

FORTINET® SECURITY DAY

VIRTUAL

Управление событиями ИБ – как основа
стратегии развития инфраструктуры

Дмитрий Купецкий, SE



Стратегия развития среды (ИТ-инфраструктуры)

Зачем в принципе нужна стратегия развития?



Положительный фактор взаимодействия:
система функционирует максимально эффективно, изменений не требуется



Неизвестный фактор взаимодействия:
система испытывает воздействие, но еще не обладает накопленными аналитическими данными о его свойствах и/или эффекте

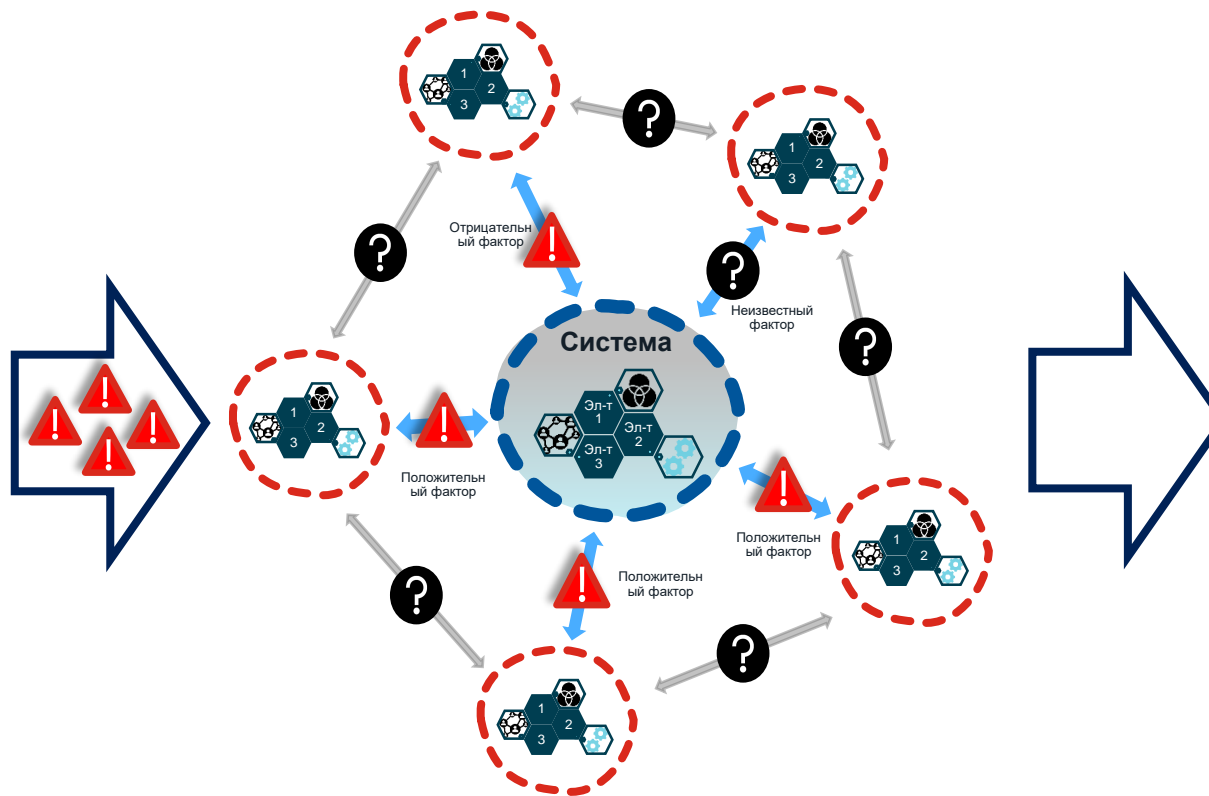


Отрицательный фактор взаимодействия:
функционирование системы деградирует, эффективность становится отрицательной, выявляется потенциальная угроза существования системы

Накопление отрицательных факторов в системе



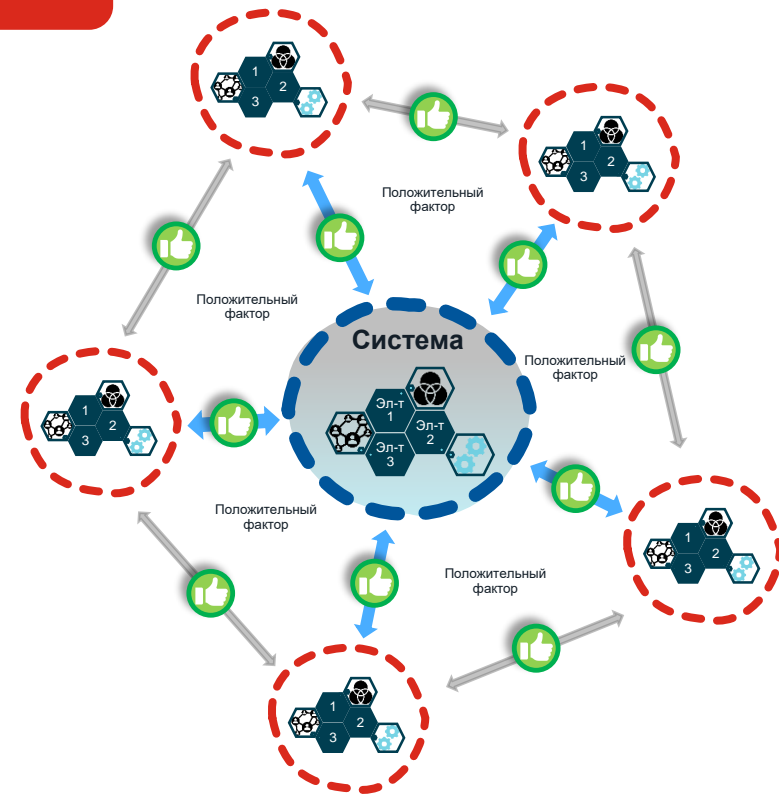
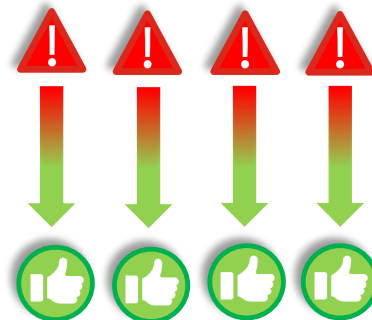
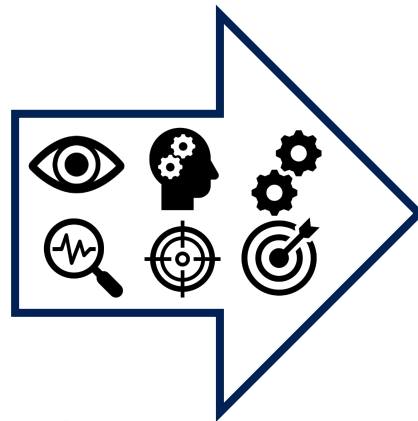
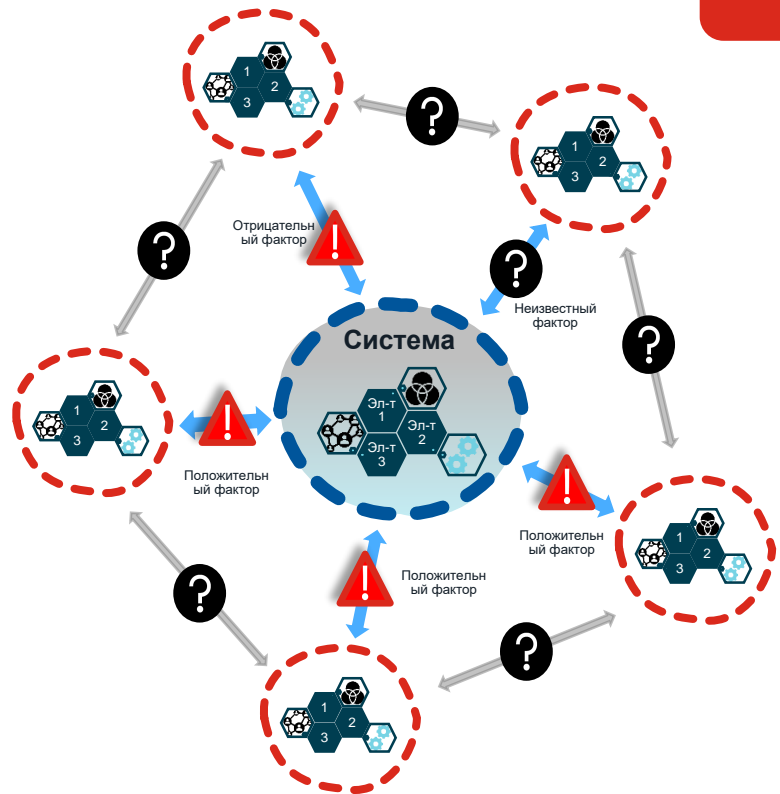
Переход неизвестных факторов в отрицательные



