Эшелон
комплексная безопасность

Применение отечественных технологий для мониторинга информационной безопасности

Пучкин Вадим
Руководитель направления
по работе с партнерами

Группа компаний «Эшелон»

Эшелон
комплексная безопасность

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 и CNews 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

Группа компаний «Эшелон»

Эшелон
комплексная безопасность

- Государственный сектор
- Промышленный сектор
- Финансовый сектор
- Телеком

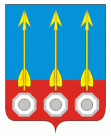







Камчатский краевой медицинский информационно-аналитический центр
оператор региональных информационных систем в сфере здравоохранения


МЧС РОССИИ
EMERCOM


МИНИСТЕРСТВО ПРИРОДНЫХ РЕСУРСОВ И ЭКОЛОГИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЦАГИ100


ЭЛЕРОН
СИСТЕМЫ БЕЗОПАСНОСТИ
ПРЕДПРИЯТИЕ ГОСКОРПОРАЦИИ «РОСАТОМ»



КОНЦЕРН ПВО АЛМАЗ-АНТЕЙ
ОАО КОНЦЕРН СОЗВЕЗДИЕ
РКС
РОССИЙСКИЕ КОСМИЧЕСКИЕ СИСТЕМЫ

ВНИИА
МЦСТ ЭЛЬБРУС
РАДИОЗАВОД
Сибирский химический комбинат
ПРЕДПРИЯТИЕ ГОСКОРПОРАЦИИ РОСАТОМ

МОСКОВСКИЙ НЕФТЕХИМИЧЕСКИЙ БАНК
ГАЗПРОМБАНК
онланта
МегаФон

РУСЬ-ТЕЛЕКОМ
оператор данных

Мониторинг информационной безопасности

Эшелон
комплексная безопасность

Процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления инцидентов информационной безопасности

Мониторинг требуется везде

Эшелон
комплексная безопасность

ИСПДН

V. Регистрация событий безопасности (РС					
РСБ.1	Определение событий безопасности, подлежащи регистрации, и сроков их хранения				
РСБ.2	Определение состава и содержания информации событиях безопасности, подлежащих регистрации				
РСБ.3	Сбор, запись и хранение информации о события безопасности в течение установленного времен хранения				
РСБ.4	Реагирование на сбои при регистрации событи безопасности, в том числе аппаратные программные ошибки, сбои в механизмах сбор информации и достижение предела ил переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатс регистрации событий безопасности и реагировани на них				
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+

ГИС

V. Аудит безопасности (АУД)				
АУД.0	Разработка политики аудита безопасности			
АУД.1	Инвентаризация информационных ресурсов			
АУД.2	Анализ уязвимостей и их устранение			
АУД.3	Генерирование временных меток и (или) синхронизация системного времени			
АУД.4	Регистрация событий безопасности			
АУД.5	Контроль и анализ сетевого трафика			
АУД.6	Защита информации о событиях безопасности			
АУД.7	Мониторинг безопасности			
АУД.8	Реагирование на сбои при регистрации событий безопасности			
АУД.9	Анализ действий пользователей			
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			+

АСУ ТП

V. Регистрация событий б				
РСБ.1	Определение событий безопа регистрации, и сроков их хранен			
РСБ.2	Определение состава и содер событиях безопасности, подлежа			
РСБ.3	Сбор, запись и хранение инф безопасности в течение установ нения			
РСБ.4	Реагирование на сбои при р безопасности, в том числе аппар ошибки, сбои в механизмах сбо стижение предела или перепол сти) памяти			
РСБ.5	Мониторинг (просмотр, анал страции событий безопасности и			
РСБ.6	Генерирование временных м низация системного времени в информационной системе			
РСБ.7	Защита информации о событиях безопасности	+	+	+
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе			

КИИ

V. Аудит безопасности (АУД)				
АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6	Защита информации о событиях безопасности	+	+	+
АУД.7	Мониторинг безопасности	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий отдельных пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			

Развитие законодательства в области безопасности КИИ и создание ГосСОПКА

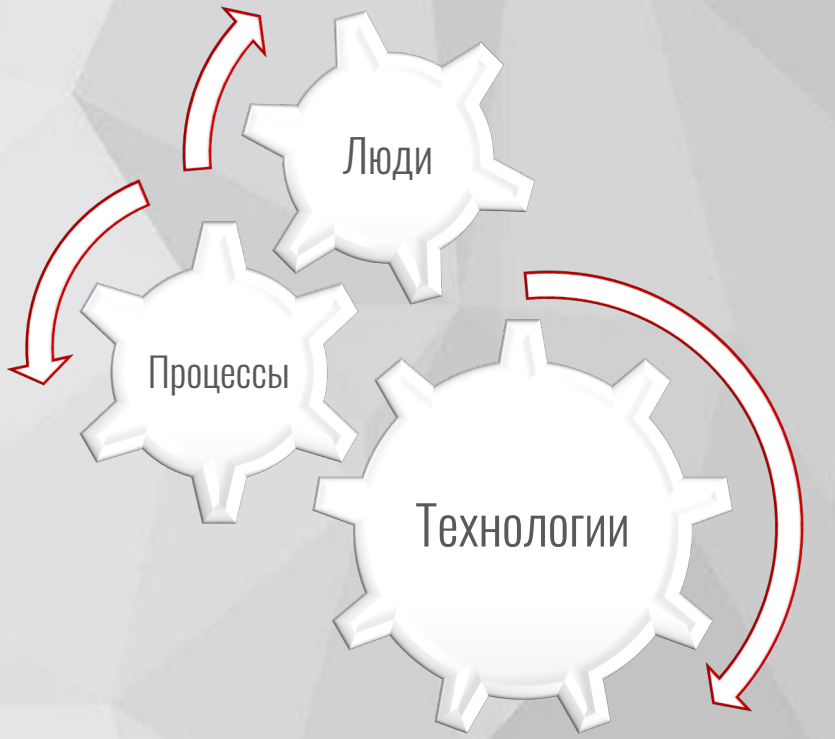
Эшелон
комплексная безопасность

Центр мониторинга информационной безопасности (Security Operations Center)

Эшелон
комплексная безопасность

Подразделение осуществляющее мониторинг событий ИБ и улучшающее защищенность компании путем предотвращения, обнаружения, анализа и реагирования на инциденты ИБ.

SOC выступает в роли центрального командного пункта, в который стекаются события со всей ИТ-инфраструктуры



