Эшелон
комплексная безопасность

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 ТОР-50 на 2017 г.) и CNews (ТОР-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

ГИС

АСУ ТП

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)	Сканер-ВС, РУБИКОН
	III. Ограничение программной среды (ОПС)	
	IV. Защита машинных носителей информации (ЗНИ)	Сканер-ВС
	V. Регистрация событий безопасности (РСБ)	РУБИКОН, КОМРАД
	VI. Антивирусная защита (АВЗ)	
	VII. Обнаружение вторжений (СОВ)	РУБИКОН
	VIII. Контроль (анализ) защищенности информации (АНЗ)	Сканер-ВС
	IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	Сканер-ВС
	X. Обеспечение доступности информации (ОДТ)	РУБИКОН, КОМРАД
	XI. Защита среды виртуализации (ЗСВ)	РУБИКОН
	XII. Защита технических средств (ЗТС)	
	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	РУБИКОН
	XIV. Выявление инцидентов и реагирование на них (ИНЦ)	РУБИКОН, КОМРАД
	XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)	КОМРАД

Состав мер защиты по 31 приказу ФСТЭК (АСУ ТП)

31 приказ ФСТЭК		
	I. Идентификация и аутентификация (ИАФ)	
	II. Управление доступом (УПД)	Сканер-ВС, РУБИКОН
	III. Ограничение программной среды (ОПС)	
	IV. Защита машинных носителей информации (ЗНИ)	Сканер-ВС
	V. Аудит безопасности (АУД)	Сканер-ВС, РУБИКОН, КОМРАД
	VI. Антивирусная защита (АВЗ)	
	VII. Предотвращение вторжений (компьютерных атак) (СОВ)	РУБИКОН
	VIII. Обеспечение целостности (ОЦЛ)	Сканер-ВС, РУБИКОН
	IX. Обеспечение доступности (ОДТ)	РУБИКОН, КОМРАД
	X. Защита технических средств и систем (ЗТС)	
	XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	РУБИКОН
	XII. Реагирование на компьютерные инциденты (ИНЦ)	РУБИКОН, КОМРАД
	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

РУБИКОН

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

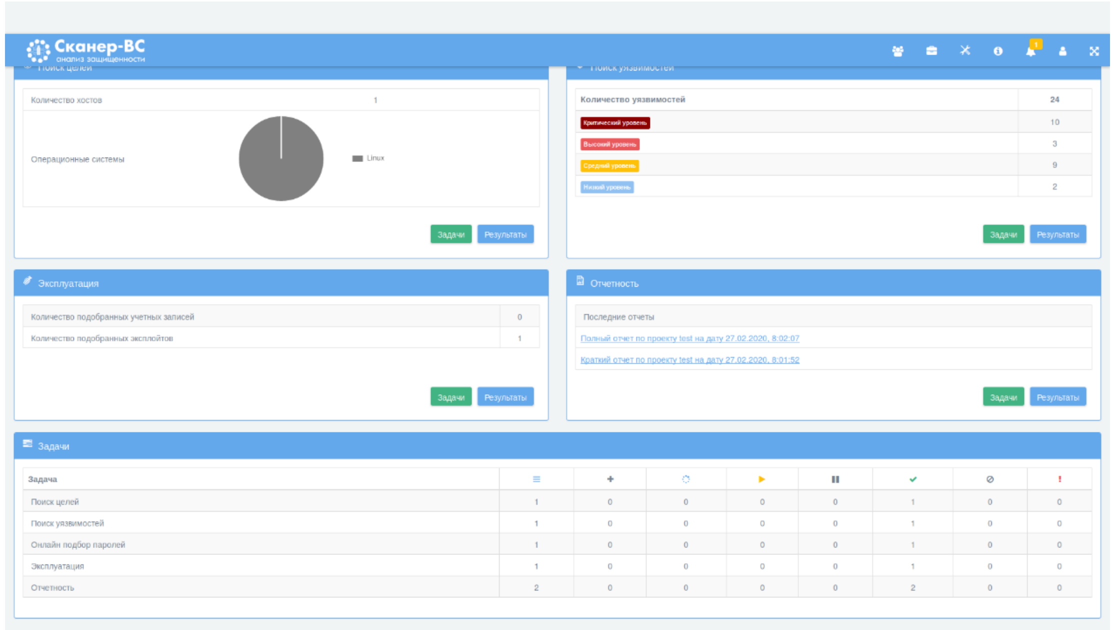
- С помощью сканеров
- Вручную (по баннерам, ошибки конфигурации)

Эксплуатация уязвимостей и проведение атак

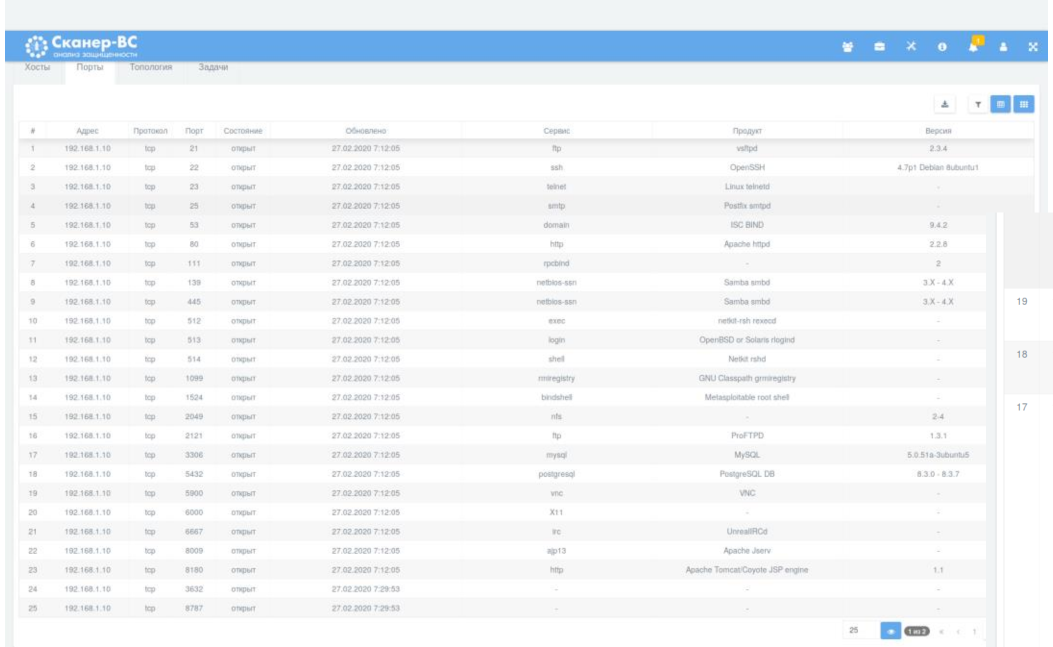
- Подбор паролей
- Перехват трафика
- Запуск эксплойтов
- и т.д.

Расширение привилегий и зоны влияния

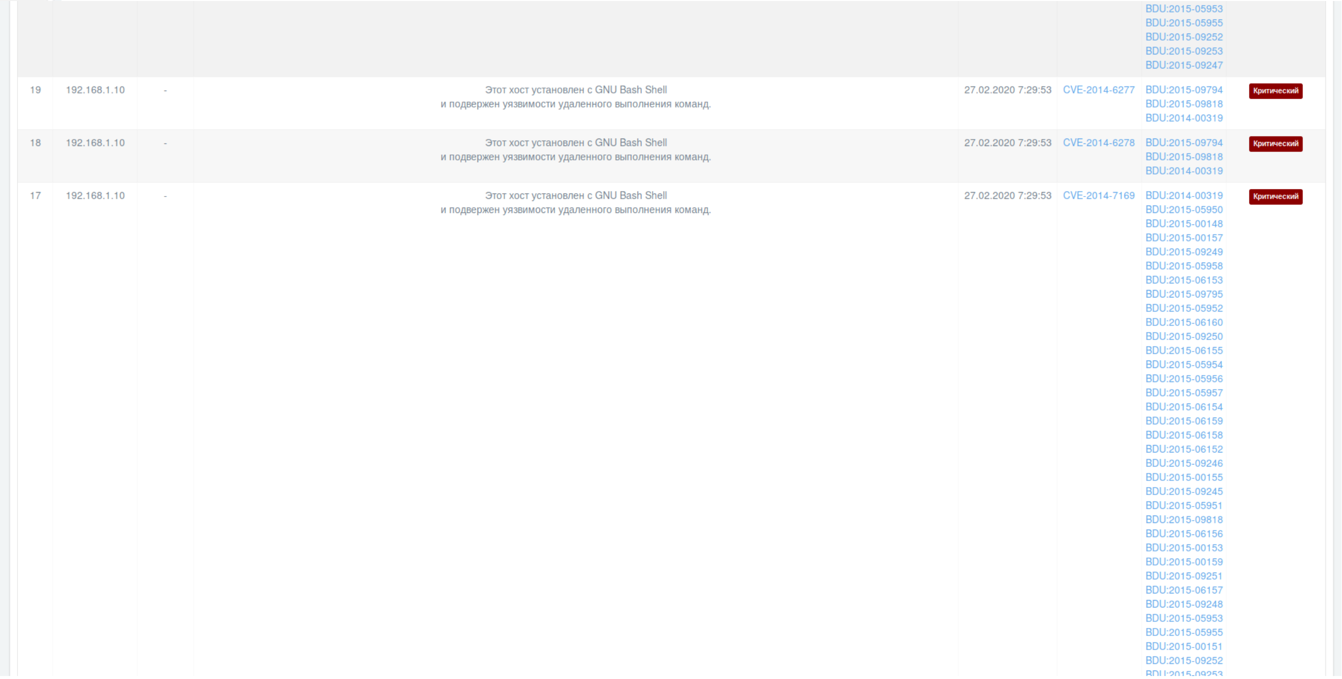
- Запуск локальных эксплойтов
- Использование собранной информации для доступа к другим системам