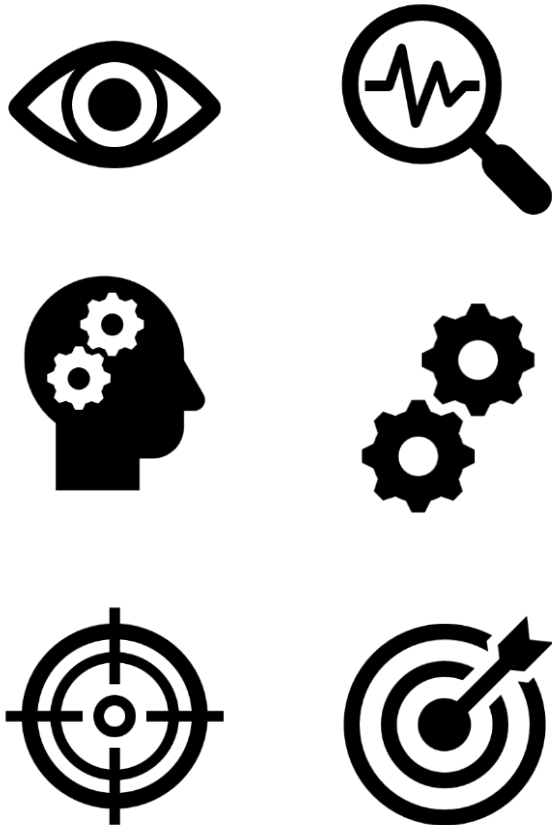
Деградация функционирования системы

Решение проблемы – механизмы адаптации

Инструменты адаптации:
Обнаружение, анализ, защита, противодействие



Стратегия развития



1. **Наличие** стратегии развития системы – это залог ее существования и эволюционного развития

2. **Суть и содержание** стратегии развития организованной системы состоит в выработке и поддержке механизмов адаптации:

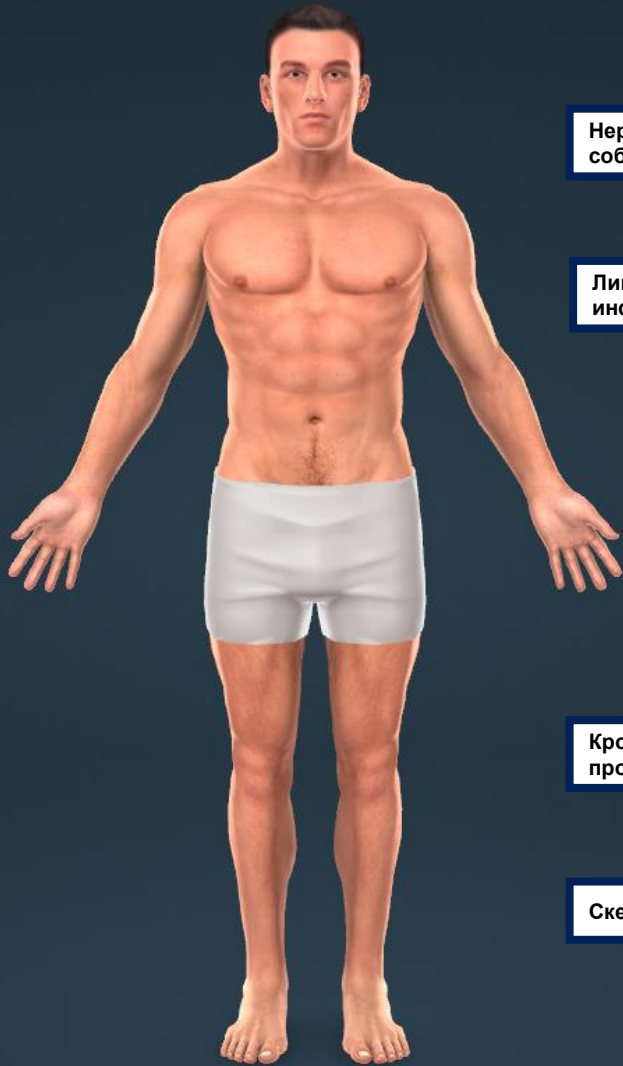
- Обнаружение события/воздействия
- Анализ события/воздействия
- Выбор, либо выработка реакции
- Выбор цели реакции при обнаружении негативного воздействия
- Применение мер противодействия

3. **Результат адаптации** – сохранение и повышение уровня эффективности функционирования и существования системы в условиях агрессивной среды



