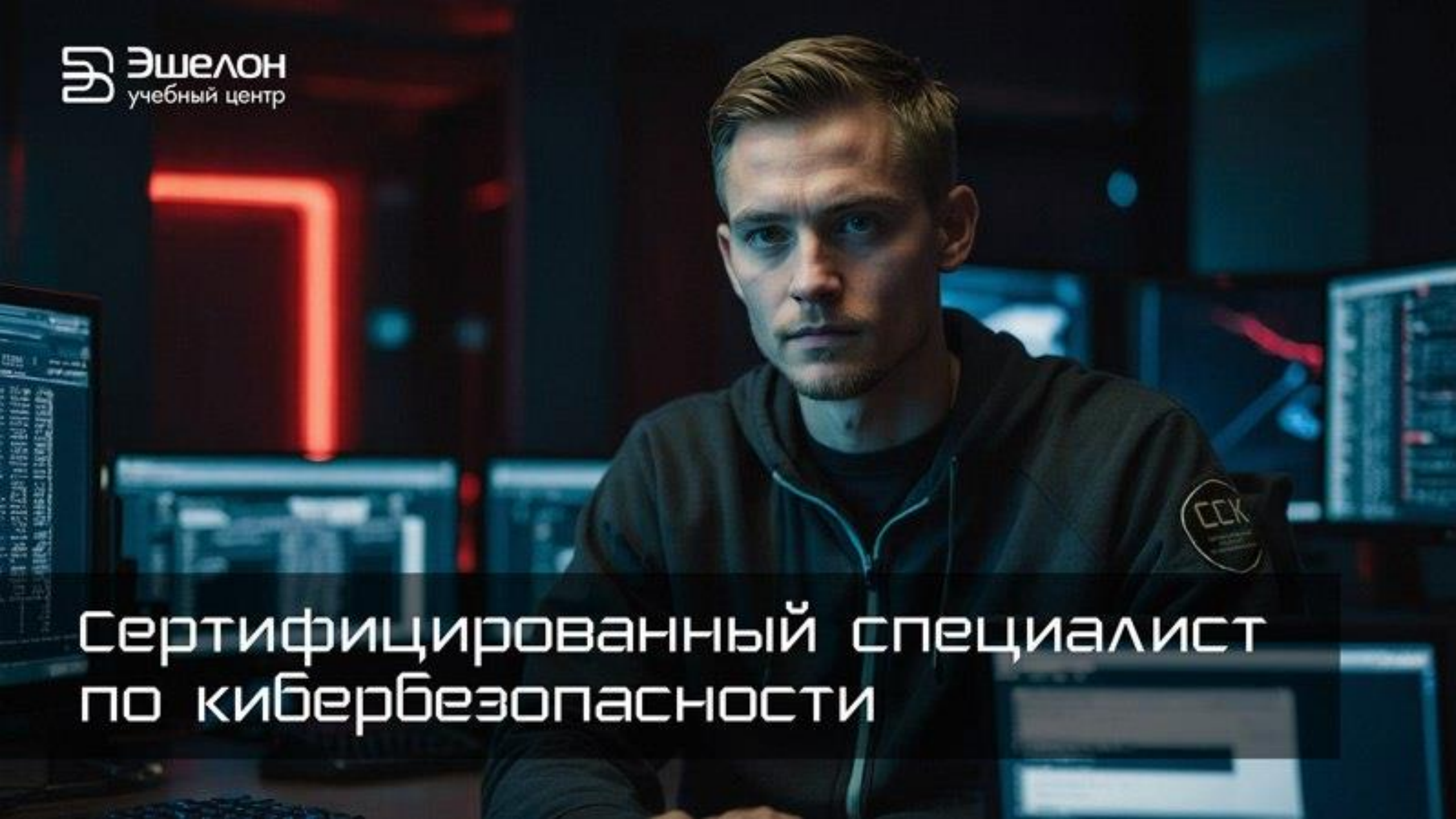
Эшелон
комплексная безопасность

Взять под контроль ИБ: управление уязвимостями и выявление инцидентов

Александр Дорофеев, генеральный директор АО «Эшелон Технологии»

ГК «Эшелон»

- 19 лет на рынке
- Входит в рейтинги крупнейших ИБ/ИТ-компаний (CNews, Эксперт РА)
- Специализация: SIEM, VM, FW, IDS, анализ кода
- Разработки включены в реестр российского ПО и сертифицированы ФСТЭК России, Минобороны России
- Создатели российской системы сертификации специалистов по кибербезопасности «ССК»

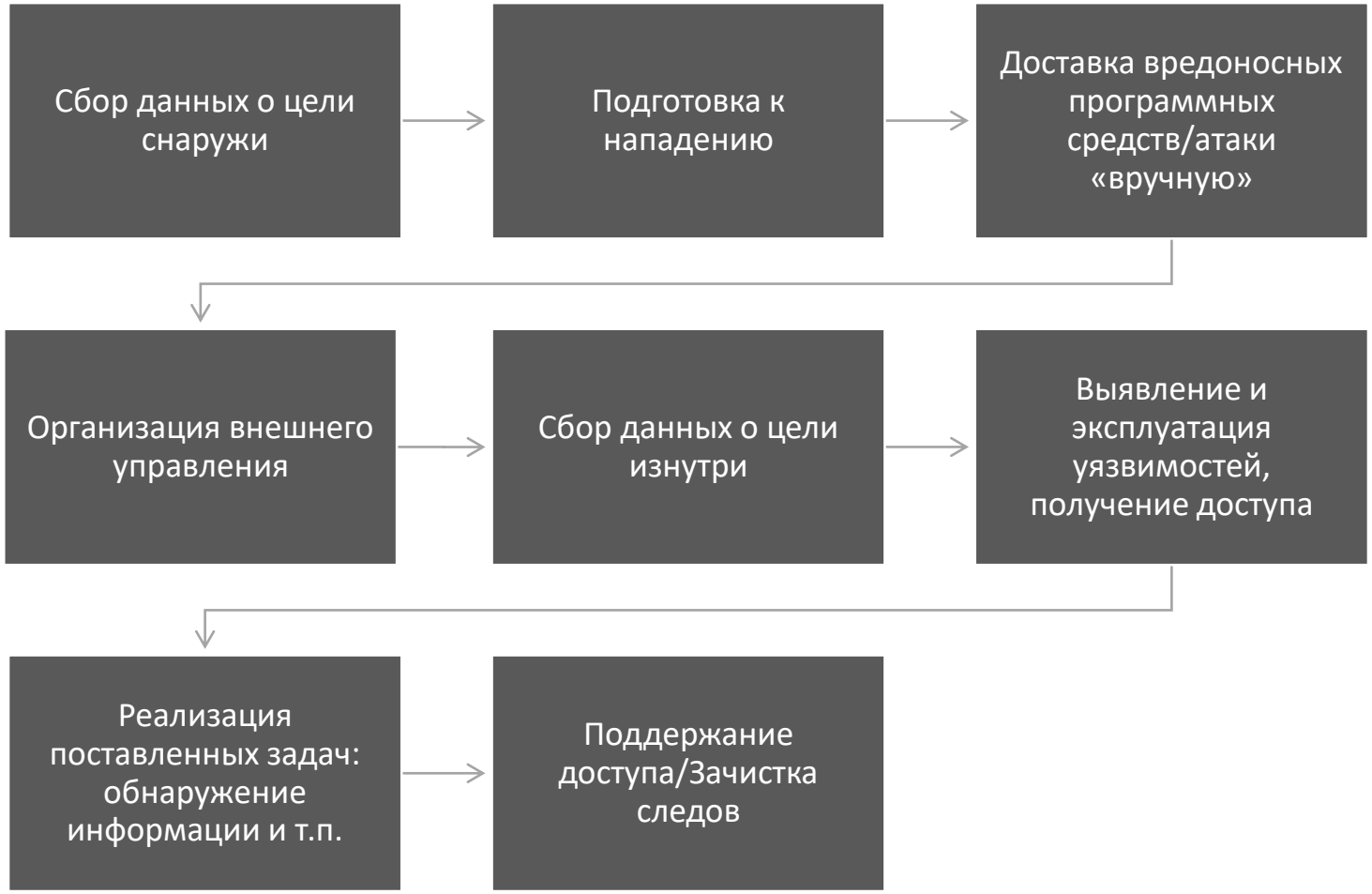


Сертифицированный специалист по кибербезопасности

План доклада

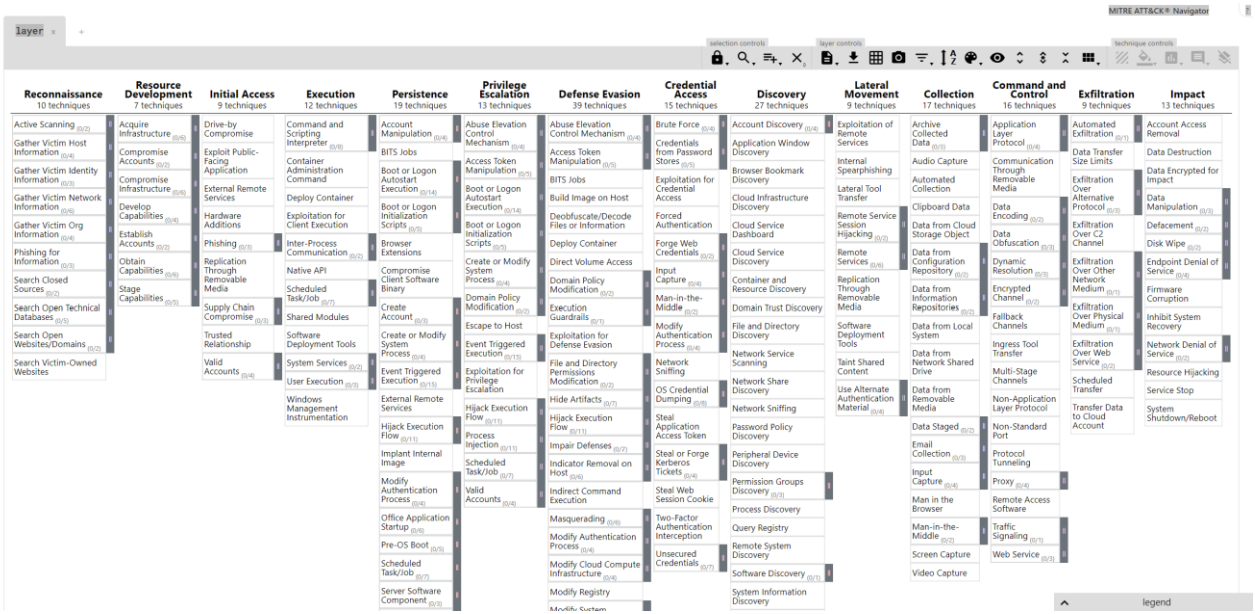
1. Современная кибератака
2. Управление уязвимостями
3. Мониторинг событий информационной безопасности

Современная кибератака



MITRE ATT&CK (1)

1. Reconnaissance – сбор информации о цели снаружи
2. Resource Development – подготовка ресурсов для нападения (например, размещение C2 сервера)
3. Initial Access – первоначальный доступ
4. Execution – попытка запуска вредоносного ПО
5. Persistence – организация постоянного доступа к целевой инфраструктуре
6. Privilege Escalation – повышение уровня доступа
7. Defense Evasion – обход средств защиты информации

