

**Реализация требований по
обеспечению безопасности
объектов информатизации
с помощью решений
НПО «Эшелон»**

О чем пойдет Речь?

1. О компании
2. Целевая аудитория
3. Зачем используют. Нормативные требования по защите объектов информатизации
4. Комплекс анализа защищенности «Сканер-ВС»
5. Комплекс межсетевого экранирования и обнаружения вторжений «Рубикон»
6. SIEM-система «КОМРАД»
7. Партнерская политика

Группа компаний «Эшелон»



Год основания: 2007



Штат: более 180 специалистов, среди которых доктора и кандидаты наук, сертифицированные специалисты (CISSP, CISA/CISM, CISCO, CP, IBM и др.), эксперты российских и международных ИТ-сообществ



Офисы компании расположены в городах: Москва, Санкт-Петербург, Саров, Севастополь



Постоянный участник рейтингов РА-Эксперт (в TOP-50 на 2017 г.) и CNews (TOP-100 на 2018 г.) крупнейших ИТ-и ИБ-компаний



Более 50 лицензий. Компания аккредитована в качестве испытательной лаборатории (Минобороны, ФСБ, ФСТЭК России), аттестационного центра (Минобороны, ФСТЭК) и др. В компании имеется центр СИ/СП/СО и аккредитован учебный центр. Компания имеет торговую марку, патенты, сертификаты

Наши заказчики

- Органы госвласти
- Государственные ведомства
- Военно-промышленный комплекс
- Медицина
- Образование
- Финансовый сектор
- Связь



Требования по защите информации



КИИ

ГОСТАЙНА



АСУ ТП



ГИС

ИСПДн



Состав мер защиты по 17 приказу ФСТЭК (ГИС)

17 приказ ФСТЭК

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

II. Управление доступом субъектов доступа к объектам доступа (УПД)



III. Ограничение программной среды (ОПС)

IV. Защита машинных носителей информации (ЗНИ)



V. Регистрация событий безопасности (РСБ)



VI. Антивирусная защита (АВЗ)

VII. Обнаружение вторжений (СОВ)



VIII. Контроль (анализ) защищенности информации (АНЗ)



IX. Обеспечение целостности информационной системы и информации (ОЦЛ)



X. Обеспечение доступности информации (ОДТ)



XI. Защита среды виртуализации (ЗСВ)



XII. Защита технических средств (ЗТС)

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

Состав мер защиты по 21 приказу ФСТЭК (ИСПДН)

21 приказ ФСТЭК

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

II. Управление доступом субъектов доступа к объектам доступа (УПД)



III. Ограничение программной среды (ОПС)

IV. Защита машинных носителей информации (ЗНИ)



V. Регистрация событий безопасности (РСБ)



VI. Антивирусная защита (АВЗ)

VII. Обнаружение вторжений (СОВ)



VIII. Контроль (анализ) защищенности информации (АНЗ)



IX. Обеспечение целостности информационной системы и информации (ОЦЛ)



X. Обеспечение доступности информации (ОДТ)



XI. Защита среды виртуализации (ЗСВ)



XII. Защита технических средств (ЗТС)

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)



XIV. Выявление инцидентов и реагирование на них (ИНЦ)



XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)



Состав мер защиты по 31 приказу ФСТЭК (АСУ ТП)

31 приказ ФСТЭК

I. Идентификация и аутентификация (ИАФ)

II. Управление доступом (УПД)



III. Ограничение программной среды (ОПС)

IV. Защита машинных носителей информации (ЗНИ)



V. Аудит безопасности (АУД)



VI. Антивирусная защита (АВЗ)

VII. Предотвращение вторжений (компьютерных атак) (СОВ)



VIII. Обеспечение целостности (ОЦЛ)



IX. Обеспечение доступности (ОДТ)



X. Защита технических средств и систем (ЗТС)

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)



XII. Реагирование на компьютерные инциденты (ИНЦ)



XIII. Управление конфигурацией (УКФ)

XIV. Управление обновлениями программного обеспечения (ОПО)

XV. Планирование мероприятий по обеспечению безопасности (ПЛН)

XVI. Обеспечение действий в нештатных ситуациях (ДНС)

XVII. Информирование и обучение персонала (ИПО)

Состав мер защиты по 239 приказу ФСТЭК (КИИ)

239 приказ ФСТЭК

I. Идентификация и аутентификация (ИАФ)

II. Управление доступом (УПД)



III. Ограничение программной среды (ОПС)

IV. Защита машинных носителей информации (ЗНИ)



V. Аудит безопасности (АУД)



VI. Антивирусная защита (АВЗ)

VII. Предотвращение вторжений (компьютерных атак) (СОВ)



VIII. Обеспечение целостности (ОЦЛ)



IX. Обеспечение доступности (ОДТ)



X. Защита технических средств и систем (ЗТС)

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)



XII. Реагирование на компьютерные инциденты (ИНЦ)



XIII. Управление конфигурацией (УКФ)

XIV. Управление обновлениями программного обеспечения (ОПО)

XV. Планирование мероприятий по обеспечению безопасности (ПЛН)

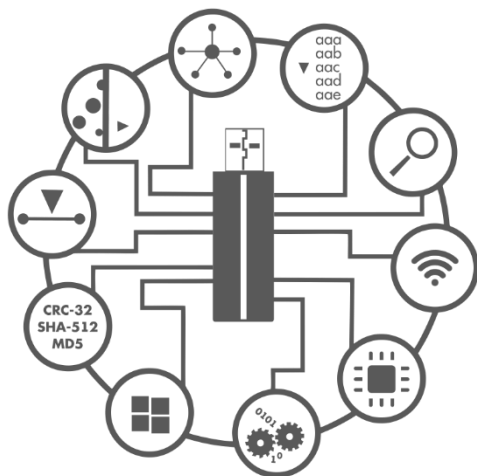
XVI. Обеспечение действий в нештатных ситуациях (ДНС)

XVII. Информирование и обучение персонала (ИПО)

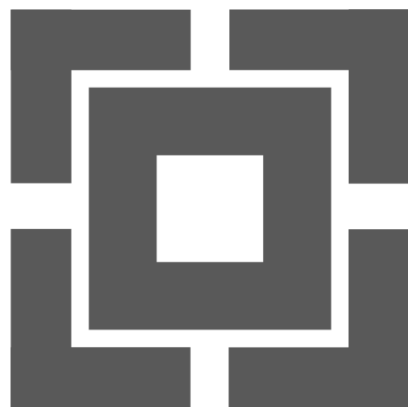
Эшелон разрабатывает набор СЗИ для обеспечения безопасности значимых объектов КИИ

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**



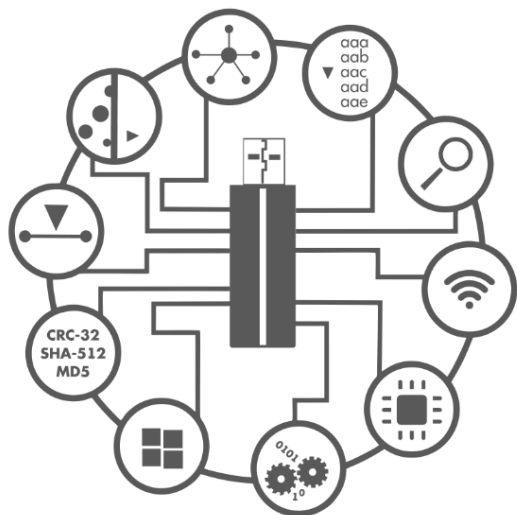
Сканер-ВС



РУБИКЕН



КОМРАД



Сканер-ВС

Универсальный инструмент для тестирования, поиска уязвимостей, анализа защищенности и контроля эффективности систем и средств защиты информации.



«Сканер-ВС» в отличие от простых сканеров позволяет провести **комплексное тестирование защищенности**

Идентификация целевых сетевых узлов

- Сбор информации о внешних ресурсах в Интернет
- Сканирование сети
- Согласование перечня с заказчиком

Поиск уязвимостей

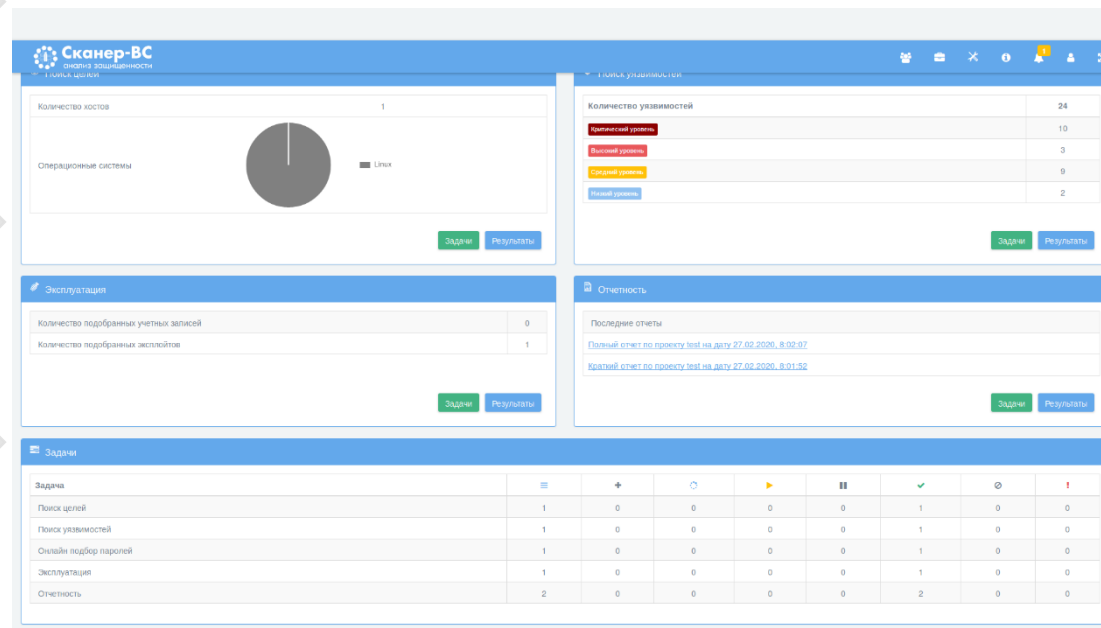
- С помощью сканеров
- Вручную (по баннерам, ошибки конфигурации)

