КЛЮЧЕВЫЕ ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ЭФФЕКТИВНОСТИ СОВРЕМЕННЫХ SOC

Роман Кобцев
Директор по развитию бизнеса
ЗАО «Перспективный мониторинг», ГК «ИнфоТеКС»

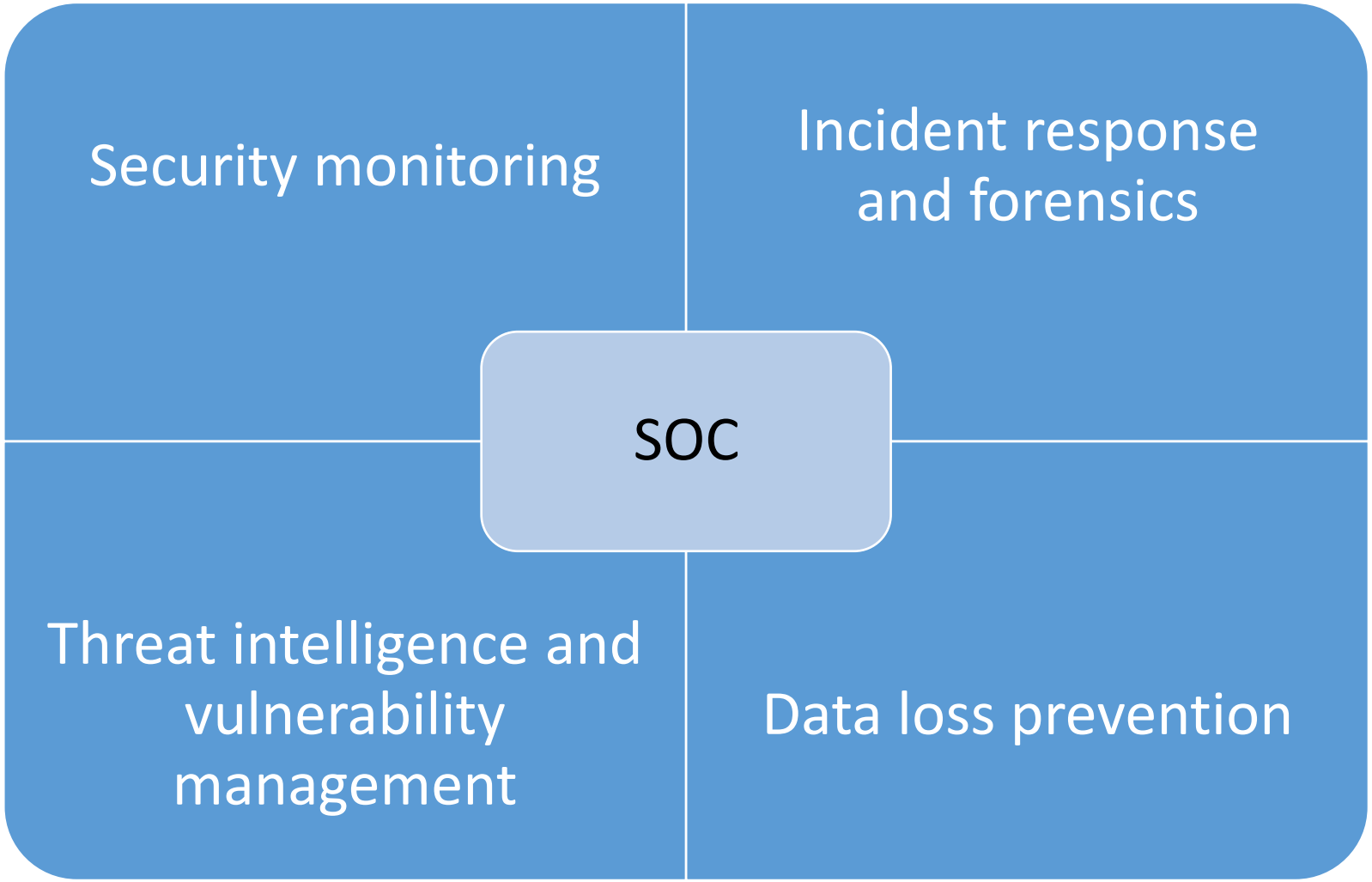
SOC-FORUM

Москва, 11 ноября 2015 г.

