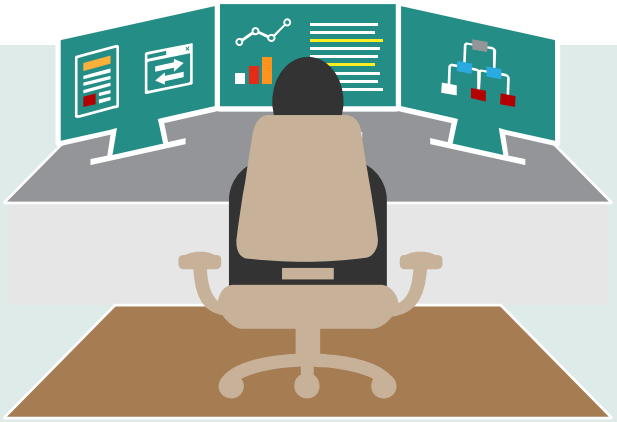
KASPERSKY lab



ЦЕНТР МОНИТОРИНГА КАК СРЕДСТВО ПРОТИВОДЕЙСТВИЯ ЦЕЛЕВЫМ АТАКАМ И ПЕРЕДОВЫМ УГРОЗАМ БЕЗОПАСНОСТИ

Олег Глебов

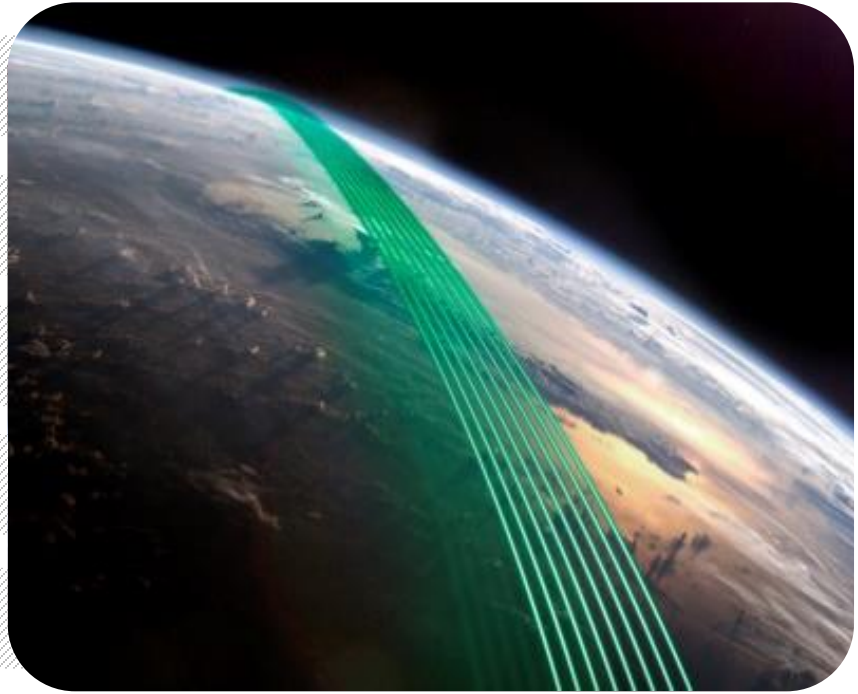
Менеджер по сопровождению корпоративных продаж

ПЕРЕДОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

Тенденции и статистика

ТЕНДЕНЦИИ КОРПОРАТИВНОЙ ИБ

- Рост нетехнических элементов «атак»
- Усложнение IT-инфраструктуры
- Сокращение стоимости атаки
- Атаки на поставщиков и 3-их лиц
- «Перегрев» периметровой защиты



