Anomali
Платформа кибербразведки и ретроспективного хантинга

Илья Осадчий, Тайгер Оптикс, io@tiger-optics.ru

Фрэнк Ландж, Anomali, flange@anomali.com

ANOMALI™

Вебинар записывается, запись будет выслана завтра

Задавайте вопросы!

Все решения доступны для теста

О компании Anomali

ANOMALI™

О компании Anomali

- Основана в 2013 создателями ArcSight
  - Пионер и лидер рынка *Threat Intelligence Platforms (TIP)*
  - Более 300 сотрудников
- Собственная конференция Anomali Detect, первая в отрасли
- Технологические партнеры в России – Kaspersky Labs и Group-IB
- Инвестиции – свыше $96M – Google, Telstra, Deutsche Telekom

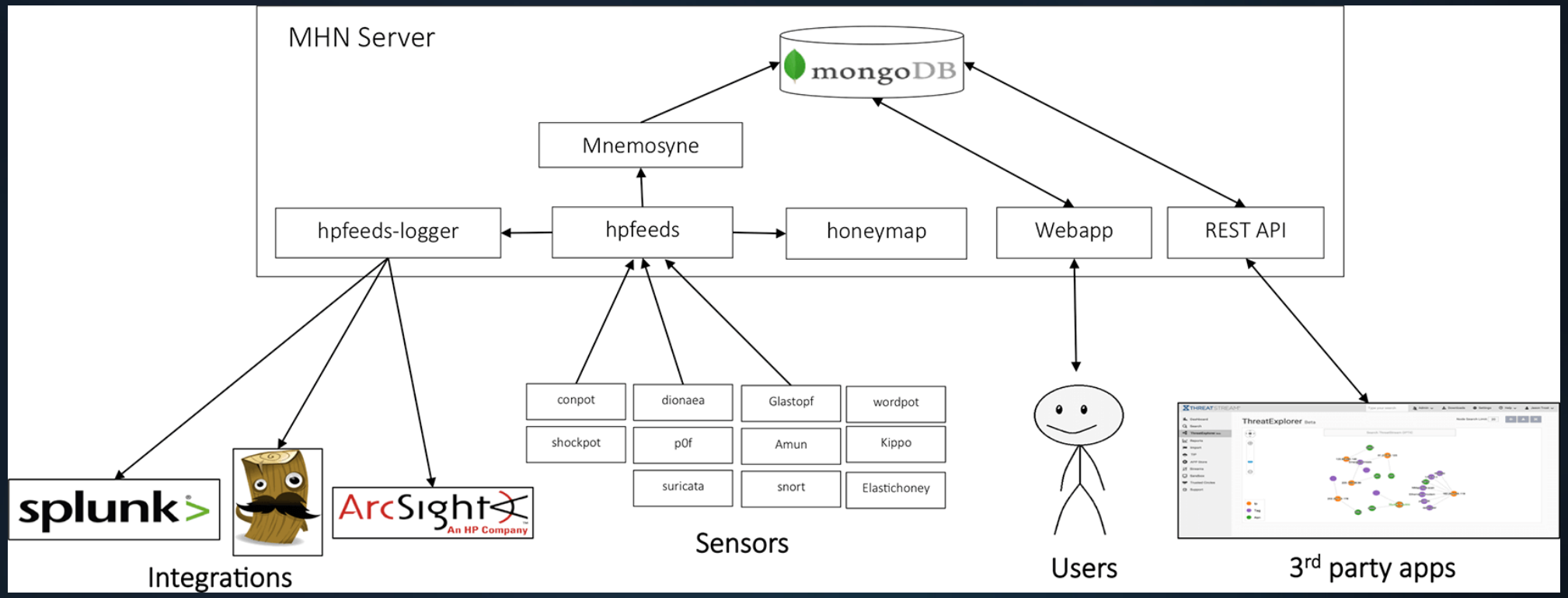
Успешные внедрения Anomali

- 35% списка Fortune 100
- Банковское сообщество ОАЭ
- Англия – обмен между банками
- Южная Африка – ISAC
- Швейцария – обмен данных на уровне страны
- Италия – CERTFin
- 1000 других пользователей

citibank® UBS CREDIT SUISSE BANK OF ENGLAND

Anomali Labs

- Крупнейшая сеть ханипотов в мире – источник данных для фида Anomali Labs
- Построена на **Modern Honey Network (MHN)** – система управления ханипотами, OSS разработка Anomali
- Более 12.000 инсталляций MHN, сбор данных со всего мира
- https://www.anomali.com/community/modern-honey-net



