KASPERSKY lab

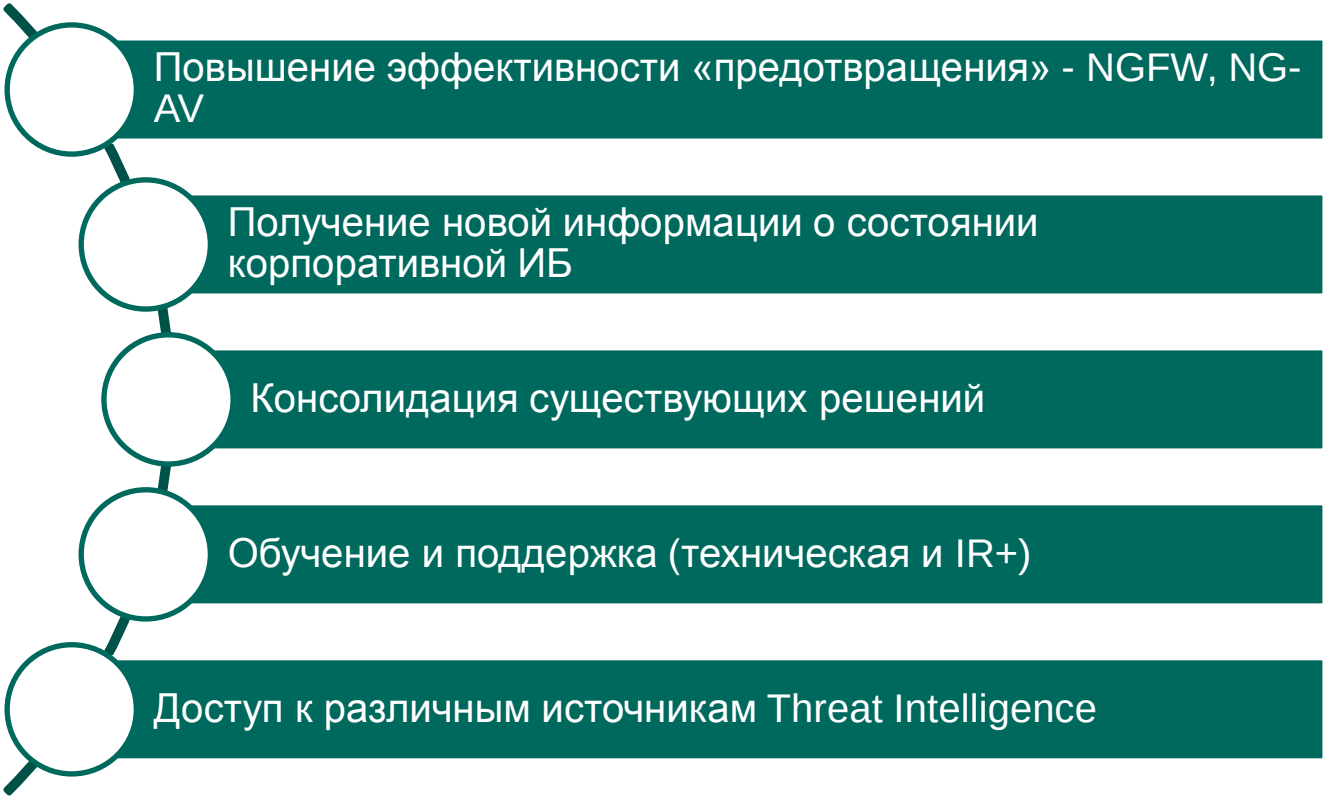
РАЗВИТИЕ ВОЗМОЖНОСТЕЙ ЦЕНТРА МОНИТОРИНГА (SOC) ДЛЯ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕНАПРАВЛЕННЫМ АТАКАМ