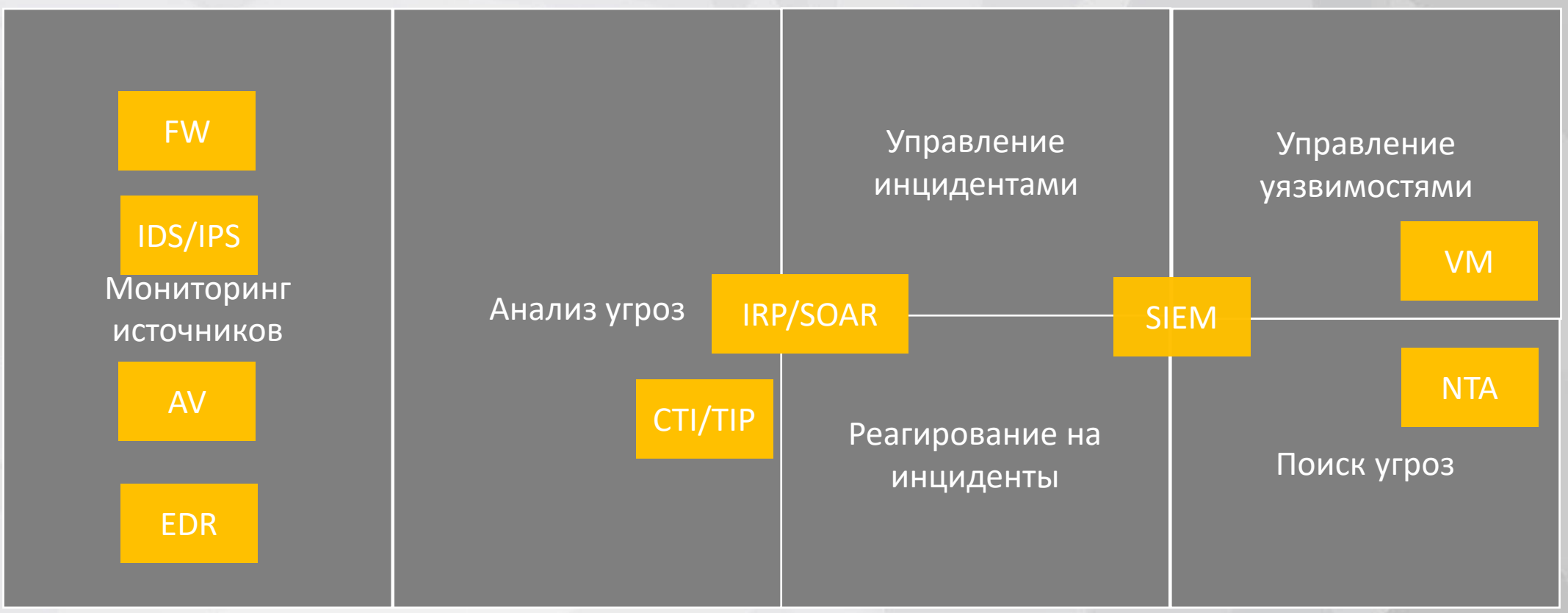
Ключевые процессы SOC

Эшелон
комплексная безопасность

- Мониторинг
- Реагирование на инциденты
- Анализ угроз (threat intelligence)
- Поиск угроз (threat hunting)

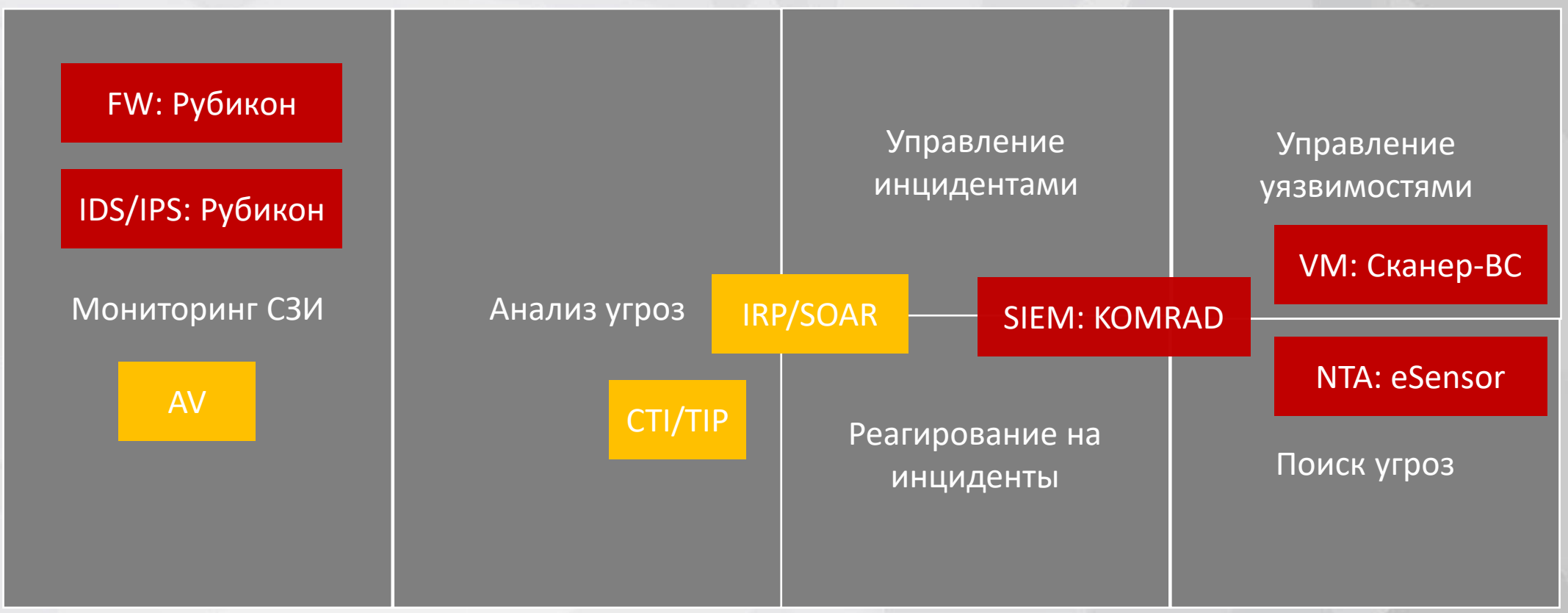
Основные функции SOC и поддерживающие технологии

Эшелон
комплексная безопасность



Решения ГК «Эшелон» для мониторинга информационной безопасности

Эшелон
комплексная безопасность



Основные решения НПО «Эшелон» для обеспечения безопасности объектов

Эшелон
комплексная безопасность

Сканер-ВС

Система комплексного анализа защищенности

ПАК «Рубикон»

Межсетевой экран, маршрутизатор, СОВ

KOMRAD Enterprise SIEM

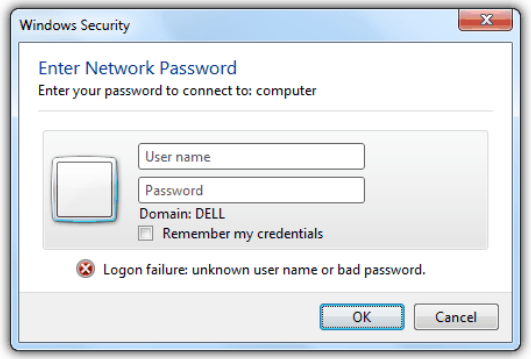
Система комплексного анализа защищенности

Эшелон
комплексная безопасность

SIEM (Security Information Event Management) – система управления событиями информационной безопасности

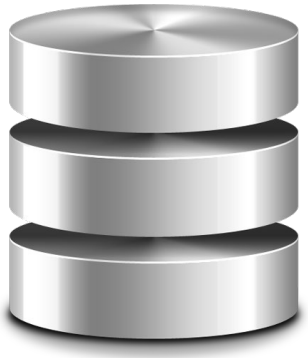
Необходимо отслеживать признаки нарушения ИБ