ИТ-инфраструктура как адаптивная экосистема

Адаптивная экосистема: человек



Нервная система и мозг – системы управления событиями и автоматизации

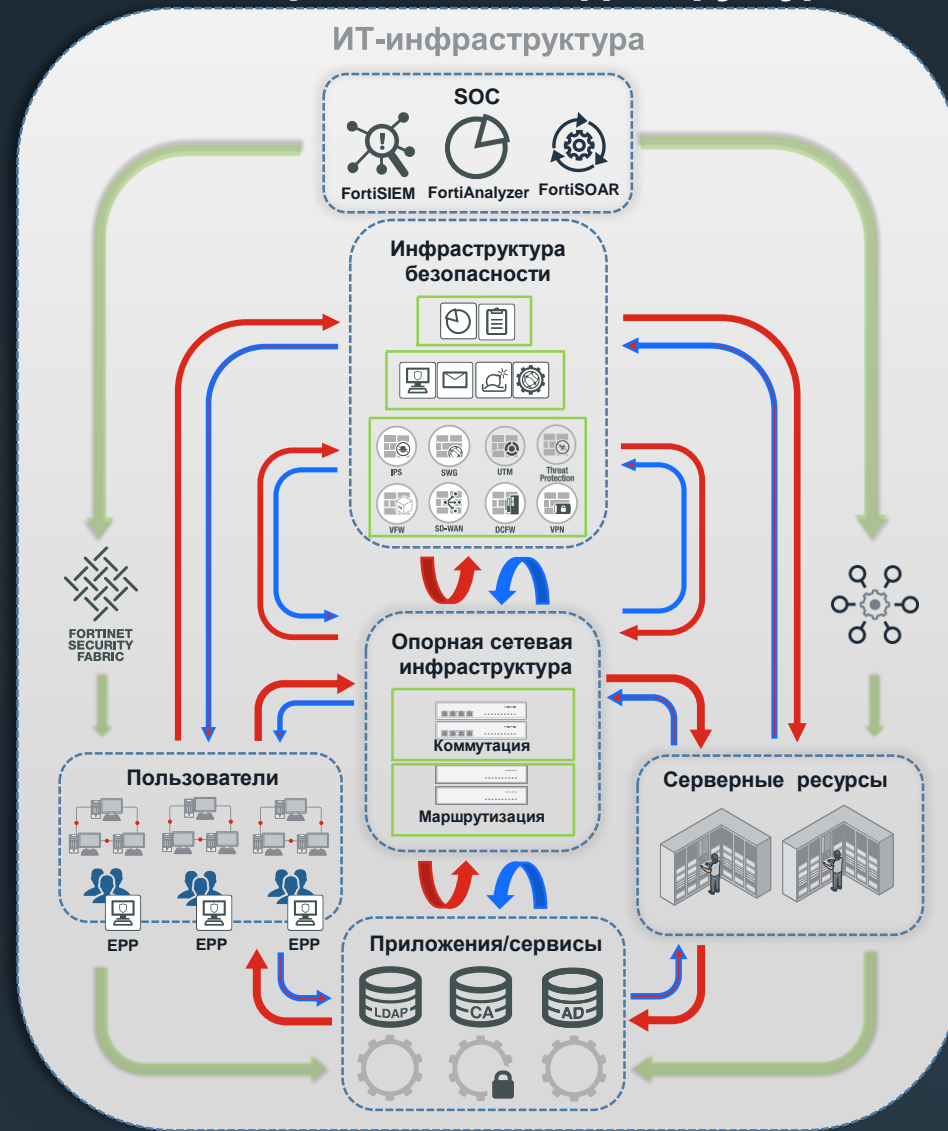
Лимфатическая и иммунная системы – инфраструктура и инструменты безопасности

