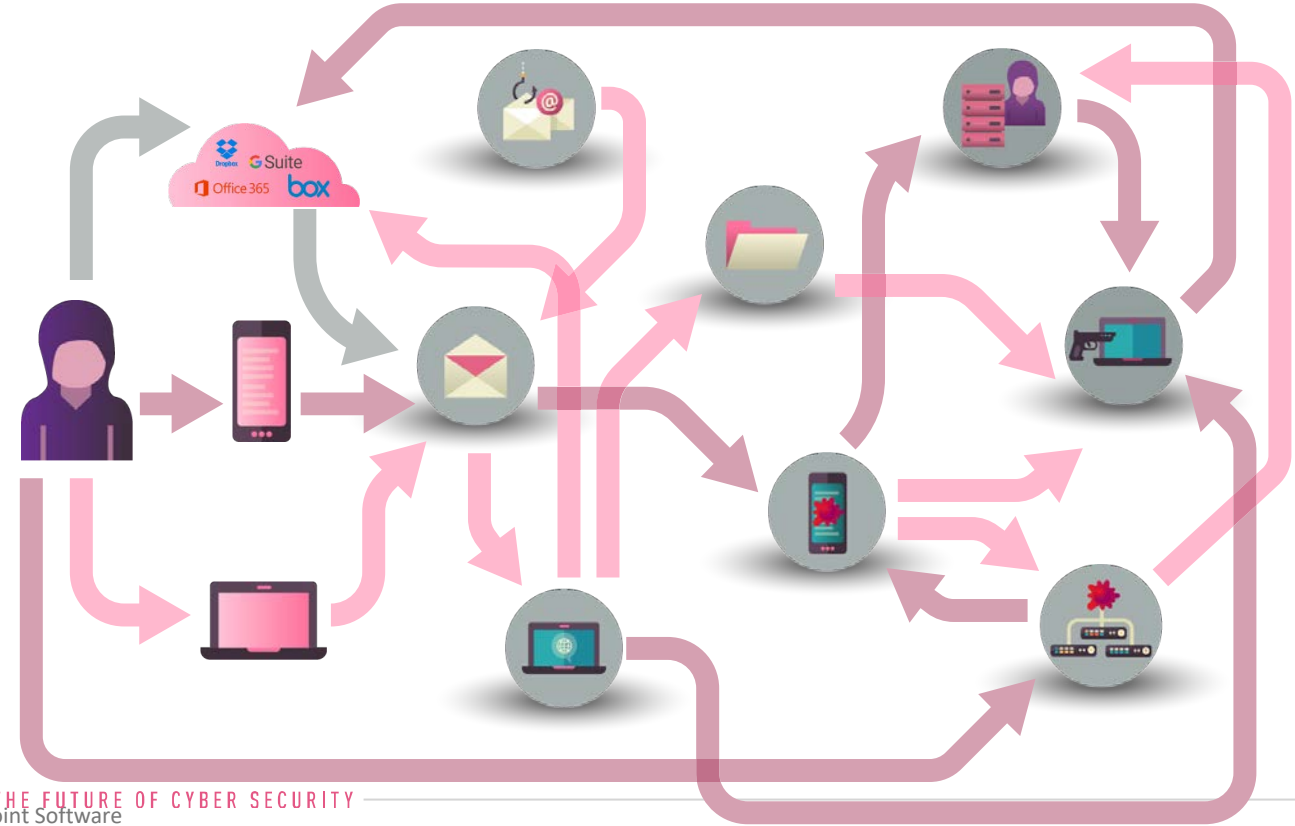
Check Point
SOFTWARE TECHNOLOGIES LTD

КАК ПРЕВЕНТИВНАЯ БЕЗОПАСНОСТЬ УПРОЩАЕТ ЖИЗНЬ SOC

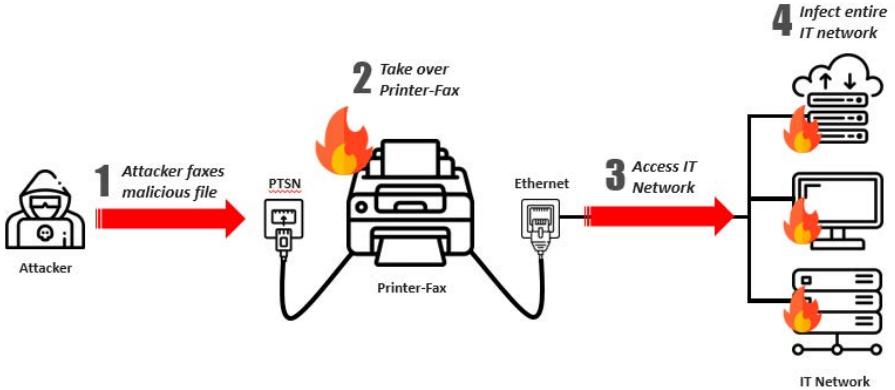
Денисов Валерий |Инженер, Check Point
vdenisov@checkpoint.com

