

JET CSIRT

Использование продуктов Fortinet в коммерческом CSIRT

20/09/2018

Алексей
Мальнев

Руководитель Jet CSIRT компании «Инфосистемы Джет»
ay.malnev@msk.jet.su / +7 985 849-89-33

SECURITYDAY

СОДЕРЖАНИЕ

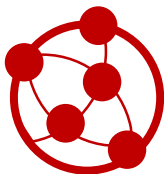
1. Введение. Обзор FortiSIEM
2. Что такое Jet CSIRT
3. Как мы строили Jet CSIRT
4. Roadmap



FortiSIEM

**Универсальная система корреляции и
управления событиями ИБ**

FortiSIEM – Ключевые функции



Обнаружение и учет активов

- Всесторонне и точно
- Контекстная оценка активов
- Оценка уязвимостей



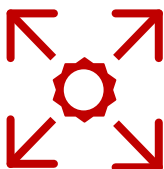
Масштабируемость, быстрая интеграция

- Поддержка собственных (custom) устройств
- Масштабируемая архитектура



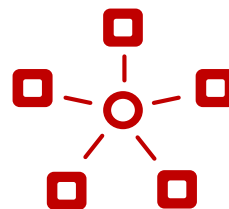
Автоматизация

- Реакция на инциденты ИБ
- Управление заявками
- Автоматизация противодействия



Единая панель управления

- Единый интерфейс управления (GUI)
- Объединение функций NOC & SOC



Унифицированная платформа

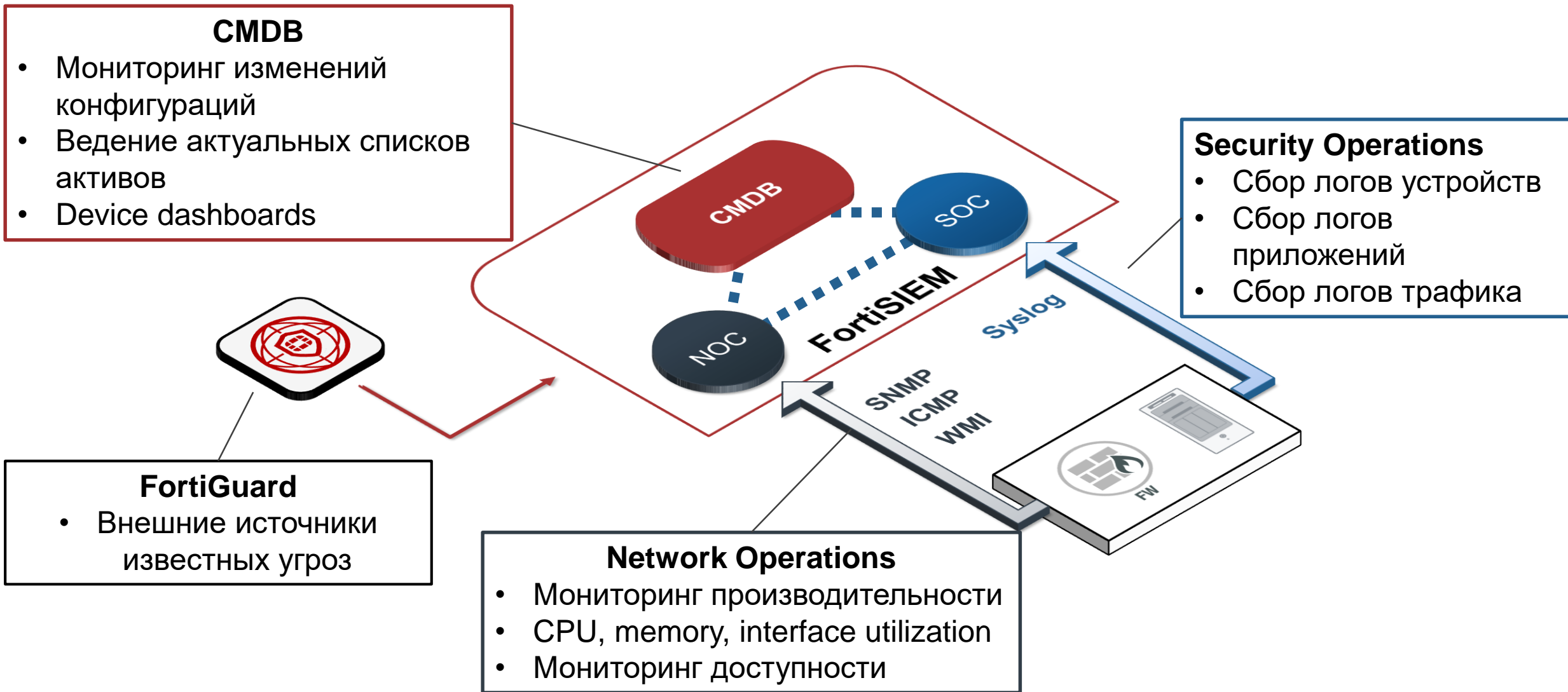
- Multi-tenancy
- Ролевая модель доступа (RBAC)



FortiGuard

- FortiGuard threat feed
- Domain, IP and URL IOCs

Объединение NOC & SOC – единая точка управления





ЧТО ТАКОЕ JET CSIRT?



