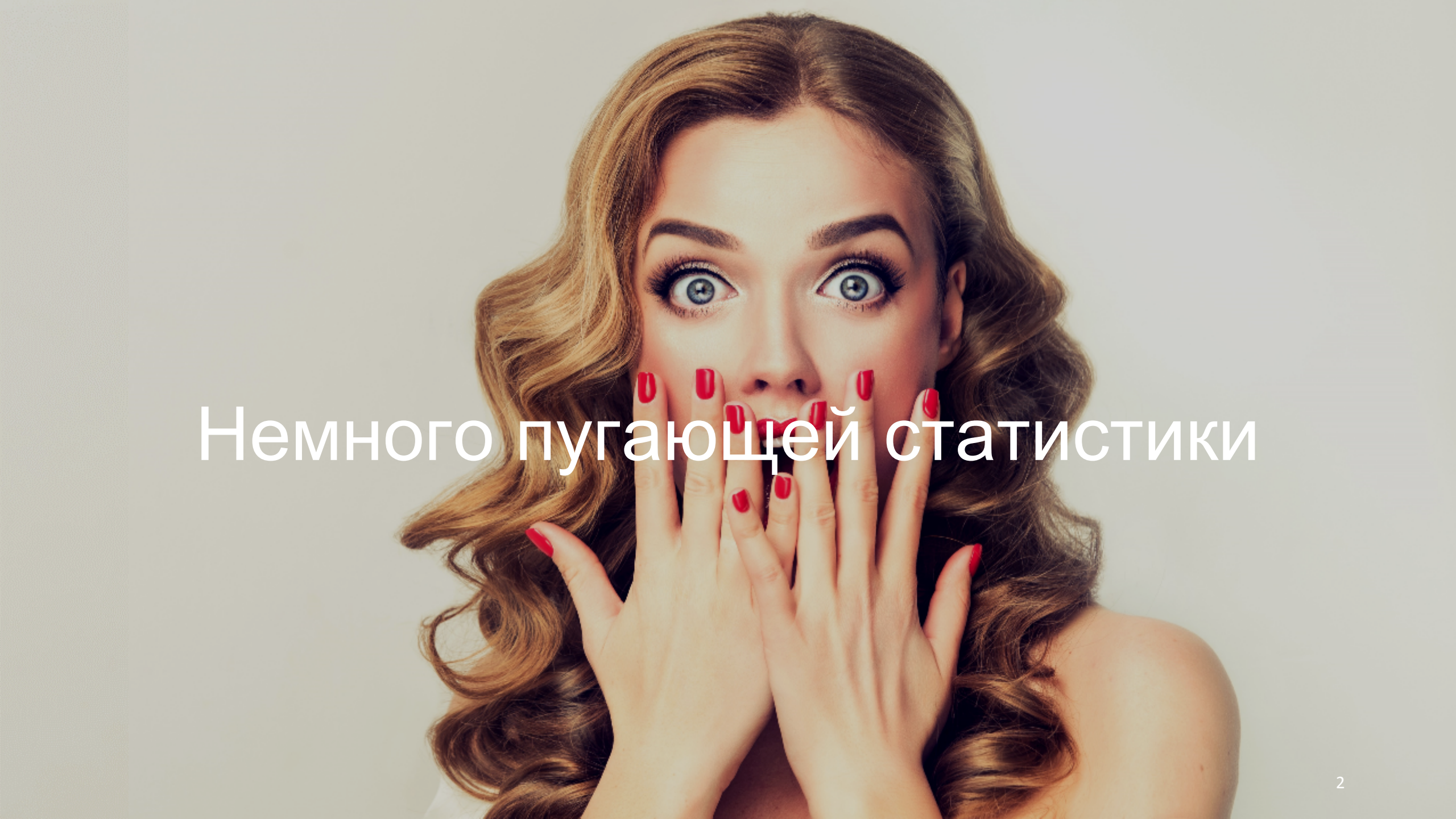
мониторинг информационной безопасности в проекте «умный город»

Эшелон
комплексная безопасность

Дмитрий Донской, ГК «Эшелон»



Немного пугающей статистики

Количество организаций, подвергшихся атакам, и их потери

49%

Столкнулись с нарушением системы защиты

Как информация о последних нарушениях системы безопасности становилась известна

(n=1389)

Недобровольное разглашение (третья сторона)	Запрос отчета правоохранительными органами	Добровольное сообщение о случившемся
31%	31%	50%

29%

Столкнулись с потерей прибыли из-за нарушений в безопасности

Убытки менее 20%	Убытки 20% - 40%	Убытки 40% - 60%	Убытки 60% - 80%	Убытки 80% - 100%
62%	20%	10%	4%	4%

38%

Зафиксировали значительные потери прибыли

По данным Cisco, 2017

Угрозы 2017 г

ENISA Threat Landscape Report 2017
ETL 2017 | 1.0 | HSA | January 2018

Легенда:

Тенденции	Рейтинг
↓ падение	↑ подъем
→ стабильность	→ прежний
↑ рост	↓ понижение

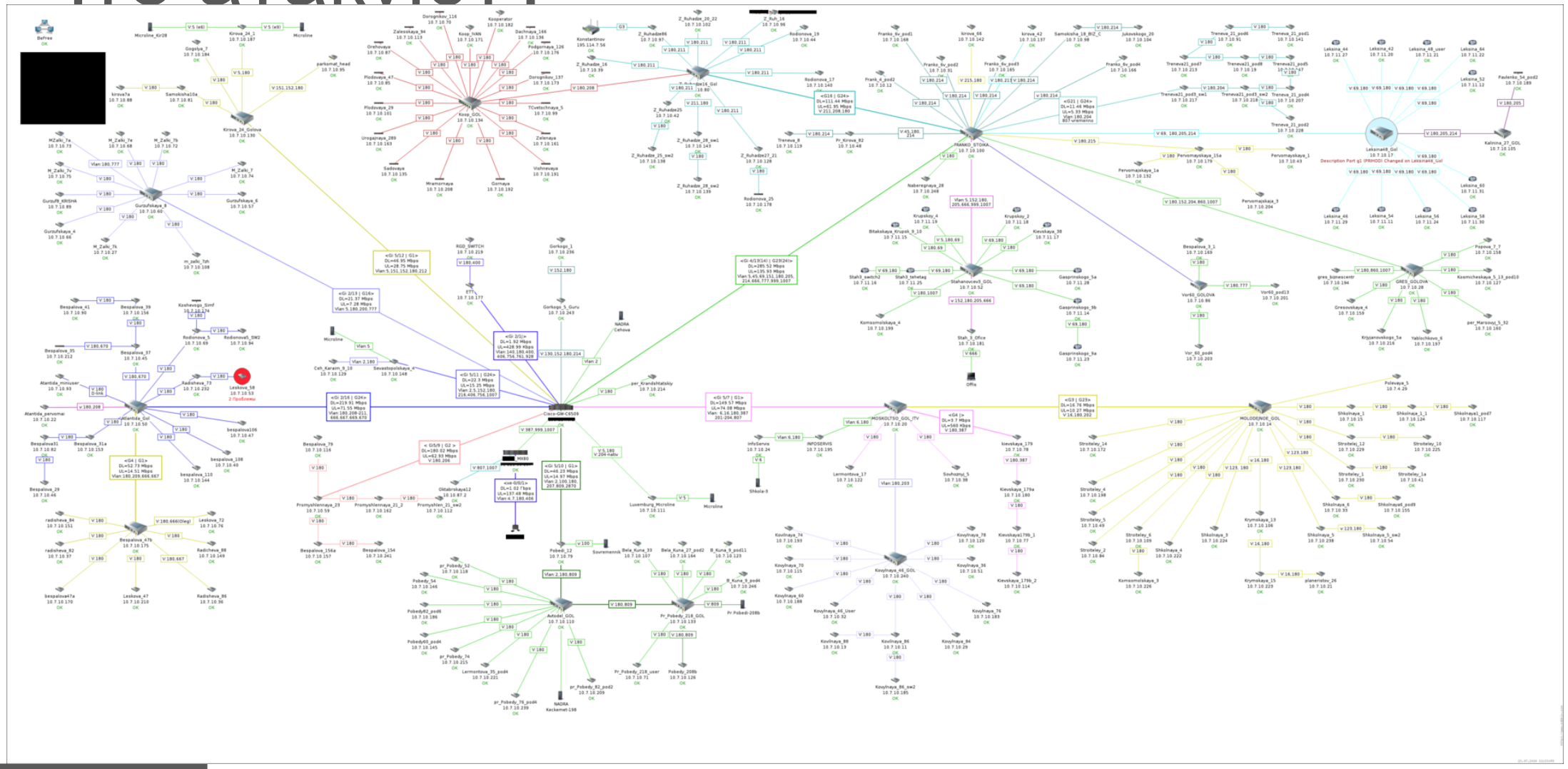
Основные угрозы 2016	Оценка тенденций 2016	Основные угрозы 2017	Оценка тенденций 2017	Изменение рейтинга
1. Вредоносное ПО	↑	1. Вредоносное ПО	→	→
2. Сетевые атаки	↑	2. Сетевые атаки	↑	→
3. Атаки на Web-приложения	↑	3. Атаки на Web-приложения	↑	→
4. DoS-атаки	↑	4. Фишинг	↑	↑
5. Ботнеты	↑	5. Спам	↑	↑
6. Фишинг	→	6. DoS-атаки	↑	↓
7. Спам	↓	7. Трояны-вымогатели	↑	↑
8. Трояны-вымогатели	→	8. Ботнеты	↑	↓
9. Угроза инсайдерской утечки	→	9. Угроза инсайдерской утечки	→	→
10. Физическое повреждение, кража, потеря	↑	10. Физическое повреждение, кража, потеря	→	→
11. Наборы эксплойтов	↑	11. Несанкционированный доступ	↑	↑
12. Несанкционированный доступ	↑	12. Кража персональных данных	↑	↑
13. Кража персональных данных	↓	13. Утечка информации	↑	↑
14. Утечка информации	↑	14. Наборы эксплойтов	↓	↓
15. Кибершпионаж	↓	15. Кибершпионаж	↑	→

