МТС ФИНТЕХ

Сколько агентов ИБ нужно для счастья?

Актуальный взгляд на мониторинг, защиту и зрелость безопасности (или нет)

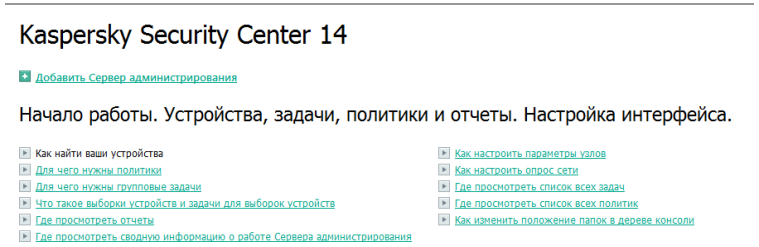
Руслан Талипов

Руководитель центра сопровождения
средств защиты и реагирования

Обзор агентов

Антивирус (AV)

Базовый «страж» на каждой рабочей станции.



Сигнатуры, эвристика.

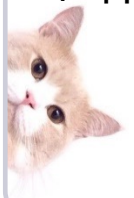
А также: МСЭ, контроль программ, file integrity, ваш АВЗ пожрал все место на диске

DLP

Система предотвращения утечек конфиденциальных данных

- На Windows
- А еще и на Mac

А также: контроль программ, file integrity, кошмарить сотрудников, учет рабочего времени, цифровой Гулаг



EDR

Отслеживает активность процессов, действия пользователя и сетевые подключения на устройстве и передает эту телеметрию в централизованный центр анализа.

А также: отсутствие адекватного контента, а зачем ты изолировал продовую БД?

На рынке множество решений (EDR, DLP, AV, NAC, SIEM, MDM (а winlogbeat точно агент?) и т.д.),
и компании часто мучаются от «зоопарка» агентов на рабочих станциях и серверах.
Зададимся вопросом: «Можно ли найти баланс?»

Detect vs Protect

Detect

Продукты «детекта» (EDR, SIEM, IDS) собирают и анализируют события, сигнатуры и поведение, чтобы выявлять аномалии, взломы, малварь

Примеры

- EDR-агент записывает все процессы и сетевые подключения, SIEM кореллирует логи
- AV/NGAV останавливает вирусы,
- NAC не пускает неизвестный хост в сеть

Достоинства: можно отследить сложные атаки, проанализировать инциденты задним числом

Недостатки: само по себе обнаружение не всегда предотвращает развитие атаки

Protect

(AV, DLP, NAC, FW) блокируют нежелательные действия, запрещают доступ, не дают вывести данные

Примеры

- DLP блокирует отправку файлов с ПДн
- AV/NGAV останавливает вирусы,
- NAC не пускает неизвестный хост в сеть

Достоинства: прямое сокращение рисков (запрет, шифрование), меньше человеческого фактора

Недостатки: требуют тонкой настройки, могут ломать бизнес-процессы (ложные блокировки)