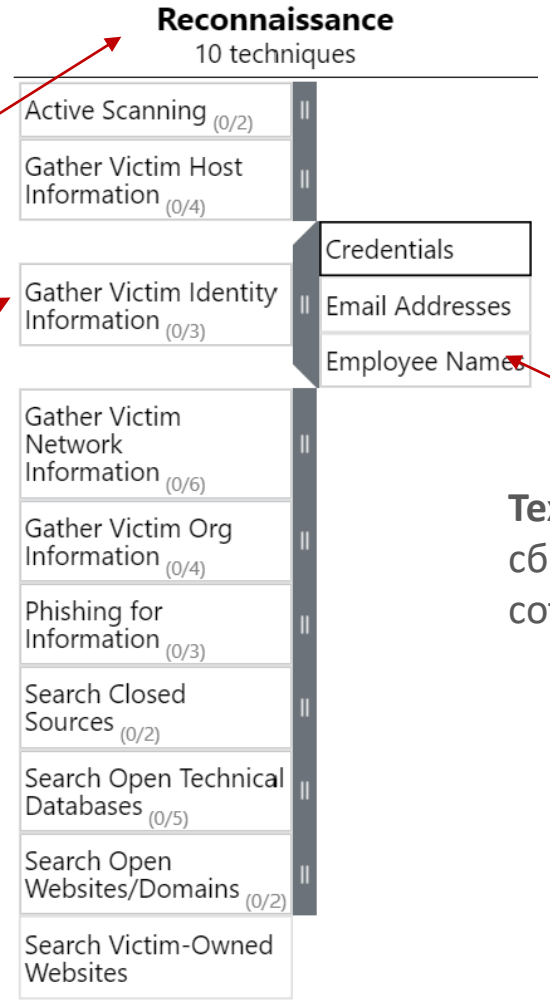


MITRE ATT&CK (2)

8. Credential Access – получение доступа с помощью действующих учетных записей
9. Discovery – сбор информации о цели изнутри
10. Lateral Movement – перемещение внутри целевой ИТ-инфраструктуры
11. Collection – сбор интересующих данных
12. Command and Control – организация внешнего управления
13. Exfiltration – передача интересующих данных вовне
14. Impact – разрушающее воздействие на ИТ-инфраструктуру

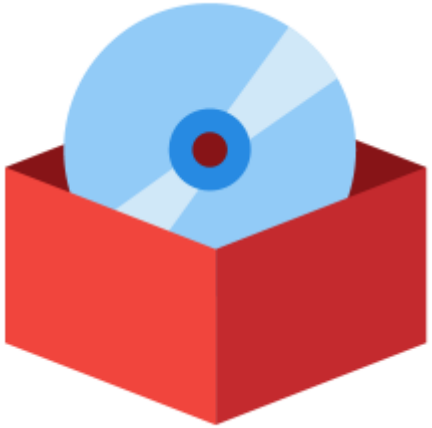
Тактическая задача (тактика):
разведка

Группа приемов (техник):
сбор данных, идентифицирующих цель



Техника:
сбор имен сотрудников

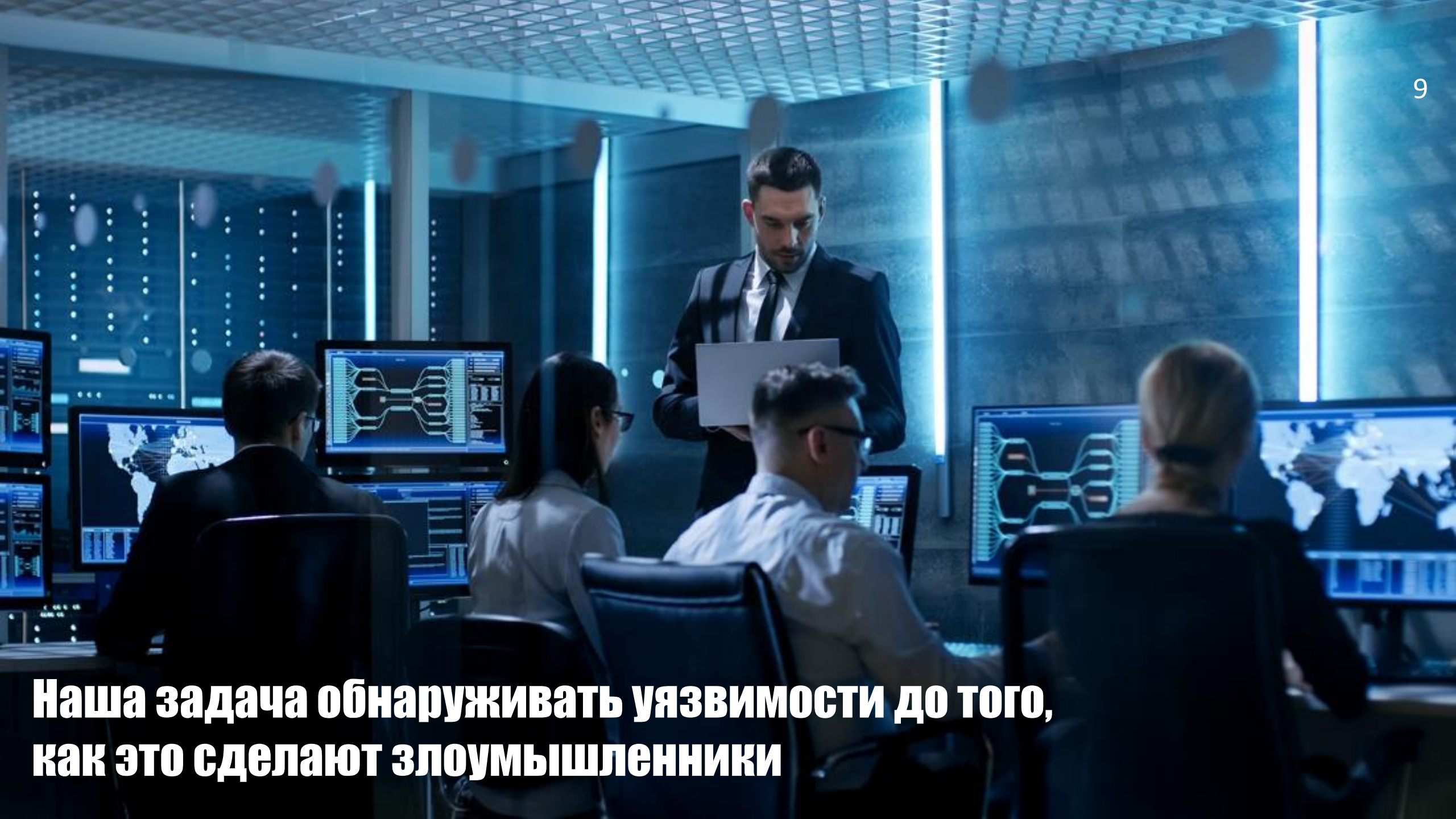
Инструментарий нападающих



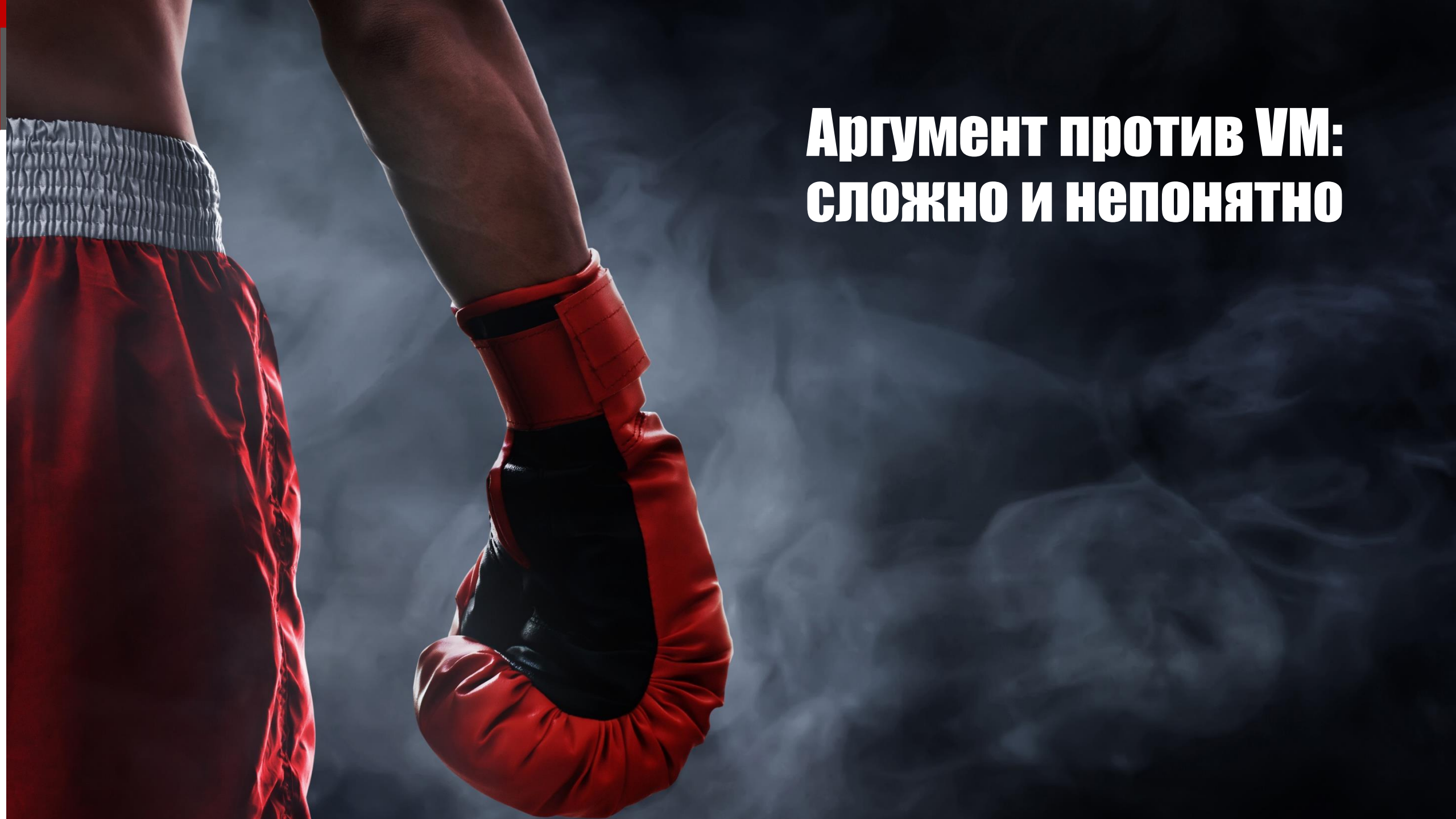
Специально разработанное вредоносное программное обеспечение

Хакерские утилиты с открытым исходным кодом

Утилиты операционной системы



Наша задача обнаруживать уязвимости до того, как это сделают злоумышленники


Аргумент против VM:
сложно и непонятно

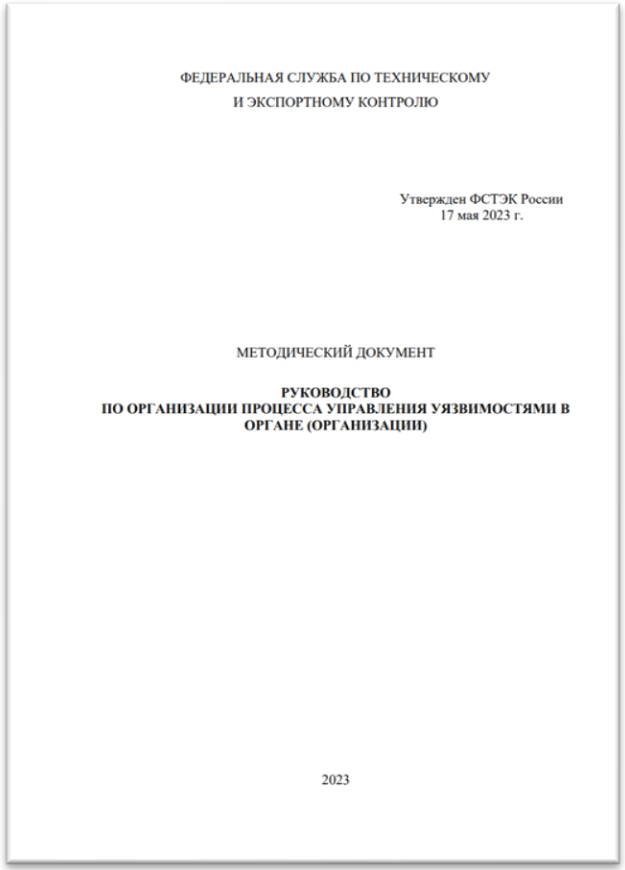
Мифы о VM

1. Для организации процесса управления уязвимостями нужен только «тяжелый» инструментарий.
2. Сканировать нужно не постоянно, а раз в месяц.
3. Приоритизировать уязвимости ну очень сложно.

