Информзащита
Системный интегратор

Анализ зарубежного опыта построения и эксплуатации SOC: различия и сходства в подходах

WWW.INFOSEC.RU

Компоненты SOC

Информзащита
Системный интегратор

Технологии

Информзащита
Системный интегратор

- SIEM/Log Management
- Сканеры анализа защищенности
- Песочницы
- Тикетные системы
- Системы визуализации/отчетности
- Платформы для киберразведки (TI)
- Базы знаний
- Внутренние средства обеспечения ИБ
- И пр.

Люди и процессы

Информзащита
Системный интегратор

Есть рекомендации и best-practices:

- MITRE – Ten Strategies of a World-Class Cybersecurity Operations Center (https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf)
- SANS Institute – Building a World-Class Security Operations Center: A Roadmap (https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907)
- Cisco – Security Operations Center: Building, Operating and Maintaining your SOC (http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052014)

Люди и процессы

Информзащита
Системный интегратор

Всегда полезен реальный опыт, особенно зарубежный с более развитыми сервисами MSSP

Magic Quadrant

Figure 1. Magic Quadrant for Managed Security Services, Worldwide

Source: Gartner (January 2017)

IDC Analyze the Future

Top Technology Based on 2016 Market Share

Source: IDC Worldwide Semiannual Security Spending Guide, 2015H2

IBM Security

Dany Gagnon
Executive Security Advisor
IBM Security Central and Eastern Europe

IBM

IBM expertise in building and operating SOCs

20+ years
building and operating
SOCs for the clients

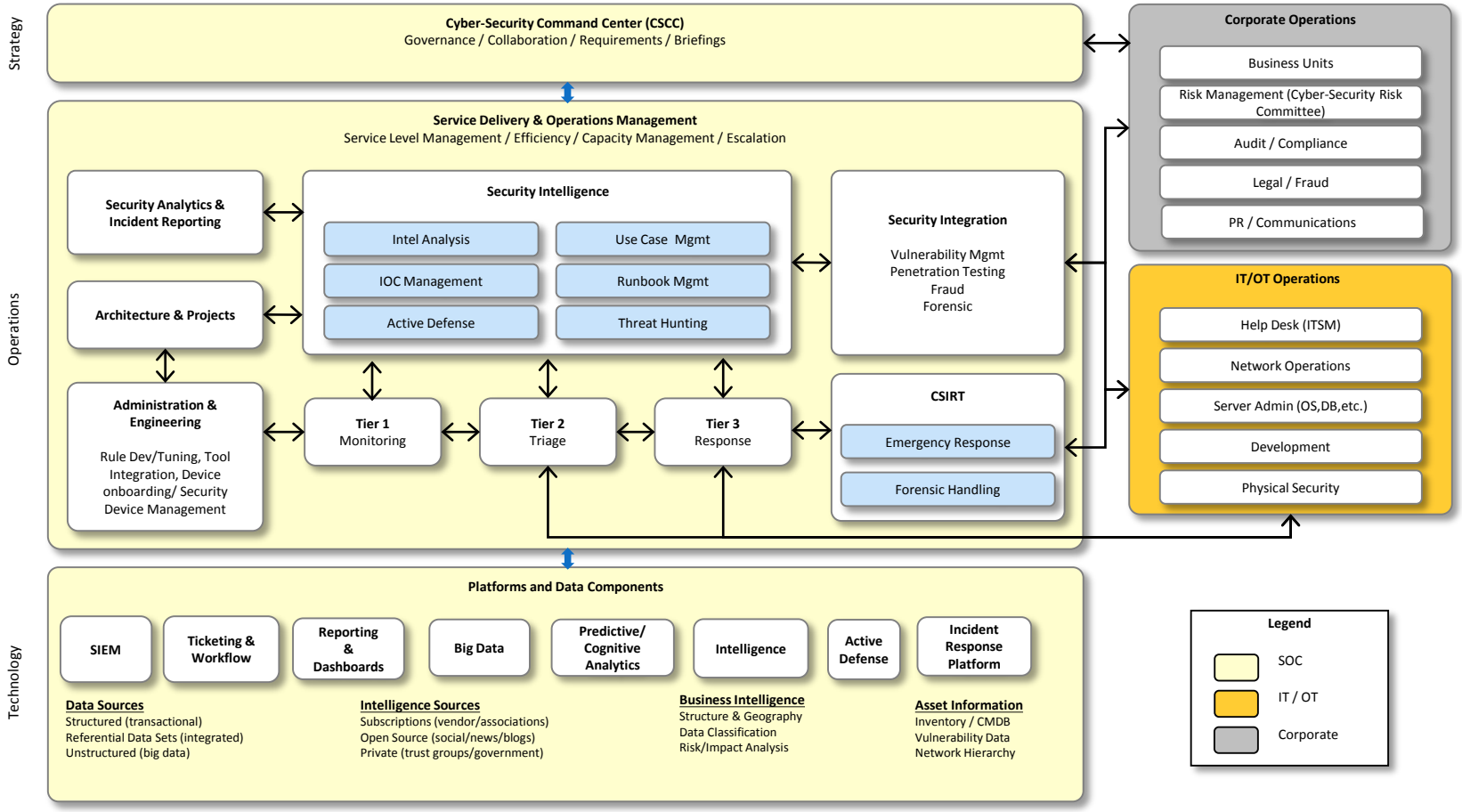
300+ customers
IBM helped building SOCs

50+ programs
of SOC transformation
for last 2 years for
Fortune Global 500 companies

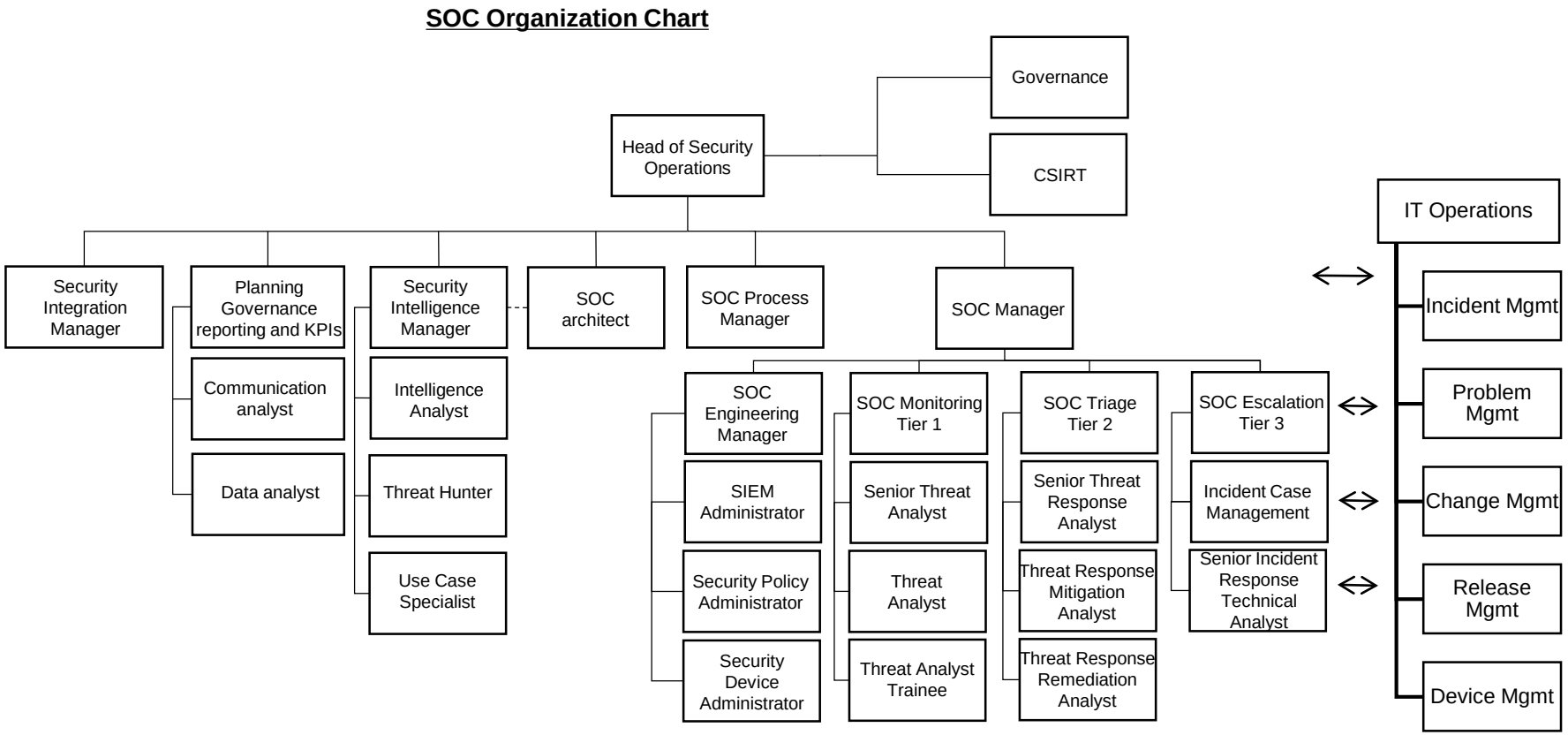
A review of ~300 Security Operation Centers (SOC's) throughout the world highlights the best practices in building and operating a SOC