Нормативная база



Выстраивание процессов



Команда и роли в ней



РС БР ИББС-2.5-2014

Технологии и архитектура



Метрики и оценка зрелости



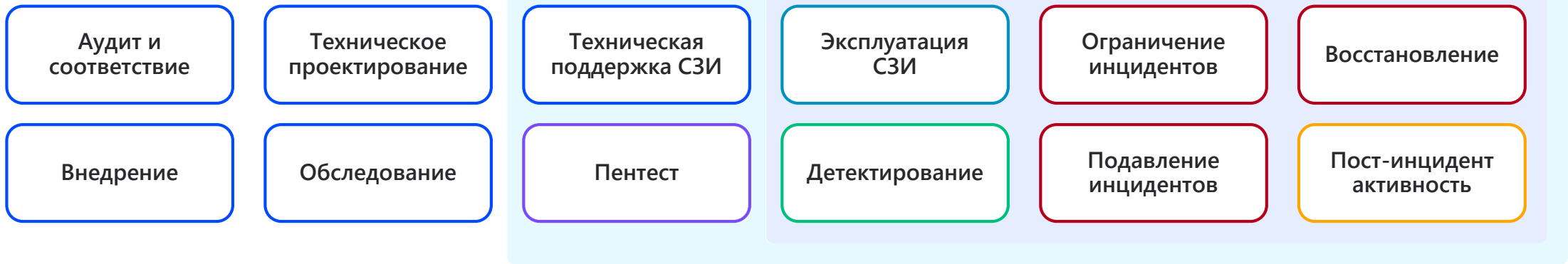
Соответствие

№187-ФЗ, ПП-79/541, СТО БР ИББС-1.0-2014

Jet CSIRT в составе услуг Центра Информационной безопасности



Аутсорсинг ИБ

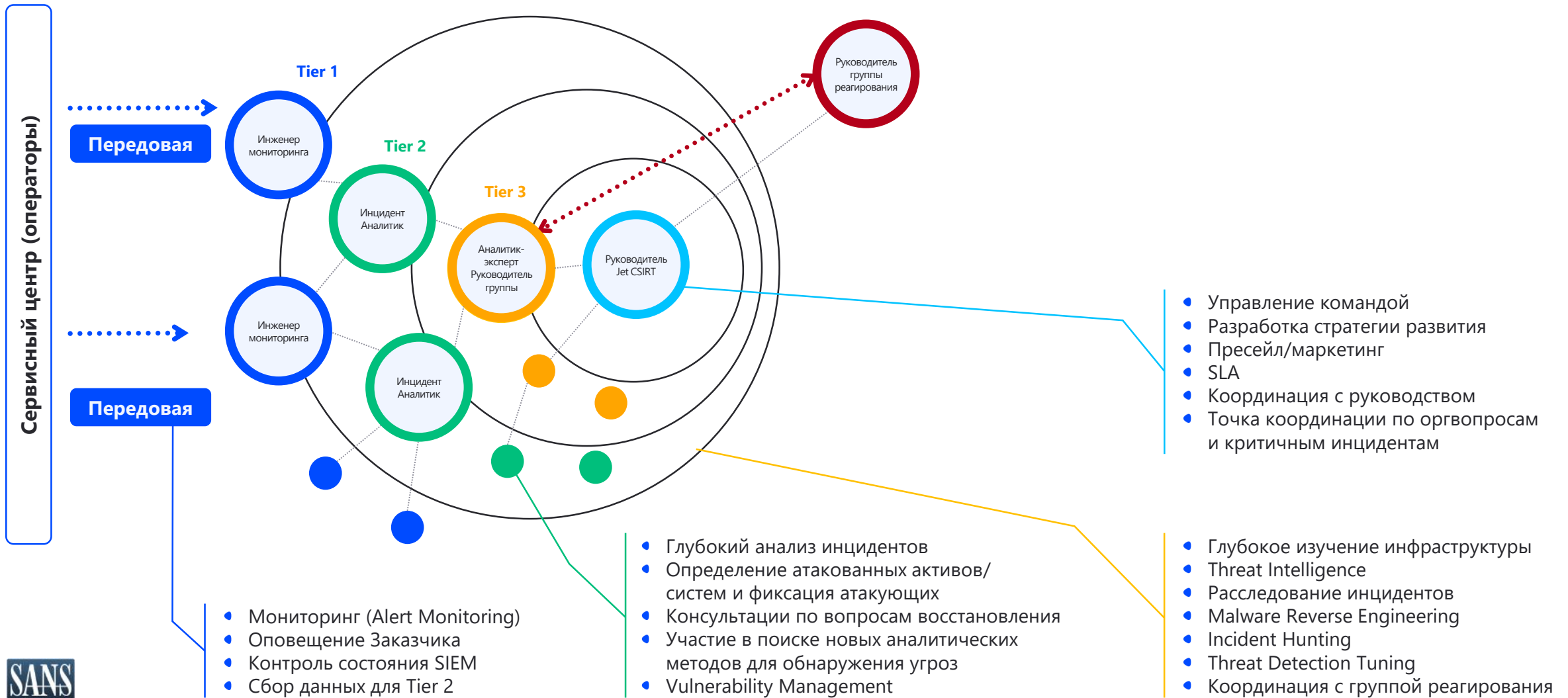


ЦИБ

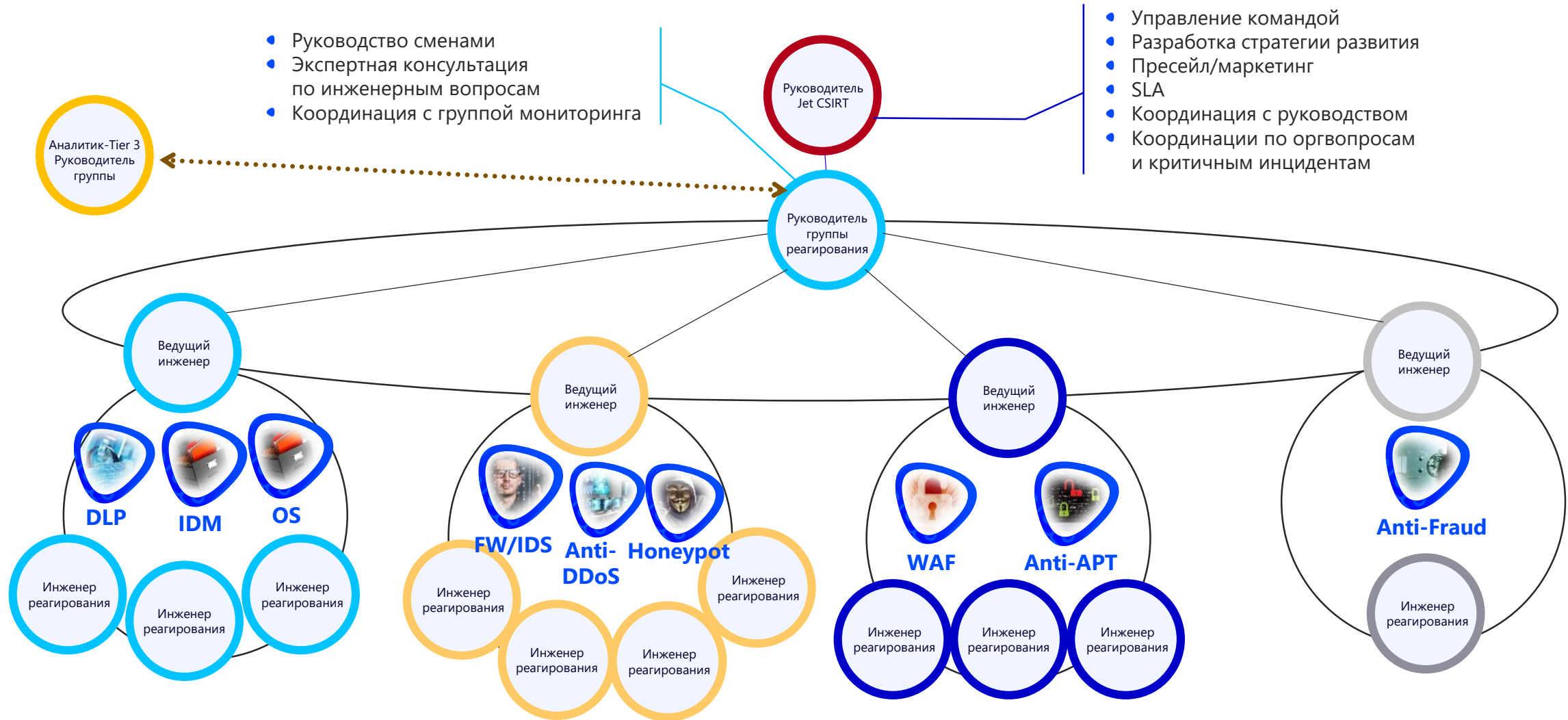
Команда Jet CSIRT. Оргструктура



Команда Jet CSIRT. Группа мониторинга



Команда Jet CSIRT. Группа реагирования



Опции Jet CSIRT



Премиум

Стандартный

Базовый

Мониторинг событий ИБ

Подключение источников событий

Расследование инцидентов ИБ

Кибераналитика по внешним угрозам

Управление уязвимостями

Разработка уникальных сценариев выявления инцидентов

Техническое реагирование
Сдерживание и нейтрализация

Проактивный поиск и обнаружение угроз

Эксплуатация СЗИ

Предоставление СЗИ по подписке

Управление жизненным циклом инцидента (IRP Jet Signal)

Изучение вредоносного кода

Аналитика по открытым данным (OSINT)