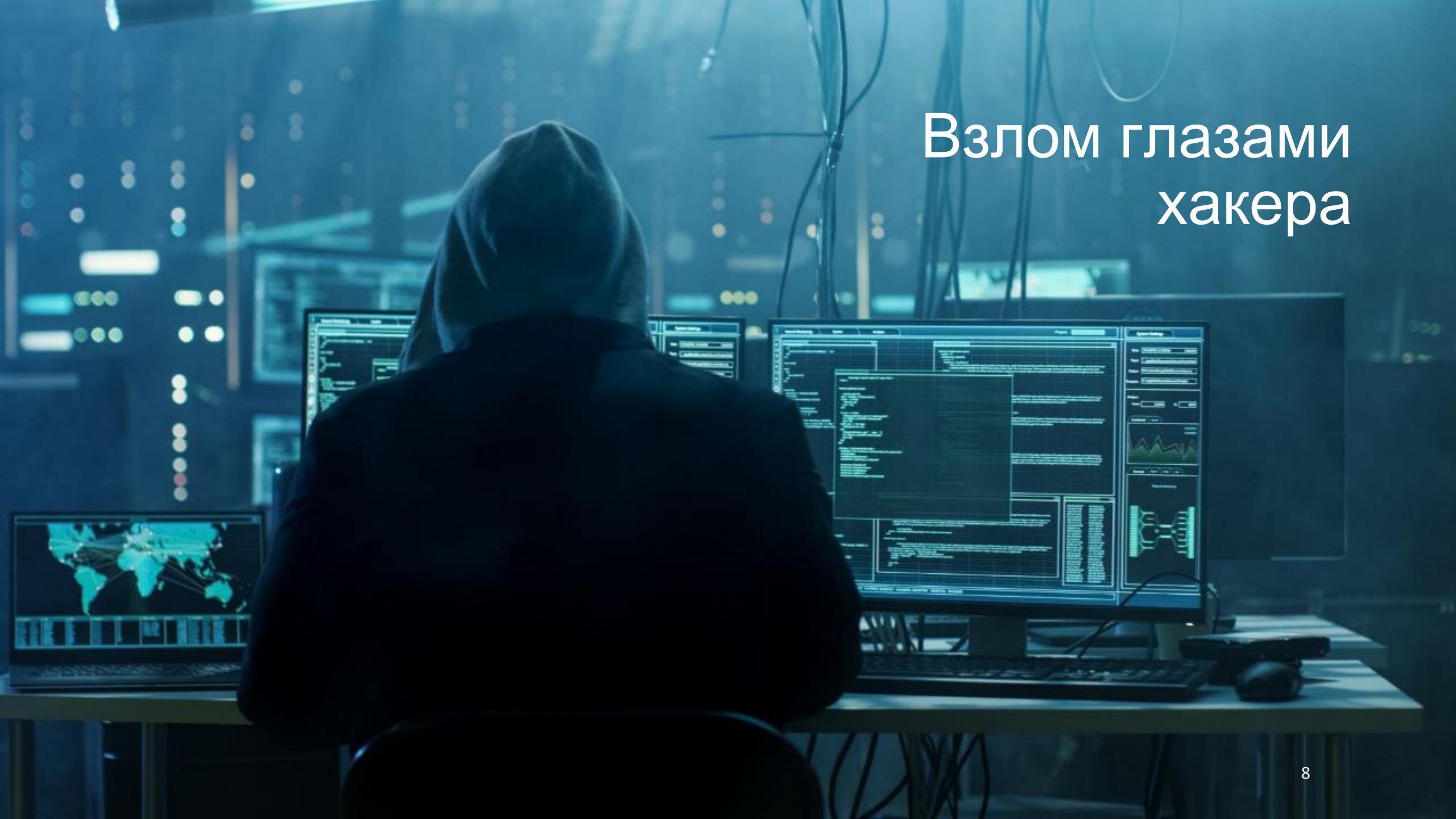
Интерактивная карта киберугроз (Россия №1 по количеству атак)

Новости 2019 года

- Вечером 10 июля 2019 года РБК сообщило, что логины и пароли примерно 450 000 клиентов Ozon попали в открытый доступ.
- Масштабная утечка 703 000 персональных данных работников РЖД.
- Издание «Коммерсант» сообщило об утечке персональных данных пользователей Альфа-банка, ОТП-банка и ХКФ-банка. Суммарно проблема затронула примерно 900 000 человек, и в обнаруженные БД включены данные о номерах телефонов, паспортах, местах работы и так далее.

Что атакуют?





Взлом глазами хакера

Фаза 1. Разведка

- Сбор информации об ИТ-инфраструктуре
  - запросы к DNS (whois)
  - построение маршрутов (traceroute)
  - анализ заголовков e-mail
  - сканирование портов
  - анализ сайтов организации и ее партнеров
  - анализ открытых вакансий
- Сбор информации о сотрудниках
  - «пробивание» людей в интернете

Фаза 2. Нападение

- Социальная инженерия
  - рассылка писем с вредоносными ссылками
  - атака через сторонние ресурсы, посещаемые пользователями из целевой организации
  - манипулирование сотрудниками, имеющих необходимый доступ
- Эксплуатация уязвимостей
  - подбор паролей
  - запуск эксплойтов
  - атаки на Web-системы (SQL-инъекция, XSS)

Фаза 3. Разведка ВНУТри

- Выявление «интересных» ресурсов
  - основные информационные системы компании
  - почтовый сервер
  - файловые серверы
  - рабочие станции руководителей организации
- Основная технология: сканирование портов

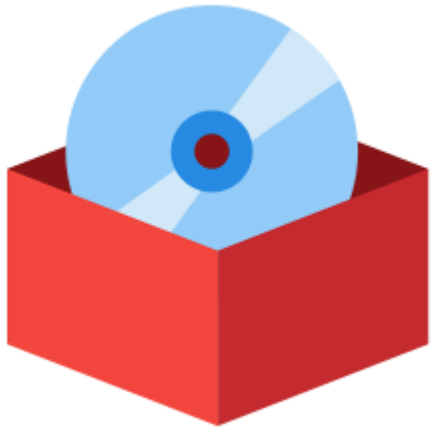
Фаза 4. получение внутреннего доступа

- **Компрометация учетных записей**
  - **перехват трафика (с целю получения хешей паролей)**
  - **подбор паролей**
  - **эксплуатация уязвимостей**

Фаза 5. ПЕРЕДАЧА ИНФОРМАЦИИ

- Скрытая передача информации
  - используется криптография
  - скрытые каналы передачи: DNS, HTTP(S) и др.

Инструментарий нападающих



Специально разработанное вредоносное программное обеспечение

Утилиты операционной системы

Хакерские утилиты с открытым исходным кодом

Специально разработанное вредоносное по

- Разрабатывается командой программистов
- Модульная структура
- Включает средства обхода и даже борьбы с антивирусами, СОВ и других СЗИ
- Использует криптографическую защиту
- Использует стандартные порты и протоколы для коммуникаций

ТОП-10 инструментов хакеров*

1. Mimikatz (хакерская утилита)
2. PsExec (утилита для администрирования)
3. Net (утилита для администрирования)
4. PoisonIvy (бэкдор)
5. Cobalt Strike (коммерческое ПО для проведения пентестов)
6. Systeminfo (утилита для администрирования)
7. Tasklist (утилита для администрирования)
8. Ipconfig (утилита для администрирования)
9. Windows Credential Editor (утилита для администрирования)
10. Reg (утилита для администрирования)

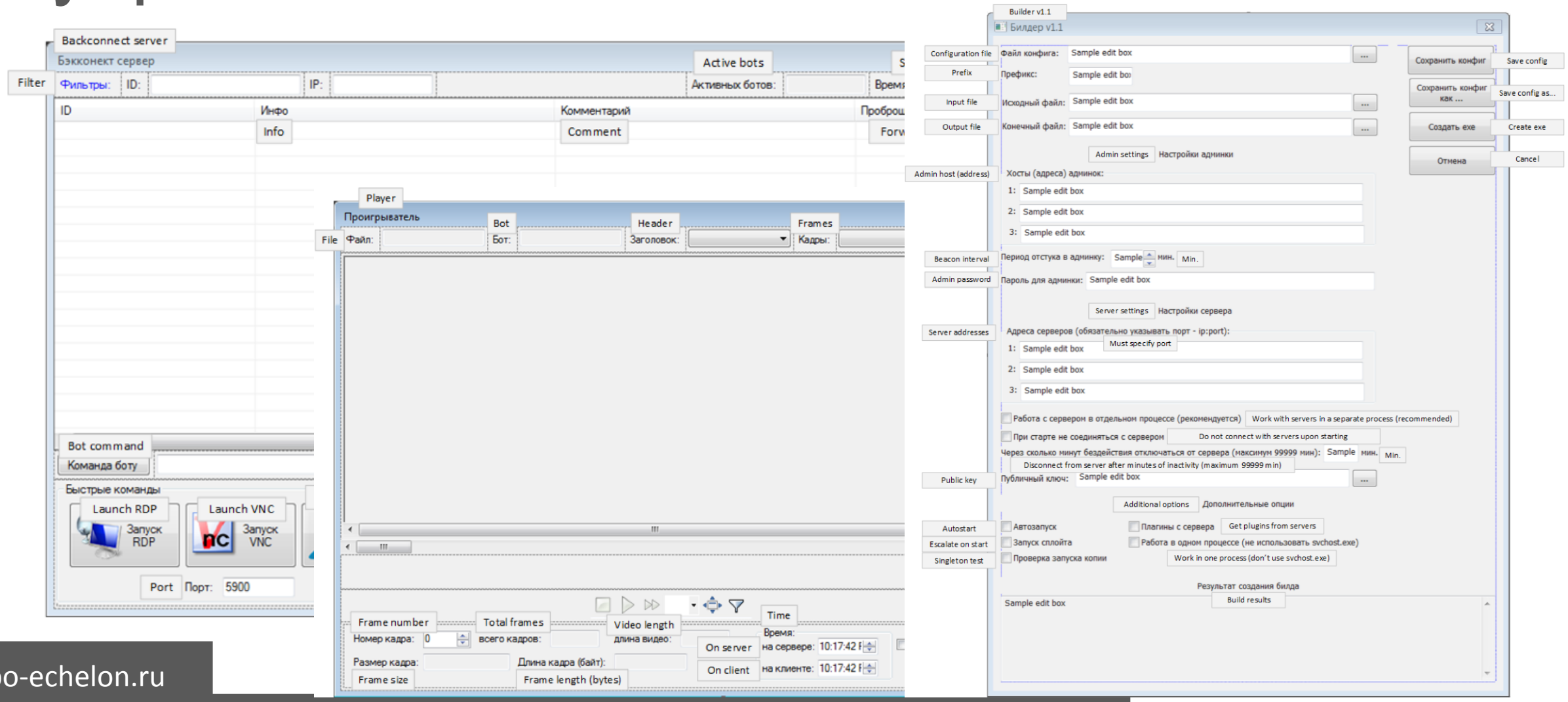
* На основе анализа данных MITRE ATT@CK

Топ-10 хакерских техник

1. Использование скриптов
2. Извлечение учетных данных пользователей (логин/хэш-пароля)
3. Провоцирование пользователей на запуск вредоносного ПО
4. Обфускация файлов
5. Использование скриптового языка PowerShell
6. Включение вредоносных файлов в электронные письма
7. Использование интерфейса командной строки
8. Использование стандартных протоколов для коммуникаций
9. Изменение процесса автозагрузки (реестр, папка автозагрузки)
10. Удаленное копирование файлов

* На основе анализа данных MITRE ATT@CK

Дружественный интерфейс для управления ботами



Описание Команд из руководства пользователя (1)

1. Video – запись видео
2. Download – загрузка и запуск файла
3. Ammyy – загрузка и запуск специального плагина
4. Update – обновление бота
5. Updklgcfg – загрузка файла конфигурации для кейлоггера
6. Httpproxy – включение прокси-сервера для организации доступа в интернет ботов, не имеющих выхода напрямую
7. Killos – нарушение работоспособности ОС
8. Tunnel – организация туннелей между ботами
9. Adminka – указывает через какой прокси сервер слать запросы
10. Server – задает IP-адрес сервера управления
11. User – создает пользователя для RDP
12. Rdp – запуск RDP

Описание Команд из руководства пользователя (2)