Эшелон
комплексная безопасность



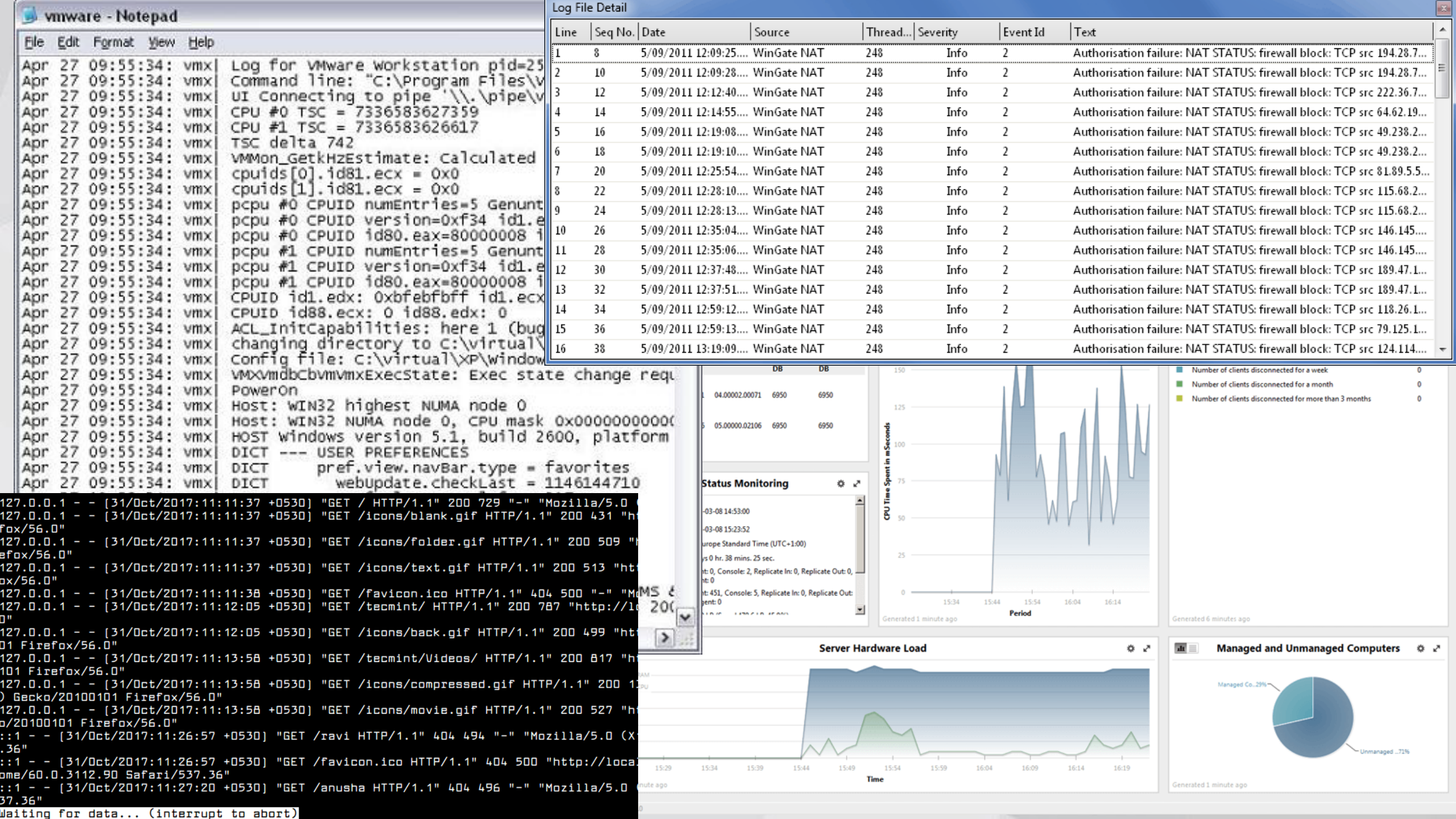
Авторизация: как успешная, так и неуспешная