Бизнес-ориентированная аналитика

Комплексное ИБ консультирование

Аудит и анализ защищенности

Форензика

Схема подключения Jet CSIRT. Вариант 1

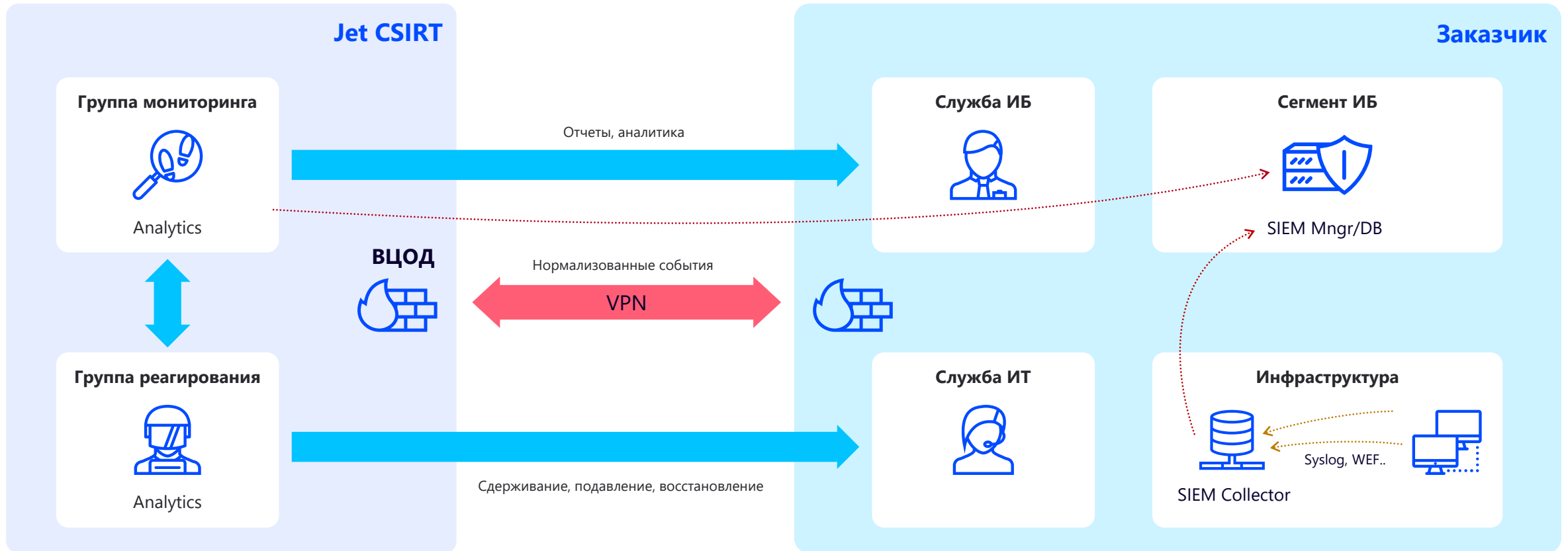
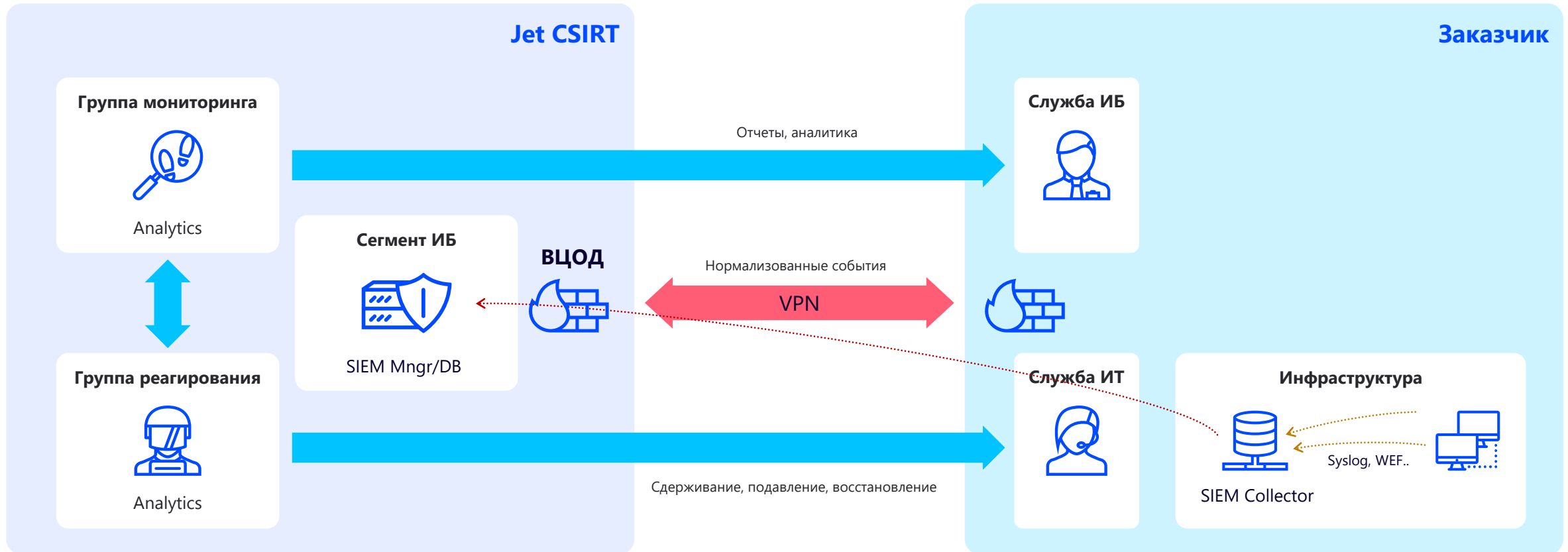


Схема подключения Jet CSIRT. Вариант 2



Инструменты Jet CSIRT



Источники данных (телеметрия)

Сетевая инфраструктура

Серверы

Рабочие станции

Приложения

Средства защиты информации

Базы данных

Мониторинг

FORTINET®

POSITIVE TECHNOLOGIES

MICRO FOCUS

IBM®

splunk >

McAfee
Together is power.

Управление жизненным циклом инцидента

JETSIGNAL

bmc Remedy

Средства реагирования

FORTINET®

CISCO

paloalto

McAfee
Together is power.

Check Point
SOFTWARE TECHNOLOGIES LTD.

POSITIVE TECHNOLOGIES

Dozor

IMPERVA

INFOWATCH®

KASPERSKY lab

radware

ARBOR NETWORKS

SKYBOX SECURITY

Средства визуализации

Qlik Q®

Sense™



КАК МЫ СТРОИМ JET CSIRT



Почему Fortinet?