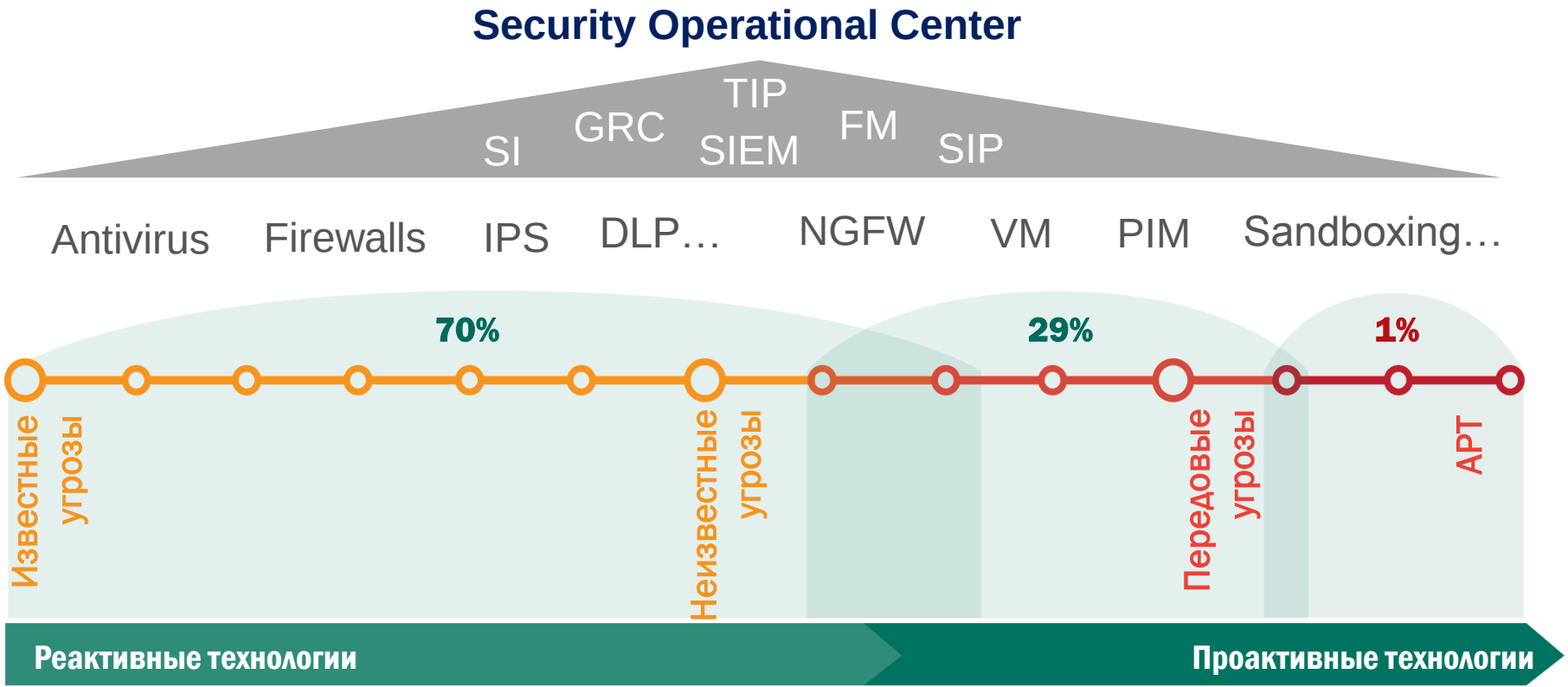
ЧТО ВЫГЛЯДИТ НАИБОЛЕЕ КРИТИЧНЫМ?

Автоматизация
Слабая мотивация
Низкая отдача

Высокая мотивация
Постоянный контроль
Большая отдача

KASPERSKY lab

ЗАЛОГ УСПЕХА В КОНСОЛИДАЦИИ ДАННЫХ И УНИФИКАЦИИ ПРОЦЕССОВ



KASPERSKY lab

ЦЕНТРАЛИЗОВАННЫЙ АНАЛИЗ СИТУАЦИИ

Центр обеспечения безопасности (SOC) и работа с контекстом

ТИПОВЫЕ СТАДИИ ЦЕЛЕВОЙ АТАКИ

ПОДГОТОВКА

- проверка доменных имен
- анализ корп. сайта
- поиск в соц. сетях

- зараженные URL
- Вредоносное ПО
- иные средства (USB, BYOD и тд)

