ANOMALI®

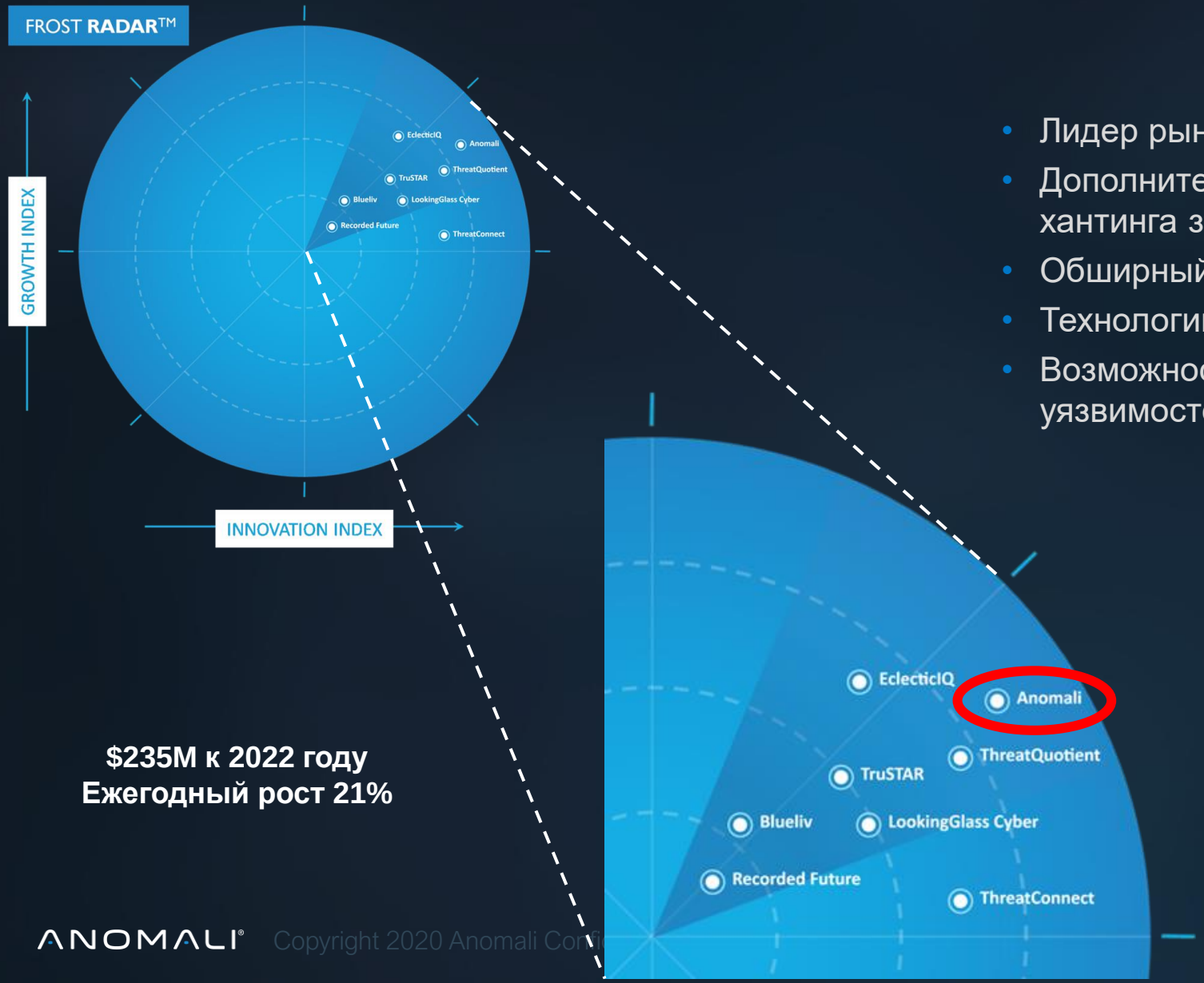
# Я — аналитик SOC.
# Что мне делать с киберразведкой, кроме отправки в SIEM и блокирования на файерволе?