Технологии



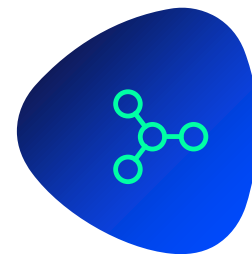
Перспективы
сертификации ФСТЭК



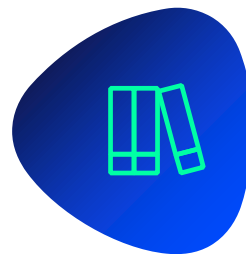
Гибкая ценовая политика



Представительство
в РФ и техподдержка



Экосистема ИБ продуктов



Обилие технической документации

Выбор инструментов Jet CSIRT. SIEM



FORTINET

splunk >

Radar

POSITIVE TECHNOLOGIES

Arcsight

McAfee

Техническое сравнение SIEM для Jet CSIRT

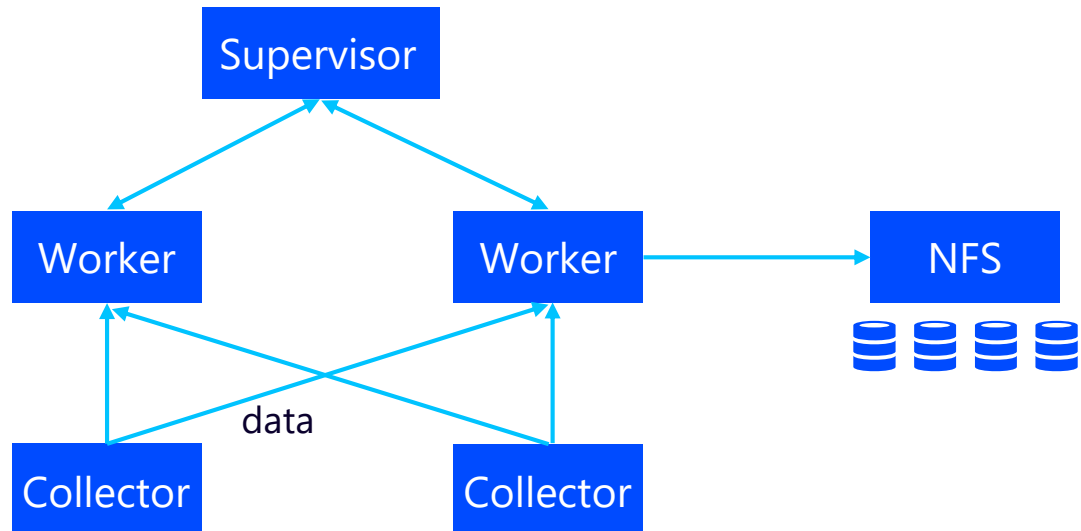


	POSITIVE TECHNOLOGIES	McAfee Together is power.	ArcSight	Radar	FORTINET	splunk
Архитектура	Green	Green	Green	Green	Green	Green
Масштабируемость	Yellow	Green	Green	Green	Green	Green
Отказоустойчивость	Red	Green	Green	Green	Yellow	Green
Ролевая модель	Red	Green	Green	Green	Green	Green
Интеграция с ticket, TI, IRP, AD	Green	Green	Green	Green	Green	Green
Работа с парсерами и правилами	Green	Yellow	Green	Green	Green	Green
Гибкость фильтров/листов	Green	Yellow	Green	Green	Yellow	Green
Механизмы оповещения и отчетности	Green	Green	Green	Green	Green	Green
Тикетная система	Green	Green	Green	Green	Green	Green
Работа с сырыми событиями	Yellow	Green	Green	Green	Green	Green
Механизмы корреляции	Red	Green	Green	Green	Green	Green
Механизмы нормализации	Green	Green	Green	Green	Green	Green
Ассетная модель	Green	Yellow	Yellow	Yellow	Green	Yellow
Удобство управления	Yellow	Green	Green	Yellow	Green	Green

Полезные для CSIRT возможности FortiSIEM

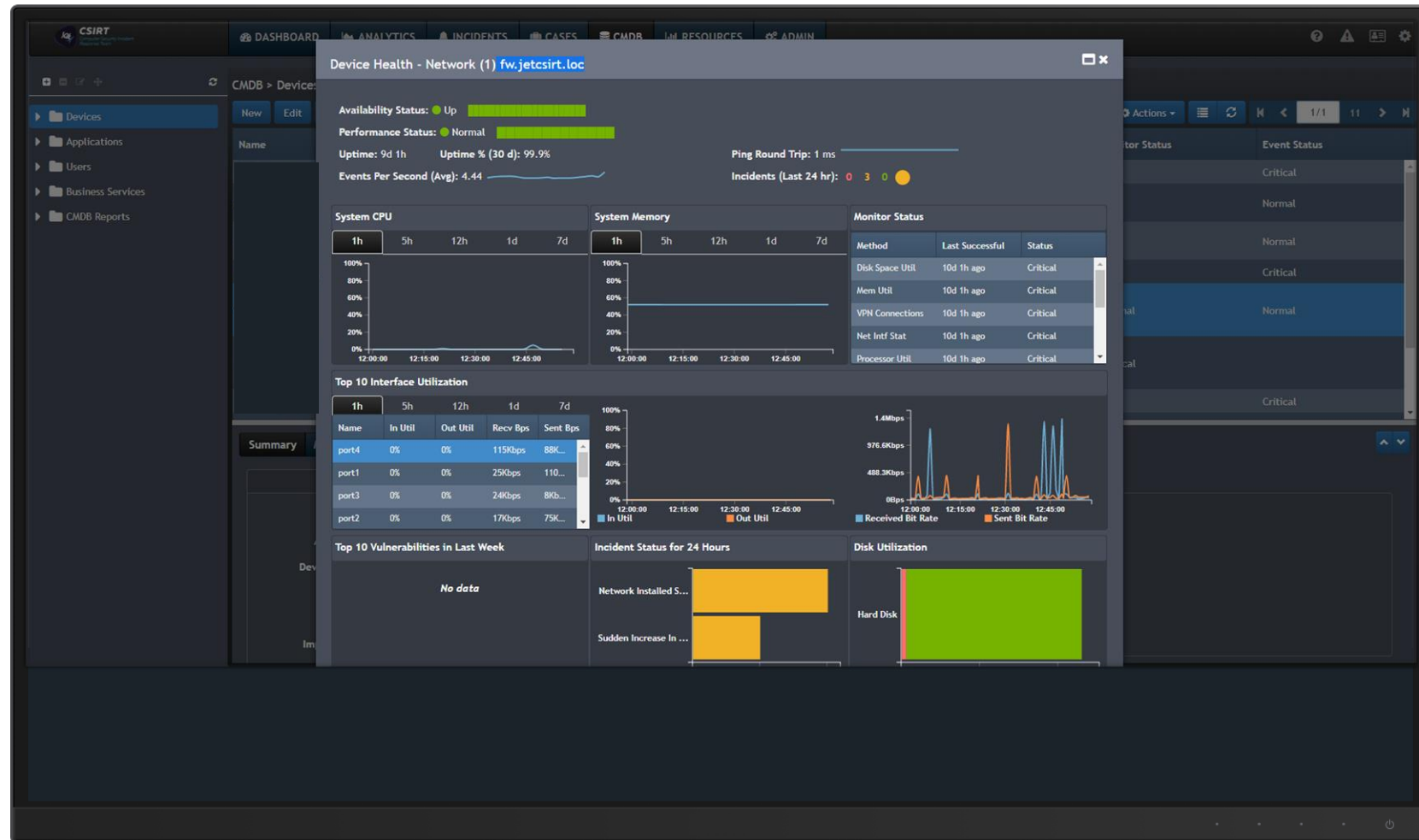
Архитектурные особенности

- Возможность планомерного масштабирования без потери данных и необходимости перенастройки компонент: увеличение числа коллекторов, наращивание производительности супервизора, поддержка виртуализации
- Не лицензируется производительность компонент (исключая EPS на supervisor)
- Бесплатные node
- Режим multitenancy
- Резервное копирование
- Интеграция с Remedy, поддержка Rest API



