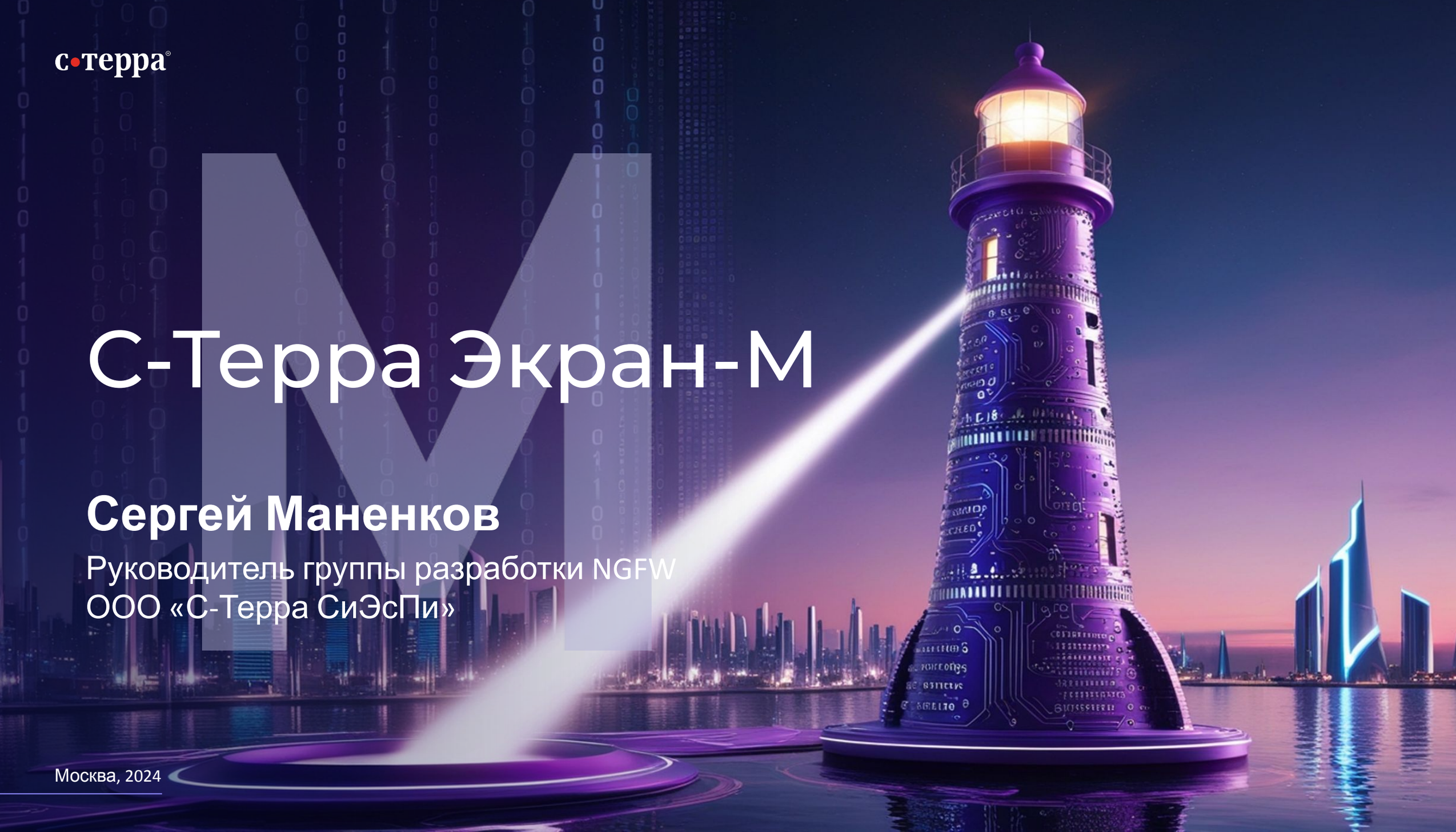


С-Терра Экран-М

Сергей Маненков

Руководитель группы разработки NGFW

ООО «С-Терра СиЭсПи»

Москва, 2024

ЧТО МЫ ПРЕДЛАГАЕМ РЫНКУ И ЧЕМ МЫ ЛУЧШЕ

[АРХИТЕКТУРА]

