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

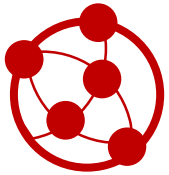
1. Введение. Обзор FortiSIEM
2. Что такое Jet CSIRT
3. Как мы строили Jet CSIRT
4. Roadmap

FortiSIEM

Универсальная система корреляции и управления событиями ИБ

FORTINET

FortiSIEM – Ключевые функции



Обнаружение и учет активов

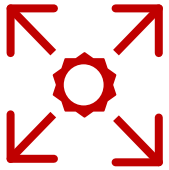
- Всесторонне и точно
- Контекстная оценка активов
- Оценка уязвимостей

Масшабируемость, быстрая интеграция

- Поддержка собственных (custom) устройств
- Масштабируемая архитектура

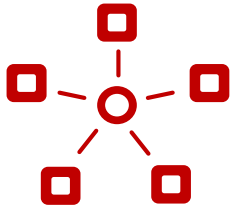
Автоматизация

- Реакция на инциденты ИБ
- Управление заявками
- Автоматизация противодействия



Единая панель управления

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



Унифицированная платформа

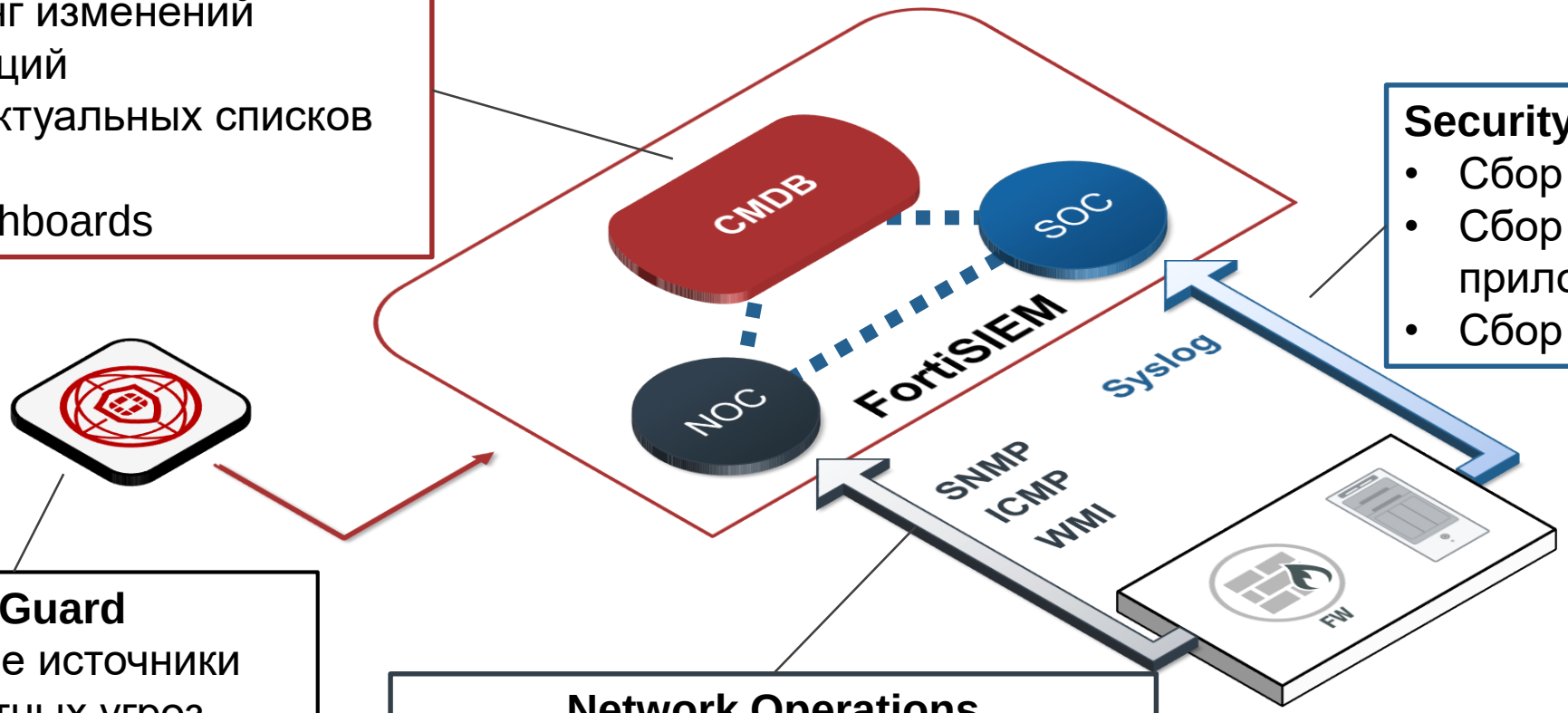
- Multi-tenancy
- Ролевая модель доступа (RBAC)

FortiGuard

- FortiGuard threat feed
- Domain, IP and URL IOCs

Объединение NOC & SOC – единая точка управления

CMDB
- Мониторинг изменений конфигураций
- Ведение актуальных списков активов
- Device dashboards



Security Operations
- Сбор логов устройств
- Сбор логов приложений
- Сбор логов трафика

FortiGuard
- Внешние источники известных угроз

Network Operations
- Мониторинг производительности
- CPU, memory, interface utilization
- Мониторинг доступности

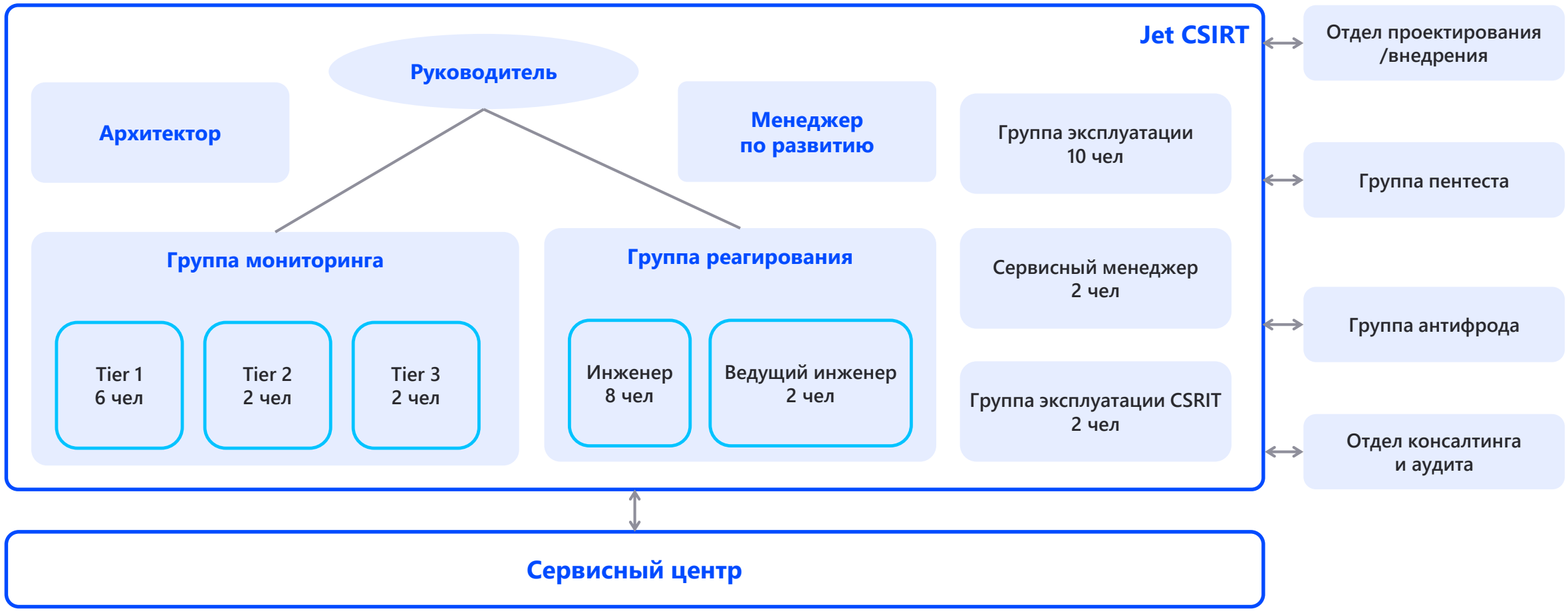
ЧТО ТАКОЕ JET CSIRT?