Продукты Anomali

ANOMALI™

ПЛАТФОРМА ANOMALI ALTITUDE

ANOMALI™

ИНФОРМАЦИЯ

ОБНАРУЖЕНИЕ

АВТОМАТИЗАЦИЯ

РАССЛЕДОВАНИЯ

ВЗАИМОДЕЙСТВИЕ

MATCH

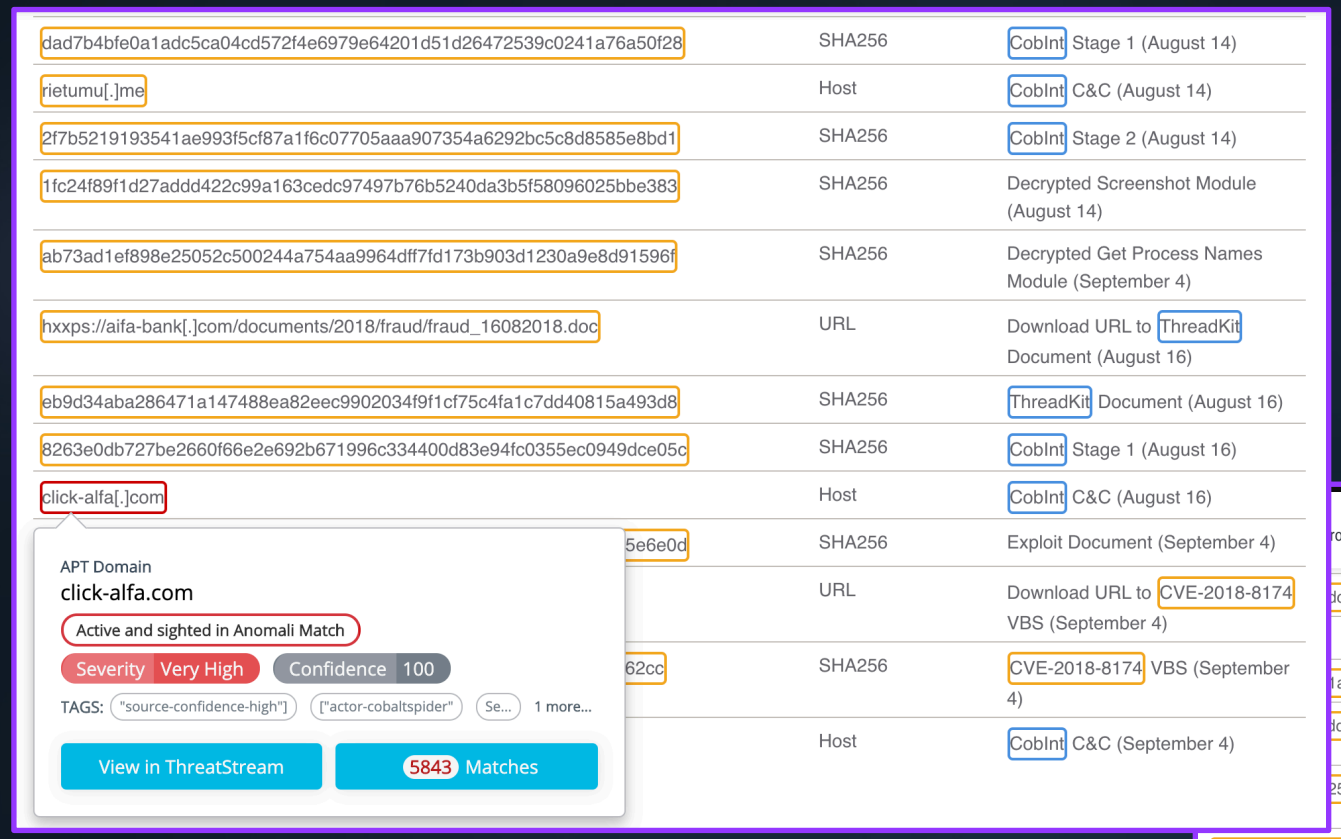
THREATSTREAM

LENS

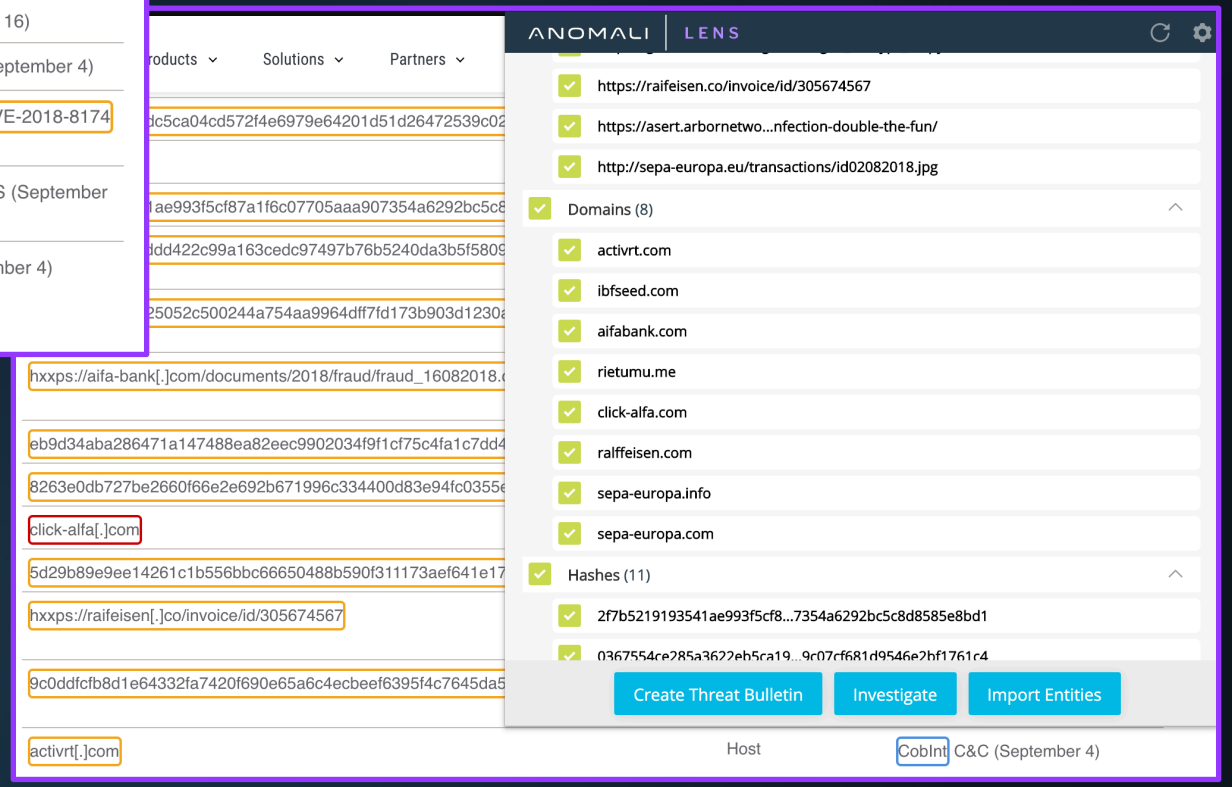
Anomali Lens

Идентификация угроз при работе в браузере

Anomali Lens – это первый парсер веб-контента, основанный на обработке естественного языка, который выделяют информацию о киберугрозах для дальнейших расследований



Anomali Lens сканирует содержимое веб-страниц и подсвечивает угрозы, которые были обнаружены в вашей сети с помощью Anomali Match.



