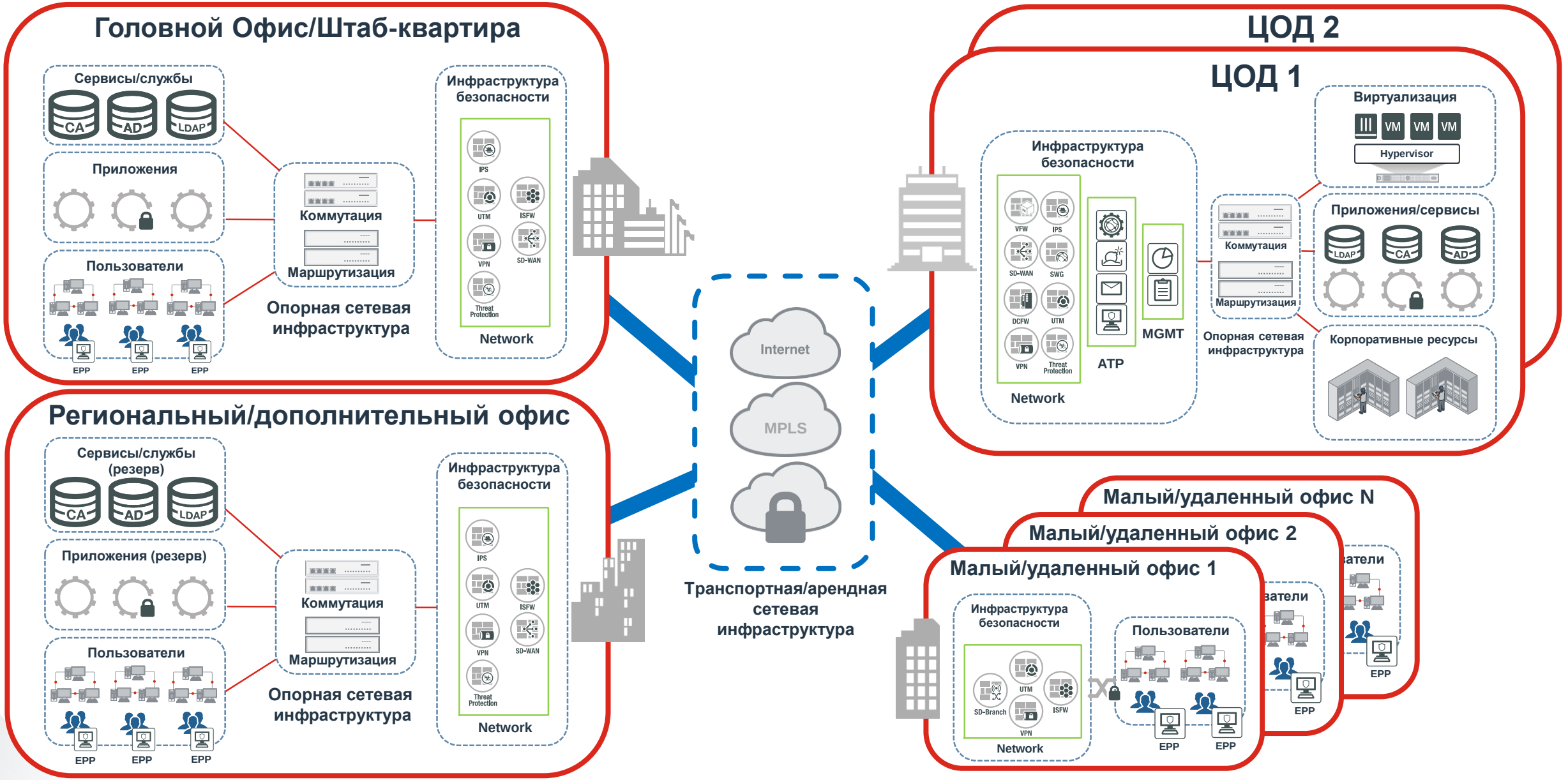
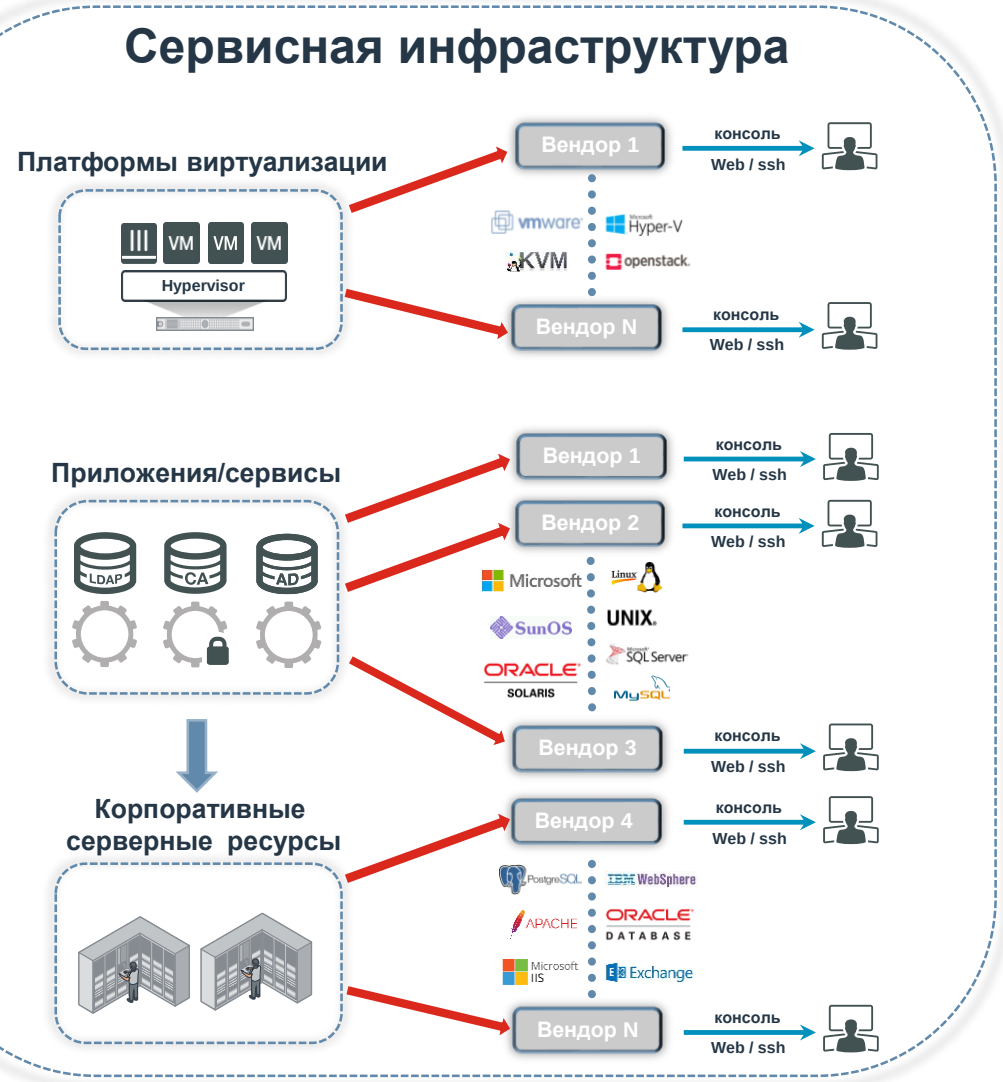
Управление событиями безопасности в неоднородном ИТ окружении