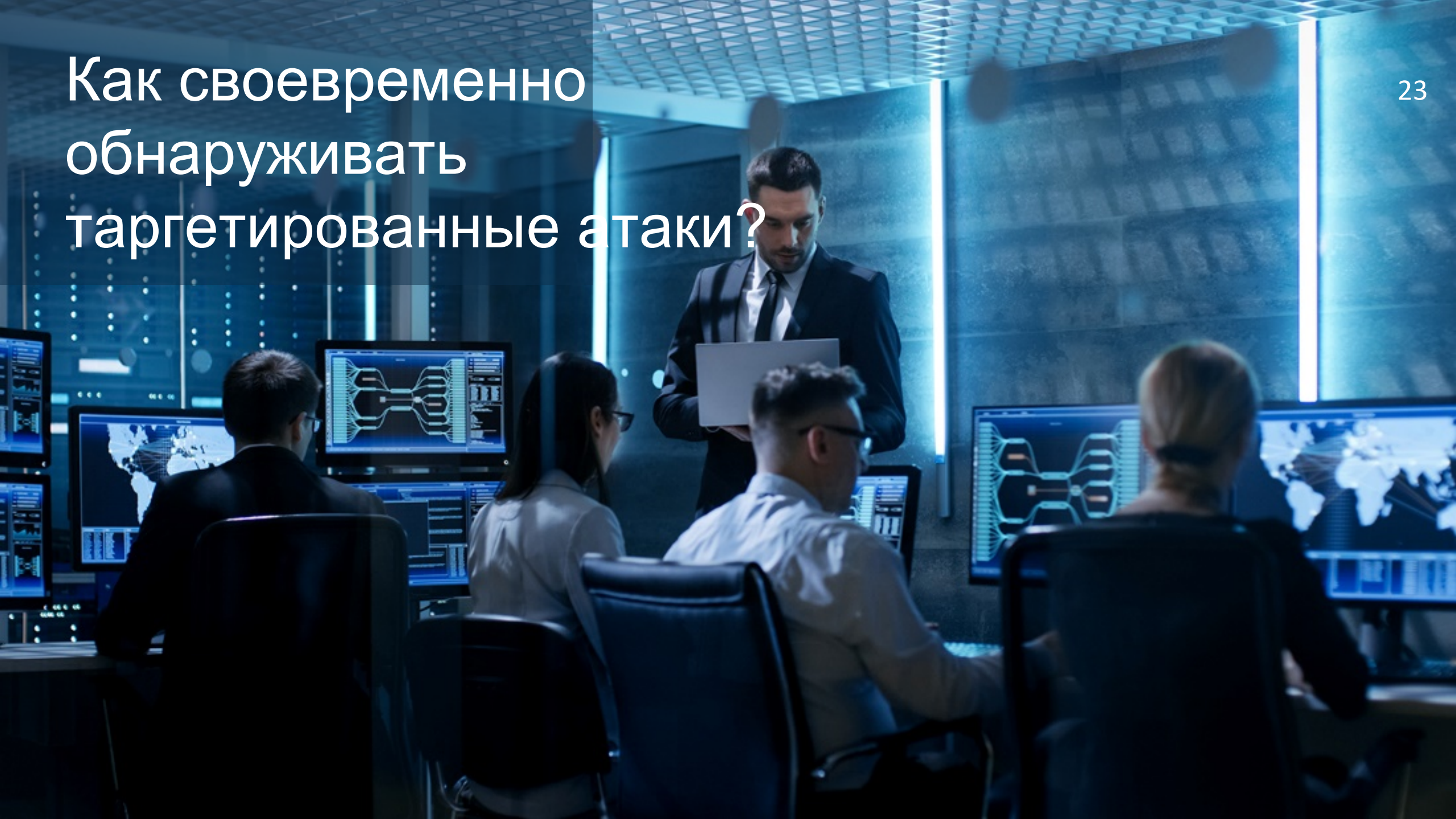
13. Secure – закрепляет бота в секретном месте
14. Del – удаляет удаление файла с затиранием
15. Startcmd – сохраняет указанную в аргументах команду в настройках бота и эта команда будет выполнится после перезапуска машины
16. Runmem – загружает файл и запускает его в памяти
17. Logonpasswords – загружает имена учетных записей и пароли, используя библиотеку mimikatz
18. Screenshot – создание скриншота экрана
19. Dupl – дублирование отсылаемых данных в локальную папку
20. Findfiles – поиск, сжатие и отправка файлов
21. Vnc – загрузка VNC и открытие сессии
22. Runfile – запуск указанного файла, размещенного локально
23. Killbot – самоуничтожение бота и зачистка следов

От чего защищают сзи?

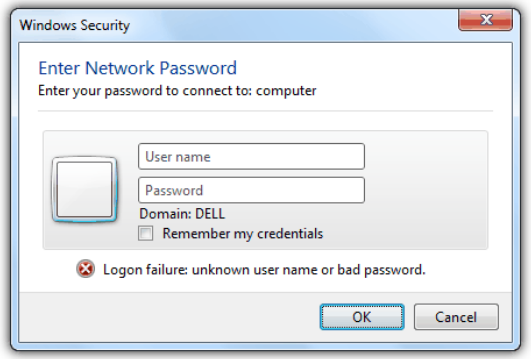
1. Действуют на основании правил
2. Имеют уязвимости
3. Постоянно активны
4. Их можно изучить

Главным образом от удаленного воздействия

Как своевременно обнаруживать таргетированные атаки?

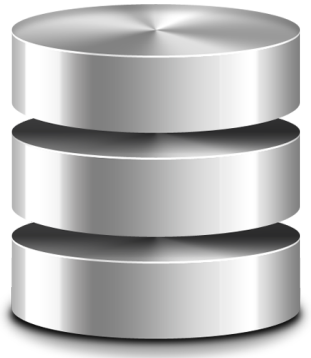


Необходимо отслеживать массу признаков нарушения ИБ



Аутентификация: как успешная, так и неуспешная

Срабатывания антивирусного ПО, СОВ



Подозрительные запросы к СУБД

Нетипичное поведение пользователя

и т.д. и т.п.

Для этого надо осуществлять мониторинг **критичных** сегментов инфраструктуры

vmware - Notepad

File Edit Format View Help

```
Apr 27 09:55:34: vmx| Log for VMware Workstation pid=2548 version=5.!
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\VMware\VMware W
Apr 27 09:55:34: vmx| UI Connecting to pipe '\\.\pipe\vmxc28be6e39c18
Apr 27 09:55:34: vmx| CPU #0 TSC = 7336583627359
Apr 27 09:55:34: vmx| CPU #1 TSC = 7336583626617
Apr 27 09:55:34: vmx| TSC delta 742
Apr 27 09:55:34: vmx| VMMon_GetkHzEstimate: Calculated 2793030 kHz
Apr 27 09:55:34: vmx| cpuids[0].id81.ecx = 0x0
Apr 27 09:55:34: vmx| cpuids[1].id81.ecx = 0x0
Apr 27 09:55:34: vmx| pcpu #0 CPUID numEntries=5 GenuntelineI
Apr 27 09:55:34: vmx| pcpu #0 CPUID version=0xf34 id1.edx=0xbfebfbff
Apr 27 09:55:34: vmx| pcpu #0 CPUID id80.eax=80000008 id81.edx=0x0 ic
Apr 27 09:55:34: vmx| pcpu #1 CPUID numEntries=5 GenuntelineI
Apr 27 09:55:34: vmx| pcpu #1 CPUID version=0xf34 id1.edx=0xbfebfbff
Apr 27 09:55:34: vmx| pcpu #1 CPUID id80.eax=80000008 id81.edx=0x0 ic
Apr 27 09:55:34: vmx| CPUID id1.edx: 0xbfebfbff id1.ecx: 0x441d id81.
Apr 27 09:55:34: vmx| CPUID id88.ecx: 0 id88.edx: 0
Apr 27 09:55:34: vmx| ACL_InitCapabilities: here 1 (bug 63252)
Apr 27 09:55:34: vmx| changing directory to C:\virtual\XP\.
Apr 27 09:55:34: vmx| Config file: C:\virtual\XP\Windows XP Professic
Apr 27 09:55:34: vmx| VMXVmdbCbvmvmxExecState: Exec state change requ
Apr 27 09:55:34: vmx| PowerOn
Apr 27 09:55:34: vmx| Host: WIN32 highest NUMA node 0
Apr 27 09:55:34: vmx| Host: WIN32 NUMA node 0, CPU mask 0x0000000000(
Apr 27 09:55:34: vmx| HOST Windows version 5.1, build 2600, platform
Apr 27 09:55:34: vmx| DICT --- USER PREFERENCES
Apr 27 09:55:34: vmx| DICT     pref.view.navBar.type = favorites
Apr 27 09:55:34: vmx| DICT       webUpdate.checkLast = 1146144710
```

```
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozilla/5.0 (
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200 431 "ht
fox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200 509 "h
efox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 513 "htt
ox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "-" "Mo
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "http://lo
0"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 499 "htt
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200 817 "ht
101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/compressed.gif HTTP/1.1" 200 1
) Gecko/20100101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/movie.gif HTTP/1.1" 200 527 "ht
0/20100101 Firefox/56.0"
::1 - - [31/Oct/2017:11:26:57 +0530] "GET /ravi HTTP/1.1" 404 494 "-" "Mozilla/5.0 (X
.36"
::1 - - [31/Oct/2017:11:26:57 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "http://loca
ome/60.0.3112.90 Safari/537.36"
::1 - - [31/Oct/2017:11:27:20 +0530] "GET /anusha HTTP/1.1" 404 496 "-" "Mozilla/5.0 (
37.36"
Waiting for data...  (interrupt to abort)
```

	Source	Thread...	Severity	Event Id	Text
12:09:25....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:09:28....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
12:12:40....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 222.36.7...
12:14:55....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 64.62.19...
12:19:08....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
12:19:10....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
12:25:54....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 81.89.5.5...
12:28:10....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
12:28:13....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
12:35:04....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12:35:06....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12:37:48....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
12:37:51....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
12:59:12....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 118.26.1...
12:59:13....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 79.125.1...
13:19:09....	WinGate NAT	248	Info	2	Authorisation failure: NAT STATUS: firewall block: TCP src 124.114....

	DB	DB
04.00002.00071	6950	6950
05.00000.02106	6950	6950

Status Monitoring

-03-08 14:53:00

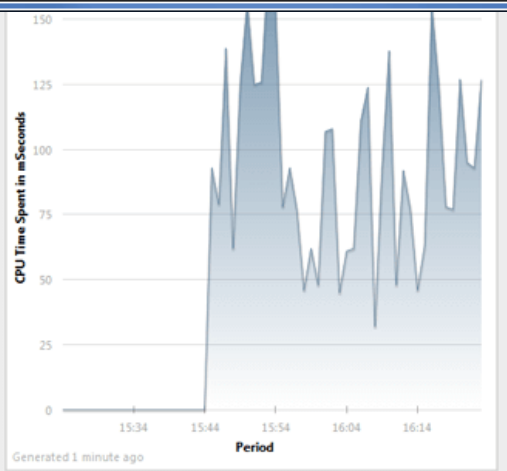
-03-08 15:23:52

urope Standard Time (UTC+1:00)

ys 0 hr. 38 mins. 25 sec.

nt: 0, Console: 2, Replicate In: 0, Replicate Out: 0, nt: 0

nt: 451, Console: 5, Replicate In: 0, Replicate Out: gent: 0



Number of clients disconnected for a week 0

Number of clients disconnected for a month 0

Number of clients disconnected for more than 3 months 0

Generated 6 minutes ago

Server Hardware Load

Managed and Unmanaged Computers

Generated 1 minute ago

Ручной сбор может быть проблематичным

РЕШЕНИЕ:
Сбор и корреляция Событий безопасности с помощью SIEM-системы

SIEM-система позволяет делать самое Сложное - выявлять приемы злоумышленников

Принцип работы SIEM-системы

Нормализация

Приоритезация

Корреляция

Фильтрация

Оповещение

ОСНОВНой функционал SIEM-системы

- Лог-менеджмент: сбор, хранение, поиск событий
- Корреляция событий
- Аналитика (отчеты, дашборды и т.п.)
- Управление инцидентами
- Оценка рисков
- Оценка выполнения требований

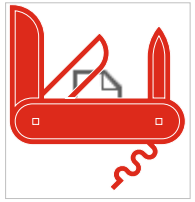
комрад

Гибкая и производительная система централизованного управления событиями информационной безопасности, совместимая с отечественными средствами защиты информации.