Вопросы презентации

- SOC это не только SIEM
- Качество сигнатур для обнаружения атак
- Строить свой SOC или MSSP
- Выявление, анализ и обработка инцидентов

SOC это не только SIEM



Источник: Security Operations Centers against cybercrime Top 10 considerations for success ©2013 EYGM Limited

Центр мониторинга. Разработанные системы.

Технические системы

Система защищенного взаимодействия

VPN/ViPNet

АРМ Аналитика уязвимостей

АРМ Сигнатурного Аналитика

АРМ Аналитика СОА

АРМ Аналитика Инцидентов

АС мониторинга Уязвимостей ПО и компонентов

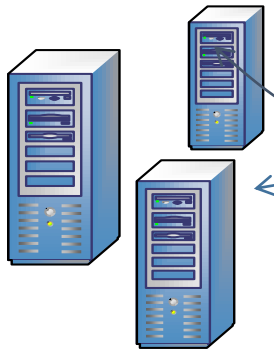
АС обработки уязвимостей

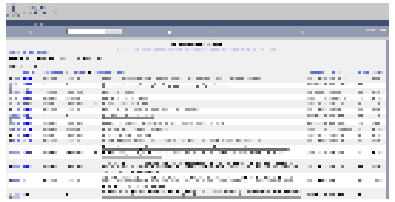
АС поиска и анализа Информации по типовым форматам в публичных (анонимных) источниках Интернета

АС анализа событий ИБ (Система обнаружения атак)

АС обработки Инцидентов

АС анализа вредоносного трафика, ПО и атак. Оперативный выпуск правил IDS





Серверы

Серверы

Качество сигнатур для COB/COA

- **SourceFire (с 2013 г. в составе Cisco Systems), США**
  - VRT community (условно бесплатные) – лицензии GNU GPL 2.0
  - VRT community (условно бесплатные) – VRT Certified Rules License

(от подразделения «Vulnerability Research Team», сейчас «Talos Group»)

- **Emerging Threats (с 2014 г. в составе Proofpoint), США**
  - ET Open (условно бесплатные) – лицензии GNU GPL 2.0, BSD License
  - ET Pro (платные) – лицензии ET Pro, GNU GPL 2.0, BSD License
- **Idappcom, Великобритания**
  - Idappcom (платные)
- **ЗАО «ПМ» в составе ГК «ИнфоТеКС»), Россия**
  - AM (платные, в продукте ViPNet IDS)

Качество сигнатур для СОВ/СОА

Риски использования сторонних (особенно бесплатных) сигнатур

- Получение сигнатур с ошибками
- Отсутствие или исчезновение сигнатур на конкретные уязвимости
- Отсутствие учета Российской специфики
- Смена политики лицензирования и/или продаж сигнатур: (смена собственника, поглощение компаний, сотрудничество со спецслужбами, санкции,…)