Олег Глебов

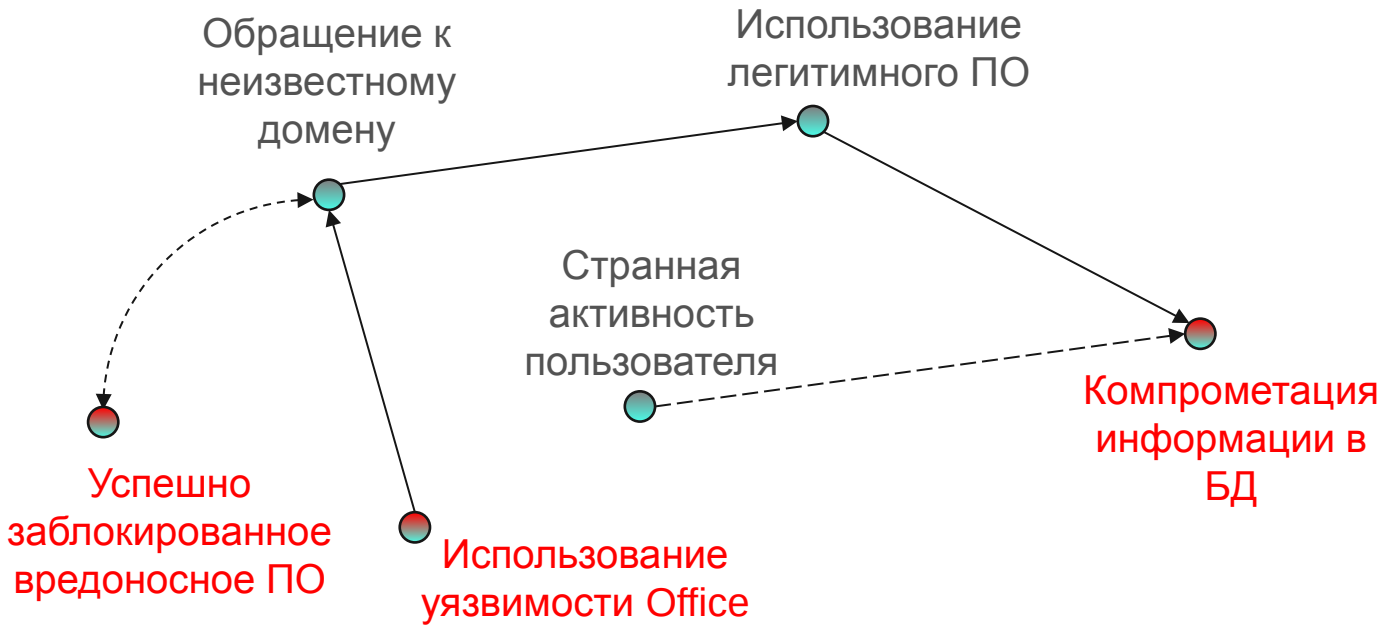
Руководитель направления развития решений
по противодействию целенаправленным атакам

Москва, 16 ноября,
SOC-Forum 2016

ТЕНДЕНЦИИ КОРПОРАТИВНОЙ ИБ



АНАТОМИЯ ЦЕЛЕНАПРАВЛЕННОЙ АТАКИ



SOC – РАБОТА С «СУЩЕСТВУЮЩИМ» КОНТЕКСТОМ

НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ

- DLP
- поведенческий анализ исходящего трафика
- прокси (MITM)
- NIDS

ПОДГОТОВКА

- логи межсетевого экрана
- логи web-сервера
- web-firewall

Консолидация данных традиционных решений по ИБ в SOC – это первый шаг в нужном направлении