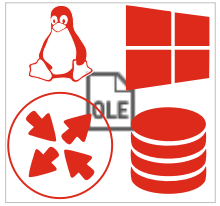
Сертификаты: ФСТЭК России №3498 Минобороны России №3899

отличительные возможности

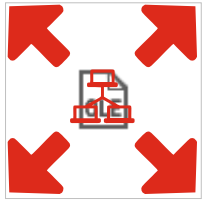
Высокая производительность



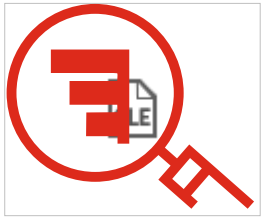
Универсальный адаптер для любого источника событий



Широкий спектр поддерживаемых источников событий



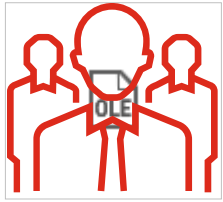
Масштабирование



Визуальный конструктор запросов и директив корреляции

Визуальный анализ данных

Оперативное оповещение об инциденте



Ролевая модель управления доступом

Поддержка отечественных СЗИ

- **Astra Linux**
- МЭ и СОВ «Рубикон»/«Рубикон-К»
- Сканер-ВС
- Kaspersky Security Center
- Форпост
- SecretNet 3.5-3.7 (сервер управления)
- БлокХост-Сеть
- vGate R2
- ViPNet Coordinator HW2000
- VIPNet IDS
- АССОИ «Матрица»
- …

Инструменты SIEM Комрад: Инциденты

КОМРАД Инциденты admin

Открытые 462
Просмотренные 156
Закрытые 258

Поиск...

Имя директивы	Всего
Brute(Uc)	9
Попытка входа на webui Dlink	19
Brute(Scanner)	21
Storage in not online	3
Рубикон Срабатывание правил СОВ (+PCAP)	48
KAV Базы устарели	53
KAV Срабатывание защиты	37
Dallas Lock Нарушение целостности реестра	2
AstraLinux Ошибка аутентификации	21
Рубикон Срабатывание правила СОВ	253
Рубикон Ошибка контрольной суммы	1
Рубикон Срабатывание правила МЭ	98
Windows Server Ошибка аутентифкации	45
Windows Server AD Удаление пользователя	3
Windows Server AD Удаление группы	1
Windows Server Критические ошибки	73
Linux Server Ошибки журнала	34
Комрад Ошибка хранилища	1

И или + Добавить + Добави

№ больше 0

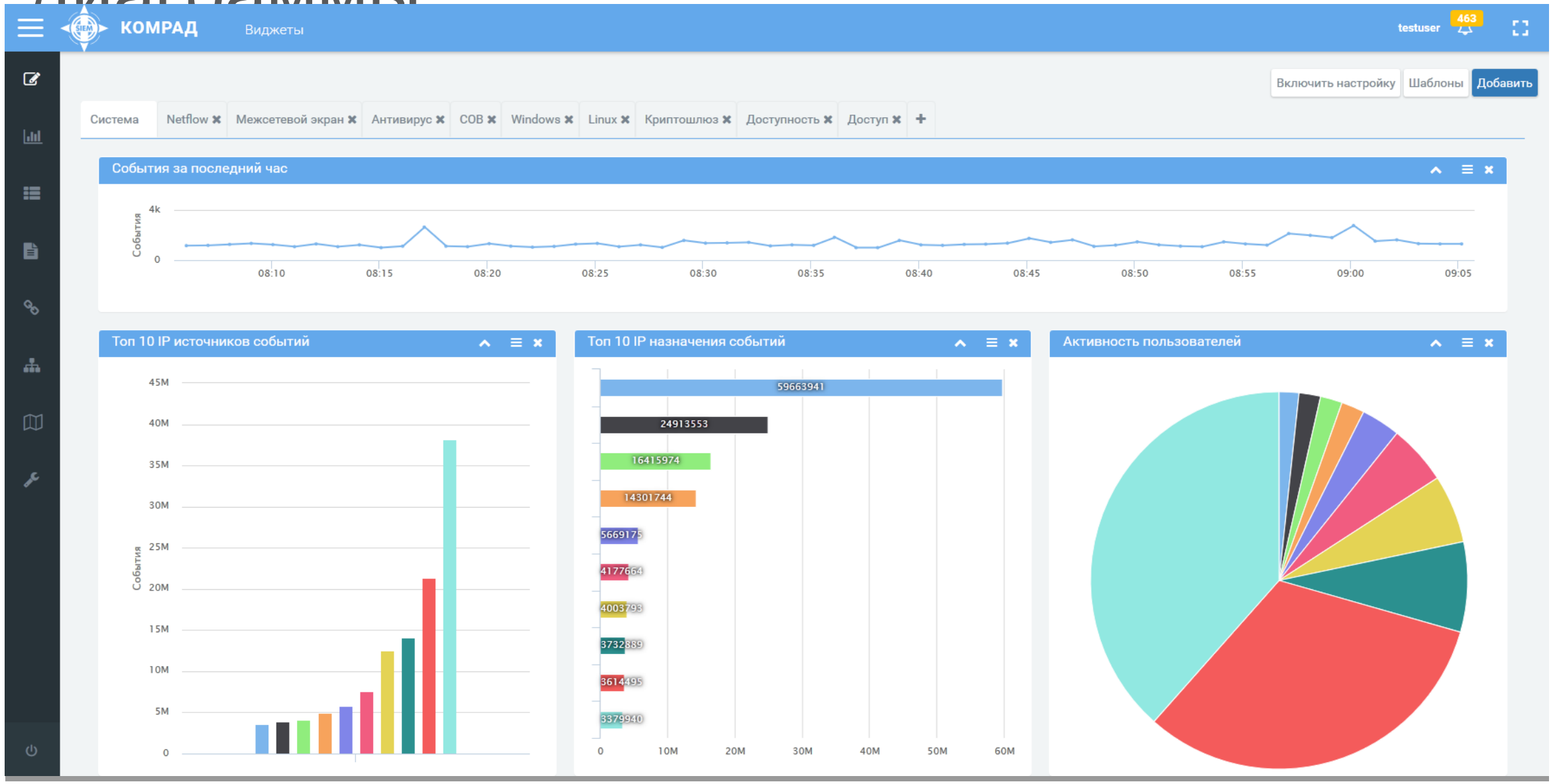
Поиск Всего найдено: 876

Отметить как Удалить

№	Имя директивы	Дата фиксации	События	Длительность	Риск	Статус	Дата начала	Действия
1908	Brute(Scanner)	10/07/2018 15:29:27	25	00:01:55	риск 3		10/07/2018 15:27:32	
1907	KAV Базы устарели	10/07/2018 15:27:03	1	00:00:01	риск 1		10/07/2018 15:25:09	
1906	Рубикон Срабатывание правила	10/07/2018 15:23:18	31	00:10:53	риск 1		10/07/2018 15:21:25	
1905	Windows Server AD Удаление	10/07/2018 15:10:19	25	00:01:53	риск 1		10/07/2018 15:08:26	
1904	Brute(Uc)	10/07/2018 15:08:06	25	00:03:34	риск 2		10/07/2018 15:06:12	
1903	Рубикон Ошибка контрольной	10/07/2018 14:56:50	1	00:00:01	риск 1		10/07/2018 14:54:57	
1902	Brute(Scanner)	10/07/2018 14:50:32	25	00:01:54	риск 1		10/07/2018 14:48:38	
1901	Brute(Scanner)	10/07/2018 14:10:31	25	00:01:53	риск 1		10/07/2018 14:08:38	
1900	Linux Server Ошибки журнала	10/07/2018 14:08:28	2	00:00:02	риск 2		10/07/2018 14:06:36	
1899	Brute(Scanner)	10/07/2018 14:06:27	25	00:01:54	риск 1		10/07/2018 14:04:33	

Первая < 1 2 3 4 5 ... 54 > Последняя

Инструменты SIEM Комрад: Виджеты и диаграммы



Инструменты SIEM Комрад: поиск по событиям

KOMRAD

Поля таблицы

- № события
- Дата генерации
- Дата фиксации
- Данные
- Тип сообщения
- ID плагина
- SID плагина
- IP источника
- IP назначения
- Протокол
- Порт источника
- Порт назначения
- Имя источника
- Имя назначения
- MAC источника
- MAC назначения
- Имя файла
- Имя пользователя
- HTTP метод
- HTTP запрос
- HTTP код возврата
- HTTP ресурс
- HTTP клиент
- GeoIP Город источника
- GeoIP Город назначения
- GeoIP Страна источника
- GeoIP Страна назначения
- АССОИ Тип объекта
- АССОИ Имя объекта
- АССОИ Инициатор