Нормативная база

Выстраивание процессов	NIST, FIRST (Improving Security Together), ISO IEC
Команда и роли в ней	SANS, РС БР ИББС-2.5-2014
Технологии и архитектура	MITRE, SANS
Метрики и оценка зрелости	Carnegie Mellon University, Rhodes University (Where leaders learn)
Соответствие	№187-ФЗ, ПП-79/541, СТО БР ИББС-1.0-2014

Jet CSIRT в составе услуг Центра Информационной безопасности

Команда Jet CSIRT. Оргструктура

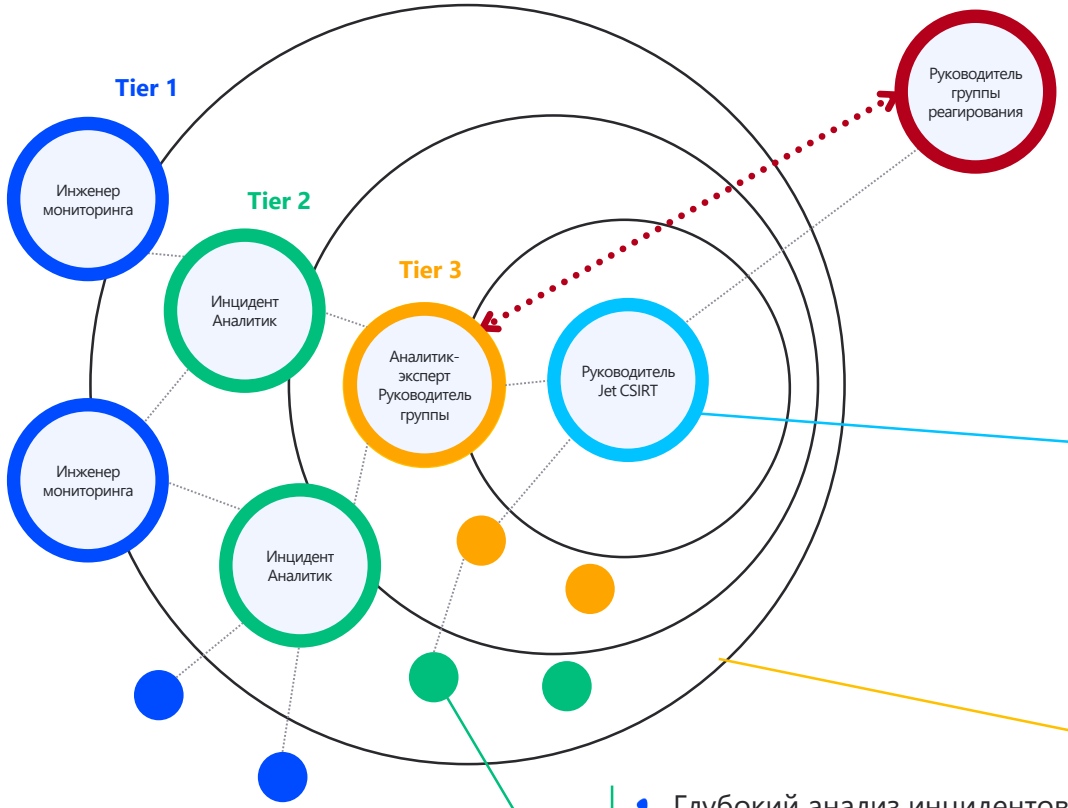


Команда Jet CSIRT. Группа мониторинга

Сервисный центр (операторы)

Передовая

Передовая



- Управление командой
- Разработка стратегии развития
- Пресейл/маркетинг
- SLA
- Координация с руководством
- Точка координации по оргвопросам и критичным инцидентам

- Мониторинг (Alert Monitoring)
- Оповещение Заказчика
- Контроль состояния SIEM
- Сбор данных для Tier 2

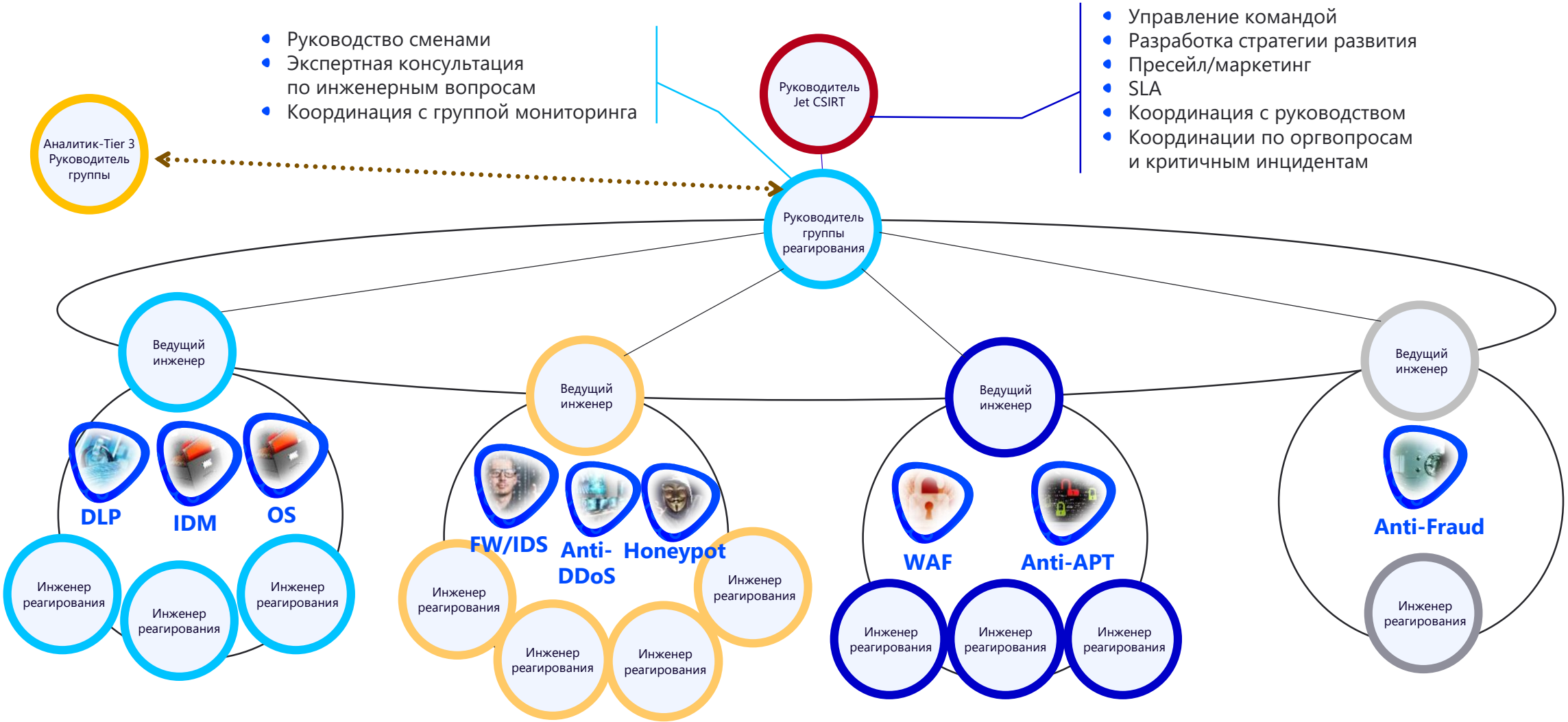
- Глубокий анализ инцидентов
- Определение атакованных активов/ систем и фиксация атакующих
- Консультации по вопросам восстановления
- Участие в поиске новых аналитических методов для обнаружения угроз
- Vulnerability Management

- Глубокое изучение инфраструктуры
- Threat Intelligence
- Расследование инцидентов
- Malware Reverse Engineering
- Incident Hunting
- Threat Detection Tuning
- Координация с группой реагирования

Команда Jet CSIRT. Группа реагирования

- Руководство сменами
- Экспертная консультация по инженерным вопросам
- Координация с группой мониторинга

- Управление командой
- Разработка стратегии развития
- Пресейл/маркетинг
- SLA
- Координация с руководством
- Координации по оргвопросам и критичным инцидентам



