scanner for Linux and FreeBSD
- ZAP: This is an open-source web application analysis tool from the OWASP project.

Some of the best tools ..

- Sematext: This is a commercial server monitoring tool that provides real-time visibility into the performance of your Linux servers. It can collect and report various metrics
- Splunk : Commercial and mostly in log management and monitoring

Some of the best tools ..

- OpenVAS: is a full-featured vulnerability scanner.

OpenVAS

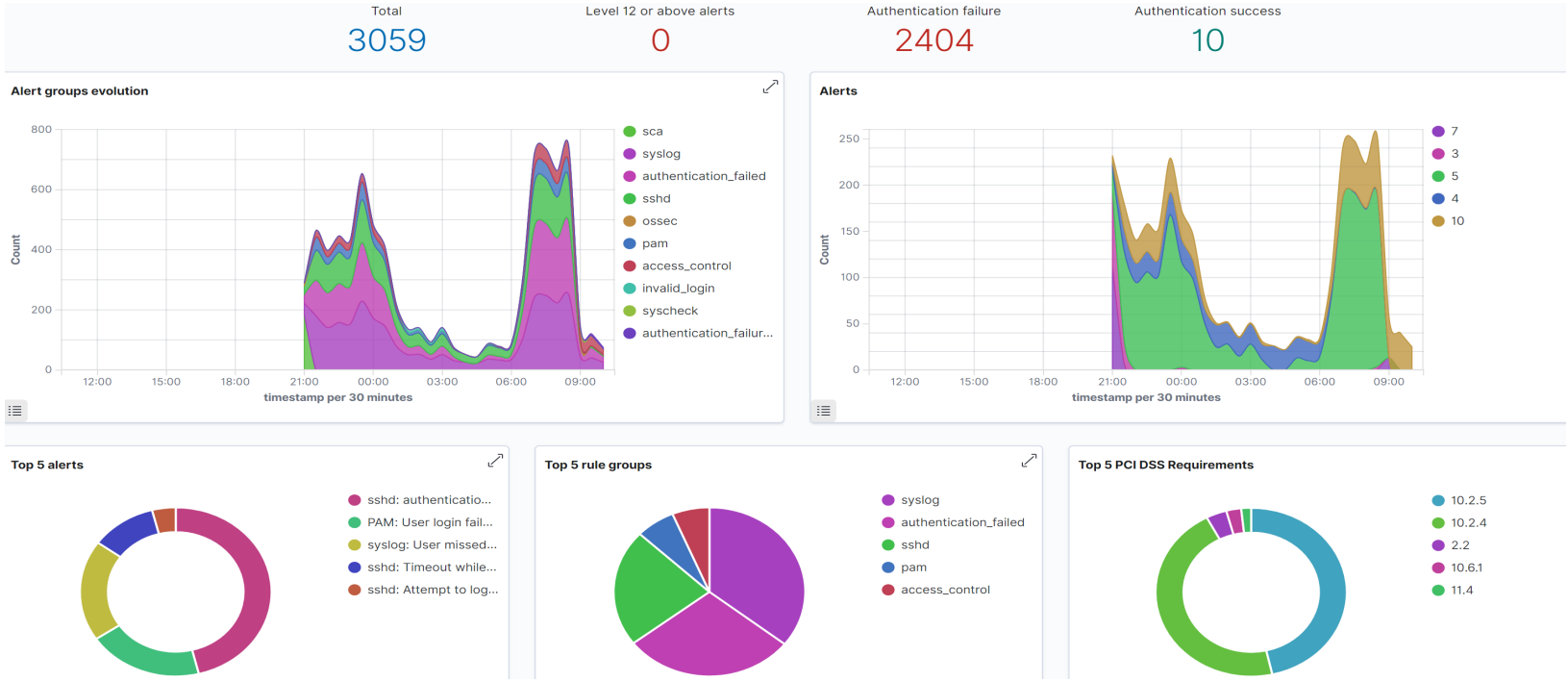
Open Vulnerability Assessment Scanner

Some of the best tools ..

- Zabbix: This is an open-source monitoring solution for any type of server, network, or application.

Some of the best tools ..

Wazuh : Unified XDR and SIEM protection for endpoints and cloud workloads.



Practice

- Wazuh installation links
- https://documentation.wazuh.com/current/installation-guide/index.html

- Zabbix server Installation links
- https://tecadmin.net/how-to-install-zabbix-server-on-ubuntu-22-04/
- Agent installation
- How to Install Zabbix Agent on Ubuntu 22.04 – TecAdmin

End

- By

- Mohamed Ali