Имя запроса: Имя запроса

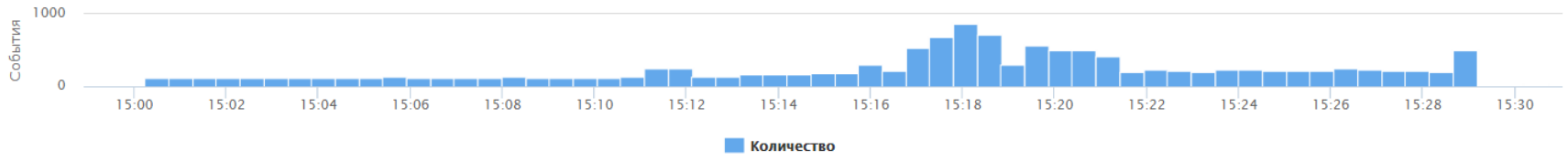
Описание: Пример описания

И ИЛИ

Добавить | Добавить группу

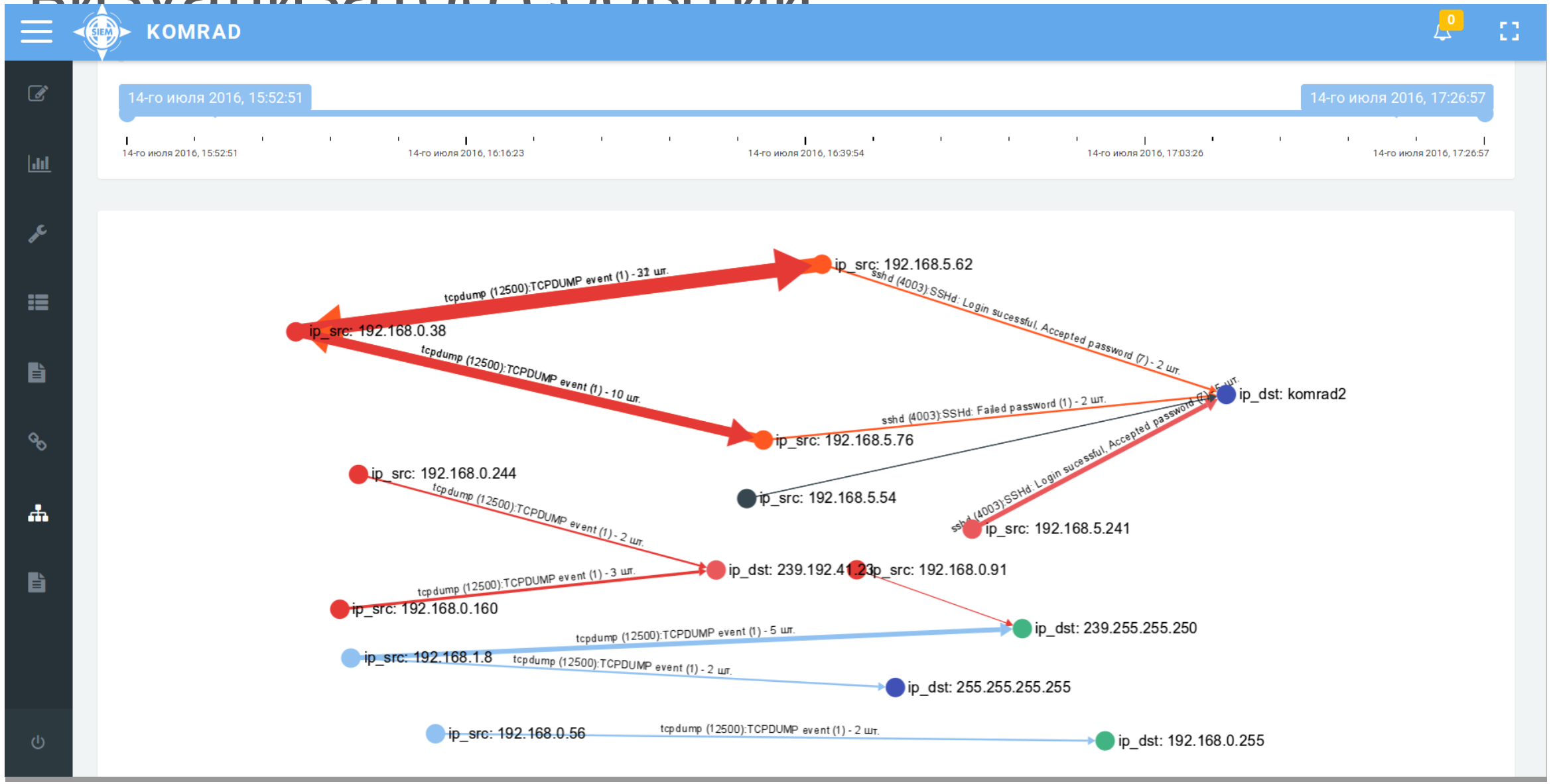
Дата фиксации | больше | 29/08/2016 15:00:00 | Удалить

Поиск | Сбросить | Сохранить | Всего найдено: 13306 | От: 29. авг 2016, 14:59:11 | До: 29. авг 2016, 15:30:28 | Скачать

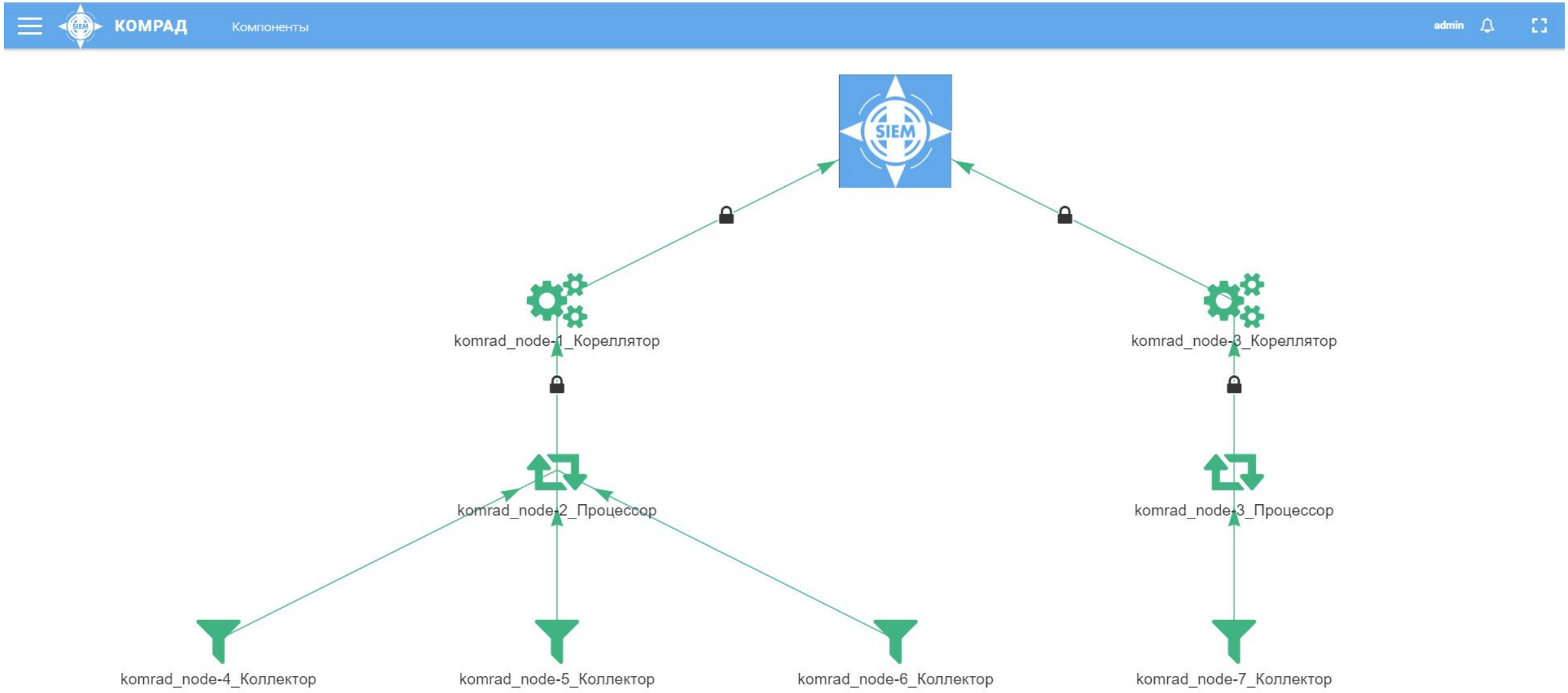


№ события	Данные
147247382...	Aug 29 15:30:16 komrad2 systemd[1]: [/etc/systemd/system/komrad-web.service:1] Missing '='.
147247381...	Aug 29 15:30:14 komrad2 gunicorn[15648]: Server initialized for eventlet.
147247381...	Aug 29 15:30:14 komrad2 gunicorn[15648]: WARNING: No route found for IPv6 destination :: (no default route?)
147247381...	Aug 29 15:30:14 komrad2 gunicorn[15648]: WARNING: Failed to execute tcpdump. Check it is installed and in the PATH
147247381...	Aug 29 15:30:14 komrad2 gunicorn[15648]: [2016-08-29 15:30:14 +0000] [15652] [INFO] Booting worker with pid: 15652
147247381...	Aug 29 15:30:14 komrad2 gunicorn[15648]: [2016-08-29 15:30:14 +0000] [15648] [INFO] Using worker: eventlet
147247381...	Aug 29 15:30:14 komrad2 gunicorn[15648]: [2016-08-29 15:30:14 +0000] [15648] [INFO] Listening at: http://127.0.0.1:8000 (15648)

Инструменты SIEM Комрад: визуализатор событий



Комрад: возможности масштабирования



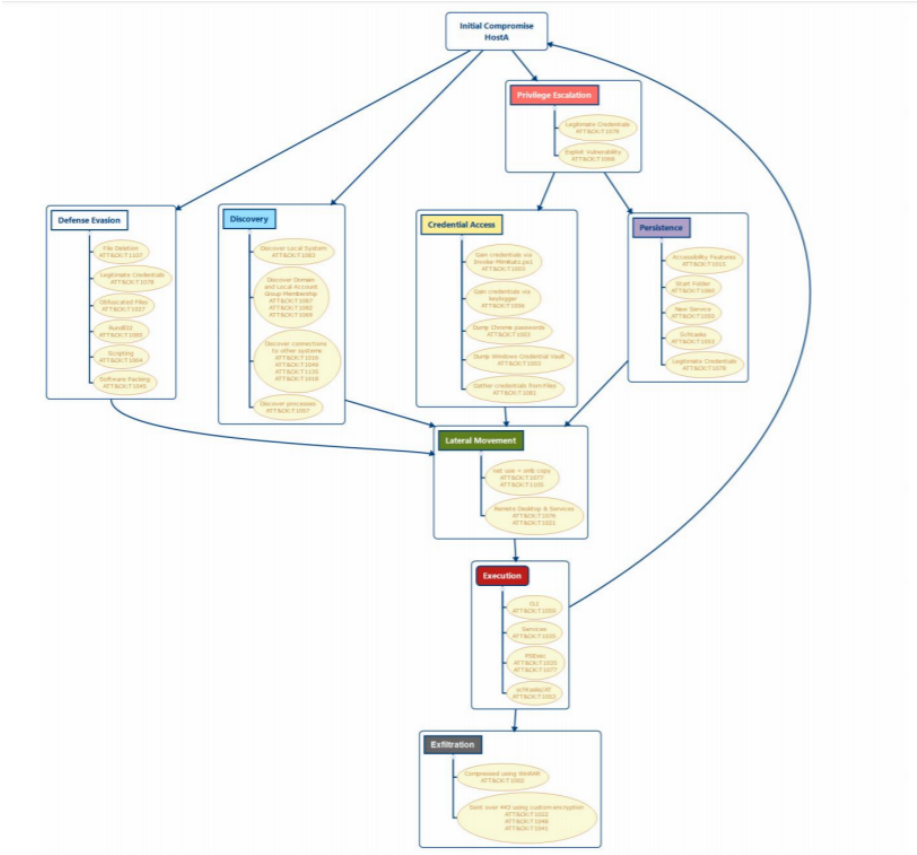
С помощью SIEM-системы можно обнаруживать хакерскую активность, но только если грамотно настроены директивы корреляции