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

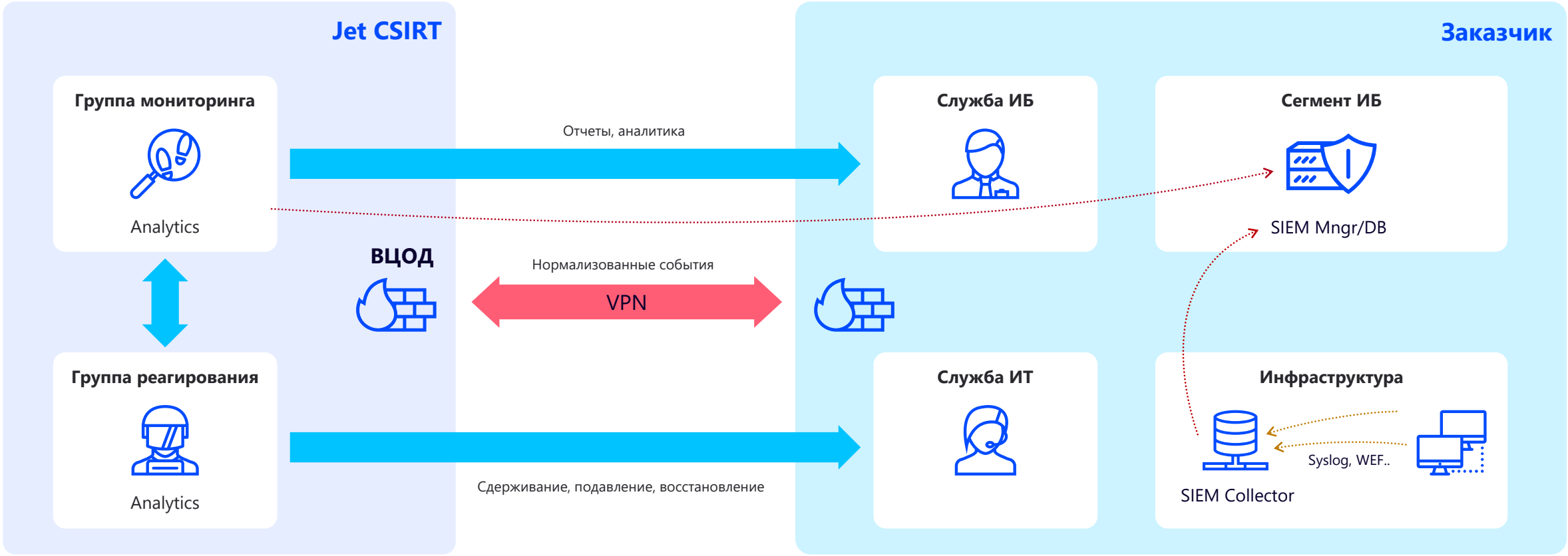
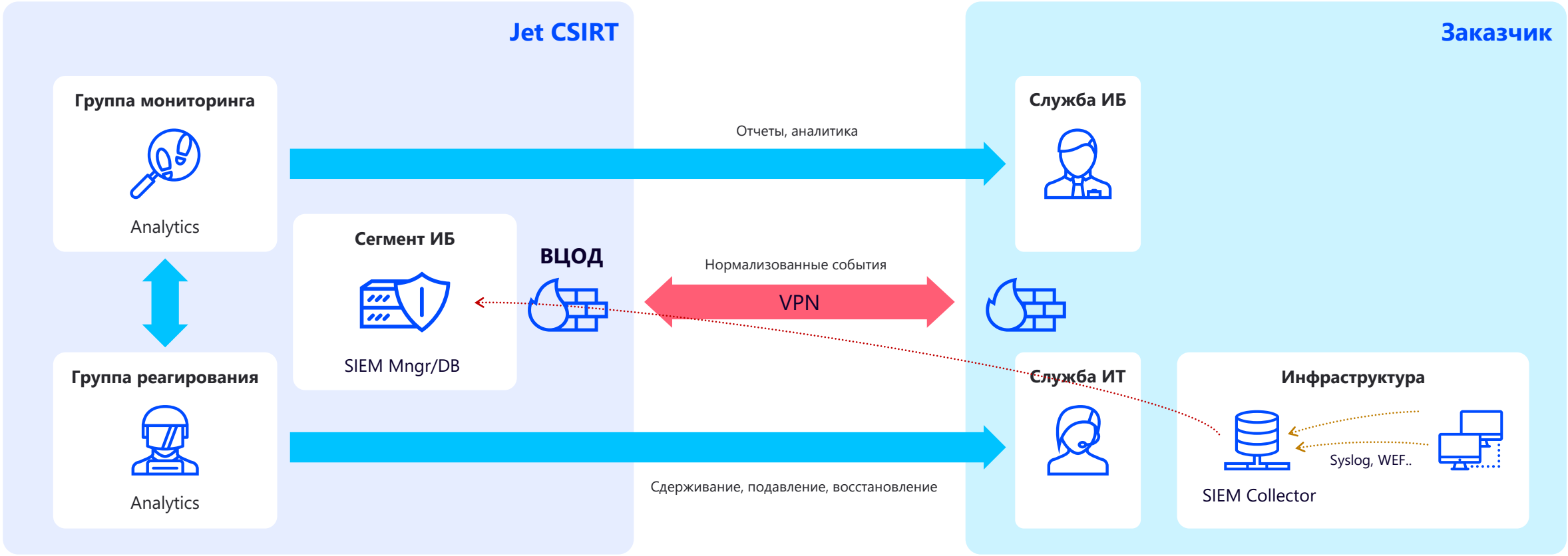


Схема подключения Jet CSIRT. Вариант 2



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
radware
ARBOR NETWORKS
SKYBOX SECURITY

Средства визуализации

Qlik Sense


КАК МЫ СТРОИМ JET CSIRT

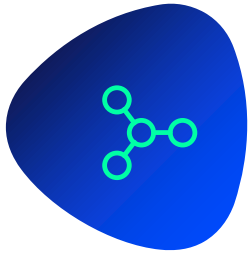
Почему Fortinet?

