

Безвыходных ситуаций не бывает. Разбираем 5 кейсов 2017 года



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Алексей Васильев, Руководитель Центра мониторинга

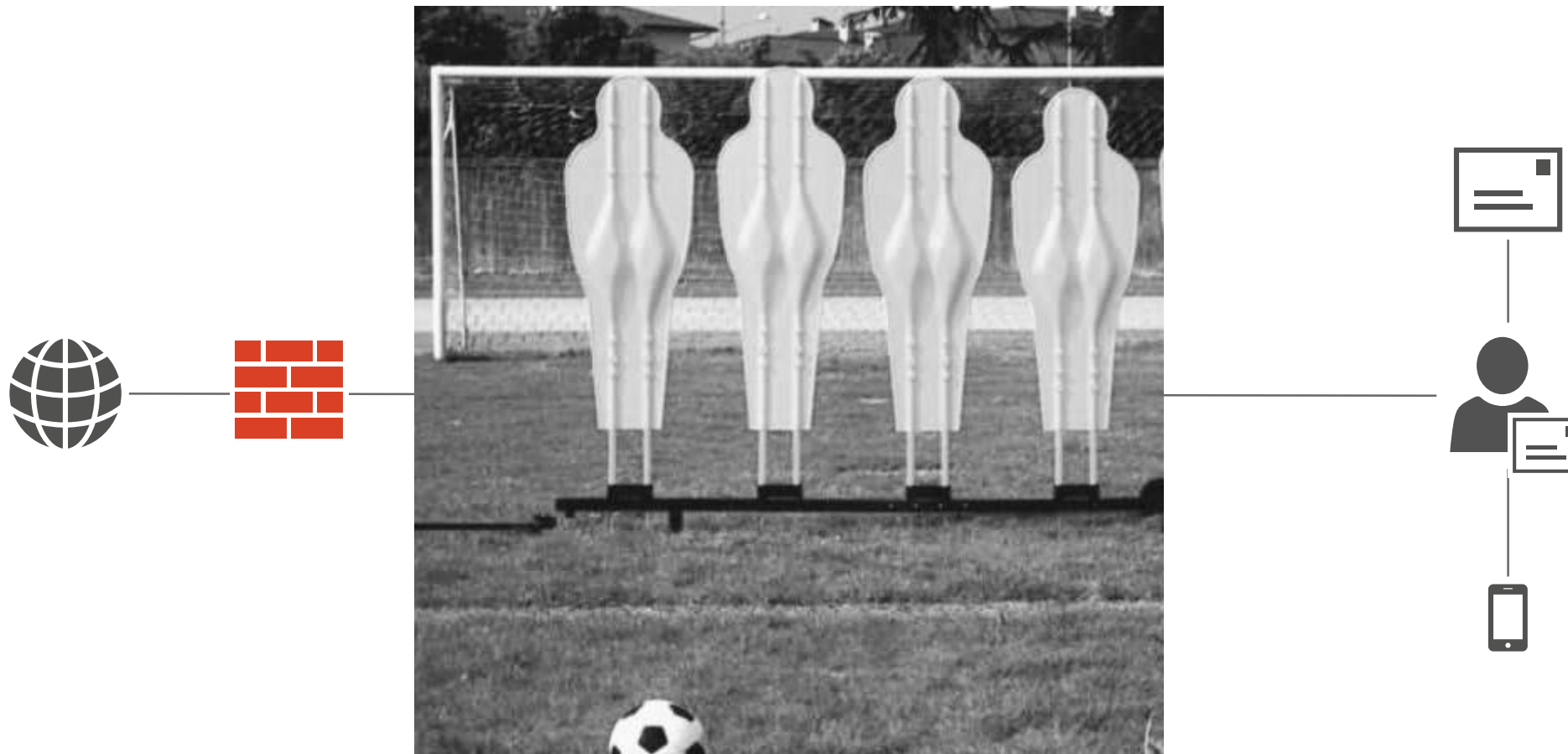
С чем сталкивается Центр мониторинга



План

- Распределение усилий
- Выявление и реагирование
- Технические возможности и ожидания

Периметр безопасности



«To breach or not to breach?»



