



Опыт внедрения Open Source решений для контроля инфраструктуры ю

Lev Shumskii
Stanislav Gontarenko

– CISO at Association Fintech
– CISO at Mandarin Bank



«Типичная инфраструктура»!!!адинадин

Сети

Виртуальные, физические,
пиринговые

Железо

Множество разнобрендовых
серверов

Виртуальные машины

KVM

Контейнеры

Docker

Репозитории пакетов/кода

SVN/Gitlab

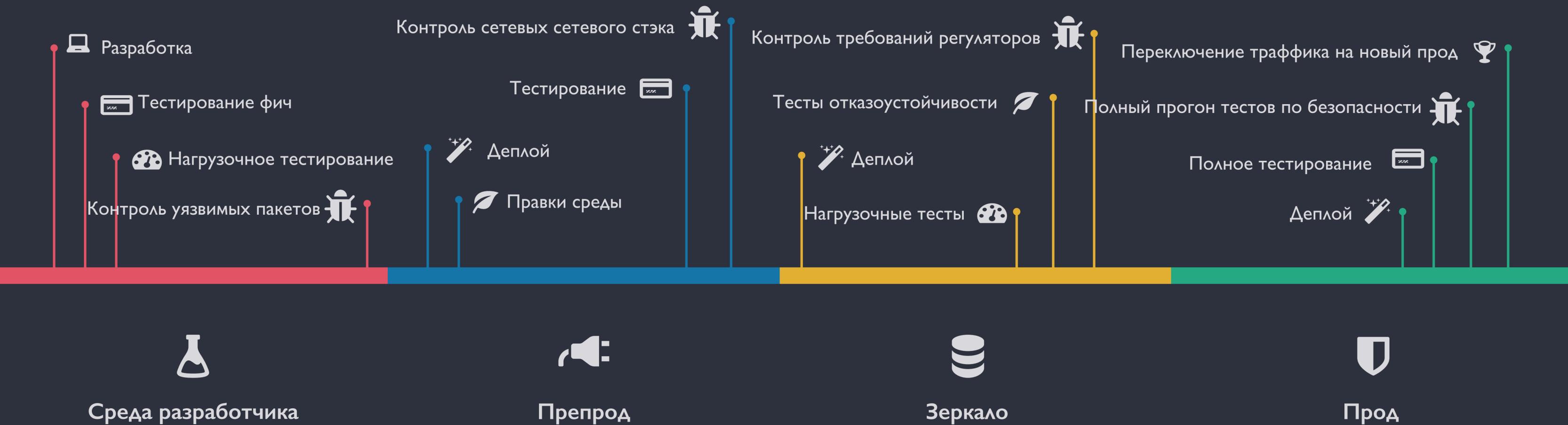
Обязка

Тестовые стенды, мониторинги,
сканнеры

Волшебный отказоустойчивый **прод**



Типичный жизненный цикл разработки ПО





☰ Задачи

- 📁 Комплаенс PCI DSS, ГОСТ 57580.1-2017
- 📄 Log Management
- ⌚ Integrity monitoring
- 📍 Vulnerability Management
- 📁 IT Asset management
- ⚠️ ... и не умереть на внедрении.