- Cross functional governance
- Industrialize your SOC, focus on both effectiveness and efficiency
- Next generation SOC's are agile development factories
- Migrate from labor based (linear cost curve) to automated, highly scalable SOC operations
- Use case framework (Digital Use Case Library)
- Metrics, scorecards, dashboards
- Program not a project
- Leverage accelerators
- Contextual data increases the resolution of security incidents
- Use case and rule portfolio will drive the ROI for the SOC

Target State Model to Build Next Generation SOC Capabilities



The SOC organization is organized around the standard plan, build and run model



Emerging Trends in Security Operations Centers

- SOC Pods, Virtual Teams
- Leverage operations management techniques to manage SOC
- Measure and communicate the value of security services (Dashboards)
- Predictive security analytics pilot are now underway
- Active Defense - SOC's will automate threat response and prevention activities
- Add a Security Integration function to minimize preventable security incidents
- Security Business Analysts
- Convergence of Risk Data (Integrated enterprise risk management platform)
- SOC is evolving into the Enterprise threat management center
- Cognitive Analytics

Ключевые вопросы

Информзащита
Системный интегратор

Считаете ли Вы подход intelligence-driven defense важным при оказании услуг SOC?

Do you consider an intelligence-driven defense approach is important in the provision of SOC services?

Ключевые вопросы

Информзащита
Системный интегратор

Как организовано взаимодействие с заказчиком в рамках реагирования, например, на критичный инцидент, произошедший ночью, в случае если заказчик работает 8x5?

How is the process of interaction with the customer organized within the response, for example, to the critical incident that occurred at night and the customer works 8x5?

Ключевые вопросы

Информзащита
Системный интегратор

Какое распределение персонала между тремя линиями SOC? Какая самая многочисленная?

What is staff distribution among Tier 1-3? What is the most numerous?

Ключевые вопросы

Информзащита
Системный интегратор

Какую финансовую ответственность несет аутсорсинговый SOC перед заказчиком в случае не выявления инцидента ИБ, приведшего к каким-либо последствиям? Насколько распространены «программы киберстраховки» на зарубежном рынке?

What is the financial responsibility of the outsourcing SOC to the customer in case of no detection of the incident that led to any consequences? How common are «cyber insurance programs» in the market?