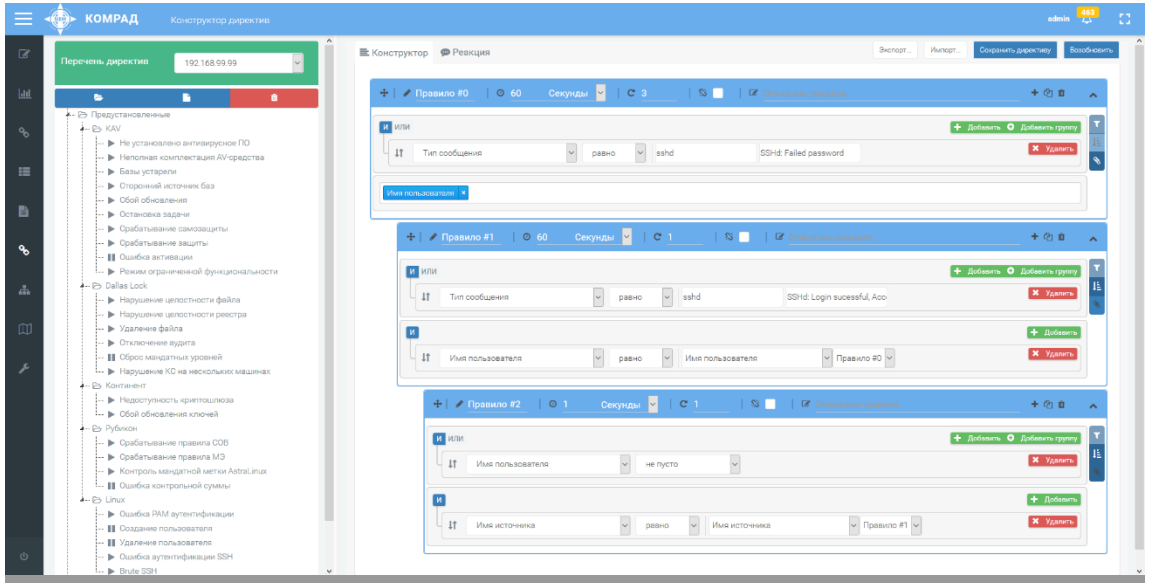
Матрица хакерских техник

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol

https://attack.mitre.org/matrices/enterprise/

директивы корреляции основываются на хакерских приемах



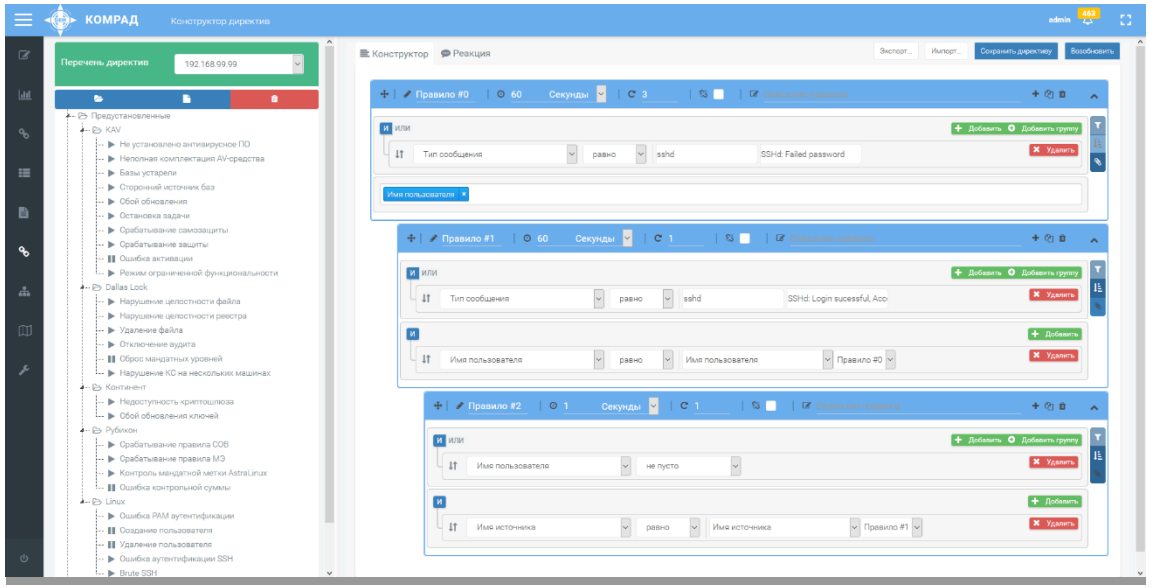


В SIEM-системе должны быть уже Предустановлены директивы корреляции

SIEM КОМРАД:

более **80**

предустановленных директив корреляции



Примеры директив корреляции SIEM КОМРАД

- Обнаружение доступа к групповым политикам
- Обнаружение использования WHOAMI
- Обнаружение передачи пользователю прав локального администратора
- Обнаружение флагов Adwind
- Обнаружение флагов WannaCry
- Обнаружение флагов PsExec
- Обнаружение превышения числа указанного числа попыток неуспешного доступа
- Обнаружение попытки подбора пароля для критичных учетных записей
- Обнаружение блокировани учетной записи после многочисленных неуспешных попыток
- Обнаружение блокирования критичной/сервисной учетной записи по превышению лимита неудачных входов
- Обнаружение интерактивный входа под служебной учетной записью
- Обнаружение попытки входа под заблокированной учетной записью

SIEM-система является ядром системы мониторинга событий иб, но далеко не единственным ее компонентом

Три ключевых компонента для организации эффективного мониторинга информационной безопасности

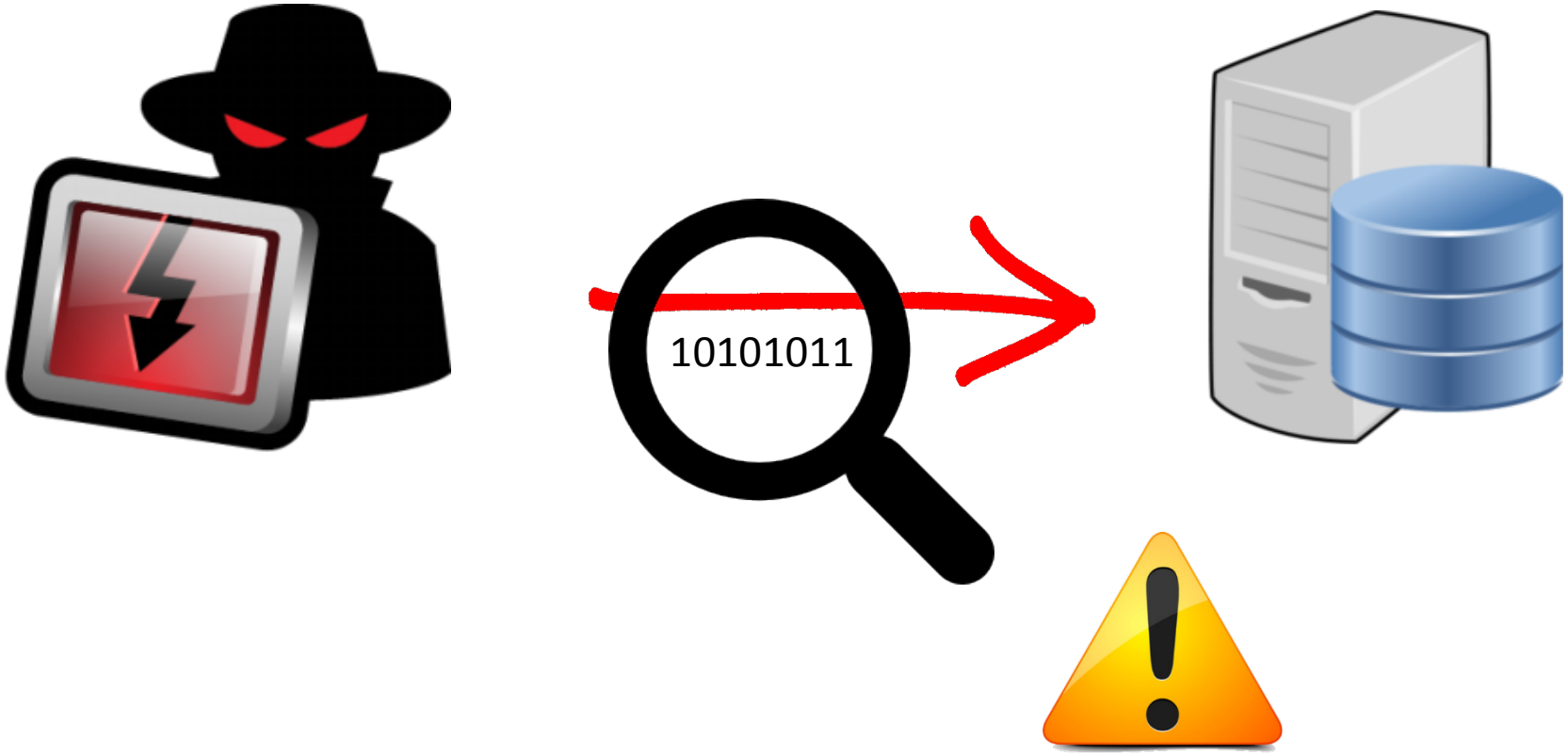
SIEM

СОВ

САЗ

Системы мониторинга ИТ

ОСНОВА СОВ – СИГНАТУРНЫЙ МЕТОД выявления атак



Пример правила СОВ

Действие
Протокол
IP-адрес отправителя пакета
Порт отправителя пакета
Направление трафика
IP-адрес получателя
Порт получателя
Сигнатура
Сообщение в случае срабатывания

alert tcp any any -> 192.168.1.0/24 111 (content:”|00 01 86 a5|”; msg: ”mountd access”;)