Качество сигнатур для СОВ/СОА

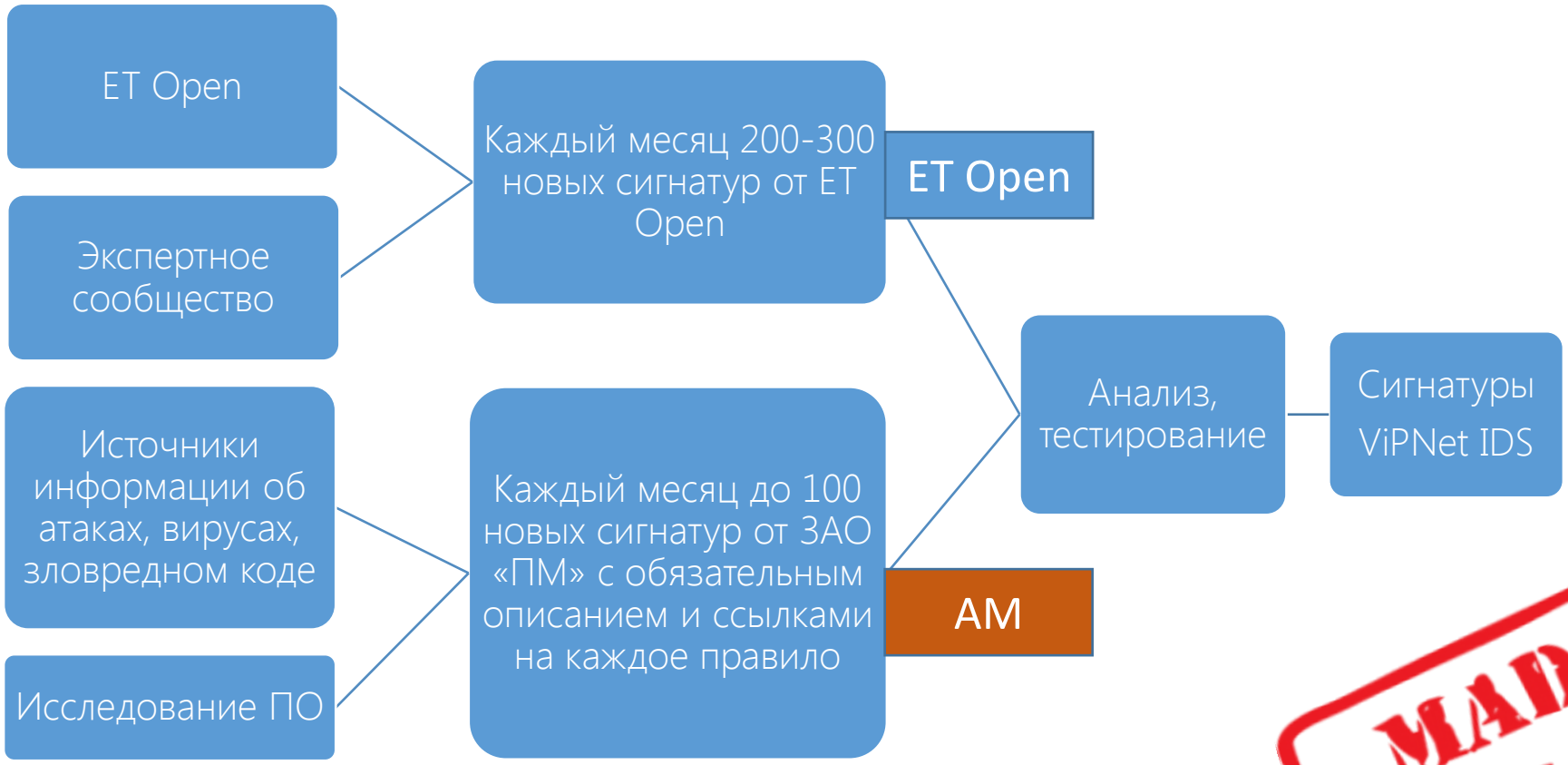
Тестирование и исправление сторонних сигнатур

Тестирование сигнатурных правил на сетевом трафике, генерируемом вредоносными файлами