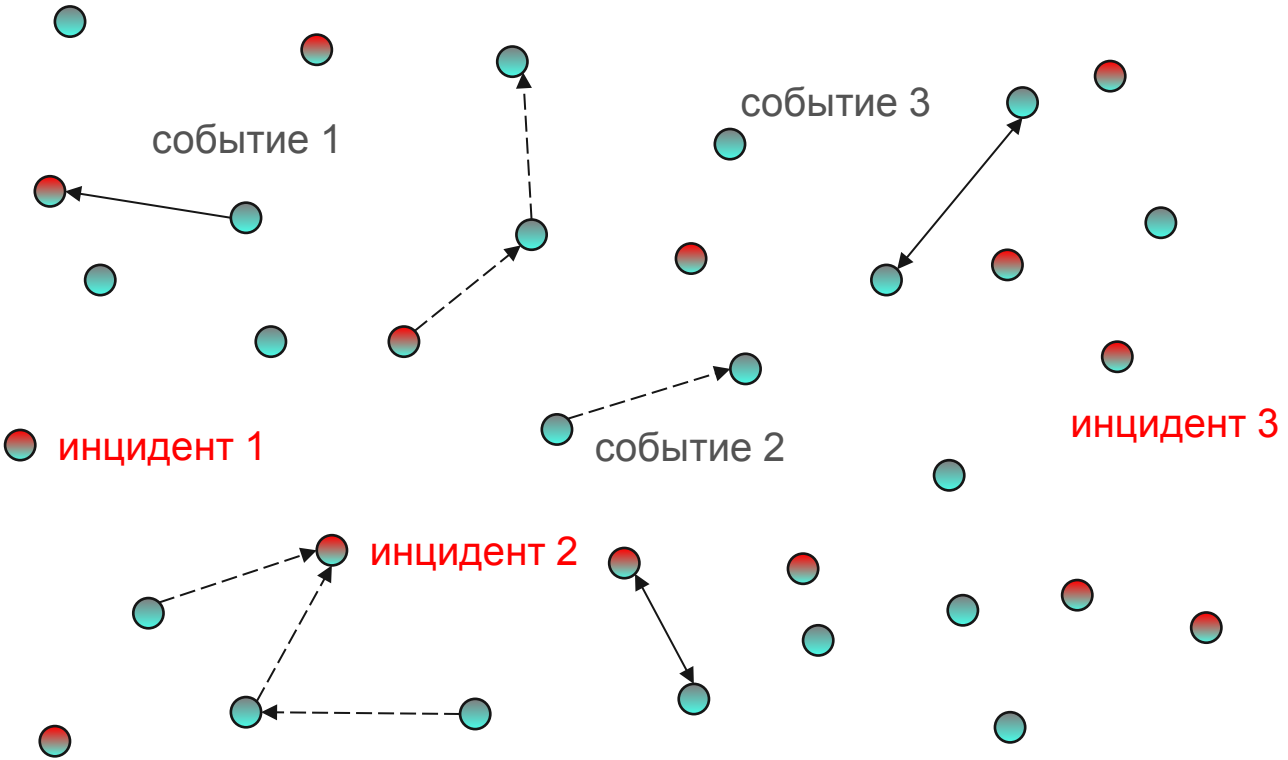
РАСПРОСТРАНЕНИЕ

- PIM
- защита баз данных
- контроль доверенной среды

ПРОНИКНОВЕНИЕ

- IoC
- mail прокси
- межсетевой экран
- сенсоры трафика
- HIDS, EPP
- логи доступа

«МИЛЛИОН АЛЕРТОВ»



ВЫЯВЛЕНИЕ СЛОЖНЫХ АТАК В SOC

МАКРО-ИНЦИДЕНТ ВЫЯВЛЕН… НО ЧТО ДАЛЬШЕ?