Технологии

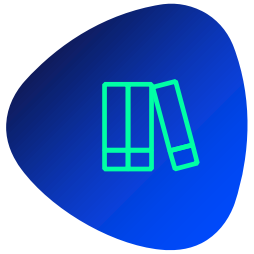
Перспективы
сертификации ФСТЭК

Гибкая ценовая политика

Представительство
в РФ и техподдержка



Экосистема ИБ продуктов



Обилие технической документации

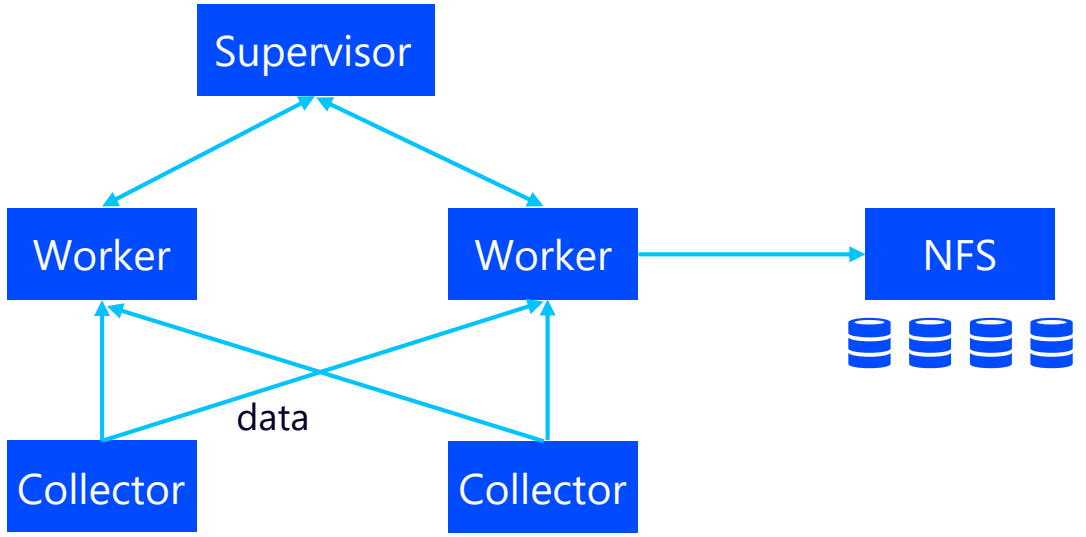
Выбор инструментов Jet CSIRT. SIEM

Техническое сравнение SIEM для Jet CSIRT

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

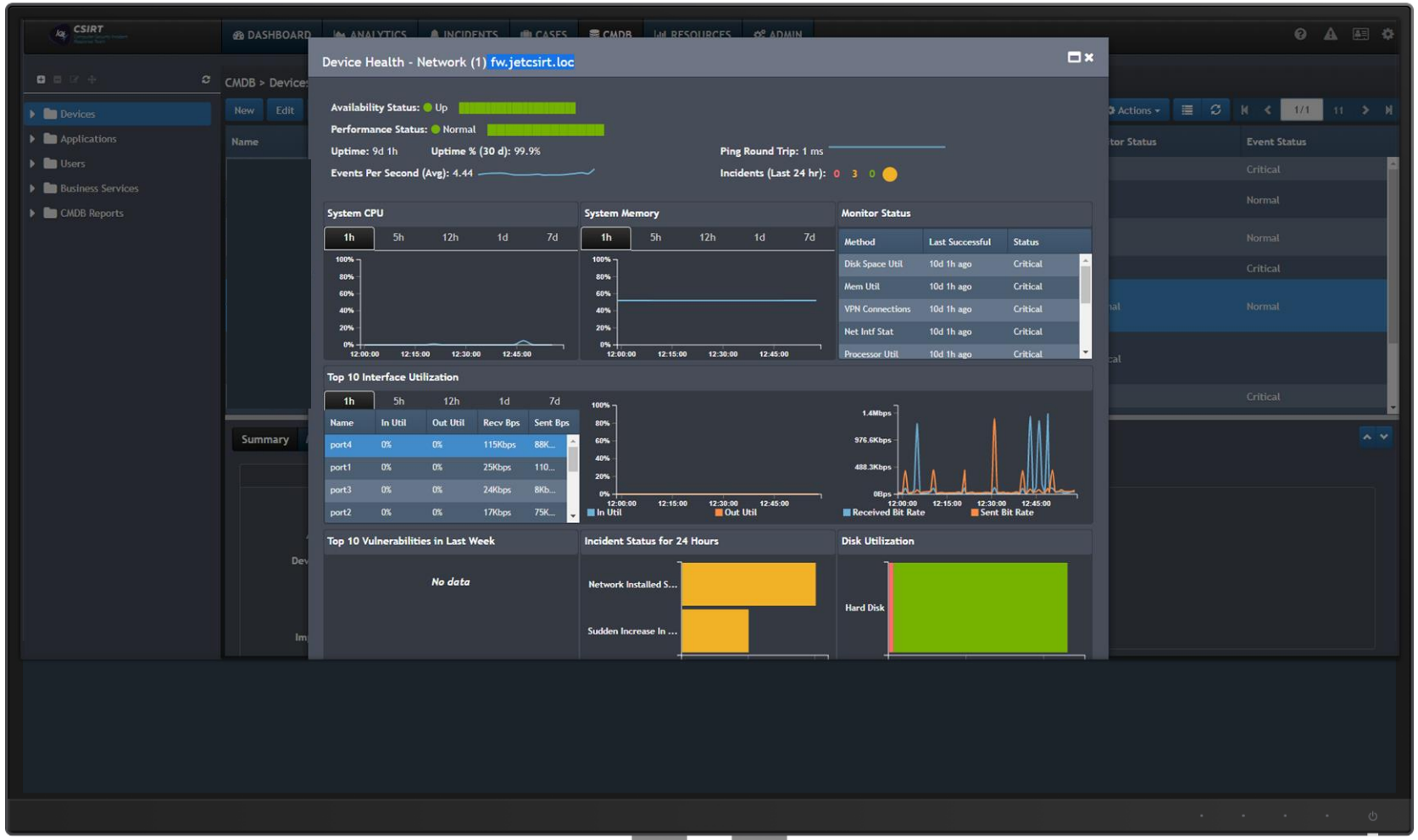
Полезные для CSIRT возможности FortiSIEM
Архитектурные особенности

- 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



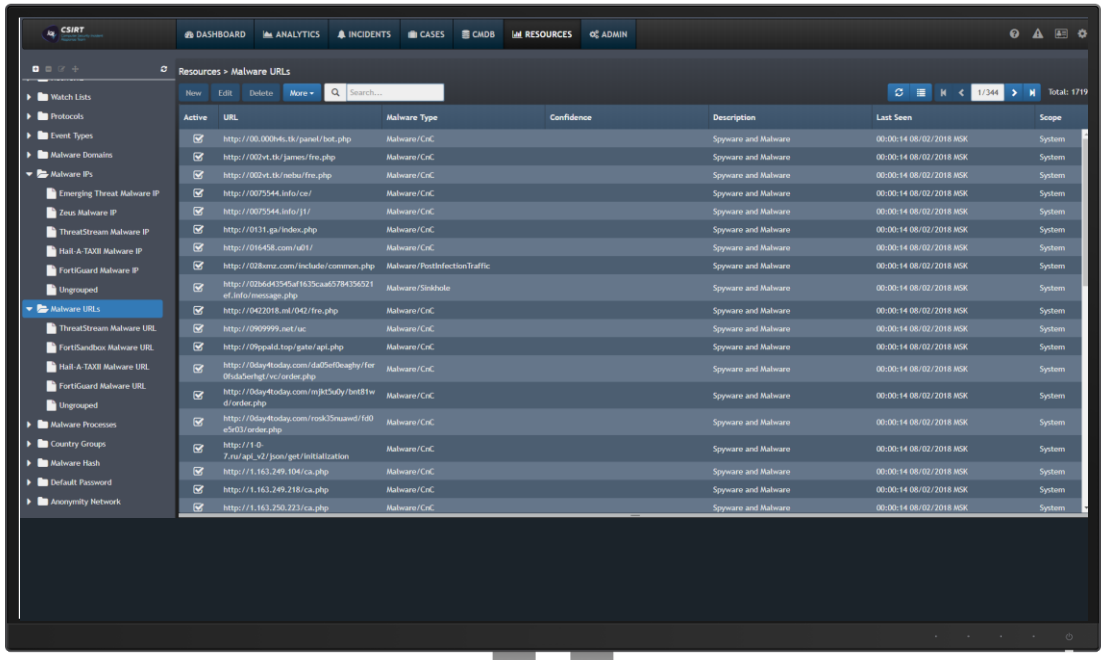
Полезные для CSIRT возможности FortiSIEM CMDB

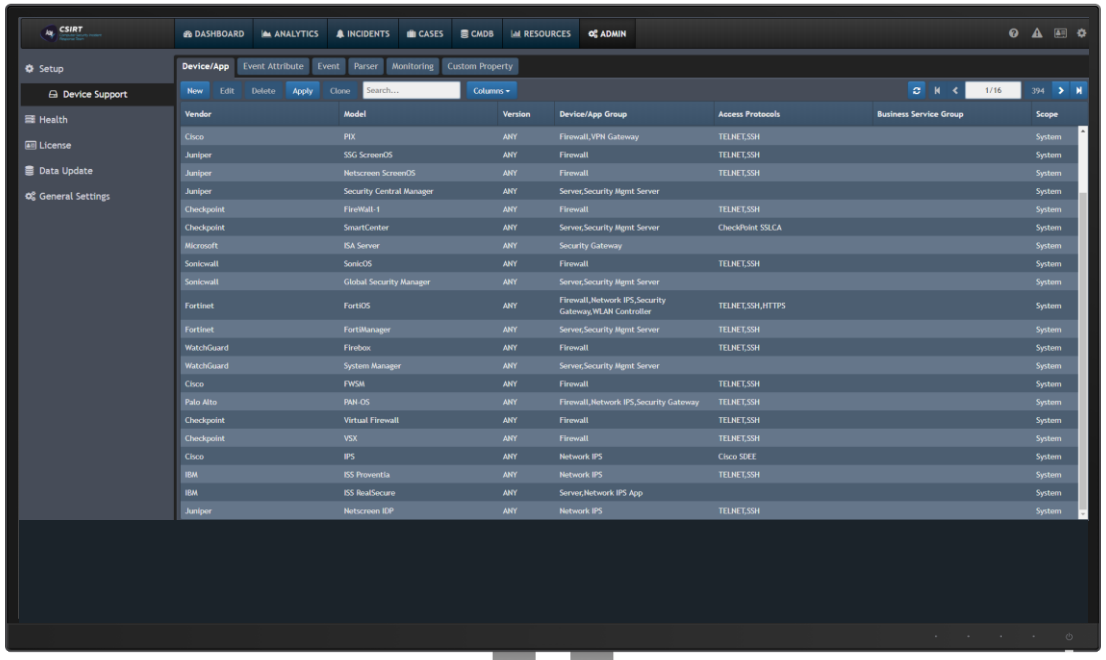
- База активов инфраструктуры, единый автоматически задокументированный срез инфраструктуры в реальном времени и в ретроспективе;
- Детальная информация по performance, конфигурациям, аппаратной платформе, интерфейсам, пользователям, запущенным сервисам и т.д.
- Автоматическая категоризация по типам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



Полезные для CSIRT возможности FortiSIEM
База знаний и поддержка источников

- Удобный и интуитивно понятный интерфейс базы знаний
- Структурированная база ресурсов по отчетам, правилам, ip-подсетям (например VPN pools), работа с Watch-list и профилированием, протоколы, Threat Intelligence, Default Passwords, хеши и т.д.
- Поддержка порядка 400 устройств «из коробки»
- Хороший уровень нормализации