Руководство от ФСТЭК России

«МЕТОДИЧЕСКИЙ ДОКУМЕНТ РУКОВОДСТВО ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)»

- Для кого:
  - государственных органов
  - организаций, в том числе субъектов КИИ
- Для чего:
  - создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования органов (организаций) и организация взаимодействия между структурными подразделениями органов (организаций) по вопросам устранения уязвимостей



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
17 мая 2023 г.

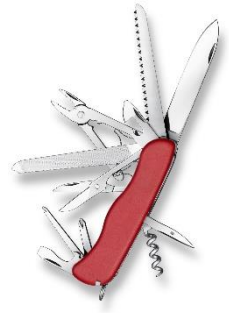
МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**РУКОВОДСТВО
ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)**

2023

Цикл управления уязвимостями

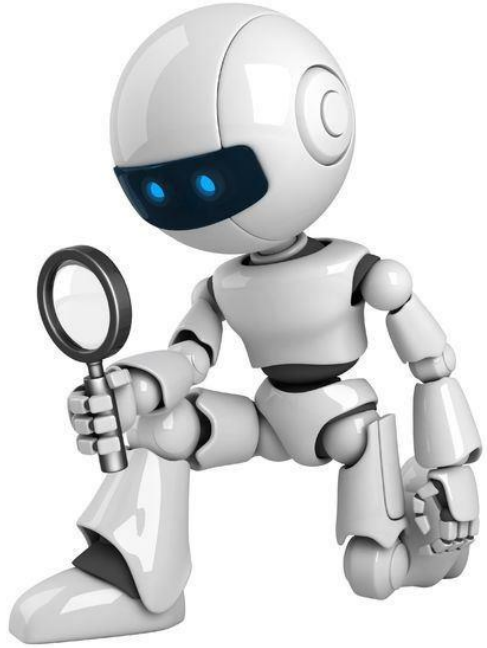
Цикл управления уязвимостями



Самое важное – иметь надежный, простой и гибкий в использовании инструмент для выявления уязвимостей.

Поиск уязвимостей

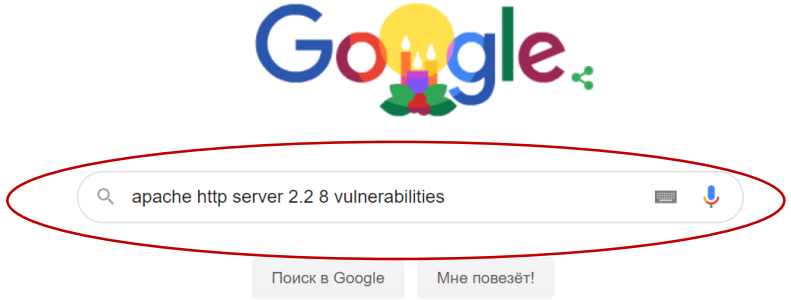
Ручной



С помощью сканеров

Технология ручного поиска уязвимостей

Apache HTTP Server 2.2.8



Apache » Http Server » 2.2.8 : Security Vulnerabilities (Execute Code)

Cpe Name:*cpe:/a:apache:http_server:2.2.8*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-1862	310		Exec Code	2013-06-10	2017-09-18	5.1	None	Remote	High	Not required	Partial	Partial	Partial

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

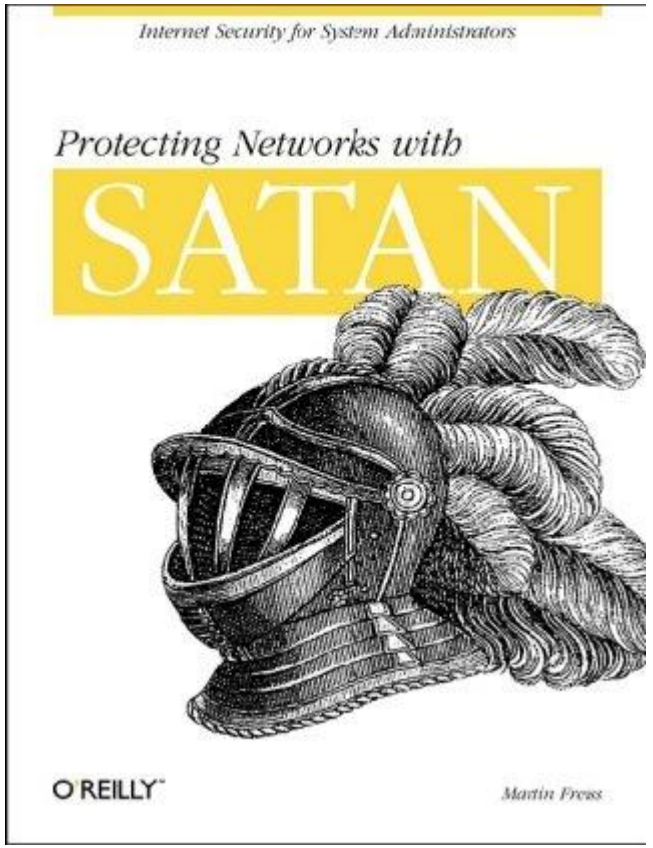
2	CVE-2010-0425			Exec Code	2010-03-05	2018-10-30	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Total number of vulnerabilities : 2 Page : 1 (This Page)

Первый сканер уязвимостей

- Релиз первого сканера уязвимостей SATAN (Security Administration Tool) состоялся в 5 апреля 1995
- Типы уязвимостей, которые он обнаруживал:
  - Файловые системы NFS, экспортируемые на произвольные хосты
  - Файловые системы NFS, экспортируемые в непривилегированные программы
  - Файловые системы NFS, экспортируемые через portmapper
  - Доступ к файлам с паролями NIS с произвольных хостов
  - Старые (т.е. до версии 8.6.10) версии sendmail
  - Доступ к REXD с произвольных хостов
  - отключен контроль доступа к X-серверу
  - доступ к произвольным файлам через TFTP
  - удаленный доступ к оболочке с произвольных хостов
  - доступный для записи домашний каталог анонимного FTP
- Написан на Perl и shell-скриптах

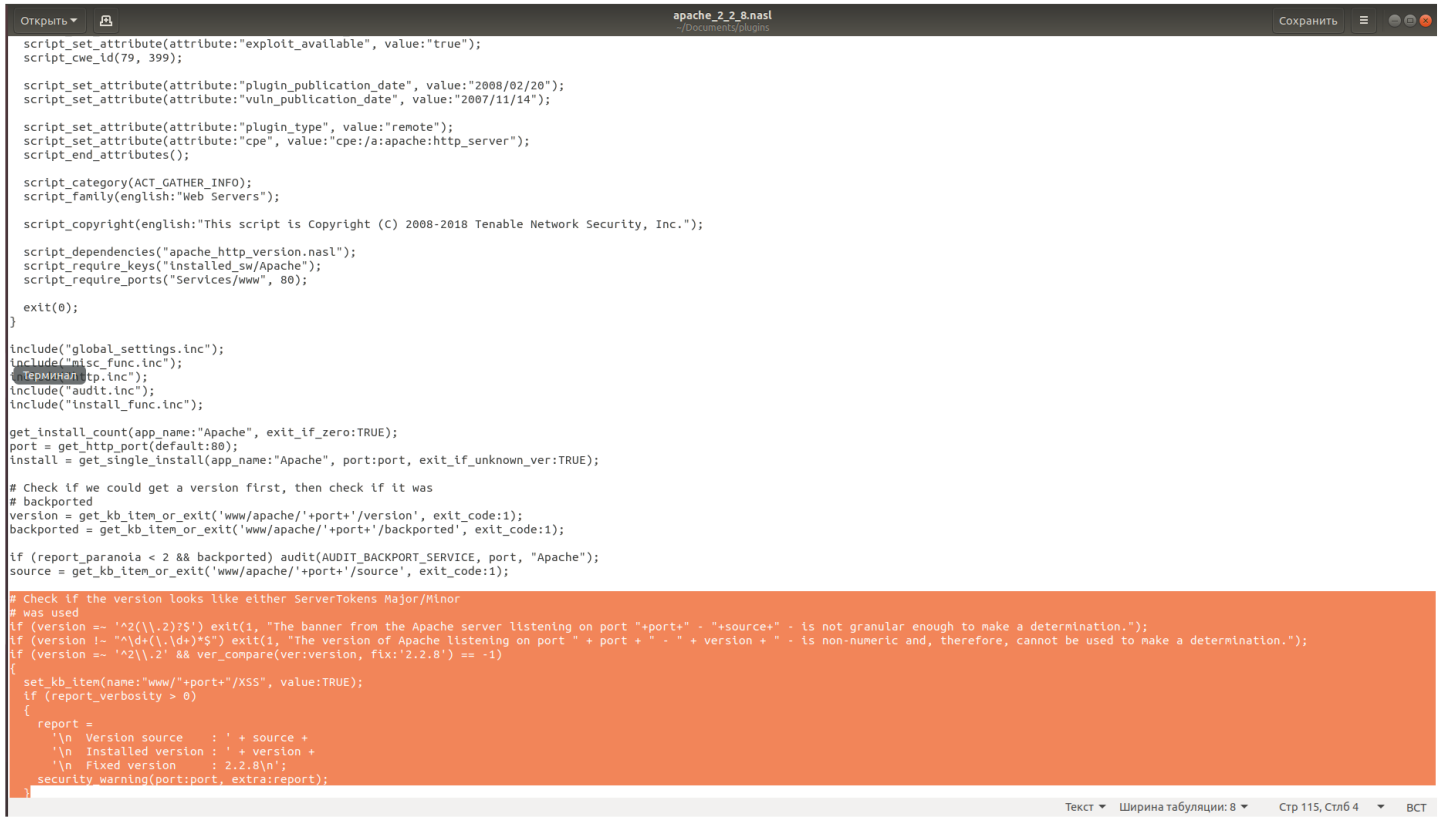


Сайт: http://www.porcupine.org/satan/

Запуск скриптов для проверок до сих пор применяется

Nessus Attack Scripting Language

Nmap Scripting Engine



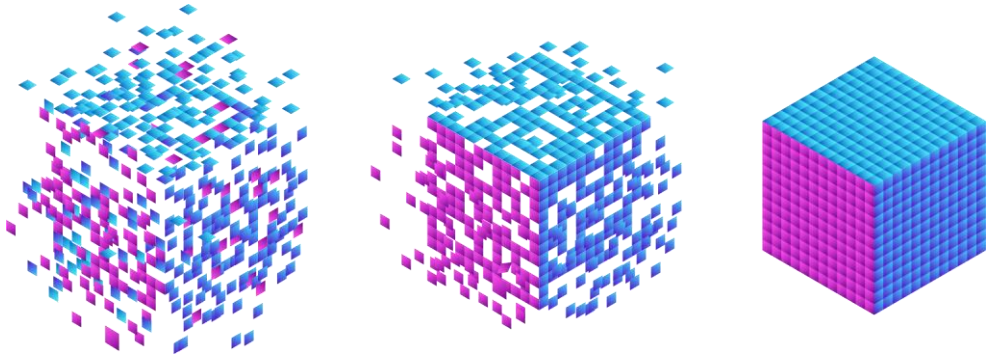

```
  script_set_attribute(attribute:"exploit_available", value:"true");
  script_cwe_id(79, 399);

  script_set_attribute(attribute:"plugin_publication_date", value:"2008/02/20");
  script_set_attribute(attribute:"vuln_publication_date", value:"2007/11/14");

  script_set_attribute(attribute:"plugin_type", value:"remote");
  script_set_attribute(attribute:"cpe", value:"cpe:/a:apache:http_server");
  script_end_attributes();

  script_category(ACT_GATHER_INFO);
  script_family(english:"Web Servers");

  script_copyright(english:"This script is Copyright (C) 2008-2018 Tenable Network Security, Inc.");

  script_dependencies("apache_http_version.nasl");
  script_require_keys("installed_sw/Apache");
  script_require_ports("Services/www", 80);

  exit(0);
}

include("global_settings.inc");
include("misc_func.inc");
include("http.inc");
include("audit.inc");
include("install_func.inc");

get_install_count(app_name:"Apache", exit_if_zero:TRUE);
port = get_http_port(default:80);
install = get_single_install(app_name:"Apache", port:port, exit_if_unknown_ver:TRUE);

# Check if we could get a version first, then check if it was
# backported
version = get_kb_item_or_exit('www/apache/'+port+'/version', exit_code:1);
backported = get_kb_item_or_exit('www/apache/'+port+'/backported', exit_code:1);

if (report_paranoia < 2 && backported) audit(AUDIT_BACKPORT_SERVICE, port, "Apache");
source = get_kb_item_or_exit('www/apache/'+port+'/source', exit_code:1);

# Check if the version looks like either ServerTokens Major/Minor
# was used
if (version =~ '^2(\\.2)?$') exit(1, "The banner from the Apache server listening on port "+port+" - "+source+" - is not granular enough to make a determination.");
if (version !~ "^\d+(\.\d+)*$") exit(1, "The version of Apache listening on port " + port + " - " + version + " - is non-numeric and, therefore, cannot be used to make a determination.");
if (version =~ '^2\\.2' && ver_compare(ver:version, fix:'2.2.8') == -1)
{
  set_kb_item(name:"www/"+port+"/XSS", value:TRUE);
  if (report_verbosity > 0)
  {
    report =
      '\n  Version source    : ' + source +
      '\n  Installed version : ' + version +
      '\n  Fixed version     : 2.2.8\n';
    security_warning(port:port, extra:report);
  }
```

Проблемы скриптового подхода

- Нужно поддерживать несколько десятков тысяч плагинов/скриптов, выявляющих уязвимости.
- Сканирование одного узла может занимать десятки минут.

