Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Wazuh SIEM для офиса 35 РМ: свой SOC без миллионных лицензий

За 5 дней разворачиваем open-source SIEM+XDR+FIM на одной VM, RDP-брутфорс ловим сразу

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Заказчик — производство на 35 РМ. Ночью зашифровали файловый сервер и 3 PC: антивирус пропустил, Windows-логи не сохранились, следов входа почти нет. Две недели присутствия атакующего никто не заметил. Нужна централизованная система, которая собирает события со всех хостов, коррелирует их правилами и шлёт алерт раньше, чем запустится шифровальщик — без коммерческого SIEM.

Почему это важно бизнесу

- Без централизации логов инцидент виден только постфактум, по факту шифрования
- Утечка 180 ГБ договоров и чертежей = репутационный и правовой ущерб
- Коммерческий SIEM для 40 хостов — сотни тыс. руб./год лицензий
- RDP/SMB наружу без мониторинга сканируются ботнетами круглосуточно
- Комплаенс (152-ФЗ, аудит доступа) требует хранимых событий безопасности

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4.14.6

актуальная стабильная ветка Wazuh, которую мы ставим (1 июля 2026)

release notes

0–16

шкала уровней правил; критичный алерт — от 12 и выше

docs ruleset

3 / 12

log_alert_level по умолчанию 3, порог e-mail-алерта 12

ossec.conf docs

1514/1515

TCP: 1514 события агентов, 1515 enrollment через authd

docs agent

8/16/500

наш стандарт all-in-one VM: vCPU/ГБ RAM/ГБ NVMe на 40 хостов

наш стандарт

55000

порт Wazuh API; индексер OpenSearch на 9200

docs architecture

РЕАЛИЗАЦИЯ 1 ИЗ 3

All-in-one развёртывание за 1 день

Что настраиваем

Производство, 35 PM + 5 серверов, домен AD, файловый сервер, 1С

Как мы это делаем

1. День 1: VM 8vCPU/16ГБ/500ГБ NVMe, установка manager+indexer+dashboard одним curl-скриптом wazuh-install.sh
2. Проверяем поднятие dashboard (443) и Wazuh API (55000), меняем дефолтные пароли indexer/admin
3. День 2: правила под AD — 4625 (RDP-брутфорс), 4720/4728/4732 (новые учётки/группы), правки GPO
4. Подключаем MITRE ATT&CK mapping и Security Configuration Assessment (CIS для Windows)

РЕЗУЛЬТАТ

Через ~40 минут после запуска скрипта веб-интерфейс живой, indexer принимает события. К концу дня 2 manager коррелирует Windows-события AD и раскладывает их по тактикам ATT&CK. Одна VM спокойно держит 40 агентов без выноса indexer на отдельный узел.

КЛЮЧЕВОЙ НЮАНС

Для SMB до 50-100 агентов разносить компоненты не нужно — all-in-one на NVMe экономит железо и упрощает бэкап и обновление.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Раскатка агентов и FIM за 2 дня

Что настраиваем

Тот же заказчик: 35 PC через GPO, 5 серверов вручную

Как мы это делаем

1. День 3: агенты на 35 PC через GPO (MSI + WAZUH_MANAGER), enrollment authd на 1515, серверы ставим руками
2. Ставим Sysmon на все хосты + подключаем Wazuh-рулсет Sysmon для powershell -enc, certutil
3. День 4: FIM (syscheck) на 1C Bases, \\fs01\Docs\Contracts, ветку реестра HKLM\SOFTWARE, report_changes=yes
4. Включаем vulnerability-detection + syscollector — сразу выявили 47 устаревших программ и 12 критичных CVE

РЕЗУЛЬТАТ

Все 40 хостов рапортуют на 1514. Syscollector собирает инвентарь ПО, модуль детекта уязвимостей сверяет его с фидами и подсвечивает CVE. FIM фиксирует изменение контрольных сумм критичных файлов с алертом уровня 7+.

КЛЮЧЕВОЙ НЮАНС

Sysmon + Wazuh-рулсет — это разница между 'запустился процесс' и 'запустился закодированный powershell'. Без него глубина аудита на Windows недостаточна.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Алертинг и первый месяц в эфире

Что настраиваем

Тот же заказчик: интеграция с Telegram и дежурство на абонентке

Как мы это делаем

1. День 5: integrator-модуль, кастомный скрипт в Telegram, фильтр level 12, канал админа и директора
2. 3-й день: пойман powershell с base64 из вложения письма — изолировали ноутбук до шифровальщика
3. 10-й день: 230 неудачных RDP с одного IP за 15 мин — алерт, блок IP и гео-фильтр на шлюзе
4. 29-й день: вторая волна RDP-подбора закрыта за 4 минуты по алерту

РЕЗУЛЬТАТ

За месяц предотвращён один крупный инцидент и закрыто 14 уязвимостей. Правило коррелирует серию 4625 по одному источнику и поднимает уровень до критичного, событие уходит в Telegram за секунды.