Множество сервисов и устройств

Множество векторов и комбинаций для атаки



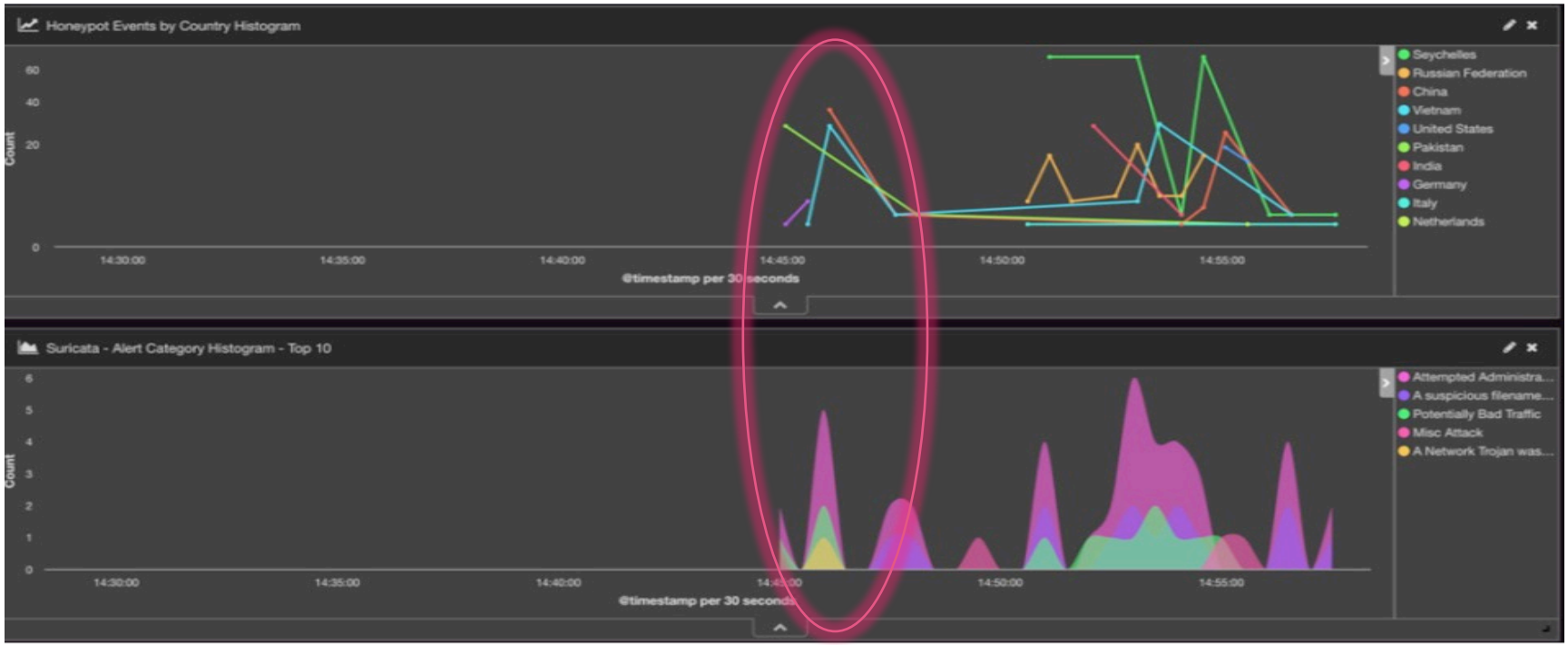
Новый неожиданный вектор атак



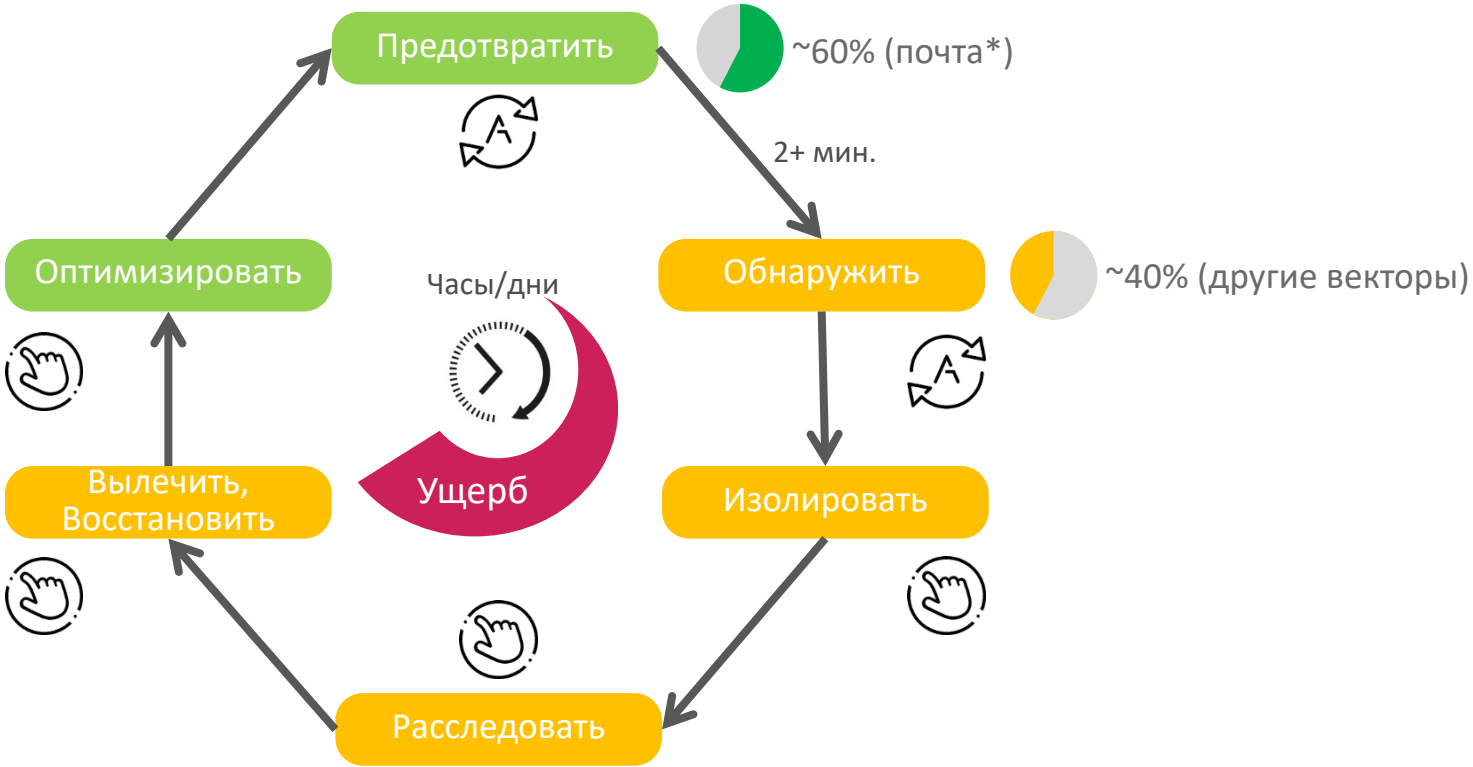
Еще больше причин для внутренней сегментации и защиты конечных станций

https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/

Уязвимые сервисы взламывают за минуты



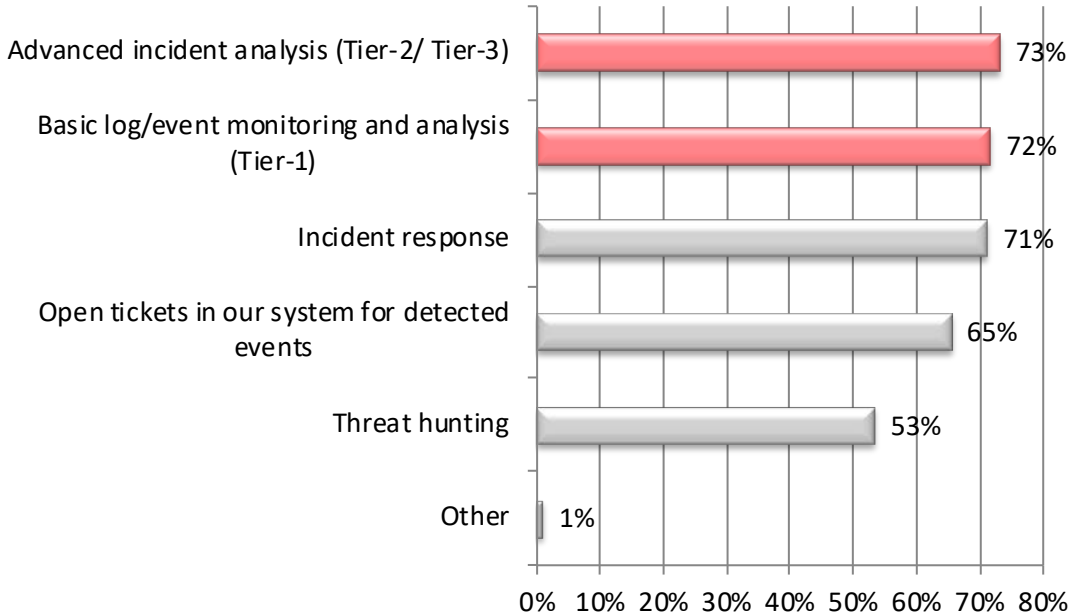
Классический подход к защите от новых угроз



*Векторы доставки вредоносных файлов в СНГ (3 мес.)