Эксплуатация уязвимостей и проведение атак

- 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



Поиск уязвимостей после инвентаризации и определения версии и названия сервисов

Сканер-ВС
анализ защищенности

Хосты | Порты | Топология | Задачи

#	Адрес	Протокол	Порт	Состояние	Обновлено	Сервис	Продукт	Версия
1	192.168.1.10	tcp	21	открыт	27.02.2020 7:12:05	ftp	vsftpd	2.3.4
2	192.168.1.10	tcp	22	открыт	27.02.2020 7:12:05	ssh	OpenSSH	4.7p1 Debian subtree1
3	192.168.1.10	tcp	23	открыт	27.02.2020 7:12:05	telnet	-	-
4	192.168.1.10	tcp	25	открыт	27.02.2020 7:12:05	smtp	Postfix smtpd	-
5	192.168.1.10	tcp	53	открыт	27.02.2020 7:12:05	domain	ISC BIND	9.4.2
6	192.168.1.10	tcp	80	открыт	27.02.2020 7:12:05	http	Apache httpd	2.2.8
7	192.168.1.10	tcp	111	открыт	27.02.2020 7:12:05	rpcbind	-	2
8	192.168.1.10	tcp	139	открыт	27.02.2020 7:12:05	netbios-smb	Samba smb	3.X - 4.X
9	192.168.1.10	tcp	445	открыт	27.02.2020 7:12:05	netbios-ssn	Samba smbd	3.X - 4.X
10	192.168.1.10	tcp	512	открыт	27.02.2020 7:12:05	exec	netkit-rsh rexecd	-
11	192.168.1.10	tcp	513	открыт	27.02.2020 7:12:05	login	OpenBSD or Solaris rlogind	-
12	192.168.1.10	tcp	514	открыт	27.02.2020 7:12:05	shell	Netkit rshd	-
13	192.168.1.10	tcp	1099	открыт	27.02.2020 7:12:05	rmiregistry	GNU Classpath gmiiregistry	-
14	192.168.1.10	tcp	1524	открыт	27.02.2020 7:12:05	bindshell	Metasploitable root shell	-
15	192.168.1.10	tcp	2049	открыт	27.02.2020 7:12:05	rfs	-	2.4
16	192.168.1.10	tcp	2121	открыт	27.02.2020 7:12:05	ftp	ProFTPD	1.3.1
17	192.168.1.10	tcp	3306	открыт	27.02.2020 7:12:05	mysql	MySQL	5.0.51a-3ubuntu5
18	192.168.1.10	tcp	5432	открыт	27.02.2020 7:12:05	postgresql	PostgreSQL DB	8.3.0 - 8.3.7
19	192.168.1.10	tcp	5900	открыт	27.02.2020 7:12:05	vnc	VNC	-
20	192.168.1.10	tcp	6000	открыт	27.02.2020 7:12:05	X11	-	-
21	192.168.1.10	tcp	6667	открыт	27.02.2020 7:12:05	irc	UnrealIRCd	-
22	192.168.1.10	tcp	8009	открыт	27.02.2020 7:12:05	ajp13	Apache Jserv	-
23	192.168.1.10	tcp	8180	открыт	27.02.2020 7:12:05	http	Apache Tomcat/Coyote JSP engine	1.1
24	192.168.1.10	tcp	3632	открыт	27.02.2020 7:29:53	-	-	-
25	192.168.1.10	tcp	8787	открыт	27.02.2020 7:29:53	-	-	-

19	192.168.1.10	-	Этот хост установлен с GNU Bash Shell и поддержан уязвимости удаленного выполнения команд	27.02.2020 7:29:53	CVE-2014-6277	BDU-2015-09794 BDU-2015-09555 BDU-2015-09252 BDU-2015-09253 BDU-2015-09247	Критический
18	192.168.1.10	-	Этот хост установлен с GNU Bash Shell и поддержан уязвимости удаленного выполнения команд	27.02.2020 7:29:53	CVE-2014-6278	BDU-2015-09794 BDU-2015-09818 BDU-2014-00319	Критический
17	192.168.1.10	-	Этот хост установлен с GNU Bash Shell и поддержан уязвимости удаленного выполнения команд	27.02.2020 7:29:53	CVE-2014-7169	BDU-2014-00319 BDU-2015-09550 BDU-2015-00148 BDU-2015-00157 BDU-2015-09249 BDU-2015-09558 BDU-2015-06153 BDU-2015-09795 BDU-2015-09552 BDU-2015-06160 BDU-2015-09250 BDU-2015-06155 BDU-2015-09554 BDU-2015-09556 BDU-2015-09557 BDU-2015-06154 BDU-2015-06159 BDU-2015-06158 BDU-2015-06152 BDU-2015-09246 BDU-2015-00155 BDU-2015-09245 BDU-2015-09551 BDU-2015-09618 BDU-2015-06156 BDU-2015-00153 BDU-2015-00159 BDU-2015-09251 BDU-2015-06157 BDU-2015-09248 BDU-2015-09553 BDU-2015-09555 BDU-2015-00151 BDU-2015-09252 BDU-2015-09249	Критический

Задачи по анализу задаются в унифицированном формате

The image displays three overlapping screenshots of the 'Сканер-ВС' (Scanner-ВС) web interface, illustrating a unified task configuration format. Each screenshot shows a blue header with the application logo and navigation icons, and a breadcrumb trail.

- Top-left screenshot:** Shows the 'Поиск целей' (Search for targets) configuration screen. The breadcrumb trail is 'Главная / Проекты / Тестовый проект / Поиск целей / Новое сканирование'. The left sidebar has 'Базовые' (Basic) selected. The main area contains settings for scanning specific TCP/UDP ports, scan speed (set to 'Normal'), timeout, and Nmap arguments. A 'Задача' (Task) section is visible at the bottom.
- Middle screenshot:** Shows the 'Поиск уязвимостей' (Search for vulnerabilities) configuration screen. The breadcrumb trail is 'Главная / Проекты / Тестовый проект / Поиск уязвимостей / Новое сканирование'. The left sidebar has 'Базовые' selected. The main area includes 'Выявление хостов' (Host discovery), 'Сканирование портов' (Port scanning), and 'Расширенные' (Advanced) options. It also features 'Цели' (Targets) and 'Импорт из файла' (Import from file) sections.
- Bottom-right screenshot:** Shows the 'Новый подбор паролей' (New password selection) configuration screen. The breadcrumb trail is 'Главная / Проекты / Тестовый проект / Эксплуатация / Новый подбор паролей'. The left sidebar has 'Базовые' selected. The main area includes 'Пользователи' (Users), 'Пароли' (Passwords), and 'Расширенные' (Advanced) options. It features a 'Сервис' (Service) dropdown set to 'ftp', a 'Цели' (Targets) text area containing '192.168.1.100', and a file selection area.

Each screenshot includes a 'Запустить' (Run) button and an 'Отмена' (Cancel) button at the bottom.

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 ограничения, выполняются сервером без проверки полномочий.

Решение: Обновления поставщика доступны. См. Ссылки для получения дополнительной информации.

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 root.

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 Objective C и часто в два или более раза быстрее, чем локальный компилятор.

Решение: Для получения дополнительной информации о безопасности DistCC см. http://distcc.samba.org/security.html

Сканер-ВС
анализ защищенности

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

Настройки Печать

Сканер-ВС Отчёт

Показ 25-09-17

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

Резюме

Распределение хостов по операционным системам

ОС	Количество
Linux	2.0
Windows	1.0

Распределение уязвимостей по уровням риска

Уровень риска	Количество
Критический	1
Высокий	1
Средний	1
Низкий	1
Заметка	1

Распределение паролей по уровням стойкости

Уровень стойкости	Количество
Очень слабый	1
Слабый	1

Распределение эксплойтов по уровням вероятности сбоя системы

Уровень вероятности сбоя системы	Количество
Низкая	1

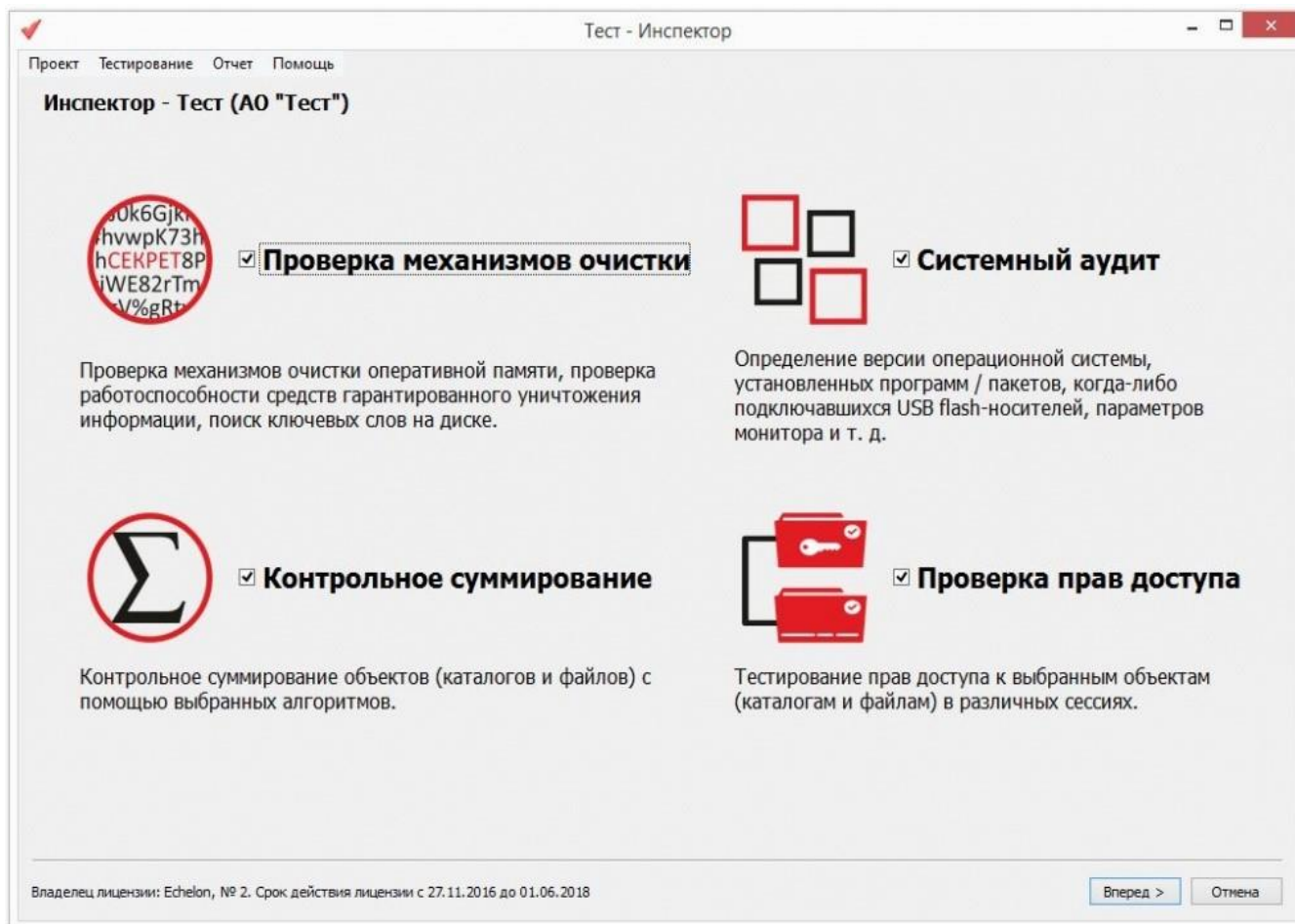
Таблица распределения уязвимостей по хостам