Дмитрий Купецкий, Fortinet

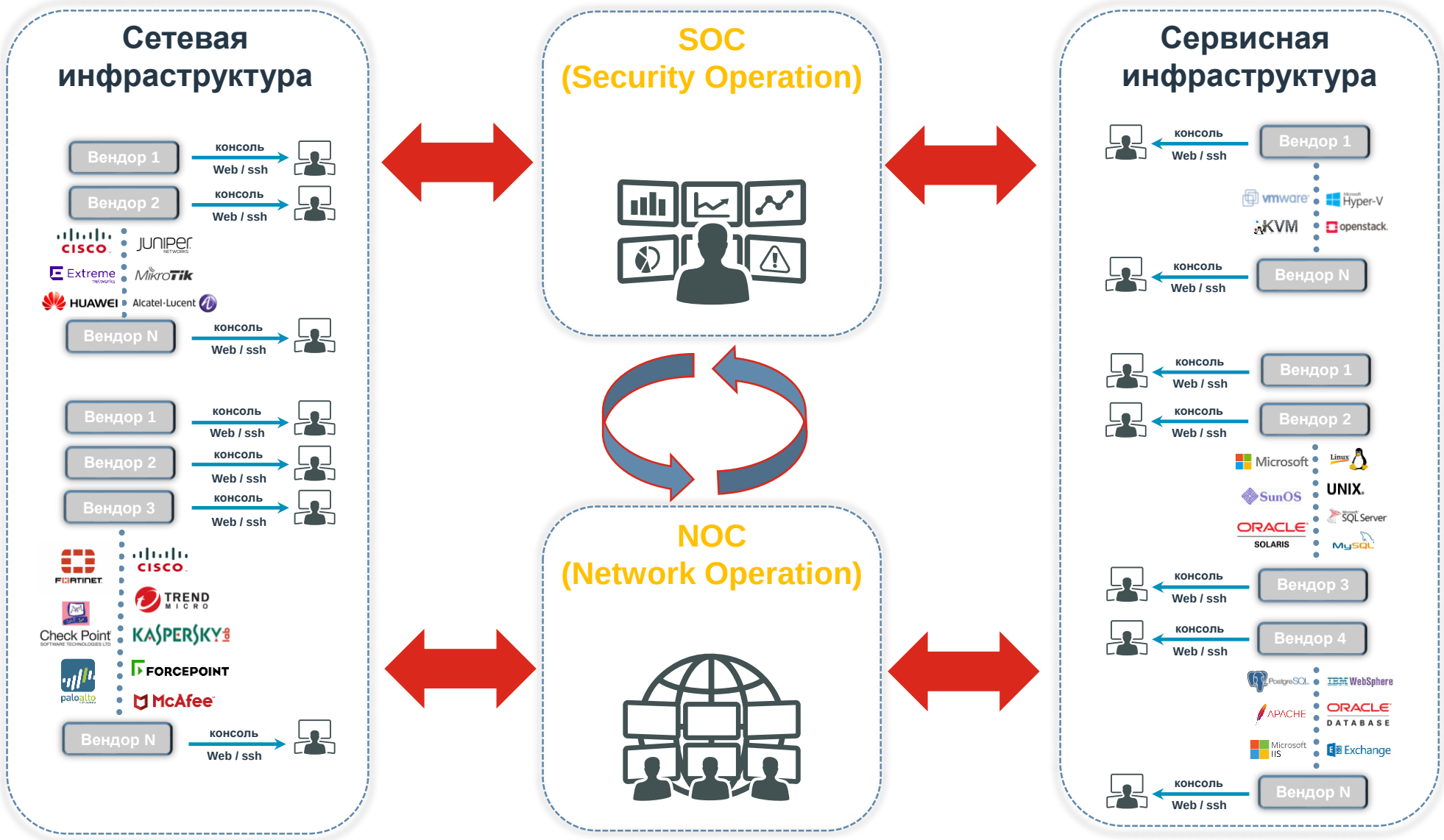
Неоднородная ИТ-инфраструктура



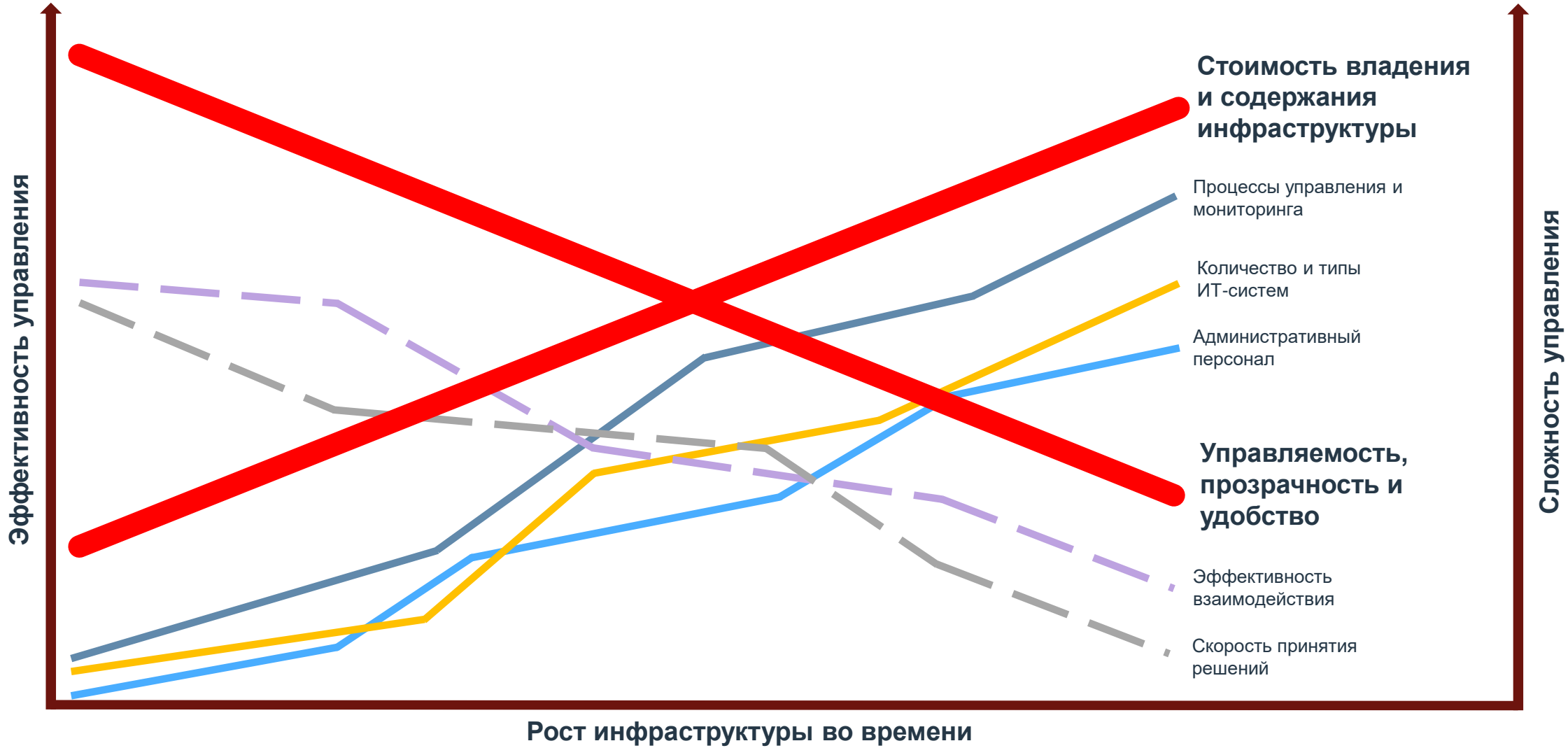
Неоднородная ИТ-инфраструктура



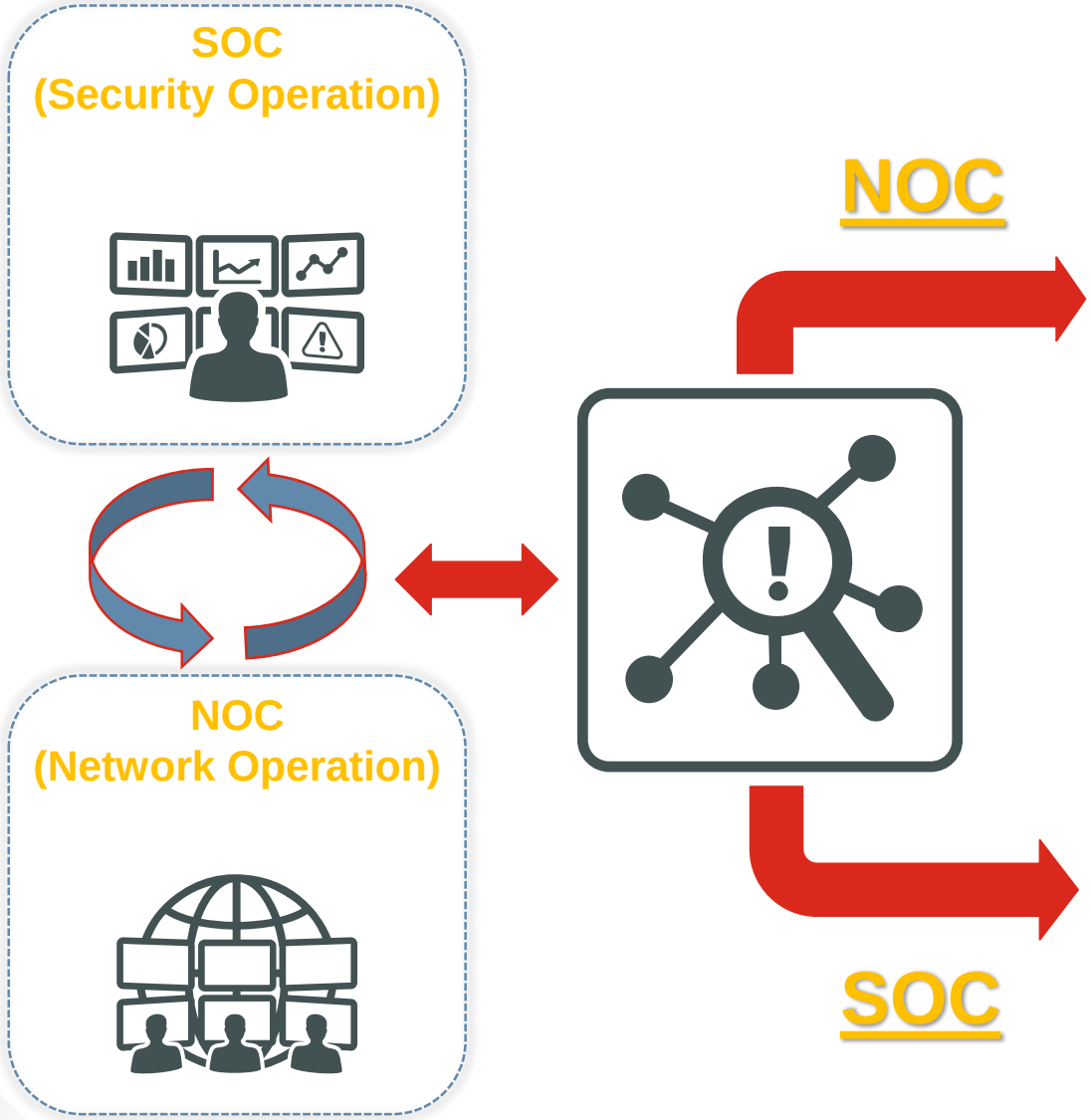
Неоднородная ИТ-инфраструктура



Неоднородная ИТ-инфраструктура



FortiSIEM как инструмент управления событиями ИБ



- **Оперативное управление**
  - Исследование и мониторинг инфраструктуры (Discovering)
  - Автоматически пополняемая база CMDB
  - Мониторинг производительности
  - Мониторинг доступности
  - Мониторинг приложений (метрик)
  - Мониторинг утилизации дискового пространства
  - Мониторинг по заданным синтетическим параметрам
  - Мониторинг изменений – конфигураций, состава ПО и др.
- **Управление инцидентами и событиями безопасности**
  - Сбор, интерпретация и хранение событий
  - Аналитика
  - Корреляция событий в реальном времени
  - Управление инцидентами, система тикетинга и реакции
  - Отчетность и соответствие

FortiSIEM – основные функции

Обнаружение и учет активов