КЛЮЧЕВОЙ НЮАНС

Первый месяц идёт калибровка — ложные срабатывания нормальны. Мы тюним пороги frequency/timeframe и исключения, иначе шум обесценит алерты.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Дефолтные пароли indexer/admin**
  all-in-one скрипт генерирует креды — их надо сразу сменить и закрыть 9200/55000 от LAN, иначе SIEM сам становится точкой входа.
- ✕ **Active Response на автобан сразу**
  Авто-блок firewalld/iptables без белых списков легко положит свою же сеть или отрубит админа. Включаем аккуратно, с исключениями.
- ✕ **Ждать, что Wazuh заменит антивирус**
  Это дополняющий HIDS/XDR, а не антивирус. Microsoft Defender или корпоративный AV остаются обязательными.
- ✕ **Агенты без Sysmon**
  Без Sysmon-рулсета не видно powershell -enc, certutil, инъекций. Голый Windows-лог даёт мало контекста для детекта.
- ✕ **Нет калибровки правил**
  Первый месяц — шквал ложных. Без тюнинга frequency/timeframe и исключений админ перестаёт читать алерты.
- ✕ **Хранить FIM без report_changes**
  Без report_changes и настроенного scan видно только факт изменения, но не что именно поменялось — расследование буксует.
- ✕ **Ждать сетевых атак от Wazuh**
  Это HIDS, трафик он не разбирает. Для сетевого детекта нужен Suricata IDS, интеграция с ним отдельная.
- ✕ **Один узел без бэкапа индексов**
  all-in-one — единая точка отказа. Снапшоты indexer и бэкап VM обязательны, иначе теряется вся история событий.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- all-in-one VM 4vCPU/8ГБ, Wazuh 4.14.x, агенты на все хосты
- Правила 4625 RDP-брутфорс + FIM на файловый сервер и 1С
- log_alert_level 3, ручной просмотр дашборда ежедневно

НОРМАЛЬНО

- VM 8vCPU/16ГБ NVMe, Sysmon + Wazuh-рулсет на всех хостах
- vulnerability-detection + syscollector + SCA (CIS)
- Integrator в Telegram/Slack для алертов уровня 12+

ХОРОШО

- Active Response с белыми списками, интеграция Suricata IDS
- Снапшоты indexer + бэкап VM, разнесение узлов при росте
- Абонентское дежурство: разбор алертов, обновление правил под новые CVE

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Сменить дефолтные пароли indexer/admin, закрыть 9200/55000/1516 от LAN
- [ ] Агенты на 100% хостов, enrollment через authd на 1515, события на 1514
- [ ] Sysmon + Wazuh Sysmon-рулсет на всех Windows-хостах
- [ ] FIM (syscheck) на 1C Bases, договоры, критичные ветки реестра, report_changes=yes
- [ ] vulnerability-detection + syscollector включены, фиды обновляются
- [ ] SCA прогоняет CIS-политику по хостам, разобраны failed-проверки
- [ ] Правила AD: 4625, 4720/4728/4732, изменения GPO, чтение NTDS.dit
- [ ] Integrator шлёт алерты уровня 12+ в Telegram, пороги откалиброваны
- [ ] Настроены снапшоты индексов и бэкап VM SIEM
- [ ] Active Response включён только с белыми списками сетей и админов

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем all-in-one Wazuh 4.14.x за 5 рабочих дней под ключ
- Пишем правила под AD, 1С и вашу инфраструктуру, мапим на MITRE ATT&CK
- Раскатываем агенты через GPO + Sysmon, настраиваем FIM и детект CVE
- Ведём алерты на абонентке: разбор, реакция 15 мин в рабочее время, отчёт директору
- Бесплатный аудит логов серверов и контроллера домена за месяц по Москве и МО

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Wazuh Release notes 4.x (4.14.6) (documentation.wazuh.com — 2026)

02 Components / architecture: manager, indexer, dashboard, agent (documentation.wazuh.com — 2026)

03 Rules classification (levels 0-16) (documentation.wazuh.com — 2026)

04 ossec.conf: syscheck (FIM), vulnerability-detection, integration (documentation.wazuh.com — 2026)

05 Agent enrollment (authd, 1514/1515) (documentation.wazuh.com — 2026)

06 Security Configuration Assessment (CIS) (documentation.wazuh.com — 2026)

07 Alert management (log_alert_level, alerts.log) (documentation.wazuh.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.