У SOC множество задач

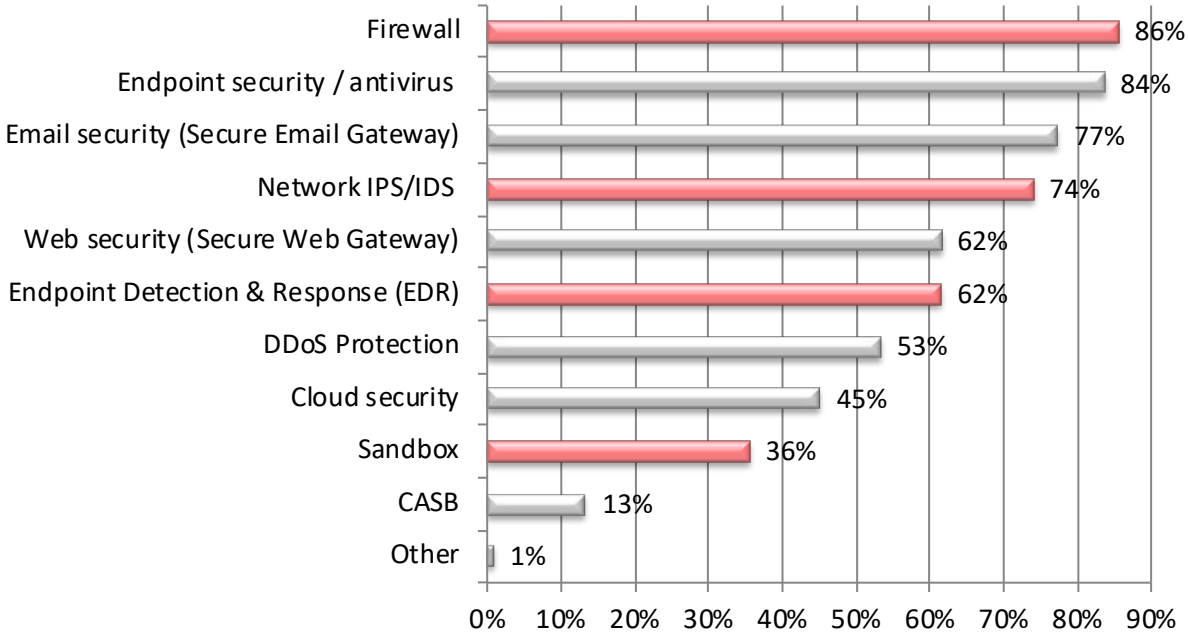
Компанией Dimensional Research был проведен опрос ИТ специалистов о задачах SOC



По данным Dimensional research, 2019

В SOC стекаются данные от целой плеяды средств ИБ

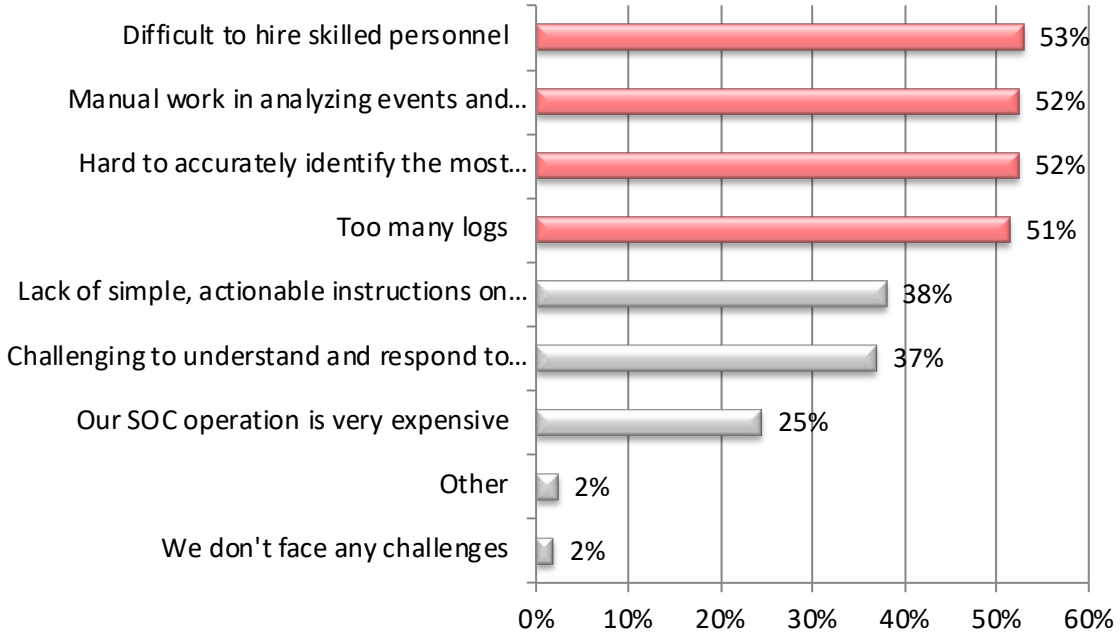
Какие средства ИБ генерируют события для SOC?



По данным Dimensional research, 2019

Большинство SOC борются с огромными объёмами событий и инцидентов

Какие основные трудности в работе SOC?



По данным Dimensional research, 2019

Что может помочь SOC ?

Автоматизация

Полная автоматизация рутинных операций, интеграция с SOAR системами

Инструменты

Понятные и простые в использовании инструменты для анализа событий ИБ

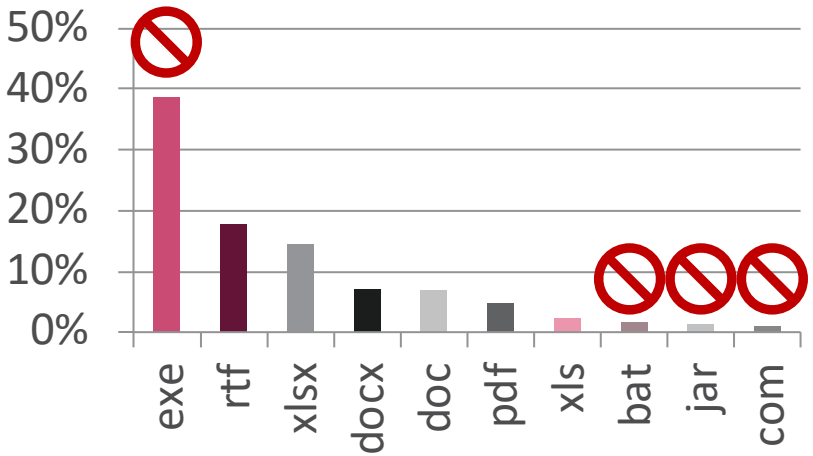
Предотвращение

Мгновенная реакция на возникающие угрозы и атаки, включая 0-day

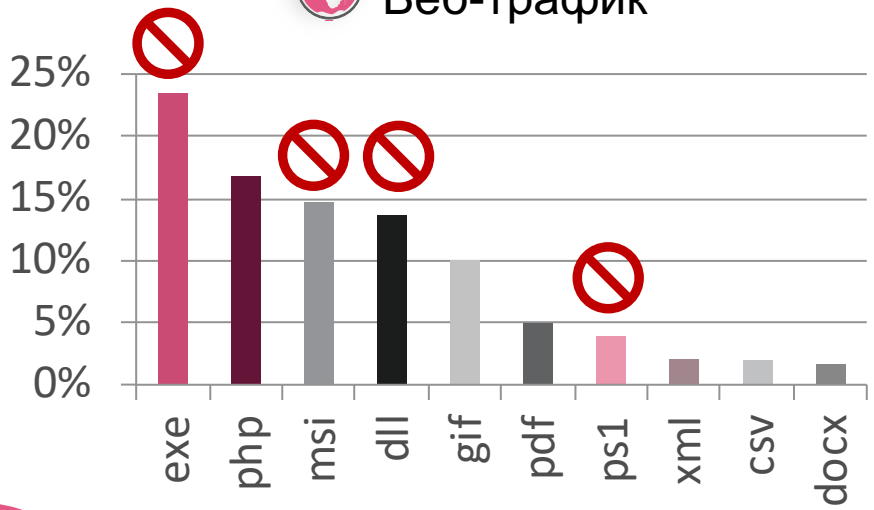
Форматы и векторы доставки вредоносных файлов в СНГ (3 мес.)