**Илья Осадчий, Тайгер Оптикс**

**Profit Security Day, 4 декабря 2020 года**

ТАЙГЕР ОПТИКС

# Anomali признана лидером в исследовании рынка платформ киберразведки Frost RADAR



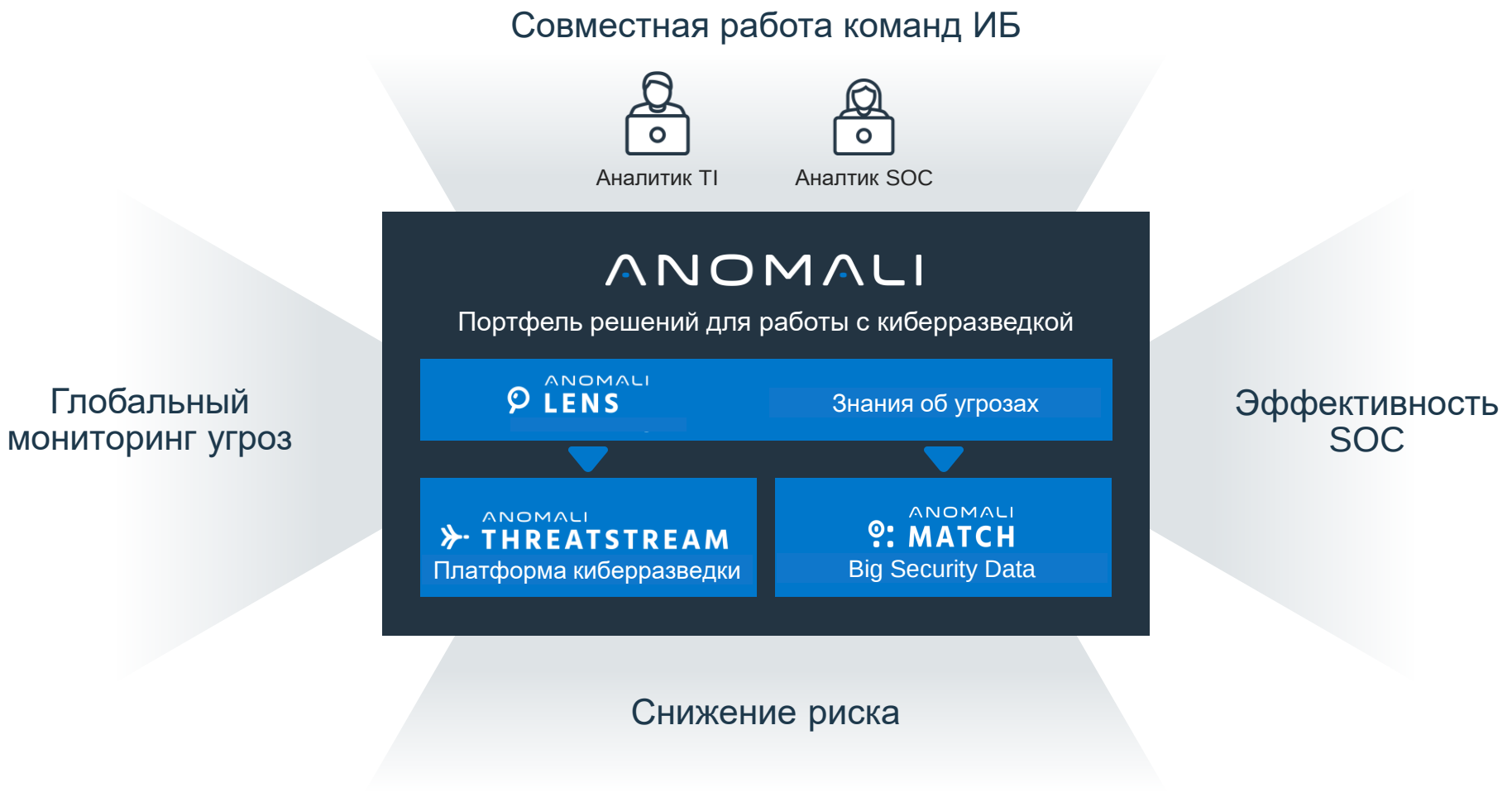

**$235M к 2022 году**
**Ежегодный рост 21%**

## Аспекты лидерства Anomali

- Лидер рынка – доля рынка 40%
- Дополнительная польза за счет выявления инцидентов и хантинга за угрозами
- Обширный список интеграций с СЗИ и фидами
- Технологии ML и обработки естественного языка
- Возможности управления риском и приоритизации уязвимостей