Поиск уязвимостей после инвентаризации и определения версии и названия сервисов

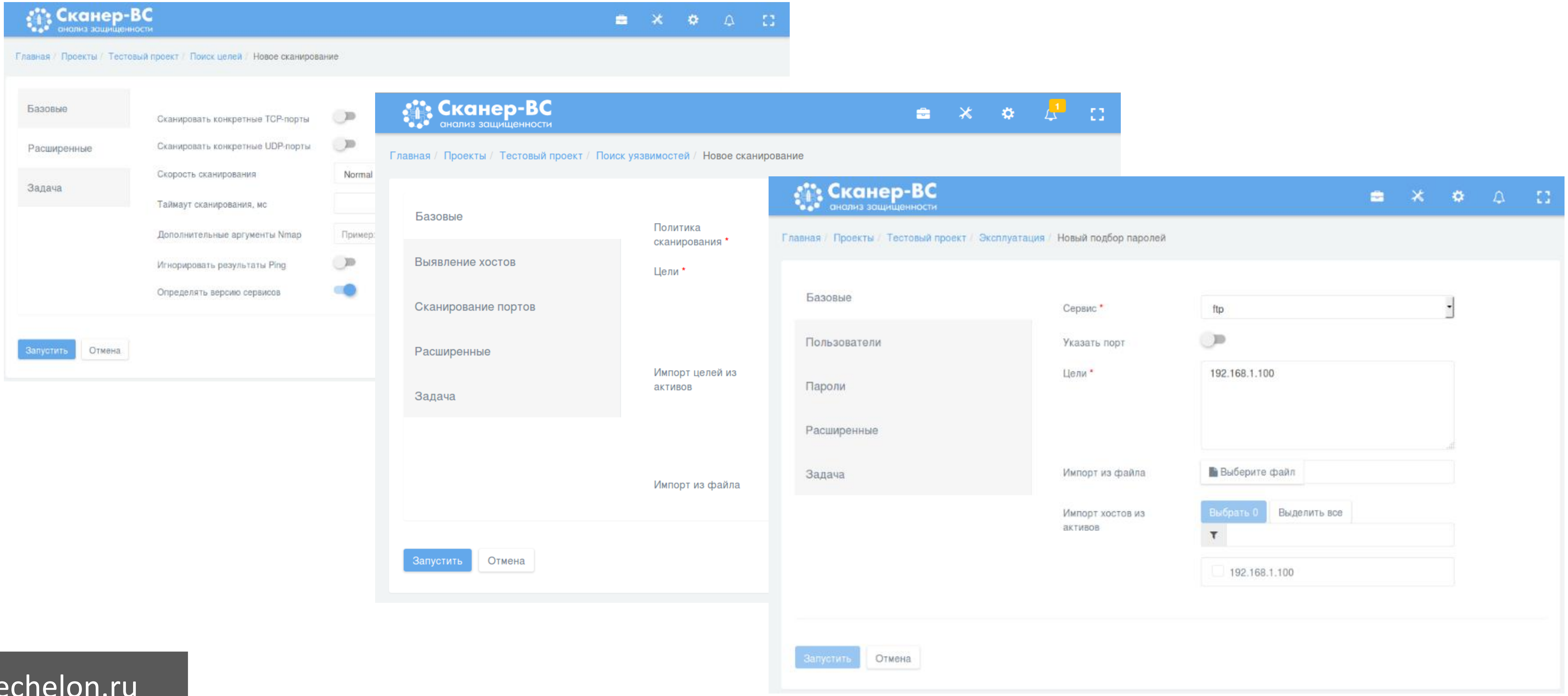


#	Адрес	Протокол	Порт	Состояние	Обновлено	Сервис	Продукт	Версия
1	192.168.1.10	tcp	21	открыт	27.02.2020 7:12:05	ftp	vsftpd	2.3.4
2	192.168.1.10	tcp	22	открыт	27.02.2020 7:12:05	ssh	OpenSSH	4.7p1 Debian 8ubuntu1
3	192.168.1.10	tcp	23	открыт	27.02.2020 7:12:05	telnet	Linux telnetd	-
4	192.168.1.10	tcp	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-ssn	Samba smbd	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 grmiregistry	-
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	nfs	-	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	-	-	-

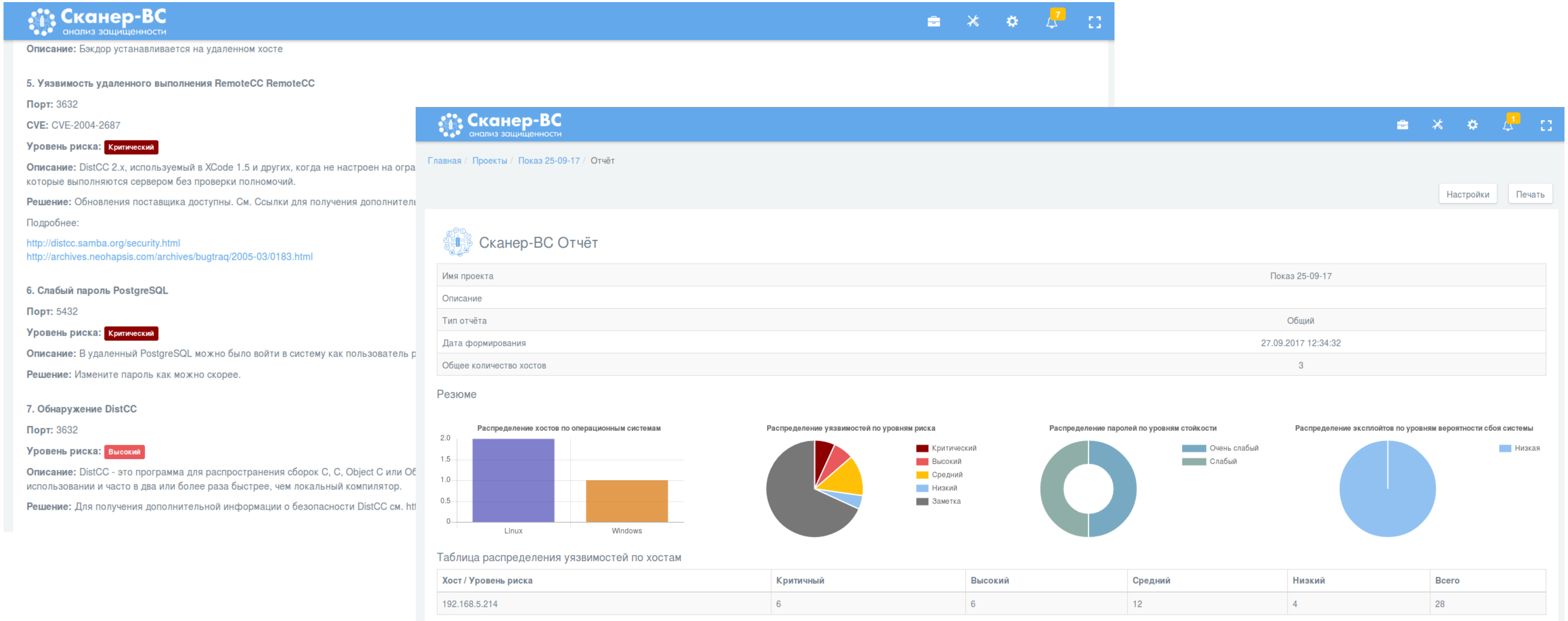


						BDU:2015-05953 BDU:2015-05955 BDU:2015-09252 BDU:2015-09253 BDU:2015-09247	
19	192.168.1.10	-	Этот хост установлен с GNU Bash Shell и подвержен уязвимости удаленного выполнения команд.	27.02.2020 7:29:53	CVE-2014-6277	BDU:2015-09794 BDU:2015-09818 BDU:2014-00319	Критический
18	192.168.1.10	-	Этот хост установлен с GNU Bash Shell и подвержен 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 подвержен уязвимости удаленного выполнения команд.	27.02.2020 7:29:53	CVE-2014-7169	BDU:2014-00319 BDU:2015-05950 BDU:2015-00148 BDU:2015-00157 BDU:2015-09249 BDU:2015-05958 BDU:2015-06153 BDU:2015-09795 BDU:2015-05952 BDU:2015-06160 BDU:2015-09250 BDU:2015-06155 BDU:2015-05954 BDU:2015-05956 BDU:2015-05957 BDU:2015-06154 BDU:2015-06159 BDU:2015-06158 BDU:2015-06152 BDU:2015-09246 BDU:2015-00155 BDU:2015-09245 BDU:2015-05951 BDU:2015-09818 BDU:2015-06156 BDU:2015-00153 BDU:2015-00159 BDU:2015-09251 BDU:2015-06157 BDU:2015-09248 BDU:2015-05953 BDU:2015-05955 BDU:2015-00151 BDU:2015-09252	Критический

