Опыт внедрения Open Source решений для контроля инфраструктуры ю

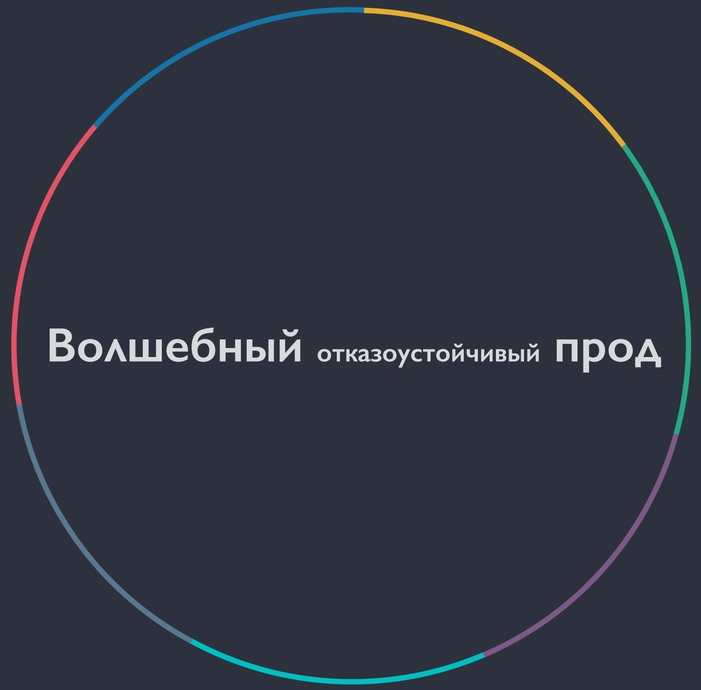
Lev Shumskii – CISO at Association Fintech
Stanislav Gontarenko – CISO at Mandarin Bank

«Типичная инфраструктура»!!!адинадин

Сети
Виртуальные, физические, пиринговые

Железо
Множество разнобрэндовых серверов

Виртуальные машины
KVM

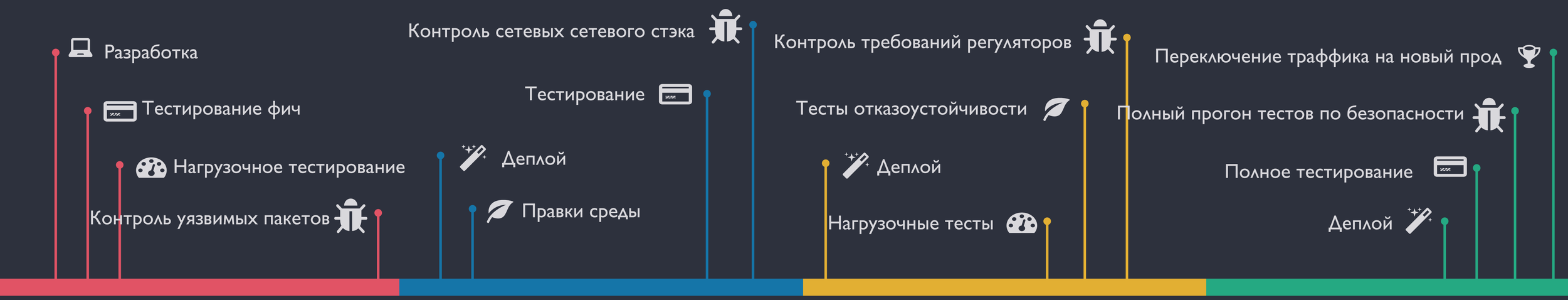


Контейнеры
Docker

Репозитории пакетов/кода
SVN/Gitlab

Обвязка
Тестовые стенды, мониторинги , сканнеры

Типичный жизненный цикл разработки ПО



Среда разработчика

Препрод

Зеркало

Прод

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

Мучительный выбор – Open Source

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?

Развёртываение

Деплой виртуальной хоста/фермы контейнеров/виртуальной машины.