# Зачем нужна кибербразведка?

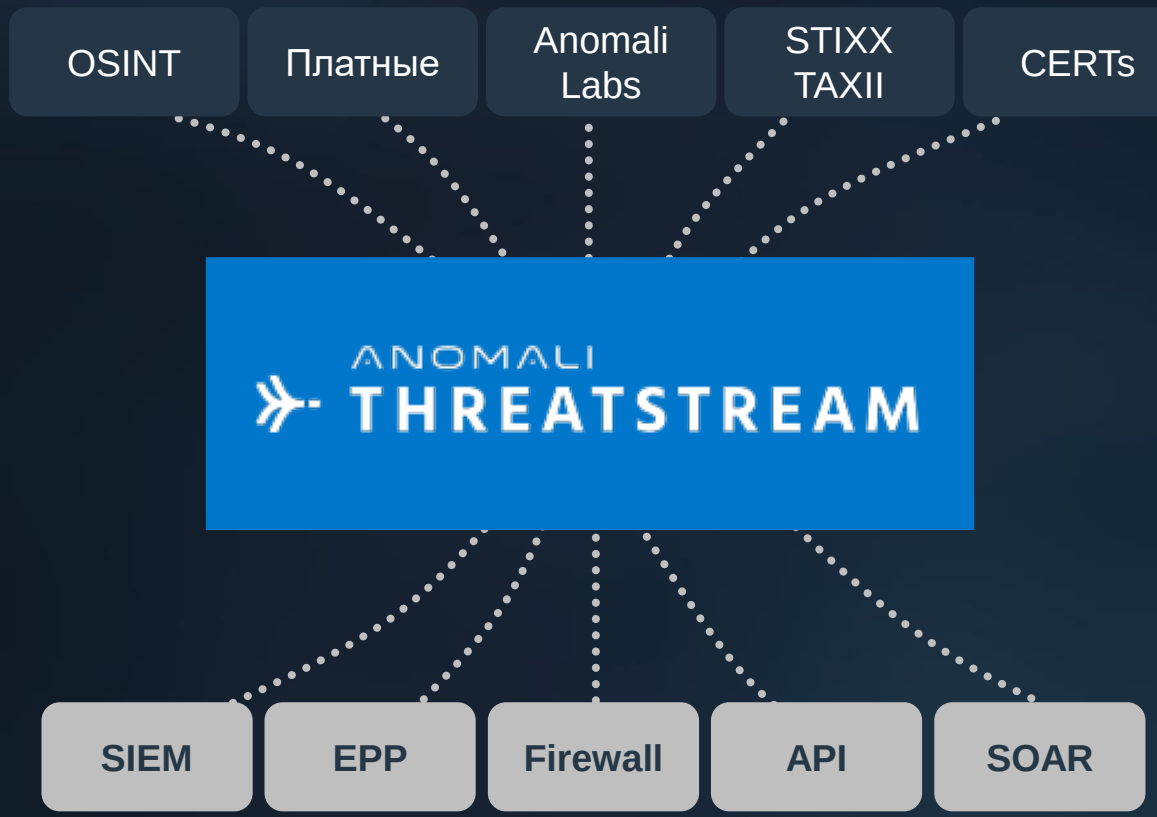
# Портфель решений Anomali для работы с киберразведкой



# Эволюция TIP по мере роста зрелости SOC

# Anomali ThreatStream

## Лидирующая платформа кибербразведки (TIP)




**СБОР**

- Сбор TI из ЛЮБЫХ источников
- Маркетплейс фидов
- Собственные фиды

**УПРАВЛЕНИЕ**

- Нормализация IOC из разных фидов
- Обогащение групп, кампаний, TTP
- Фолзы, дедубликация

**ИНТЕГРАЦИЯ И ОБМЕН**

- Обмен с коллегами и партнерами
- Интеграции с внешними СЗИ
- API для произвольных решений

# Маркетплейс кибербразведки
## 130+ премиальных фидов, обогащений и инструментов

### Фиды

INTEL471
FLASHPOINT
CROWDSTRIKE
REVERSINGLABS
KASPERSKY lab
Blueliv.
FIREEYE
Symantec

### Обогащения

VirusTotal
SILOBREAKER
FORSIGHT SECURITY
DOMAINTOOLS
Recorded Future
RISKIQ
ThreatCrowd
Cisco Umbrella