Срабатывания антивирусного ПО, СОВ



Подозрительные запросы к СУБД

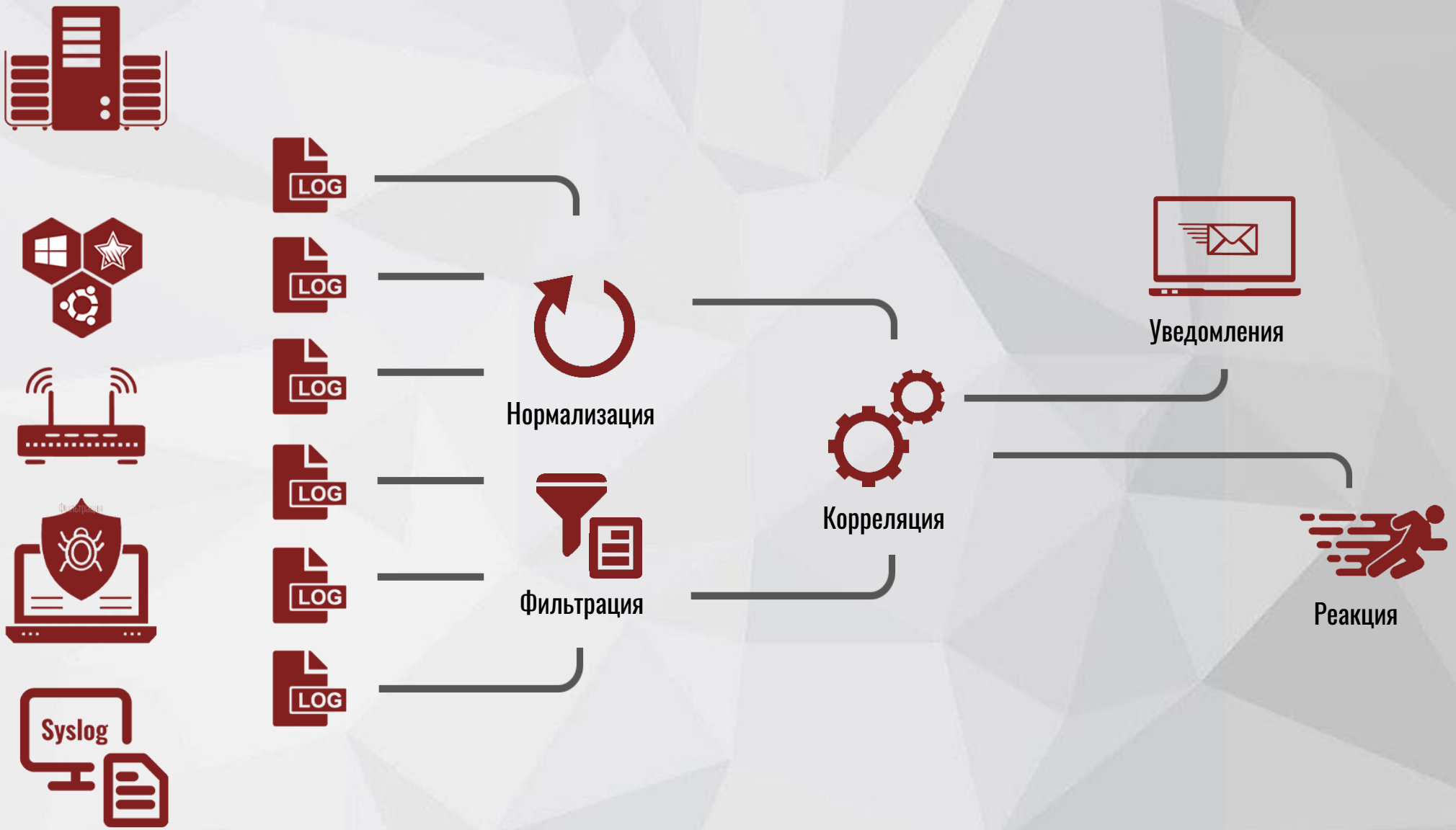
Нетипичное поведение пользователя


vmware - Notepad
File Edit Format View Help
Apr 27 09:55:34: vmx| Log for VMware Workstation pid=25
Apr 27 09:55:34: vmx| Command line: "C:\Program Files\v
Apr 27 09:55:34: vmx| UI Connecting to pipe '\\.\pipe\v
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
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 Genunt
Apr 27 09:55:34: vmx| pcpu #0 CPUID version=0xf34 id1.e
Apr 27 09:55:34: vmx| pcpu #0 CPUID id80.eax=80000008 i
Apr 27 09:55:34: vmx| pcpu #1 CPUID numEntries=5 Genunt
Apr 27 09:55:34: vmx| pcpu #1 CPUID version=0xf34 id1.e
Apr 27 09:55:34: vmx| pcpu #1 CPUID id80.eax=80000008 i
Apr 27 09:55:34: vmx| CPUID id1.edx: 0xbfebfbff id1.ecx
Apr 27 09:55:34: vmx| CPUID id88.ecx: 0 id88.edx: 0
Apr 27 09:55:34: vmx| ACL_InitCapabilities: here 1 (bug
Apr 27 09:55:34: vmx| changing directory to C:\virtual\
Apr 27 09:55:34: vmx| Config file: C:\virtual\XP\Window
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
Log File Detail
Line Seq No. Date Source Thread... Severity Event Id Text
1 8 5/09/2011 12:09:25.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
2 10 5/09/2011 12:09:28.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 194.28.7...
3 12 5/09/2011 12:12:40.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 222.36.7...
4 14 5/09/2011 12:14:55.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 64.62.19...
5 16 5/09/2011 12:19:08.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
6 18 5/09/2011 12:19:10.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 49.238.2...
7 20 5/09/2011 12:25:54.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 81.89.5.5...
8 22 5/09/2011 12:28:10.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
9 24 5/09/2011 12:28:13.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 115.68.2...
10 26 5/09/2011 12:35:04.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
11 28 5/09/2011 12:35:06.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 146.145....
12 30 5/09/2011 12:37:48.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
13 32 5/09/2011 12:37:51.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 189.47.1...
14 34 5/09/2011 12:59:12.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 118.26.1...
15 36 5/09/2011 12:59:13.... WinGate NAT 248 Info 2 Authorisation failure: NAT STATUS: firewall block: TCP src 79.125.1...
16 38 5/09/2011 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.
t: 0, Console: 2, Replicate In: 0, Replicate Out: 0,
ht: 0
t: 451, Console: 5, Replicate In: 0, Replicate Out:
gent: 0
CPU Time Spent in mSeconds
150
125
100
75
50
25
0
15:34 15:44 15:54 16:04 16:14
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
15:29 15:34 15:39 15:44 15:49 15:54 15:59 16:04 16:09 16:14 16:19
Time
Managed and Unmanaged Computers
Managed Co...29%
Unmanaged ...71%
Generated 1 minute ago
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
0"
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"
Waiting for data... (interrupt to abort)

Решение: применение SIEM-системы

Принцип работы SIEM-системы

Эшелон
комплексная безопасность



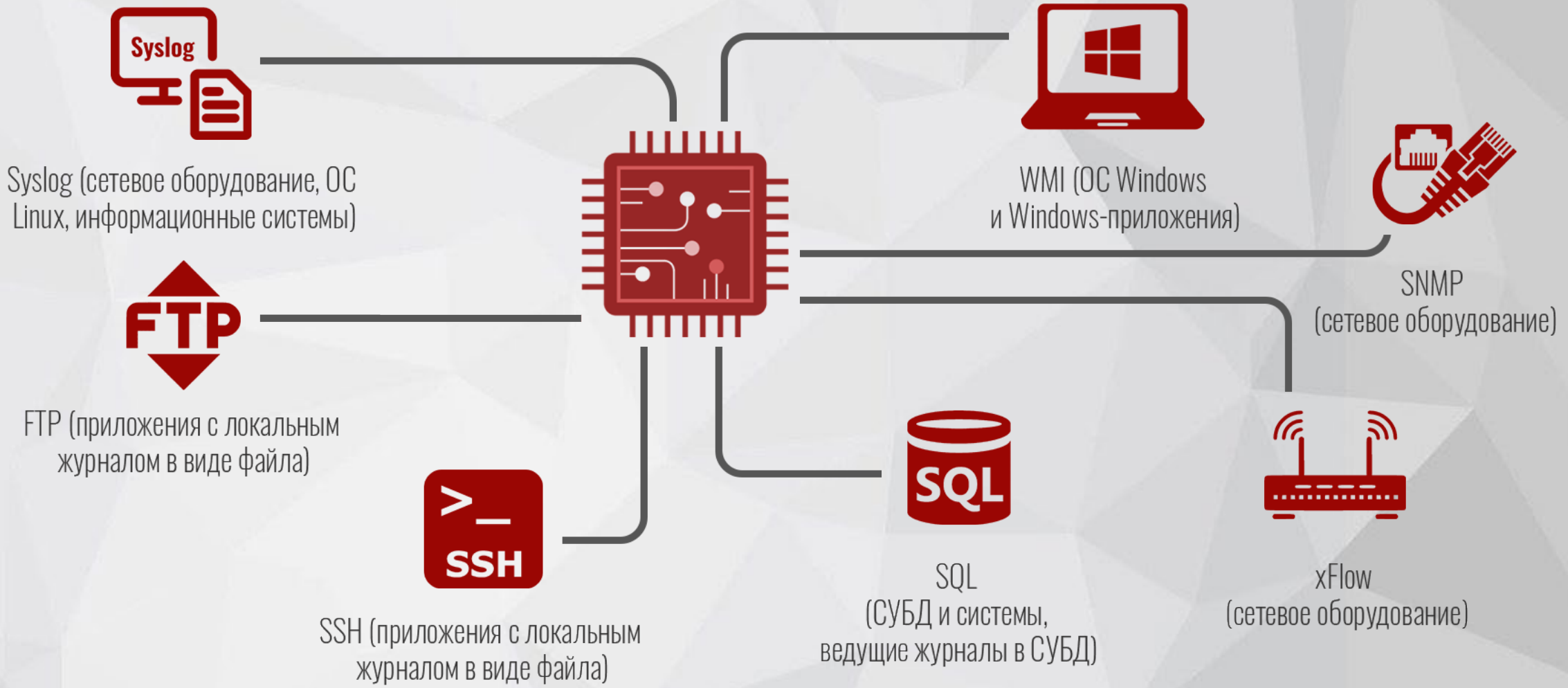
Ключевой функционал SIEM-системы

Эшелон
комплексная безопасность

1. Лог-менеджмент: сбор и хранение событий
2. Обработка событий:
   - нормализация
   - фильтрация
   - корреляция событий
   - ретро-поиск событий
3. Управление инцидентами
4. Механизмы уведомления
5. Автоматическое реагирование на инцидент
6. Интеграция с внешними системами API, передача инцидентов по CEF, интеграция с API Госсопка.