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

Инструменты для # продвинутых сисадминов

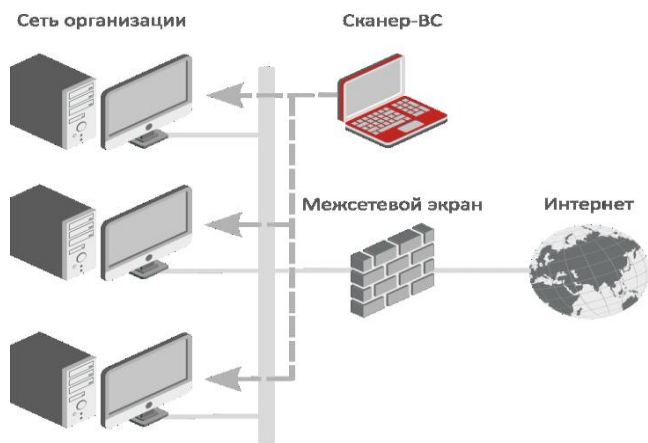
- Сбор информации
- Поиск уязвимостей
- Анализ веб-приложений
- Анализ баз данных
- Атаки на пароли
- Аудит беспроводных сетей
- Реверс-инжиниринг
- Эксплуатация уязвимостей
- Сниффинг и спуффинг
- Пост-эксплуатация
- Форензика
- Генерация отчетов
- Социальная инженерия
- Управление сервисами
- Аудит ОС Astra Linux
- Аудит обновлений Windows
- Аудит беспроводных сетей
- Локальный аудит паролей
- Системный аудитор
- Сетевой анализатор
- Поиск остаточной информации
- Гарантированное уничтожение информации
- Контрольное суммирование

Средство проведения комплексных проверок «Инспектор»

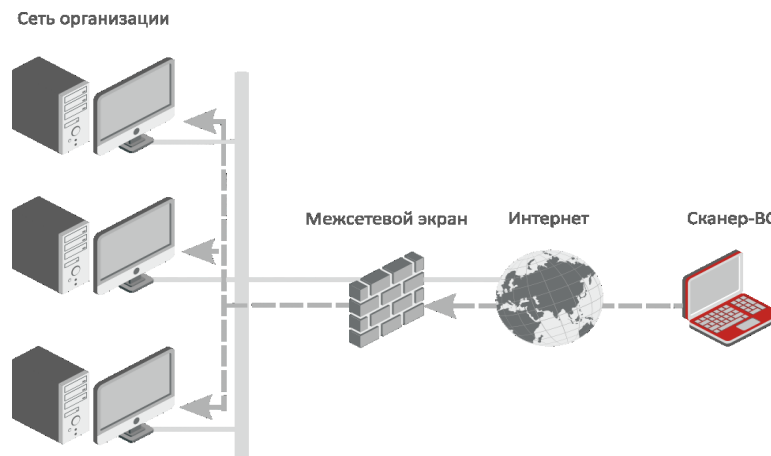


- Автоматизированный процесс проверки отдельных требований нормативных документов
- Возможность сбора подробной информации об автоматизированной (информационной) системе (номера лицензий на некоторые виды ПО, идентификаторы подключающихся внешних носителей и др.)

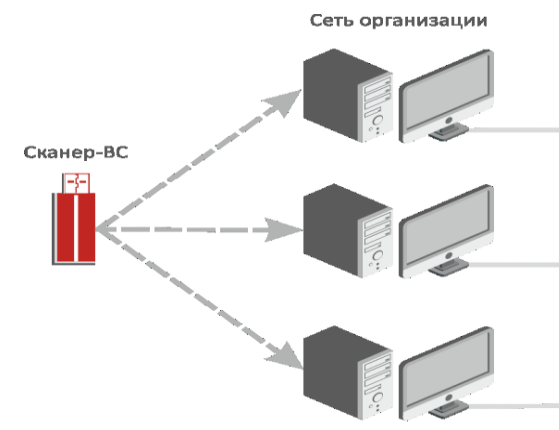
Сценарии применения «Сканер-ВС»



Внутреннее
тестирование защищенности



Внешнее
тестирование защищенности



Тестирование защищенности
выделенных сегментов

«Сканер-ВС» сертифицирован ФСТЭК России и Минобороны России



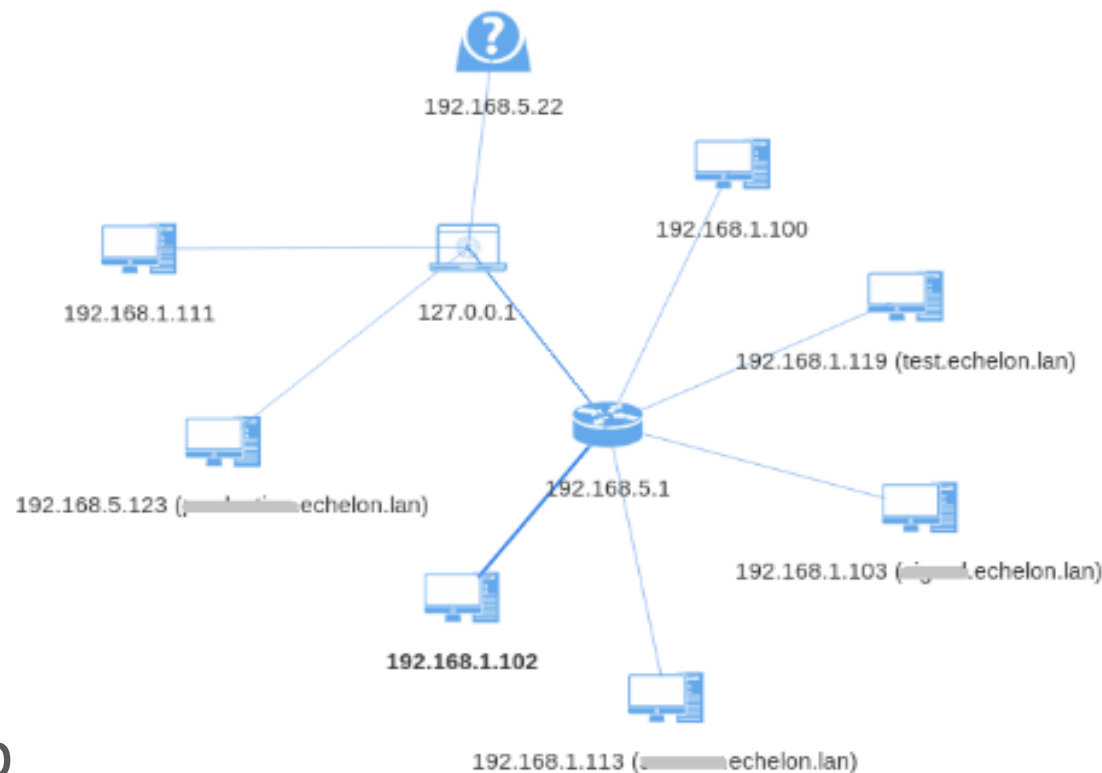
ФСТЭК России №2204
(4 уровень доверия)



Минобороны России №3872
(НДВ-2, РДВ)

Преимущества

- Нет лицензионной привязки к IP-адресам (при смене IP-адреса не нужно обновлять лицензии)
- Построение топологии сети
- Расписание сканирований
- Установка на жесткий диск
- Новая подсистема отчетов (экспорт в форматы HTML, PDF, RTF, XML)



СТОИМОСТЬ

Количество IP адресов + Техподдержка 1 год	Сканер-ВС	Простой сетевой сканер
4 IP-адреса на 1 год	5 000,00	14 000
8 IP-адресов на 1 год	10 000,00	23 400
16 IP-адресов на 1 год	20 000,00	35 000
32 IP-адреса на 1 год	35 000,00	50 400
64 IP-адреса на 1 год	50 000,00	71 000
128 IP-адресов на 1 год	80 000,00	96 700
256 IP-адресов на 1 год	100 000,00	119 600
512 IP-адресов на 1 год	150 000,00	219 000
1024 IP-адреса на 1 год	270 000,00	378 000
без ограничения IP-адресов на 1 год	800 000,00	Не предоставляется

Разработка нового «СКАНЕР-ВС» 6.0 (Релиз в 2020)

- Масштабирование
- Высокая скорость обнаружения уязвимостей
- Кросс-платформенность (Windows\Linux)
- Централизованное управление
- Анализ конфигураций

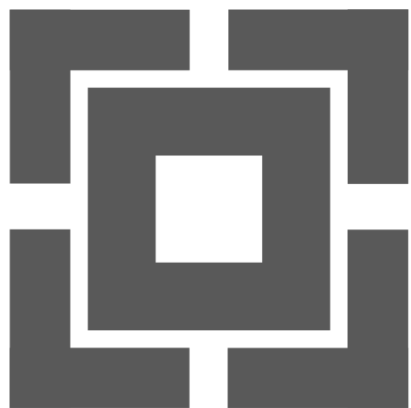
The screenshot displays the configuration interface for a network scanning task. At the top, there are navigation tabs: '< Тип задачи', 'Общие', 'Расширенные', 'Расписание', 'Уведомления', and 'Отчет'. The 'Общие' (General) tab is selected.