Задачи по анализу задаются в унифицированном формате



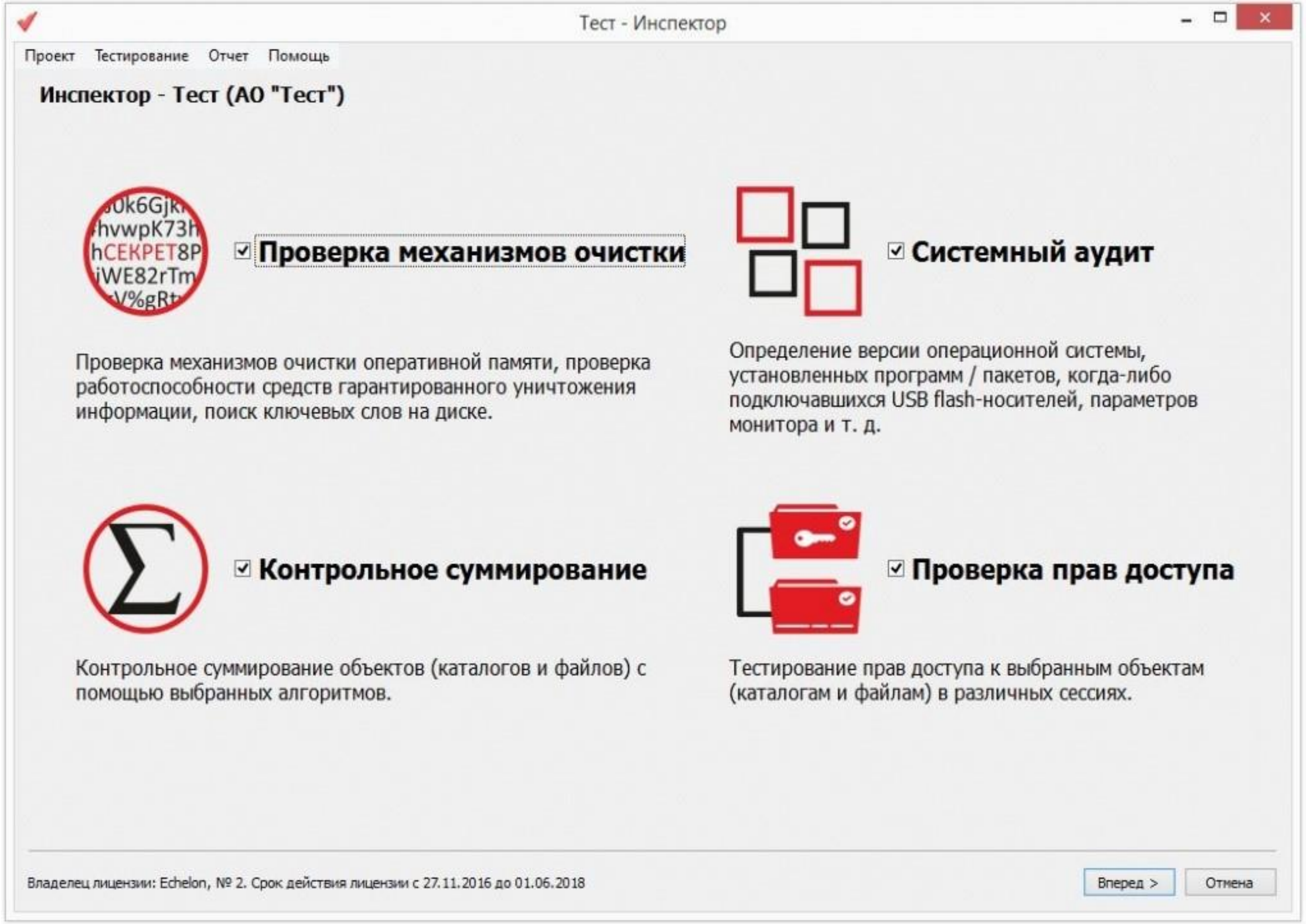
Полный ОТЧЕТ: сервисы, уязвимости, пароли и наличие подходящих эксплойтов



Инструменты для
продвинутых сисадминов

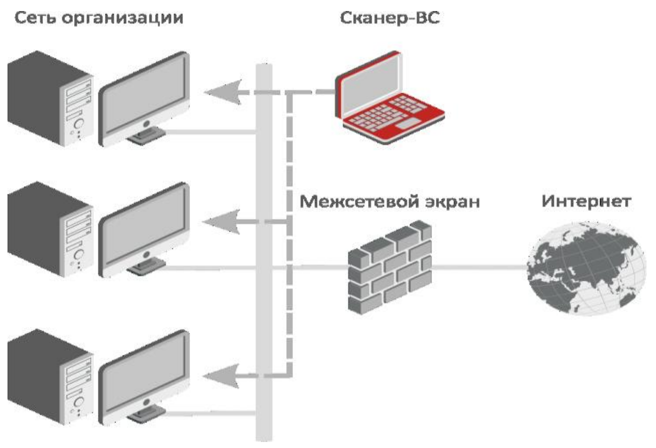
- Сбор информации
- Поиск уязвимостей
- Анализ веб-приложений
- Анализ баз данных
- Атаки на пароли
- Аудит беспроводных сетей
- Реверс-инжиниринг
- Эксплуатация уязвимостей
- Снифинг и спуфинг
- Пост-эксплуатация
- Форензика
- Генерация отчетов
- Социальная инженерия
- Управление сервисами
- Аудит ОС 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»

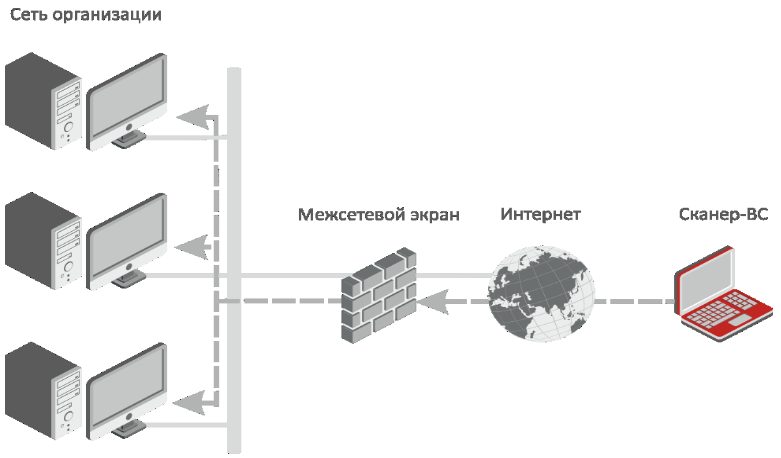


- Автоматизированный процесс проверки отдельных требований нормативных документов
- Возможность сбора подробной информации об автоматизированной (информационной) системе (номера лицензий на некоторые виды ПО, идентификаторы подключавшихся внешних носителей и др.)

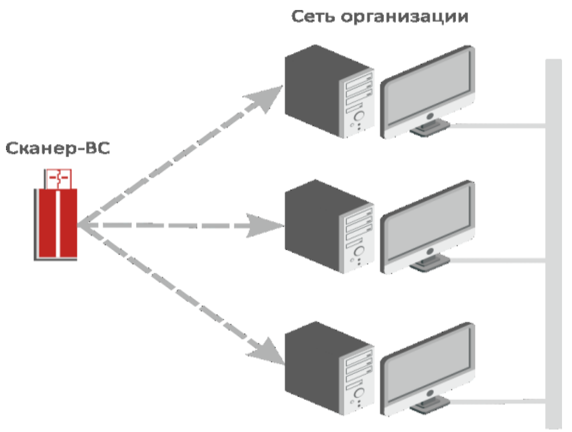
Сценарии применения «Сканер-ВС»



Внутреннее
тестирование защищенности



Внешнее
тестирование защищенности



Тестирование защищенности
выделенных сегментов

«Сканер-ВС» сертифицирован ФСТЭК России и Минобороны России

ФСТЭК России №2204

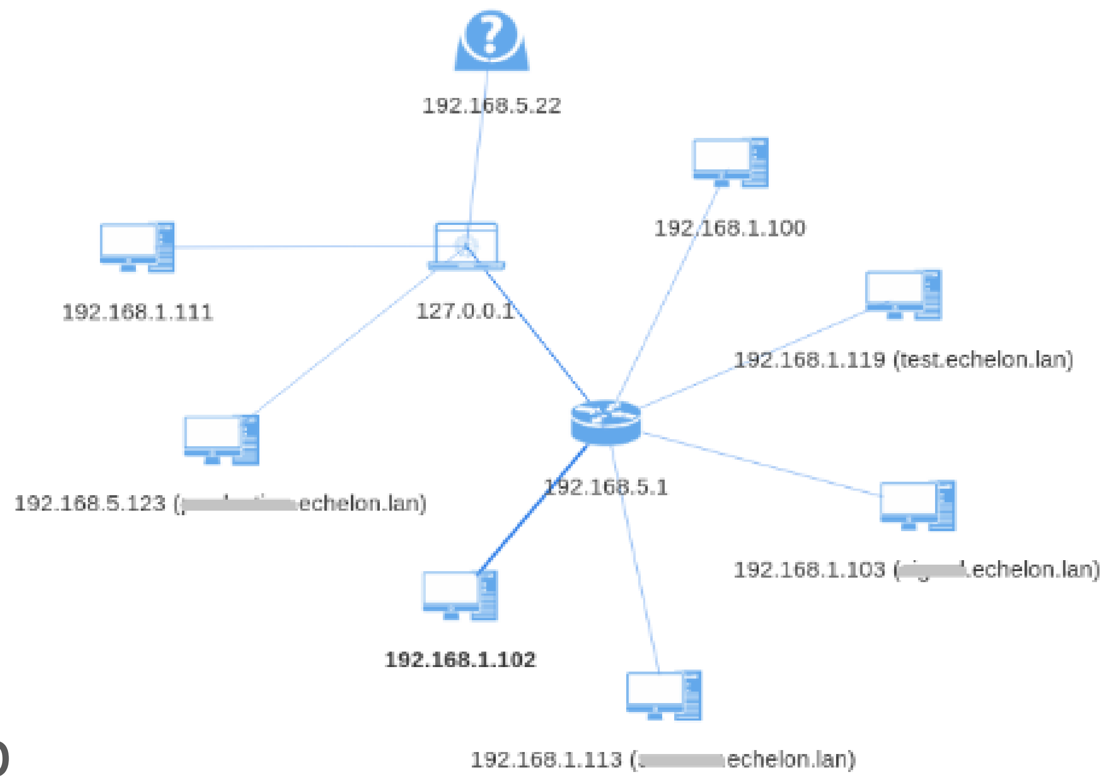
(4 уровень доверия)

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 (экспор в форматы HTML, PDF, RTF, XML)