Тестирование внешних сетевых атак

Разработка собственных сигнатур

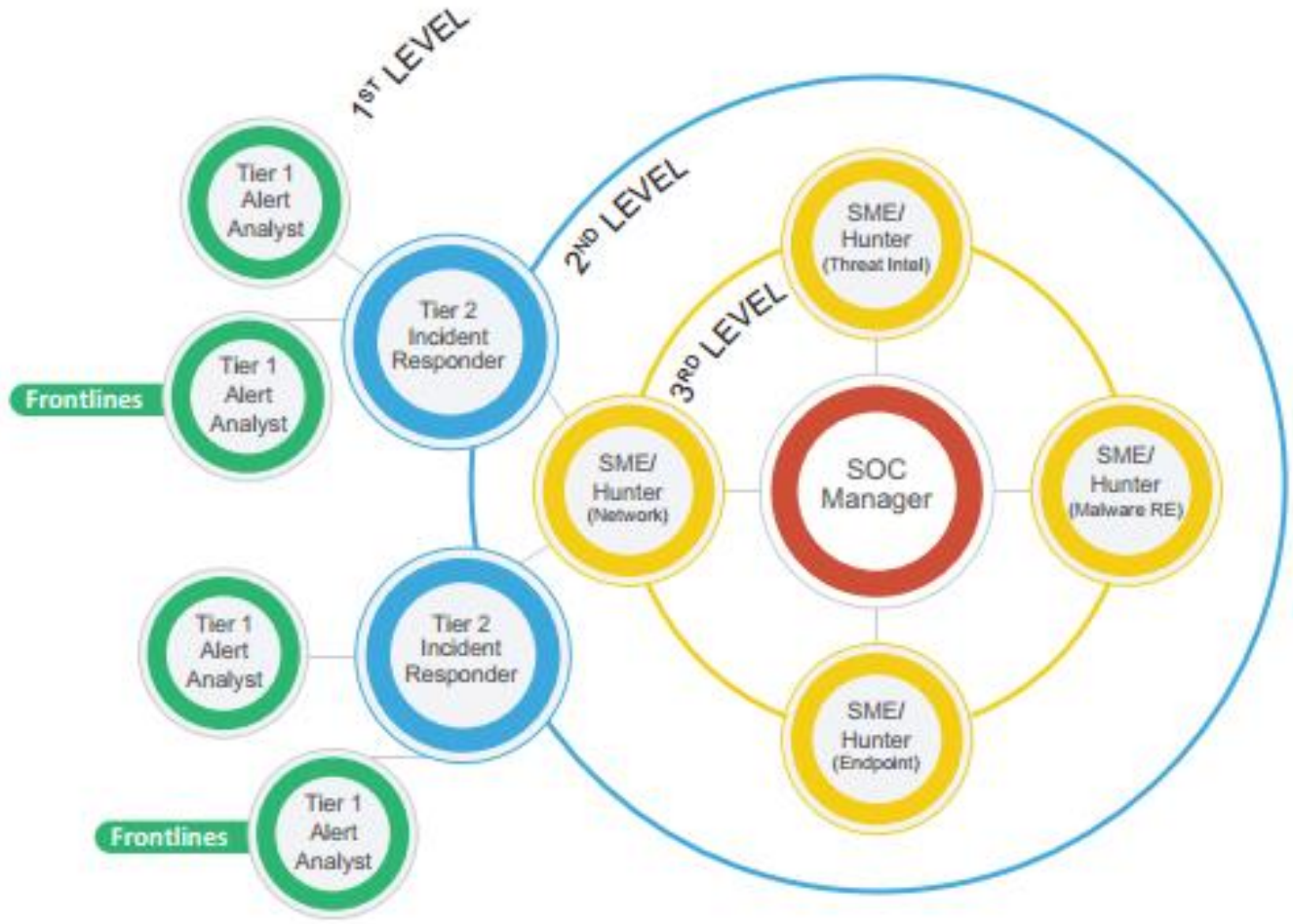
Разработка сигнатур для СОВ/СОА



Строить свой SOC или MSSP

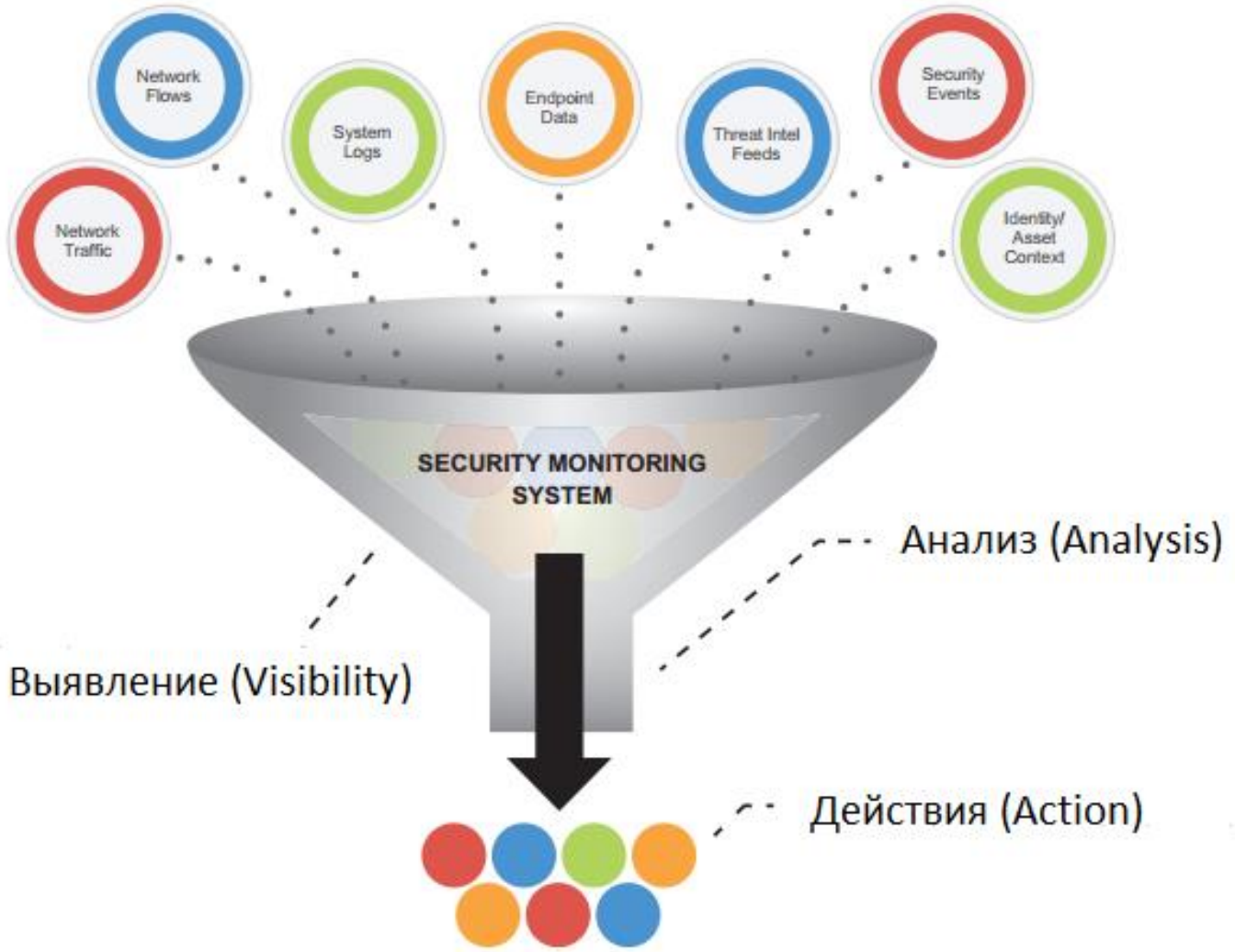
Все решает
наличие ресурсов
и экспертизы

Организационная структура SOC



Источник: Building a World-Class Security Operations Center: A Roadmap © 2015 SANS™ Institute

Выявление, анализ и обработка инцидентов



Источник: Building a World-Class Security Operations Center: A Roadmap © 2015 SANS™ Institute

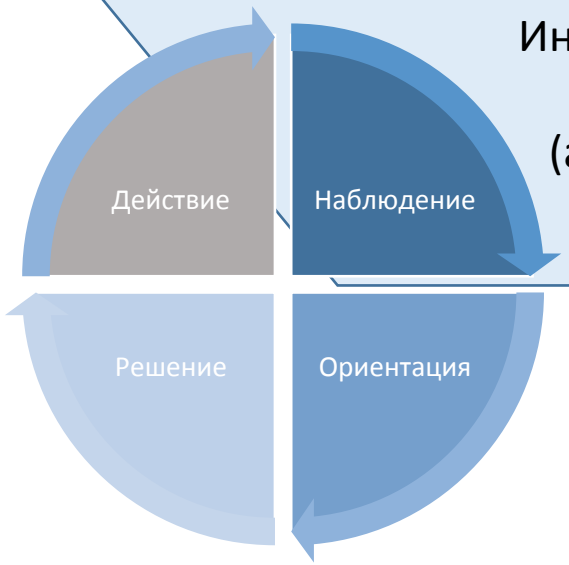
Выявление, анализ и обработка инцидентов

Источник: The Business Case for Managed Security Services © 2012 Solutionary, Inc.

Выявление, анализ и обработка инцидентов

Центр мониторинга. Работа с данными

100 Mbit/s * 60 сек* 60 мин* 24 ч/8 бит*0,5 = 540 GB



Информационный обмен в сети до 500 АРМ; ИТ служба (администратор) + СЗИ (НСД, АВСЗ,+)

Центр мониторинга. Сортировка событий ИБ

- ViPNet IDS
- ViPNet StateWatcher
- ViPNet Coordinator
- СЗИ
- АВСЗ
- Syslog WS, SRV
- Сканеры
- и др.

Детальный анализ ~150 МВ:
События ИБ, Инциденты

СПАСИБО ЗА ВНИМАНИЕ!