Check Point
SOFTWARE TECHNOLOGIES LTD

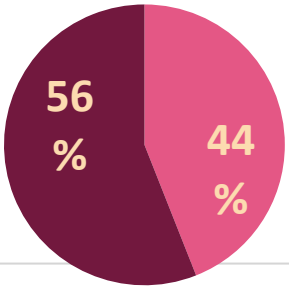
Электронная почта



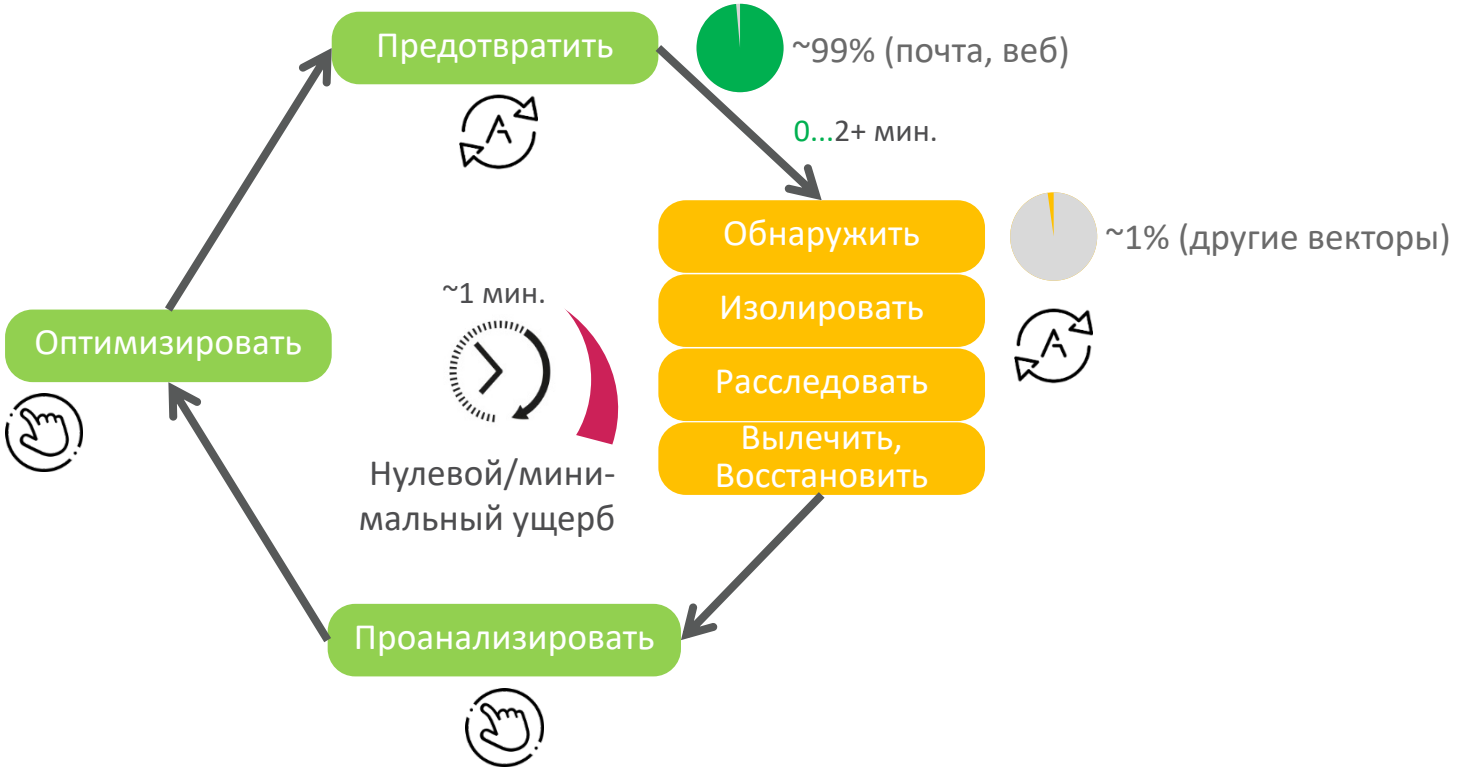
Веб-трафик

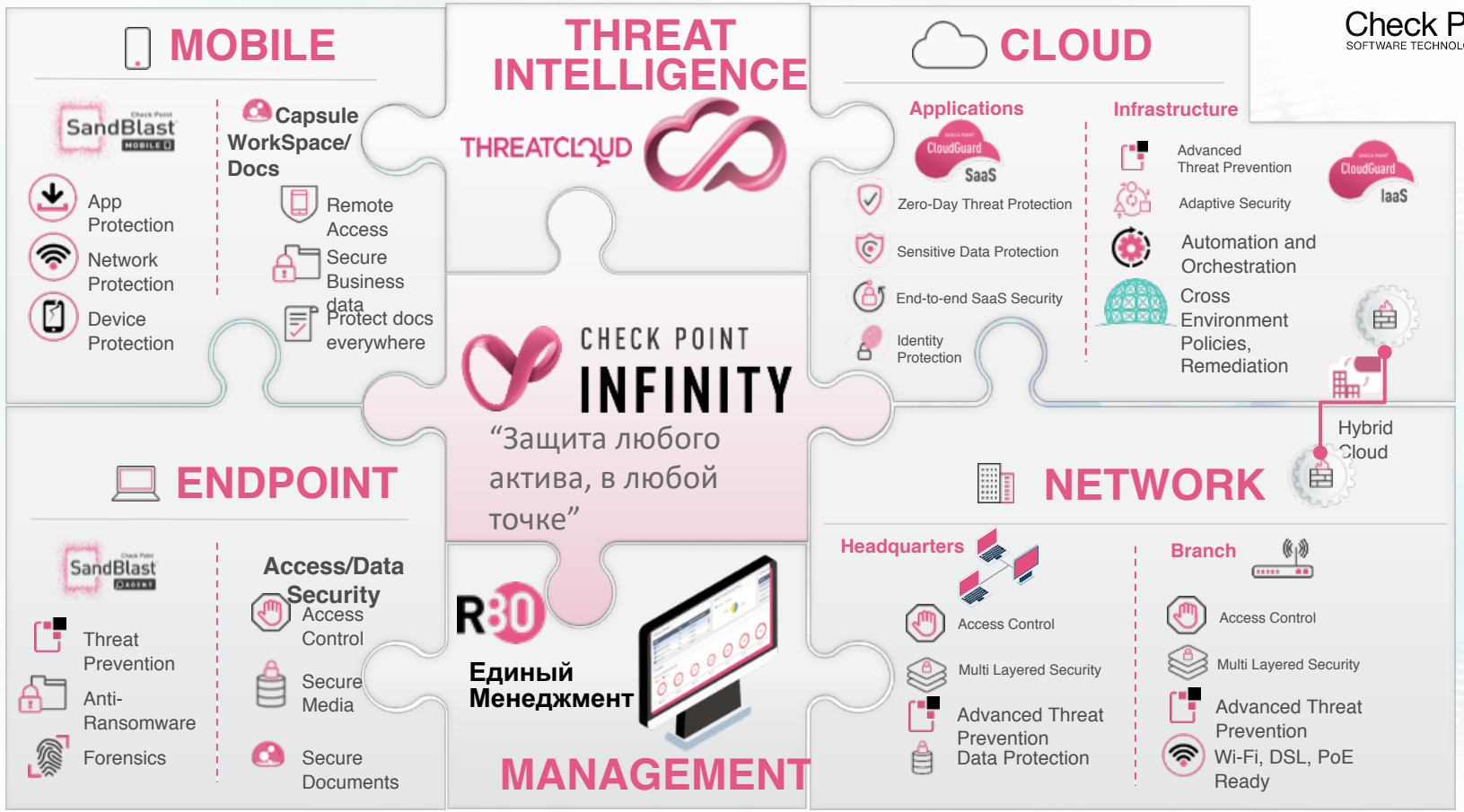


Блокируем лишнее:
Уменьшаем количество инцидентов



Подход Check Point к защите от новых угроз





THREATCLOUD

Check Point
SOFTWARE TECHNOLOGIES LTD

Внешние Фиды

- CERTs
- ИБ вендора

INFINITY

- Защита Мобильных устройств
- Агенты на ПК
- 0phishing
- Песочницы

Исследования

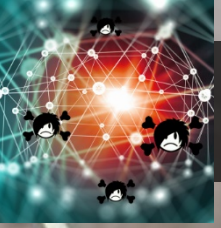
- Поиск компаний
- Анализ вредоносов

ML & AI

- DGA lab
- Toctopus
- Miners

Заказчики

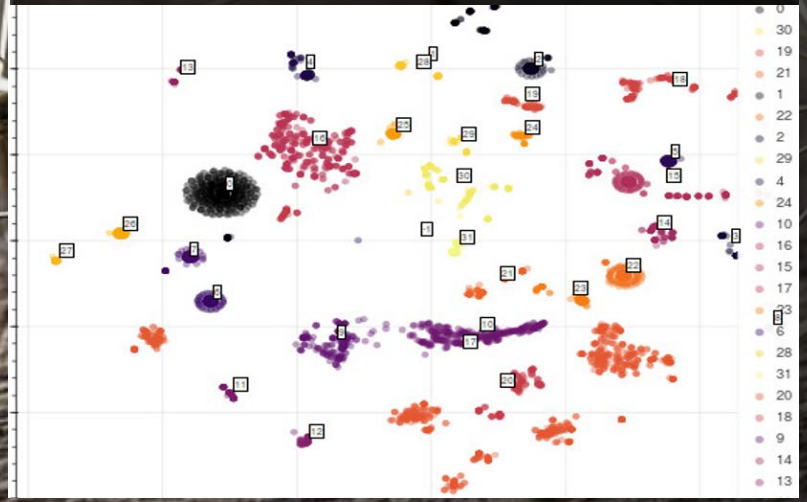
- Пилоты
- Расследование инцидентов
- Анализ событий