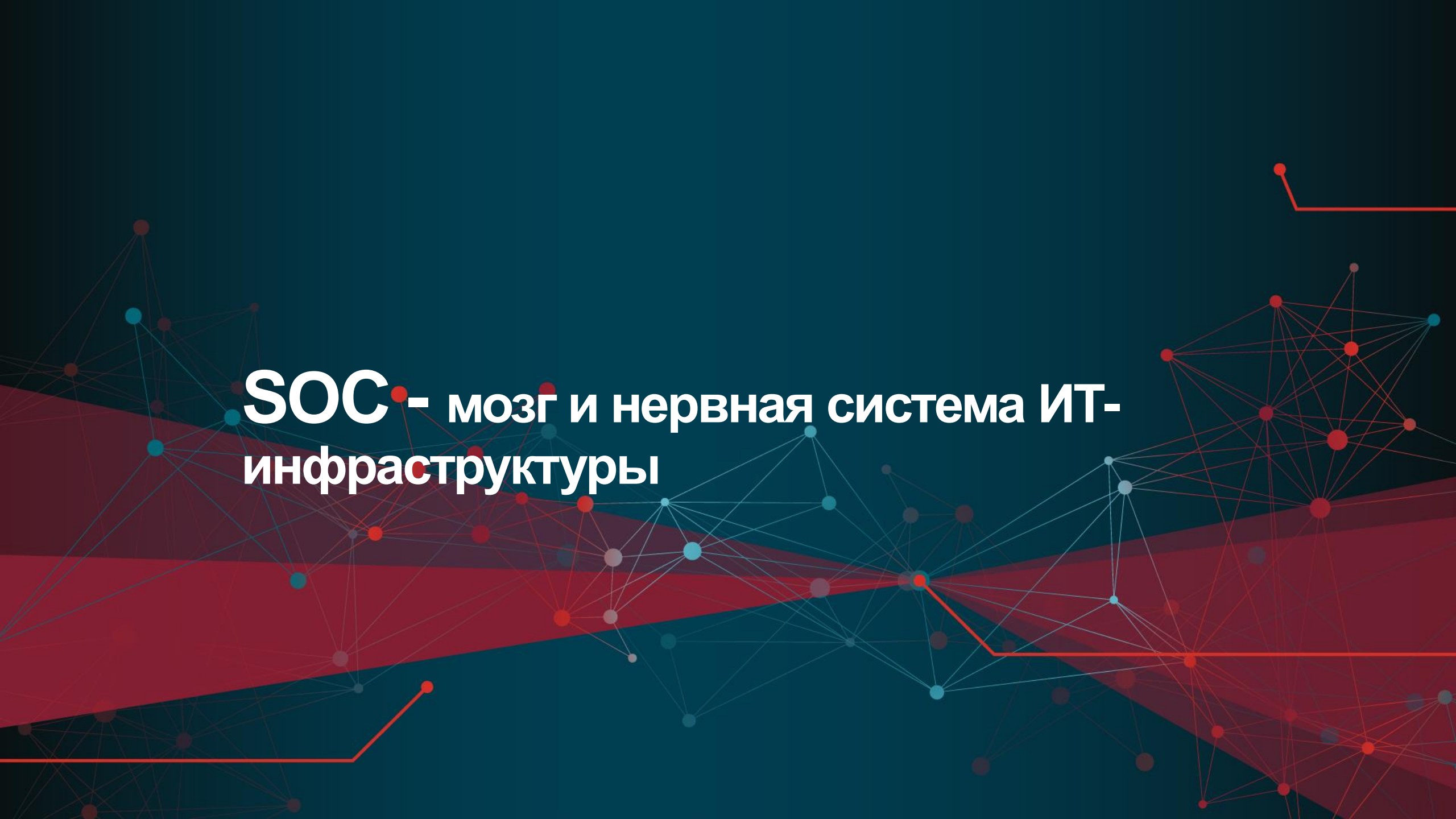


Кровеносная система – циркуляция обменных процессов внутри инфраструктуры

Скелет – опорная сетевая инфраструктура

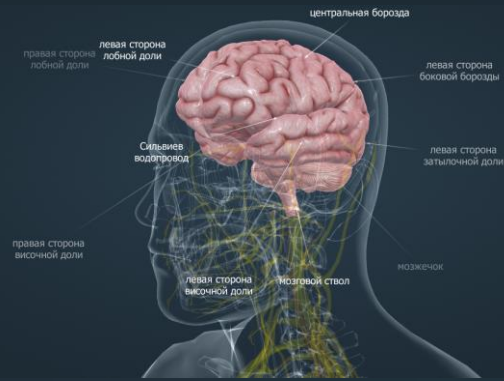
Адаптивная экосистема : неоднородная ИТ-инфраструктура





SOC - мозг и нервная система ИТ-инфраструктуры

Security Operation Center – мозг адаптивной неоднородной ИТ-инфраструктуры



Адаптация организма к изменяющимся условиям внешней среды, противодействие угрозам

Управление нервной деятельностью организма



Работа иммунной системы – ответ на негативные воздействия, обучение



Адаптация ИТ-инфраструктуры к изменяющимся условиям внешней среды, противодействие угрозам

SOC



FortiSIEM FortiSOAR FortiAnalyzer

Управление событиями в ИТ-инфраструктуре:



Работа систем автоматизации – ответ на возникающие инциденты, угрозы, расследование, противодействие

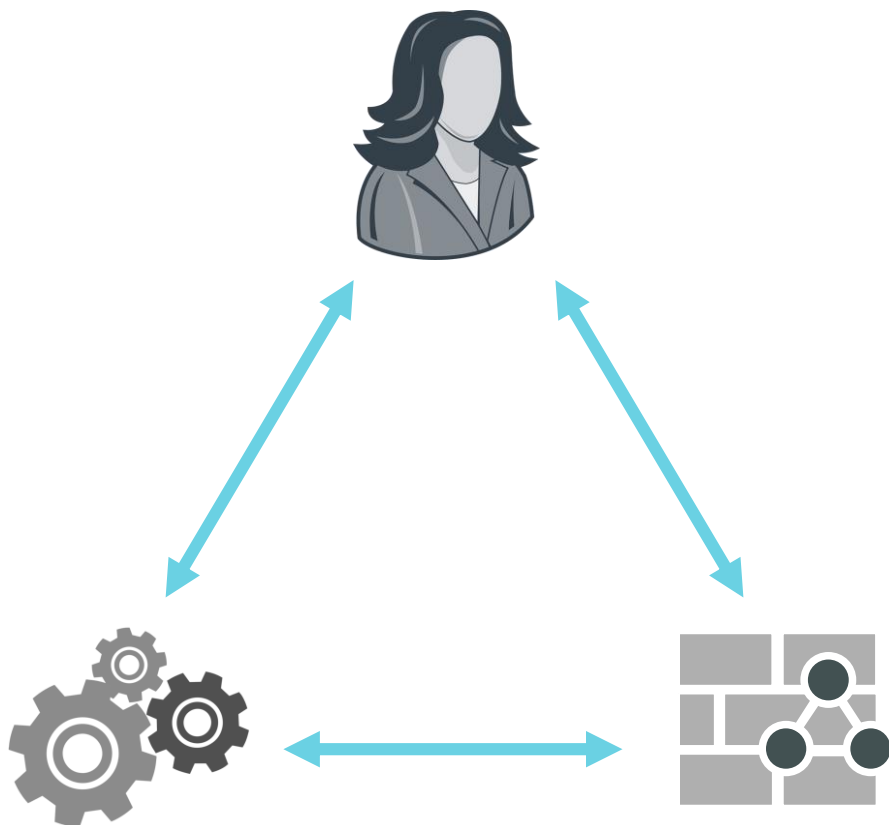


Что такое SOC?