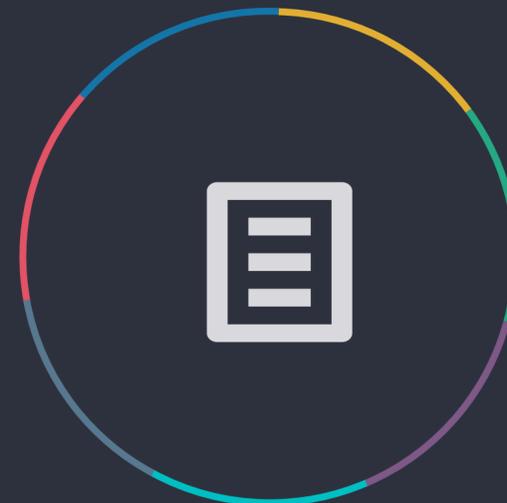
Мучительный выбор – за деньги



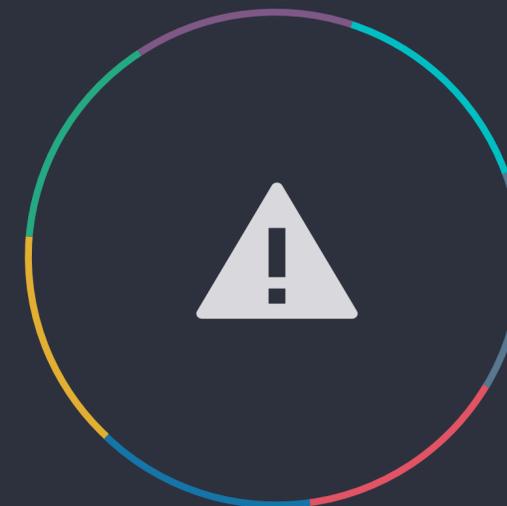
HIDS: AlienVault
Atomicorp
Solarwinds



SIEM: Splunk,
HP ArcSight,
FortiSIEM



Inventory: LanSweeper (\$1300/annual),
PT Maxpatrol



VM: Teanable.io,
PT Maxpatrol



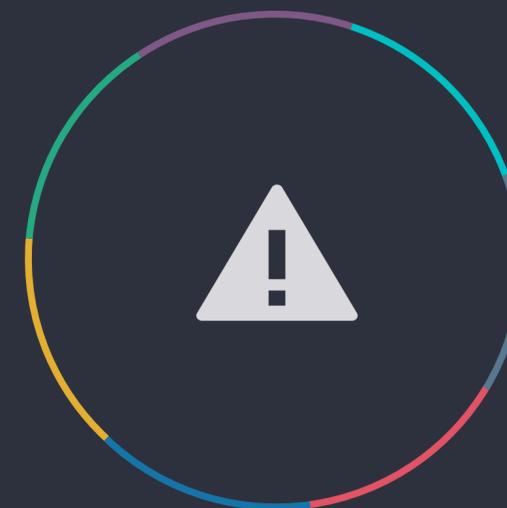
HIDS: HIDS OSSEC +
Wazuh



SIEM: OSSIM



Inventory: Fusion Inventory,
Alloy Navigator,
SpiceWorks



VM: vulners.com,
OpenVAS,
OSCAP



OSSEC

Log Analysis

File Integrity Monitoring

Intrusion Detection

Active Response

OpenSCAP

Policy Monitoring

Security Compliance

Vulnerability Assessment

System Hardening

Elastic Stack

Search Engine

Storage

Analytics

Visualization



Как выглядит подключение агента?

Развёртывание

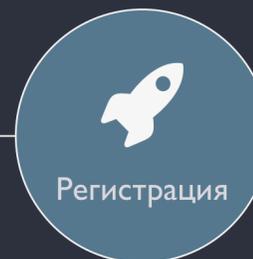
Деплой виртуальной
хоста/фермы
контейнеров/виртуальной
машины.