### Интеграции

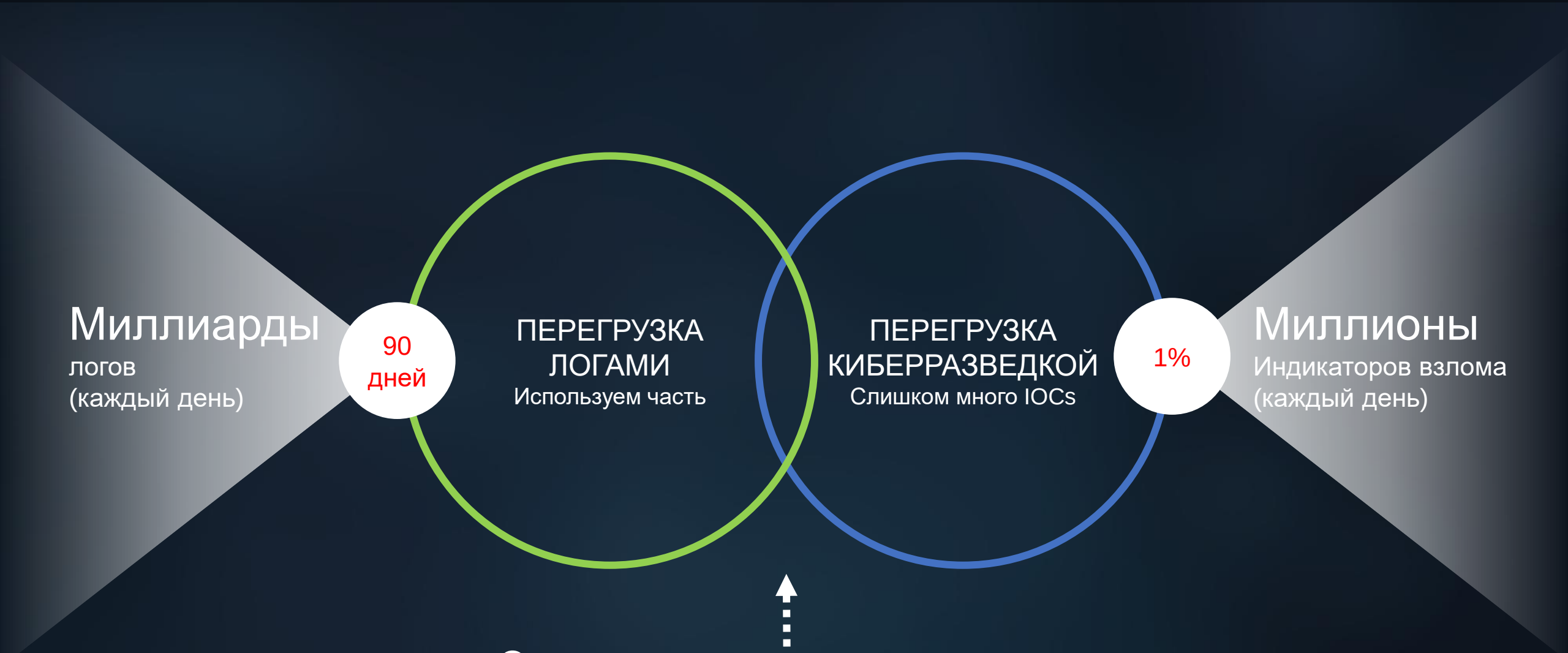
splunk>
IBM QRadar
ArcSight
FireEye
paloalto NETWORKS
elastic
zscaler
LogRhythm

### Инструменты

OpenDNS
MALTEGO
digital shadows_
VERODIN
LogicHub
JoeSecurity
servicenow
resilient an IBM Company

# Эволюция TIP по мере роста зрелости SOC

# SIEM не справляются со всем объемом данных




Ограниченное выявление угроз

# Anomali Match позволяет SOC снять ограничения SIEM


Полное выявление угроз

# Anomali Match
## Платформа Big Security Data для быстрого выявления угроз


**СБОР**

- 5 и более лет телеметрии
- 100 миллионов IOCs
- Данные об активах и уязвимостях

**ВЫЯВЛЕНИЕ**

- Непрерывный матчинг IOC
- Используя ВСЕ данные

**РАССЛЕДО-ВАНИЯ**

- Контекст и обогащения сработок
- Визуальный пивотинг и раскрытие

**ХАНТИНГ**

- Поиск за секунды
- Таймлайн, многомерный анализ

**РЕАГИРОВАНИЕ**

- Движок алертов и оркестрации
- Приоритизация по риску и критичности
- Автоматическое оповещение СЗИ