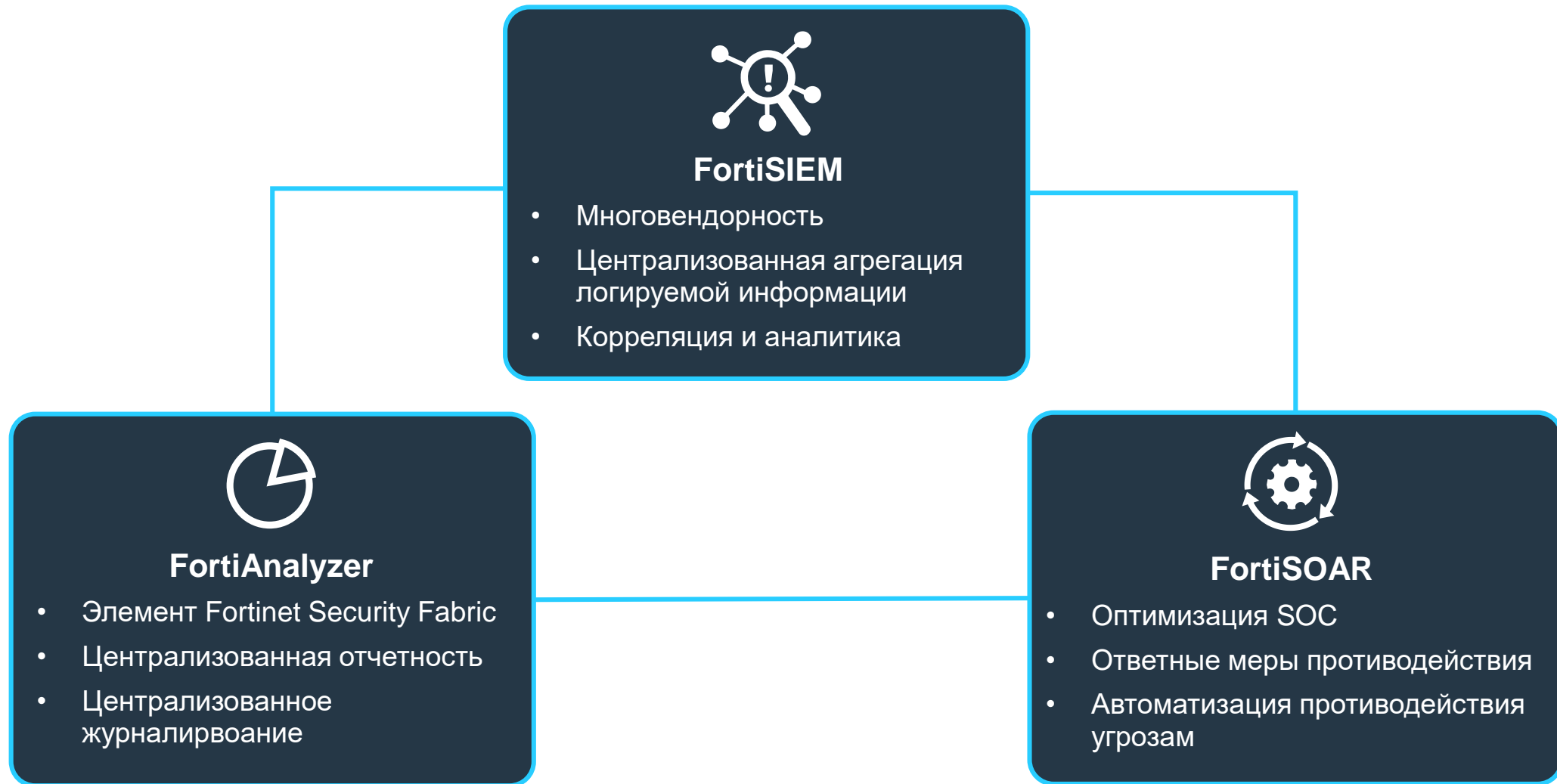
Security Operation Center

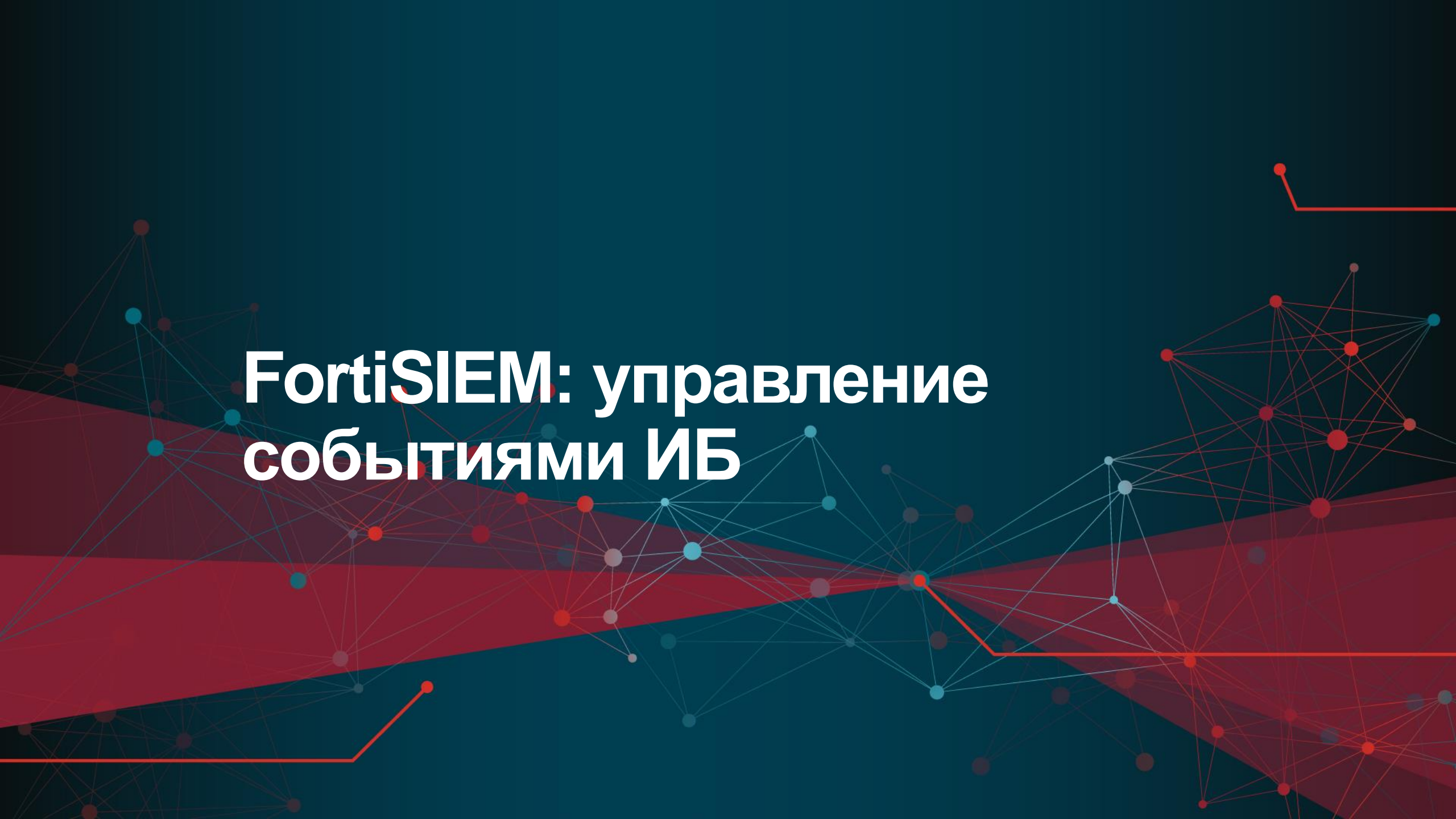
Представляет собой совокупность целевых процессов, реализуемых и поддерживаемых командой квалифицированного персонала посредством специализированных технологий и инструментов, отвечающих за решение таких задач, как:

- *Мониторинг и защита активов ИТ-инфраструктуры;*
- *Детектирование и учет угроз безопасности;*
- *Расследование возникающих инцидентов безопасности (и не только);*
- *Применение и автоматизация мер противодействия возникающим угрозам и разрешение инцидентов.*