ПОИСК КАМПАНИЙ

ПРЕДСКАЗАНИЕ THREAT INTELLIGENCE

Кластеры семейств вредоносов



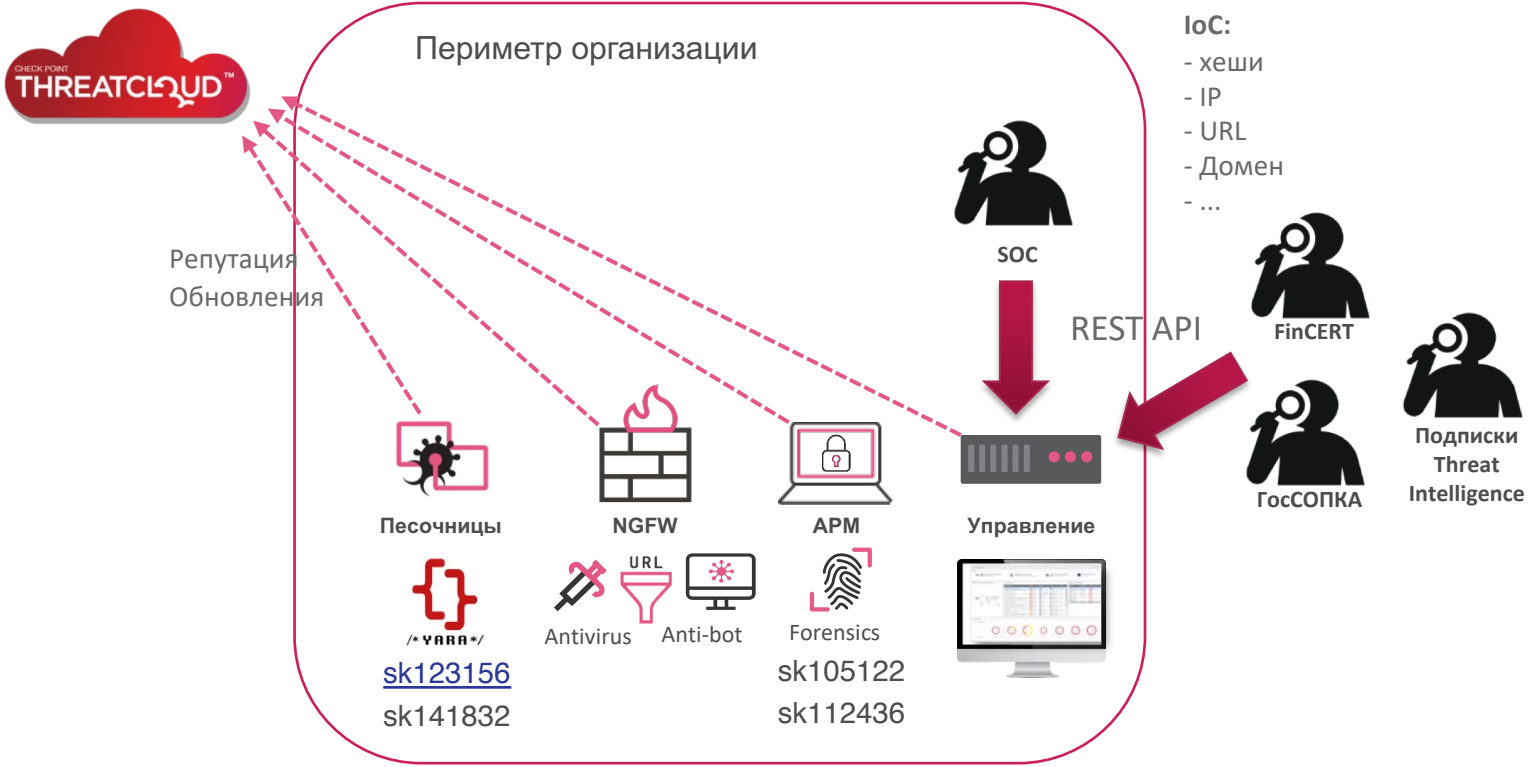
Определить “ДНК” семейства вредоносов

Автоматических классифицировать новые самплы

Обнаружить новые адреса и домены C&C

Пополнить базу Threat Intelligence для предотвращения кампаний

Импорт сторонних индикторов компрометации



CHECK POINT
SandBlast™
ZERO-DAY PROTECTION

Семейство продуктов

SandBlast
Облако Check Point

SandBlast
Партнерский SandBlast Service

Локальное устройство SandBlast

NETWORK

Шлюз на периметре, эл. почта, ЦОД

AGENT

Агенты на ПК и серверах

CLOUD

New: CloudGuard SaaS

Office 365
G Suite
Dropbox
salesforce
box
servicenow

<API>

Интеграция с веб-порталами, CRM, СЭД

SANDBLAST THREAT EMULATION

Единственная песочница, защищенная от обхода

CPU-LEVEL

- Human Interaction Simulator
- UAC Monitor
- SMEP Detector
- Static Analyzer

MACRO ANALYSIS & OVERRIDE

- DeepScan

TRAPS & DECOYS

- FP Guard
- Icon Similarity
- Virtual Network Service
- Evasion Detection

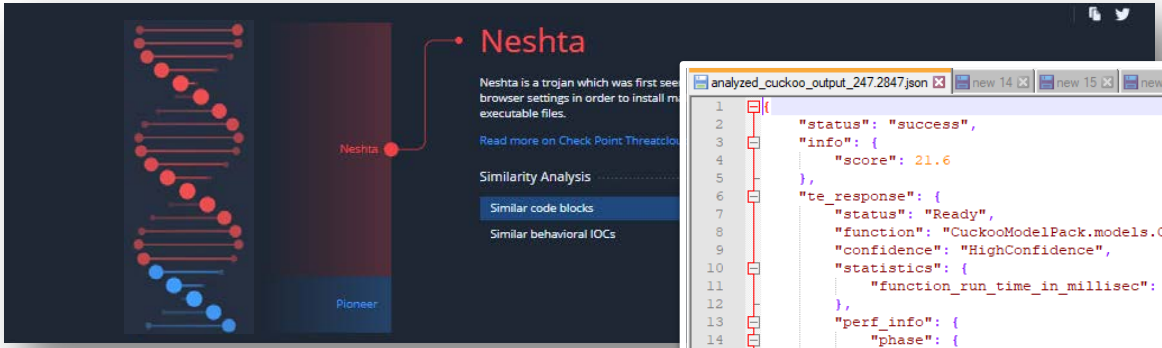
FLASH PUSH-FORWARD

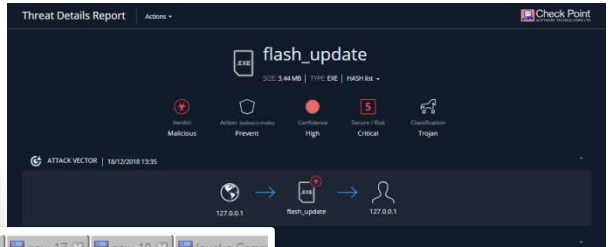
- Image Sanitation
- Network Activity Monitor
- DGA Generator
- Link Scanner

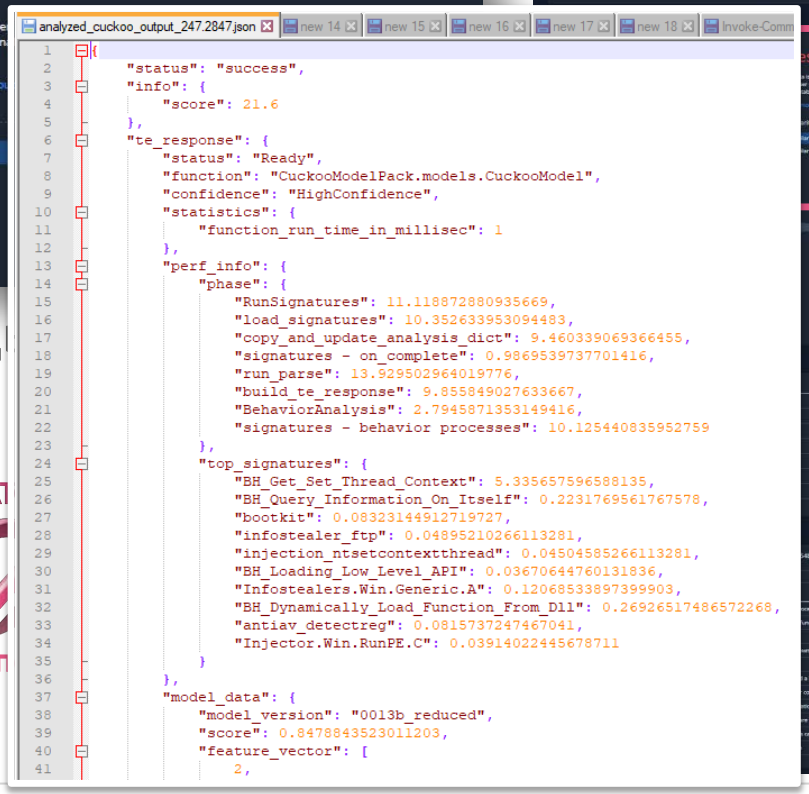
MACHINE LEARNING

- Dropped File Emulation
- Shellcode Detector

Выявление «ДНК» новых вредоносов







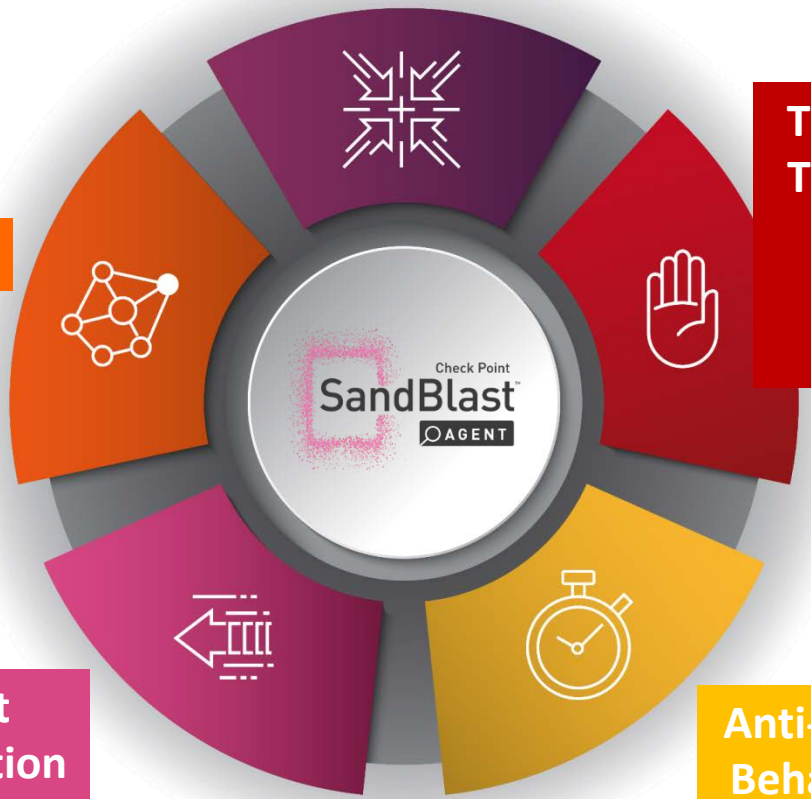
Классификация с помощ
обучения

Что должен уметь современный ендпоинт (EDR) ?