РУБИКОН

МЭ и СОВ в одном устройстве

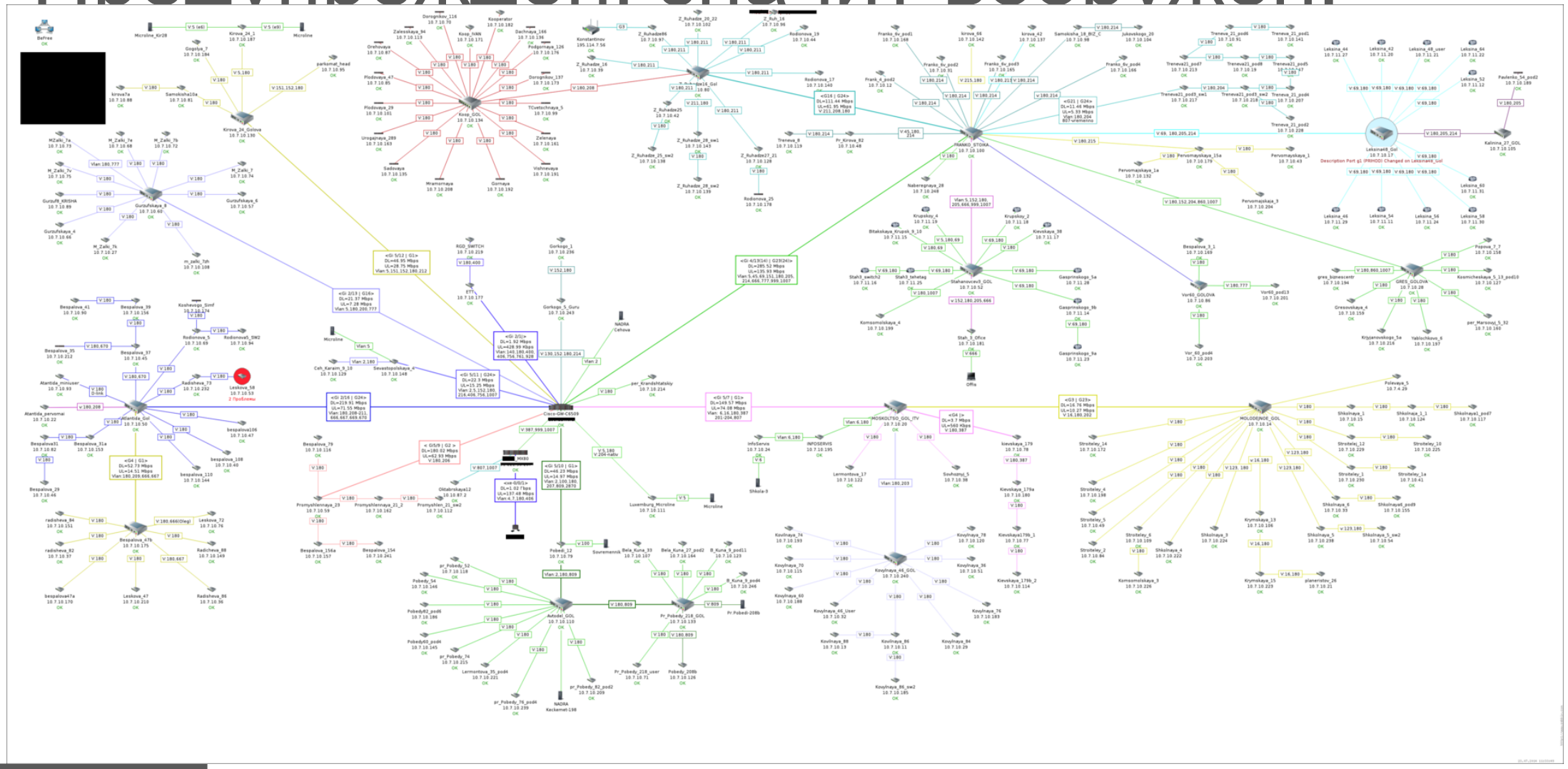
позволяет выявить сетевую активность современных «зловредов»

Варианты исполнений Пак «рубикон»

	МИКРО	МИНИ	1U	ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ	МУЛЬТИПОРТОВЫЙ	ЗАЩИЩЕННЫЙ	СПЕЦИАЛЬНОЕ ИСПОЛНЕНИЕ
Производительность МЭ	до 1,1 Gb/s	до 2 Gb/s	до 5 Gb/s	до 9 Gb/s	до 6 Gb/s	до 600 Mb/s	до 8,5 Gb/s
Производительность СОВ	до 580 Mb/s	до 1 Gb/s	до 3 Gb/s	до 3 Gb/s	до 2,5 Gb/s	до 400 Mb/s	до 2,5 Gb/s
Производительность маршрутизации	до 1,1 Gb/s	до 2 Gb/s	до 5 Gb/s	до 9 Gb/s	до 6 Gb/s	600 Mb/s	до 8,5 Gb/s
Последовательные интерфейсы	2xUSB, 1xVGA	2xUSB, 1xVGA, 1xConsole	2xUSB,1xConsole	2xUSB, 1xConsole	2xUSB, 1xConsole	6xUSB, 4xCOM, 1xDVI, 1xVGA	8xUSB, 1xDVI, 1xVGA, 1XHDMI
Сетевые интерфейсы	4xRJ45 10/100/1000	6xRJ451 10/100/1000	6xRJ45 10/100/1000 (+1 модуль расширения)	4 модуля расширения	8 модулей расширения	2xRJ45 10/100/1000	1xRJ45 10/100/1000, 1xSFP (+3 модуля расширения)
ОЗУ	2-8 Gb	2-16 Gb	2-64 Gb	2-64 Gb	2-512 Gb	1-2 Gb	4-32 Gb
Питание	10W 12V	40W 220V	250W 220V	280W 220V	720W 220V	100W 9-30V	250W 220V
Дополнения	нет	нет	4xRJ45 8xRJ45 4xSFP 8xSFP 2xSFP+	4xRJ45 8xRJ45 4xSFP 8xSFP 2xSFP+	4xRJ45 8xRJ45 4xSFP 8xSFP 2xSFP+	нет	1xRJ45 4xRJ45 4xSFP 2xSFP+
Решение	«Рубикон-К» «Рубикон-А»	«Рубикон» «Рубикон-К» «Рубикон-А»	«Рубикон» «Рубикон-К» однонаправленный шлюз «Рубикон» «Рубикон-А»	«Рубикон» «Рубикон-К» «Рубикон-А»	«Рубикон» «Рубикон-К» «Рубикон-А»	«Рубикон» «Рубикон-К»	«Рубикон-К» «Рубикон-А»

Регулярный контроль эффективности системы мониторинга информационной безопасности

Предупрежден, значит вооружен!



ЛУЧШе БИТь Первым!

НЕОБХОДИМО пользоваться арсеналом злоумышленников

Берем из практики реальных взломов

- цели злоумышленников
- инструменты
- методики

СКАНЕР-ВС делает комплексный анализ защищенности доступным

Сканер-ВС

анализ защищенности

Сканер-ВС позволяет провести комплексное тестирование защищенности

идентификация целевых сетевых узлов

- сбор информации о внешних ресурсах в Интернет
- сканирование сети
- согласование перечня с заказчиком

поиск уязвимостей

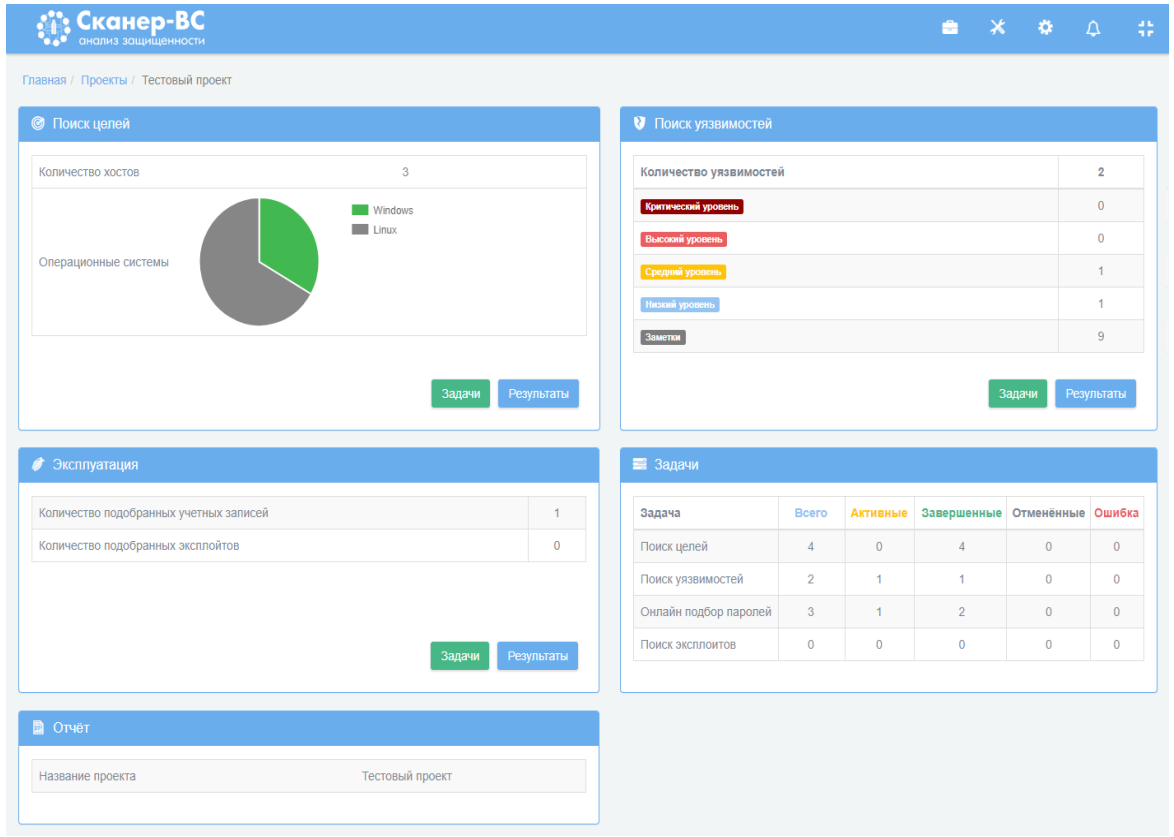
- с помощью сканеров
- вручную (по баннерам, ошибки конфигурации)

эксплуатация уязвимостей

- подбор паролей
- перехват трафика
- запуск эксплойтов
- и т.д.

расширение привилегий и зоны влияния

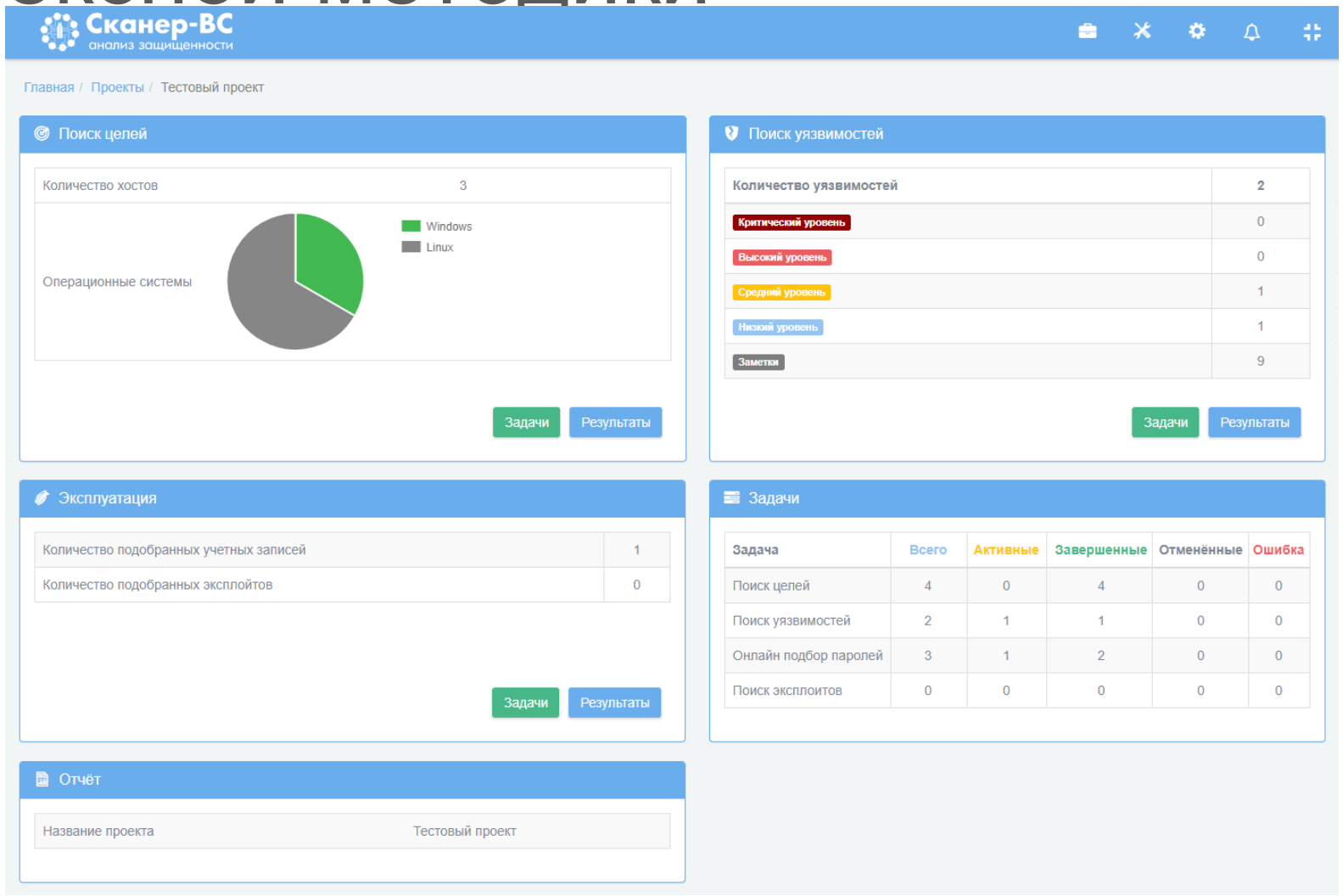
- запуск локальных эксплойтов
- использование собранной информации для доступа к другим системам