Современный подход: использование агрегированной базы данных уязвимостей

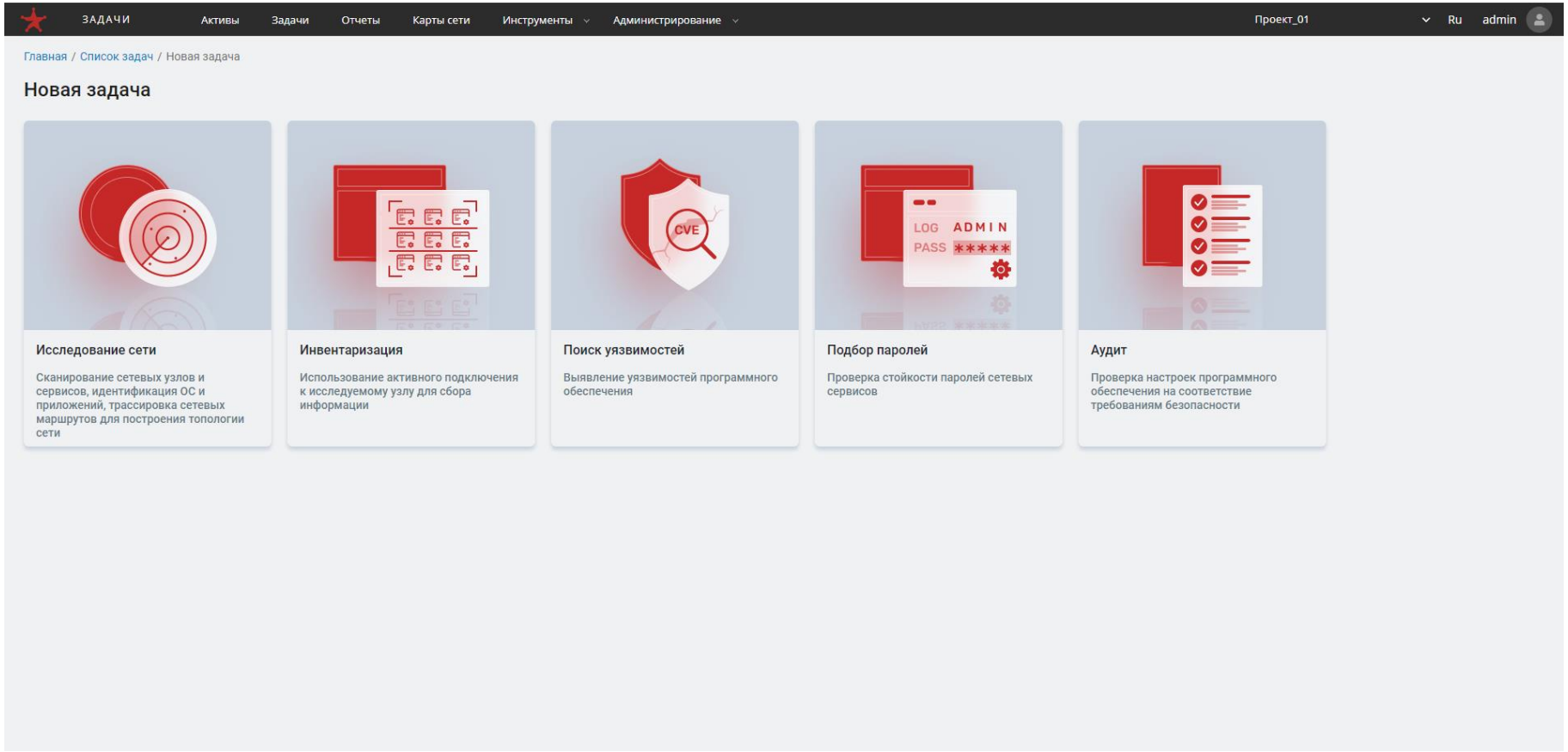
- БДУ ФСТЭК России
- NIST National Vulnerability Database
- База обновлений Windows
- RHEL/CentOS Security Data
- Ubuntu CVE Tracker
- Debian GNU/Linux Security Bug Tracker
- …



Сравнение подходов

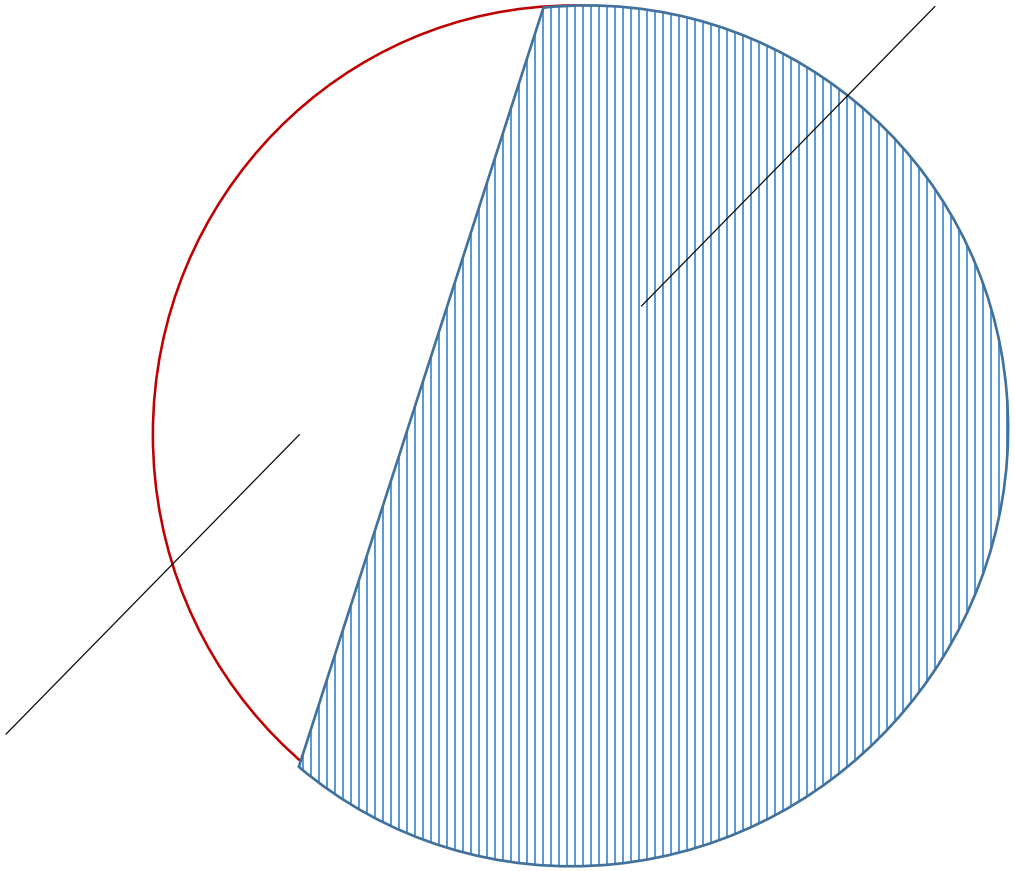
	Поиск по версиям	SCAP (OVAL)	Скрипты
Скорость выпуска обновлений	Высокая	Средняя	Средняя
Полнота покрытия уязвимостей	Высокая	Средняя	Средняя
Возможность сетевого сканирования без учетной записи	Да	Нет	Да
Возможность сетевого сканирования с учетной записью	Да	Да	Да

Сканер-ВС 6: основные функции



Источник информации о версиях: сетевое сканирование и инвентаризация

Все программные пакеты, включая локальные.
Требуется административный доступ по SSH/WinRM.



Сетевые сервисы:
требуется только доступ по сети

Используемы источники информации об уязвимостях

- БДУ ФСТЭК России: https://bdu.fstec.ru/
- NIST NVD: https://nvd.nist.gov/
- Chinese National Vulnerability Database (CNNVD): https://www.cnvd.org.cn/
- Debian GNU/Linux Security Bug Tracker

https://security-tracker.debian.org/tracker/

- Ubuntu CVE Tracker

https://people.canonical.com/~ubuntu-security/cve/

- RHEL/CentOS Security Data https://www.redhat.com/security/data/metrics/
- и д.р.

Методология управления уязвимостями и Сканер-ВС 6

Ежедневное обновление базы уязвимостей

Исследование сети, инвентаризация, поиск уязвимостей

CVSS, критичность активов, информация о наличии эксплойтов

Рекомендации по устранению уязвимостей

Выполнение задач по расписанию, интеграция с SIEM

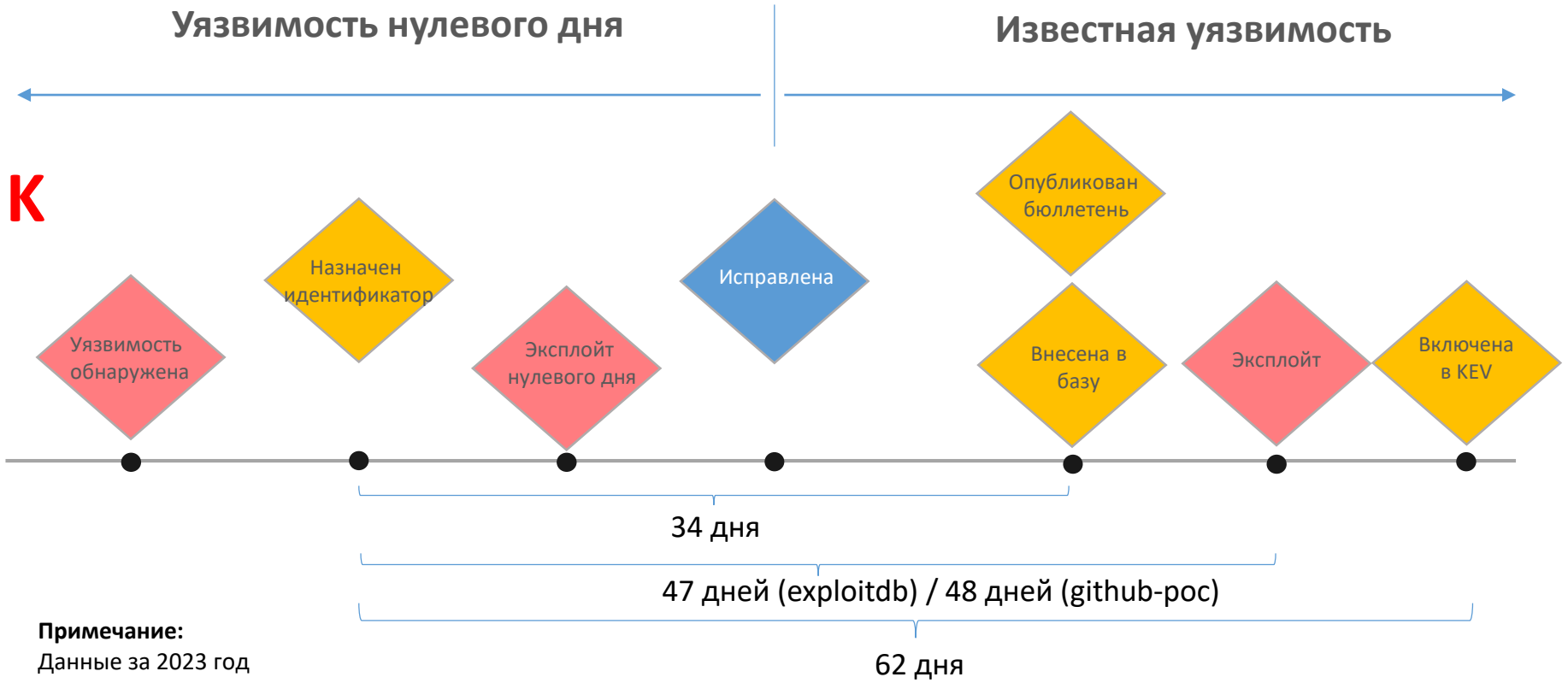
Миф о периодическом сканировании

Рекомендуемые ФСТЭК России сроки для устранения уязвимостей:

- критический уровень опасности до **24 часов**
- высокий уровень опасности – до 7 дней
- средний уровень опасности – до 4 недель
- низкий уровень опасности – до 4 месяцев

Миф о приоритизации

Путь уязвимости:



Примечание:
Данные за 2023 год
Медианные значения

От чего зависит наше восприятие опасности уязвимости?