FW, AppCtrl, URLF

Threat Emulation
Threat Extraction
Anti-Exploit
Zero-Phishing
NGAV

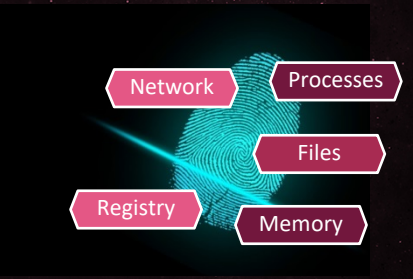
Forensics



FW, Anti-Bot
Auto-Remediation

Anti-Ransomware
Behavioral Guard

Перехват угроз в реальном времени на конечной станции



ANTI-RANSOMWARE | ANTI-EXPLOIT | ANTI-BOT | BEHAVIORAL GUARD

Все время

МОНИТОРИНГ И ЛОГИРОВАНИЕ АКТИВНОСТИ ПРОЦЕССОВ

Шифровальщики | Аномалии в памяти | Трафик к C&C | Модели поведения

Резервирование

Измененные файлы

В момент обнаружения

АНАЛИЗ, КАРАНТИН, ВОССТАНОВЛЕНИЕ

Все элементы атаки на основе данных форенсики

Восстановление	Остановка	Блокировка	Классификация
Зашифрованные файлы	Взломанный процесс	Обратные каналы	Семейство вред.