- Всеобъемлюще & точно
- Контекстная оценка
- Оценка уязвимости

Простота внедрения, масштабирование

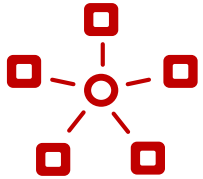
- Поддержка собственных устройств
- Горизонтальное масштабирование

Автоматизация

- Реагирование на инциденты
- Управление кейсами/заявками
- Автоматизация противодействия

Единая точка управления/мониторинга

- Единый интерфейс (GUI)
- Унификация функционала NOC/SOC
- Мониторинг производительности инфраструктуры



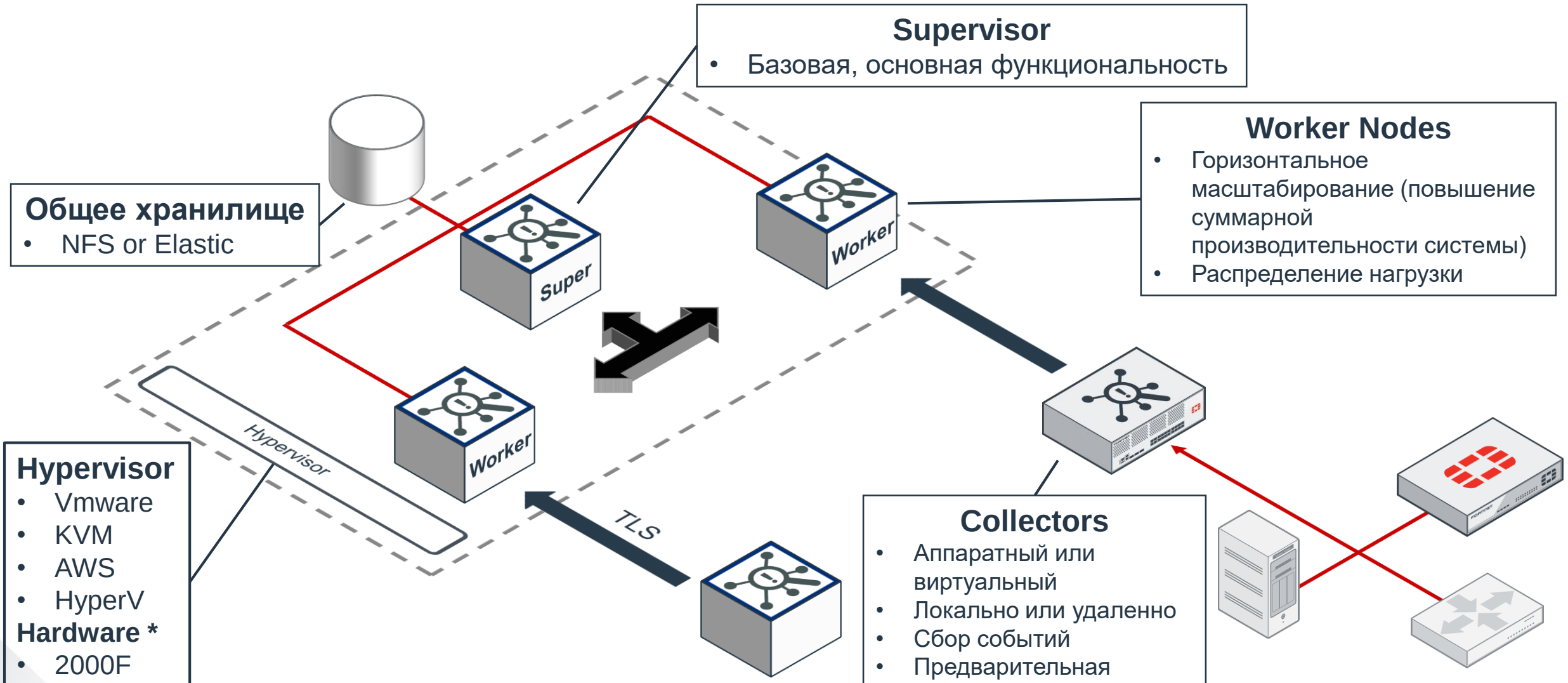
Унифицированная платформа

- Multi-tenancy
- Ролевая модель доступа (RBAC)

FortiGuard

- FortiGuard: данные об угрозах (threat feed)
- Domain, IP and URL – индикаторы компрометации

Масштабируемая архитектура



Supervisor
- Базовая, основная функциональность

Общее хранилище
- NFS or Elastic

Worker Nodes
- Горизонтальное масштабирование (повышение суммарной производительности системы)
- Распределение нагрузки

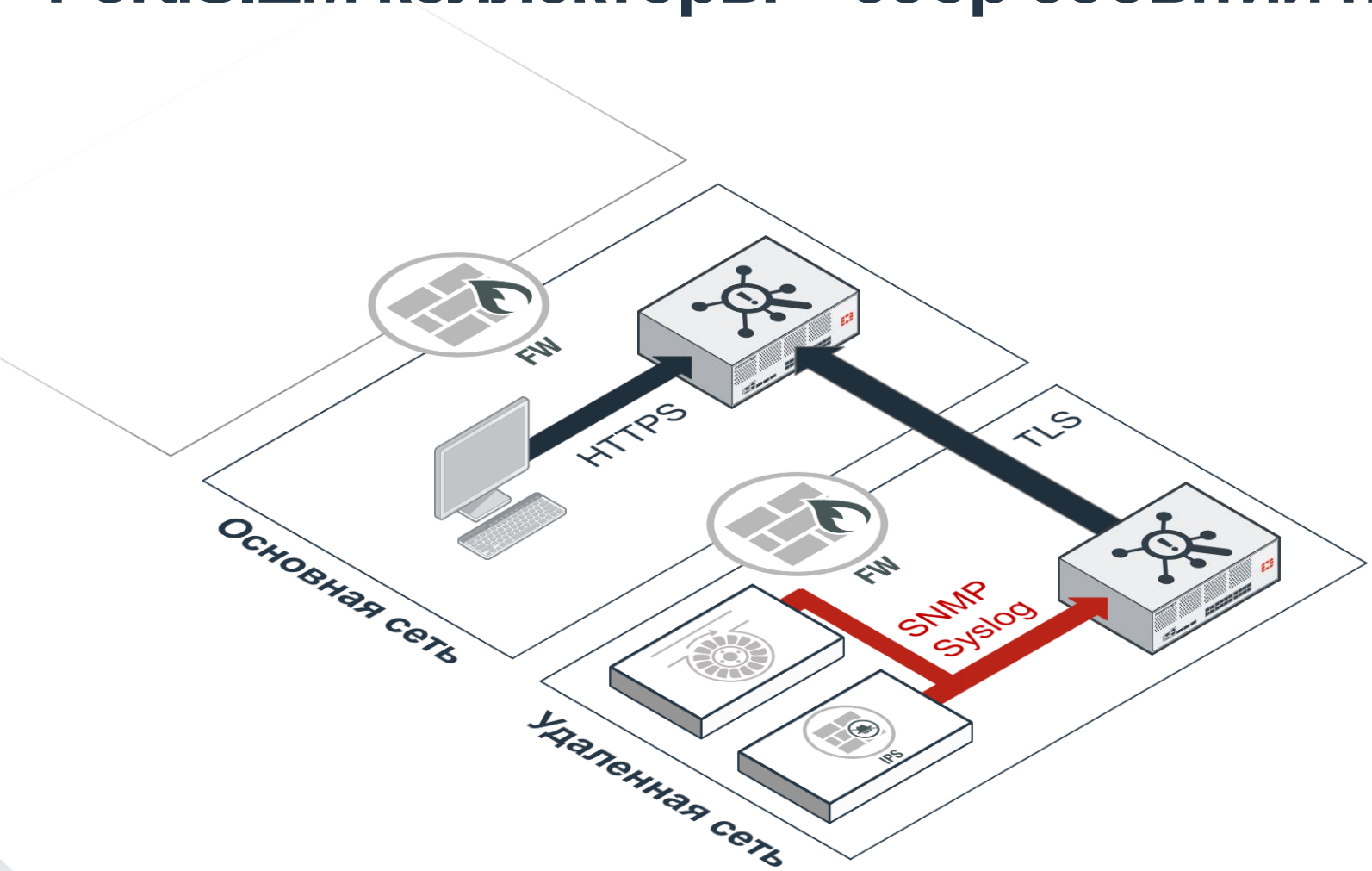
Hypervisor
- Vmware
- KVM
- AWS
- HyperV