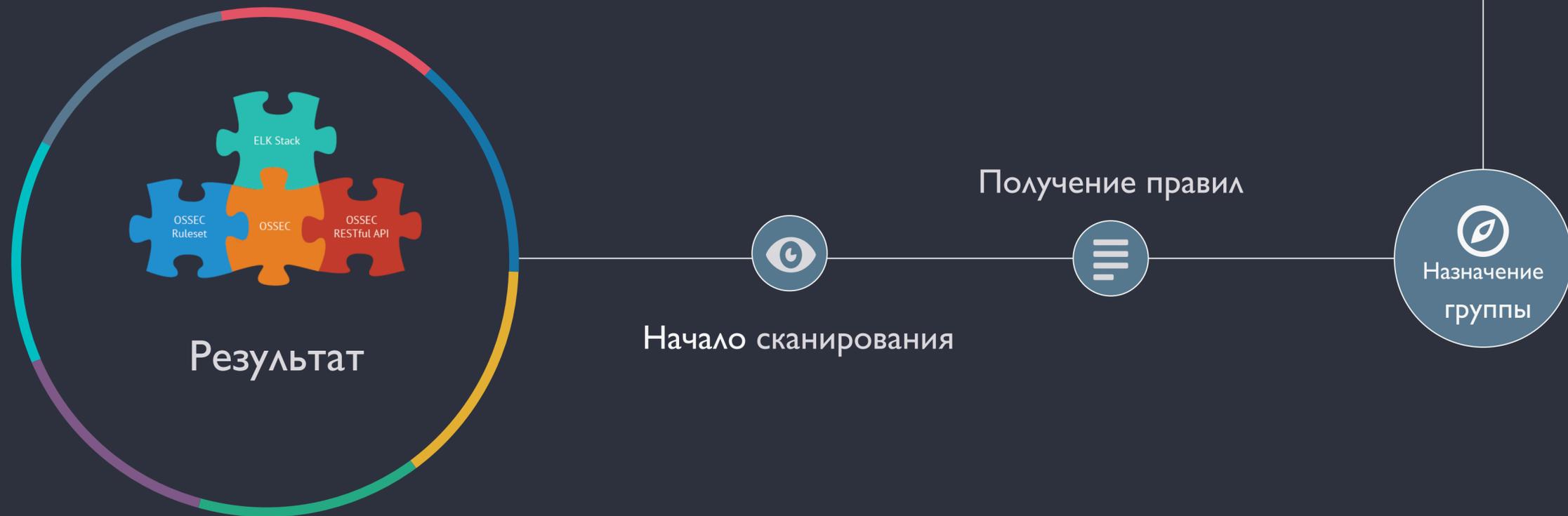
Обмен ключами
Любым способом



Запуск агента
Любым способом



Регистрация



Life Demo

Регистрация агента Wazuh:

```
File Edit View Search Terminal Help
[root@localhost shared]#
[root@localhost shared]# /var/ossec/bin/agent-auth -m i.wazi . .
2019/04/14 17:43:31 agent-auth: INFO: Started (pid: 23408).
INFO: No authentication password provided.
INFO: Connected to 10.0.0.4:1515
INFO: Using agent name as: localhost.localdomain
INFO: Send request to manager. Waiting for reply.
INFO: Received response with agent key
INFO: Valid key created. Finished.
INFO: Connection closed.
[root@localhost shared]#
```

Запуск агента Wazuh:

```
File Edit View Search Terminal Help
[root@localhost shared]#
[root@localhost shared]#
[root@localhost shared]#
[root@localhost shared]#
[root@localhost shared]#
[root@localhost shared]# service wazuh-agent start
Starting wazuh-agent (via systemctl): [ OK ]
[root@localhost shared]# service wazuh-agent status
wazuh-modulesd is running...
ossec-logcollector is running...
ossec-syscheckd is running...
ossec-agentd is running...
ossec-execd is running...
[root@localhost shared]#
```

Обратная сторона Wazuh - Inventory:

Agents / localhost.localdomain (235) / Inventory data

ACTIVE



Search by name, ID or IP address



Security events Integrity monitoring Inventory data

Cores: 1 Memory: 974.54 MB Arch: x86_64 OS: CentOS Linux 7 (Core) CPU: Intel(R) Core(TM) i7-7820HQ CPU @ 2.90GHz

📦 Packages

Last scan: 2019/04/15 05:48:46

Filter packages...



Name	Architecture	Version	Vendor	Description
plymouth-scripts	x86_64	0.8.9-0.31.20140113.el7.centos	CentOS	Plymouth related scripts
strace	x86_64	4.12-6.el7	CentOS	Tracks and displays system calls associated with a running process
python-linux-procfs	noarch	0.4.9-3.el7	CentOS	Linux /proc abstraction classes
resteasy-base-jaxrs	noarch	3.0.6-4.el7	CentOS	Module jaxrs for resteasy-base
xml-common	noarch	0.6.3-39.el7	CentOS	Common XML catalog and DTD files
alsa-firmware	noarch	1.0.28-2.el7	CentOS	Firmware for several ALSA-supported sound cards

1607 items (0.52 seconds)

1 2 3 4 5 Next »

Обратная сторона Wazuh – Integrity monitoring & Inventory:

Agents / localhost.localdomain (235) / Security events **ACTIVE** Discover

[Security events](#) Integrity monitoring Inventory data Auto-refresh This week

>_ Search... (e.g. status:200 AND extension:PHP) Options Refresh

manager.name: "wazuh" agent.id: "235" Add a filter +

Name: **localhost.localdomain** IP: **any** Version: **Wazuh v3.8.2** OS: **CentOS Linux 7**

Groups: **default**

Last keep alive: **2019-04-15 12:49:25** Registration date: **2019-04-15 12:48:26** Last syscheck scan: **ND** Last rootcheck scan: **2019-04-15 00:42:56**

Top 5 alerts

- System Audit event.
- kernel: out-of-bound...
- 389-ds-base: Mishan...
- glusterfs: Informatio...
- glusterfs: "features/i...