ЗАРАЖЕНИЕ

- дроппер/руткит/бот
- сбор и передача данных
- модульность

РАСПРОСТРАНЕНИЕ

- кража идентификационных данных
- повышение привилегий
- налаживание связей
- легитимизация действий

ИЗВЛЕЧЕНИЕ

- скрытое управление
- выгрузка данных по шифрованному каналу
- сокрытие следов
- «тихий» уход

SOC – РАБОТА С «СУЩЕСТВУЮЩИМ» КОНТЕКСТОМ

ИЗВЛЕЧЕНИЕ

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

ПОДГОТОВКА

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

РАСПРОСТРАНЕНИЕ

- PIM
- защита баз данных
- контроль доверенной среды

ЗАРАЖЕНИЕ

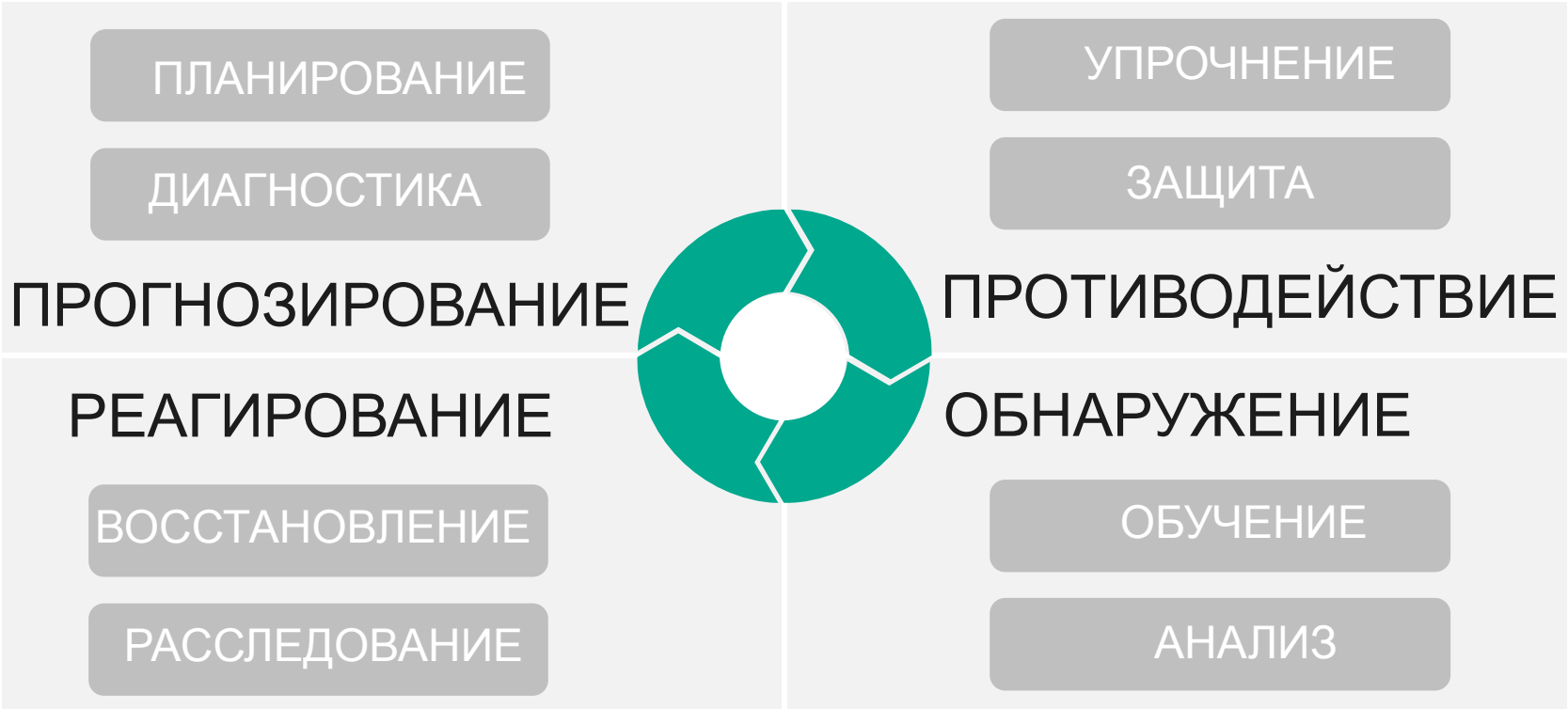
- IoC
- mail прокси
- межсетевой экран
- сенсоры трафика
- HIDS, EPP
- логи доступа