По нашему опыту

Информзащита
Системный интегратор

Гибридный подход

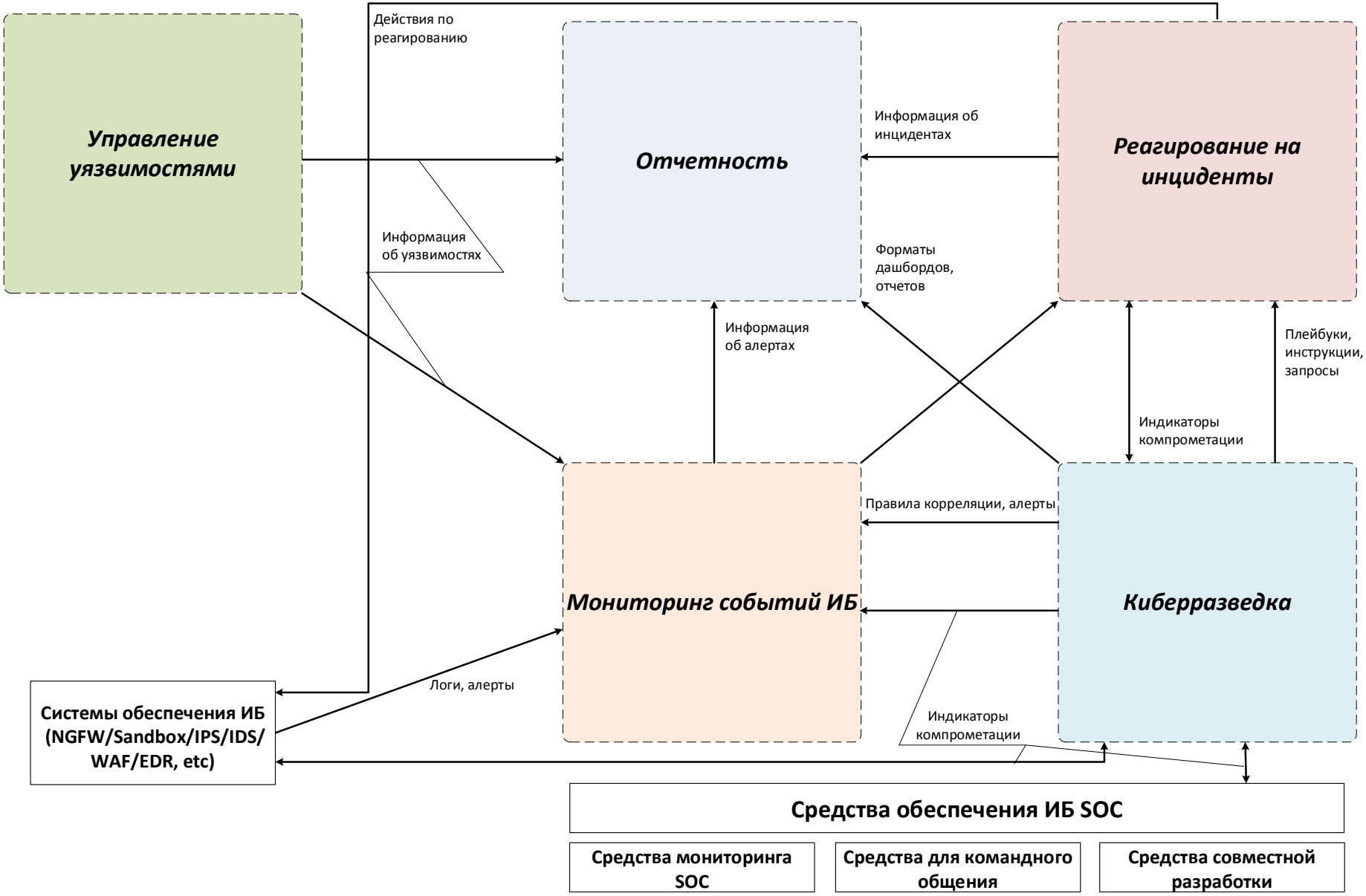
- **Intelligence-driven defense** – фокусирование на атаках/поведении нарушителей

в дополнение к

- **Классическому подходу** – фокусирование на:
  - обнаружении и устранении уязвимостей, использовании превентивных мер
  - Усиление периметра – IPS/IDS/NGFW/WAF и пр., а также AV на конечных устройствах.