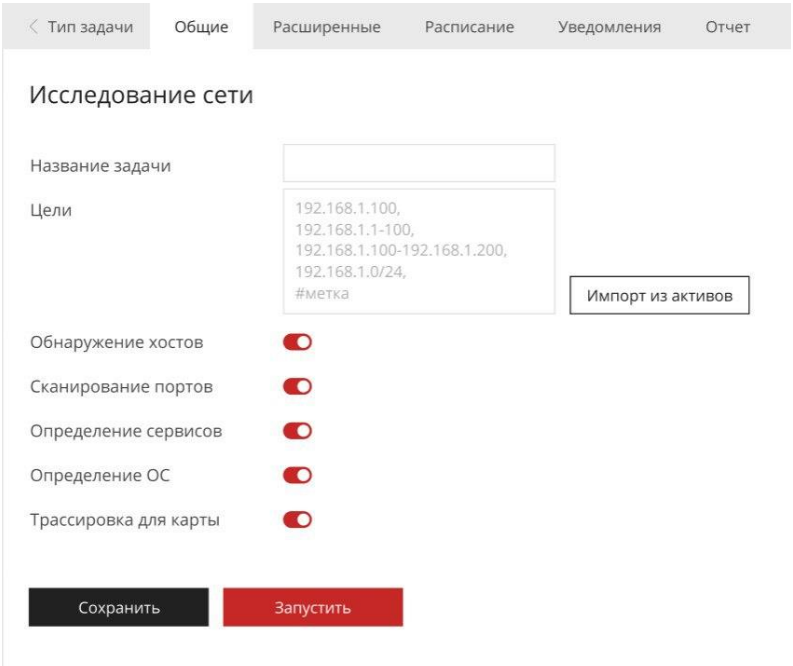


Стоимость

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



МЭ и СОВ в одном устройстве

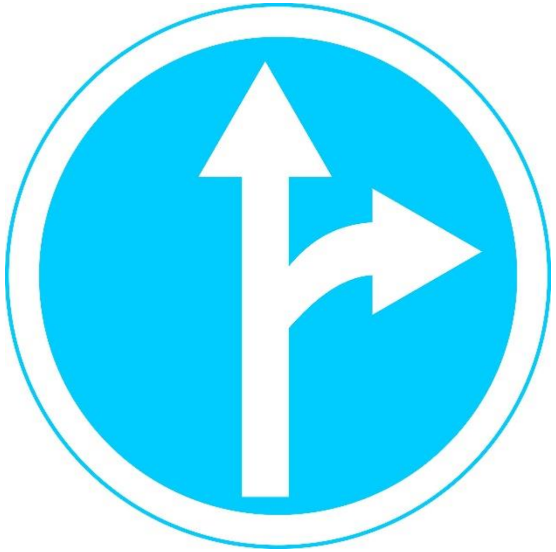
РУБИКОН

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 СОВ: 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.П3, ИТ.МЭ.Б4.П3, ИТ.СОВ.С4.П3

Рубикон-А

ФСТЭК России №2574: ИТ.МЭ.А2.П3, ИТ.СОВ.С2.П3.