Hardware *
- 2000F
- 3500F

Collectors
- Аппаратный или виртуальный
- Локально или удаленно
- Сбор событий
- Предварительная обработка

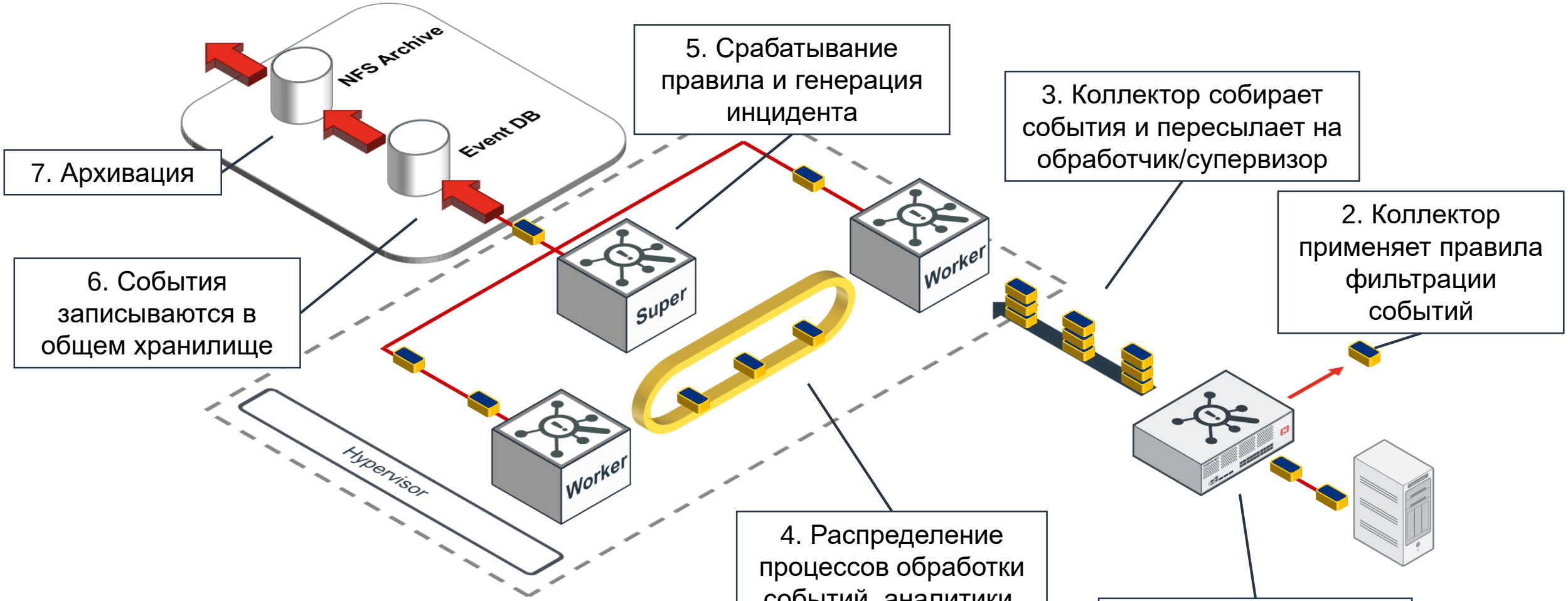
*** Аппаратный кластер поддерживается, начиная с 5.1.3 / 5.2.1**

FortiSIEM коллекторы – сбор событий на удаленных сайтах

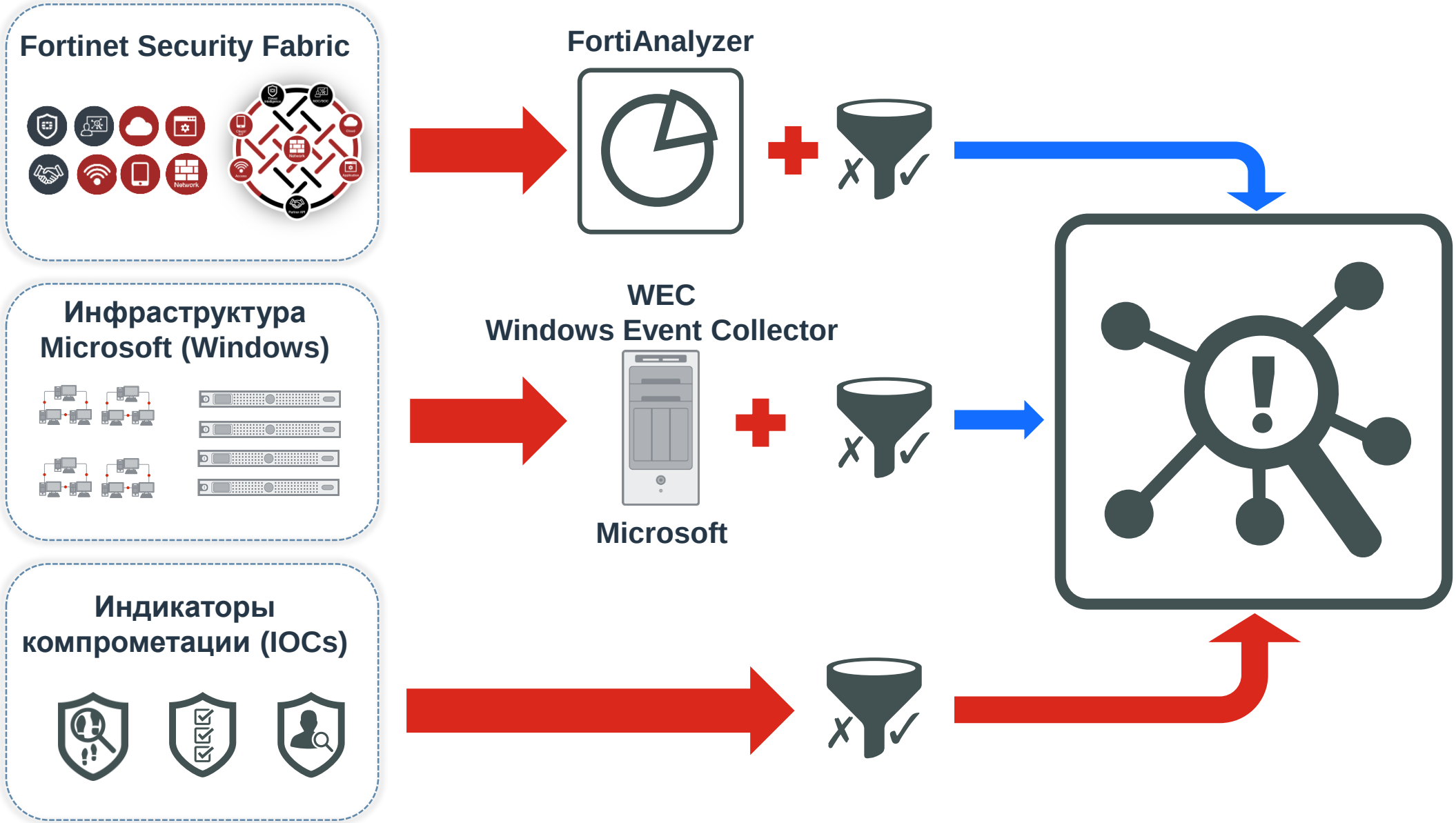


- Сбор событий устройств на удаленных площадках
- Передача по защищенному каналу
- Первичная обработка
- Сжатие событий перед передачей
- Обнаружение (discovery) инфраструктуры удаленной площадки
- Мониторинг метрик производительности