- Внешние факторы:
  - Оценка уязвимости по CVSS
  - Оценка потенциальной возможности эксплуатации (EPSS)
  - Наличие опубликованных эксплойтов
- Внутренние факторы:
  - Доступность актива извне
  - Особенности ИТ-инфраструктуры
  - Особенности конфигурации систем
  - Критичность активов с точки зрения бизнеса

Степень опасности уязвимости

- Common Vulnerability Scoring System (CVSS) — это открытый стандарт, используемый для расчета количественной оценки степени опасности.
- При расчете учитываются такие факторы, как наличие эксплойта, возможность удаленной эксплуатации, необходимость авторизации, возможные последствия.
- Калькуляторы для расчета CVSS 2/3/3.1: https://bdu.fstec.ru/calc

Пример: Opera DLL search order hijacking (CVE-2018-18913)

CVSS v3.1 Base Score: 7.8

Метрика	Значение	Комментарии
Attack Vector	Local	Атакующий должен получить локальный доступ к машине либо напрямую, либо с помощью методов социальной инженерии, чтобы загрузить вредоносную DLL.
Attack Complexity	Low	Атака легко воспроизводится.
Privileges Required	None	Специальных привилегий атакующему не требуется.
User Interaction	Required	Требуется взаимодействие с жертвой для запуска вредоносной DLL.
Scope	Unchanged	Уязвимый компонент.
Confidentiality	High	Позволяет атакующему захватить полный контроль над системой
Integrity	High	Позволяет атакующему захватить полный контроль над системой
Availability	High	Позволяет атакующему захватить полный контроль над системой

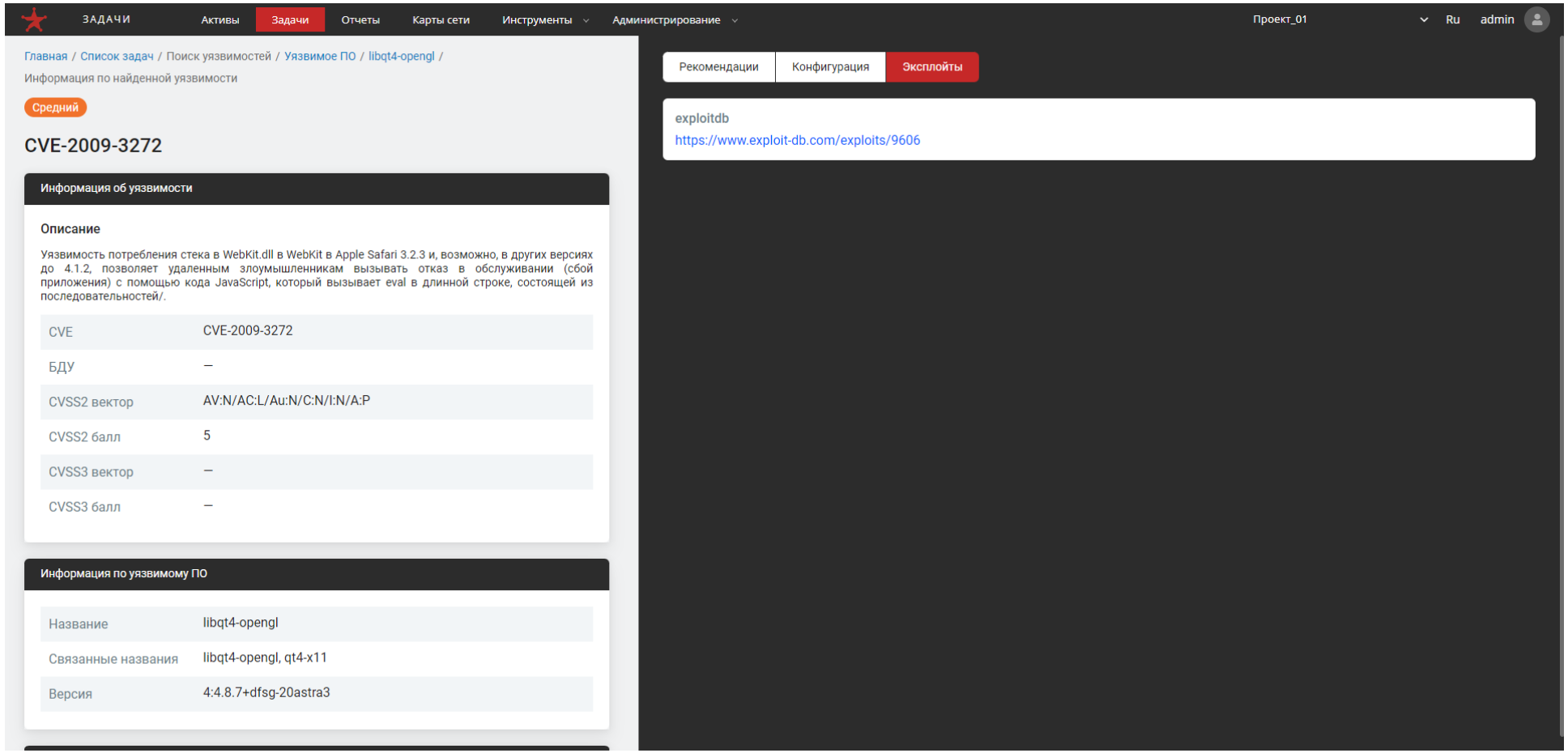
Упрощенно:

- Низкая – получение информации о системе
- Средняя – получение информации о системе, которая будет полезна для проведения дальнейшей атаки, либо уязвимость, которую очень сложно проэксплуатировать.
- Высокая и критическая – получение административного доступа, либо запуск произвольного кода.

Самые простые критерии для выделения самых приоритетных уязвимостей

1. Уровень опасности: критический или высокий
2. Наличие эксплойта или PoC.
3. CWE – «что-то с памятью».
4. Уязвимое ПО доступно извне, на критичном сервере или является массовым в инфраструктуре. Особое внимание ОС и офисный пакет от Microsoft.
5. Наличие уязвимости в каталоге KEV.
6. Оценка модели EPSS, приближающаяся к 1.

Информация о доступных эксплойтах



Сканер-ВС 6: доступный постоянный мониторинг появления уязвимостей

Кто уже использует?

- ИБ/ИТ-интеграторы
- Банки
- Школы
- Медицинские учреждения
- ФОИВы
- ВПК
- Лицензиаты ФСТЭК/Минобороны России

Сканер-ВС: ресурсы

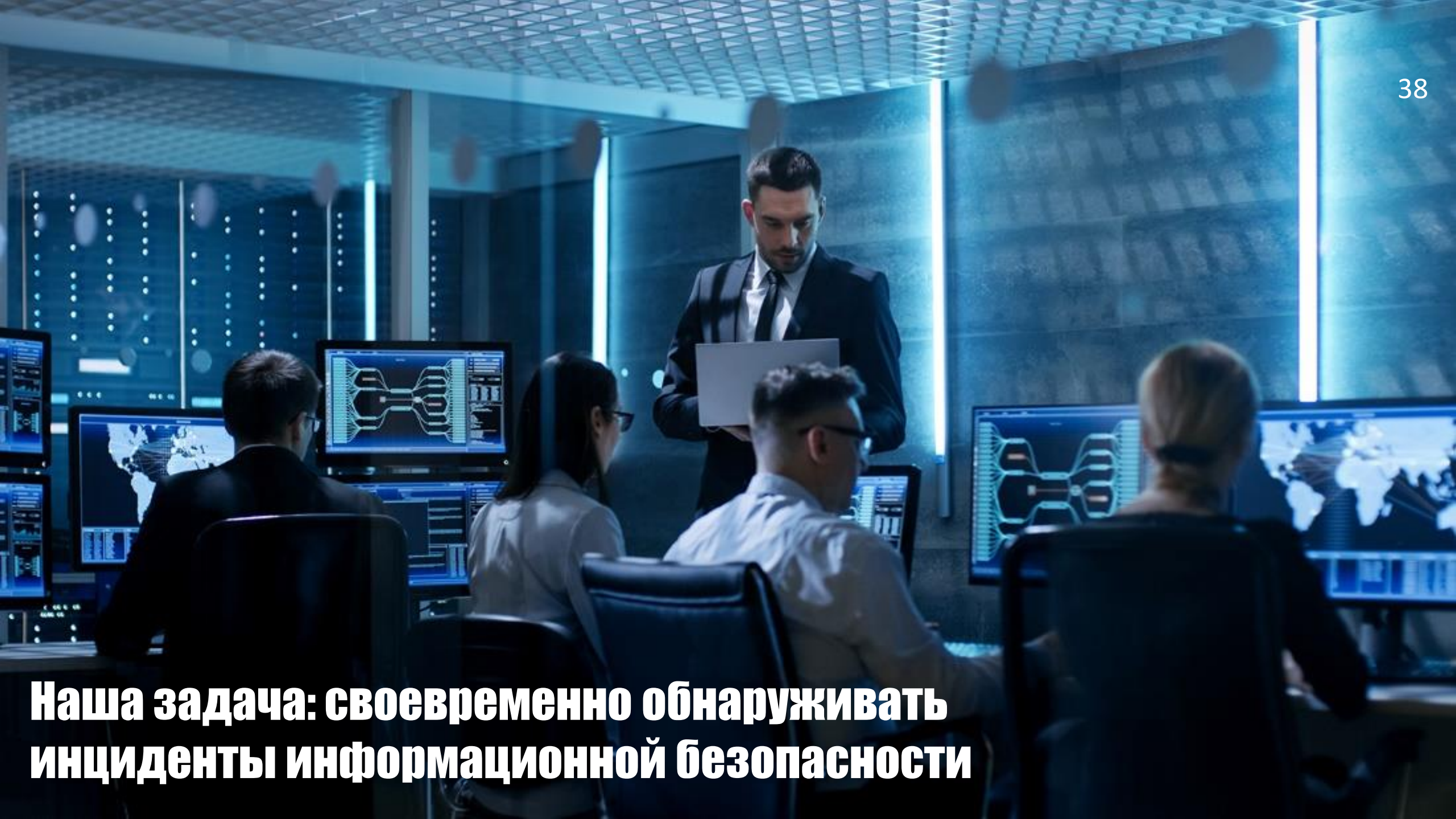
- Группа в ТГ: https://t.me/scanervs
- Онлайн-документация: https://docs.etecs.ru/
- Учебное видео: https://rutube.ru/channel/36354965/
- Форум техподдержки: https://forum.etecs.ru/c/skaner-vs-6/6
- **Демо-версия**: https://scaner-vs.ru/