Ускорение расследований за счет импорта контента в **Anomali ThreatStream** для дальнейшего анализа и интеграции с вашими СЗИ

Anomali ThreatStream

Выявление, расследование и реагирование на угрозы

ThreatStream позволяет операционализировать киберразведку и объединить все СЗИ, ускоряя выявление угроз и проактивную защиту

РАССЛЕДОВАНИЕ КИБЕРУГРОЗ

СБОР

Сбор фидов из любого источника
Поддержка STIX/TAXII
Двусторонний обмен IOC

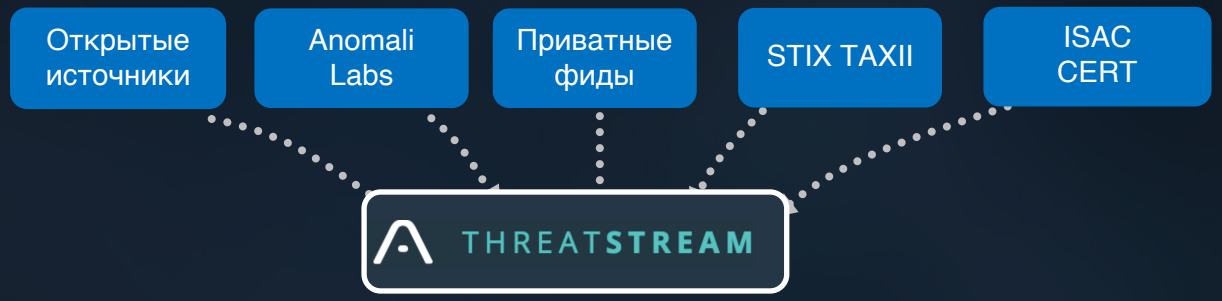
УПРАВЛЕНИЕ

Нормализация IOC между источниками
Обогащение Акторами, Кампаниями, TTP
Дедубликация, ложные срабатывания

ИНТЕГРАЦИЯ

Скачивание индикаторов
Интеграции с внутренними СЗИ
Любые интеграции с SDK и API

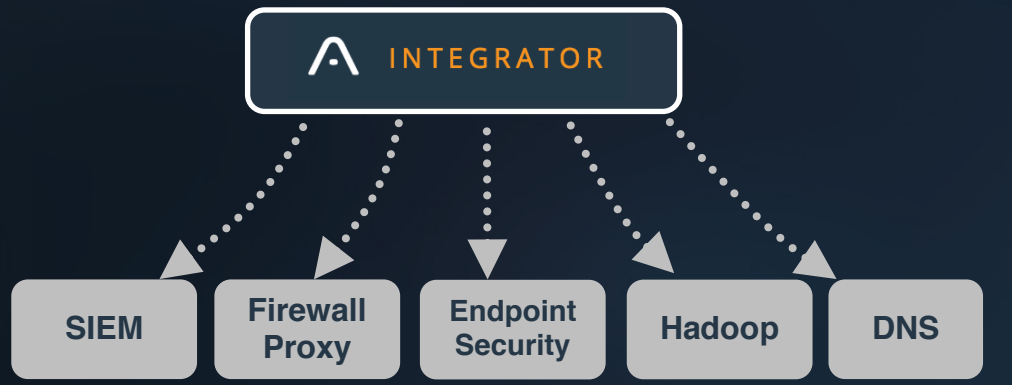
Источники информации об угрозах



ANOMALI | Blueliv. | cisco | COFENSE | CROWDSTRIKE
CSIS | digital shadows_ | FLASHPOINT | fraudlogix | Georgia Tech Research Institute
GROUP-IB | iDefense Part of Accenture Security | INTEL471 | iSIGHTPARTNERS | KASPERSKY lab
proofpoint. | REVERSING LABS | Silobreaker | SIXGILL Deep, Dark & Beyond | Support Intelligence TOTAL NETWORK SECURITY MONITORING
Symantec. | THE MEDIA TRUST CONTINUOUS INSIGHT. | | WAPACK LABS CYBER INTELLIGENCE SERVICE | WEBROOT

+ свободные интеграции на базе веб-интерфейса, API или SDK

Интеграции с приемниками данных



accelops
ArcSight An HP Company
BlueCoat
The Bro Network Security Monitor
Bit9 + CARBON BLACK
Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO ASA
cloudera
CROWDSTRIKE
FireEye
HIVE
Infoblox
LogRhythm
McAfee
MISP Threat Sharing
Phantom
paloalto NETWORKS
Radar
RSA SECURITY ANALYTICS
splunk>
TANIUM