The main section is titled 'Исследование сети' (Network Research). It contains the following fields and controls:

- Исследование сети**: Section header.
- Название задачи**: A text input field.
- Цели**: A text area containing the following IP ranges and a tag: 192.168.1.100, 192.168.1.1-100, 192.168.1.100-192.168.1.200, 192.168.1.0/24, #метка. To the right of this field is a button labeled 'Импорт из активов' (Import from assets).
- Обнаружение хостов**: A toggle switch, currently turned off.
- Сканирование портов**: A toggle switch, currently turned off.
- Определение сервисов**: A toggle switch, currently turned off.
- Определение ОС**: A toggle switch, currently turned off.
- Трассировка для карты**: A toggle switch, currently turned off.

At the bottom of the configuration area, there are two buttons: 'Сохранить' (Save) and 'Запустить' (Run).

МЭ и СОВ в одном устройстве



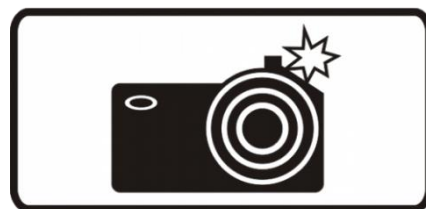
РУБИКОН

Предназначен для организации эффективной защиты периметра сетей предприятий различного масштаба в соответствии с нормативными требованиями регуляторов.

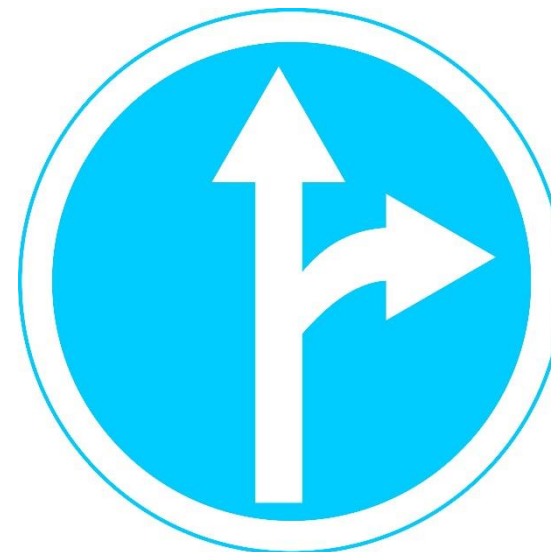
ФУНКЦИОНАЛ АПК «РУБИКОН»



МЕЖСЕТЕВОЙ ЭКРАН



СИСТЕМА
ОБНАРУЖЕНИЯ
ВТОРЖЕНИЙ









МАРШРУТИЗАТОР

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Производительность МЭ: до 9Gb/s
- Производительность COB: до 3Gb/s
- Производительность маршрутизации: до 9 Gb/s
- Возможность горячего резервирования: на уровне устройств (VRRP, Ethernet Bypass), на уровне портов (VLAN bonding), на уровне каналов связи (динамическая маршрутизация OSPF)
- Поддержка мандатных меток отечественных защищенных операционных систем в сетевом трафике
- Возможность интеграции с SIEM-системами
- Модульная структура аппаратных платформ
- Возможность конфигурации до 64 портов в одном комплексе
- Не требует узкоспециализированных технических специалистов
- BGP для динамической маршрутизации

Варианты исполнений Пак «рубикон»

Форм-фактор	Производительность МЭ	Производительность СОВ	Сетевые интерфейсы	Последовательные интерфейсы	ОЗУ	Питание	Дополнения	Решение
МИНИ 	до 2 Gbit/s	до 1,6 Gbit/s	6xRJ45 10/100/1000	2xUSB, 1xConsole	4-86 GB	40W 12V	нет	«Рубикон» «Рубикон-А» «Рубикон-К»
ЗАЩИЩЕННЫЙ (4 порта) 	до 600 Mbit/s	до 400 Mbit/s	4xEthernet 100/1000 Base-T	2xUSB, 1xVGA	8 GB	220V	нет	«Рубикон»
ЗАЩИЩЕННЫЙ (10 портов) 	до 600 Mbit/s	до 400 Mbit/s	10xGbe Ethernet 10/100/1000 M12	2xRS-232/422/485, 2xRS-232, 2xUSB 3.0, 2xUSB 2.0 (M12) 2xHDMI, 1xVGA	8 GB	24V	нет	«Рубикон»
1U 	до 5 Gbit/s	до 3 Gbit/s	6xRJ45 10/100/1000 (+1 модуль расширения)	2xUSB, 1xConsole	8-16 GB	220W 220V	4xRJ45, 8xRJ45 4xSFP, 8xSFP 4xSFP+	«Рубикон» «Рубикон-А» «Рубикон-К» «Рубикон-ОШ»
ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ 	до 9 Gbit/s	до 3 Gbit/s	4 модуля расширения	2xUSB, 1xConsole	8-64 GB	300W 220V	4xRJ45, 8xRJ45 4xSFP, 8xSFP 4xSFP+	«Рубикон» «Рубикон-А» «Рубикон-К»
МУЛЬТИПОРТОВЫЙ 	до 6 Gbit/s	до 2.5 Gbit/s	8 модулей расширения	2xUSB, 1xConsole	8-128 GB	600W 220V	4xRJ45, 8xRJ45 4xSFP, 8xSFP 4xSFP+	«Рубикон» «Рубикон-А» «Рубикон-К»



Рубикон Рубикон-А



Рубикон-К

Сертификаты соответствия

Рубикон-К



ФСТЭК России №3290: ИТ.МЭ.А4.ПЗ,
ИТ.МЭ.Б4.ПЗ, ИТ.СОВ.С4.ПЗ

Рубикон-А



ФСТЭК России №2574: ИТ.МЭ.А2.ПЗ,
ИТ.СОВ.С2.ПЗ.

Рубикон



Минобороны России №3168

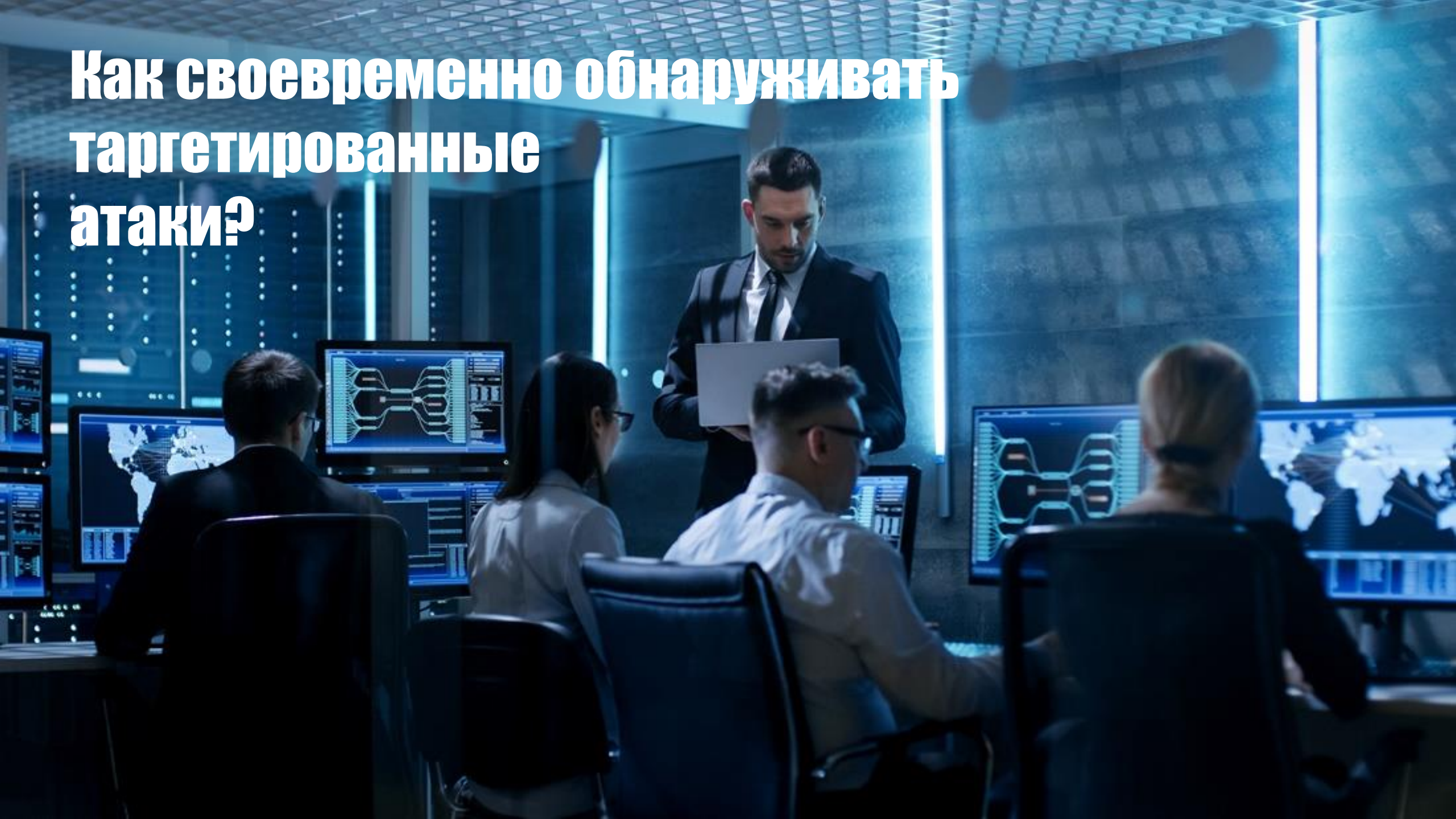
SIEM-система КОМРАД



КОМРАД

Гибкая и масштабируемая система централизованного управления событиями информационной безопасности, поддерживающая широкий спектр отечественных средств защиты информации.

