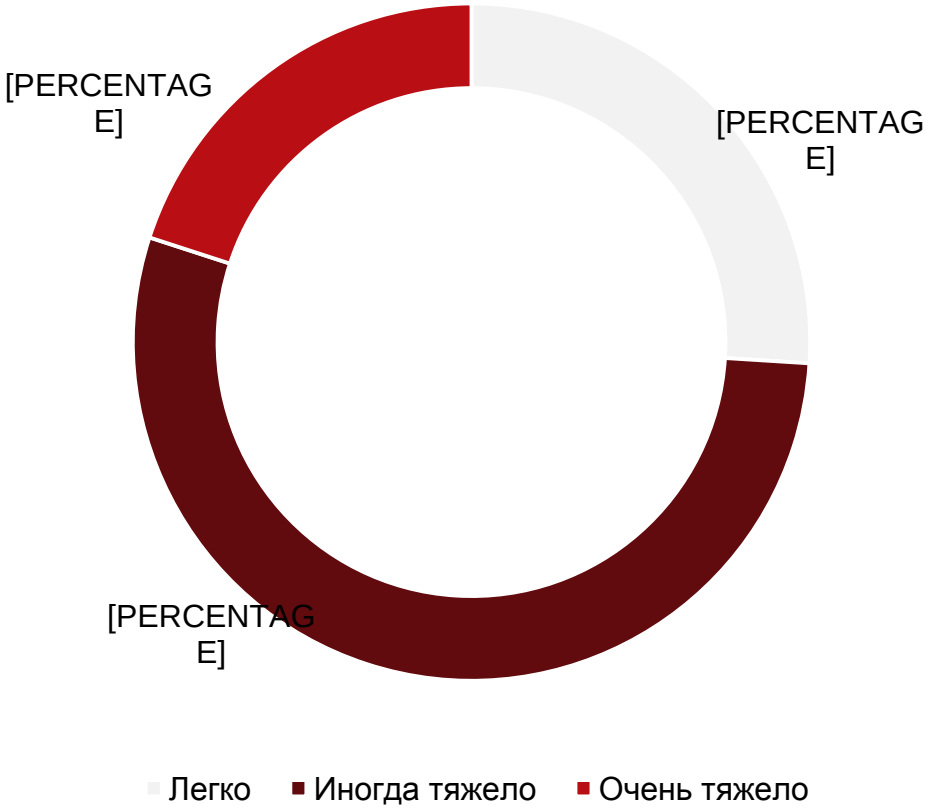
kaspersky

Threat Intelligence: что скрывается за красивым названием

Александр Мазикин,
Руководитель группы развития продаж сервисов

Проблема: рост количества инцидентов

Проблематика управления инцидентами



Многие инциденты не расследуются и не устраняются

Источник: Cisco 2018 Capabilities Benchmark Study

Трансформация рынка

2013

Threat intelligence - это основанные на фактических данных знания, включая контекст, механизмы, индикаторы, последствия и действенные рекомендации, о существующей или возникающей угрозе или угрозе активам, которые могут использоваться для принятия решений относительно реакции субъекта на эту угрозу или опасность.

Gartner

“Intelligence” - модное слово, которое может означать все, что вы хотите, чтобы оно значило

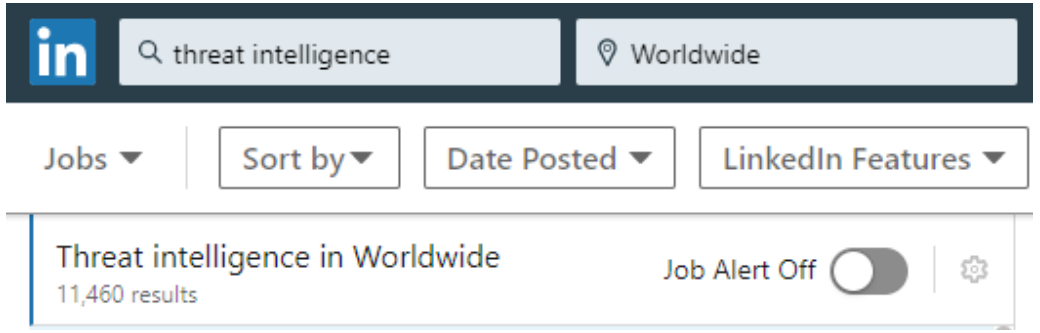
David Bianco, Incident Detection & Response Specialist