Обмен ключами
Любым способом

Запуск агента
Любым способом

Результат

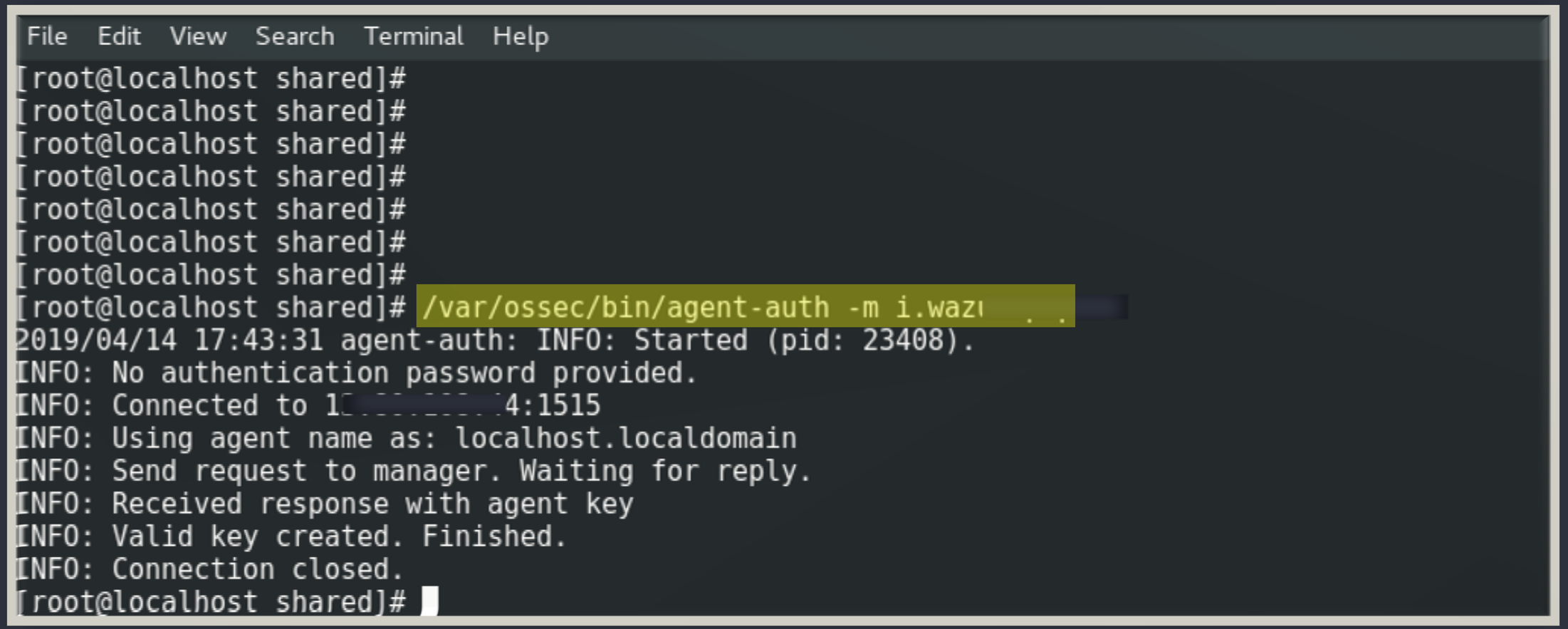
Начало сканирования

Получение правил