Как своевременно обнаруживать таргетированные атаки?




```

vmware - Notepad
File Edit Format View Help
Apr 27 09:55:34: vmx| Log for VMware workstation pid=2548 version=5.1
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\VMware\VMware v
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 Genunteline1
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 id
Apr 27 09:55:34: vmx| pcpu #1 CPUID numEntries=5 Genunteline1
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 id
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 Professio
Apr 27 09:55:34: vmx| VMXvmbDbvMmxExecState: 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 0x000000000000
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

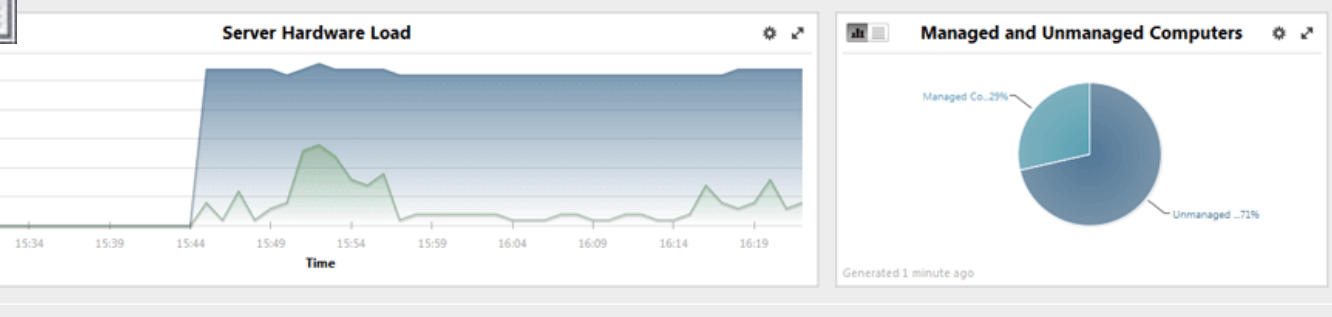
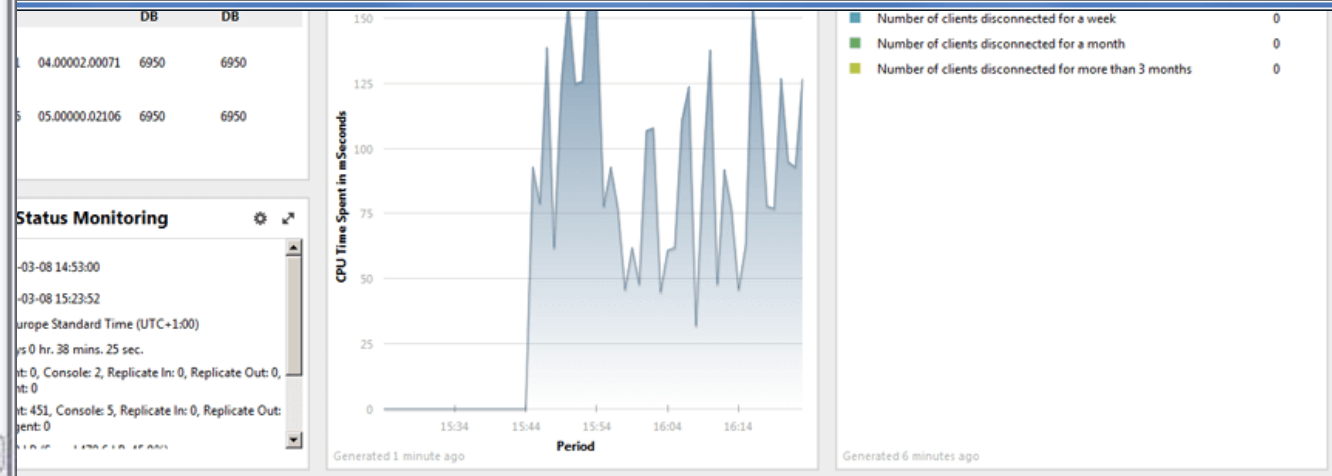
```

```

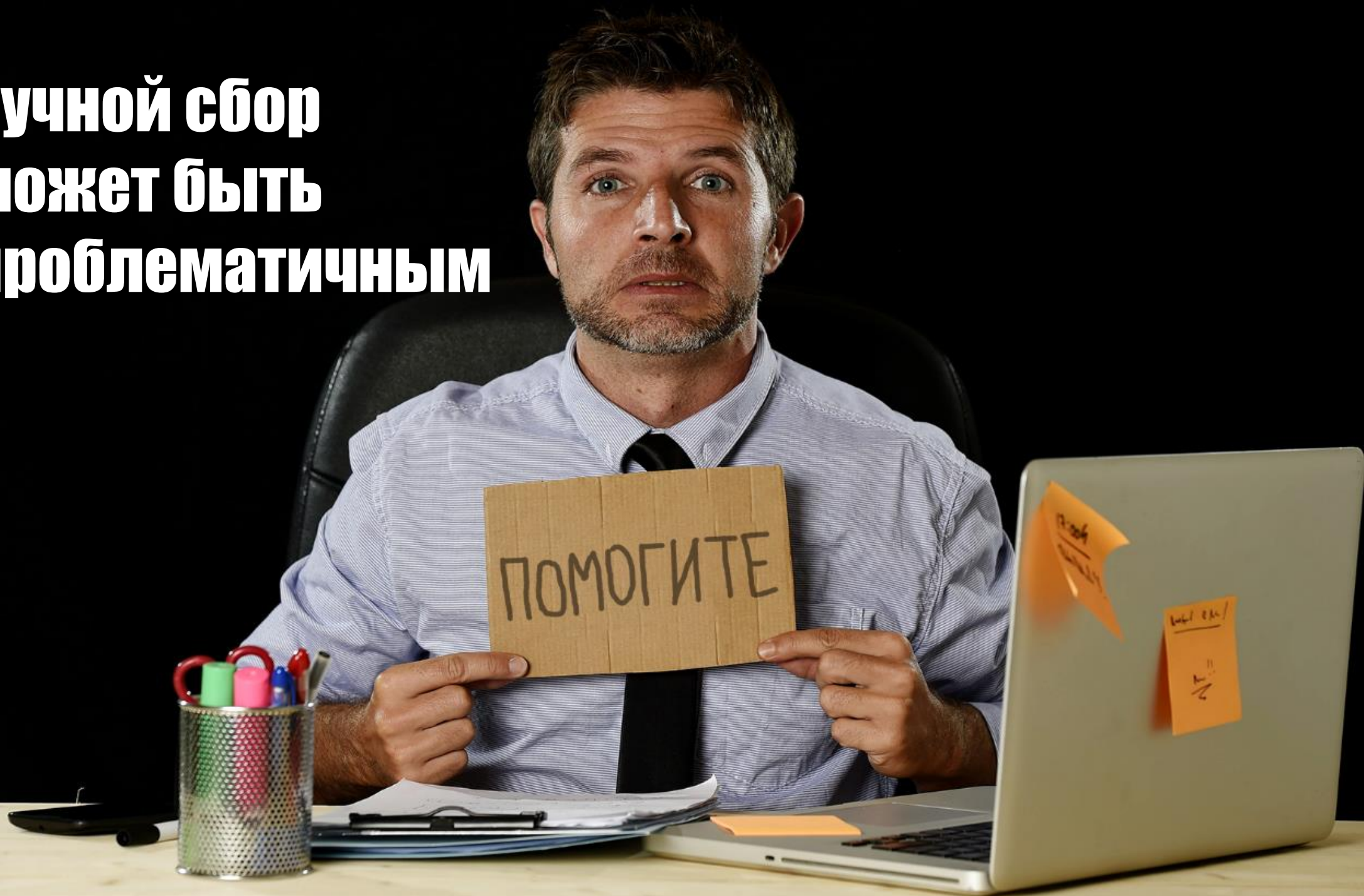
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozilla/5.0
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200 431 "ht
Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200 509 "ht
Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 513 "ht
Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500 "-" "M
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "http://lo
"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 499 "ht
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200 817 "ht
01 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
o/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"

```

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...