Протоколы сбора событий

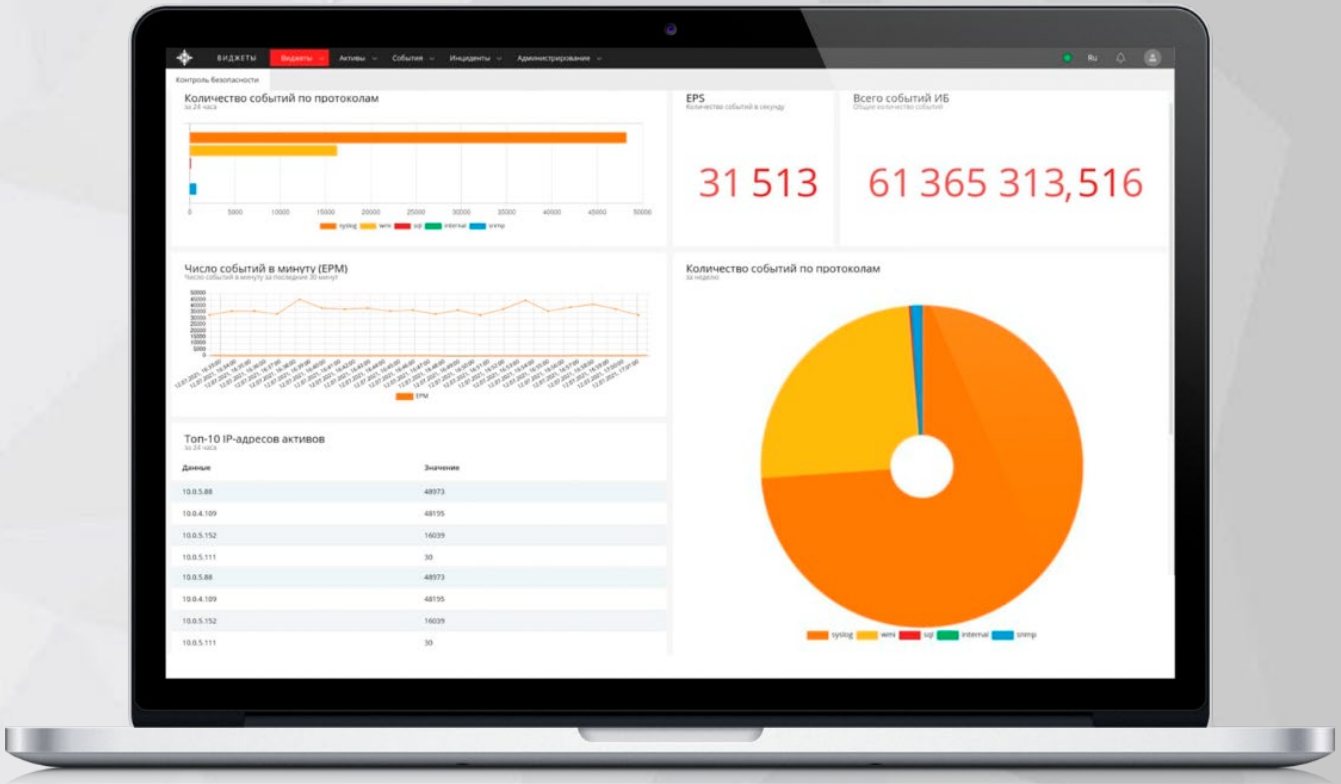
Эшелон
комплексная безопасность



KOMRAD Enterprise SIEM

Эшелон
комплексная безопасность

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



Отличительные особенности

Эшелон
комплексная безопасность

Высокая производительность и минимальные требования к аппаратному обеспечению

Поддерживаемые источники «из коробки»

Возможность подключения нестандартного источника событий

Возможности самостоятельной настройки системы

Способы оперативного оповещения об инциденте

Возможность автоматического реагирования на инциденты

ГОССОПКА
Обнаружение. Предупреждение. Ликвидация.

Возможность передачи инцидентов в систему ГосСОПКА

ASTRA LINUX

Дистрибутив под Astra Linux

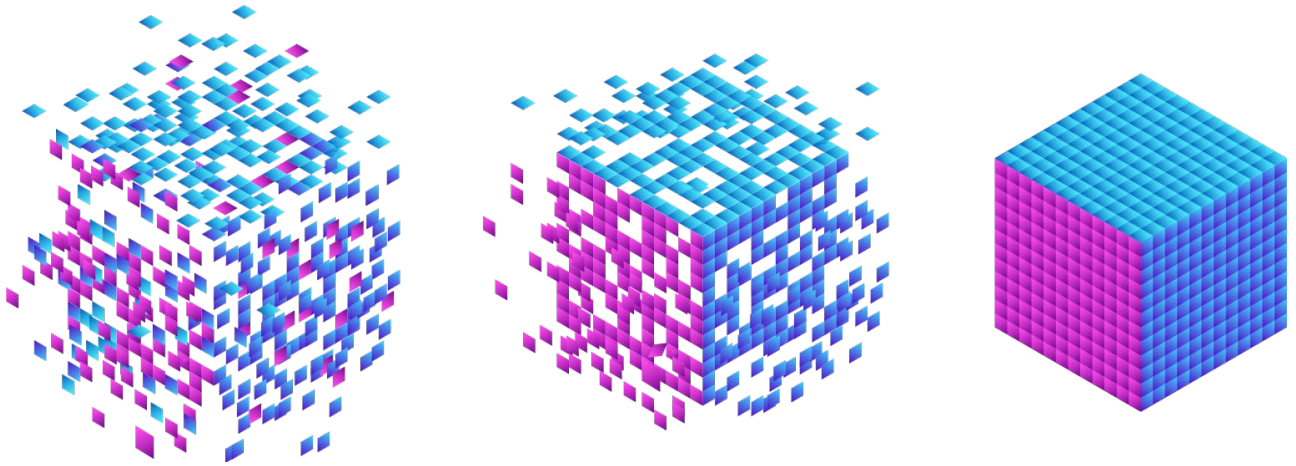
Комплексы анализа защищенности

- Ручной
- Автоматический, с помощью сканеров

Современный подход: использование агрегированной базы данных уязвимостей

Эшелон
комплексная безопасность

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



Что умеет Сканер-ВС 6

Эшелон
комплексная безопасность

Исследование сети

Сканирование сетевых узлов и сервисов, идентификация ОС и приложений, трассировка сетевых маршрутов для построения топологии сети

Инвентаризация

Использование активного подключения к исследуемому узлу для сбора информации

Поиск уязвимостей

Выявление уязвимостей программного обеспечения

Подбор паролей

Проверка стойкости паролей сетевых сервисов

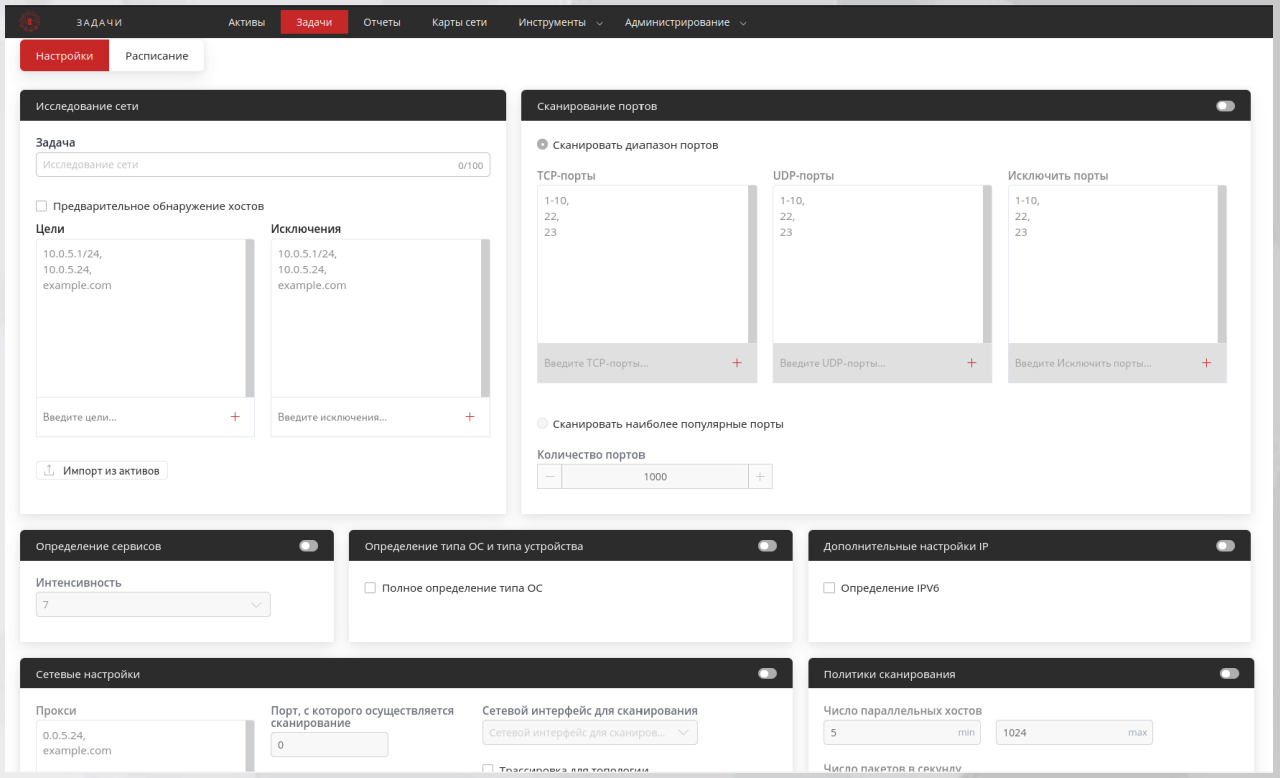
Аудит

Проверка настроек программного обеспечения на соответствие требованиям безопасности