2019

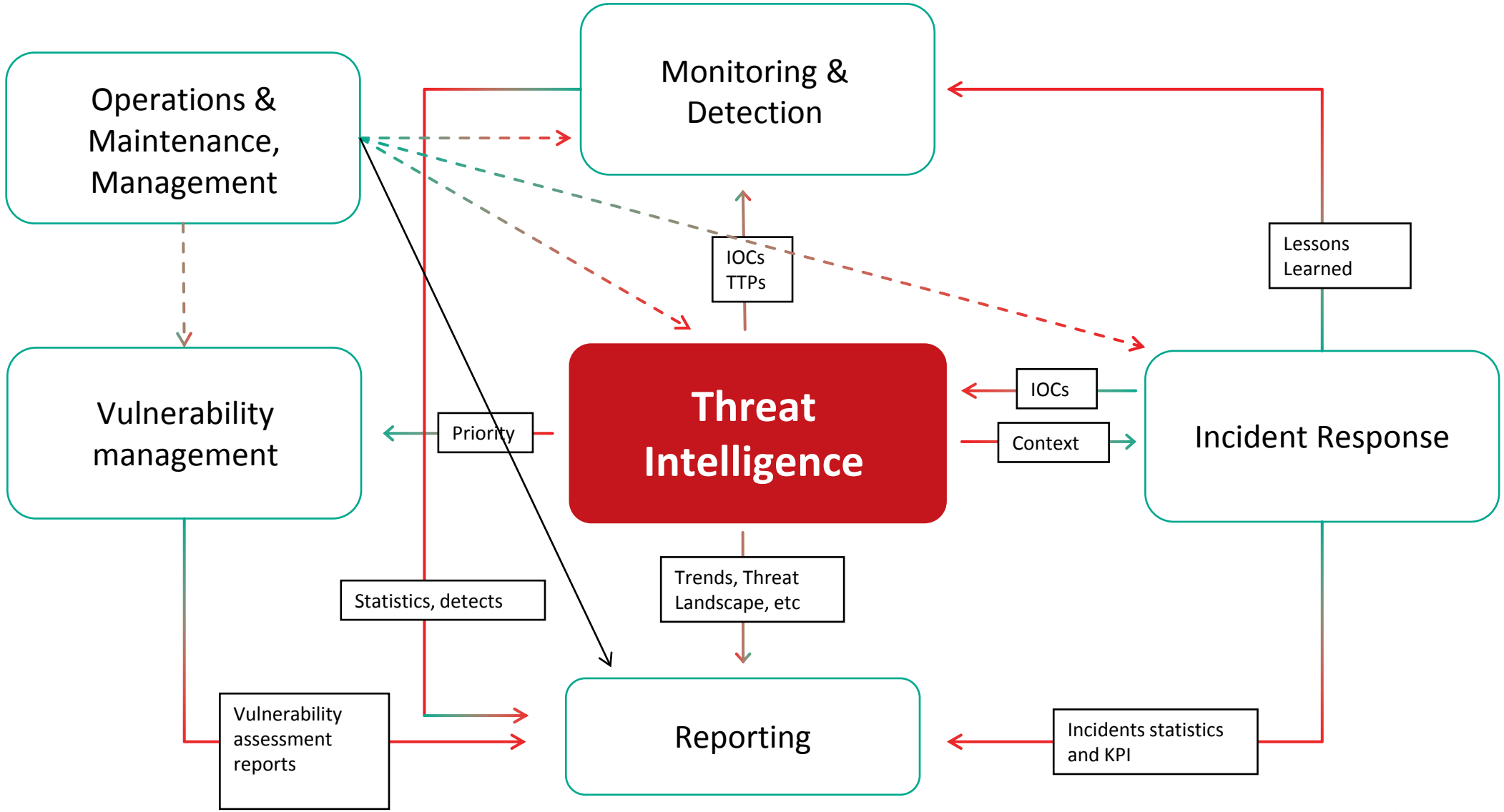
Полноценный «взрослый» рынок с большим количеством Агрегаторов и Стартапов