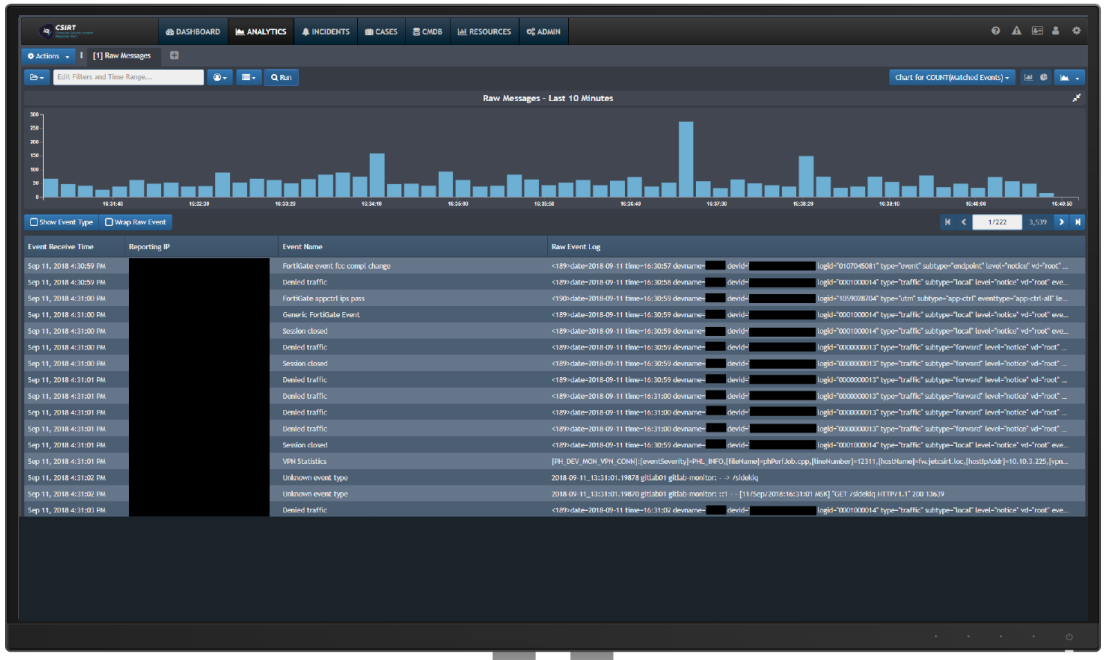


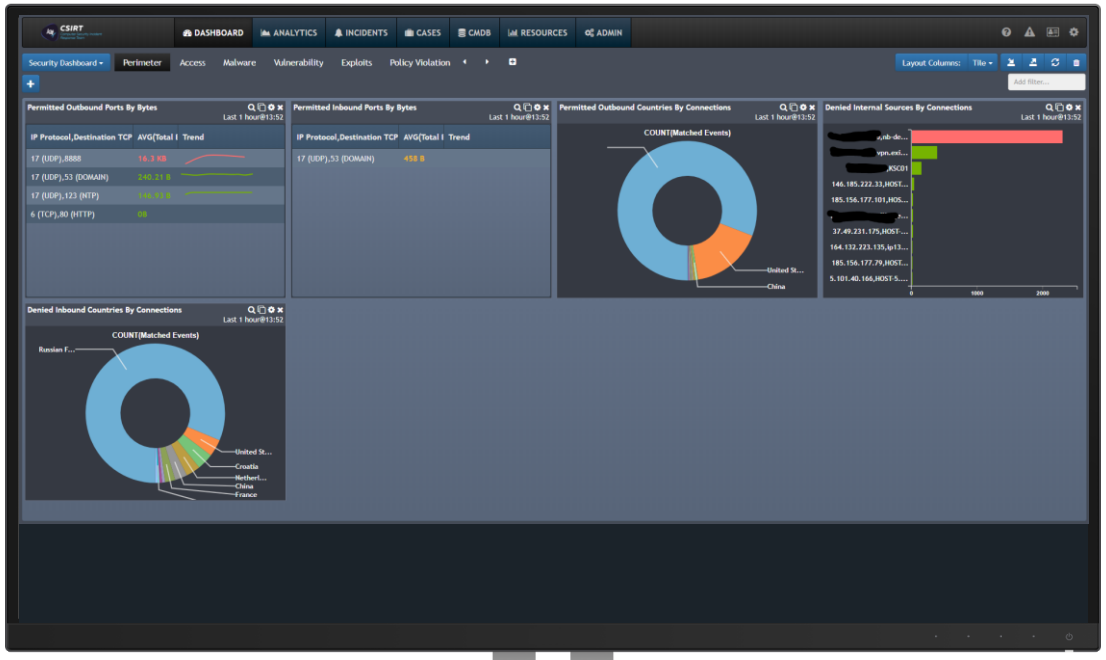


Полезные для CSIRT возможности FortiSIEM
Инструменты аналитики и отчетности

- Поисковые 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)