FortiSIEM: процесс обработки событий



FortiSIEM: дополнительные инструменты



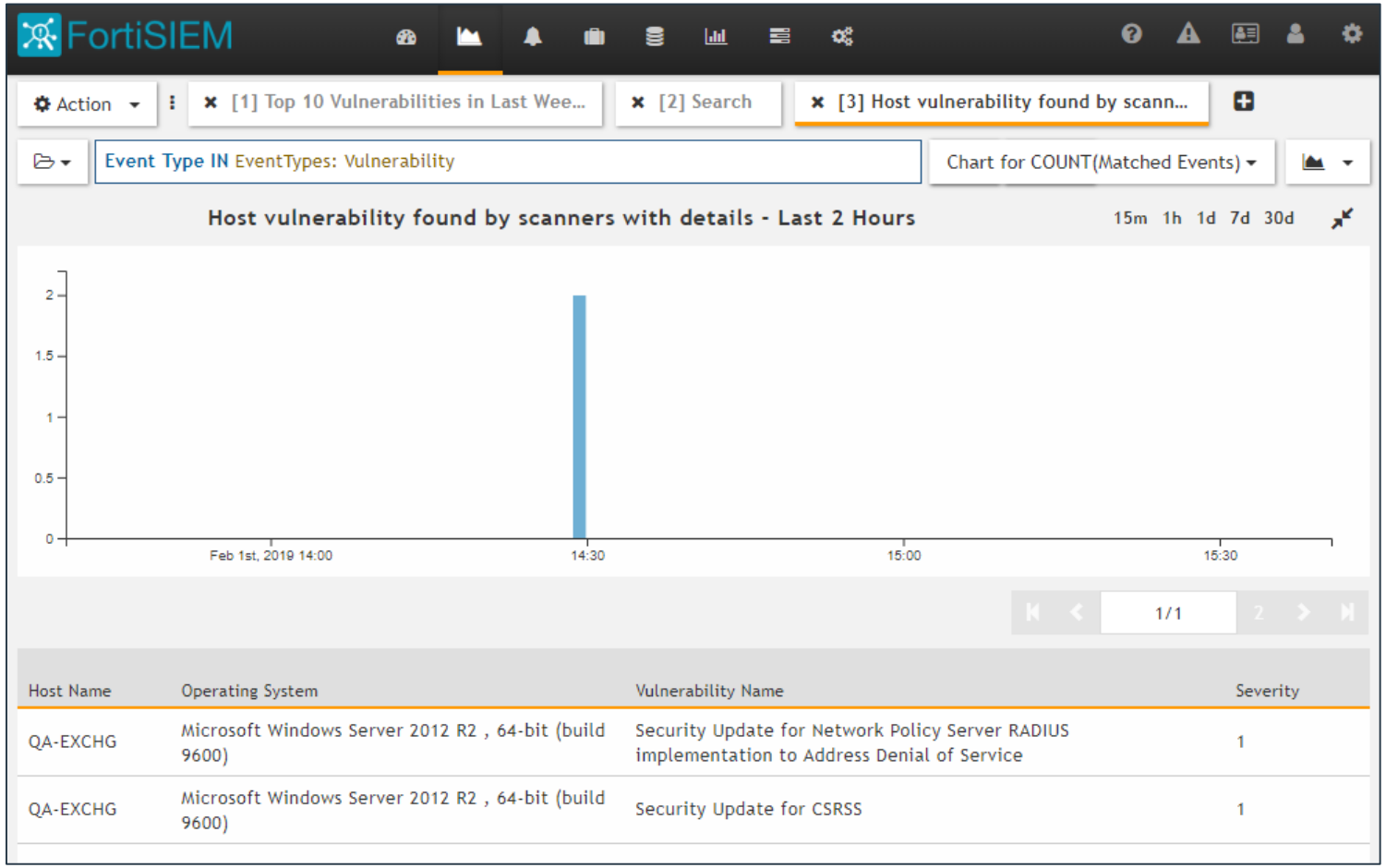
FortiSIEM: интеграция со сканерами уязвимостей

Поддерживаемые сканеры уязвимостей

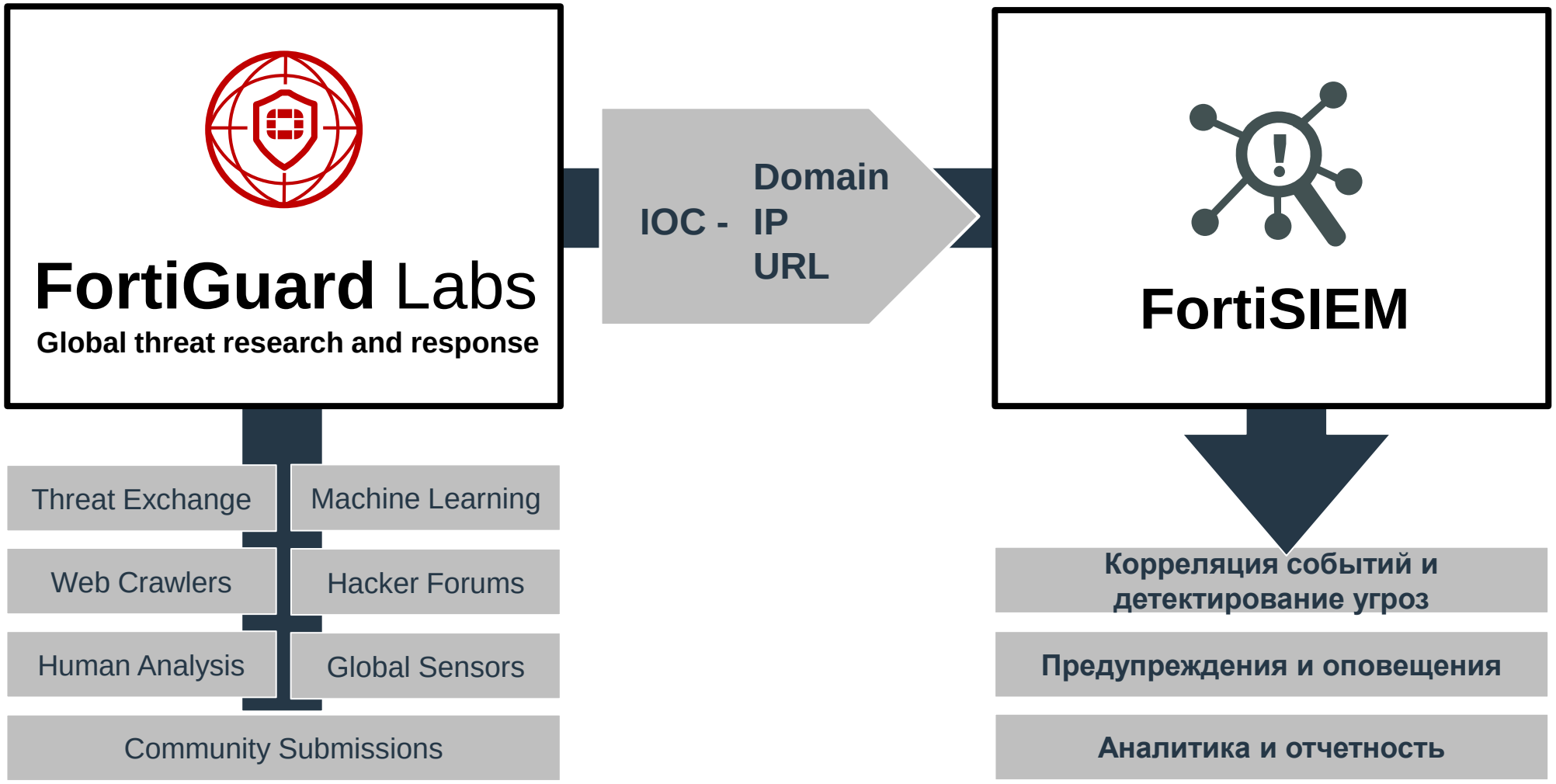
- FortiClient
- Tenable.io (Nessus)
- Rapid7 InsightVM
- McAfee Foundstone
- Qualys

Интегрировано в:

- CMDB
- Queries / Reports
- Host Risk Score



FortiGuard: глобальная база данных угроз



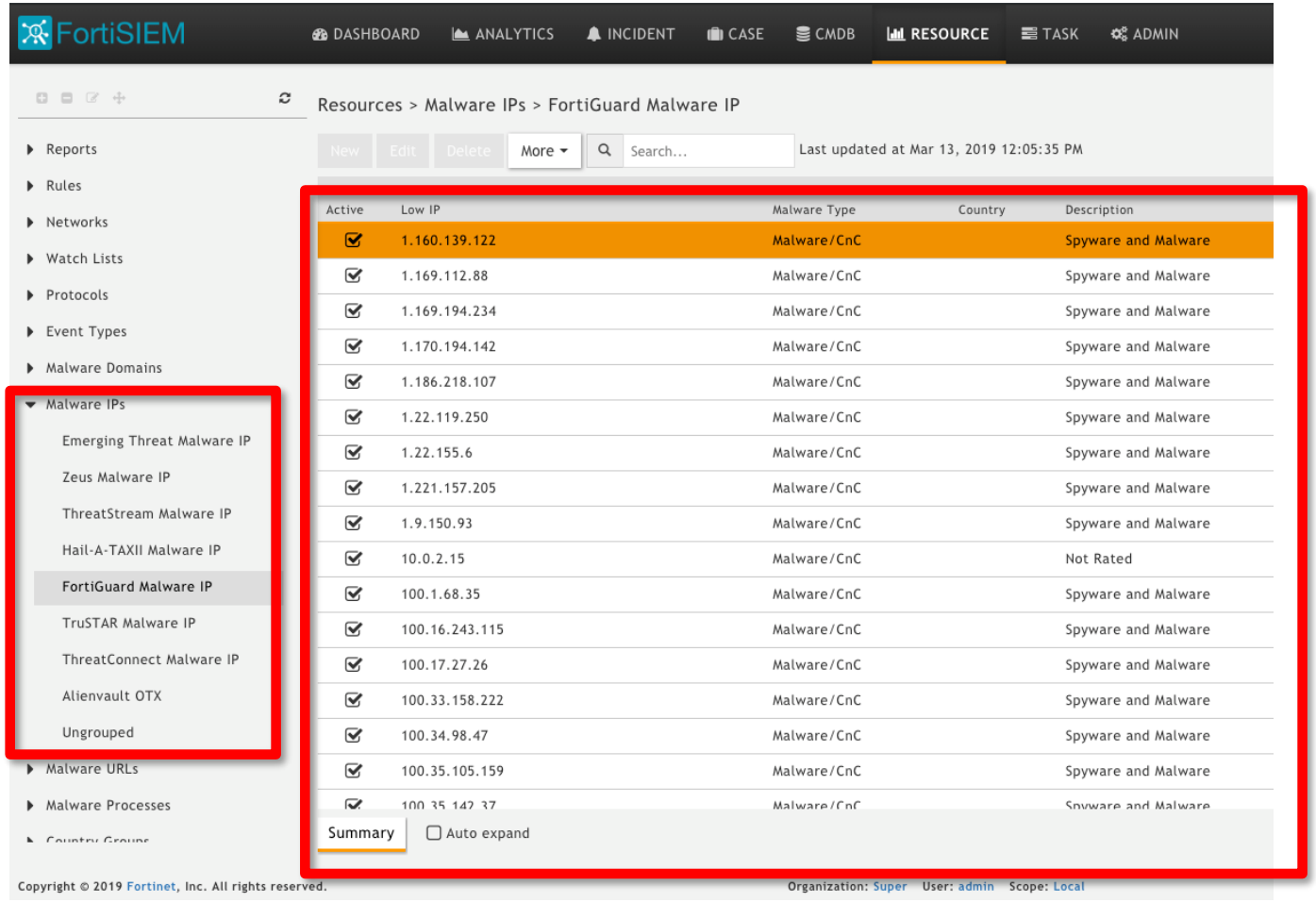
FortiSIEM: обнаружение и противодействие угрозам

1

- **Использование Сетевых индикаторов компрометации (IOCs).**

- **STIX v1.2 and v2 Support**
- **TAXII Support**
- **FortiGuard IOC**
- **3rd Party Commercial IOC Feeds**
- **CSV**

Threat Intelligence



FortiSIEM: обнаружение и противодействие угрозам

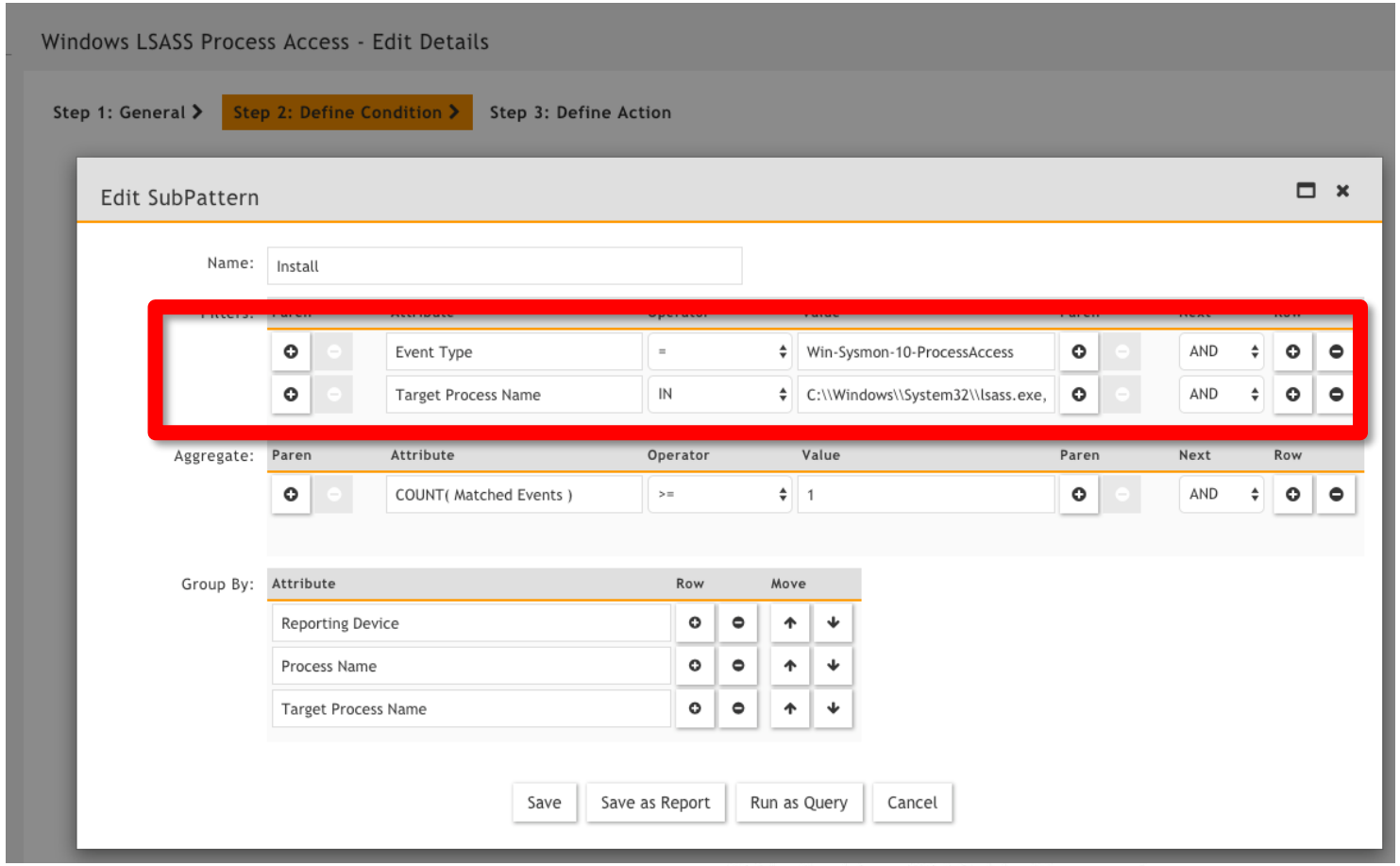
Rules Framework

1. Использование Сетевых индикаторов компрометации

2. **Использование Системных индикаторов компрометации**

- **Встроенные правила для предупреждения о подозрительной активности**
- **Sysmon - набор правил.**

Windows Remote Thread in LSASS



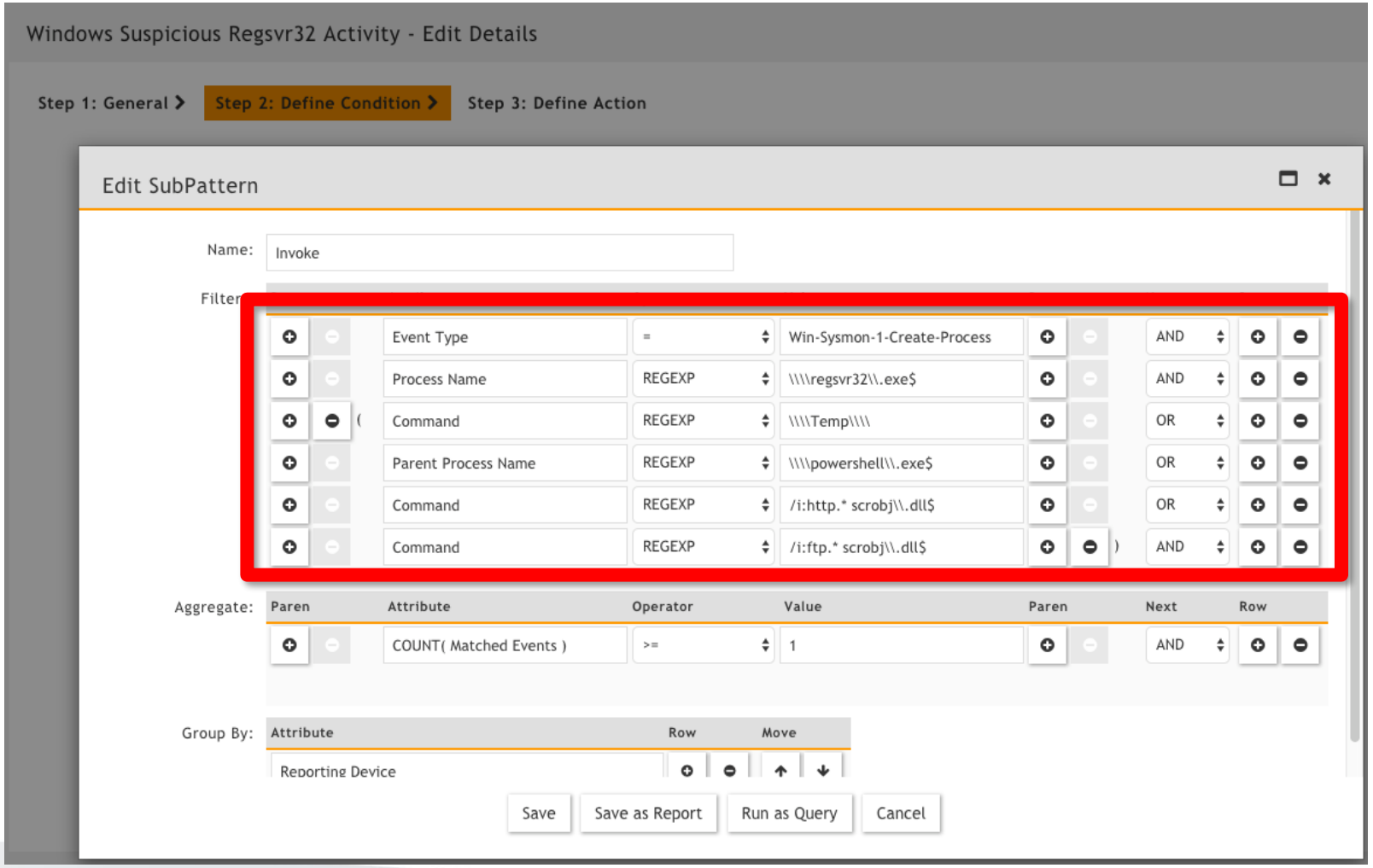
FortiSIEM: обнаружение и противодействие угрозам