Изоляция

Процессы или станция целиком

После инцидента

Автоматизированное расследование инцидента

С помощью скоррелированных логов и детального отчета форенсики

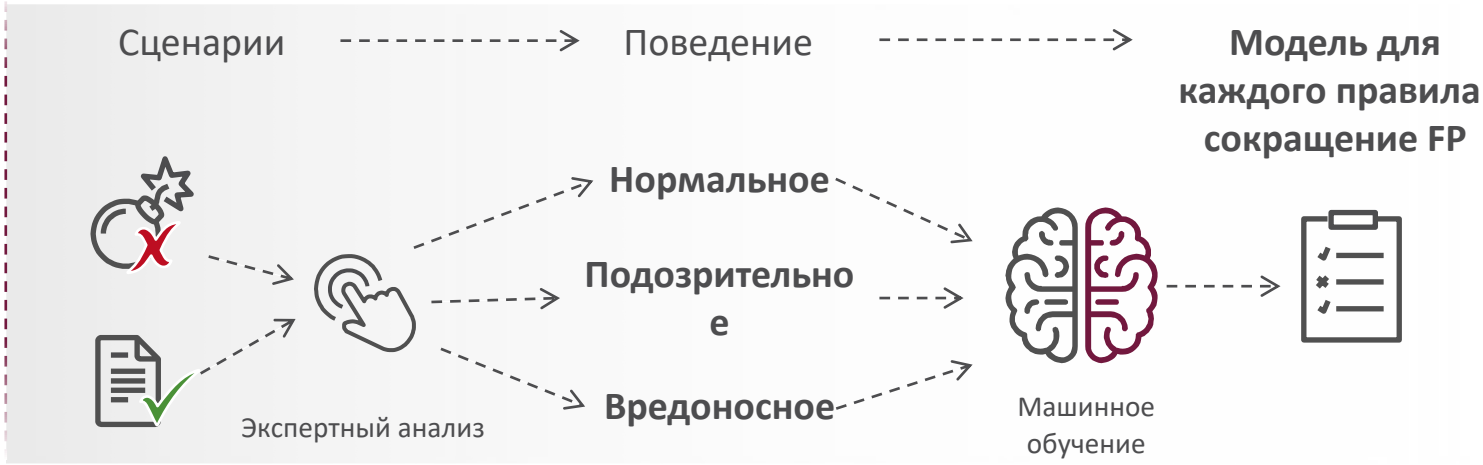
Подключаем ИИ к поведенческому анализу

Check Point
SOFTWARE TECHNOLOGIES LTD

Этап 1

Обучение

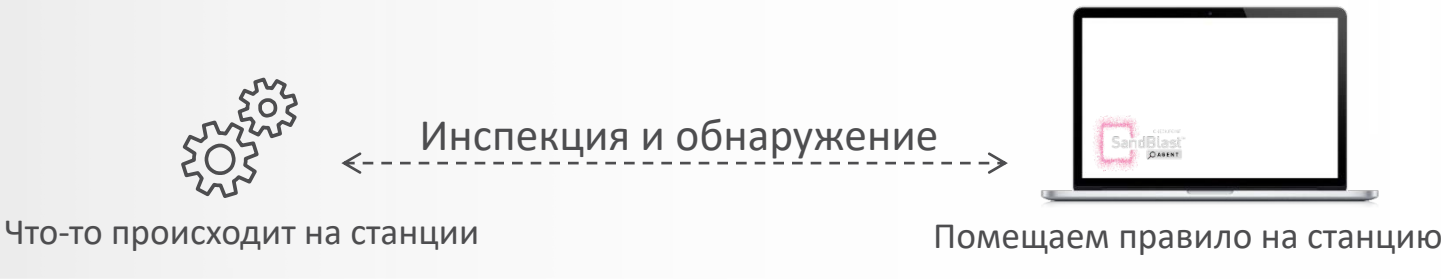
THREATCLOUD



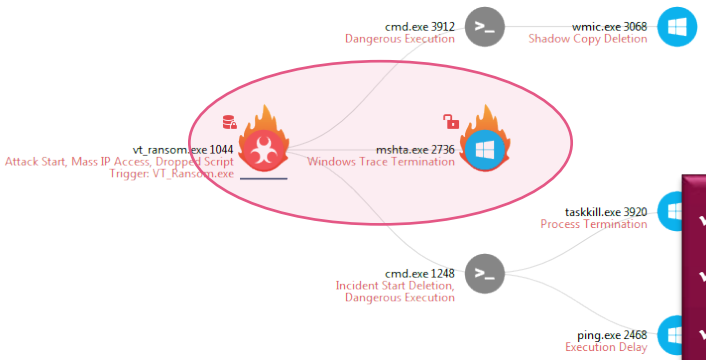
Этап 2

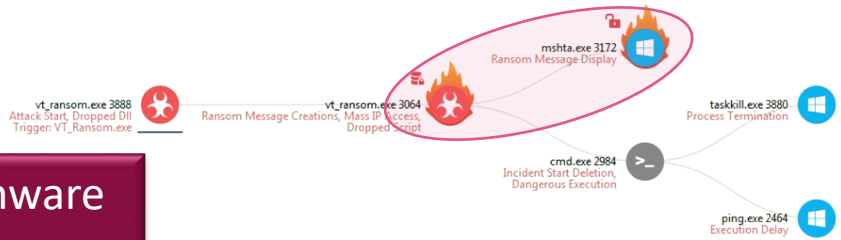
Применение

Защищенная станция

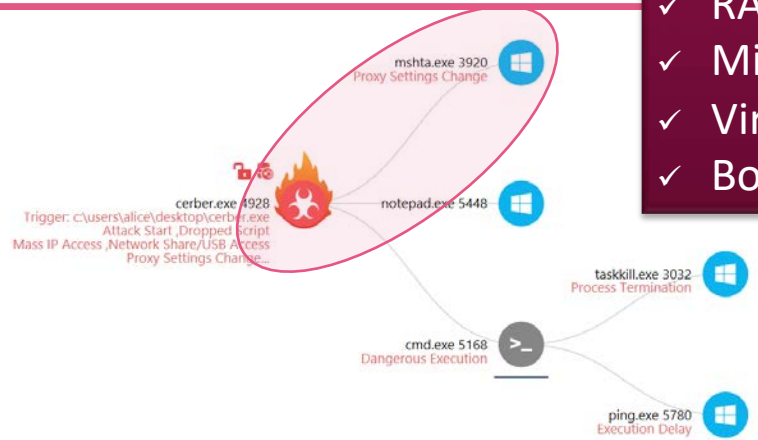


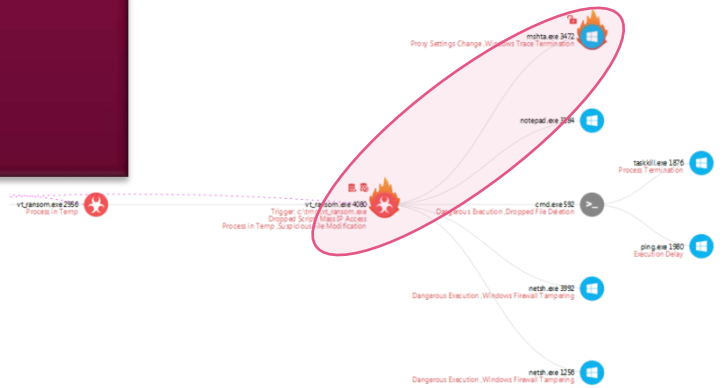