- разработана с нуля в 2023–2024 г.
- создавалась под требования ФСТЭК

[МОДУЛЬНОСТЬ]

- интеграции с внешними системами
- гибкое изменение состава модулей

[СЕРТИФИКАЦИЯ]

- ФСТЭК по профилю защиты многофункци-
  ональных межсетевых экранов уровня сети четвертого класса защиты.
- российская разработка под ОС Astra Linux

[ОПЫТ]

- существующие решения С-Терра
- экспертиза и компетенции компании с 20 летним опытом работы на рынке ИБ

[ПРОИЗВОДИТЕЛЬНОСТЬ]

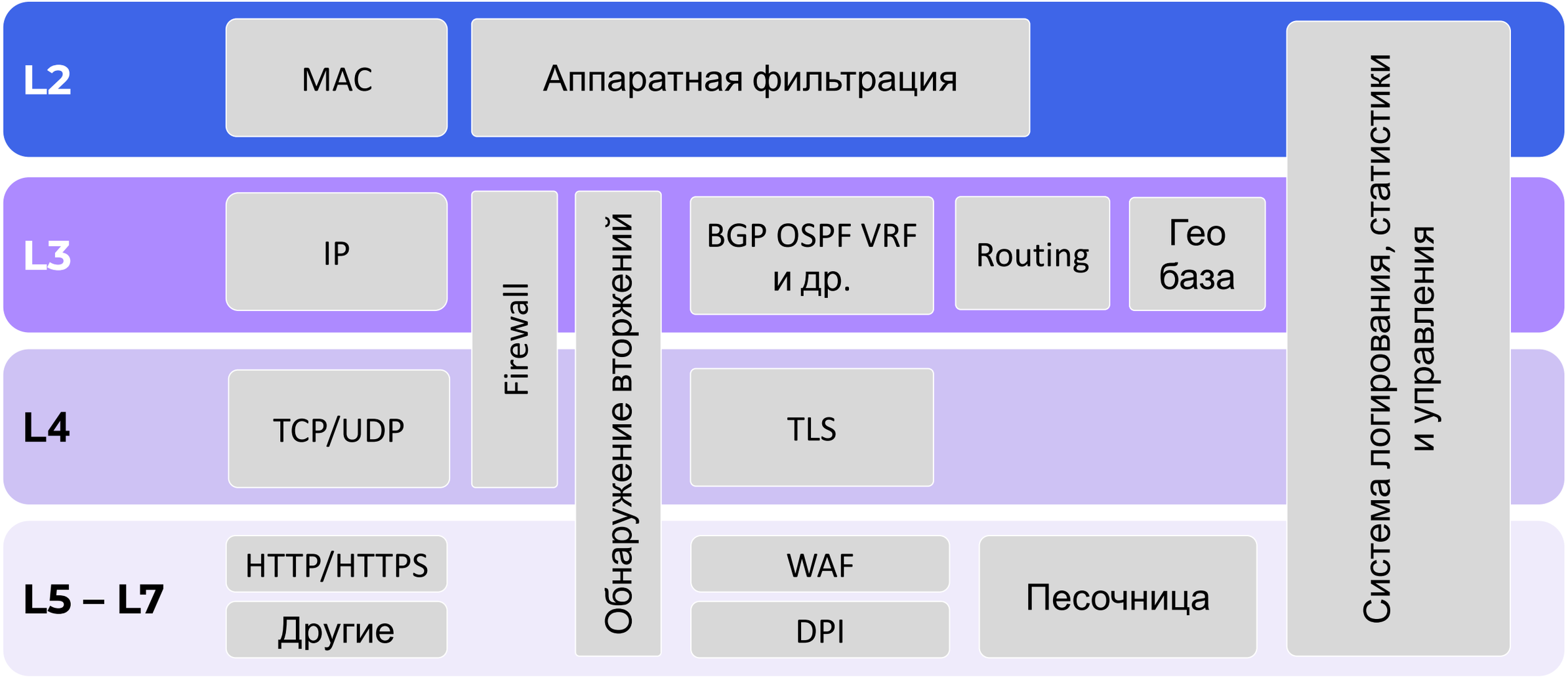
- обработка трафика вынесена за пределы ядра в пользовательское пространство. Взаимодействие с сетевой картой напрямую.
- технологии DPDK и VPP

Режим работы	Пропускная способность на один канал	Количество правил
FW + Statfull	80 Гбит/с	10 тыс.
FW + IDS/IPS	до 15 Гбит/с	40 тыс.
FW + IDS/IPS + WAF	до 10 Гбит/с	60 тыс.
FW + IDS/IPS + DPI + WAF + Antivirus + SandBox	до 2.5 Гбит/с	150 тыс.