Полезные для CSIRT возможности FortiSIEM CMDB

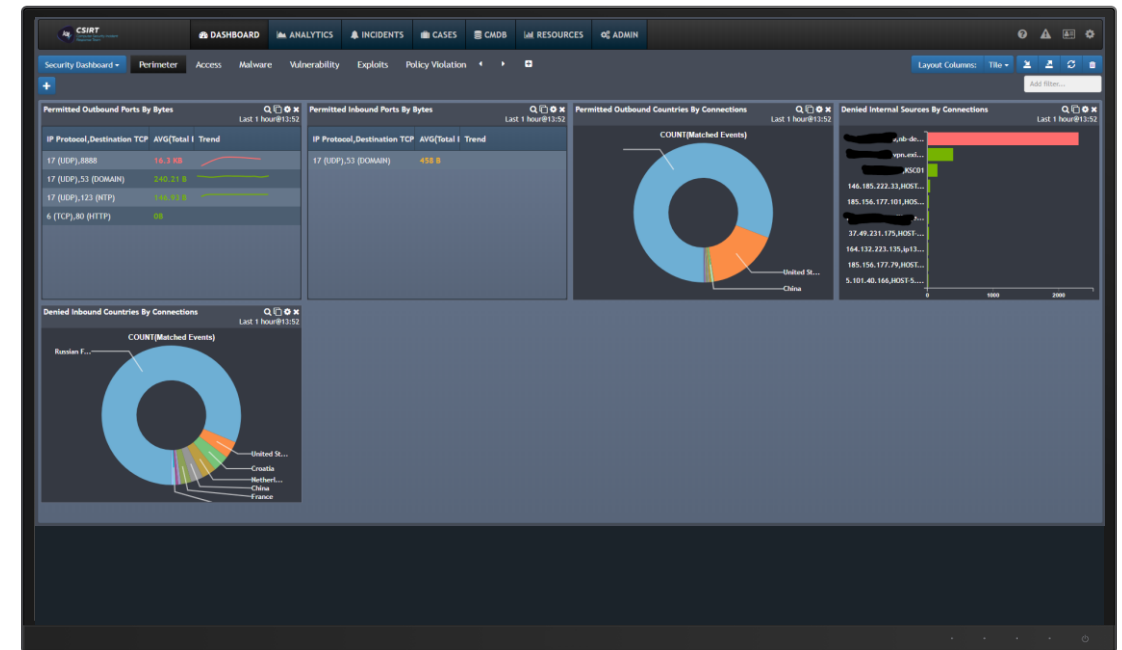
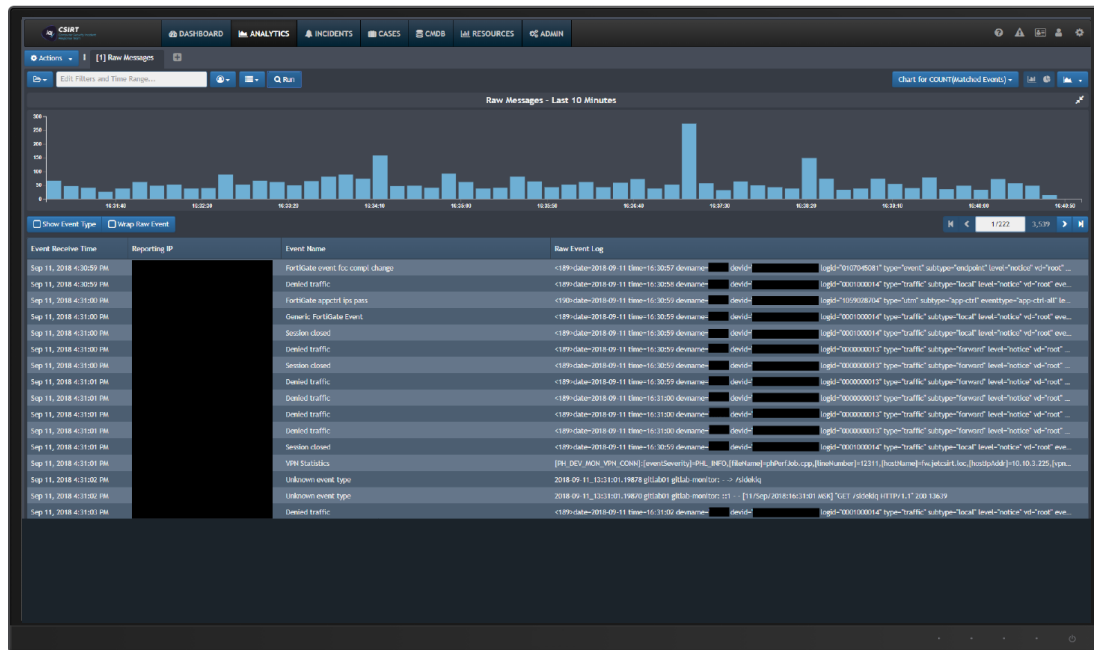
- База активов инфраструктуры, единый автоматически задокументированный срез инфраструктуры в реальном времени и в ретроспективе;
- Детальная информация по performance, конфигурациям, аппаратной платформе, интерфейсам, пользователям, запущенным сервисам и т.д.
- Автоматическая категоризация по типам устройств, приложениям, пользователям, бизнес-сервисам
- Большое количество встроенных полезных отчетов по активам



Полезные для CSIRT возможности FortiSIEM Инструменты аналитики и отчетности

- Поисквые запросы по полям из CMDB
- Кастомизированные оперативные View для 1-й линии, 2-й и 3-й линии мониторинга

- Развитые инструменты аналитики и отчетности
- Отчетность NOC (iSCSI, CPU, Network, VMWare, DISK, Memory)
- Прикладные отчеты (IIS, Apache, Websphere, JBOSS, Tomcat, Glassfish)