Ключевые технические проверки

- Сканирование портов
- Определение версий сервисов
- Сканирование уязвимостей
- Анализ конфигурации и уровня обновлений узла
- Подбор паролей
- Поиск подходящих эксплойтов

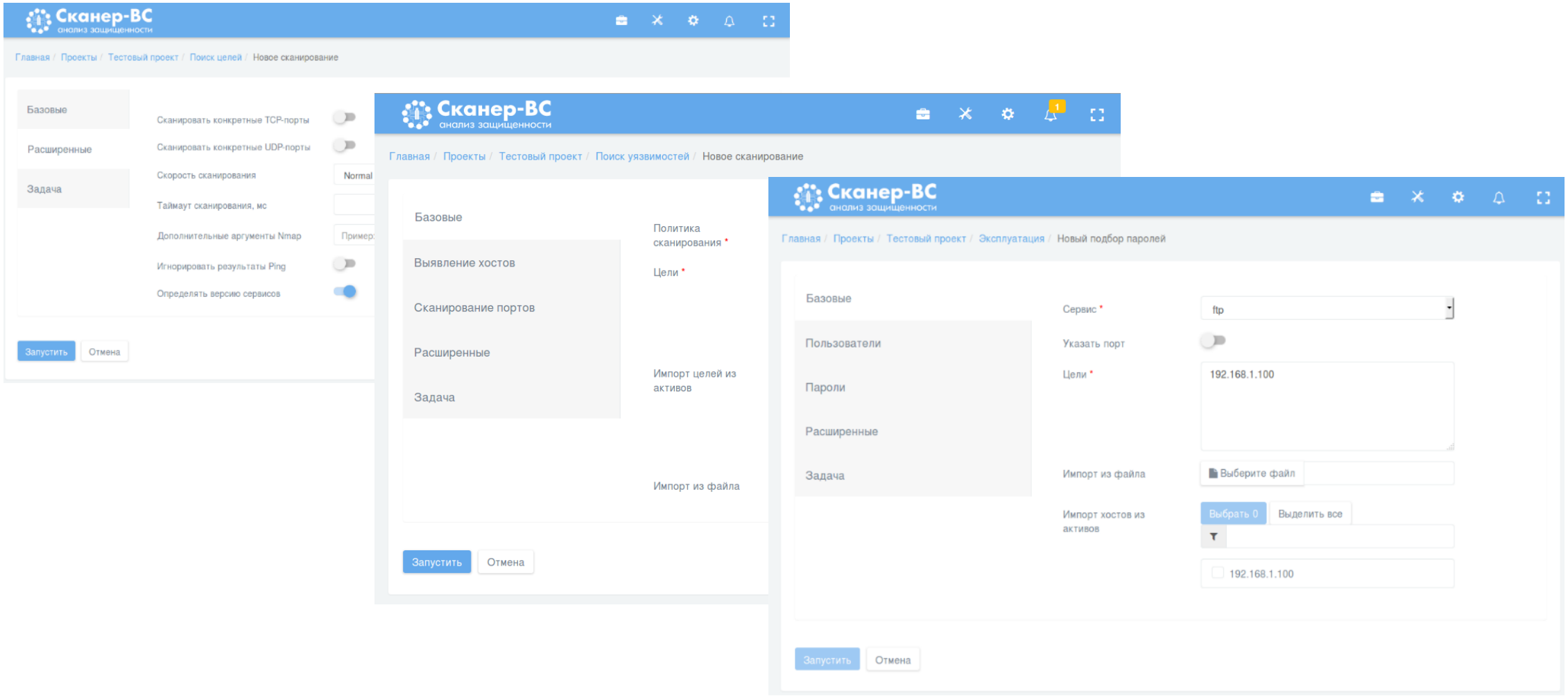
Сканер-ВС Поддерживает этапность комплексной методики



В едином Web-интерфейсе доступен функционал:

- Инвентаризация узлов и сервисов
- Поиск уязвимостей
- Подбор паролей к сетевым сервисам (поддерживается более 40 протоколов, различные готовые словари)
- Поиск доступных эксплойтов по версиям и типам сервисов
- Формирование единого отчета

Задачи по анализу задаются в унифицированном формате



СКАНЕР-ВС позволяет провести Аудит КОНФИГУРАЦИИ ASTRA Linux

- Проверка подсистемы безопасности PARSEC;
- Проверка СУБД PostreSQL
- Тесты для проверки Security Updates для версии 1.5
- Автоматизированы различные проверки из руководства по КСЗ, руководства администратора, руководства по эксплуатации
- Сбор дополнительной информации: перечень соединений в режиме ожидания (netstat tunpl) и перечень сервисов, загружаемых при запуске системы (chkconfig --list)

Полный ОТЧЕТ: СЕРВИСЫ, уязвимости, пароли и наличие подходящих эксплойтов

Сканер-ВС
анализ защищенности

Описание: Бэкдор устанавливается на удаленном хосте

5. Уязвимость удаленного выполнения RemoteCC RemoteCC

Порт: 3632

CVE: CVE-2004-2687

Уровень риска: Критический

Описание: DistCC 2.x, используемый в XCode 1.5 и других, когда не настроен на огра
которые выполняются сервером без проверки полномочий.

Решение: Обновления поставщика доступны. См. Ссылки для получения дополнитель

Подробнее:

http://distcc.samba.org/security.html
http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html

6. Слабый пароль PostgreSQL

Порт: 5432

Уровень риска: Критический

Описание: В удаленный PostgreSQL можно было войти в систему как пользователь р

Решение: Измените пароль как можно скорее.

7. Обнаружение DistCC

Порт: 3632

Уровень риска: Высокий

Описание: DistCC - это программа для распространения сборок C, C, Object C или Об
использовании и часто в два или более раза быстрее, чем локальный компилятор.

Решение: Для получения дополнительной информации о безопасности DistCC см. htt

Сканер-ВС
анализ защищенности

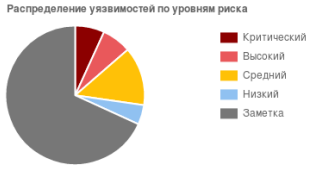
Главная / Проекты / Показ 25-09-17 / Отчёт

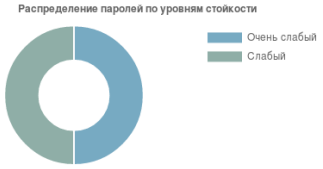
Настройки Печать

Сканер-ВС Отчёт

Имя проекта	Показ 25-09-17
Описание	
Тип отчёта	Общий
Дата формирования	27.09.2017 12:34:32
Общее количество хостов	3

Резюме





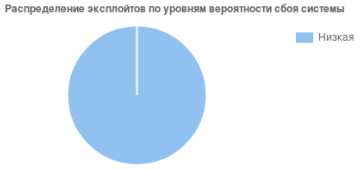


Таблица распределения уязвимостей по хостам

Хост / Уровень риска	Критичный	Высокий	Средний	Низкий	Всего
192.168.5.214	6	6	12	4	28

Анализ защищенности должен проводиться на всех ключевых этапах жизненного цикла информационных систем:

проектирование и разработка, сертификация, внедрение, аттестация, эксплуатация

В отношении значимых Объектов КИИ анализ защищенности должен проводиться регулярно

Приказ ФСТЭК России от 21.12.2017 № 235

Современная нормативная база по защите КИИ

ВИДЫ СЗИ, применяемые для обеспечения безопасности значимых объектов КИИ

Согласно Приказу ФСТЭК России №235 «**Об утверждении Требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования**» к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, относят следующие виды СЗИ:

- *средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение)*
- ***межсетевые экраны***
- ***средства обнаружения (предотвращения) вторжений (компьютерных атак)***
- *средства антивирусной защиты*
- ***средства (системы) контроля (анализа) защищённости***
- ***средства управления событиями безопасности***
- ***средства защиты каналов передачи данных***

Состав мер по обеспечению безопасности значимых объектов КИИ (приказ № 239)

Приказ ФСТЭК России №239 «**Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации**».

- Идентификация и аутентификация (ИАФ);
- **Управление доступом (УПД);** Сканер-ВС
- Ограничение программной среды (ОПС);
- **Защита машинных носителей информации (ЗНИ);** Сканер-ВС
- **Аудит безопасности (АУД);** Сканер-ВС КОМРАД
- Антивирусная защита (АВЗ);
- **Предотвращение вторжений (компьютерных атак) (СОВ);** РУБИКОН
- **Обеспечение целостности (ОЦЛ);** Сканер-ВС
- Обеспечение доступности (ОДТ);

РУБИКОН

КОМРАД

Важно: Применение решений ГК Эшелон обязательно!

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+	+	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+
ЗИС.5	Организация демилитаризованной зоны	+	+	+
ЗИС.6	Управление сетевыми потоками			
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")			

Стоимость владения

РУБИКОН + Сканер-ВС анализ защищенности + КОМРАД

СОВ – МЭ- маршрутизатор

Сканер уязвимости

SIEM-система

Малое предприятие	Среднее предприятие	Крупное предприятие
От 330 тыс.руб	От 1000 тыс.руб	От 3 900 тыс.руб

На что обратить внимание

- Правильно выбрать аппаратно-программные средства с поддержкой:
  - Аутентификации и идентификации пользователей
  - Возможность аудита и протоколирования
  - Использование лицензионного ПО, а ещё лучше сертифицированного
  - Наличие энергонезависимой памяти, чтобы не было возможности сброса к заводским настройкам при отключении питания
- Проверить наличие уязвимостей по базе данных CVE и БДУ ФСТЭК
- Проверить историю обновлений ПО у производителей
- Создать демо-стенд и провести пентест системы

Что сделать обязательно:

- Изменить дефолтные значения логин\пароль и установить взломо стойкие пароли
- Удалить лишних пользователей
- Включить аудит и протоколирование событий
- Организовать мониторинг
- Своевременно проводить обновление баз данных угроз, уязвимостей, сигнатур систем антивирусной защиты, систем обнаружения вторжений, сканеров уязвимости, а также своевременно устанавливать обновления выпускаемые производителями программных и аппаратных средств.

Эшелон

комплексная безопасность