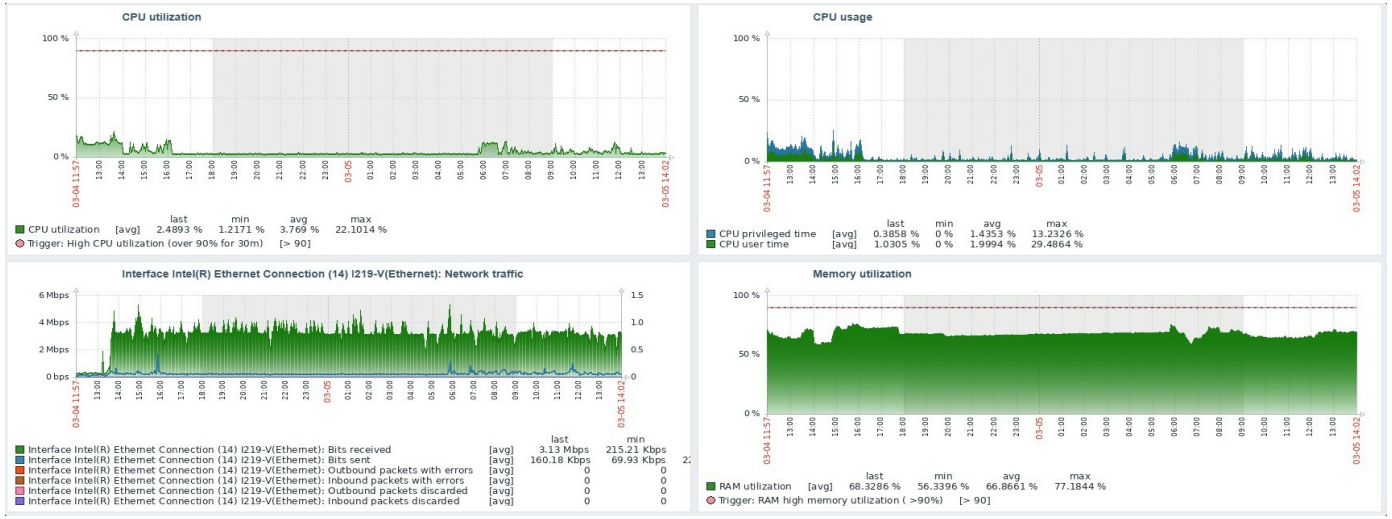
Агенты и их последствия

Проблемы избытка

Где-то нужен detect, где-то protect — и вот уже 5+ агентов у каждого пользователя.
EDR, DLP, NAC, SIEM-коллектор, MDM-агенты для мобильных устройств и ноутов, vulnerability-сканеры, конфигурационные менеджеры, агенты шифрования дисков и т.д.

agent fatigue (усталость)

- средняя крупная компания может использовать до 75 различных средств кибербезопасности одновременно
- некоторые устройства имеют >10 различных защитных агентов*



На графиках видим — проблема не в нас

* Данные absolute.com

Проблемы избытка агентов:

1. **Конфликты:** агенты разных производителей могут мешать друг другу.
2. **Нагрузка:** каждый агент потребляет CPU, память, диск. Несколько агентов одновременно могут заметно замедлять систему
3. **UX:** обилие агентов = обилие уведомлений, перезагрузок и прочих неудобств

Мониторим нагрузку, проактивно отдаем триггеры в ИТ, отключаем избыточные контроли

Linux встроенные «агенты» и службы

- auditd – отслеживает доступ к ключевым файлам (например, /etc/shadow, /bin/bash)
- osquery – опрашивает систему через SQL-интерфейс: пользователи, процессы, конфигурации
- eBPF – собирает и фильтрует события ядра (процессы, сеть) без установки драйверов
- nftables – управляет сетевыми фильтрами, предотвращает нежеланные соединения
- syslog – перенаправляет события в центральную систему (SIEM, logserver)
- fail2ban – автоматически блокирует IP-адреса после неудачных попыток логина (SSH)

```
# auditd: отслеживаем изменения паролей
 -w /etc/passwd -p wa -k passwd_changes
# osquery: поиск изменённого bash
 SELECT name, path, md5 FROM hash
WHERE path = '/bin/bash';
 # fail2ban: лог блокировки
 fail2ban.actions: NOTICE [sshd] Ban
192.0.2.10
```

- Эти инструменты дают минимально необходимую телеметрию: можно видеть вмешательства в систему, выявлять lateral movement и попытки эскалации.
- Можно использовать без внешних агентов — что важно на серверах, где ИТ против дополнительных компонентов.
- Оркестрация (Ansible, SaltStack) — в идеале контролируется совместно, но при зрелой ИБ — лучше иметь read-only аудит и отдельную логику для систем повышенного риска.