Характеристики и состав потока трафика на примере режима FW + IDS/IPS:

СТРУКТУРА С-ТЕРРА ЭКРАН-М

ЭКРАН·М многофункциональный модульный межсетевой



ОПТИМИЗАЦИЯ ЖУРНАЛИРОВАНИЯ: СРАВНЕНИЕ

ЭКРАН·М ногофункциональный одульный ежсетевой

Показатель	S-terra log	Logstash
Средняя загрузка всех CPU	4.5 %	30.2%
Количество загруженных CPU	1	12-14
Использование физической памяти	1.1 %	8.1%
Занимаемое место на диске elasticsearch (индекс *stat)	3,225 kb	6,854 kb
Занимаемое место на диске elasticsearch (индекс *alert)	0,241 kb	3,7685 kb
Занимаемое место на диске elasticsearch (индекс *other)	0,160 kb	2,972 kb

ЭКРАН•М

Информационная панель

srmkv Sterra 99+

- Информационная Панель
- Конфигурация
- Пользователи
- Мониторинг
- Сервисы
- Правила Трафика
- Отчеты И Журналы
- Внешние Системы
- Песочница
- Антивирус (ClamAV)
- Расширенное Логирование

Оповещения систем

Данные WAF за 1 месяц Отобразить Очистить

Песочница

Всего: 39

Опасное ПО	Потенциально опасное ПО	Угроз не обнаружено
11	0	28

COB

Всего: 61436

Критический	Высокий	Средний	Низкий	Уведомление
58608	2828	0	0	0

WAF

Всего: 852

Критический	Ошибка	Предупреждение	Уведомление	Информация
158	0	655	39	0

Антивирус (ClamAV)

Всего: 6320

Вирус	Угроз не обнаружено
3978	2342

Состояние модулей

COB Отключен	Контроль приложений Отключен	WAF Отключен
Маршрутизация Работает	Прокси	Аппаратная фильтрация
Логирование	Песочница Работает	Антивирус (ClamAV) Работает
DLP	SIEM	Firewall Работает

Службы

Информация о системе

Модель Model-1S

Сетевая информация

Хосты

ЭКРАН•М

Учетные записи

srmkv Sterra 99+

- Информационная Панель
- Конфигурация
- Пользователи
  - Учетные Записи
  - Авторизация
  - VPN Подключения
  - Профили Устройств
  - RADIUS
  - Обнаруженные Устройства
- Мониторинг
- Сервисы
- Правила Трафика
- Отчеты И Журналы
- Внешние Системы
- Песочница
- Антивирус (ClamAV)
- Расширенное Логирование

Логин | Поиск | Новый пользователь | Управление ролями

Логин	E-mail	Роль	Последний вход	Блокировка
Denis	d.user2@yandex.ru	Sterra		
admin_2	anton198512@mail.ru	Sterra		
arabotinsky	arabotinsky@s-terra.ru	Sterra		
ashiryaev	ashiryaev@s-terra.ru	Sterra		
asuhov	hikuro@mail.ru	Администратор ММЭ		

Пользователей на странице: 5 1-5 из 12

События

Очистить журнал событий

Дата изменения | Поиск

Дата изменения	Действие	Объект	Администратор
23.09.2024 12:16:14	Для роли установлены отображаемые события безопасности	Администратор безопасности	asuhovIB

Информационная Панель
Конфигурация
Пользователи
Мониторинг
Сервисы
Правила Трафика
СОВ
Правила
Данные
NAT
Firewall
Контроль Приложений
WAF
Geo IP
Ограничение Скорости
Антивирус Веб-Трафика
Исключения
Квоты
Отчеты И Журналы
Трафик

Поиск источника

Интерфейс (по-умолчанию vpp0):