KASPERSKY lab

ПРОТИВОДЕЙСТВИЕ ЦЕЛЕВЫМ АТАКАМ В КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЕ

Технологии и процессы

СТРАТЕГИЯ АДАПТИВНОЙ ЗАЩИТЫ ОТ ПЕРЕДОВЫХ УГРОЗ БЕЗОПАСНОСТИ*



*GARTNER'S ADAPTIVE SECURITY STRATEGY

ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕВЫМ АТАКАМ

ПРОГНОЗИРОВАНИЕ

ПРОТИВОДЕЙСТВИЕ и ОБНАРУЖЕНИЕ

Анализ поведения сети

HTTP/HTTPS/Mail/FTP/DNS сенсоры, агенты рабочих станций

Анализ объектов

Песочница

Анализ поведения рабочих станций

Мониторинг процессов и конфигураций

РЕАГИРОВАНИЕ

Сетевое расследование

DPI, аналитические решения

Расследование рабочих станций

Сервисы безопасности

ПОДВОДНЫЕ КАМНИ ИНТЕГРАЦИИ АНТИ-APT В СОК

Сложная архитектура сети	Множество точек контроля – раздувание бюджетов
Требования мультивендорности	Невозможность отказа от существующих решений
Изолированные сети и соответствия требованиям	Невозможность использовать глобальную статистику, подрыв доверия
Уникальные атаки и методы обхода средств защиты	Невидимы для «сигнатурных» и поведенческих средств анализа

ПЕРСПЕКТИВЫ СОВРЕМЕННЫХ СОКОВ

Оценка и прогнозы развития

ОЦЕНКА ЗРЕЛОСТИ СОВРЕМЕННОГО SOC*

Уровень зрелости	Описание
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 87 СОК В 18 СТРАНАХ*

87%
не достигли рекомендованного «уровня 3»

20%
не соответствуют даже «уровню 1»

Наивысший уровень
Промышленность

Самый низкий
Телеком

По сравнению с 2014 годом главным драйвером эффективности СОК становится информация об угрозах (Threat Intelligence Sharing)

** Источник HP State of security operations 2015*

КОМПЛЕКСНЫЕ ЗАДАЧИ ДЕПАРТАМЕНТА ИБ И SOC

Комплексный подход к обеспечению корпоративной защиты требует глобального мониторинга и глубокой компетенции в киберугрозах для ответа на ключевые вопросы служб ИБ:

- Атака целевая или широконаправленная?
- Сталкивался в мире кто-то с аналогичным вредоносом или аномалией?
- Как противодействовать заражению пока не выпущена сигнатура?
- Как оперативно выявлять неизвестные ранее угрозы?
- Как оценить степень опасности аномального ПО?
- Как выявить источник заражения и предотвратить повторение?
- Как минимизировать ущерб в случае заражения?

ИНТЕЛЛЕКТУАЛЬНЫЕ СЕРВИСЫ БЕЗОПАСНОСТИ ЛАБОРАТОРИИ КАСПЕРСКОГО

ПРОГНОЗИРОВАНИЕ

- оценка уязвимости приложений
- тесты на проникновение
- расширенные курсы офицеров ИБ