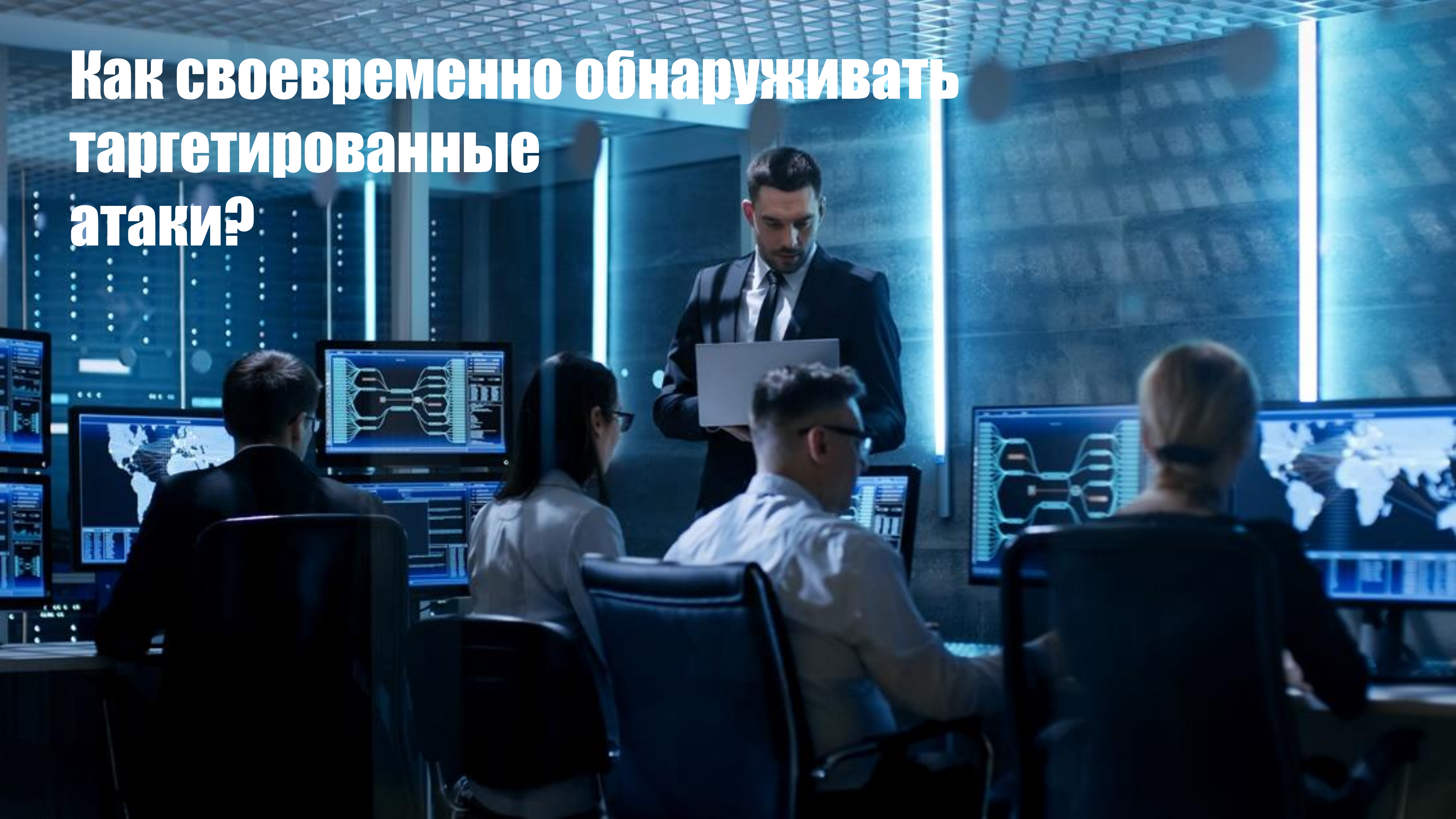
Рубикон

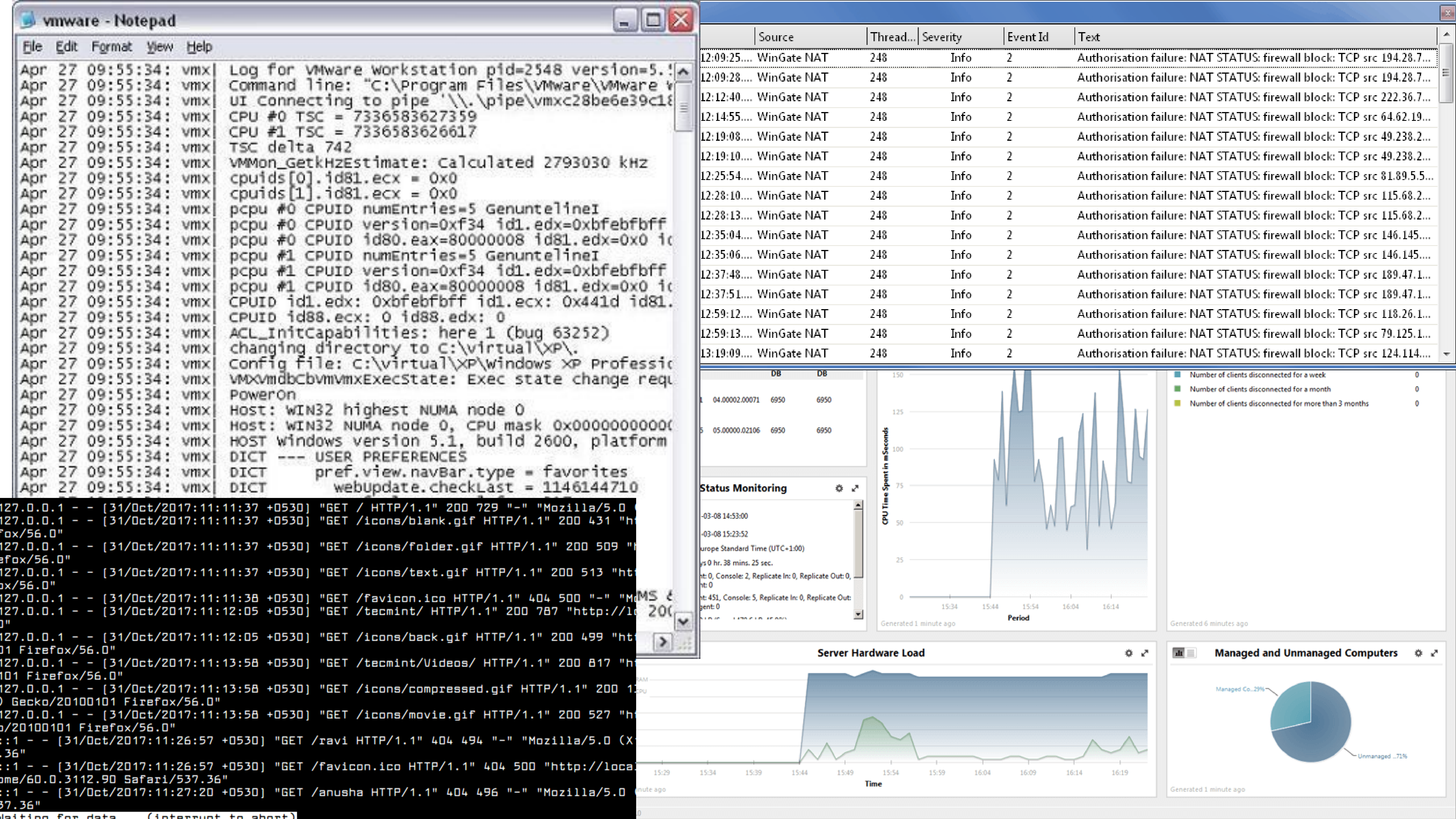
Минобороны России №3168

SIEM-система КОМРАД

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

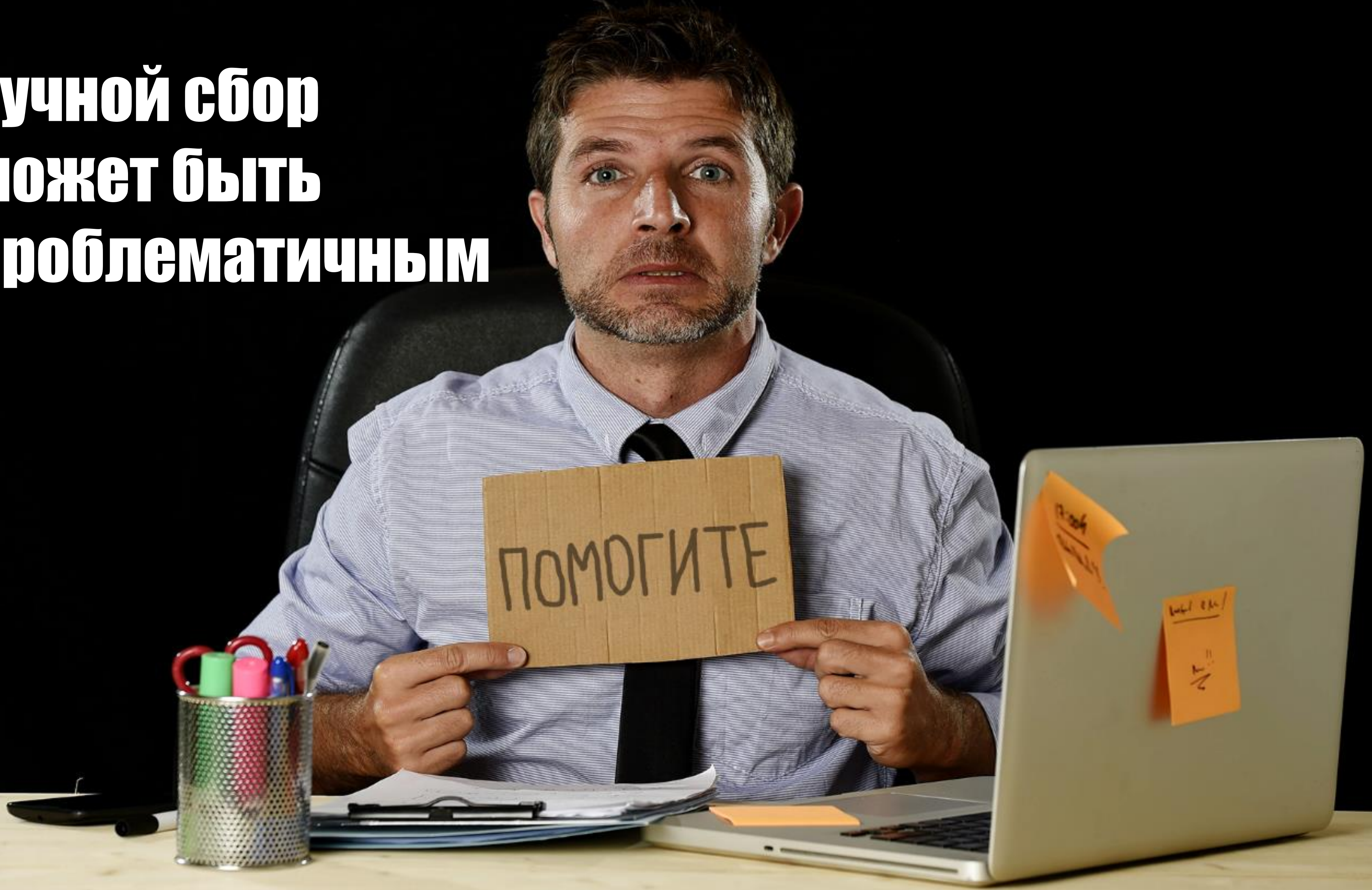
Как своевременно обнаруживать таргетированные атаки?





vmware - Notepad
File Edit Format View Help
Apr 27 09:55:34: vmx| Log for VMware Workstation pid=2548 version=5.
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\VMware\VMware
Apr 27 09:55:34: vmx| UI Connecting to pipe '\\.\pipe\vmxc28be6e39c1
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 i
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 i
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 Professi
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
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....
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 "h
fox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200 509 "
efox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 513 "ht
ox/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://l
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 "h
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 "h
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"
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.
CPU Time Spent in mSeconds
Period
Generated 1 minute ago
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
Time
Managed and Unmanaged Computers
Managed Co...29%
Unmanaged ...71%
Generated 1 minute ago

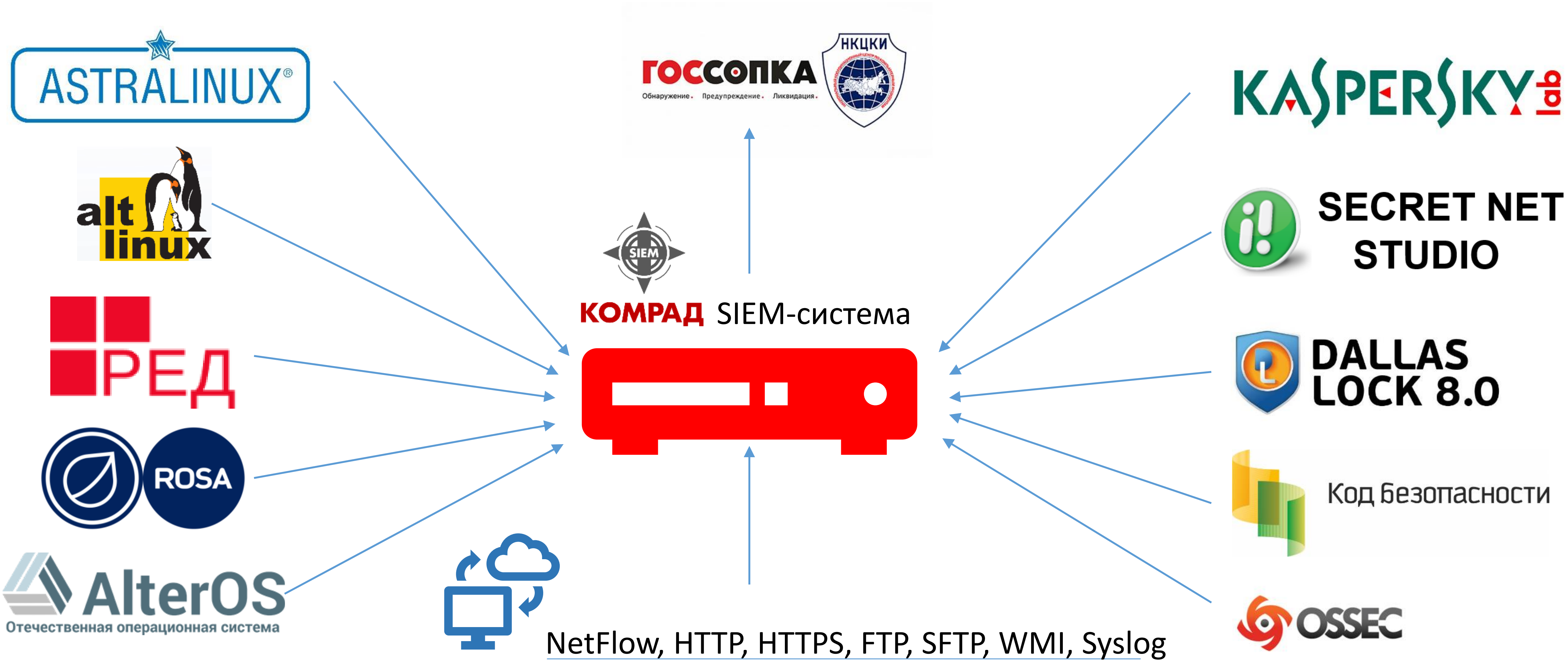
Ручной сбор может быть проблематичным



Категории и типы инцидентов на которые надо реагировать

Категория инцидента	Типы инцидентов
Внедрение вредоносного ПО	Заражение ВПО
Распространение вредоностного ПО	• Использование контролируемого ресурса для распространения или управления модулями ВПО • Попытки внедрения модулей ВПО
Нарушение или замедление работы контролируемого информационного ресурса	• 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	• Успешная эксплуатация уязвимости • Компрометация учетной записи
Попытки НСД в систему или к информации	• Попытки эксплуатации уязвимости • Попытки авторизации в информационном ресурсе
Сбор сведений с использованием информационно-коммуникационных технологий	• Сканирование информационного ресурса • Прослушивание (захват) сетевого трафика • Социальная инженерия
Нарушение безопасности информации	• Несанкционированное разглашение информации • Несанкционированное изменение информации
Распространение информации с неприемлемым содержимым	• Рассылка незапрашиваемых электронных сообщений • Публикация запрещенной законодательством РФ информации
Мошенничество с использованием информационно-коммуникационных технологий	• Злоупотребление при использовании информационного ресурса • Публикация мошеннического информационного ресурса
Наличие уязвимости или недостатков конфигурации в информационном ресурсе	• 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»