Кейс 1. Организационные вопросы

Проблемы обработки

- 1 я линия: отбор событий
- 2 я линия: анализ событий и обработка инцидентов





Кейс 2. Реагирование

Проблемы реагирования



То густо



То пусто

- МНОГО ОТВЕТСТВЕННЫХ ЛИЦ

- ОТСУТСТВИЕ ОТВЕТСТВЕННЫХ ЛИЦ

Координация действий



Технические возможности и ожидания

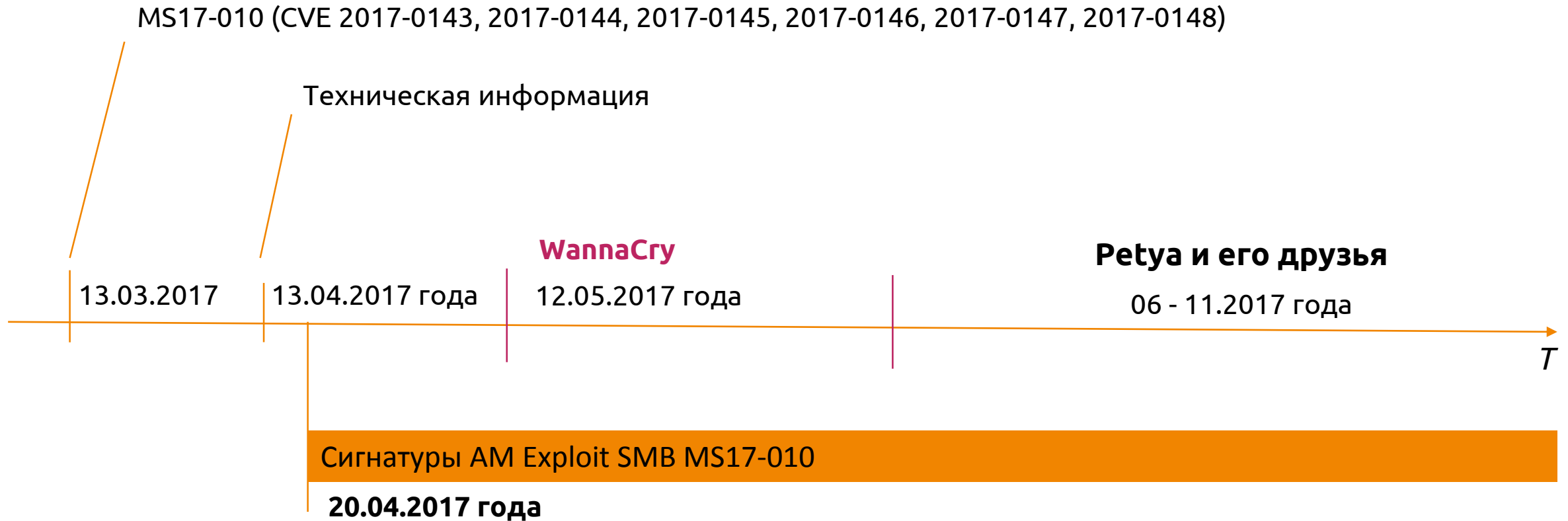


- База знаний для систем обнаружения вторжений
- Интеллектуальные системы принятия решений по инцидентам
- Анализ уязвимостей и их устранения
- Улучшение контроля защищенности информационной сети



Кейс 3. База знаний

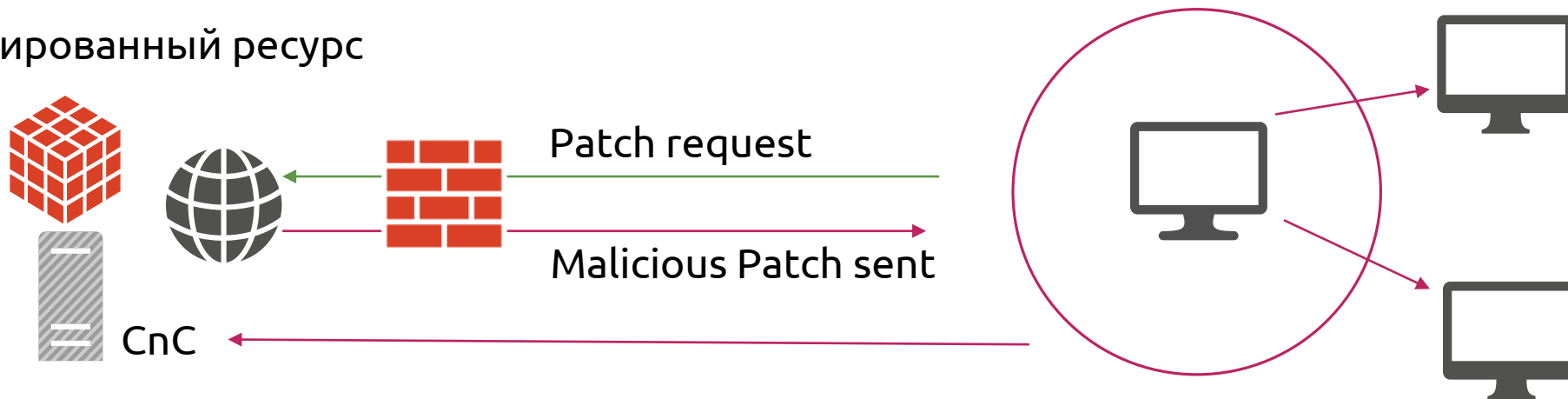
Применение базы знаний обнаружения вторжений