MDM: как мы доставляем защиту

- **Позволяет централизованно устанавливать и обновлять агенты безопасности** (например, EDR, DLP) на корпоративные устройства (ноуты, смартфоны, планшеты)
- **Автоматическое развертывание и конфигурация:** не нужно вручную бегать к каждой машине
- **Управление политиками:** заставить устройство шифровать диск, включать пароль/PIN, проверять, стоит ли нужный агент

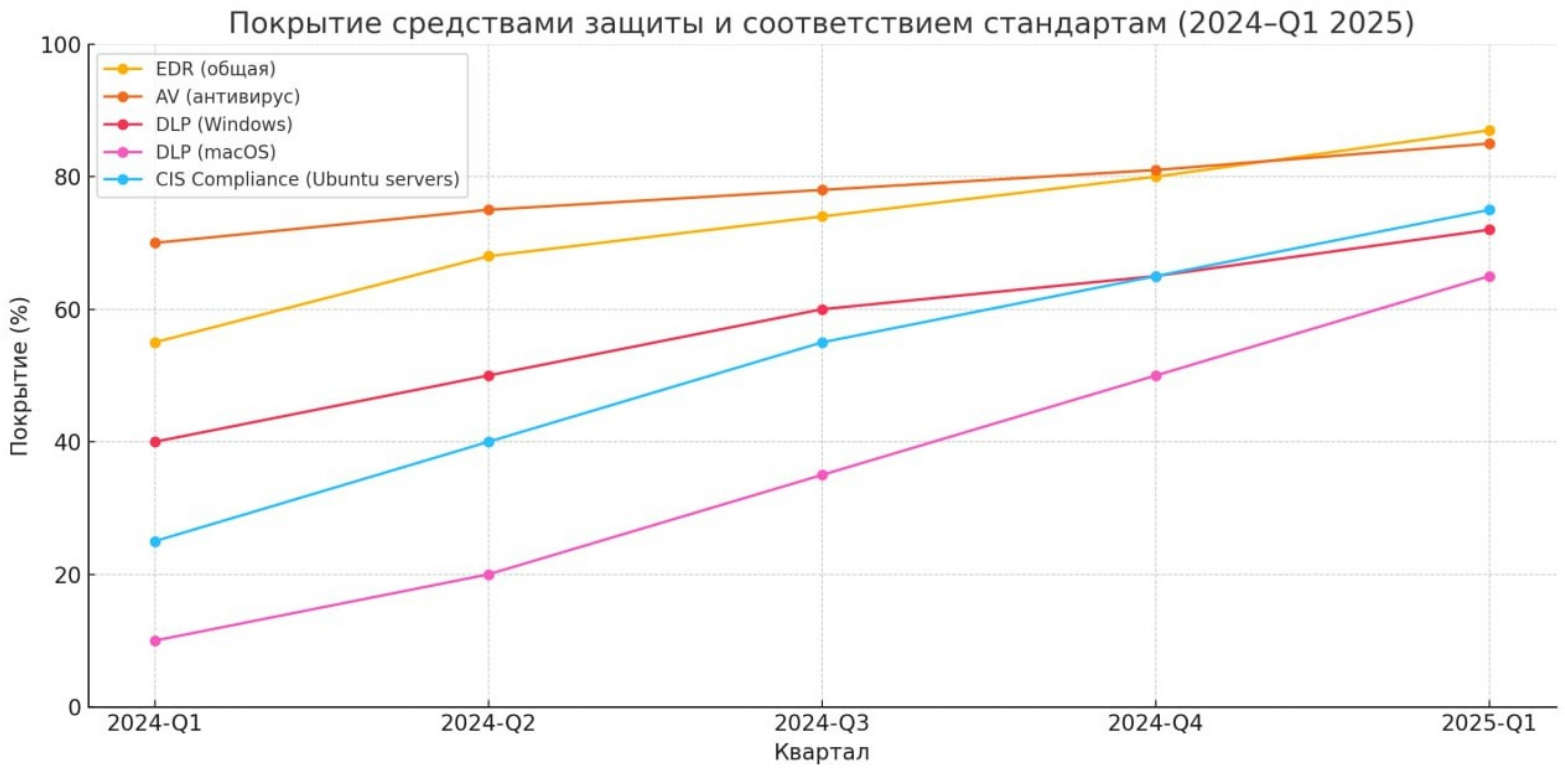
Плюсы

- ✓ Единый способ внедрить нужное ПО на сотни/тысячи устройств
- ✓ Можно в реальном времени убеждаться, что агент актуален, не отключен