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

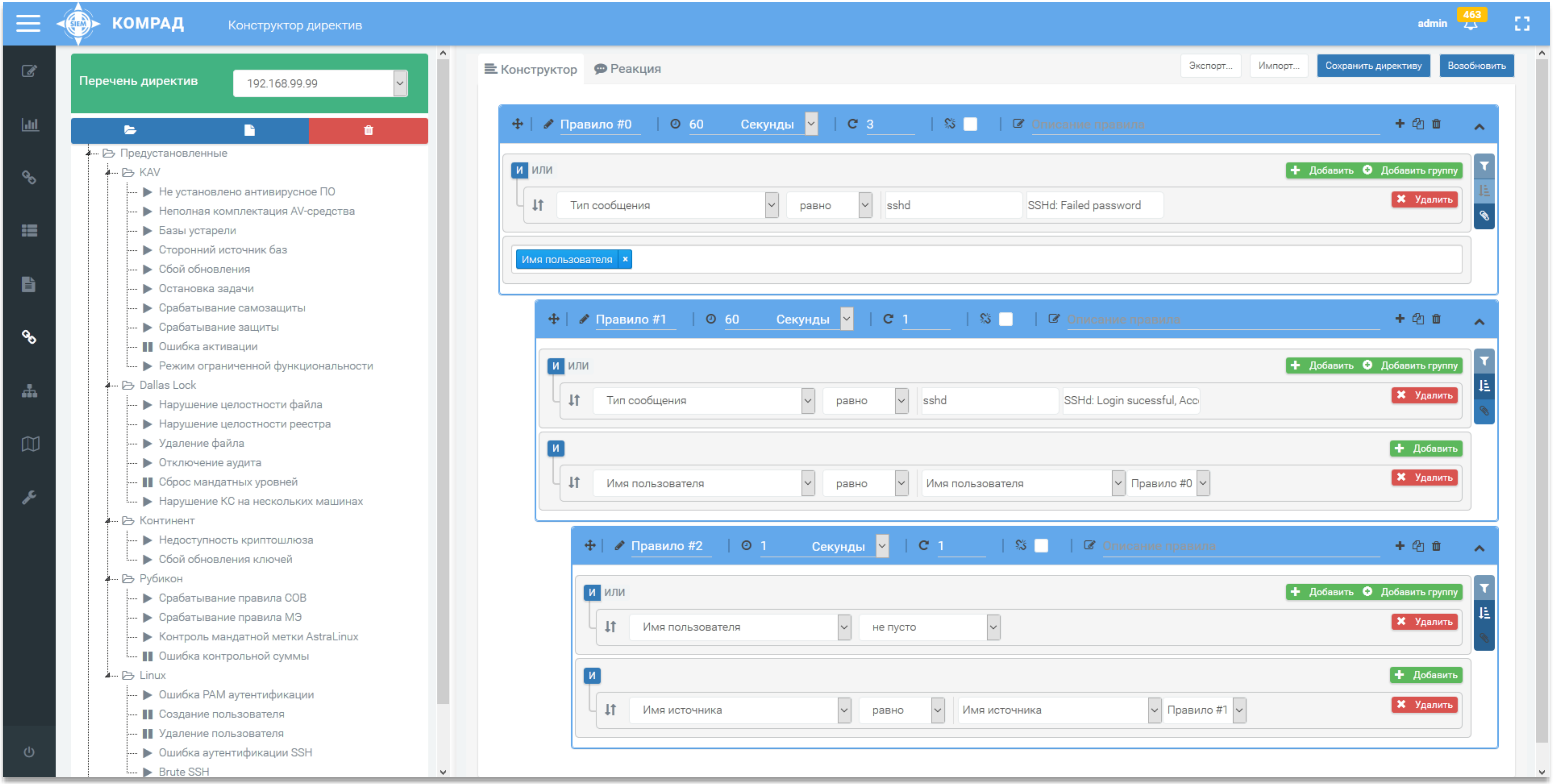
Оперативное оповещение об инциденте

Ролевая модель управления доступом

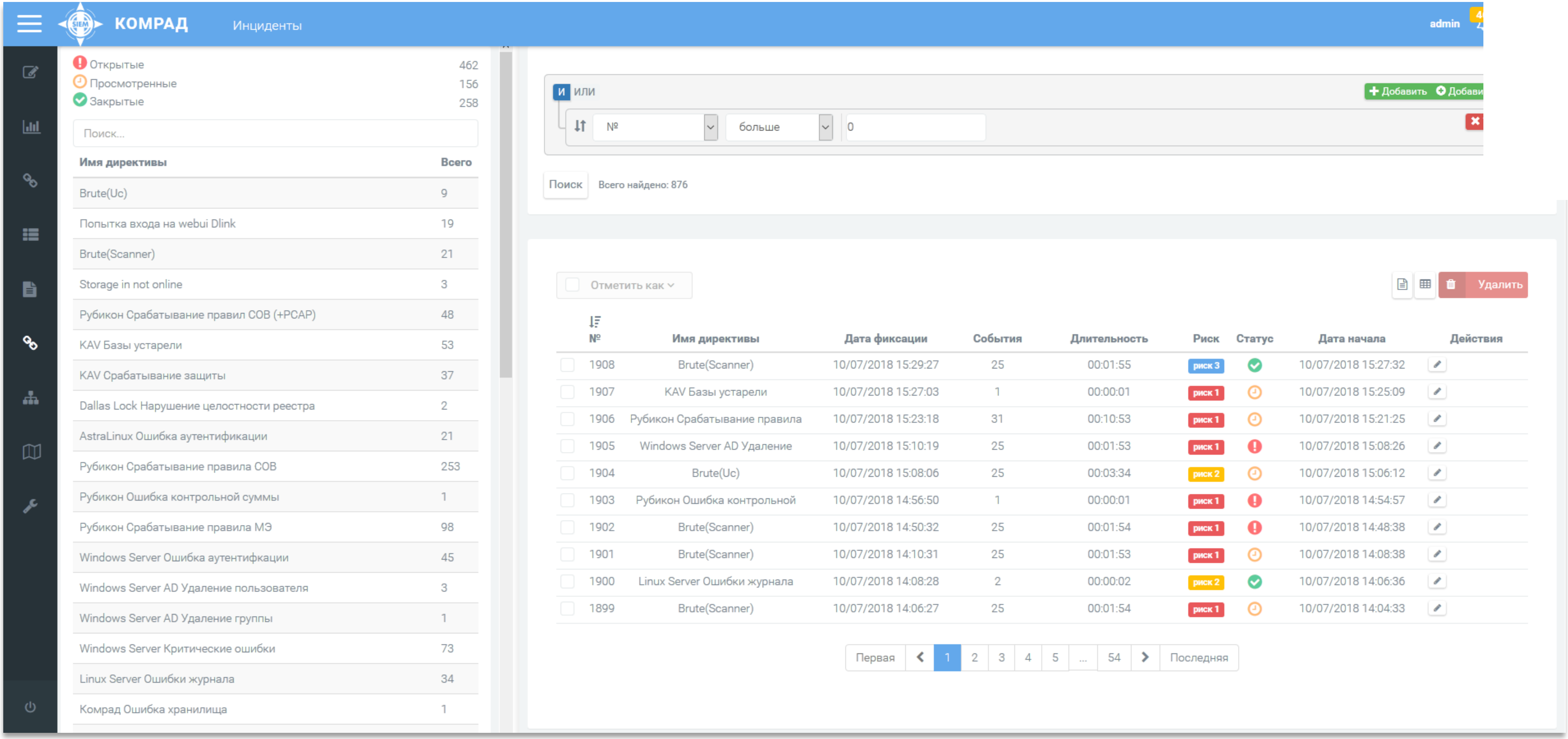
Основные преимущества

- 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

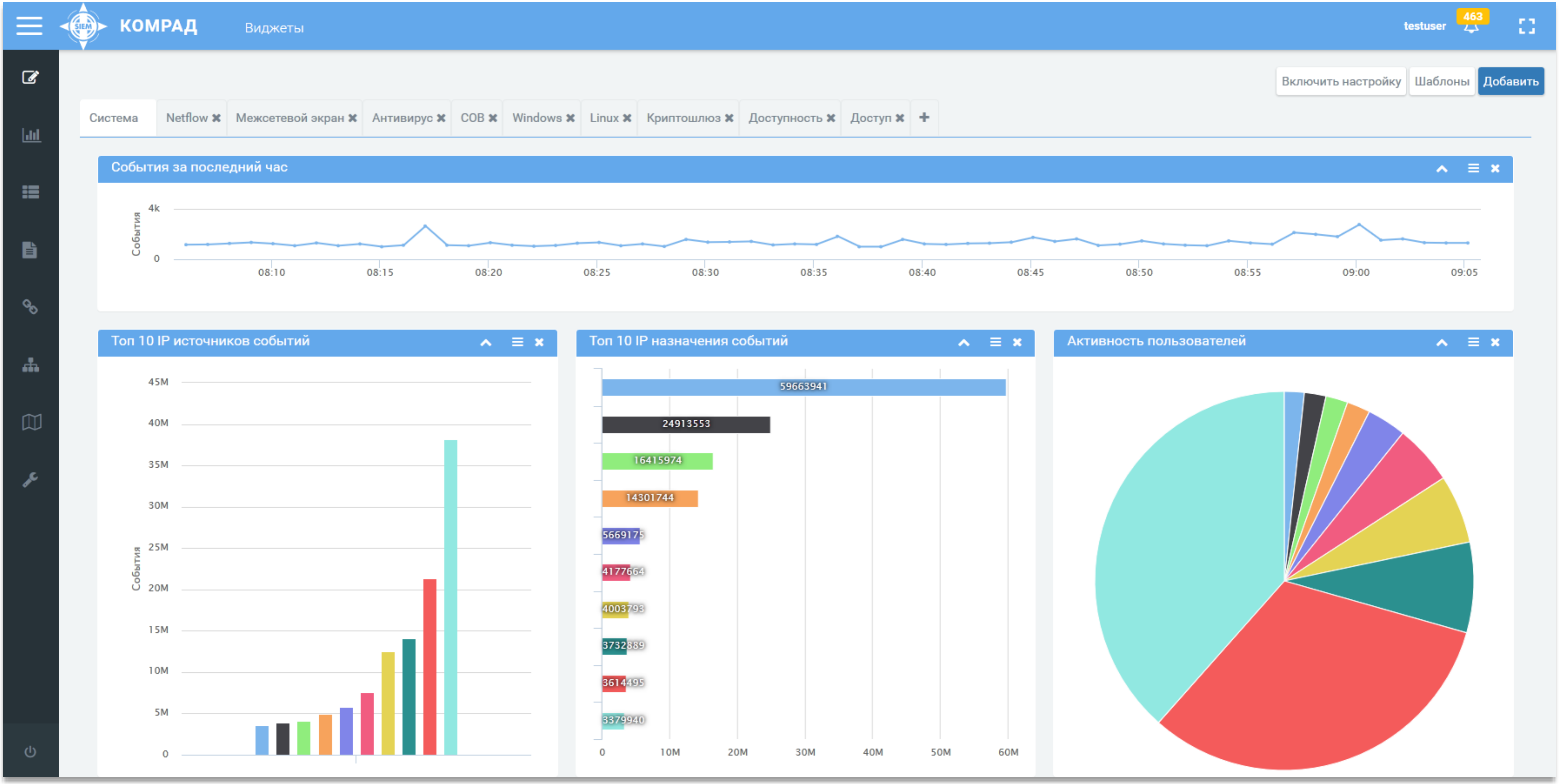
Инструменты SIEM Комрад: Конструктор директив