Отключен | Применить правила | Добавить

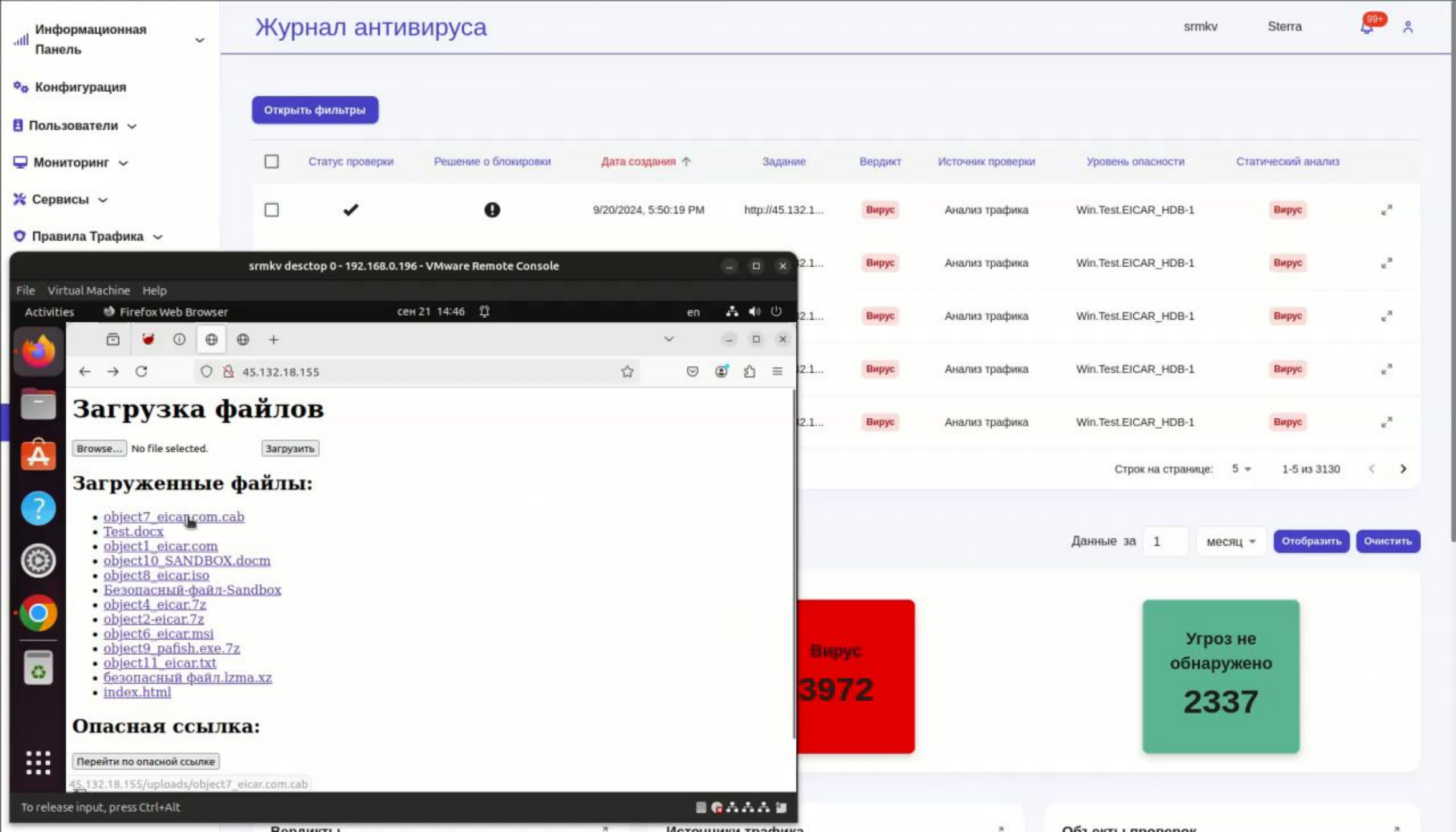
Название	URI	Последнее обновление	Логин	Категории	Правила
Ptsecurity-Attack	https://aasystem.ru/rules/ptsecurity-attack.rules	9/23/2024, 1:13:55 PM	srmkv	1	1841

Поиск категории

Название	Время создания	Последнее обновление	Логин
Ptsecurity-Attack	9/18/2024, 2:04:48 PM	9/23/2024, 1:13:55 PM	srmkv