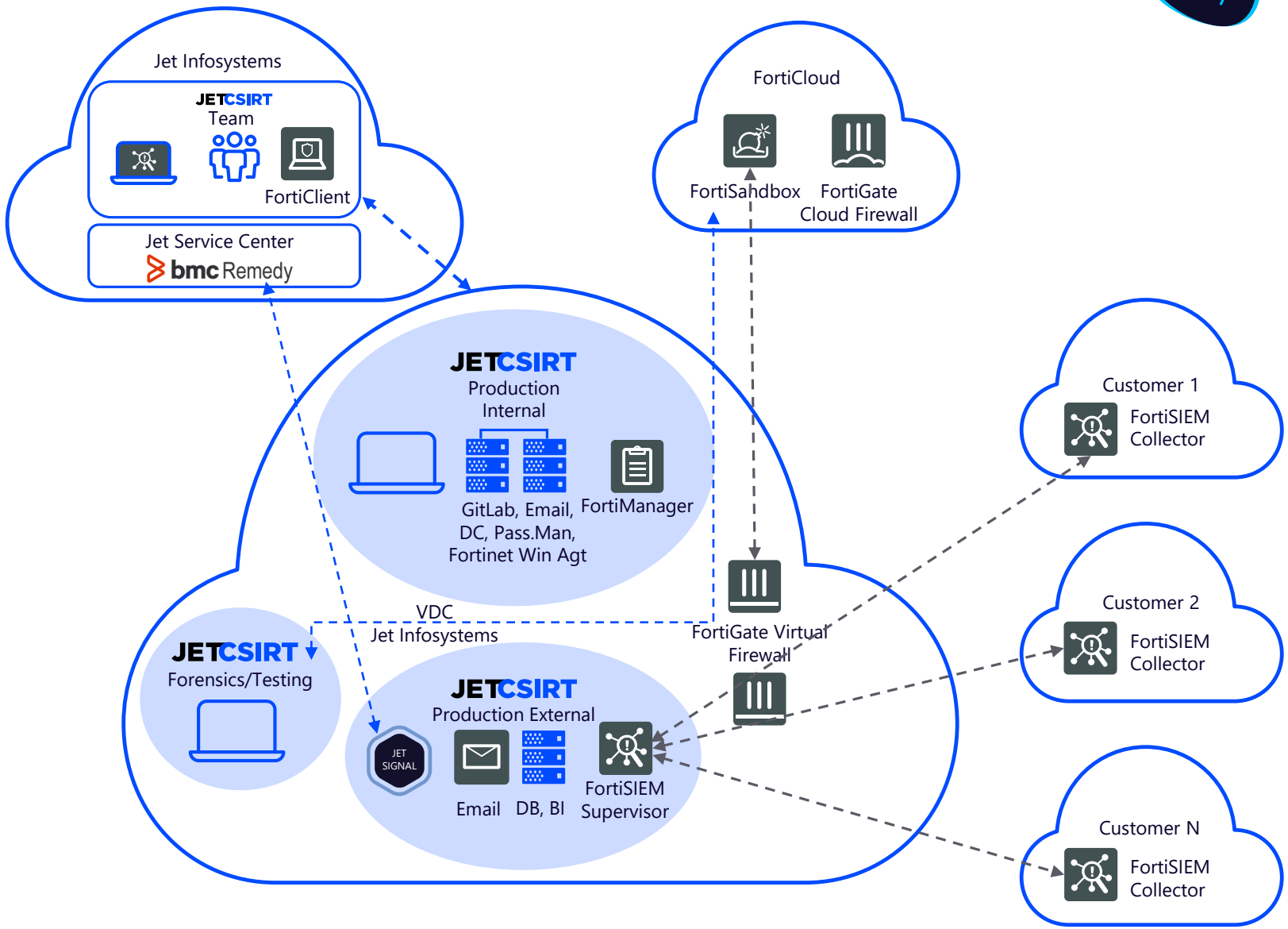
Техническая платформа Jet CSIRT

11

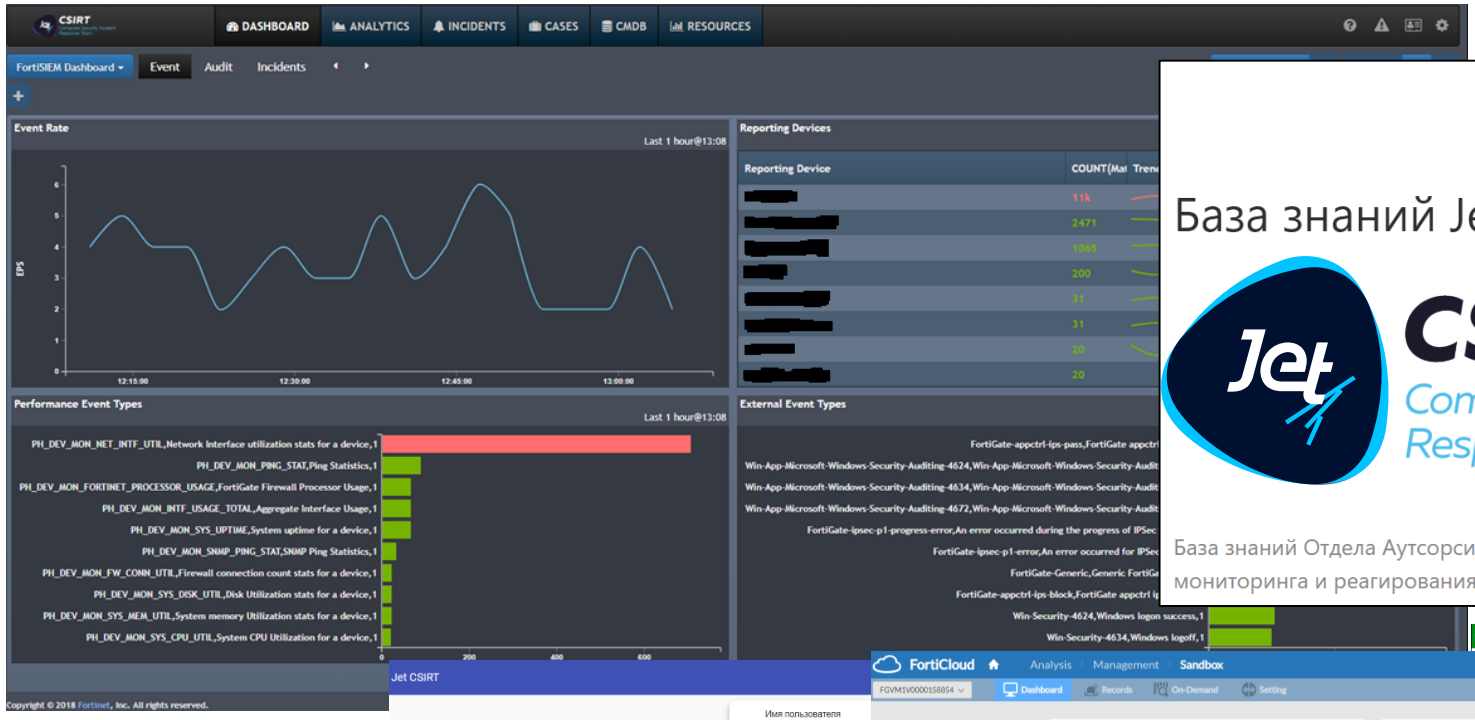
подсистем

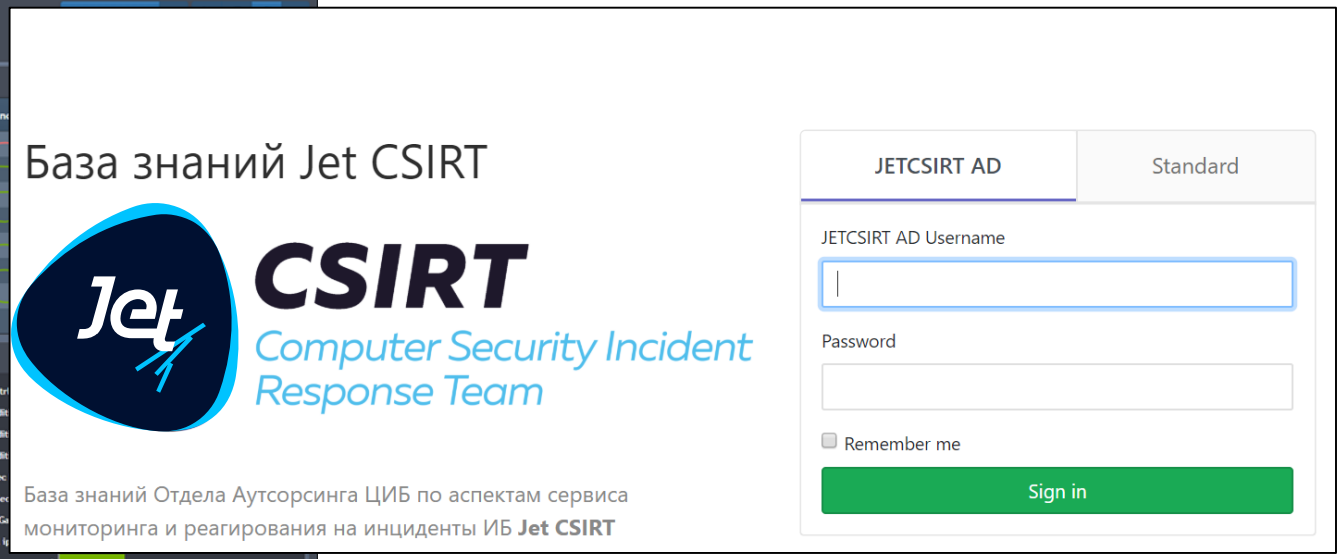
CSIRT

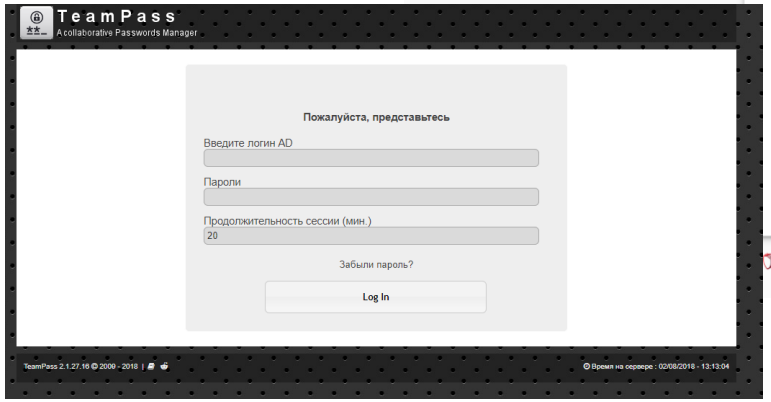
Оказание облачных услуг

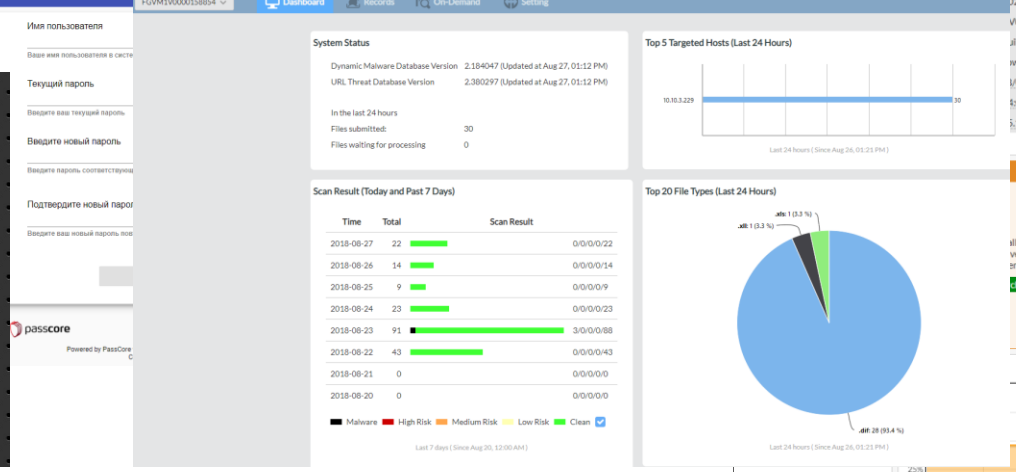


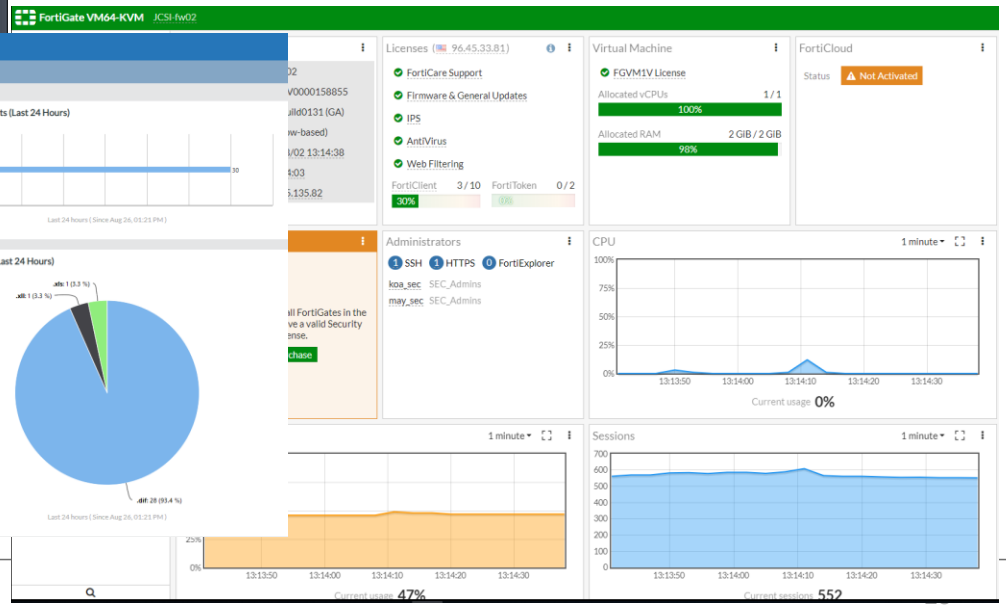
Техническая платформа Jet CSIRT