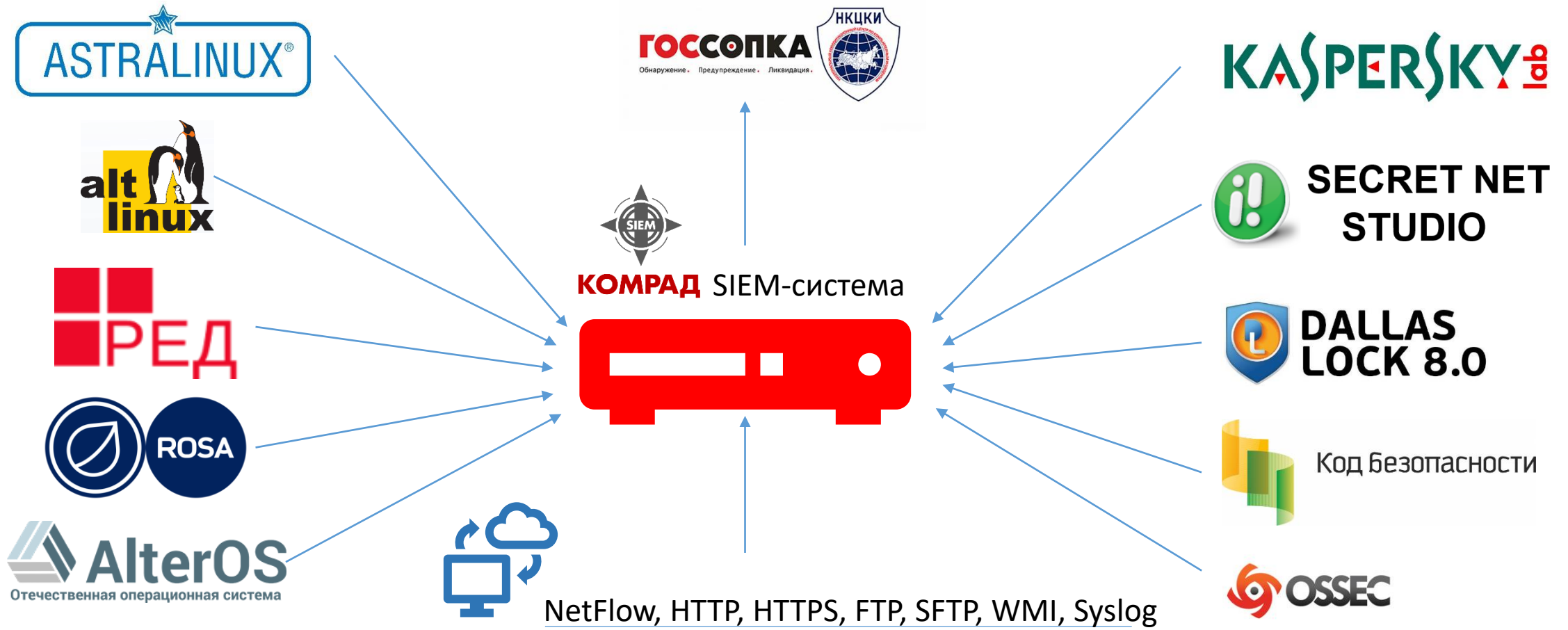
Ручной сбор может быть проблематичным



Категории и типы инцидентов на которые надо реагировать

Категория инцидента	Типы инцидентов
Внедрение вредоносного ПО	Заражение ВПО
Распространение вредоносного ПО	<ul style="list-style-type: none">• Использование контролируемого ресурса для распространения или управления модулями ВПО• Попытки внедрения модулей ВПО
Нарушение или замедление работы контролируемого информационного ресурса	<ul style="list-style-type: none">• Компьютерная атака типа «отказ в обслуживании»• Распределенная компьютерная атака типа «отказ в обслуживании»• Контролируемый несанкционированный вывод системы из строя• Контролируемое отключение системы (без злого умысла)
НСД в систему	<ul style="list-style-type: none">• Успешная эксплуатация уязвимости• Компрометация учетной записи
Попытки НСД в систему или к информации	<ul style="list-style-type: none">• Попытки эксплуатации уязвимости• Попытки авторизации в информационном ресурсе
Сбор сведений с использованием информационно-коммуникационных технологий	<ul style="list-style-type: none">• Сканирование информационного ресурса• Прослушивание (захват) сетевого трафика• Социальная инженерия
Нарушение безопасности информации	<ul style="list-style-type: none">• Несанкционированное разглашение информации• Несанкционированное изменение информации
Распространение информации с неприемлемым содержанием	<ul style="list-style-type: none">• Рассылка незапрашиваемых электронных сообщений• Публикация запрещенной законодательством РФ информации
Мошенничество с использованием информационно-коммуникационных технологий	<ul style="list-style-type: none">• Злоупотребление при использовании информационного ресурса• Публикация мошеннического информационного ресурса
Наличие уязвимости или недостатков конфигурации в информационном ресурсе	<ul style="list-style-type: none">• Наличие уязвимости или недостатков конфигурации в информационном ресурсе

Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов



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»

ASTRA  **LINUX**



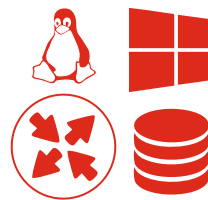
Отличительные возможности



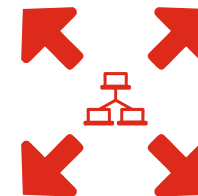
Высокая
производительность



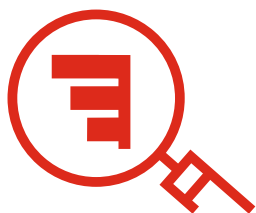
Универсальный
адаптер для любого
источника событий



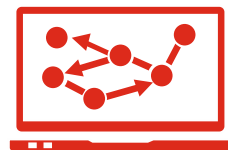
Широкий спектр
поддерживаемых
источников событий



Масштабирование



Визуальный конструктор
запросов и директив
корреляции



Визуальный анализ
данных



Оперативное оповещение
об инциденте



Ролевая модель
управления доступом

Основные преимущества

- Отсутствуют лицензионные ограничения по количеству источников событий/производительности
- Поддержка основных источников событий (в особенности отечественных СЗИ)
- Интуитивно-понятный интерфейс
- Самый доступный сертифицированный SIEM на российском рынке решений по информационной безопасности
- Масштабируемость

Инструменты SIEM Комрад: Конструктор директив

The screenshot displays the 'Конструктор директив' (Rule Builder) interface of the Komrad SIEM system. The interface is divided into three main sections:

- Left Panel (Directory Tree):** A tree view showing the installed rules. The root is 'Предустановленные' (Pre-installed), followed by 'KAV', 'Dallas Lock', 'Континент' (Continent), 'Рубикон' (Rubicon), and 'Linux'. Each category contains a list of specific rule names, such as 'Не установлено антивирусное ПО' under KAV and 'Ошибка PAM аутентификации' under Linux.
- Top Bar:** Contains the 'КОМРАД' logo, the user name 'admin', and a notification badge with the number '463'. Action buttons for 'Экспорт...' (Export), 'Импорт...' (Import), 'Сохранить директиву' (Save rule), and 'Возобновить' (Refresh) are also present.
- Right Panel (Rule Configuration):** Shows three active rule configuration windows, each with a title bar indicating the rule name and its trigger interval (e.g., 'Правило #0', '60 Секунды').
 - Правило #0:** Configured with a trigger interval of 60 seconds and a count of 3. It features a single condition: 'Тип сообщения' (Message type) is 'равно' (equal) to 'sshd' with the message content 'SSHd: Failed password'. A search field for 'Имя пользователя' (Username) is visible below the condition.
 - Правило #1:** Configured with a trigger interval of 60 seconds and a count of 1. It has two conditions: 'Тип сообщения' is 'равно' to 'sshd' with message content 'SSHd: Login successful, Acco...', and 'Имя пользователя' is 'равно' to 'Имя пользователя' with a dropdown for 'Правило #0'.
 - Правило #2:** Configured with a trigger interval of 1 second and a count of 1. It has two conditions: 'Имя пользователя' is 'не пусто' (not empty), and 'Имя источника' (Source name) is 'равно' to 'Имя источника' with a dropdown for 'Правило #1'.

Инструменты SIEM КОМРАД: Инциденты

admin

Инциденты

4

2

И или + Добавить Добавить

№ больше 0

Поиск Всего найдено: 876

Отметить как Удалить

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

Имя директивы	Всего
Brute(Uc)	9
Попытка входа на webui Dlink	19
Brute(Scanner)	21
Storage in not online	3
Рубикон Срабатывание правил COB (+PCAP)	48
KAV Базы устарели	53
KAV Срабатывание защиты	37
Dallas Lock Нарушение целостности реестра	2
AstraLinux Ошибка аутентификации	21
Рубикон Срабатывание правила COB	253
Рубикон Ошибка контрольной суммы	1
Рубикон Срабатывание правила МЭ	98
Windows Server Ошибка аутентификации	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

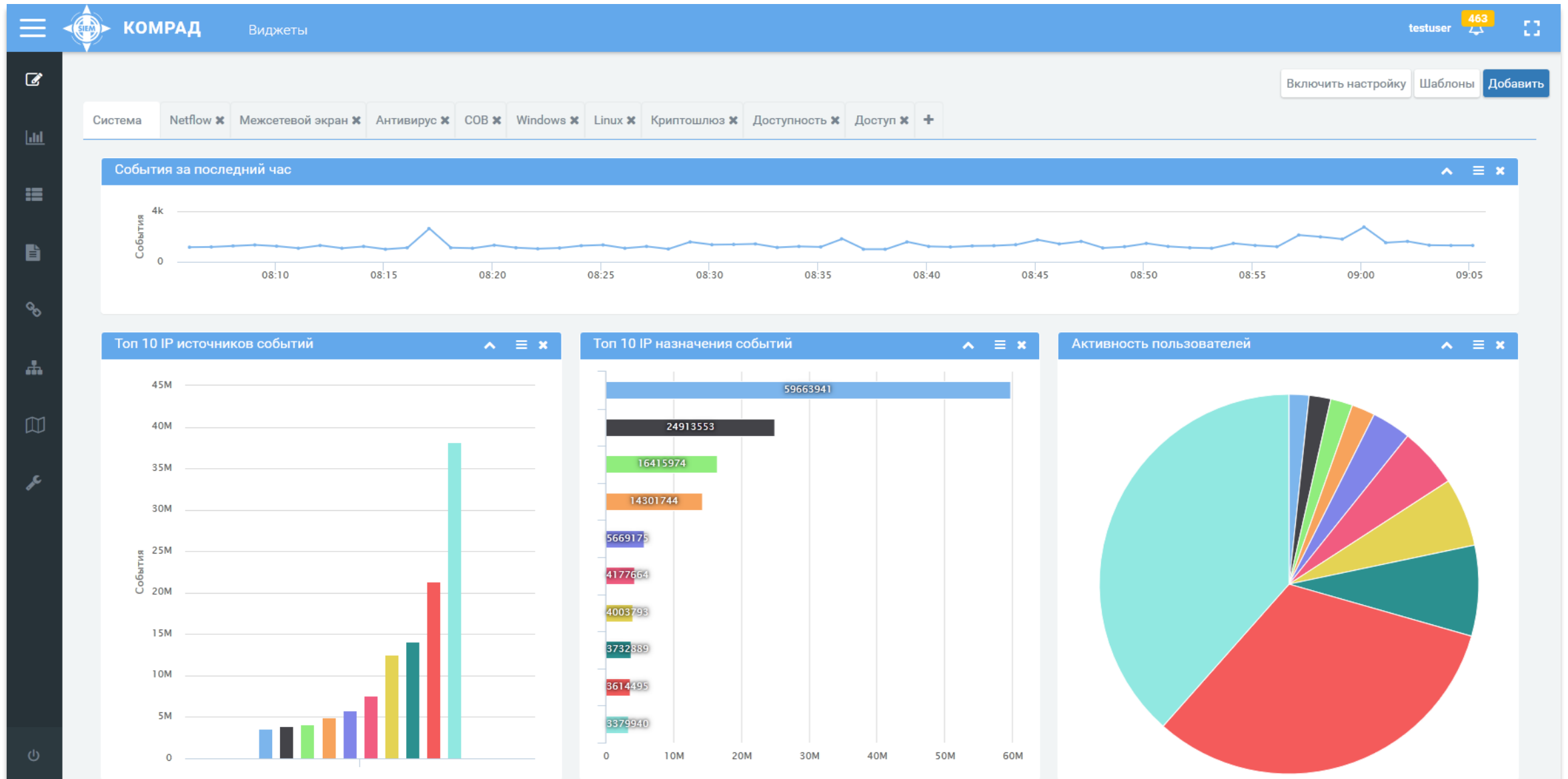
Открытые 462

Просмотренные 156


Закрытые 258

Поиск...