Приведен не полный список. Доступны другие готовы интеграции, а также SDK и API

Anomali Match

Идентификация злоумышленников вашей сети. Ретроспективный анализ и Security Big Data

Ранее выявление и идентификация злоумышленников в сети за счет корреляции десятков миллионов индикаторов угроз с сетевыми логами и журналами активности в реальном времени

Anomali Match позволяет видеть угрозы в вашей сети и сокращать время выявления критических взломов за счет сопоставления журнальных данных за несколько лет со всеми данными кибербразведки в реальном времени

Anomali. От тактики к стратегии

RAW IOCs

IP: 123.45.67.89

MAL: A07DV0D7A...

URL: WWW.BADDOM...

EML: J0E@MA1BANK...

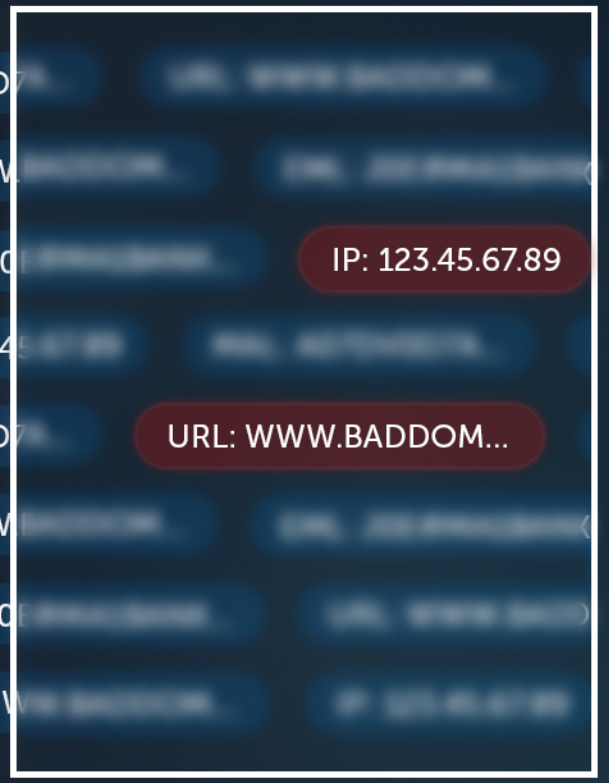
IP: 123.45.67.89

MAL: A07DV0D7A...

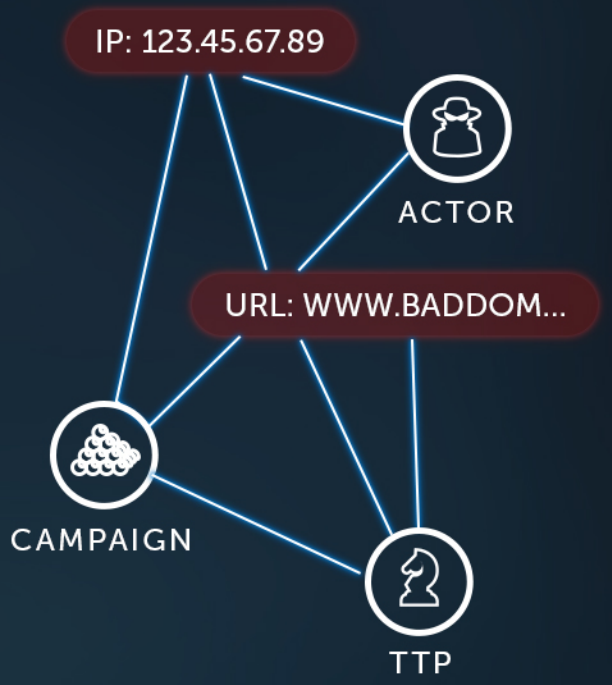
URL: WWW.BADDOM...

EML: J0E@MA1BANK...

DETECT



ASSOCIATE



INVESTIGATE

ДЕМОНСТРАЦИЯ

Закажите бесплатный пилот:
sales@tiger-optics.ru

ANOMALI™

Спасибо!

Илья Осадчий, Тайгер Оптикс, io@tiger-optics.ru