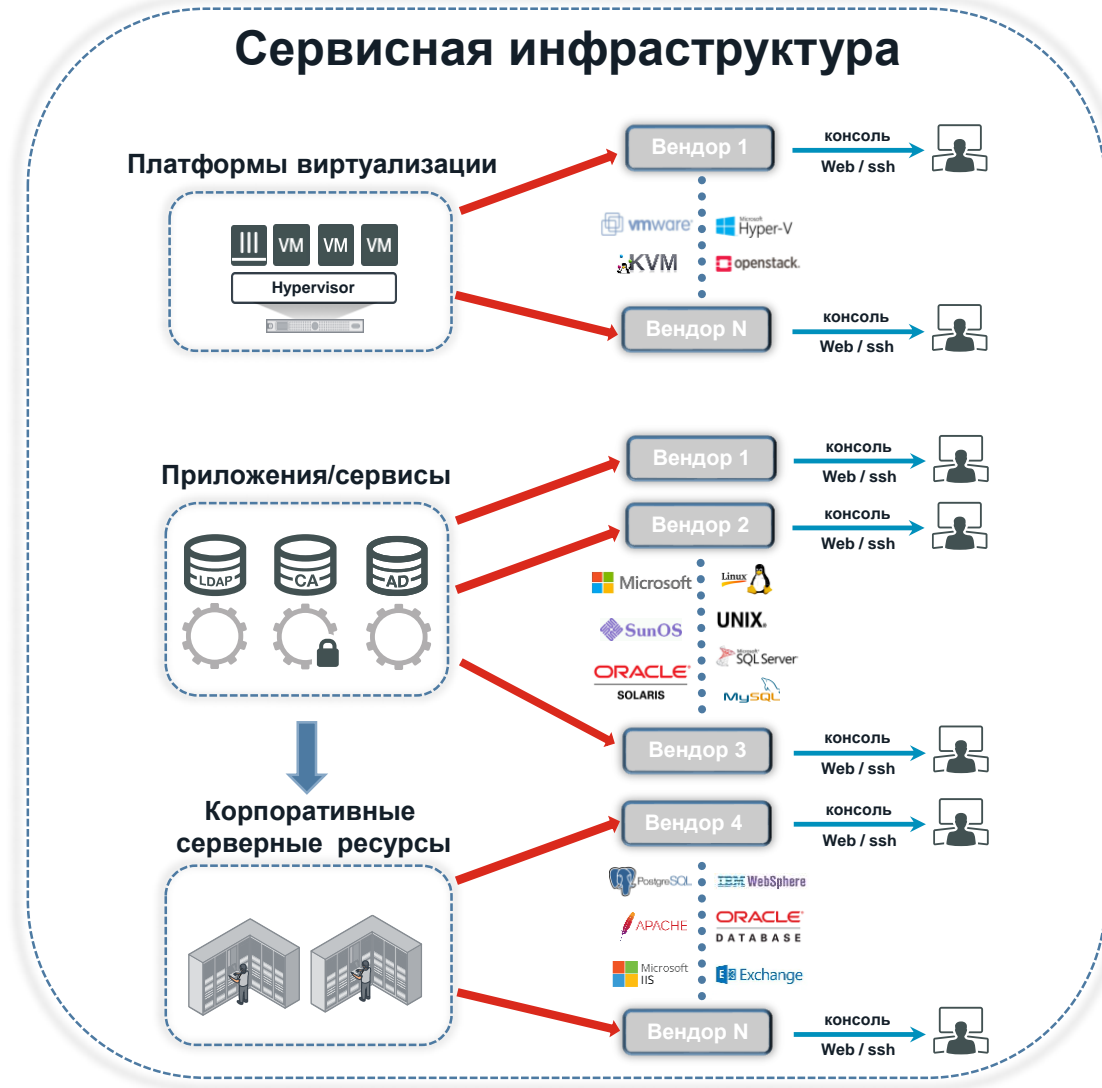
Инструменты SOC – FortiSIEM, FortiSOAR, FortiAnalyzer



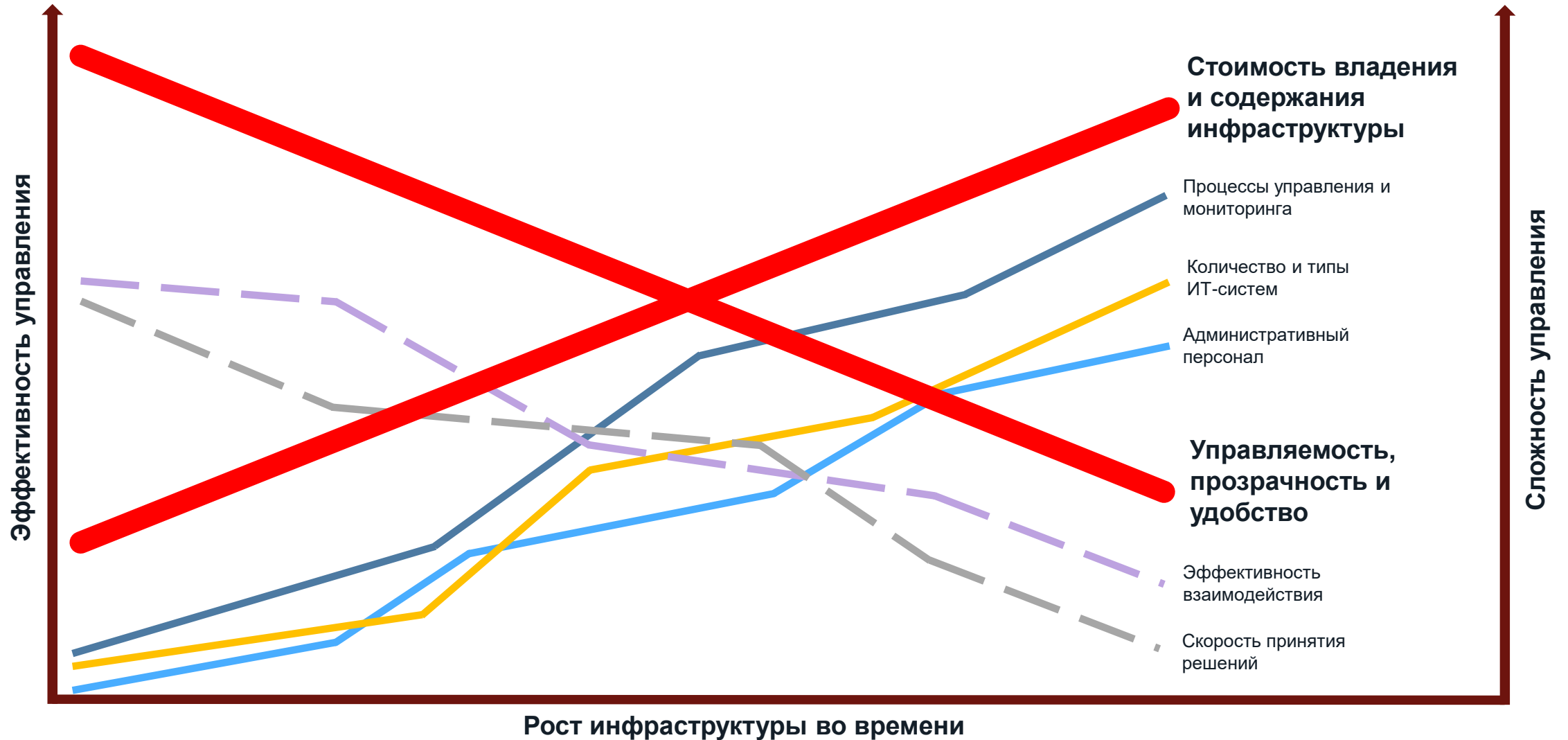


FortiSIEM: управление событиями ИБ

Неоднородная ИТ-инфраструктура



Неоднородная ИТ-инфраструктура



Что такое SIEM?