1. Использование Сетевых индикаторов компрометации

2. **Использование Системных индикаторов компрометации**

Rules Framework

Windows Suspicious Regsvr32 Activity



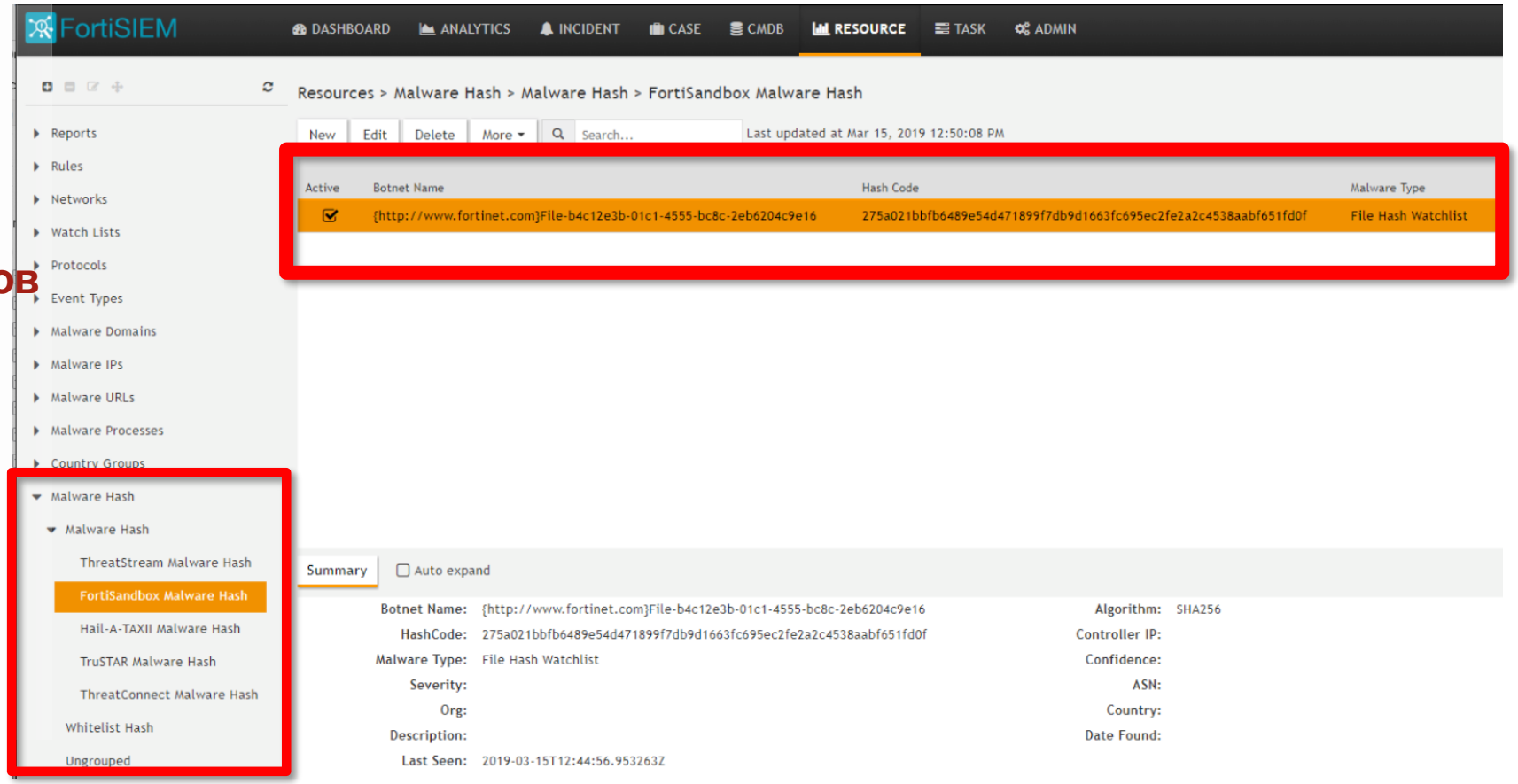
FortiSIEM: обнаружение и противодействие угрозам

1. Использование Сетевых индикаторов компрометации

2. **Использование Системных индикаторов компрометации**

Malware Hash

FortiSandbox -> FortiSIEM

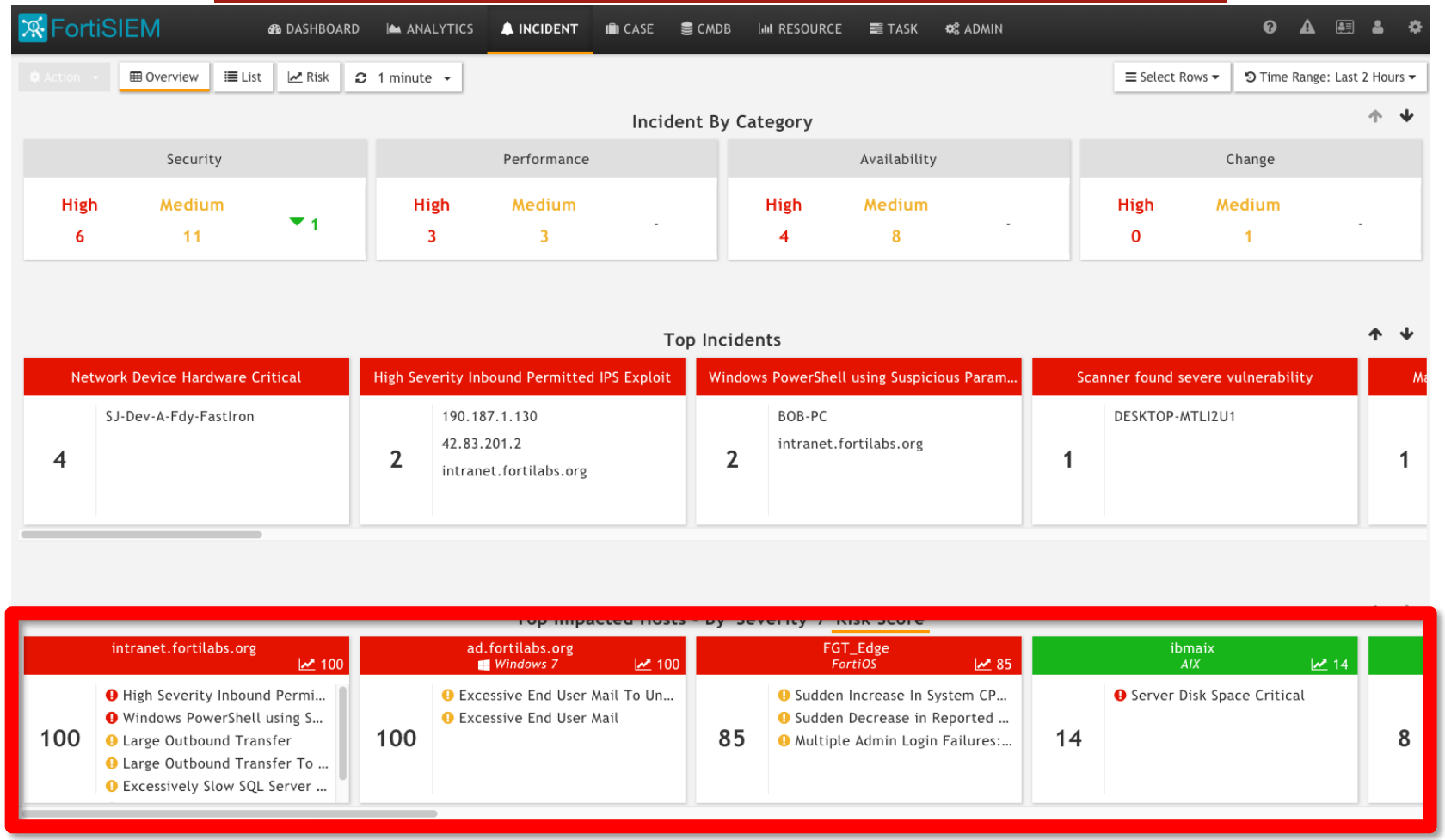


FortiSIEM: обнаружение и противодействие угрозам

1. Использование Сетевых индикаторов компрометации
2. Использование Системных индикаторов компрометации
3. **Обнаружение аномального поведения**