Исследование сети

Эшелон
комплексная безопасность

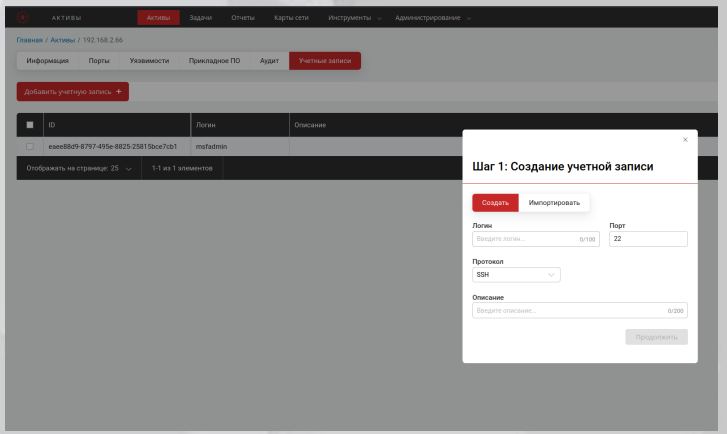
- Сканирование открытых портов
- Определение сетевых сервисов
- Трассировка для создания карты сети

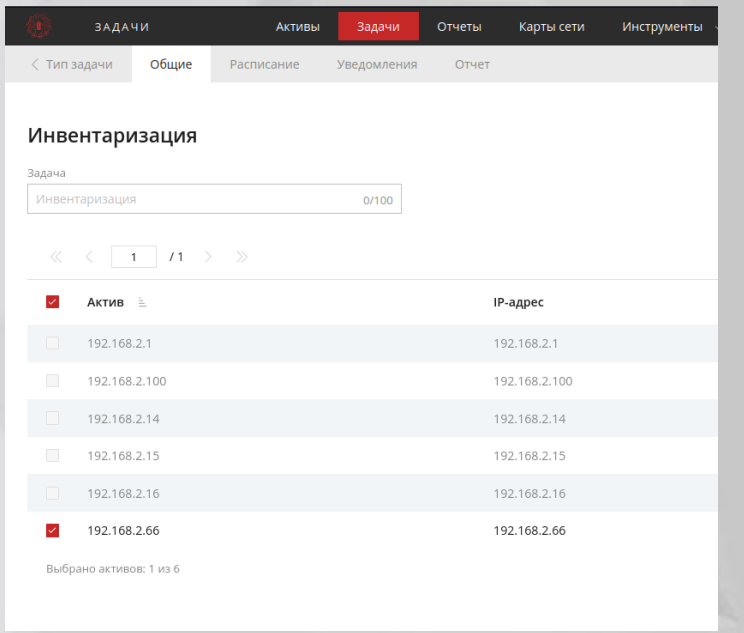


Инвентаризация

Эшелон
комплексная безопасность

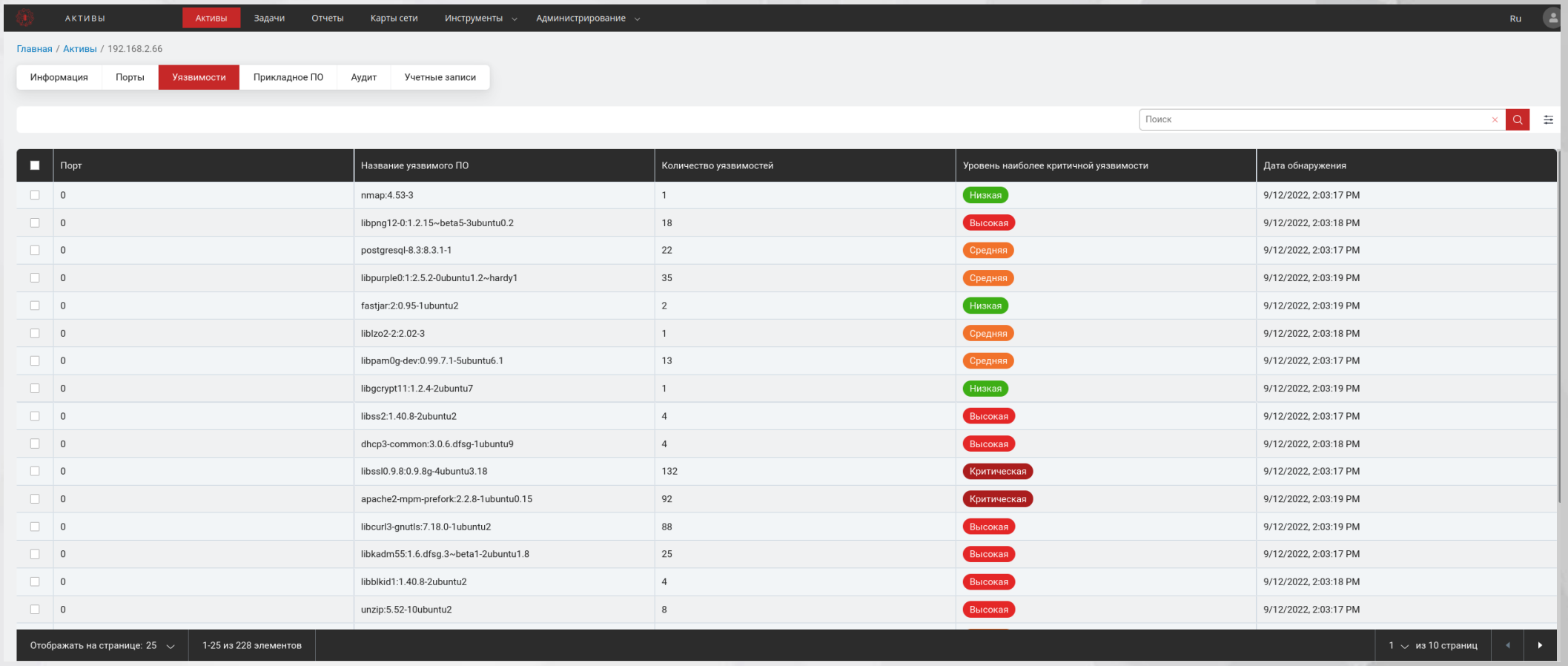
- Добавление учетной записи SSH/WinRM
- Подключение к машине под управлением Windows/Linux
- Выгрузка установленных пакетов ПО