- SIEM - Security Information & Event Management – система управления событиями информационной безопасности
- Ввод - централизованная точка сбора логов всей инфраструктуры
- Обработка – Анализ/корреляция событий
- Вывод – оповещение/отчетность/текущий мониторинг

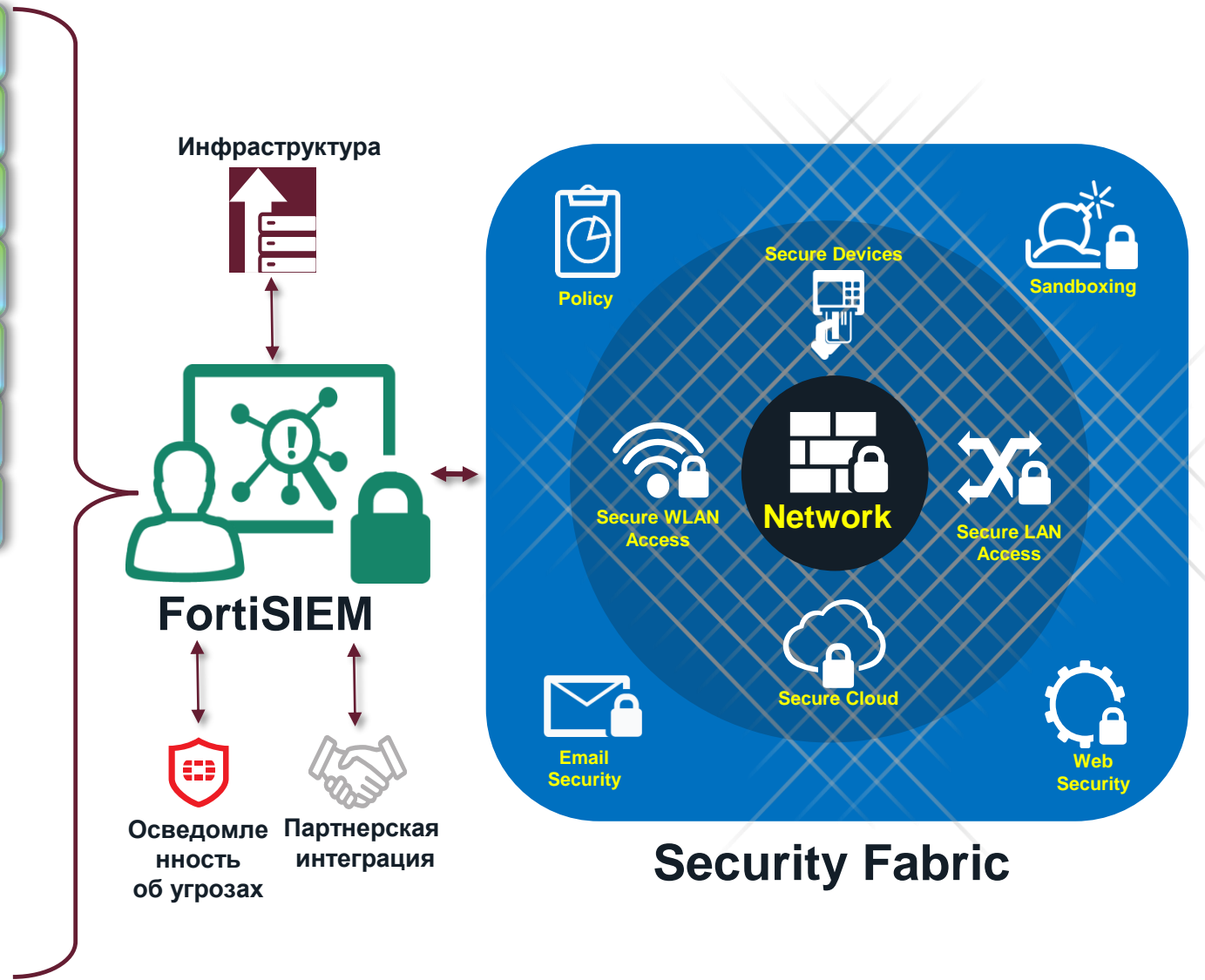
```
May 6 17:55:48 squid[1773]: [ID 702911 local4.info] 192.168.20.39 1715 2.2.2.2 172.16.10.6  
3128 674 - - - - [06/May/2008:17:55:48 -0700] GET "http://mail.abc.com/mail/?" HTTP/1.1 302  
1061 568 "http://www.abc.com/" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.14)  
Gecko/20080404 Firefox/2.0.0.14" TCP_MISS:DIRECT
```



SIEM vs. FortiSIEM

- Единая точка управления
- Аналитика NOC & SOC
- Простая и гибкая интеграция
- Архитектура Multi-Tenant
- Легко масштабируемая архитектура
- Обнаружение активов/конфигураций в режиме реального времени
- Аналитика в режиме реального времени (patented)

Gartner
SIEM
критерии

- ✓ Analytics
- ✓ Application Log Analysis
- ✓ Behavior Profiling
- ✓ Data & User Monitoring
- ✓ Deployment/Support Simplicity
- ✓ Log Management
- ✓ Real-Time Monitoring
- ✓ Threat Intelligence





FortiSOAR: управление инцидентами и автоматизация противодействия

FortiSOAR: основные возможности

Ключевая функциональность FortiSOAR

1. Управление инцидентами и заявками на исполнение
2. Оркестрация и автоматизация
3. Выстраивание процессов и взаимодействий (workflow)
4. Интеллектуальное управление угрозами