Минусы

- ✓ MDM сам по себе может быть еще одним «агентом»
- ✓ Увеличивает сложность администрирования, если не интегрировать с другими системами

Метрики — как единая точка



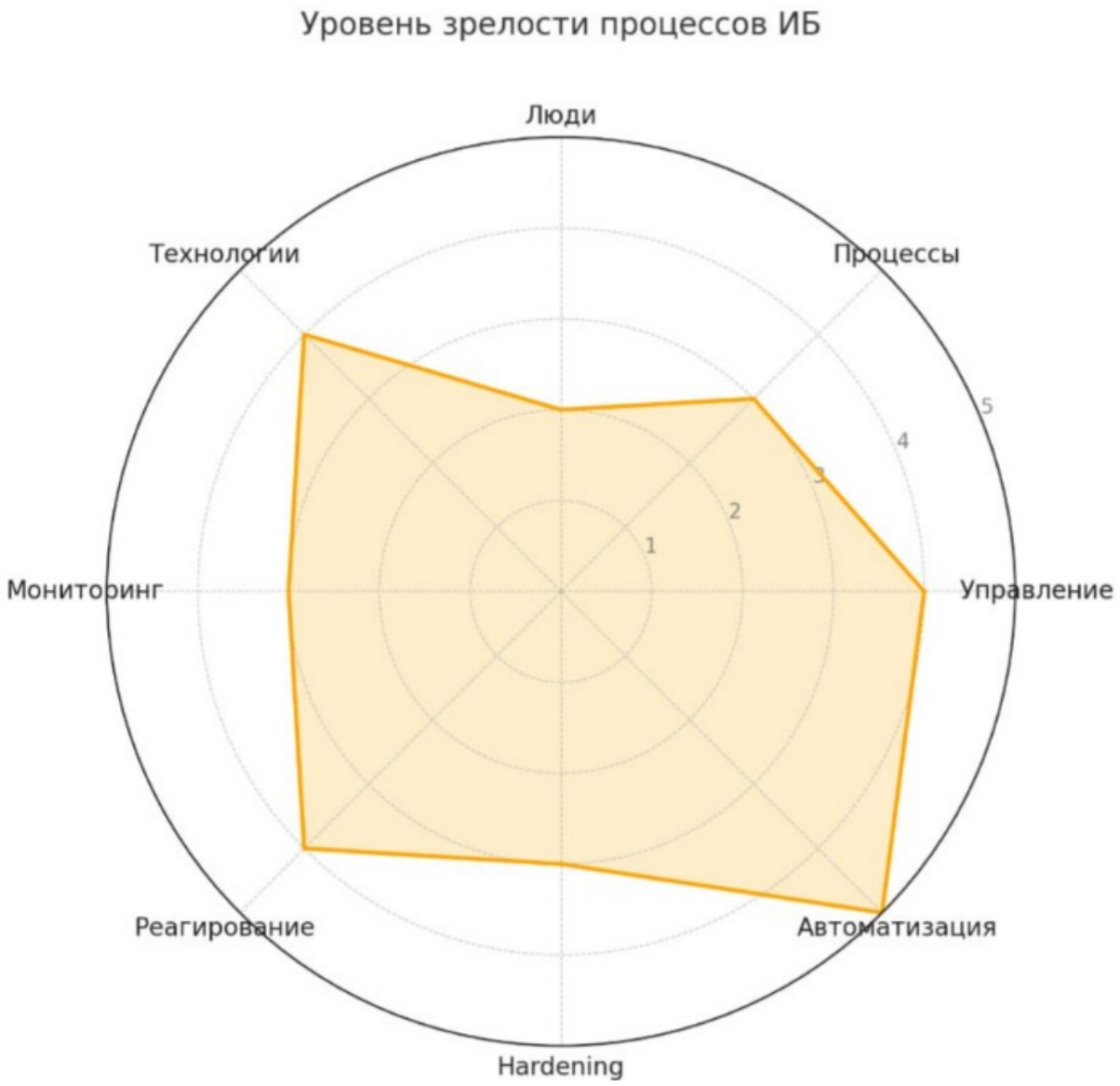
От «сводных таблиц» — в реальное бизнес-принятие решений