Фокус на заказчика и стандартизация

Threat Intelligence Аналитик стал полноценным членом команды



Security Operations



Рецепт приготовления

Proper Threat Intelligence Recipe:

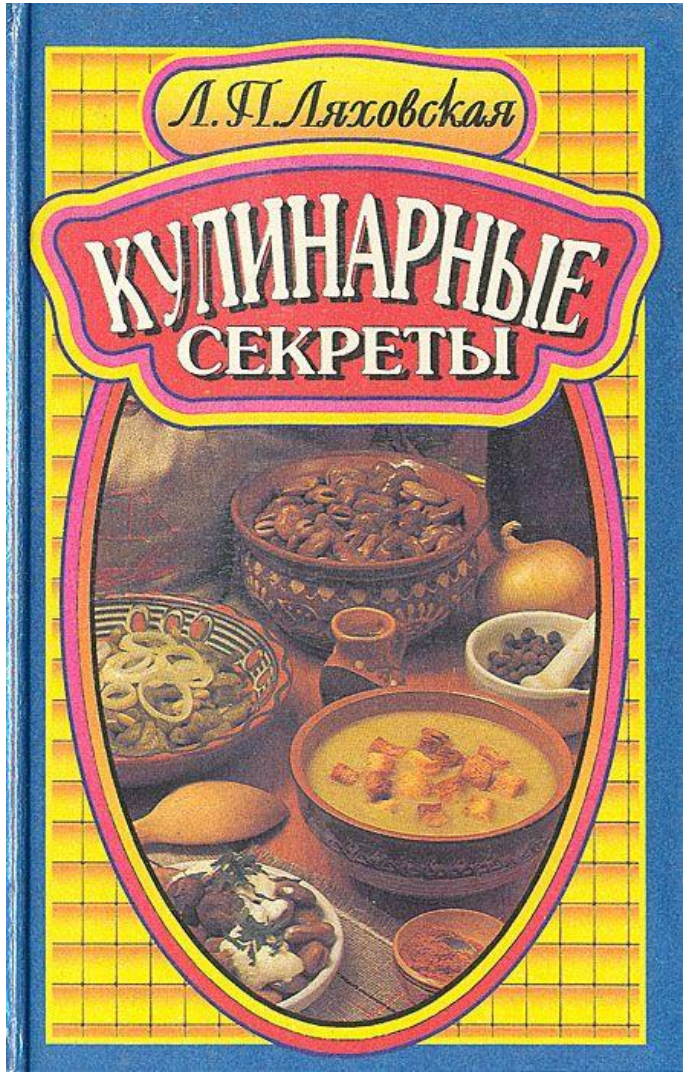
1. Acquire
2. Aggregate
3. Action

Intelligence с глобальным охватом, для получения широкого покрытия атаки

Провайдер с опытом в выявлении новых угроз на раннем этапе

Оперативные данные с контекстом

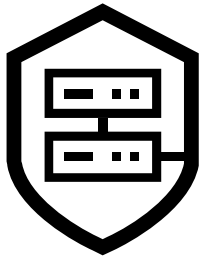
Форматы и механизмы доставки, позволяющие интегрироваться в существующие средства контроля безопасности