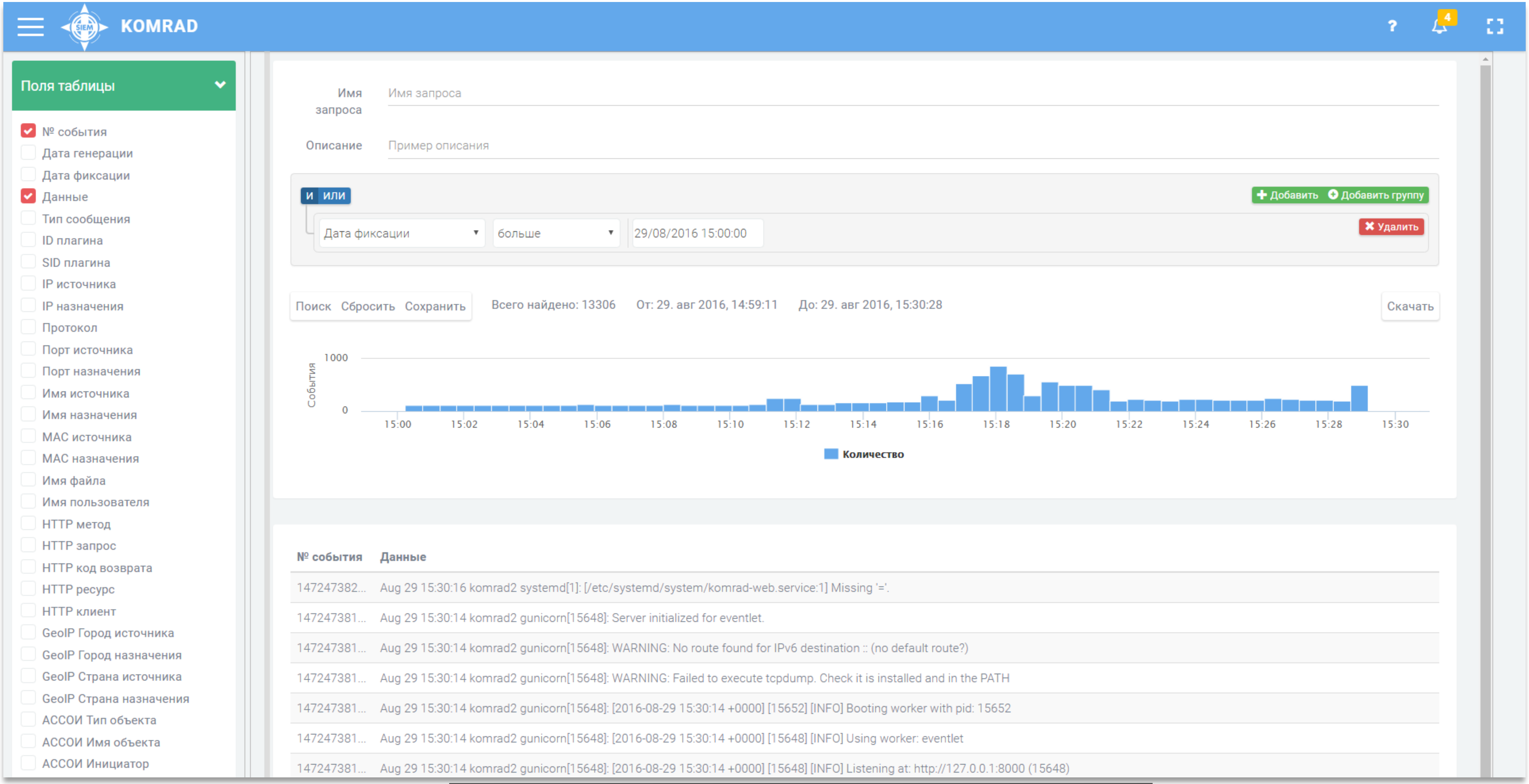
Инструменты SIEM КОМРАД: Инциденты



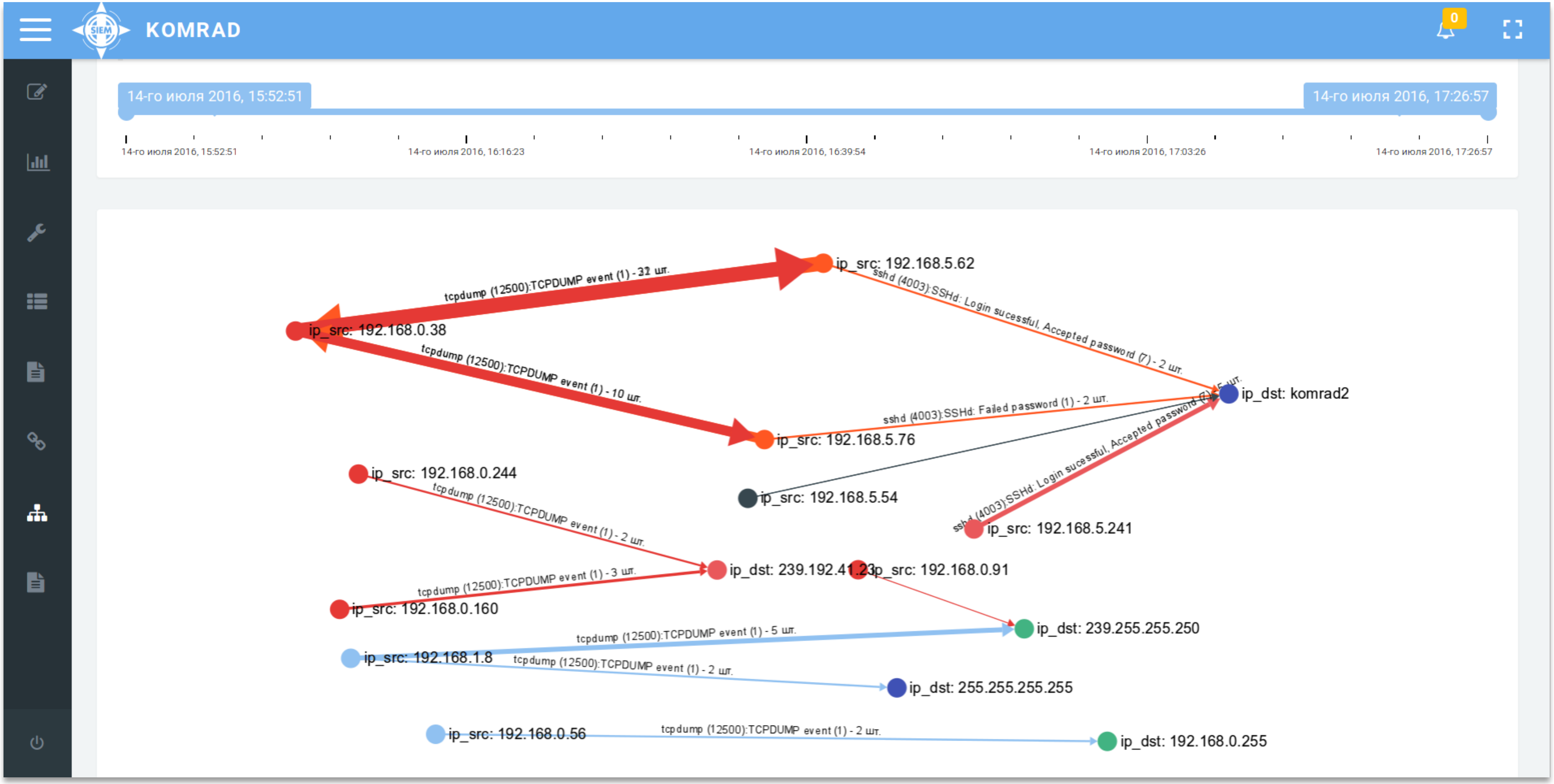
Инструменты SIEM КОМРАД: Виджеты и диаграммы



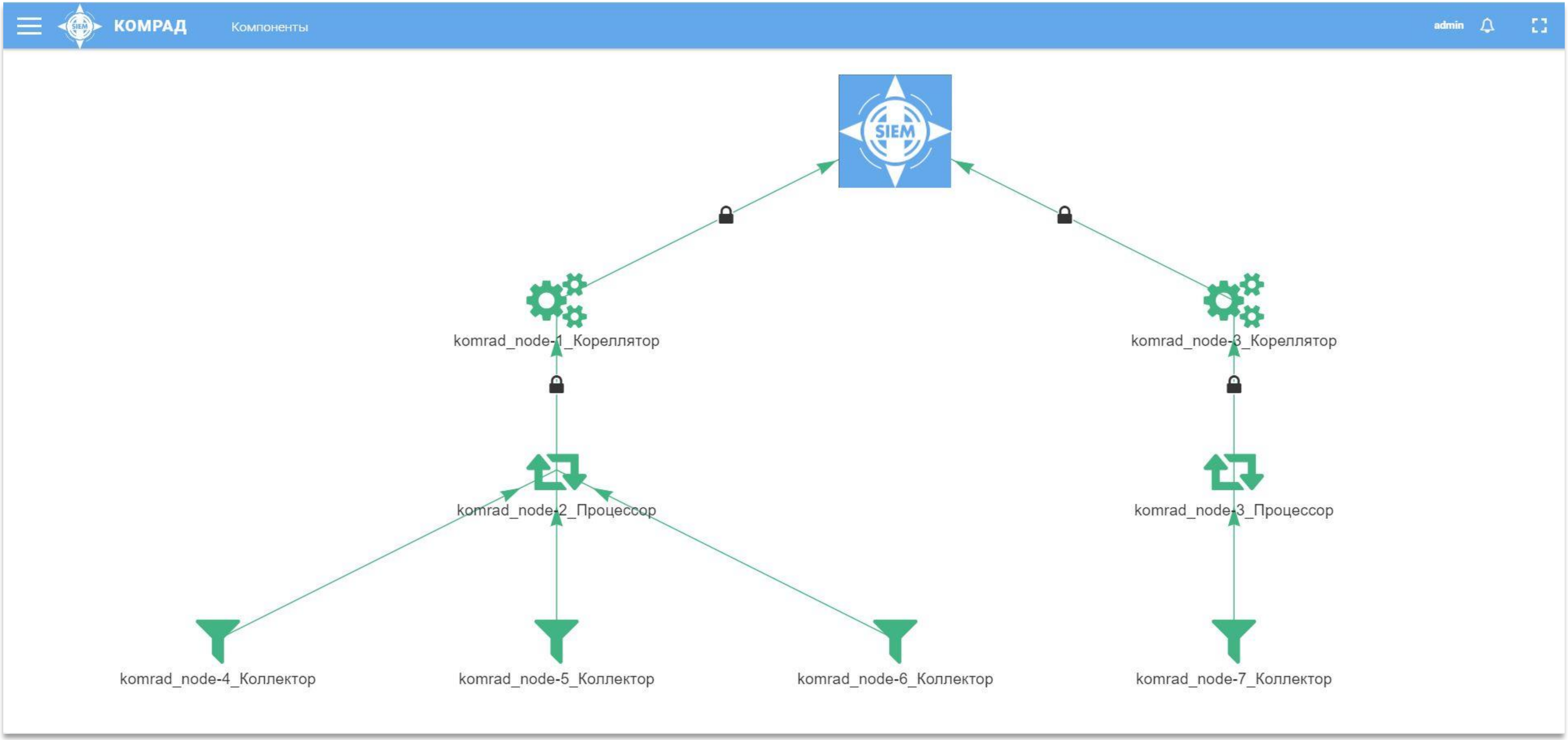
Инструменты SIEM КОМРАД: поиск по событиям