ПРОТИВОДЕЙСТВИЕ

- повышение осведомленности (+ Cybersecurity games)
- базовые курсы офицеров ИБ

РЕАГИРОВАНИЕ

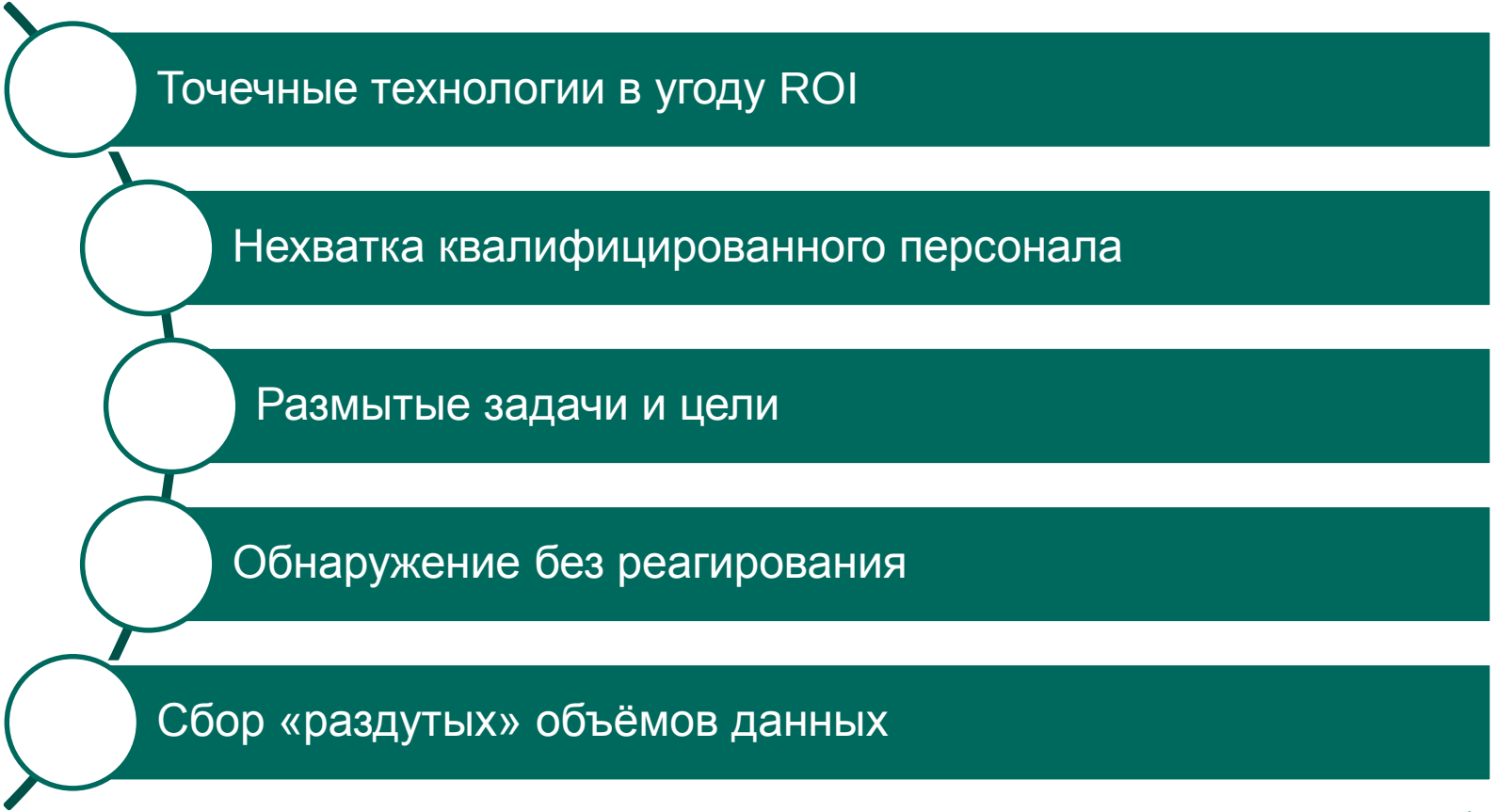
- расследование инцидентов
- анализ вредоносного кода
- реагирование на инциденты целевых атак

ОБНАРУЖЕНИЕ

- информация об угрозах (Threats Intelligence)
- обучение офицера по противодействию целевым атакам

KASPERSKY lab

ОСНОВНЫЕ НЕДОСТАТКИ СУЩЕСТВУЮЩИХ SOC



СПАСИБО!

АО «Лаборатория Касперского»
www.kaspersky.com

Олег Глебов
Менеджер по сопровождению
корпоративных продаж

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