Детектирование notPetya



Скомпрометированный ресурс



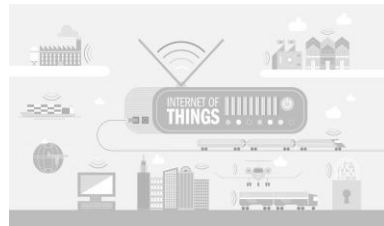
Правила обнаружения уровня сети



Более 2100 правил в 2017 году



- Прикладные системы (Apache CVE-2017-5638, 2017-9805, Equifax)



- Атаки с применением IoT, (Mirai)



- АСУ ТП, (Compromise)





- Банковские трояны, (IceID)

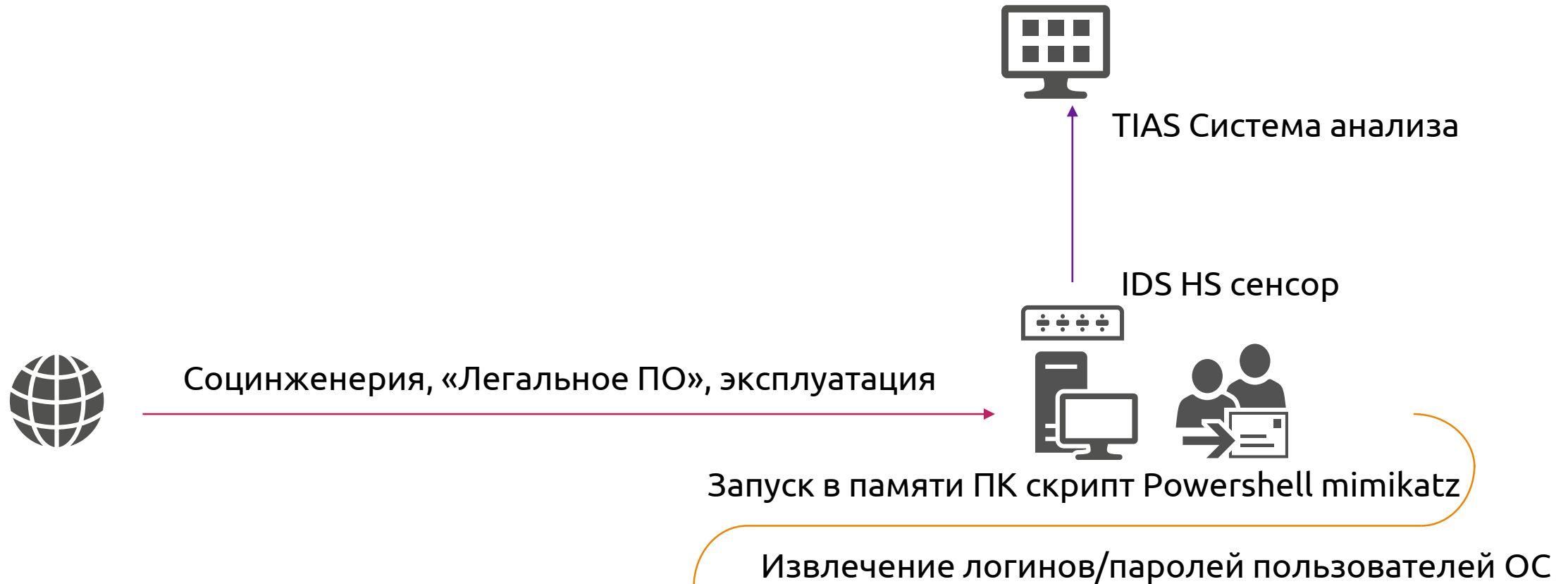
Не забывайте про обновление правил!