Инструменты SIEM КОМРАД: визуализатор событий



КОМРАД: возможности масштабирования

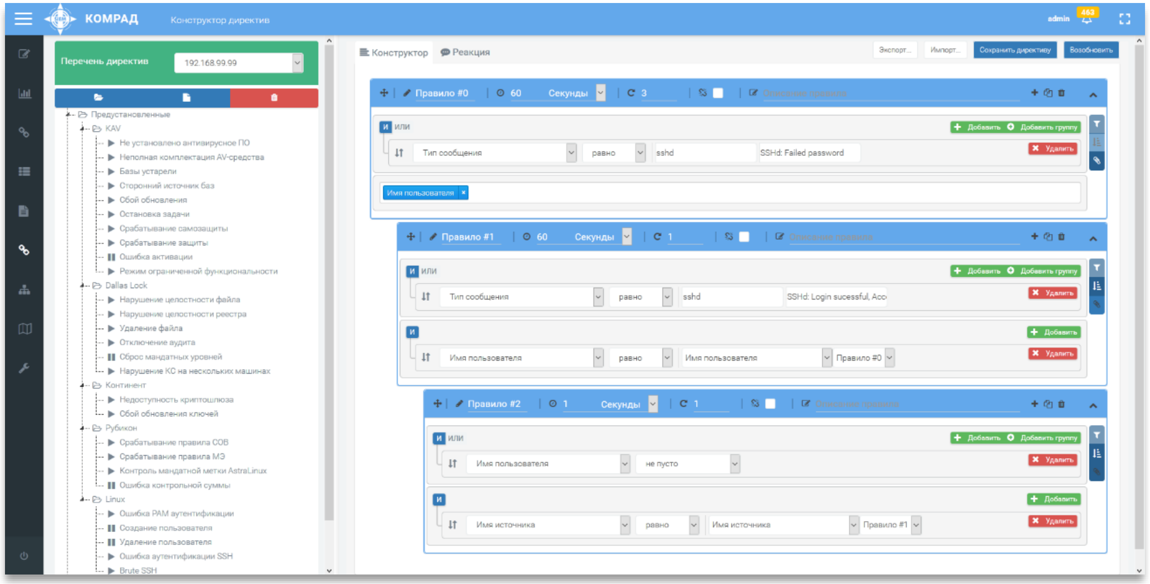


В SIEM-системе должны быть уже Предустановлены директивы корреляции

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 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

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)

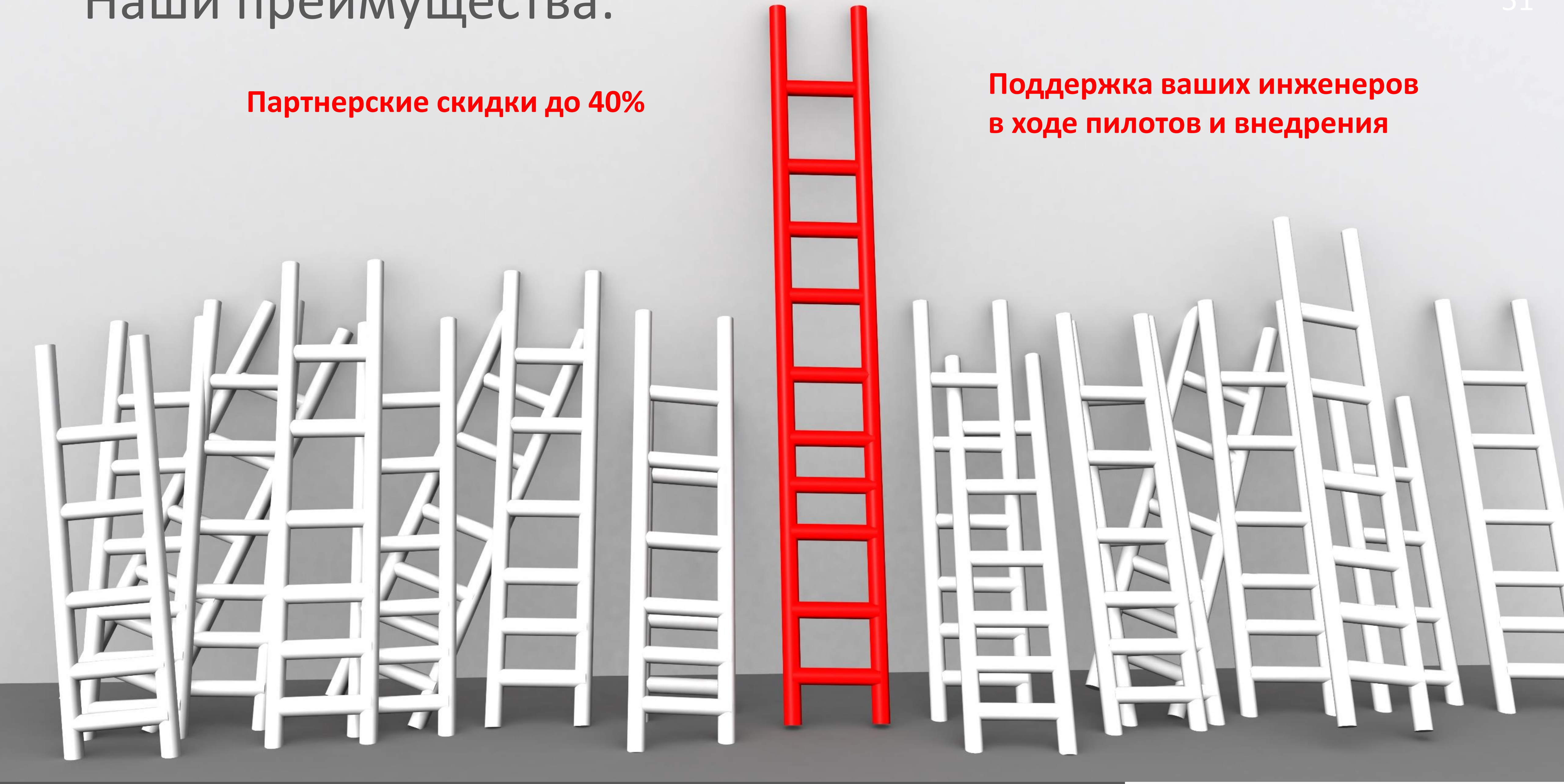
- Кроссплатформенность (Windows\Linux)
- Высокая скорость обработки событий (несколько десятков тысяч EPS)
- Большое количество источников событий

Как можно с нами заработать?

Наши преимущества:

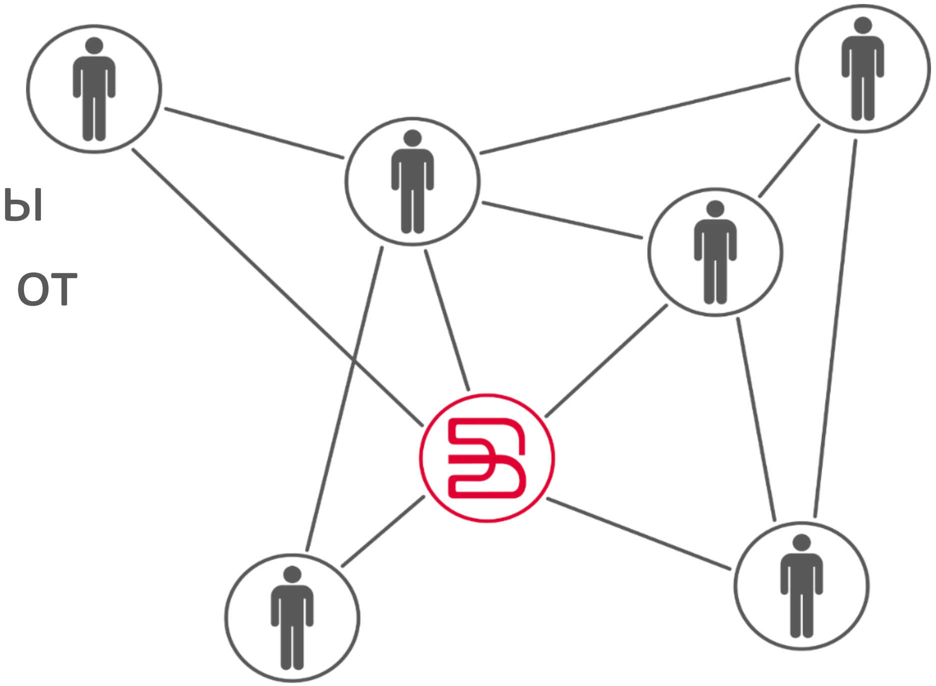
Партнерские скидки до 40%

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