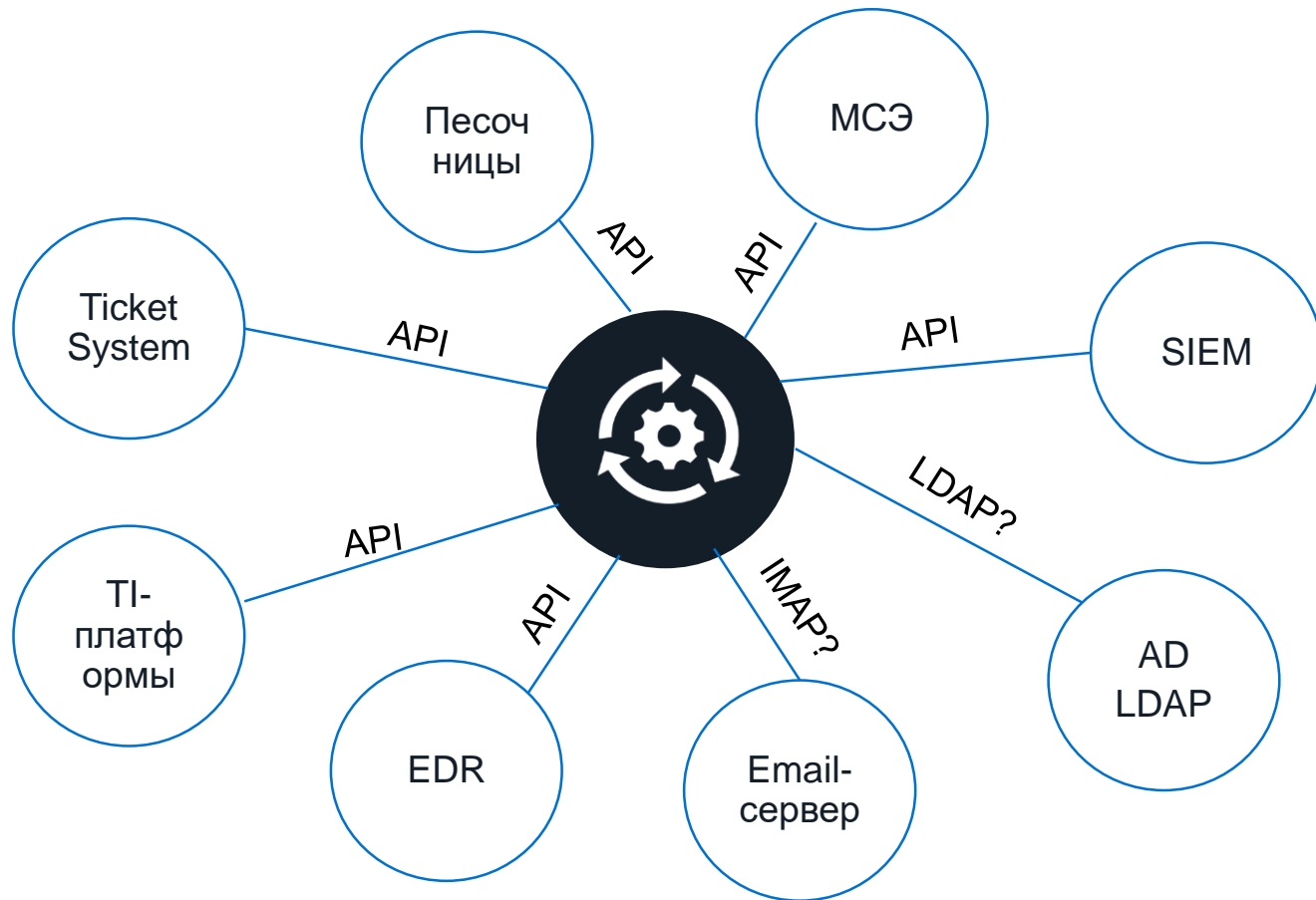
FortiSOAR: управление инцидентами и заявками на исполнение

Типовой сценарий



FortiSOAR: оркестрация и автоматизация противодействия

Методы интеграции/оркестрации



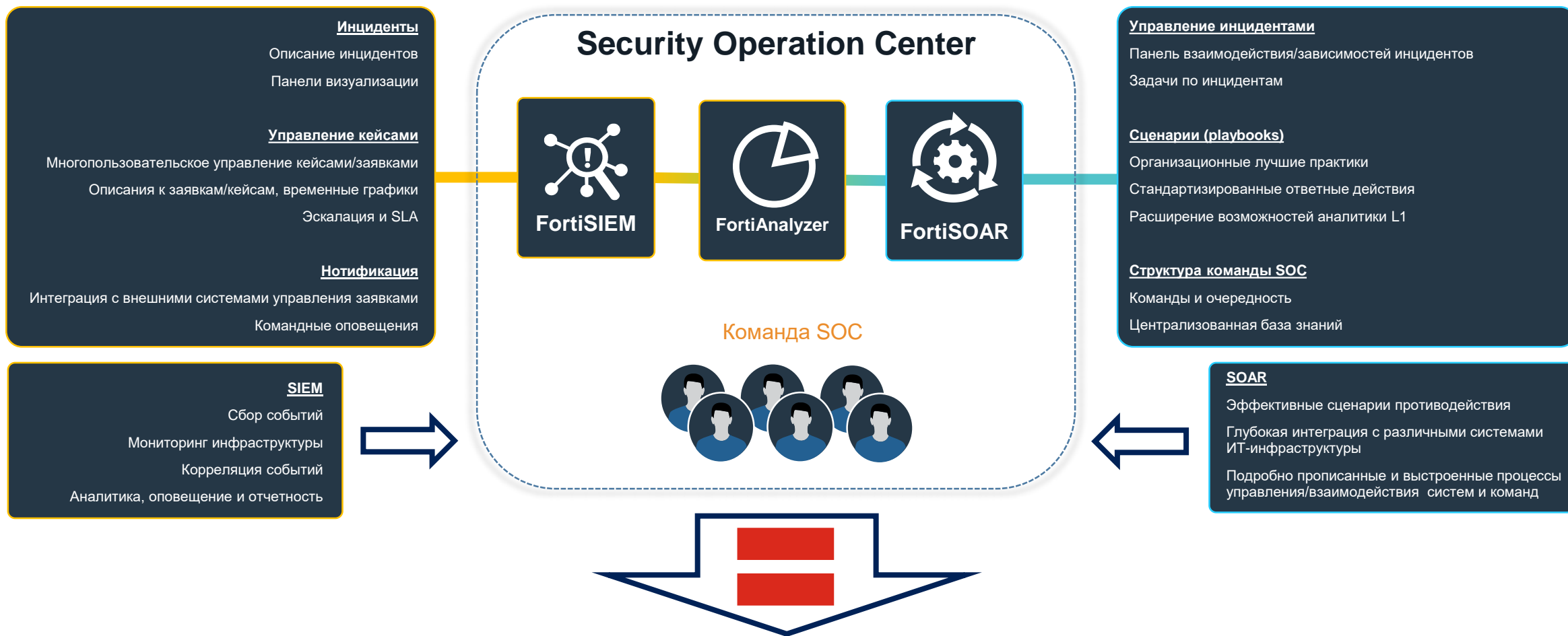
Коннекторы

- Усвоение
- Обогащение
- Содержание
- Исправление
- Сортировка
- Расследование

FortiSIEM & FortiSOAR:

управление событиями и автоматизация процессов —
залог эффективной стратегии

FortiSIEM + FortiSOAR + FortiAnalyzer



Эффективно функционирующая, защищенная и адаптивная к любым внешним воздействиям ИТ-инфраструктура

FORTINET[®]