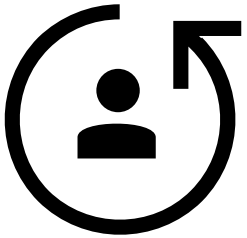
Kaspersky Threat Intelligence

Тренды и будущее

Унификация данных и автоматизация



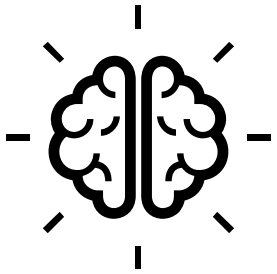
Цифровые риски



Целевая информация

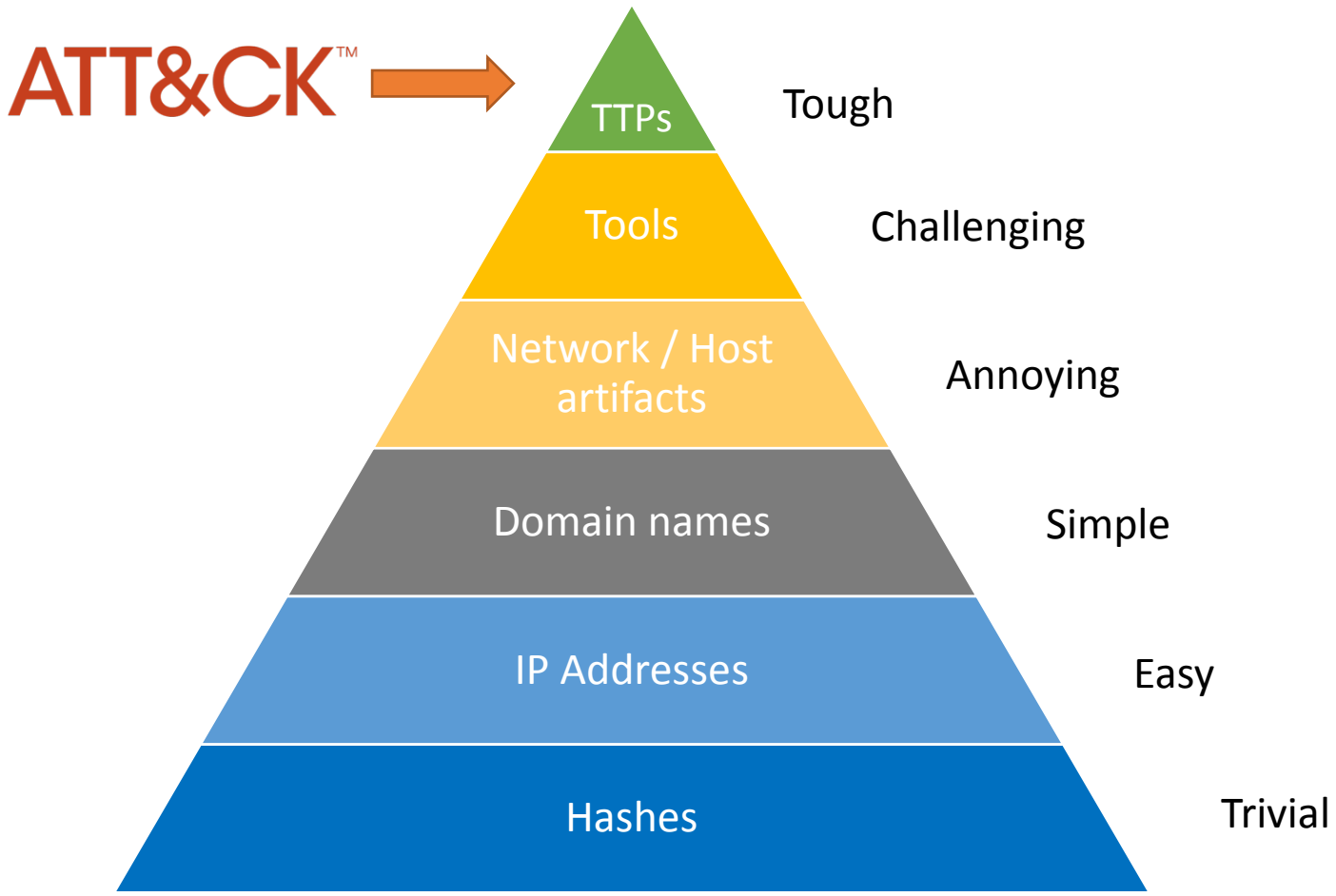
Поддержка бизнес-решений

Обмен информацией



Упрощение

MITRE



Источник: http://detect-respond.blogspot.coml

MITRE разработали базу знаний и структуру, известную как Adversarial Tactics, Techniques и Common Knowledge (ATT&CK). ATT&CK предоставляет базу знаний, описывающую поведение, действия и процессы, которые злоумышленники могут использовать после получения начального доступа в сети организации.

kaspersky

Спасибо за внимание

Alexander.Mazikin@kaspersky.com

Intelligence@kaspersky.com

kaspersky.com