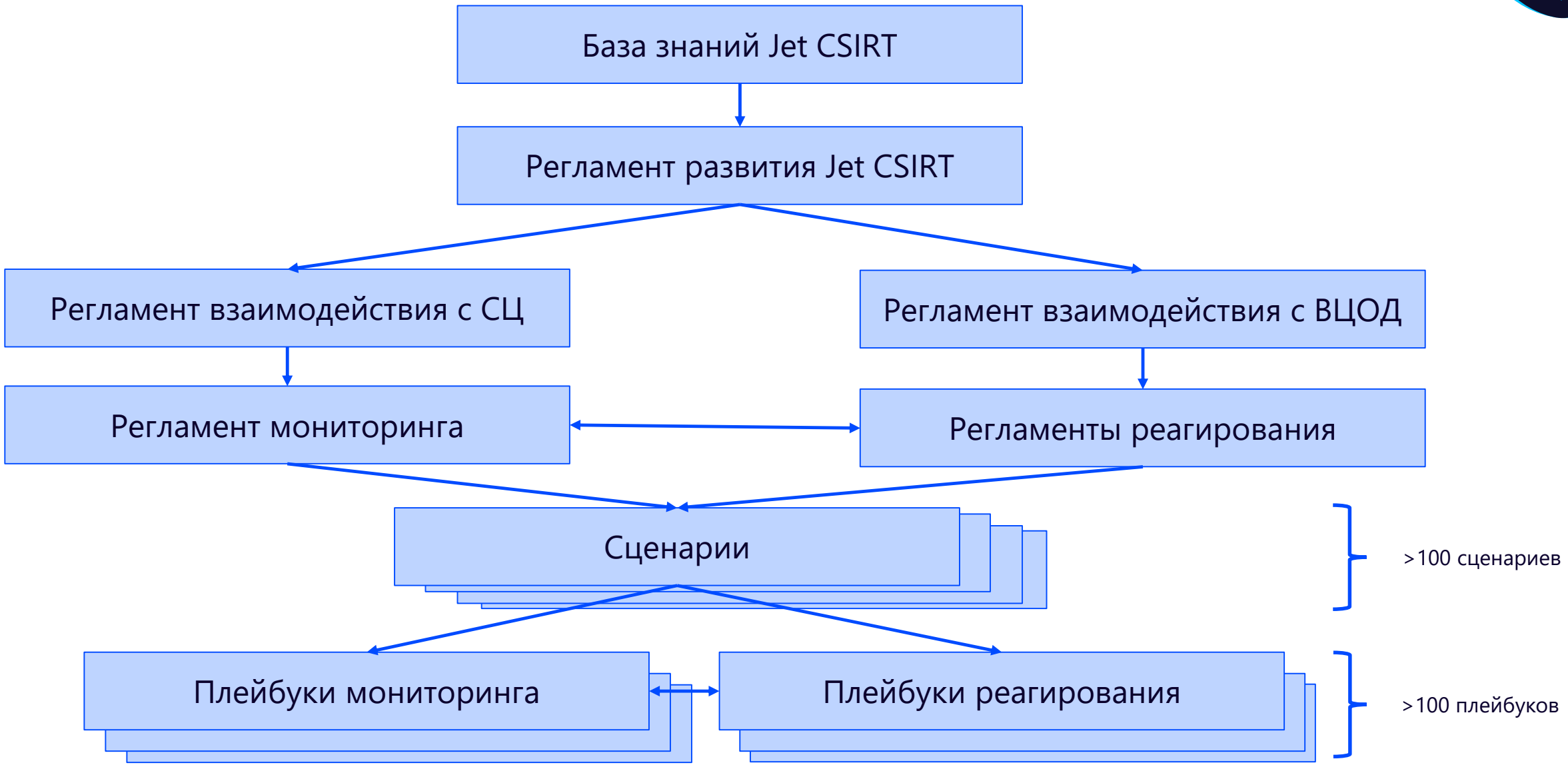








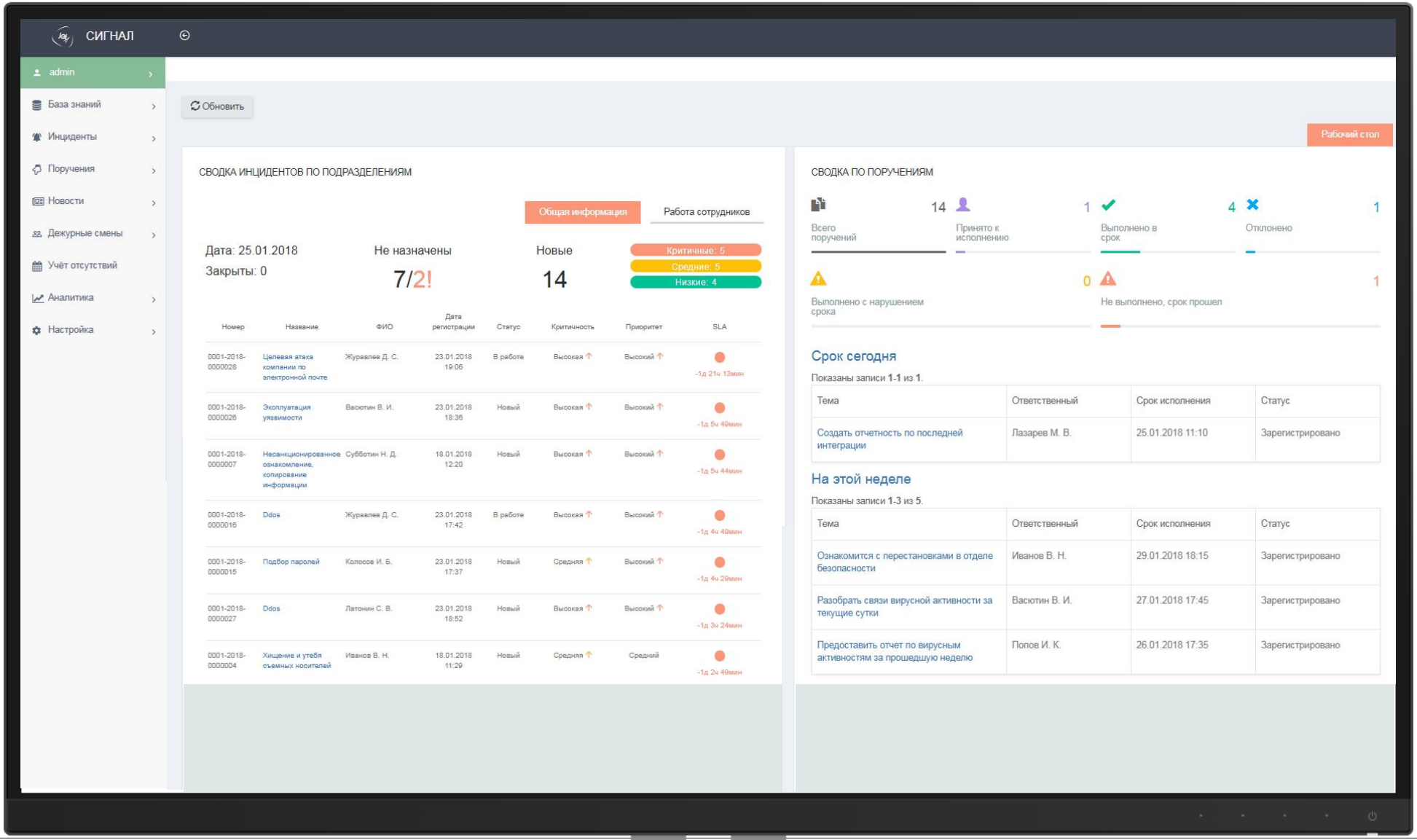
База знаний Jet CSIRT



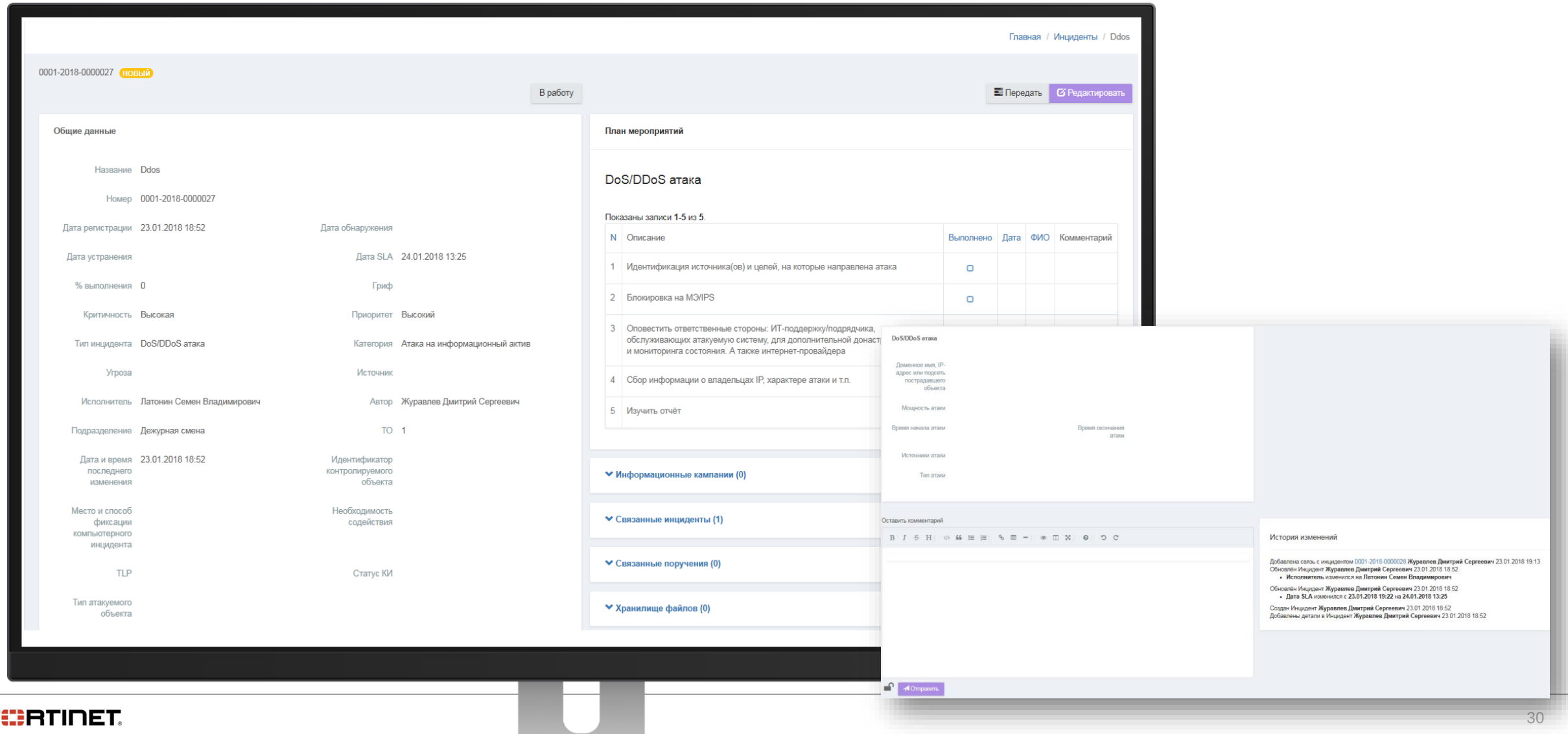
Incident Response Platform: Jet Signal

Единое информационное пространство

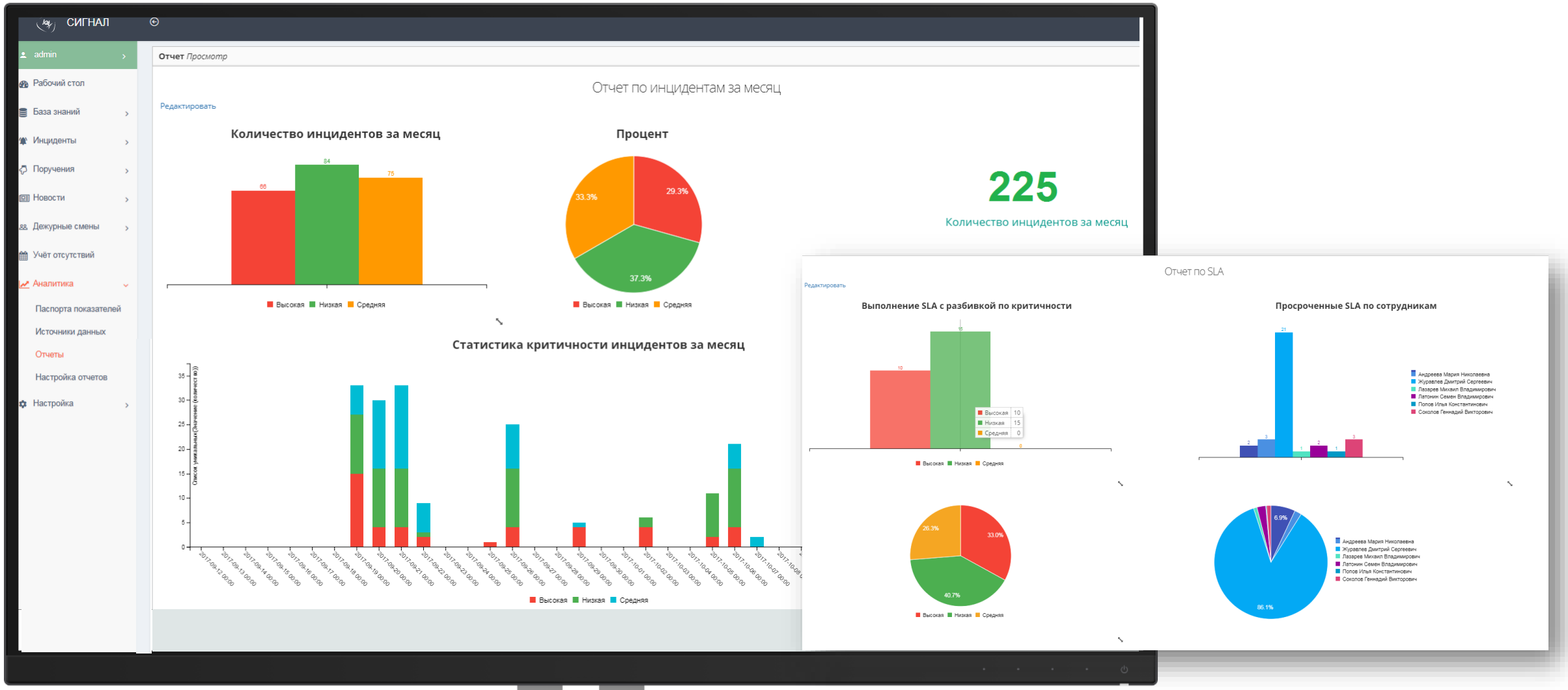
Интерфейсы Jet Signal. Рабочие столы



Интерфейсы Jet Signal. Карточка инцидентов



Интерфейсы Jet Signal. Аналитика



ROADMAP

Jet CSIRT. Roadmap

Команда

Техническая платформа

Лицензия ФСТЭК

Договор с ФСБ

Расширение Fortinet Security Fabric

FortiMail

Forensic

Threat Hunting

Расширение Fortinet Security Fabric

FortiWeb

OSINT

Malware Research

Расширение Fortinet Security Fabric

FortiAnalyzer

СПАСИБО ЗА ВНИМАНИЕ

Алексей Мальнев

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

SECURITYDAY