Top 5 groups

- vulnerability-detector
- ossec
- rootcheck

Top 5 PCI DSS Requirements

- 2.2.4
- 10.6.1
- 4.1
- 10.2.6
- 10.2.7

Alert level evolution

Count

@timestamp per hour

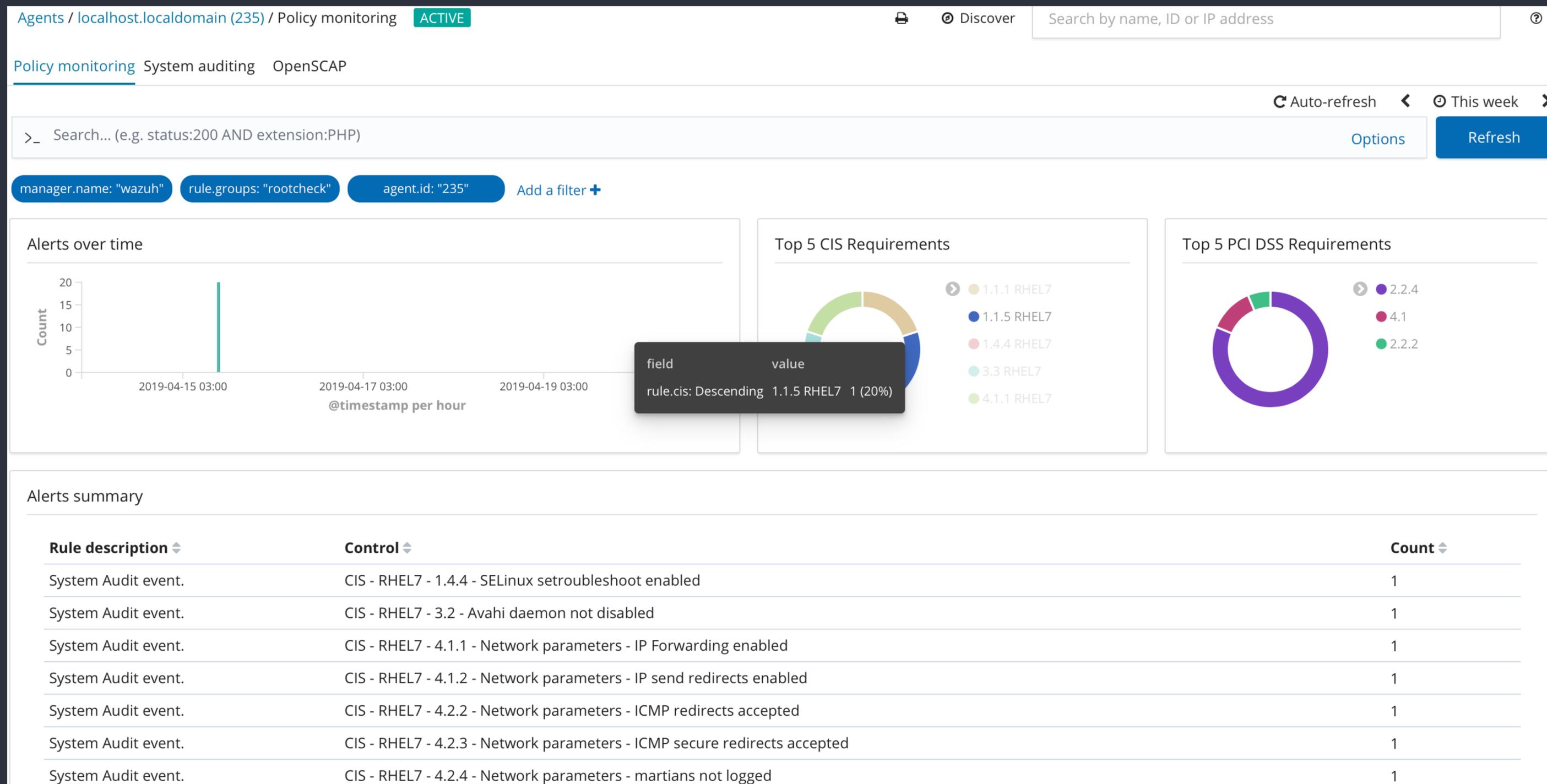
- 7
- 10
- 5
- 3
- 13

Alerts