Техническая платформа Jet CSIRT

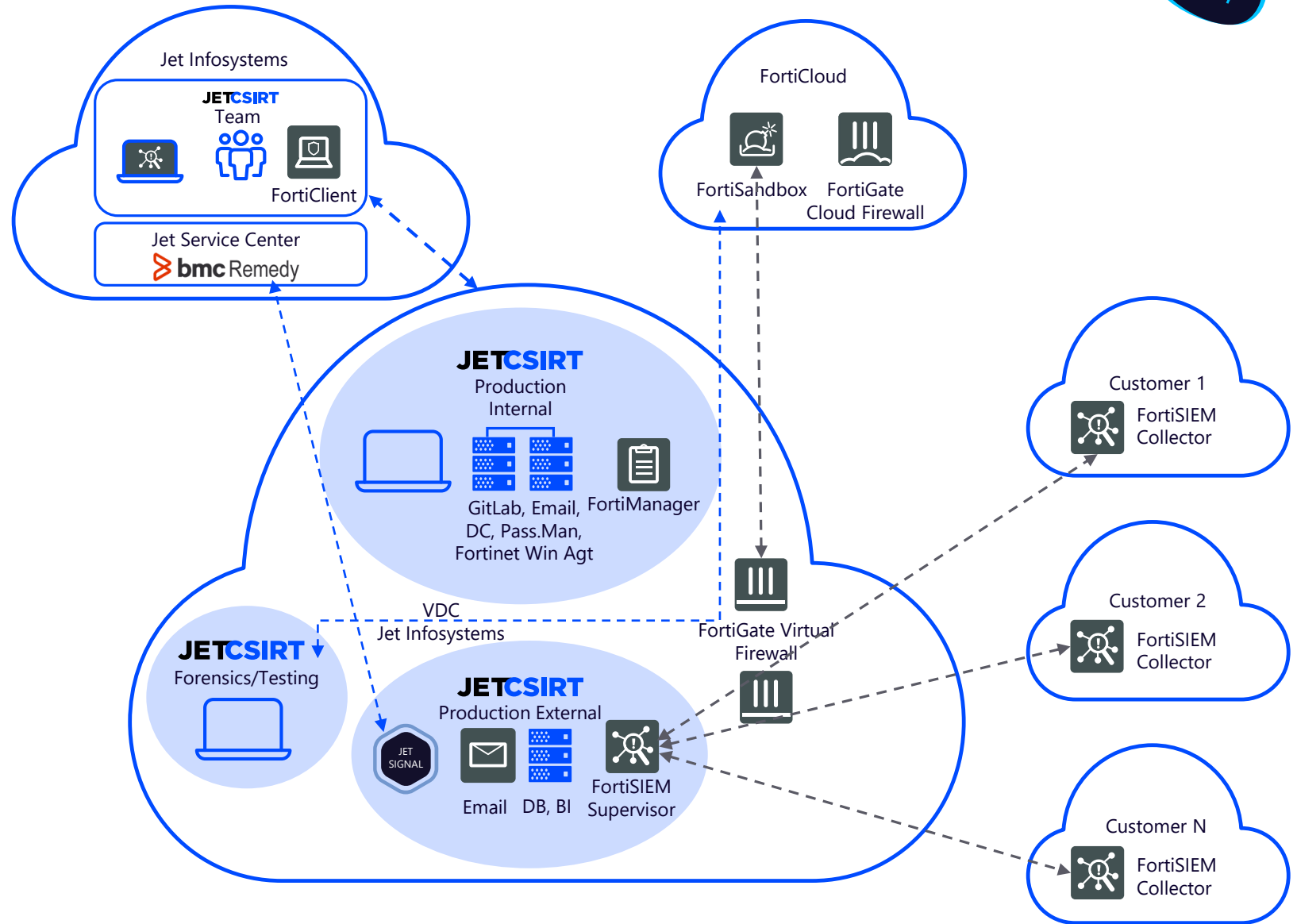


11

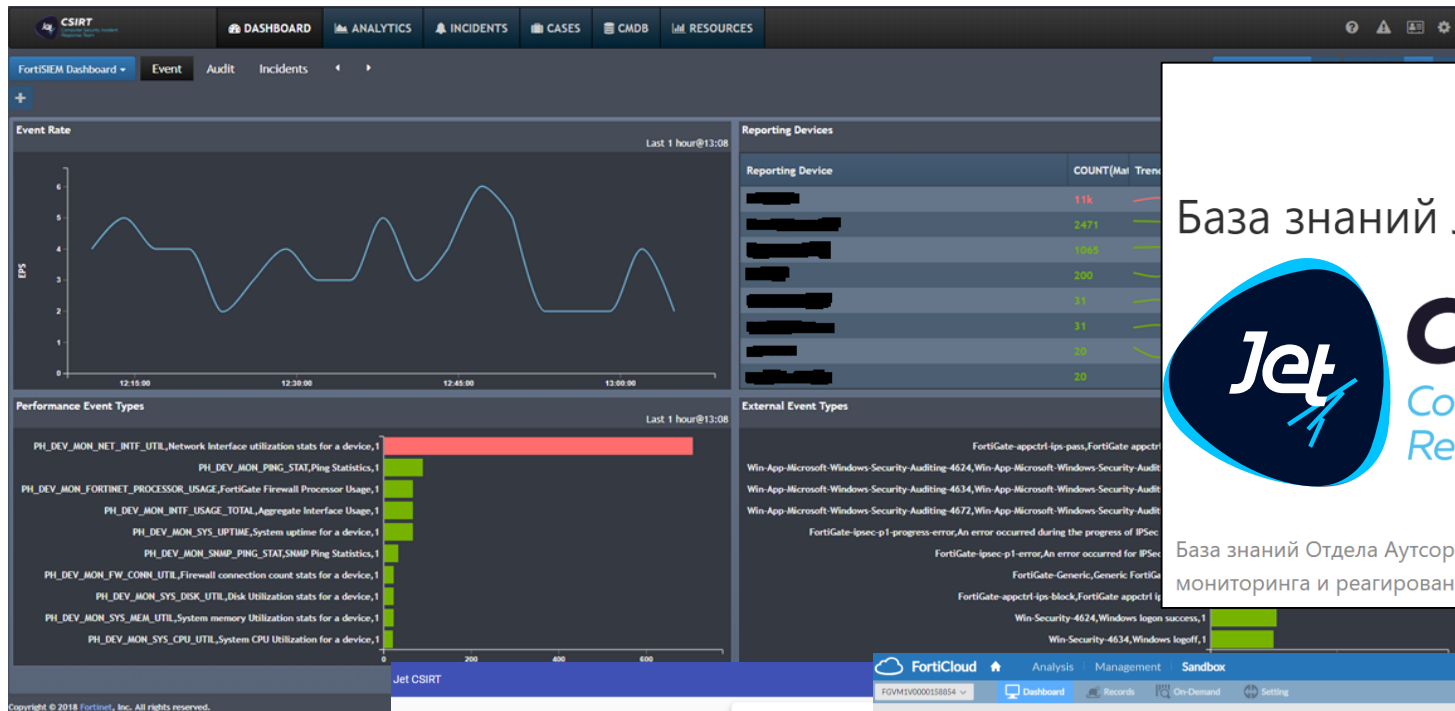
подсистем

CSIRT

Оказание облачных услуг



Техническая платформа Jet CSIRT



База знаний Jet CSIRT

Jet CSIRT
Computer Security Incident Response Team

База знаний Отдела Аутсорсинга ЦИБ по аспектам сервиса мониторинга и реагирования на инциденты ИБ Jet CSIRT

JETCSIRT AD | Standard

JETCSIRT AD Username

Password

Remember me

Sign in

TeamPass
A Collaborative Passwords Manager

Пожалуйста, представьтесь

Введите логин AD

Пароли

Продолжительность сессии (мин.)

20

Забыли пароль?