Ближайшее будущее

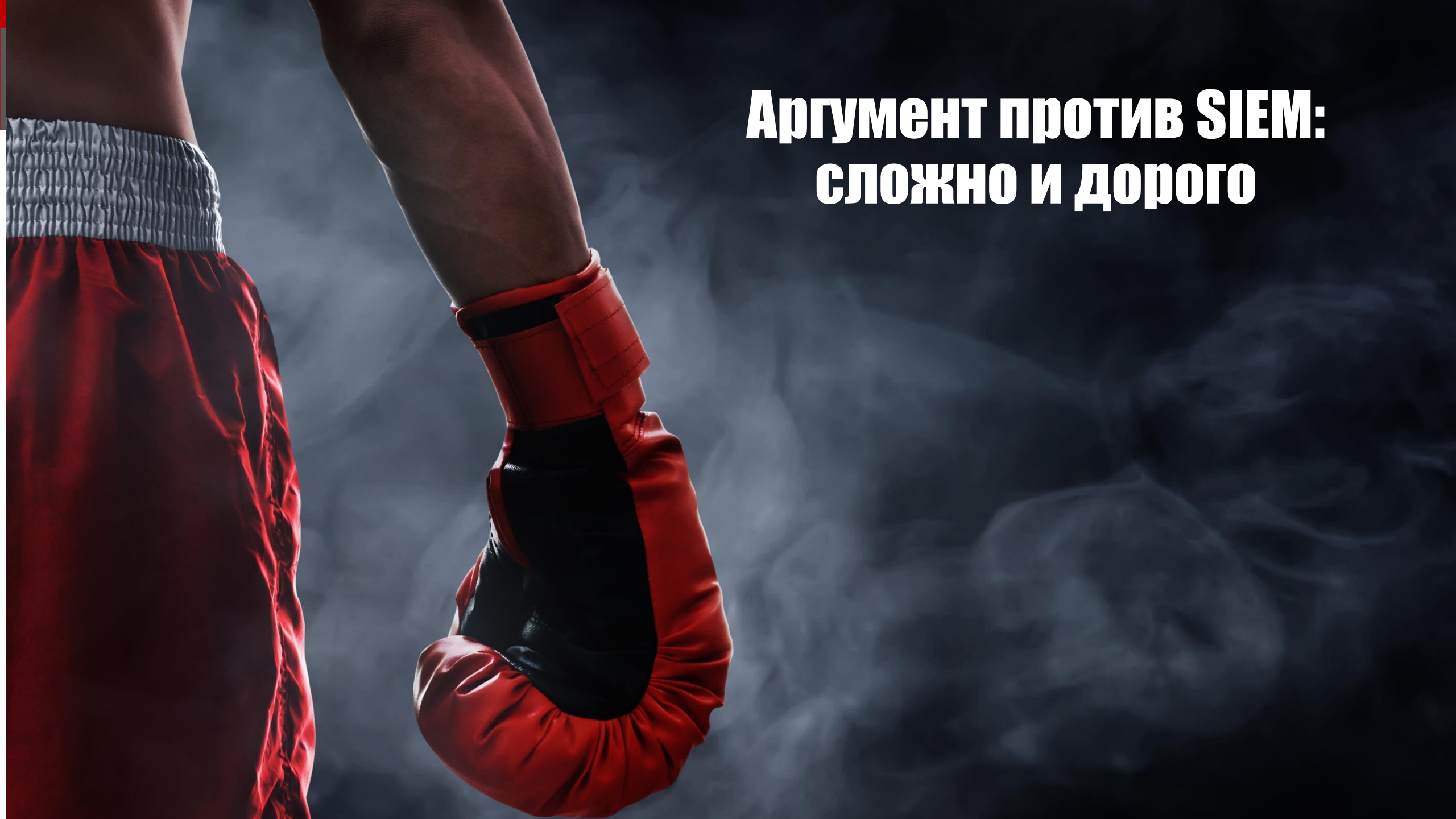
- Повышение производительности
- Повышение точности выявления уязвимостей
- Аудит конфигураций ОС, сетевого оборудования, СЗИ

Сканер-ВС 7.0

Сканер-ВС Enterprise



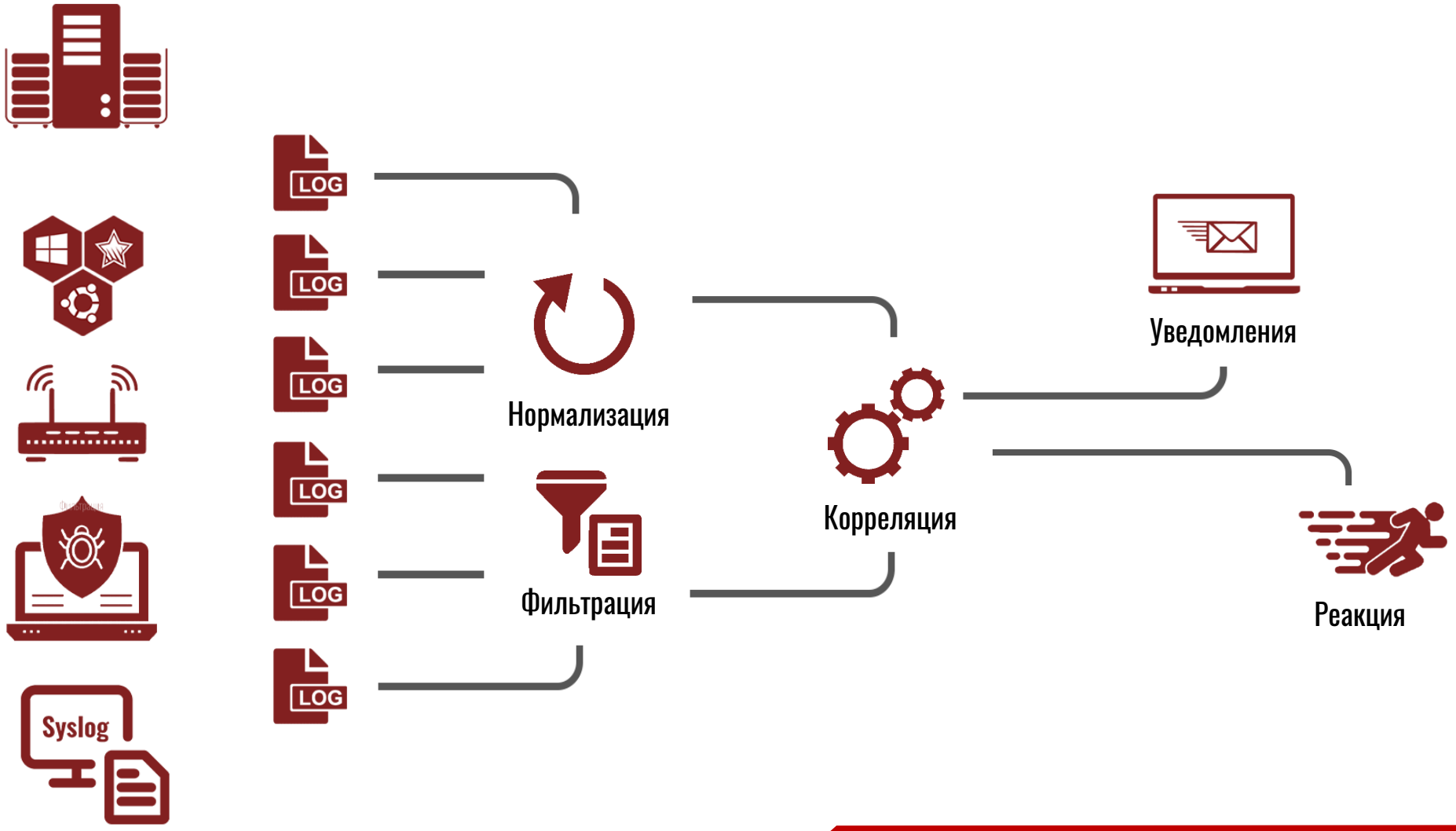
Наша задача: своевременно обнаруживать инциденты информационной безопасности


Аргумент против SIEM:
сложно и дорого

Мифы о SIEM

1. Сложно развернуть систему и подключить источники
2. Сложно писать правила
3. SIEM – это всегда дорого

Принцип работы SIEM-системы



Миф о сложности развертывания

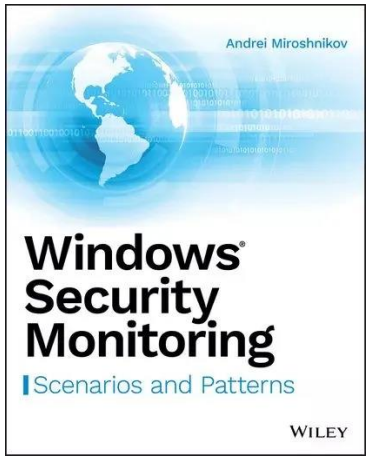
KOMRAD Enterprise SIEM: 5 минут на установку

Что отслеживать?

- Манипуляции с учетными записями
- Выполнение скриптов и утилит командной строки
- Запуск новых сервисов
- Добавление новых параметров в автозагрузку
- Изменение способов аутентификации (загрузка дополнительных ключей/сертификатов)
- Открытие дополнительных сетевых ресурсов
- Сетевую активность
- и т.п.

Полезные материалы по теме

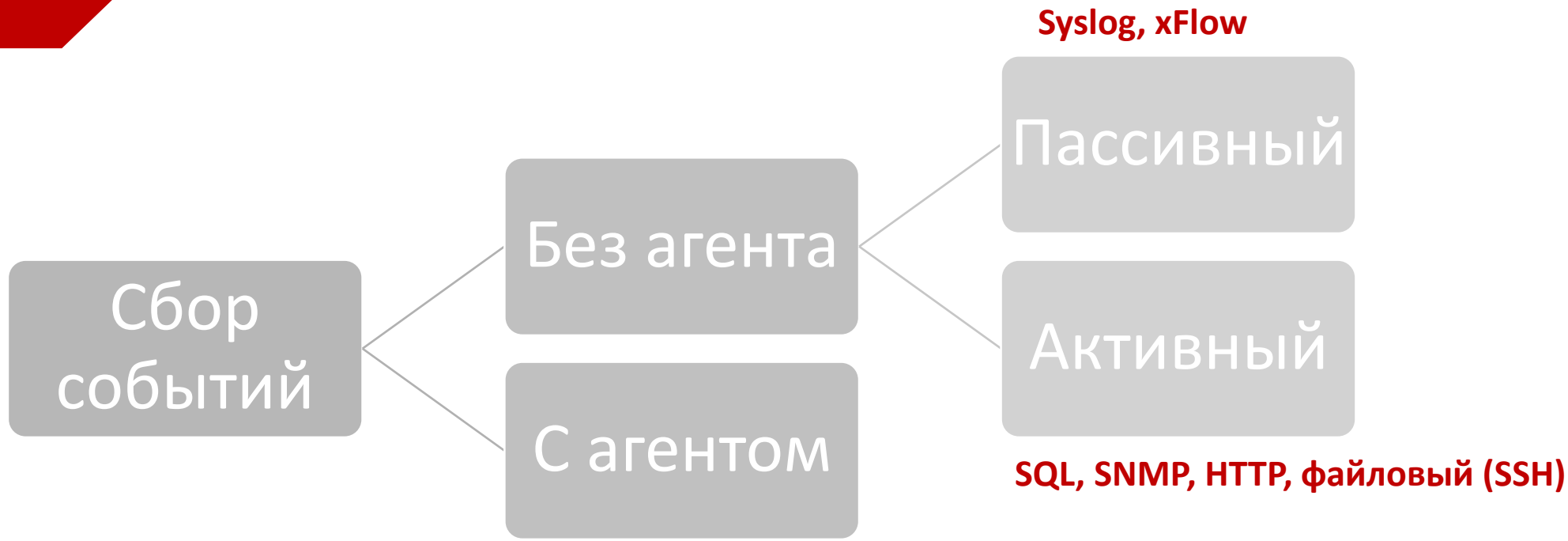
- Рекомендации НКЦКИ по первоочередным мерам, направленным на обнаружение, предупреждение и ликвидацию последствий компьютерных атак (https://safe-surf.ru/upload/ALRT/ALRT-20220316.1.pdf)
- Материалы нашего курса по мониторингу событий ИБ: https://rutube.ru/plst/393079/ или https://youtube.com/playlist?list=PLAs36PQnfDQ1BfIj3cqJ9tbAvsQWc8TDU&feature=shared
- Best practices for event logging and threat detection (https://www.ic3.gov/Media/News/2024/240822.pdf)
- Windows Event Logging and Forwarding (https://github.com/AustralianCyberSecurityCentre/windows_event_logging)
- 11 Strategies of a World-Class Security Operations Center https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf



Источники событий

1. СЗИ
2. Серверы
3. Критичные рабочие станции (например, администраторов)
4. Периметр: МЭ, СОВ, маршрутизаторы
5. Ресурсы, доступные из интернет: почтовый сервер, VPN

Миф о сложности подключения источника



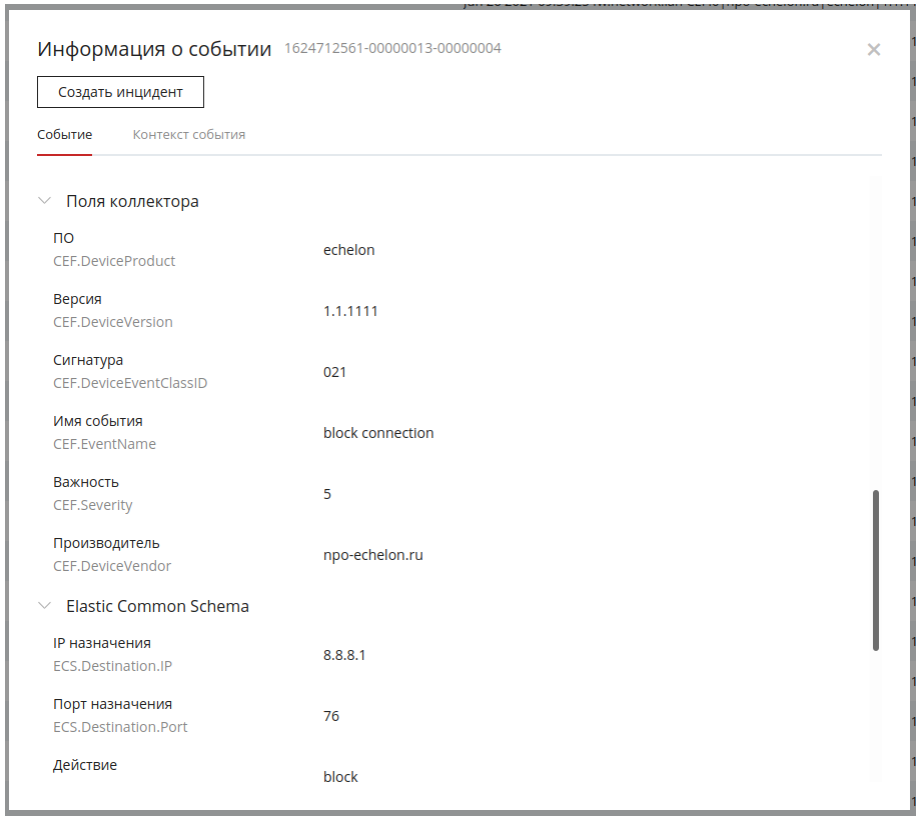
KOMRAD Enterprise SIEM: сбор данных с любого источника

Нормализация событий

Сырое событие:

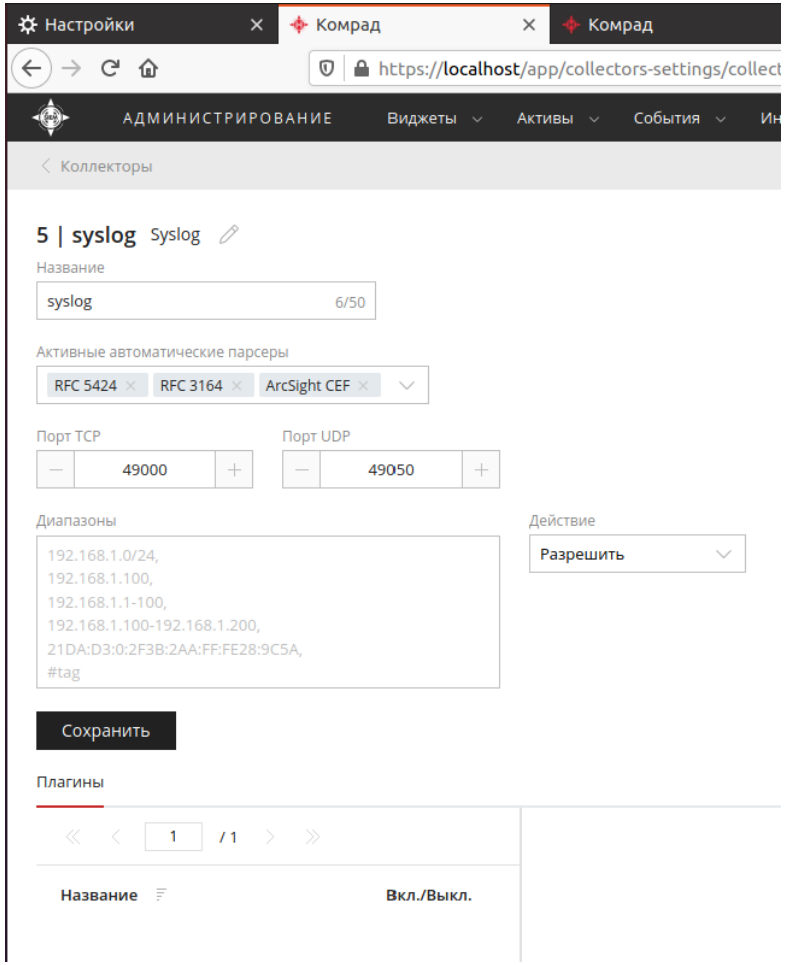
Jun 26 2021 09:02:35 fw.network.lan CEF:0
npo-echelon.ru|echelon|
1.1.1111|021|block connection|5|
src=8.8.8.10 spt=56117 dst=8.8.8.1 dpt=76
act=block

Разобранное событие:

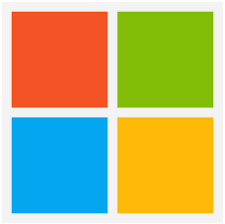


Поддерживаемые стандарты и технологии разбора событий

- Поддержка стандартов:
  - RFC 5424
  - RFC 3164
  - ArcSight CEF
- Поддержка возможности разработки плагинов с помощью регулярных выражений (реализован стандарт RE2)
- Поддержка стандарта структурирования события: Elastic Common Schema

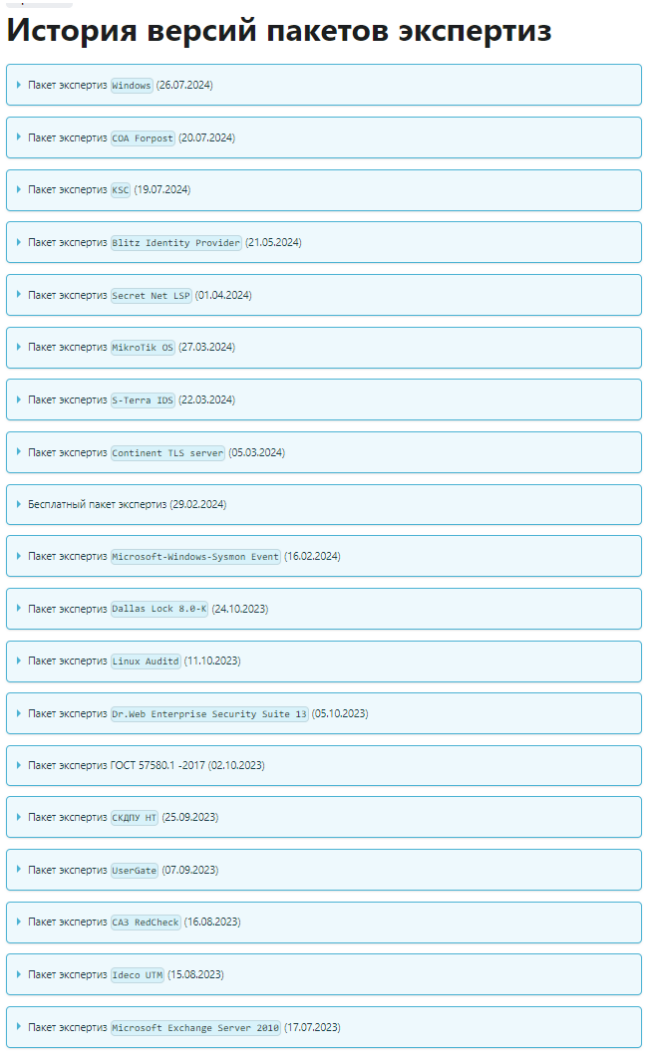


Вендоры, решения которых можно спокойно подключить



Миф о сложности правил

- Есть пакеты экспертизы открытые и в рамках расширенной технической поддержки: https://docs.etecs.ru/komrad/docs/ec/changelog/
- Для интересующихся - открытые технологии для легкого создания своих правил: графический редактор и возможность создания фильтров на языке Lua.

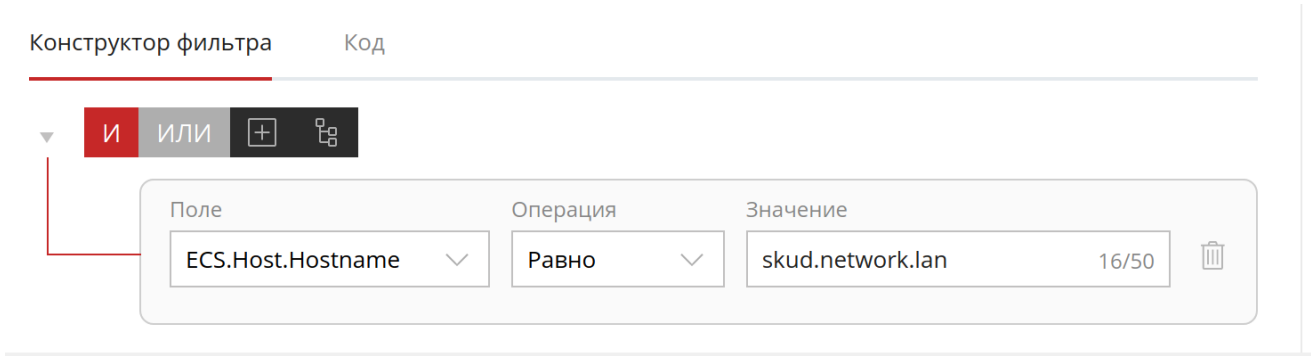


Важно не попадать в зависимость от вендора

- Наличие открытых и бесплатных пакетов экспертиз
- Распространенность технологий, используемых в SIEM, например, языка для создания правил нормализации, фильтрации и корреляции.
- Экспертиза должна оставаться в компании в независимости от смены персонала или технологий.