Высокорисковые Активы могут быть легко идентифицированы

Аналитика – Risk Profile

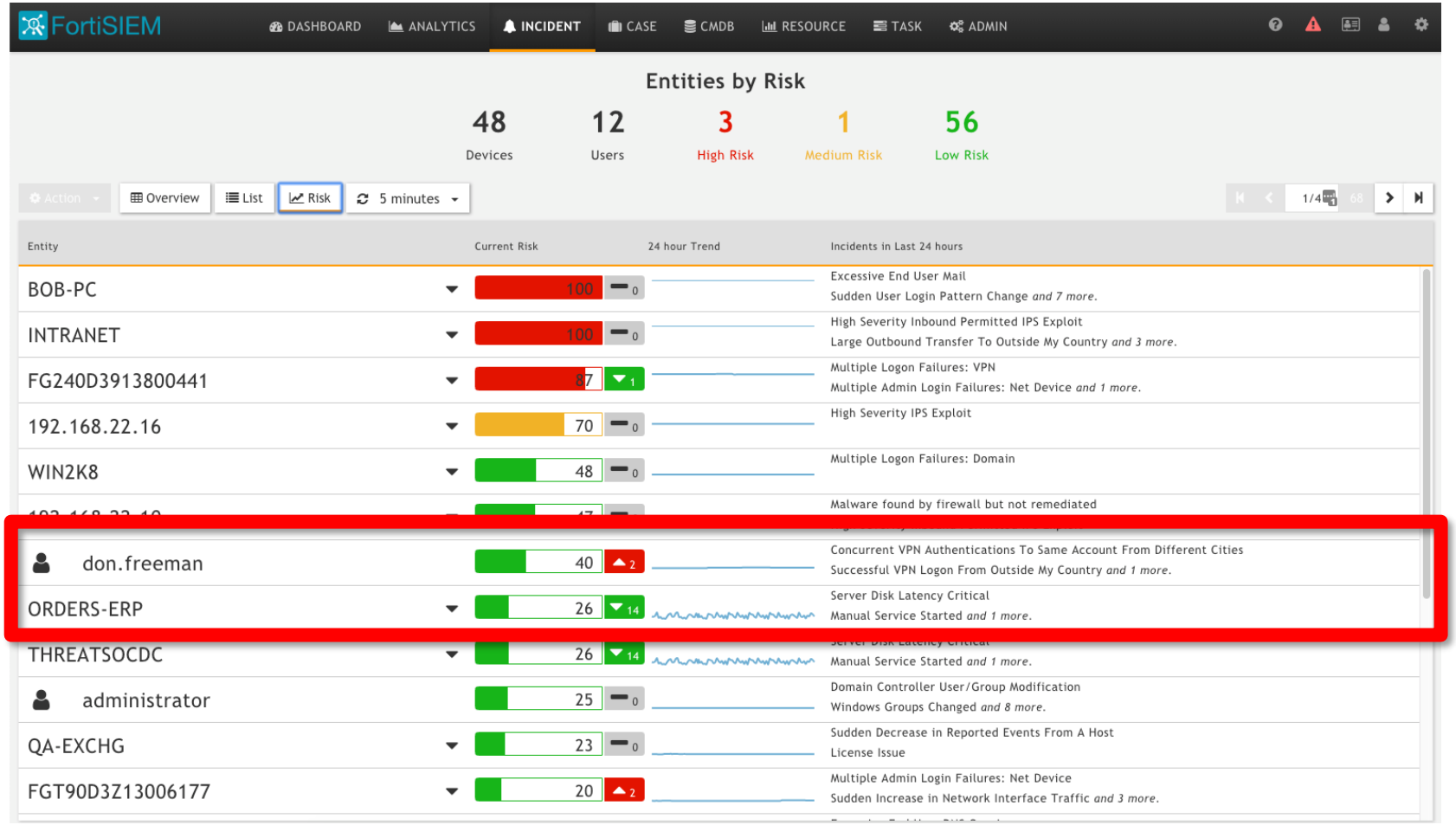


FortiSIEM: обнаружение и противодействие угрозам

1. Использование Сетевых индикаторов компрометации
2. Использование Системных индикаторов компрометации
3. **Обнаружение аномального поведения**

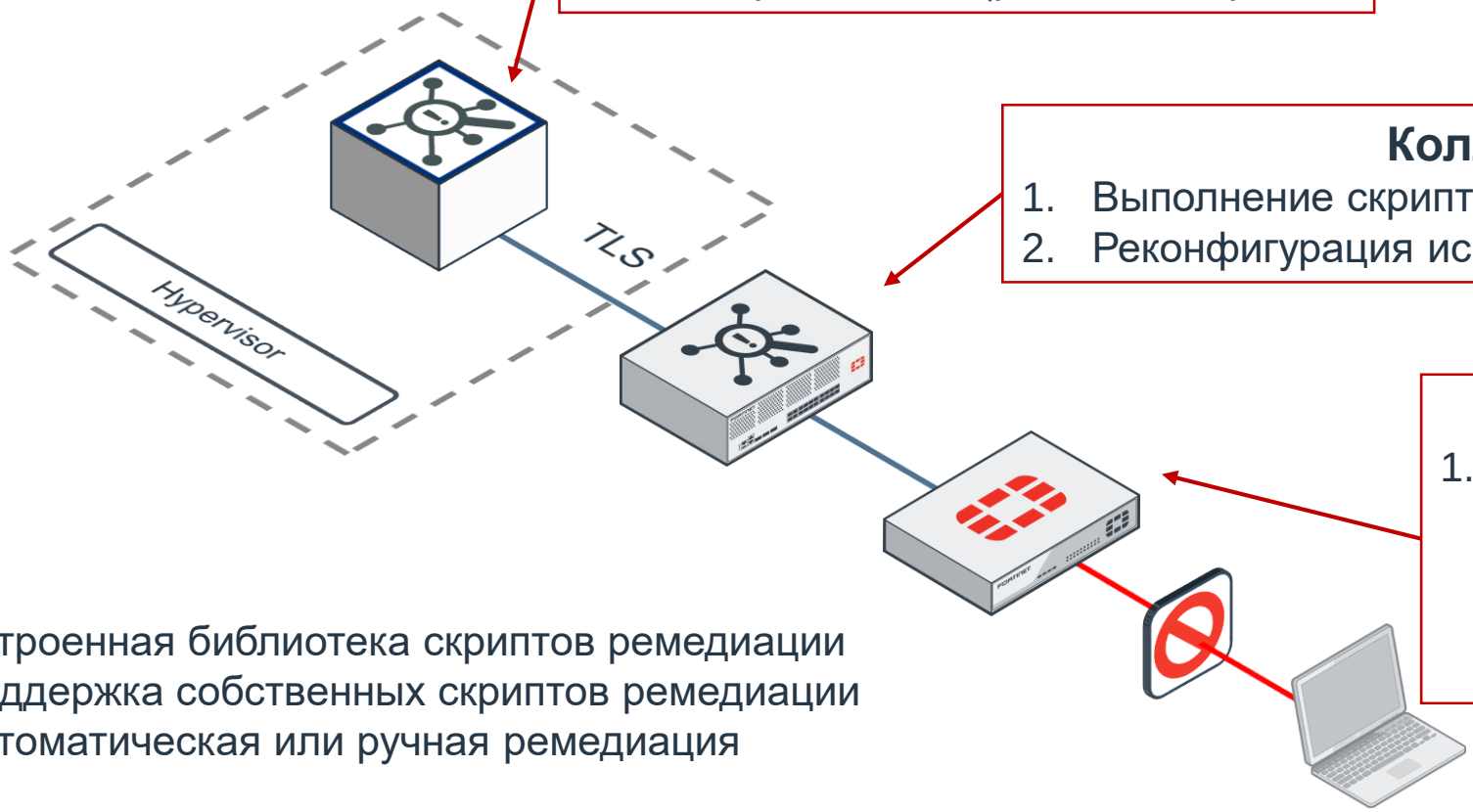
Пользователи с высоким уровнем риска могут быть легко идентифицированы.

Аналитика – Risk Profile



FortiSIEM: реагирование (исправление) в рамках инцидента

Супервизор
1. Срабатывание правила корреляции
2. Генерация инцидента
3. Выбор действия (ремедиация)



Коллектор
1. Выполнение скрипта ремедиации
2. Реконфигурация исполнительного устройства

Исполнительное устройство
1. Применяет заданное действие
   1. Блокировка/карантин
   2. Де-аутентификация пользователя
   3. И т.д.…

- Встроенная библиотека скриптов ремедиации
- Поддержка собственных скриптов ремедиации
- Автоматическая или ручная ремедиация


FORTINET