Инструменты SIEM КОМРАД: Виджеты и диаграммы



Инструменты SIEM КОМРАД: поиск по событиям

☰  КОМРАД ? 🔔 4 🗄

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:

Описание:

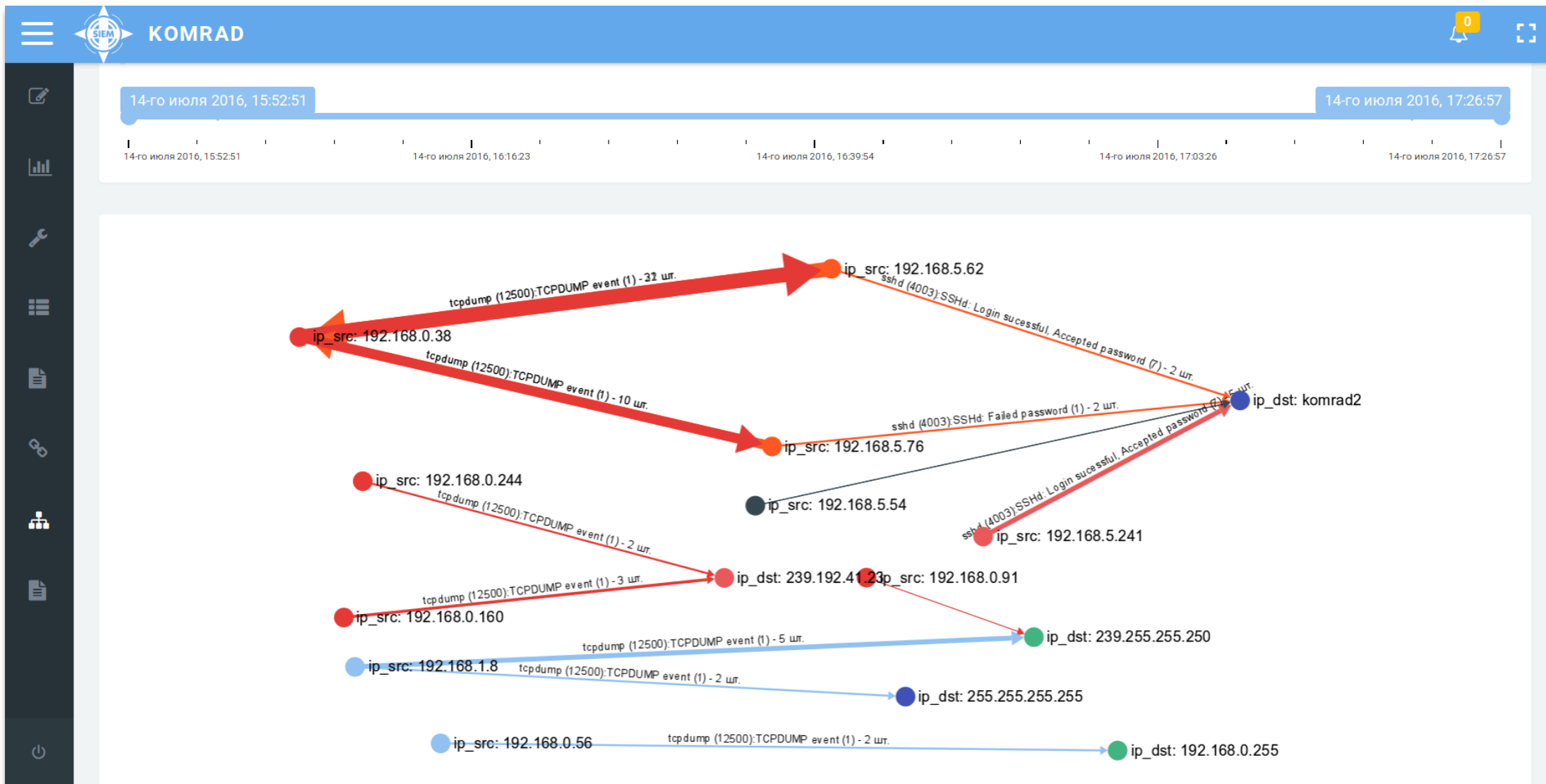
и или + Добавить + Добавить группу

✖ Удалить

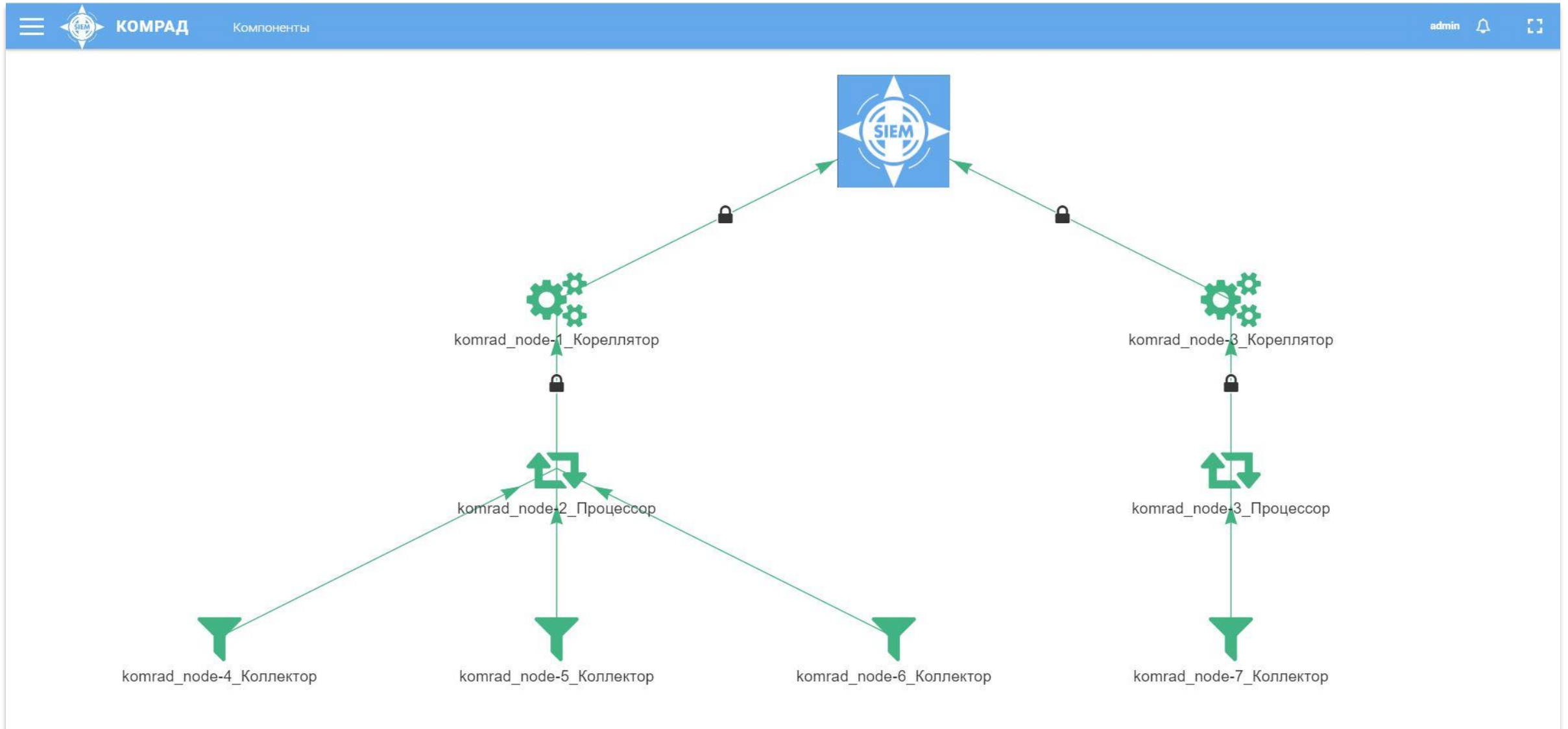
Поиск Всего найдено: 13306 От: 29. авг 2016, 14:59:11 До: 29. авг 2016, 15:30:28