Фильтрация

- Все события от СКУДа, поступившие за сутки:



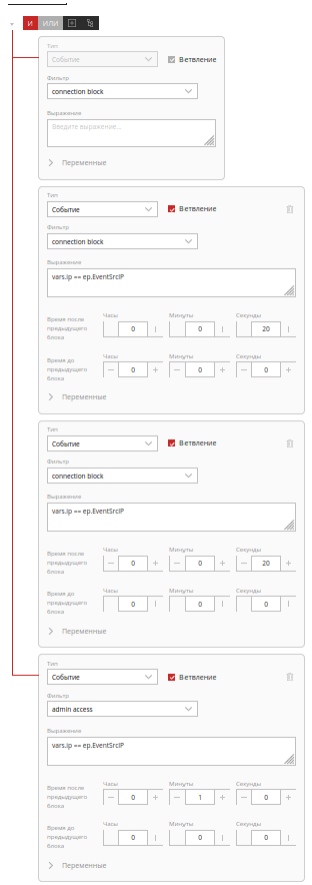
СОБЫТИЯ | Виджеты | Активы | События | Инциденты | Администрирование | Ru

1 / 1 | События, поступающие от С | 26.06.2021, 00:00 — 26.06.2021, 23:59 | Найти

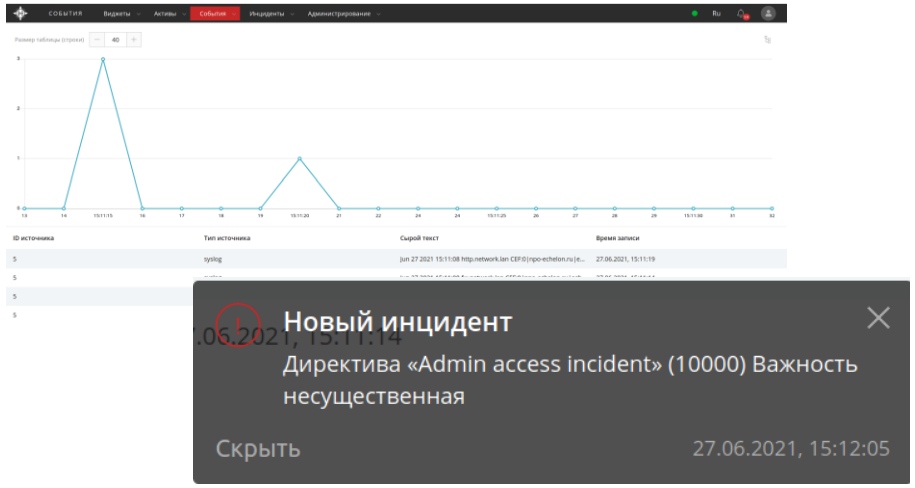
ID источника	Тип источника	Сырой текст	Время записи
syslog 5	syslog	Jun 26 2021 11:20:56 skud.network.lan CEF:0|...	26.06.2021, 18:21:02
syslog 5	syslog	Jun 26 2021 11:20:56 skud.network.lan CEF:0|...	26.06.2021, 18:21:02
syslog 5	syslog	Jun 26 2021 11:00:22 skud.network.lan CEF:0|...	26.06.2021, 18:00:28
syslog 5	syslog	Jun 26 2021 11:00:22 skud.network.lan CEF:0|...	26.06.2021, 18:00:28

Корреляция

- Фиксация последовательности событий
- Определение временных интервалов
- Проверка отсутствия события
- Сопоставление данных из разных событий



Уведомление



В пользовательском интерфейсе

ГОССОПКА

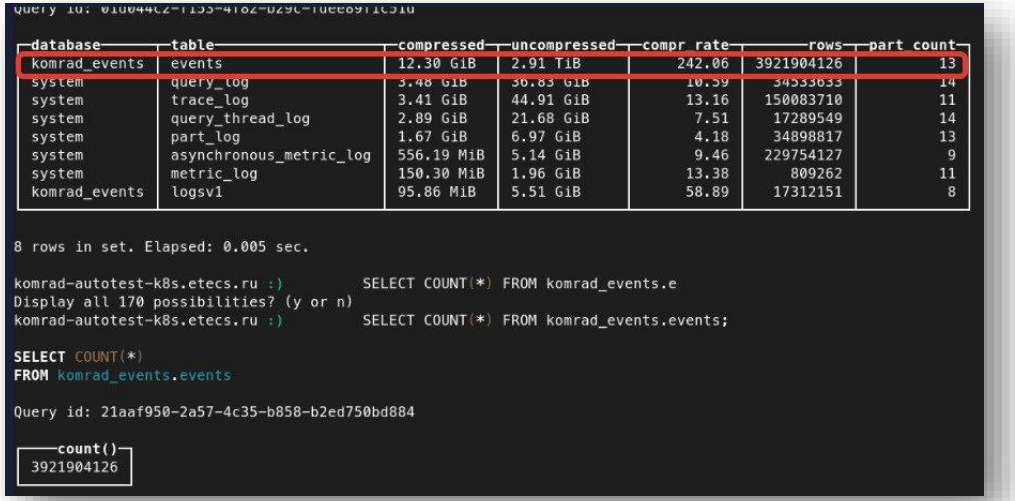
Обнаружение. Предупреждение. Ликвидация.

НКЦКИ

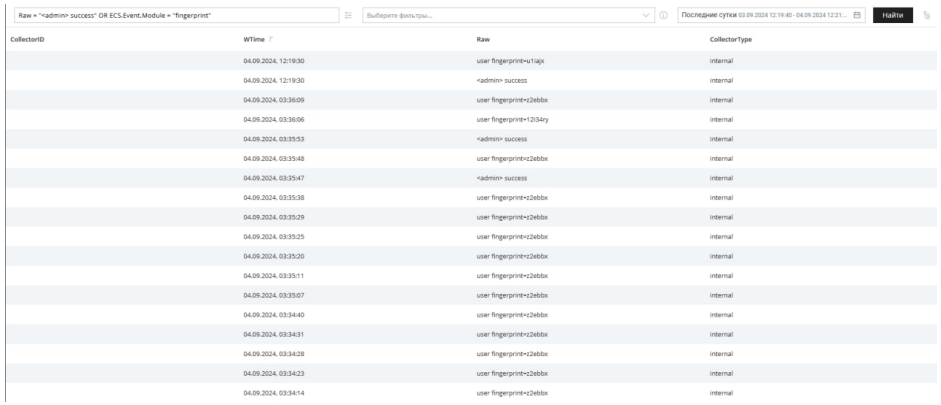
В мессенджере (KOMRAD 4.5)

Что еще важно и не сложно?

- Горячее/холодное хранение
- Сжатие данных
- Удобный поиск
- Аналитика

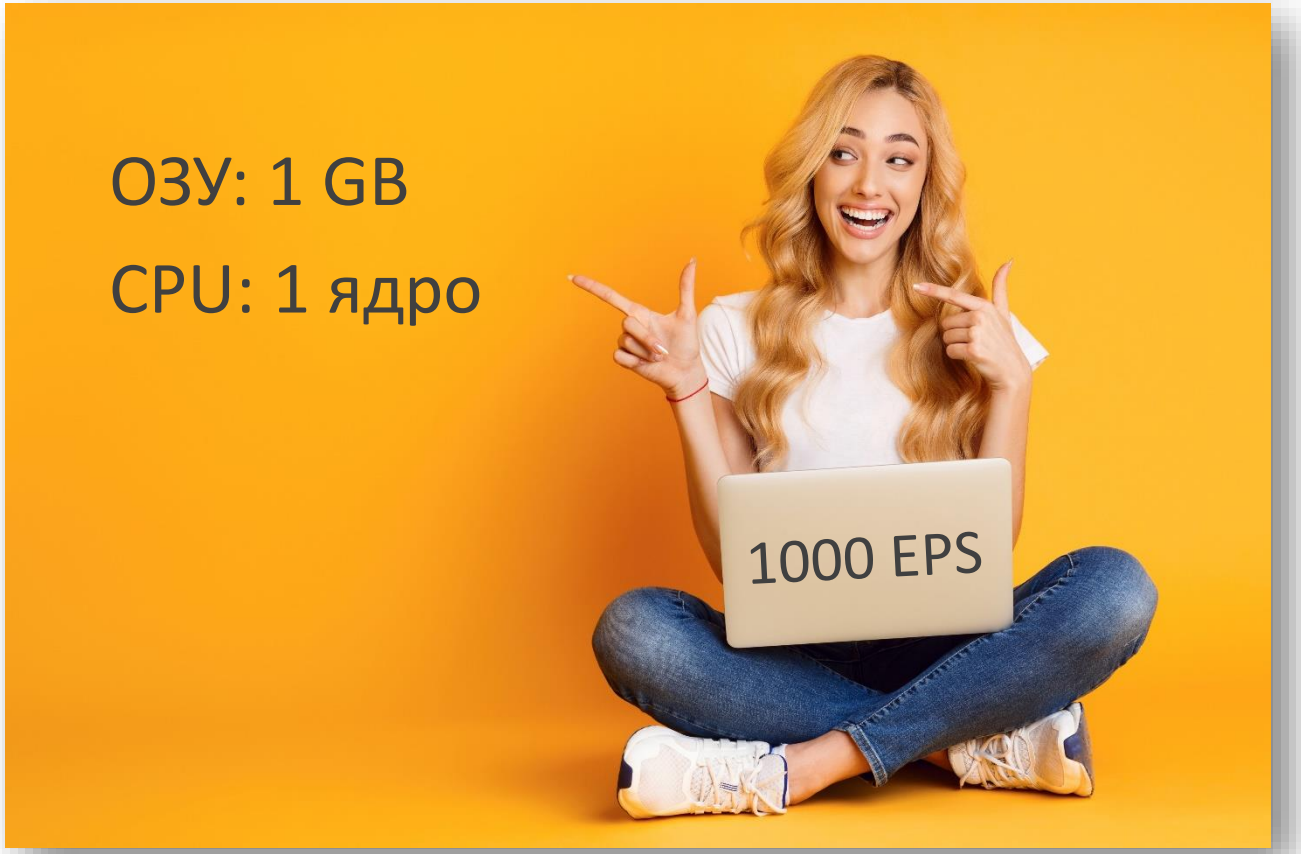


```
Query id: 010044c2-7133-4182-b29c-7dee691fc510

┌─database──────┬─table──────────────────┬─compressed─┬─uncompressed─┬─compr_rate─┬─────rows─┬─part_count─┐
│ komrad_events │ events                 │ 12.30 GiB  │ 2.91 TiB     │     242.06 │ 3921904126 │         13 │
│ system        │ query_log              │ 3.48 GiB   │ 36.83 GiB    │      10.59 │ 34333633 │         14 │
│ system        │ trace_log              │ 3.41 GiB   │ 44.91 GiB    │      13.16 │ 150083710 │         11 │
│ system        │ query_thread_log       │ 2.89 GiB   │ 21.68 GiB    │       7.51 │ 17289549 │         14 │
│ system        │ part_log               │ 1.67 GiB   │ 6.97 GiB     │       4.18 │ 34898817 │         13 │
│ system        │ asynchronous_metric_log │ 556.19 MiB │ 5.14 GiB     │       9.46 │ 229754127 │          9 │
│ system        │ metric_log             │ 150.30 MiB │ 1.96 GiB     │      13.38 │ 809262 │         11 │
│ komrad_events │ logsv1                 │ 95.86 MiB  │ 5.51 GiB     │      58.89 │ 17312151 │          8 │
└───────────────┴────────────────────────┴────────────┴──────────────┴────────────┴──────────┴────────────┘

8 rows in set. Elapsed: 0.005 sec.

komrad-autotest-k8s.etecs.ru :)         SELECT COUNT(*) FROM komrad_events.e
Display all 170 possibilities? (y or n)
komrad-autotest-k8s.etecs.ru :)         SELECT COUNT(*) FROM komrad_events.events;

SELECT COUNT(*)
FROM komrad_events.events

Query id: 21aaf950-2a57-4c35-b858-b2ed750bd884

┌─count()─┐
│ 3921904126 │
└─────────┘
```



Миф о дороговизне железа для SIEM

Действительно минимальные требования



Оптимизированный код

KOMRAD Enterprise SIEM изначально создан для работы в ОС Linux

ASTRA LINUX®

ОСНОВА

ubuntu®

debian

уже

альт сп

РЕДОС

уже в 4.5

KOMRAD Enterprise SIEM: ресурсы

Комплекс
Оперативного
Мониторинга,
Реагирования и
Анализа
Данных

- Документация: https://docs.etecs.ru
- Обучающее видео: https://www.youtube.com/@ETtrainingcybersec/videos
- Группа пользователей в ТГ: https://t.me/komrad4
- Запросить демо: sales@npo-echelon.ru

Ближайшее будущее

- Повышение производительности.
- Расширен список поддерживаемых ОС: Astra Linux 1.8, РЕД ОС 8 и Альт 8 СП.
- Переработан поиск по событиям, добавлены «выражения поиска».
- Новые плагины: eBPF, http-scraping, sigma, Zeek JSON, Агент Auditd и ряд вспомогательных плагинов.
- Добавлен эвристический анализ событий для формирования правил парсинга для многих плагинов. Перенос фильтрации на коллекторы.
- Продвинутые виджеты: редактируемые встроенные + Grafana.

И многое другое…

KOMRAD Enterprise SIEM 4.5

Кто уже использует?

- ИБ/ИТ-интеграторы
- Коммерческие и ведомственные SOC
- КИИ
- Банки
- Медицинские учреждения
- ФОИВы
- Организации ВПК
- Лицензиаты ФСТЭК
- Лицензиаты Минобороны России

KOMRAD Enterprise SIEM: эффективно и доступно

Остаемся на связи!

Телеграм-канал Echelon Eyes

https://t.me/EchelonEyes