Поиск правила

SID	Логин	Сообщение	Изменено
10000001	srmkv	Alert Http Any Any -> Any Any (Msg: "ATTACK [PTsecurity] Easy File Sharing 7.2 SEH Overflow";Urilen:...	9/23/2024, 1:13:55 PM
10000002	srmkv	Alert Udp $EXTERNAL_NET Any -> $HOME_NET Any (Msg: "ATTACK [PTsecurity] Possible Kamailio < 4.3.4 Ex...	9/18/2024, 2:04:48 PM
10000003	srmkv	Alert Http Any Any -> Any Any (Msg: "ATTACK [PTsecurity] Sysax < 6.51 Post Authentification Exploita...	9/18/2024, 2:04:48 PM
10000007	srmkv	Alert Dns $EXTERNAL_NET Any -> $HOME_NET Any (Msg: "ATTACK [PTsecurity] Attempt To Double SIT Option...	9/18/2024, 2:04:48 PM


Информационная Панель
Конфигурация
Пользователи
Мониторинг
Сервисы
Правила Трафика
Журнал антивируса
srmkv
Sterra
Открыть фильтры
Статус проверки
Решение о блокировки
Дата создания
Задание
Вердикт
Источник проверки
Уровень опасности
Статический анализ
9/20/2024, 5:50:19 PM
http://45.132.1...
Вирус
Анализ трафика
Win.Test.EICAR_HDB-1
Строк на странице: 5
1-5 из 3130
Данные за 1 месяц
Отобразить
Очистить
Вирус 3972
Угроз не обнаружено 2337
srmkv desctop 0 - 192.168.0.196 - VMware Remote Console
File Virtual Machine Help
Activities
Firefox Web Browser
сен 21 14:46
en
45.132.18.155
Загрузка файлов
Browse...
No file selected.
Загрузить
Загруженные файлы:
object7_eicar.com.cab
Test.docx
object1_eicar.com
object10_SANDBOX.docm
object8_eicar.iso
Безопасный-файл-Sandbox
object4_eicar.7z
object2-eicar.7z
object6_eicar.msi
object9_pafish.exe.7z
object11_eicar.txt
безопасный файл.lzma.xz
index.html
Опасная ссылка:
Перейти по опасной ссылке
45.132.18.155/uploads/object7_eicar.com.cab
To release input, press Ctrl+Alt

События безопасности

Настроить Выгрузить

События администрирования

Действия администраторов

Время изменения | Поиск

Время изменения	Модуль	Событие	Пользователь
2024-09-23T12:16:14+03:00	Пользователи ММЭ	Для роли установлены отображаемые события безопасности	asuhovIB
2024-09-23T12:03:18+03:00	Пользователи ММЭ	Для роли установлены отображаемые события безопасности	asuhovIB
2024-09-23T12:03:11+03:00	Пользователи ММЭ	Для роли установлены отображаемые события безопасности	asuhovIB
2024-09-23T11:53:21+03:00	Пользователи ММЭ	Для роли установлены отображаемые события безопасности	asuhovIB
2024-09-23T10:14:42+03:00	СОВ	Обновление источника	srmkv

Элементов на странице: 5 1 - 5 из 402

События обнаружения компьютерных атак

События безопасности СОВ

Время | Поиск

Время	ID	Сообщение	Тип атаки	Вердикт	IP-клиента	IP-хоста
2024-09-19T12:01:33+03:00	10003587	TOOLS [PTsecurity] DNSCAT2 Activity	Exploitation Attributes was Detected	1	16.0.0.208	48.0.3.205

ДОРОЖНАЯ КАРТА

Январь 2024
Устранение замечаний к прототипу

Март 2024
Реализация функций потокового антивируса

Май 2024
Реализация функционала DPI

Июль 2024
Реализация функций песочницы, доверенной загрузки.

Сентябрь 2024
Выпуск 1-го релиз-кандидата удовлетворяющего требованиям ФСТЭК

Октябрь 2024
Устранение замечаний

Ноябрь 2024
Подача документов на сертификацию ФСТЭК

Декабрь 2024
Разрешение ФСТЭК приступить к сертификации

2025
Получение сертификата ФСТЭК, старт продаж


с•терра®
Ваш ориентир в мире безопасности
СПАСИБО ЗА ВНИМАНИЕ!
Сергей Маненков
Руководитель группы разработки NGFW
ООО «С-Терра СиЭсПи»
Москва, 2024