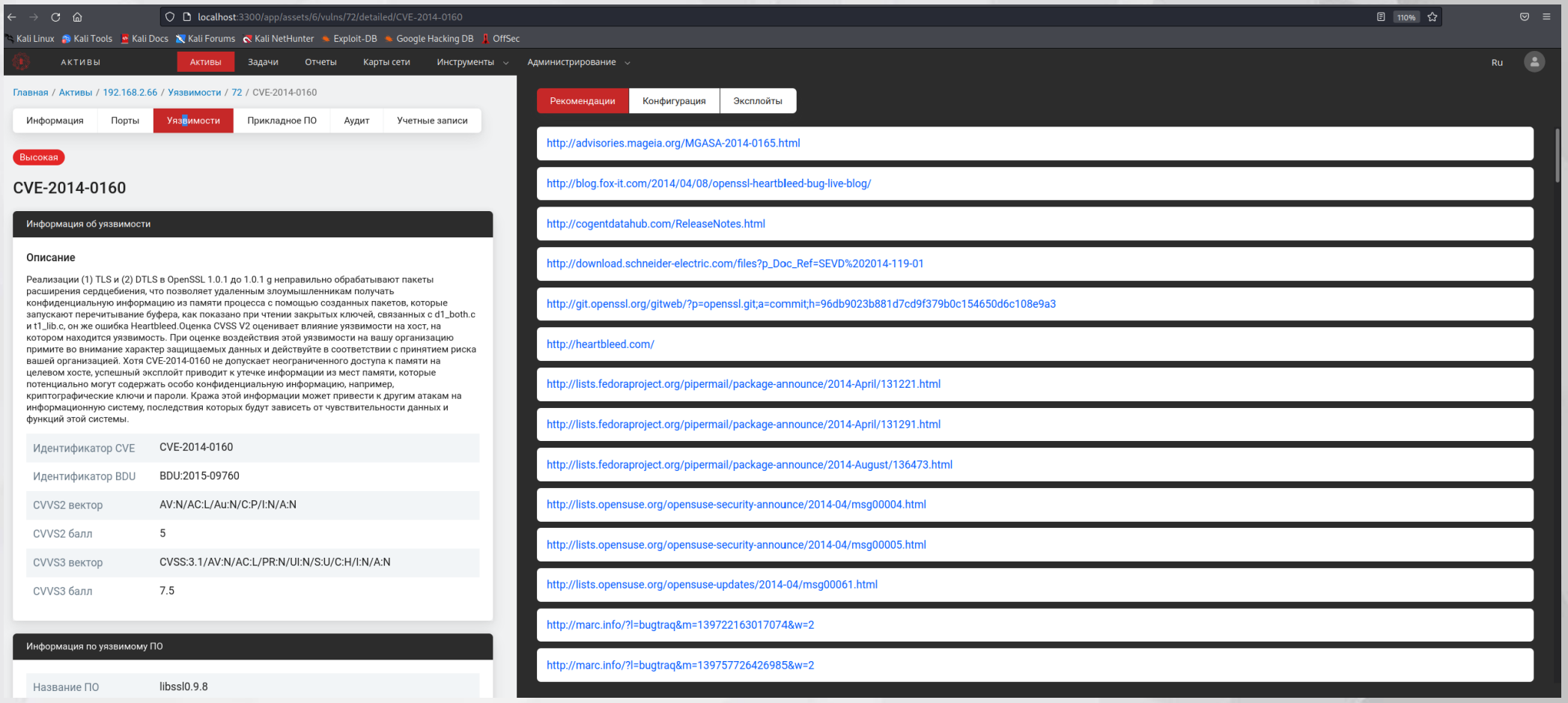
Поиск уязвимостей: список уязвимых пакетов