Правила обнаружения вторжений уровня узла. Поведенческий анализ



Закрепление	Повышение привилегий	Отключение защитных технологий ОС
Изменение системной конфигурации	  более 750 правил	Инструменты: powershell фреймворки/скрипты
Сбор данных о хосте/сети	Подозрительная активность	Вредоносные артефакты: IOCs, включая APT

Детектирование Mimikatz



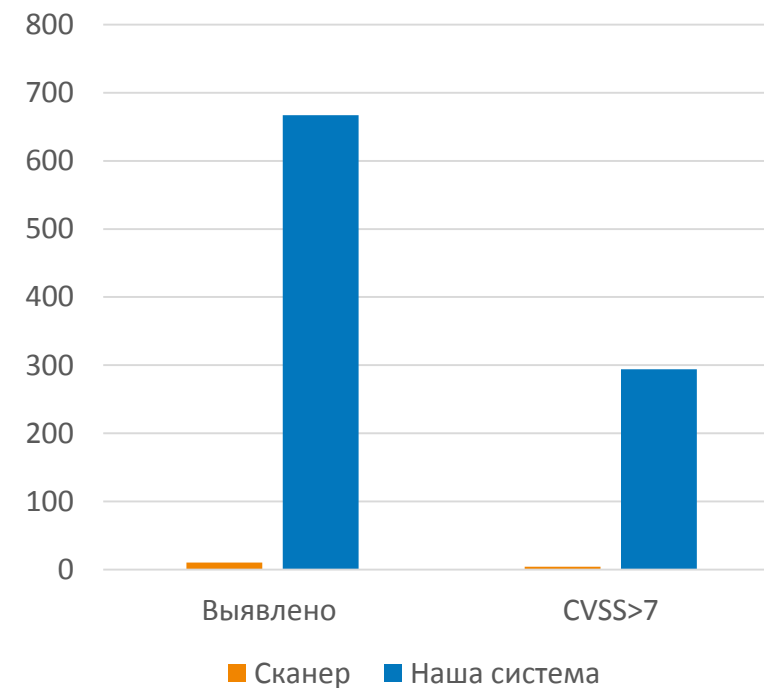


Кейс 4. Ожидание

Сравнение данных анализа уязвимостей



	Сканер	Наша система анализа
Всего	10	667
CVSS >7	4	294

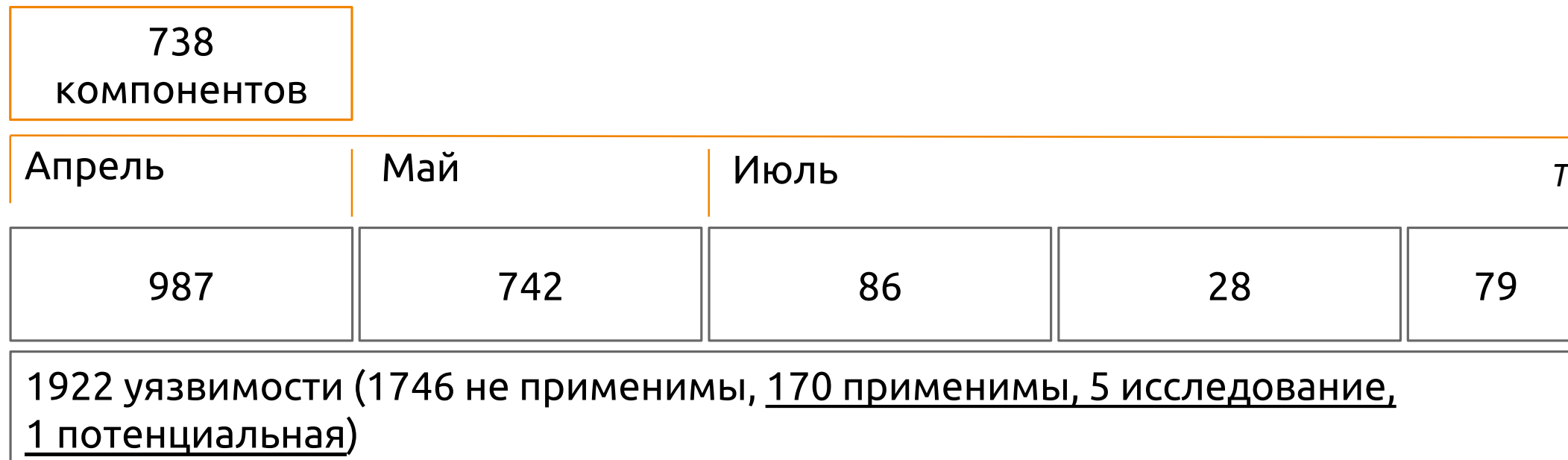


Анализ уязвимостей и их устранение