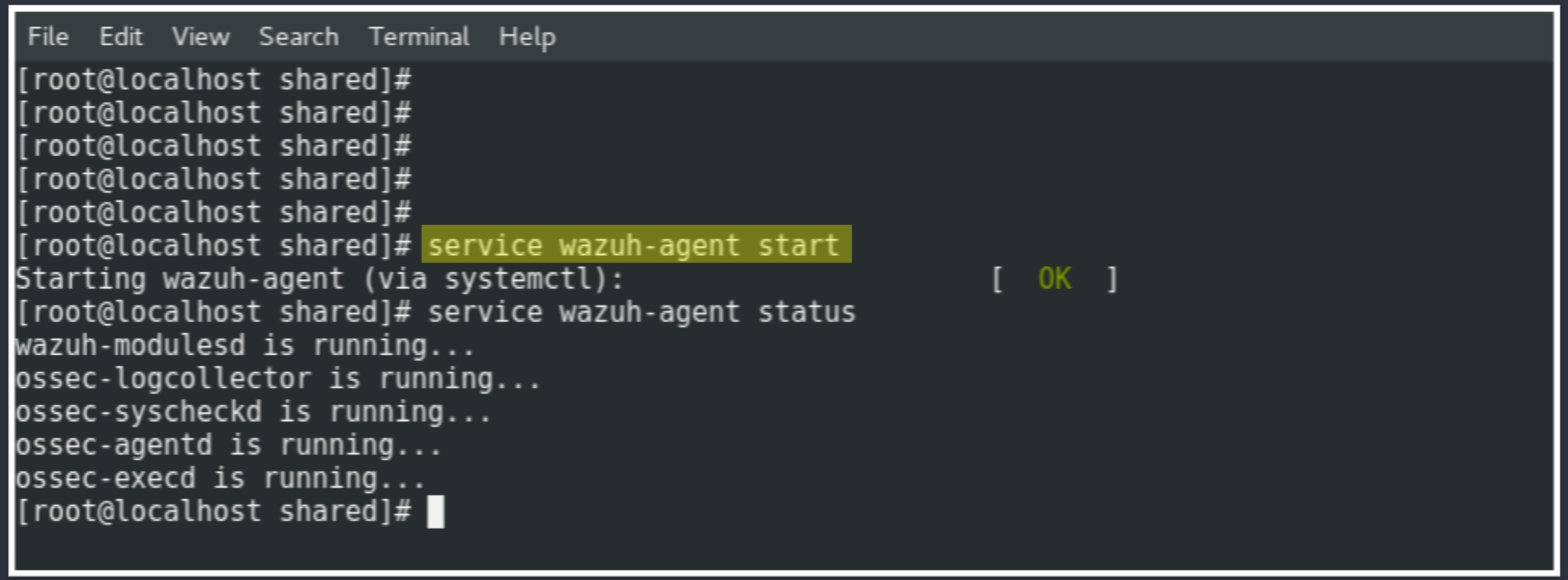
Назначение группы

Life Demo

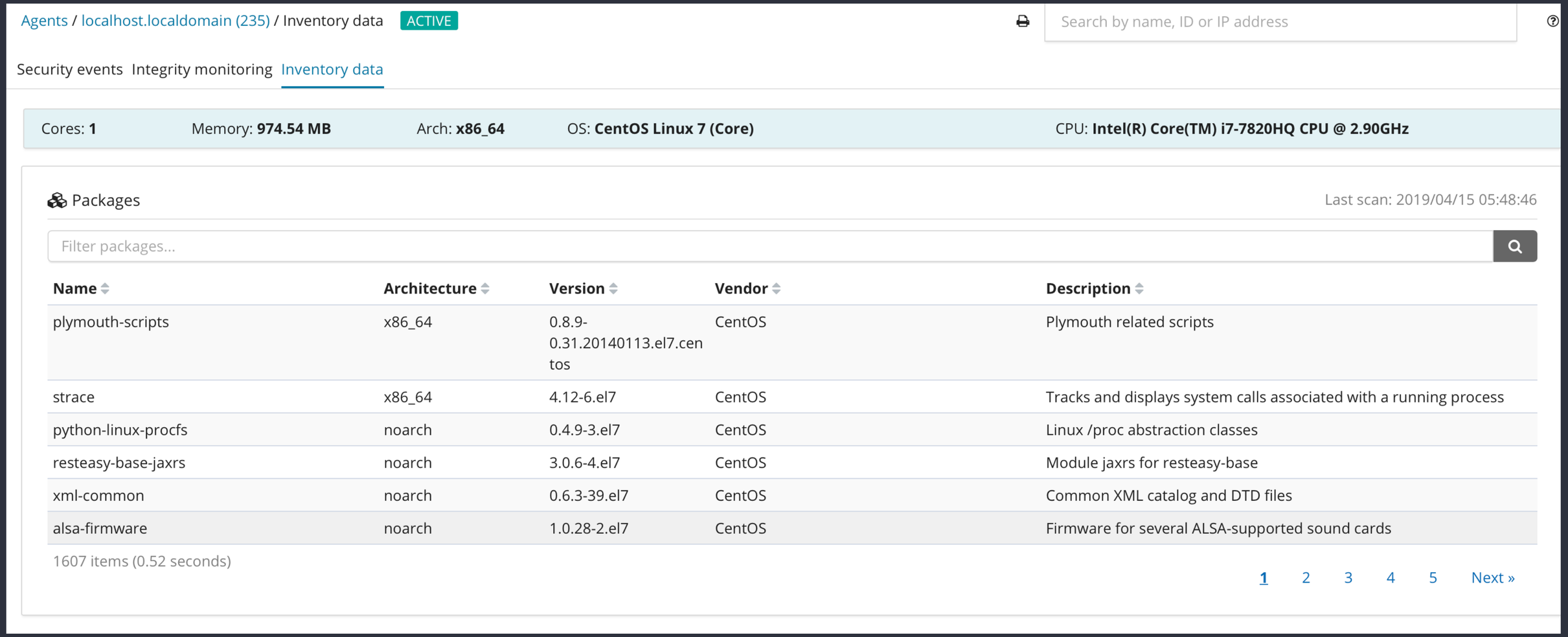
Регистрация агента Wazuh:



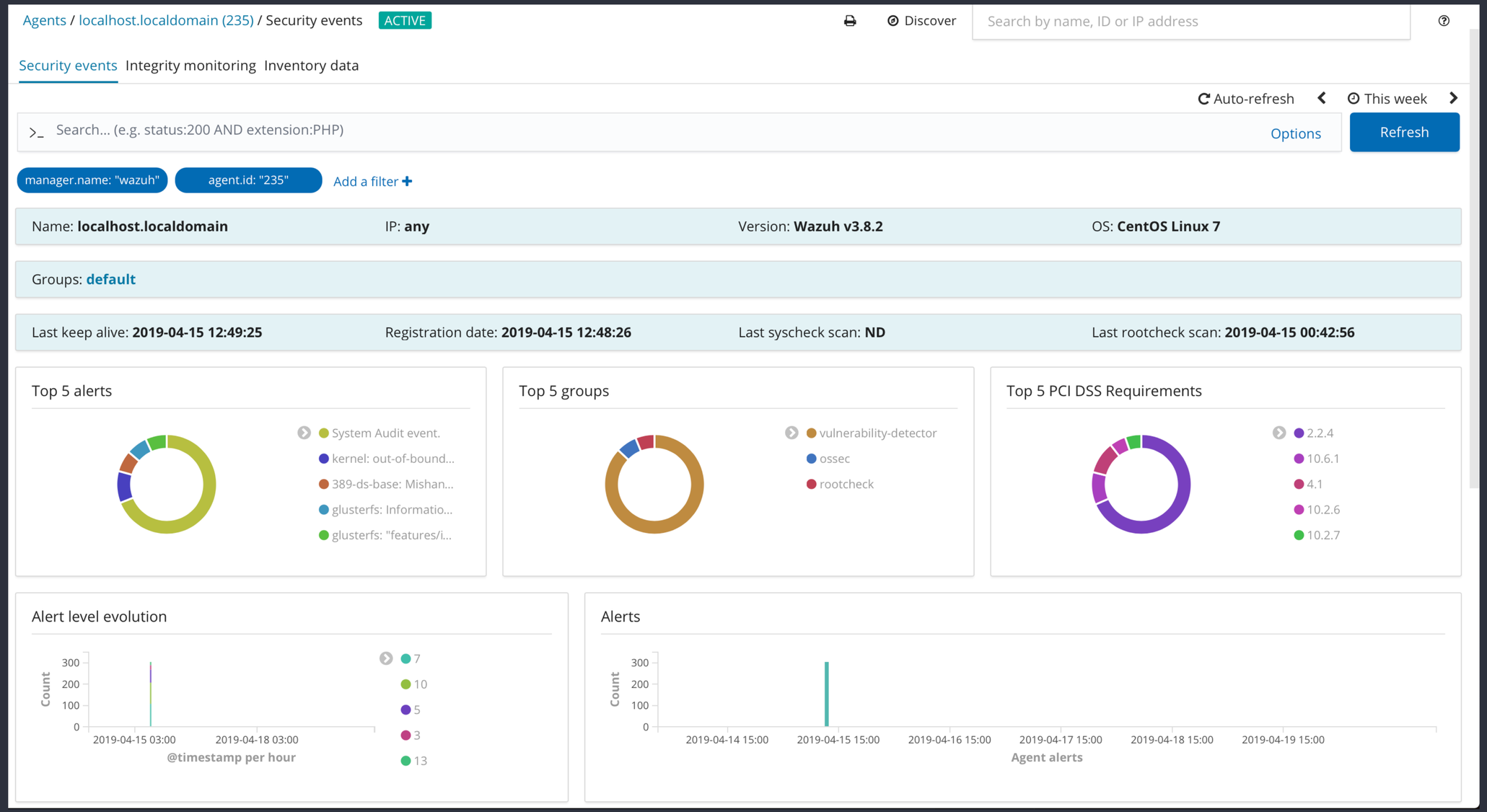
Запуск агента Wazuh:



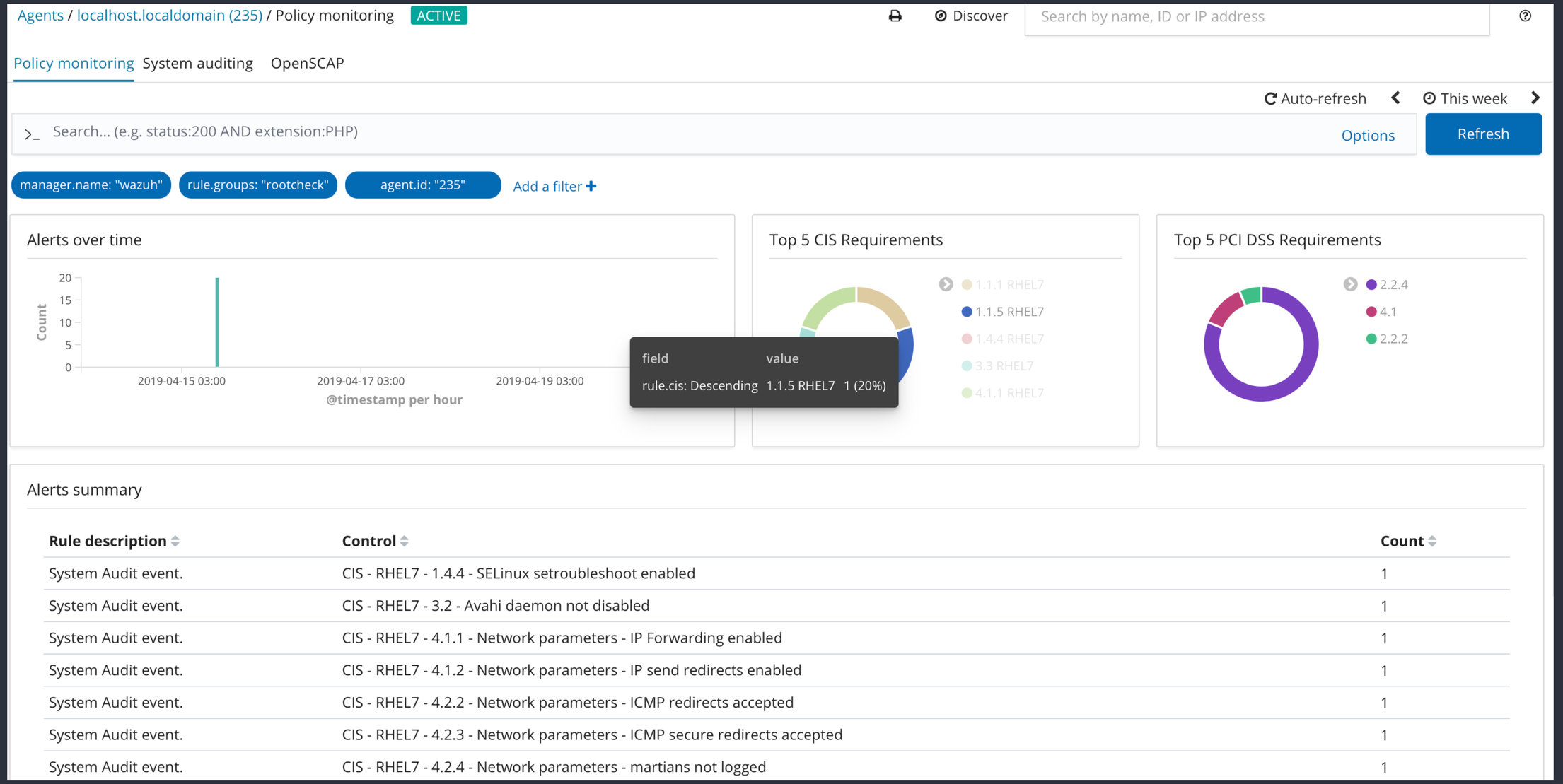
Обратная сторона Wazuh - Inventory:



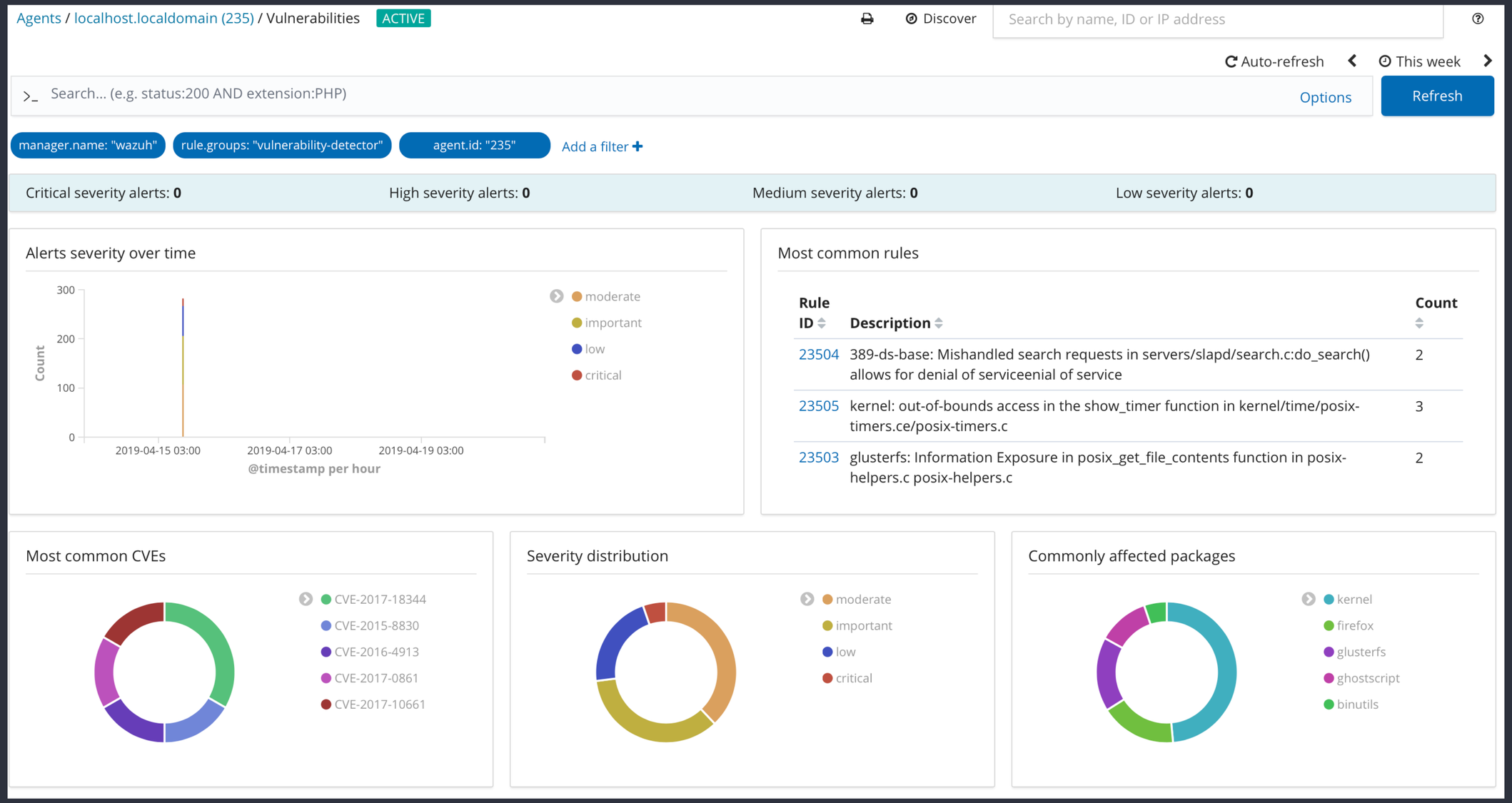
Обратная сторона Wazuh – Integrity monitoring & Inventory:



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