Log In

TeamPass 2.1.27.10 © 2009 - 2018 | © Время на экране: 02/05/2018 - 13:13:04

Имя пользователя

Ваше имя пользователя в системе

Текущий пароль

Введите ваш текущий пароль

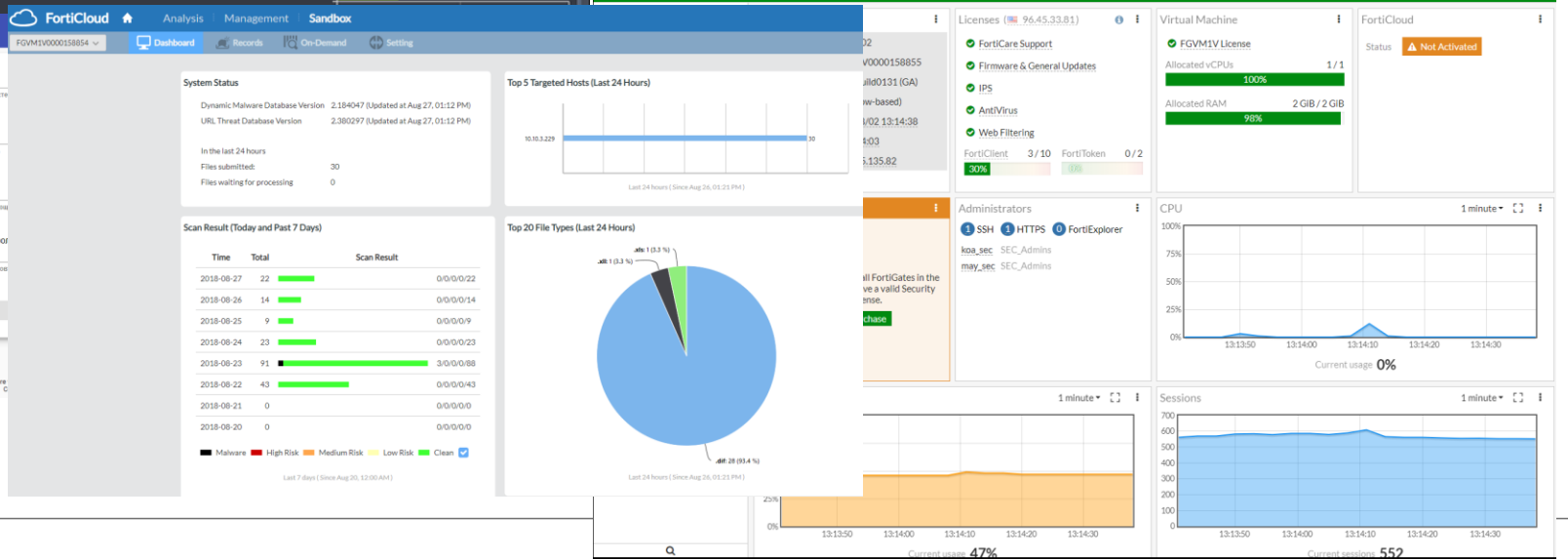
Введите новый пароль

Введите пароль соответствующий

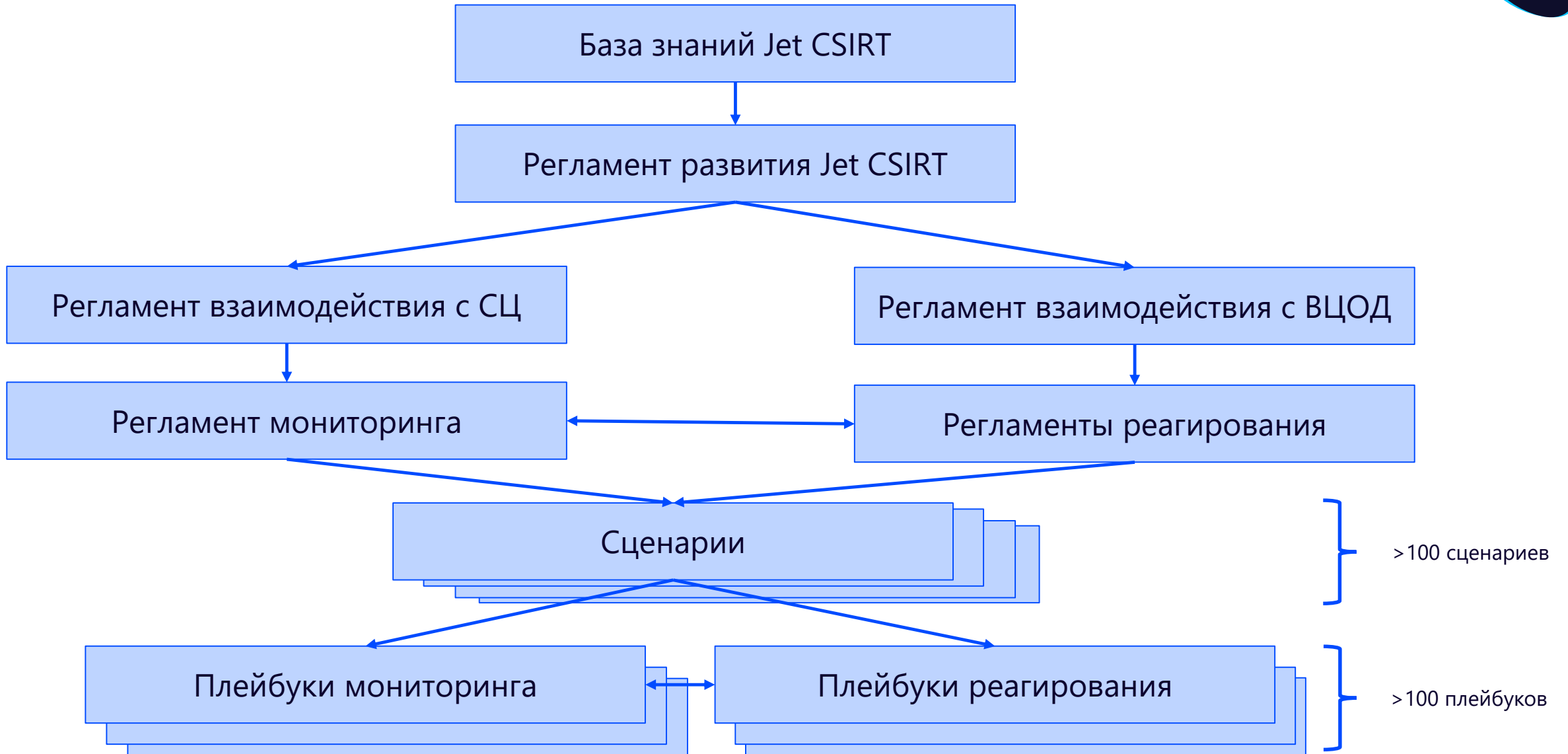
Подтвердите новый пароль

Введите ваш новый пароль повторно

passcore
Powered by PassCore



База знаний Jet CSIRT



Incident Response Platform: Jet Signal



Единое информационное пространство



Интерфейсы Jet Signal. Рабочие столы



СИГНАЛ
admin

- База знаний
- Инциденты
- Поручения
- Новости
- Дежурные смены
- Учёт отсутствий
- Аналитика
- Настройка

Обновить
Рабочий стол

СВОДКА ИНЦИДЕНТОВ ПО ПОДРАЗДЕЛИЯМ

Дата: 25.01.2018

Закрыты: 0

Не назначены

7/2!

Новые

14

Критичные: 5

Средние: 5

Низкие: 4

Номер	Название	ФИО	Дата регистрации	Статус	Критичность	Приоритет	SLA
0001-2018-0000028	Целевая атака компании по электронной почте	Журавлев Д. С.	23.01.2018 19:06	В работе	Высокая ↑	Высокий ↑	-1д 21ч 13мин
0001-2018-0000026	Эксплуатация уязвимости	Васютин В. И.	23.01.2018 18:36	Новый	Высокая ↑	Высокий ↑	-1д 5ч 40мин
0001-2018-0000007	Несанкционированное ознакомление, копирование информации	Субботин Н. Д.	18.01.2018 12:20	Новый	Высокая ↑	Высокий ↑	-1д 5ч 44мин
0001-2018-0000016	Ddos	Журавлев Д. С.	23.01.2018 17:42	В работе	Высокая ↑	Высокий ↑	-1д 4ч 49мин
0001-2018-0000015	Подбор паролей	Колосов И. Б.	23.01.2018 17:37	Новый	Средняя ↑	Высокий ↑	-1д 4ч 29мин
0001-2018-0000027	Ddos	Латонин С. В.	23.01.2018 18:52	Новый	Высокая ↑	Высокий ↑	-1д 3ч 24мин
0001-2018-0000004	Хищение и утеря съемных носителей	Иванов В. Н.	18.01.2018 11:29	Новый	Средняя ↑	Средний	-1д 2ч 49мин

СВОДКА ПО ПОРУЧЕНИЯМ

Всего поручений: 14

Принято к исполнению: 1

Выполнено в срок: 4

Отклонено: 1

Выполнено с нарушением срока: 0

Не выполнено, срок прошел: 1

Срок сегодня

Показаны записи 1-1 из 1.

Тема	Ответственный	Срок исполнения	Статус
Создать отчетность по последней интеграции	Лазарев М. В.	25.01.2018 11:10	Зарегистрировано

На этой неделе

Показаны записи 1-3 из 5.

Тема	Ответственный	Срок исполнения	Статус
Ознакомиться с перестановками в отделе безопасности	Иванов В. Н.	29.01.2018 18:15	Зарегистрировано
Разобрать связь вирусной активности за текущие сутки	Васютин В. И.	27.01.2018 17:45	Зарегистрировано
Предоставить отчет по вирусным активностям за прошедшую неделю	Попов И. К.	26.01.2018 17:35	Зарегистрировано

Интерфейсы Jet Signal. Карточка инцидентов



0001-2018-0000027 **НОВЫЙ**

В работу Передать Редактировать

Общие данные

Название	Ddos		
Номер	0001-2018-0000027		
Дата регистрации	23.01.2018 18:52	Дата обнаружения	
Дата устранения		Дата SLA	24.01.2018 13:25
% выполнения	0	Гриф	
Критичность	Высокая	Приоритет	Высокий
Тип инцидента	DoS/DDoS атака	Категория	Атака на информационный актив
Угроза		Источник	
Исполнитель	Латонин Семен Владимирович	Автор	Журавлев Дмитрий Сергеевич
Подразделение	Дежурная смена	ТО	1
Дата и время последнего изменения	23.01.2018 18:52	Идентификатор контролируемого объекта	
Место и способ фиксации компьютерного инцидента		Необходимость содействия	
TLR		Статус KI	
Тип атакуемого объекта			

План мероприятий

DoS/DDoS атака

Показаны записи 1-5 из 5.