Сервис	Текущая версия
PHP	5.5.9 -1, 5.3.5, .3.28, 5.1.4, 5.3.3, 5.3.3, 5.3.2, 5.3.6, 5.3.27, 5.5.38
Microsoft SQL Server	Microsoft SQL Server 2012 SP1 Версия 11.0.3000
OpenSSL	0.9.8n

Пример анализа уязвимостей сервер Linux



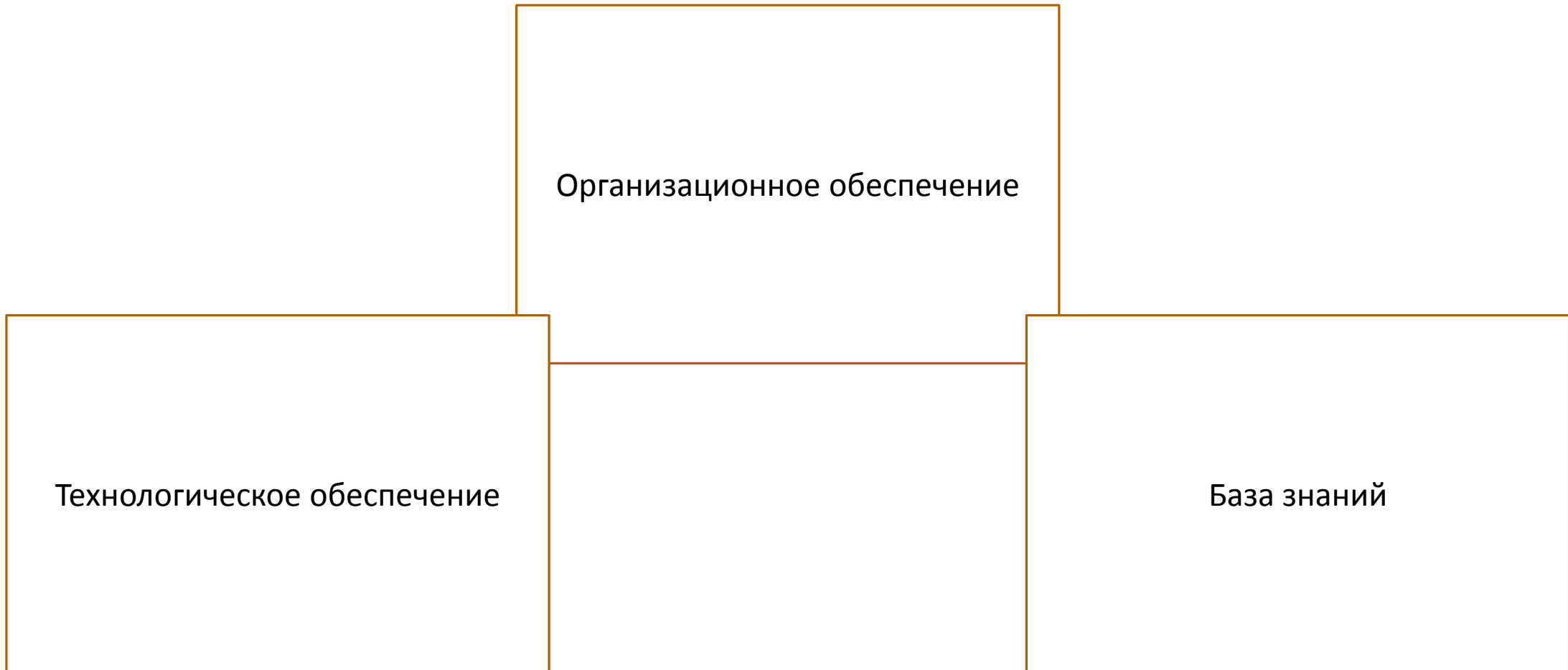


Кейс 5. Улучшение

Улучшение контроля защищенности информационной сети



Для Центров мониторинга





Спасибо за
внимание!

Алексей Васильев

Начальник отдела разработки и
эксплуатации систем мониторинга и
аналитики

Руководитель Центра мониторинга

Aleksey.Vasilyev@amonitoring.ru