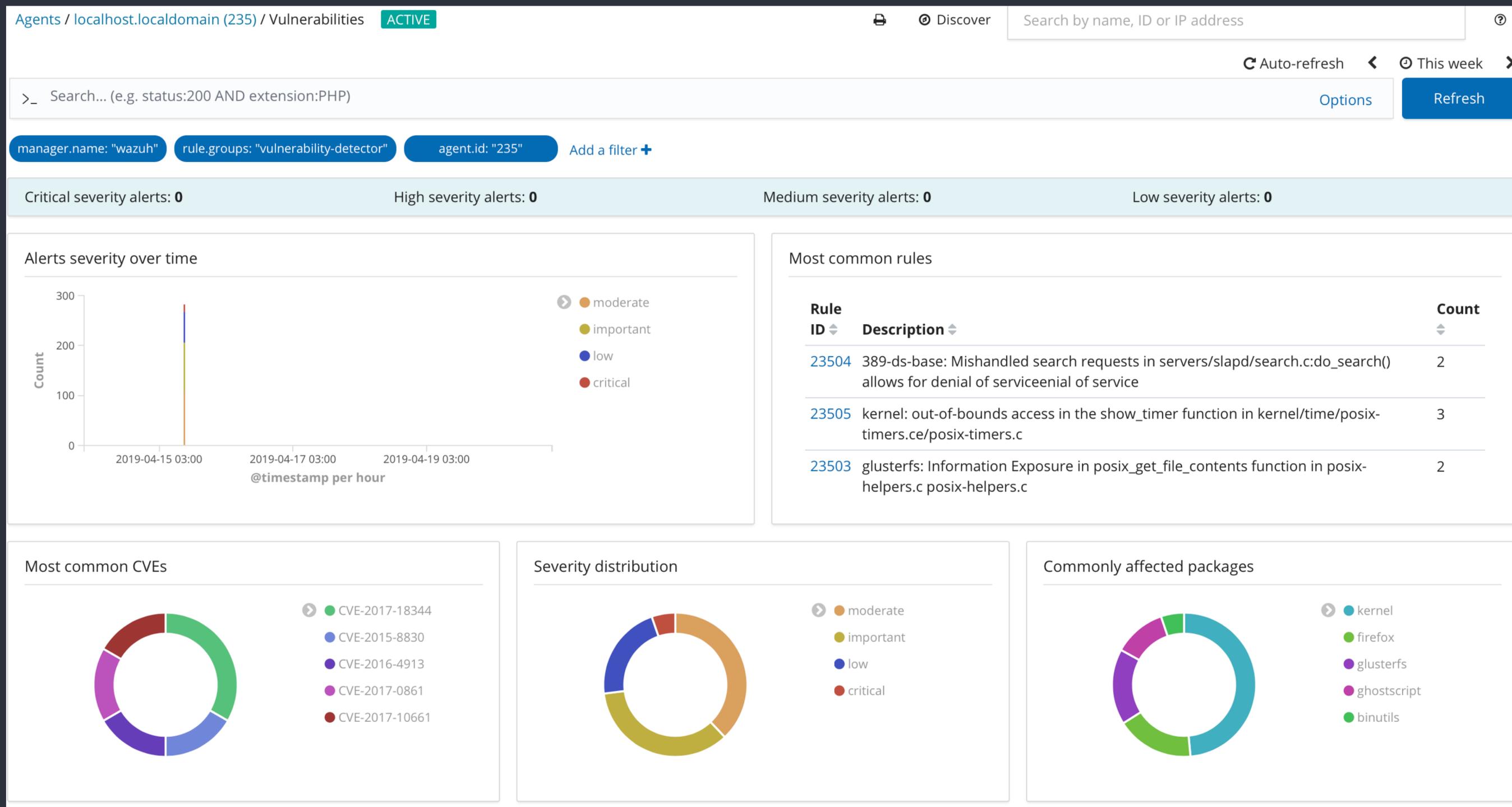
Count

Agent alerts

Обратная сторона Wazuh – OpenSCAP Report:



Обратная сторона Wazuh – Vulnerabilities Report:



В итоге:

Порядок с требованиями

Контроль конфигураций

Инвентаризация в реальном времени

Контроль уязвимостей ОС и прикладного ПО