N	Описание	Выполнено	Дата	ФИО	Комментарий
1	Идентификация источника(ов) и целей, на которые направлена атака	<input type="checkbox"/>			
2	Блокировка на МЭЛПС	<input type="checkbox"/>			
3	Оповестить ответственные стороны: ИТ-поддержку/подрядчика, обслуживающих атакуемую систему, для дополнительной диагностики и мониторинга состояния. А также интернет-провайдера				
4	Сбор информации о владельцах IP, характере атаки и т.п.				
5	Изучить отчёт				

DoS/DDoS атака

Доменное имя, IP-адрес или подсеть пострадавшего объекта	
Мощность атаки	
Время начала атаки	Время окончания атаки
Источники атаки	
Тип атаки	

Информационные кампании (0)

Связанные инциденты (1)

Связанные поручения (0)

Хранилище файлов (0)

Оставить комментарий

В I N ← → ☰ ☷ % ⌨ ⌂ ⌕ ↺ ↻

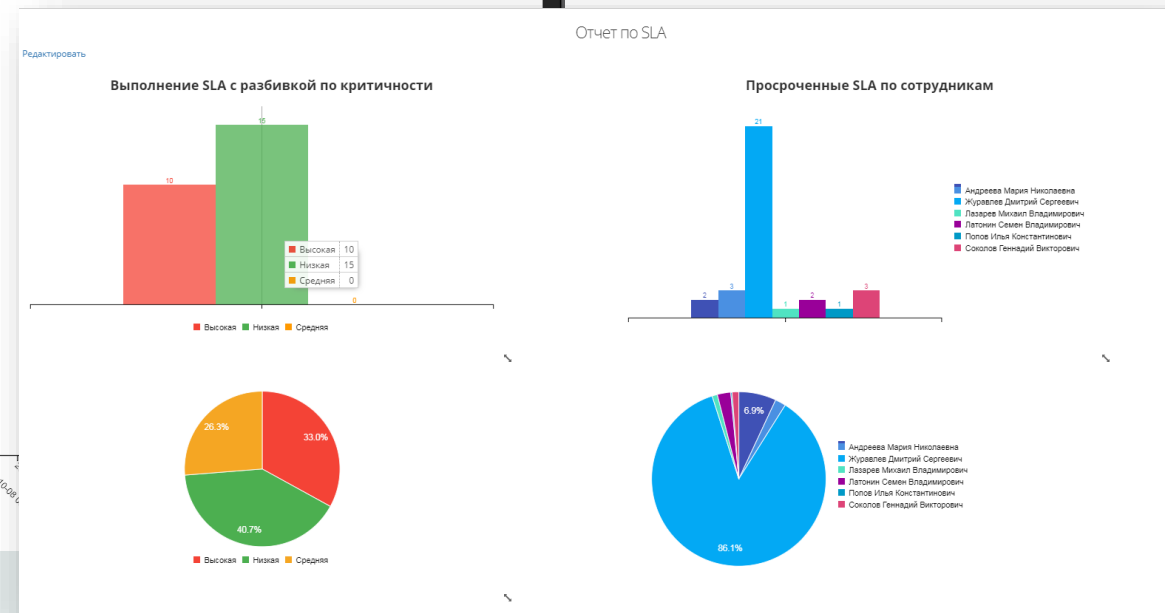
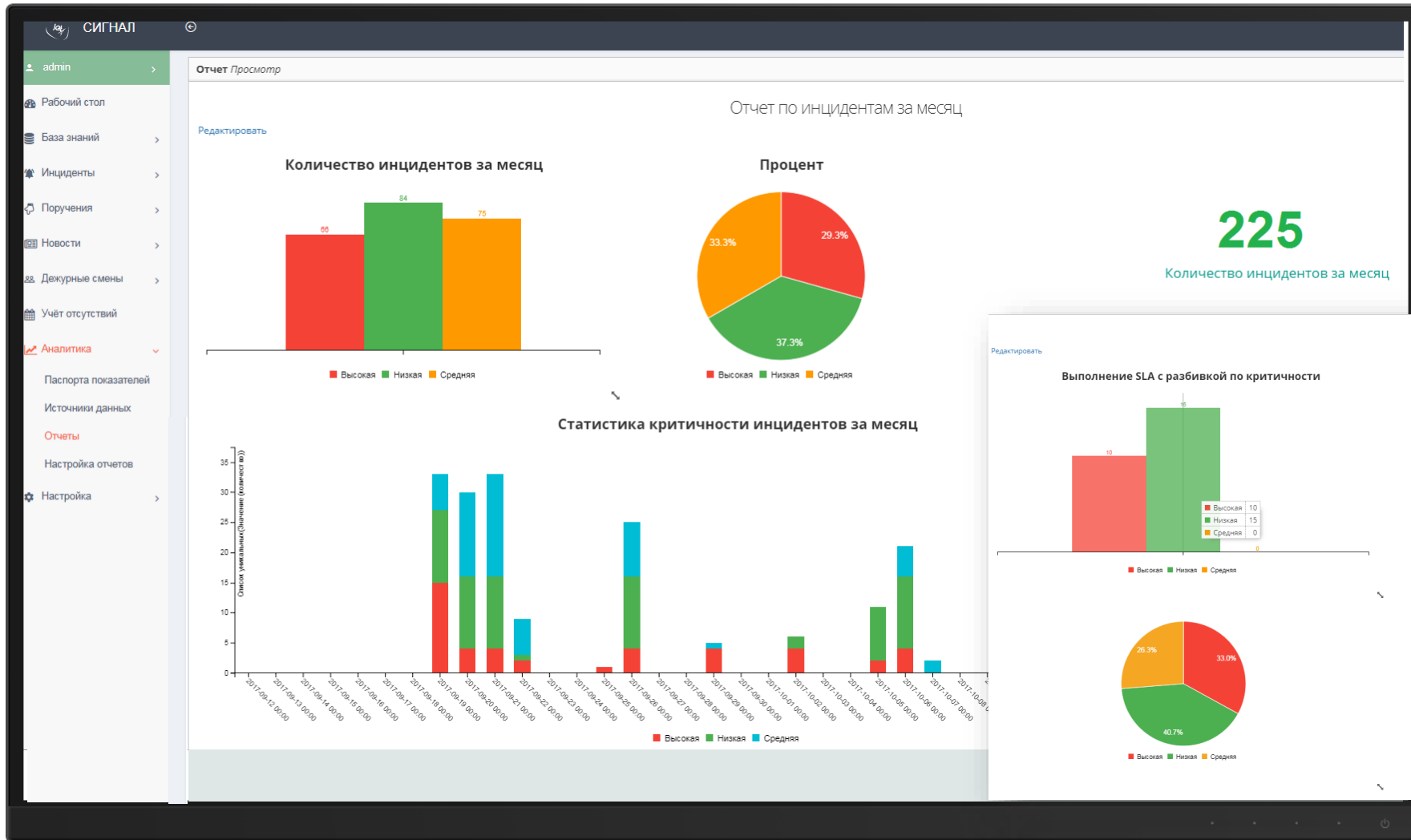
Отправить

История изменений

Добавлена связь с инцидентом 0001-2018-0000028 Журавлев Дмитрий Сергеевич 23.01.2018 19:13

- Обновлен Инцидент Журавлев Дмитрий Сергеевич 23.01.2018 18:52
 - Исполнитель изменен на Латонин Семен Владимирович
- Обновлен Инцидент Журавлев Дмитрий Сергеевич 23.01.2018 18:52
 - Дата SLA изменен с 23.01.2018 19:22 на 24.01.2018 13:25
- Создан Инцидент Журавлев Дмитрий Сергеевич 23.01.2018 18:52
- Добавлены детали в Инцидент Журавлев Дмитрий Сергеевич 23.01.2018 18:52

Интерфейсы Jet Signal. Аналитика





ROADMAP



Jet CSIRT. Roadmap



СПАСИБО ЗА ВНИМАНИЕ

Алексей
Мальнев

Руководитель Jet CSIRT компании «Инфосистемы Джет»
ay.malnev@msk.jet.su / +7 985 849-89-33

SECURITYDAY