# Эволюция TIP по мере роста зрелости SOC

# Anomali ThreatStream и SOAR

Anomali SOAR Integrations

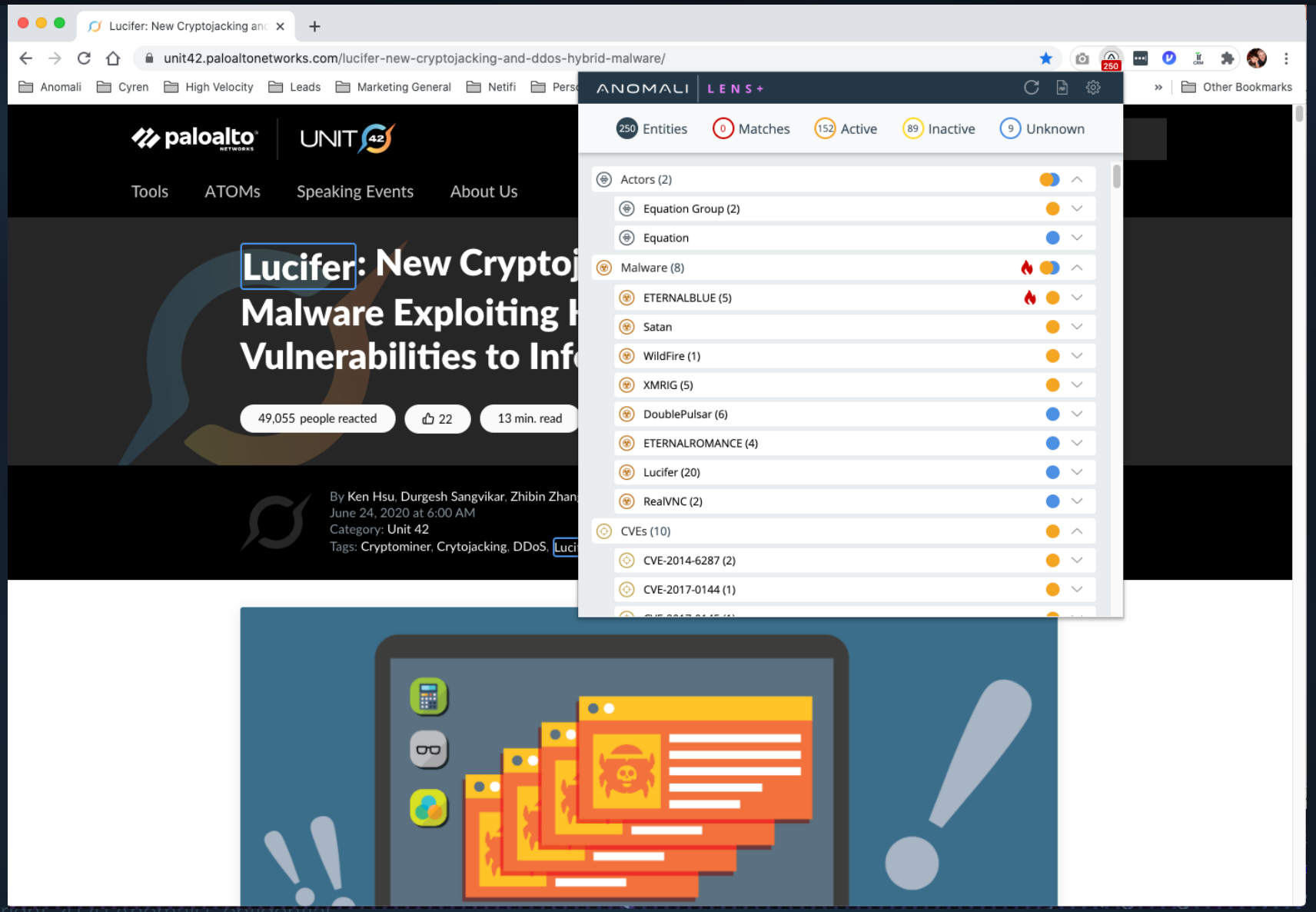
# Эволюция TIP по мере роста зрелости SOC

# Интеграции помогают лучше использовать TI

- Готовые интеграции с СЗИ
- Внутренние системы
- Блокирование, мониторинг
- Поддержка SIEM, FW, EPP…
- API для произвольных интеграций


splunk> · cisco · Carbon Black.
IBM QRadar · Check Point SOFTWARE TECHNOLOGIES LTD. · CROWDSTRIKE
ArcSight · paloalto NETWORKS · FIREEYE
McAfee · FORCEPOINT · TANIUM
Azure Sentinel · Infoblox · Qualys.
sumo logic · zscaler · tenable

# Инновации: Anomali Lens делает жизнь аналитика лучше



# ANOMALI®

Спасибо!

Пишите: io@tiger-optics.ru

Тайгер Оптикс