Эшелон
комплексная безопасность



Поиск уязвимостей: информация об уязвимости

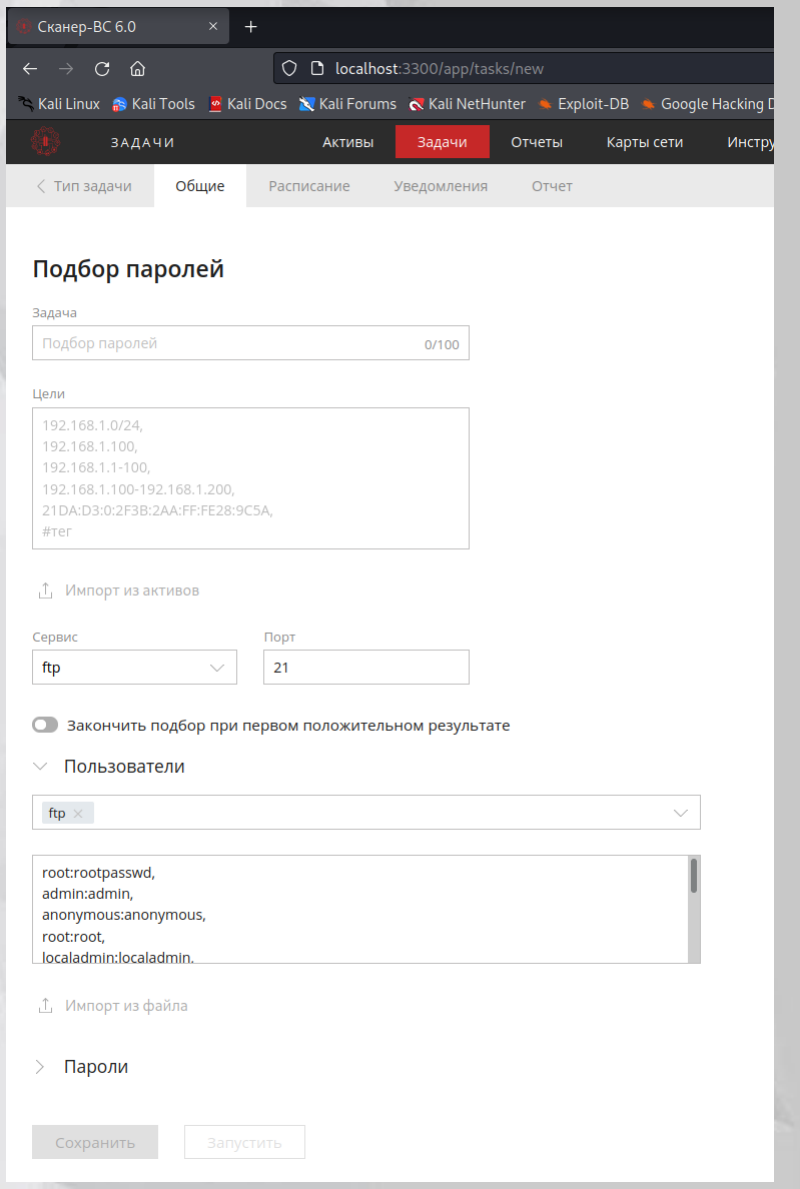
Эшелон
комплексная безопасность



Подбор паролей

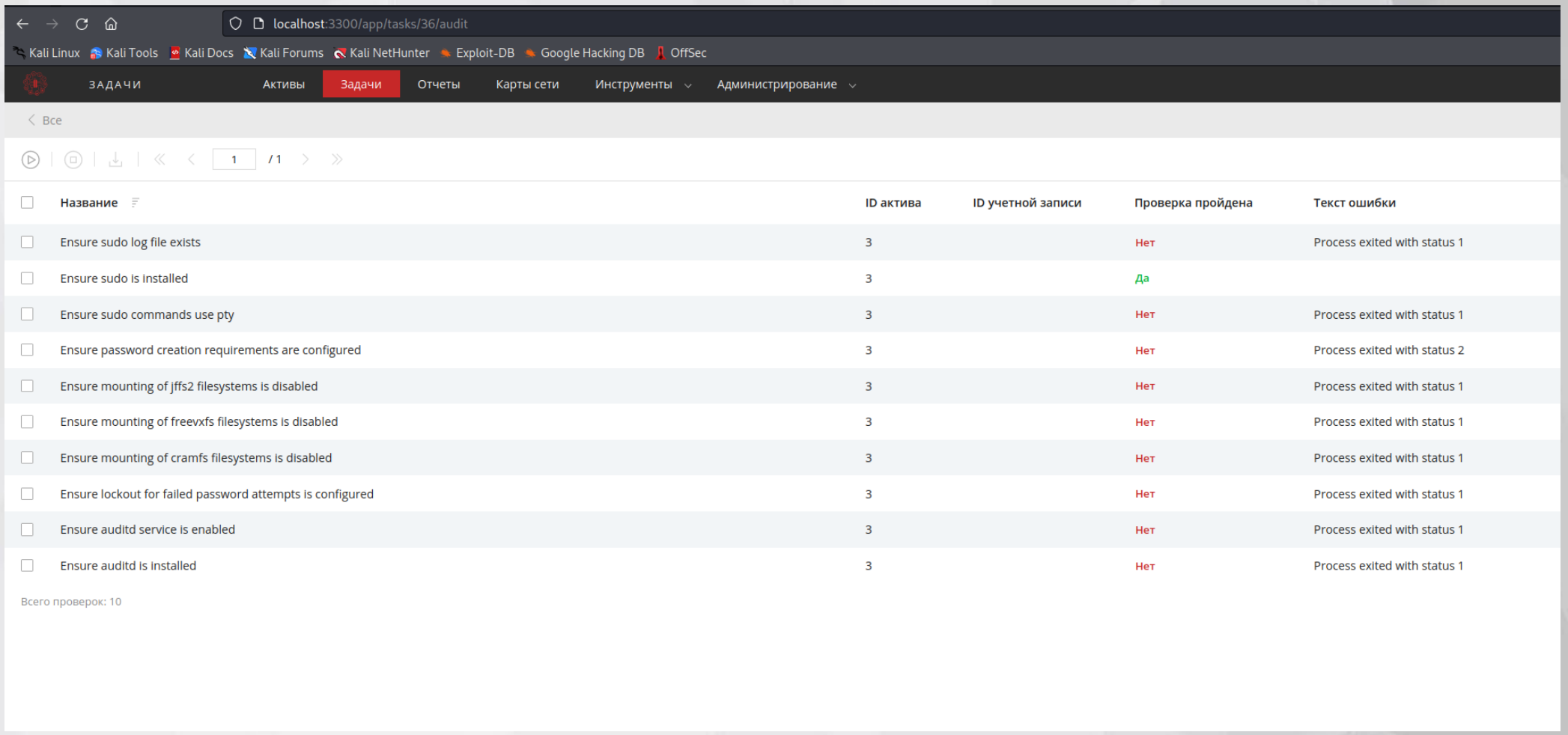
Эшелон
комплексная безопасность

- Поддерживаются все основные сетевые протоколы, требующие авторизации.
- Встроенные словари: самые распространенные пароли, цифры, имена, клавиатурные последовательности.
- Проверка пустых паролей, паролей, совпадающих с логином, пароля, совпадающего с логином в обратном порядке



Аудит настроек безопасности

Эшелон
комплексная безопасность

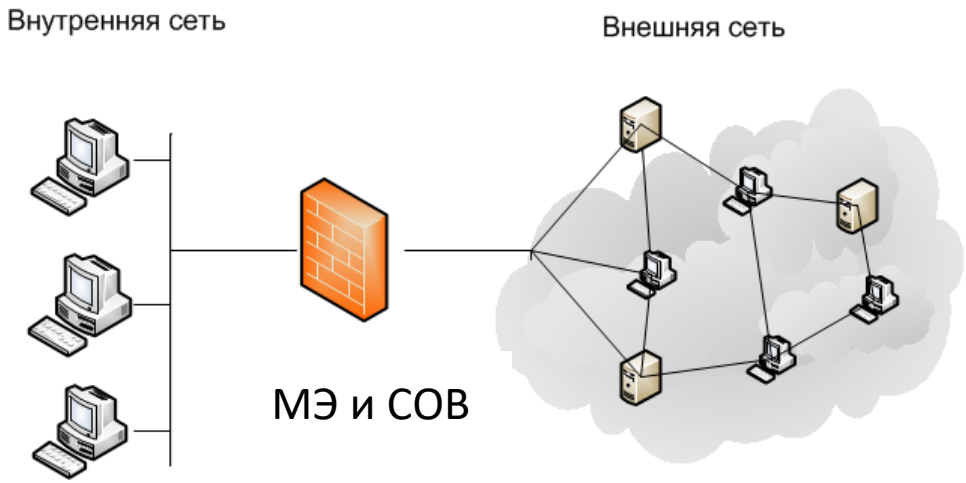


Название	ID актива	ID учетной записи	Проверка пройдена	Текст ошибки
Ensure sudo log file exists	3		Нет	Process exited with status 1
Ensure sudo is installed	3		Да	
Ensure sudo commands use pty	3		Нет	Process exited with status 1
Ensure password creation requirements are configured	3		Нет	Process exited with status 2
Ensure mounting of jffs2 filesystems is disabled	3		Нет	Process exited with status 1
Ensure mounting of freevxfs filesystems is disabled	3		Нет	Process exited with status 1
Ensure mounting of cramfs filesystems is disabled	3		Нет	Process exited with status 1
Ensure lockout for failed password attempts is configured	3		Нет	Process exited with status 1
Ensure auditd service is enabled	3		Нет	Process exited with status 1
Ensure auditd is installed	3		Нет	Process exited with status 1

Всего проверок: 10

Программно-аппаратный комплекс «Рубикон»

Эшелон
комплексная безопасность



РУБИКОН

Программно-аппаратный комплекс «Рубикон» объединяет функции маршрутизатора, межсетевого экрана типа «А» и типа «Б» второго класса защиты и системы обнаружения вторжений уровня сети второго класса защиты. ПАК «Рубикон» может использоваться в автоматизированных системах военного назначения для обработки информации, содержащей сведения, составляющие государственную тайну и имеющие степень секретности не выше «совершенно секретно».

Программно-аппаратный комплекс «Рубикон»

Эшелон
комплексная безопасность

1. Мини
2. Защищенный
3. 1U
4. Высокопроизводительный
5. Мультипортовый

Технические характеристики

Эшелон
комплексная безопасность

Форм-фактор	Производительность МЭ	Производительность СОВ	Сетевые интерфейсы
МИНИ 	до 2 Gbit/s	до 1,6 Gbit/s	6xGbE Ethernet 100/1000 RJ45
1U 	до 5 Gbit/s	до 3 Gbit/s	6xGbE Ethernet 100/1000 RJ45 (+1 модуль расширения)
ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ 	до 9 Gbit/s	до 3 Gbit/s	4 модуля расширения
МУЛЬТИПОРТОВЫЙ 	до 6 Gbit/s	до 2.5 Gbit/s	8 модулей расширения
ЗАЩИЩЕННЫЙ 	до 600 Mbit/s	до 400 Mbit/s	4xEthernet 100/1000 Base-T

Комплекс «Рубикон» доступен в различных форм-факторах, применимых для встроенного и настольного использования, а также для монтирования в стандартную 19” стойку.

NTA-система eSensor: сенсор

Эшелон
комплексная безопасность

1. Сигнатурный анализ
2. Эвристический анализ
3. Запись трафика
4. Разбор трафика
5. Передача событий

Выводы

Эшелон
комплексная безопасность

- Российские центры мониторинга информационной безопасности играют ключевую роль в отражении атак на критическую информационную инфраструктуру.

- Основой центров помимо профессиональных команд и выстроенных процессов являются современные отечественные решения по мониторингу событий информационной безопасности (SIEM), анализа защищенности (VA) и обнаружения атак в сетевом трафике (NTA/NDR/IDS).

СПАСИБО ЗА ВНИМАНИЕ!

Эшелон
комплексная безопасность

Вадим Пучкин
Руководитель направления по работе с партнерами
АО «НПО «Эшелон»
моб.+7 (985) 225 67 68
v.puchkin@npo-echelon.ru
https://npo-echelon.ru/