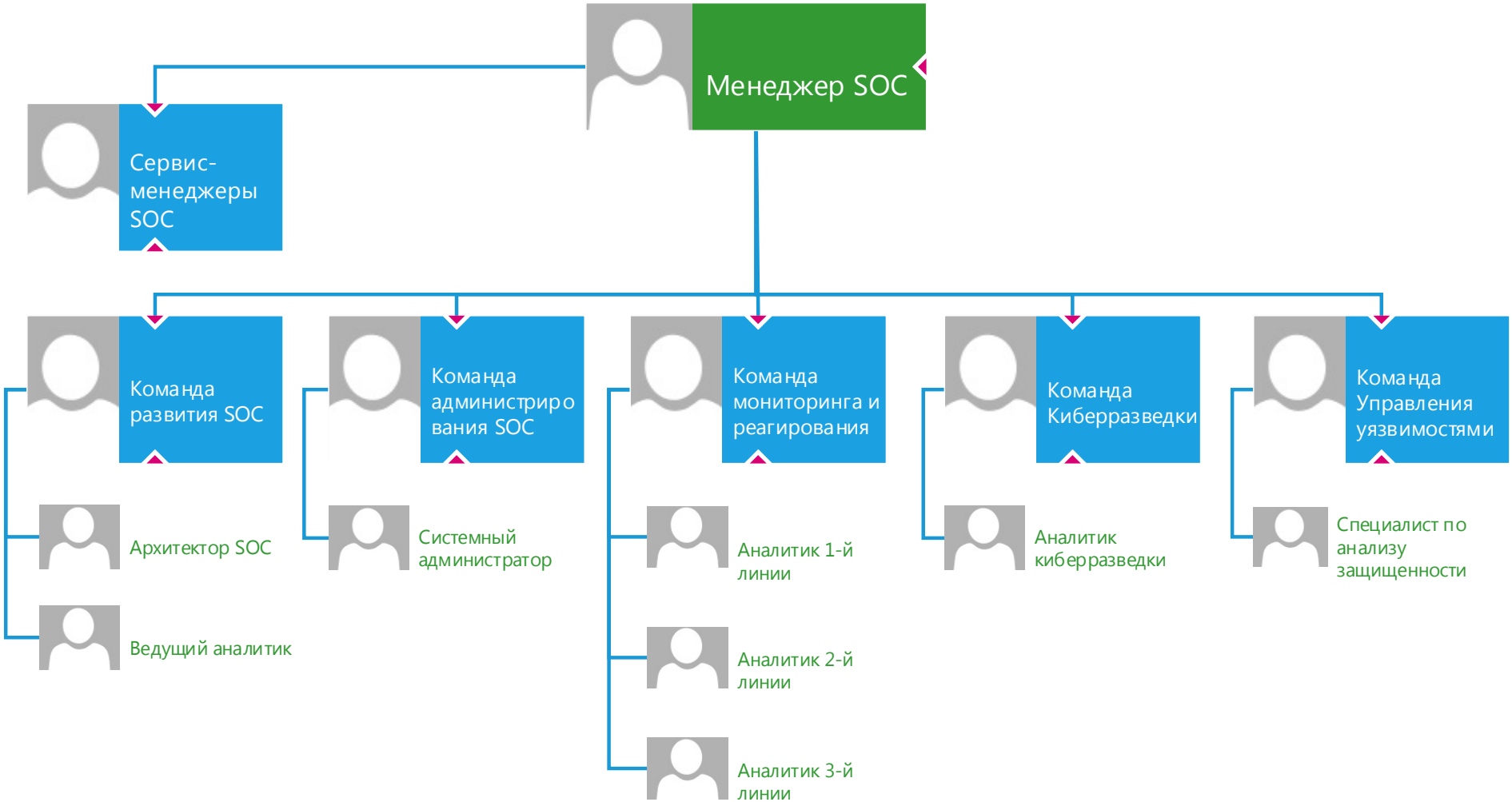
Процессы

Информзащита
Системный интегратор



Люди (роли)

Информзащита
Системный интегратор



Выводы

Информзащита
Системный интегратор

- В России и зарубежом применяются схожие подходы построения и эксплуатации SOC, основанные на intelligence-driven defense
- Основные отличия заключаются в:
  - Количестве и зрелости выстроенных процессов
  - Организационной структуре
  - Меньшем распространении MSSP услуг
  - Требованиях регуляторов

- Необходимо активно взаимодействовать с мировым сообществом и применять накопленный опыт с учетом наших реалий

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 24x7x365

«ИНФОРМЗАЩИТА»:

- **СИСТЕМНЫЙ ИНТЕГРАТОР WWW.INFOSEC.RU**
- **СЕРВИСНЫЙ ЦЕНТР WWW.ITSOC.RU**
- **УЧЕБНЫЙ ЦЕНТР WWW.ITSECURITY.RU**