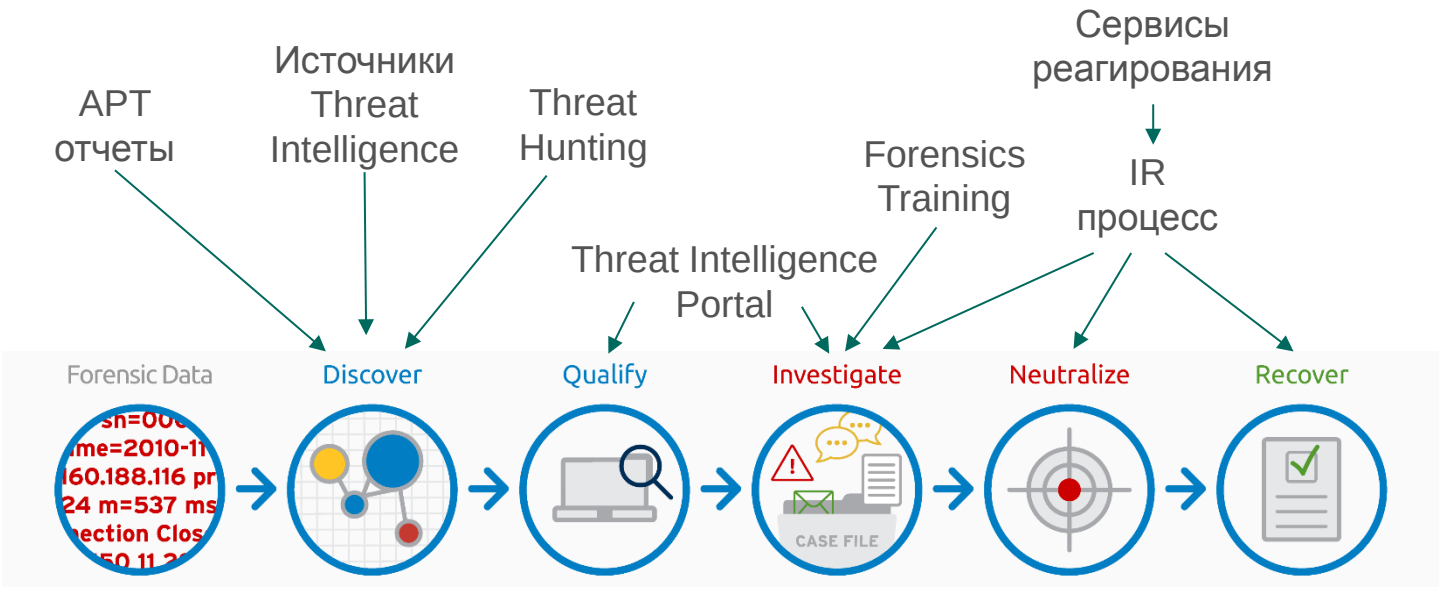
Кто и как должен отреагировать?

Как и на основе чего оценить уровень риска?

Где взять доп. информацию для расследования?

Кого привлекать на outsourcing?

КАК РАЗВИВАТЬ ПРОЦЕСС ВЫЯВЛЕНИЯ Ц.А.



Специализированное решение для обнаружения (Анти-APT)

Автоматизация процесса реагирования и расследования (EDR)

ПЕРСПЕКТИВЫ СОВРЕМЕННЫХ SOC

Оценка и прогнозы развития

ОЦЕНКА ЗРЕЛОСТИ СОВРЕМЕННОГО SOC*

Уровень зрелости	Классификация
Неполный	Элементы управления (SOC) не внедрены
Начальный	Неорганизованные и хаотичные процессы мониторинга
Регулируемый	Централизация управления и унификация операций
Рекомендованный	Внедренные стандарты, отражающие уникальные аспекты и задачи организации
Измерительный	Сбор и анализ данных в реальном времени с отражением в процессах управления и мониторинга ИБ
Оптимизированный	Прогнозирование и постоянный анализ результатов ранее принятых решений, их пересмотр и адаптация в реальном времени

**CARNEGIE MELLON SOFTWARE ENGINEERING INSTITUTE CAPABILITY MATURITY MODEL FOR INTEGRATION (SEI-CMMI)*

РЕЗУЛЬТАТ ОЦЕНКИ 114 SOC ЗА 5 ЛЕТ*

85%
не достигли рекомендованного «уровня 3»

Наивысший уровень
Промышленность 1.82

Самый низкий
Телеком - 0.95

25%
не соответствуют даже «уровню 1»

- **Мышление «нас уже взломали» привело к успешному развитию аналитических решений и команд по поиску угроз (Threat Hunting)**
- **Гибридное планирование службы SOC**
- **Автоматизация этапов сбора данных и выявления угроз**
- **Драматический рост компаний оценивающих риск целенаправленных атак как приоритетный по сравнению с 2015 годом**

** Источник HP State of security operations 2016*

ДРАЙВЕРЫ РАЗВИТИЯ SOC

СПАСИБО!

АО «Лаборатория Касперского»
www.kaspersky.com

Олег Глебов
Руководитель направления развития решений
по противодействию целенаправленным атакам

Oleg.Glebov@kaspersky.com
D: +7 495 797 87 00 x5609
M: +7 910 476 94 10

https://ru.linkedin.com/in/glebovoleg

KASPERSKY lab