Метрики можно автоматизировать и визуализировать

Позволяет говорить с бизнесом цифрами: «у нас покрытие 78%, но 200 устройств без шифрования»

```sql
SELECT
  quarter,
  AVG(CASE WHEN control = 'EDR' THEN coverage ELSE NULL END) AS edr,
  AVG(CASE WHEN control = 'AV' THEN coverage ELSE NULL END) AS av,
  AVG(CASE WHEN control = 'DLP_WINDOWS' THEN coverage ELSE NULL END) AS dlp_win,
  AVG(CASE WHEN control = 'DLP_MAC' THEN coverage ELSE NULL END) AS dlp_mac,
  AVG(CASE WHEN control = 'CIS_UBUNTU' THEN coverage ELSE NULL END) AS cis_ubuntu
FROM security_coverage
GROUP BY quarter
ORDER BY quarter;
```

Maturity model — не бегите сразу за всем



Уровни зрелости

Уровень 1 (Initial):
• Только базовый AV / Firewall
• Нет единого мониторинга

Уровень 2 (Managed):
• EDR, DLP, MDM
• Частичное применение SIEM, настройка политик

Уровень 3 (Integrated):
• Централизованный мониторинг (SIEM + SOAR)
• Процессы инцидент-менеджмента (участие IT и бизнеса)

Уровень 4 (Automated):
• XDR, собственные сценарии Threat Hunting
• Автоматизация рутин (плейбуки SOAR)

Уровень 5 (Optimized):
• Культура Continuous Improvement
• Глубокая интеграция ИБ-практик и KPI в бизнес

Коробочный контент — не панацея

Коробка

ТН

```yaml
title: Suspicious PowerShell Encoded
logsource:
  product: windows
  service: powershell
detection:
  selection:
    CommandLine|contains: 'EncodedCommand'
  condition: selection
level: high
```

Коробочный контент — не панацея

Кастомный контент

ТН

```yaml
title: Suspicious PowerShell Encoded Command from Uncommon Parent
description: Detects PowerShell launching with an encoded command from an unusual parent process often
associated with malware droppers or document exploits.
status: experimental
date: 2025/04/14 # Пример даты
logsource:
  category: process_creation # Используем общую категорию создания процессов
  product: windows
detection:
  selection_pwsh:
    Image|endswith: '\powershell.exe' # Имя процесса PowerShell
    CommandLine|contains: # Ищем флаг кодирования и его варианты
      - 'EncodedCommand'
      # - '-Enc ' # Раскомментируйте для добавления вариантов, если нужно
      # - '-E ' # Будьте осторожны, '-E ' может дать много ложных срабатываний
  selection_parent:
    ParentImage|endswith: # Список подозрительных родительских процессов
      - '\winword.exe'
      - '\excel.exe'
      - '\outlook.exe'
      - '\powerpnt.exe'
      - '\mshta.exe'
      - '\wscript.exe'
      - '\cscript.exe'
      - '\rundll32.exe'
      # - '\services.exe' # Может быть легитимным, но иногда используется вредоносами
      # - '\wmiprvse.exe' # Тоже требует осторожности
  condition: selection_pwsh and selection_parent
falsepositives:
  - Некоторые специфические административные скрипты или ПО для развертывания (очень редко).
  - Требует анализа и возможной подстройки списка родительских процессов под конкретную инфраструктуру.
level: high
tags:
  - attack.execution
  - attack.defense_evasion
  - attack.t1059.001 # PowerShell
  - attack.t1027     # Obfuscated Files or Information
```

Выводы

- Количество агентов: баланс между рисками и удобством
- Зрелость: корень успеха, нужны люди и процессы, а не только коробка
- Threat Hunting — реальная защита от сложных целевых атак
- Помним про бизнес-ценность — безопасность должна помогать, а не мешать
- Количество агентов безопасности должно быть оптимальным и минимально необходимым. Счастье — не в количестве, а в качестве и согласованности их работы

Автоматизируйте рутину, интегрируйте инструменты — и будет вам счастье, и пользователям, и бизнесу! (или нет)

Вопросы?