№ 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



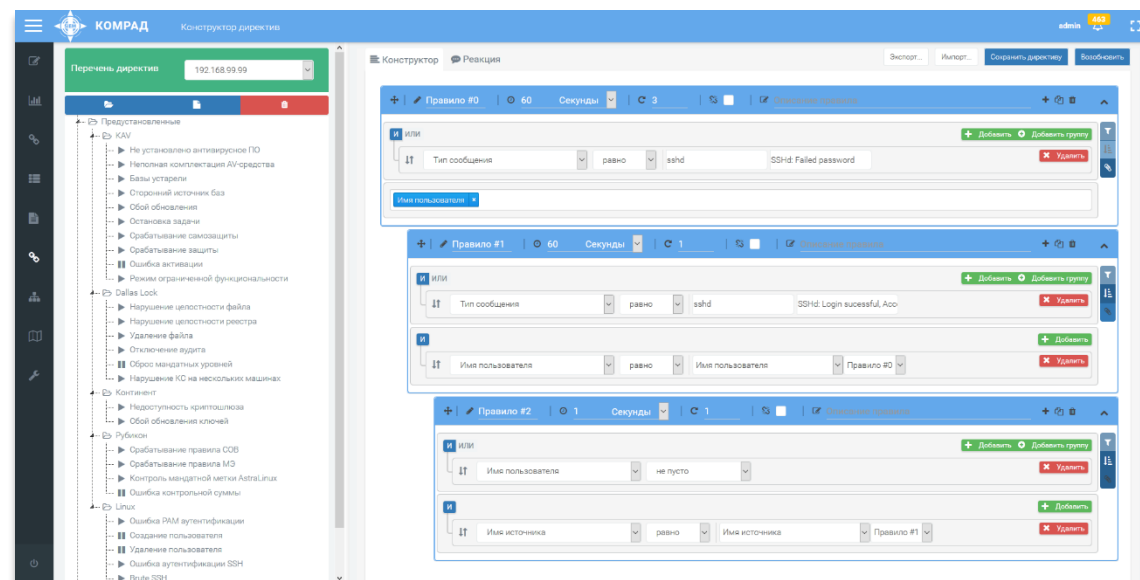
КОМРАД: возможности масштабирования



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 блокировки 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

Сертификаты соответствия



ФСТЭК России №3498 НДВ-2, РДВ



Минобороны России №3899 НДВ-4, ТУ

Варианты поставки

Показатель	BASE	ALL-IN-ONE	ENTERPRISE
Количество коллекторов	1	1	2
Количество EPS\сек.	до 2500	до 2500	«неограниченно»
Сбор и фильтрация событий	✓	✓	✓
Хранение событий	✓	✓	✓
Поиск по событиям	✓	✓	✓
Корреляция	✓	✓	✓
Веб-интерфейс	✓	✓	✓
Поддерживаемые типы источников:			
- syslog, ossec	✓	✓	✓
- WMI		✓	✓
- SNMP		✓	✓
- SSH		✓	✓
- NetFlow			✓
Масштабируемость			✓
Стоимость	210.000	910.000	1.710.000

Новое в комрад 4.0 (Релиз в 2020)

- Кроссплатформенность (Windows\Linux)
- Высокая скорость обработки событий (несколько десятков тысяч EPS)
- Большое количество источников событий

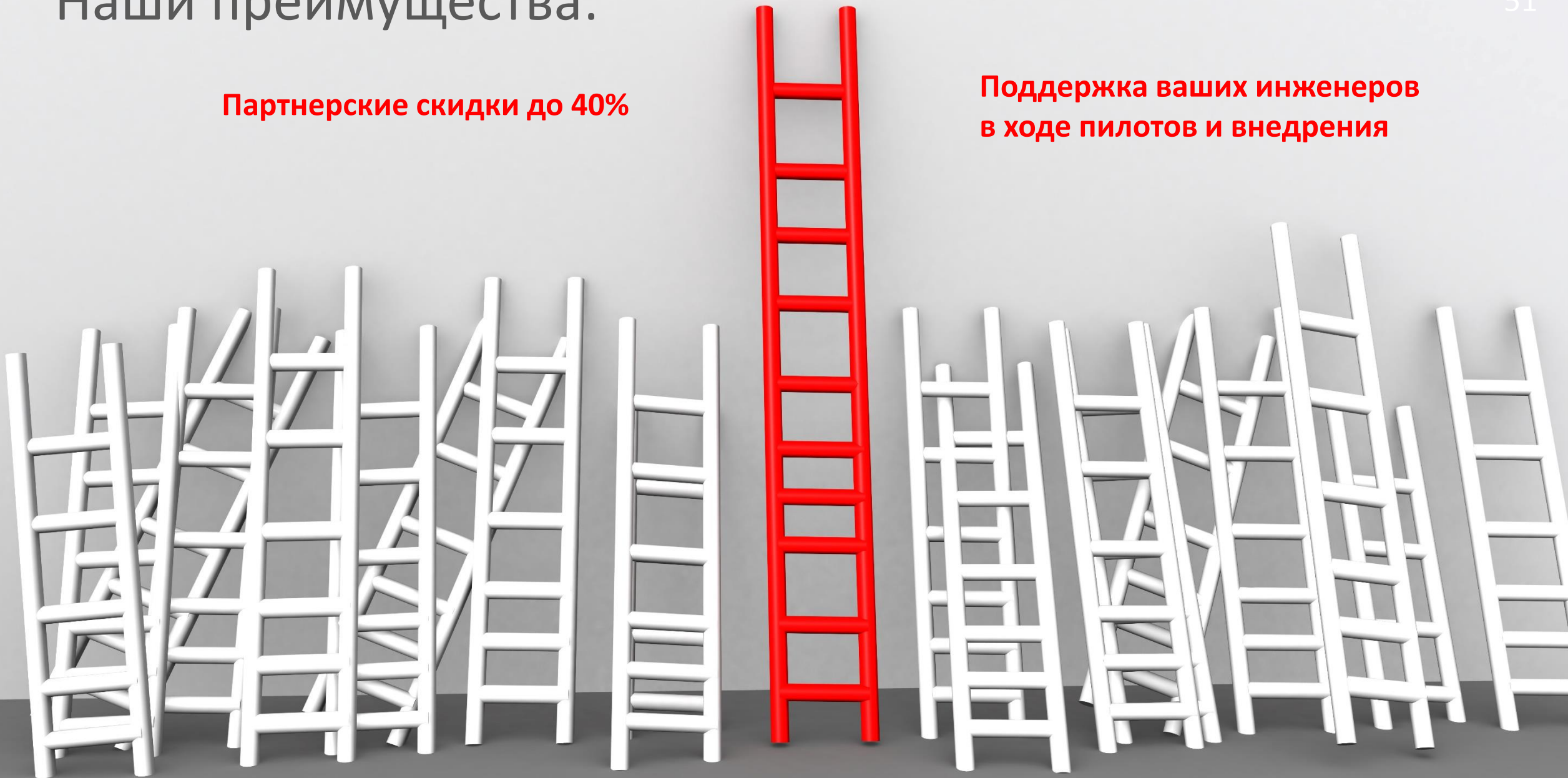


Как можно с нами
заработать?

Наши преимущества:

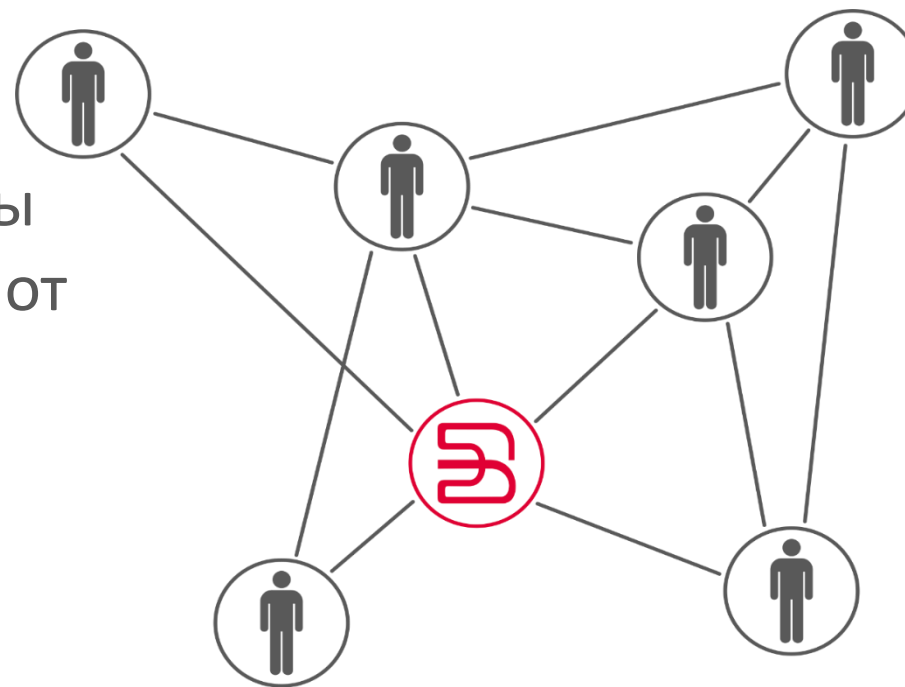
Партнерские скидки до 40%

**Поддержка ваших инженеров
в ходе пилотов и внедрения**



Партнерская стратегия

- Технический консалтинг – сопровождение в проектах (демо-стенды, проведение пилотных проектов, подготовка ТЗ, подготовка решений)
- Защита инвестиций партнеров в проекты
- Маркетинговая поддержка независимо от статуса
- Маркетинговые материалы, участие в мероприятиях партнеров, вебинары
- Персональный менеджер по работе с партнером (предоставление ТКП, презентации, выезд менеджеров к Заказчику)



Возможности для продвижения

- Развертывания пилота у партнера: дадим полноценные версии, поможем развернуть;
- Проведение вебинара для заказчиков партнера;
- Проведение пилотирования у заказчика партнера дистанционно под флагом партнера;
- Предоставление печатных материалов (буклетов) и дополнительной информации (сравнения и т.п.);
- Написание совместных пресс-релизов и т.п.

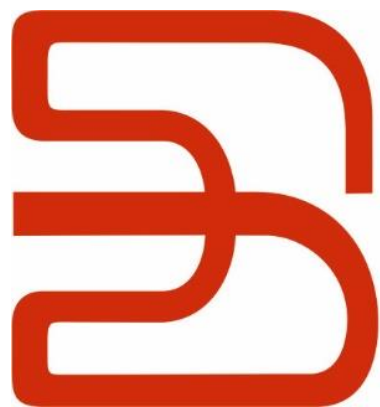
Поддержка продаж

- Предоставление лицензий для организации демо-стенда для показа заказчикам (виртуальные машины)
 - «Сканер-ВС Инспектор» на 64 IP-адреса
 - «КОМРАД» Enterprise
 - «Рубикон»
- Предоставление промо-стойки с буклетами
- После успешного совместного внедрения SIEM «КОМРАД» – выдача сертификата о прохождении обучения



Теперь Вопросы!





Эшелон

комплексная безопасность

+7 (495) 223-23-92

E-mail: partners@npo-echelon.ru