Behavioral Guard блокирует атаки по поведению





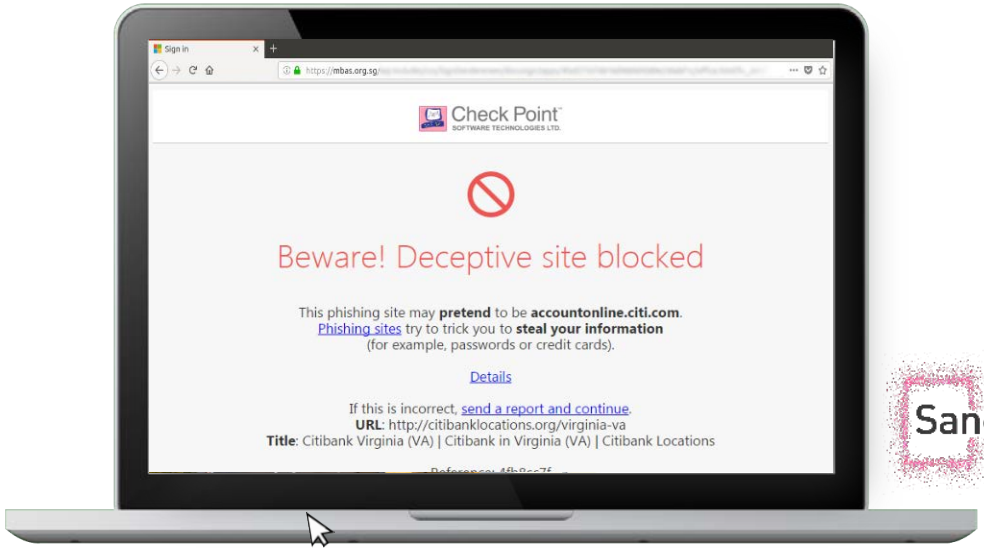
- ✓ Ransomware
- ✓ Bankers
- ✓ Trojans
- ✓ RATs
- ✓ Miners
- ✓ Viruses
- ✓ Botnets



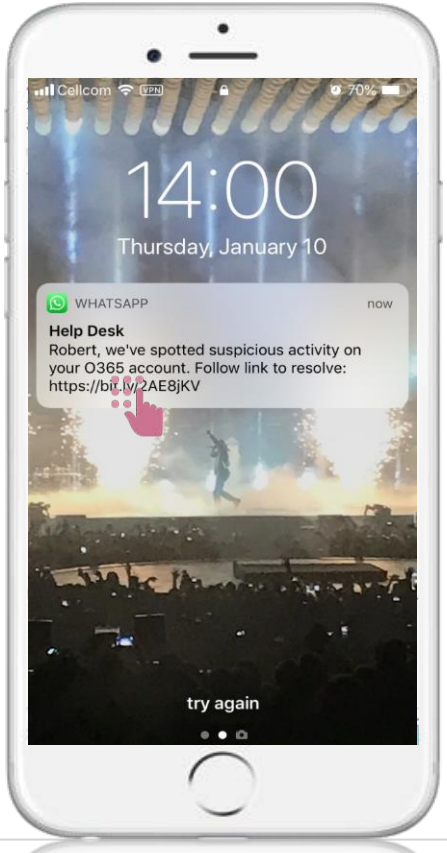


*на примере отчетов для CERBER

Защита от 0-day фишинговых сайтов непосредственно в браузере



Check Point SandBlast AGENT



Check Point SandBlast MOBILE

Анализ **содержимого** веб-страницы, а не только репутации

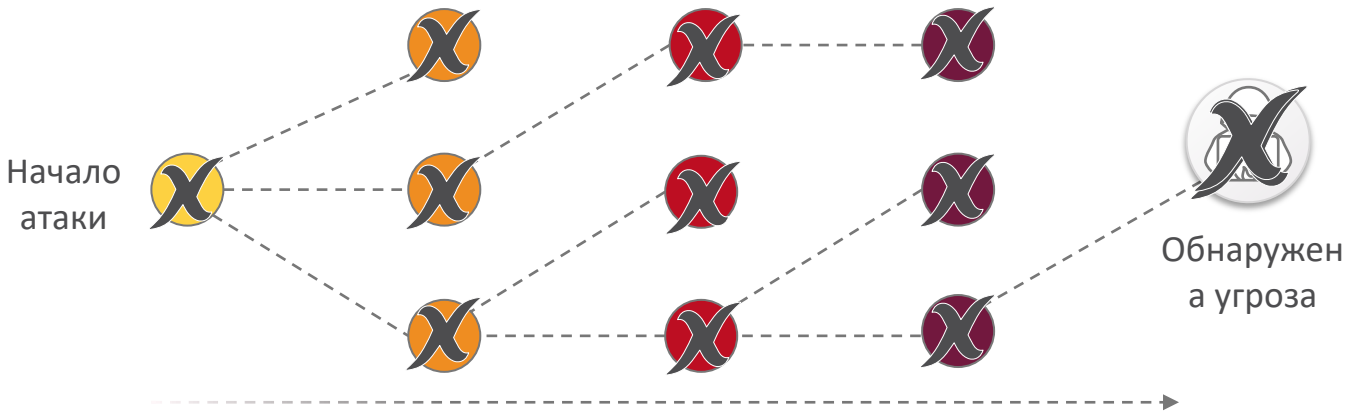
Автоматическое лечение и восстановление

Современные атаки: сложные, в несколько стадий

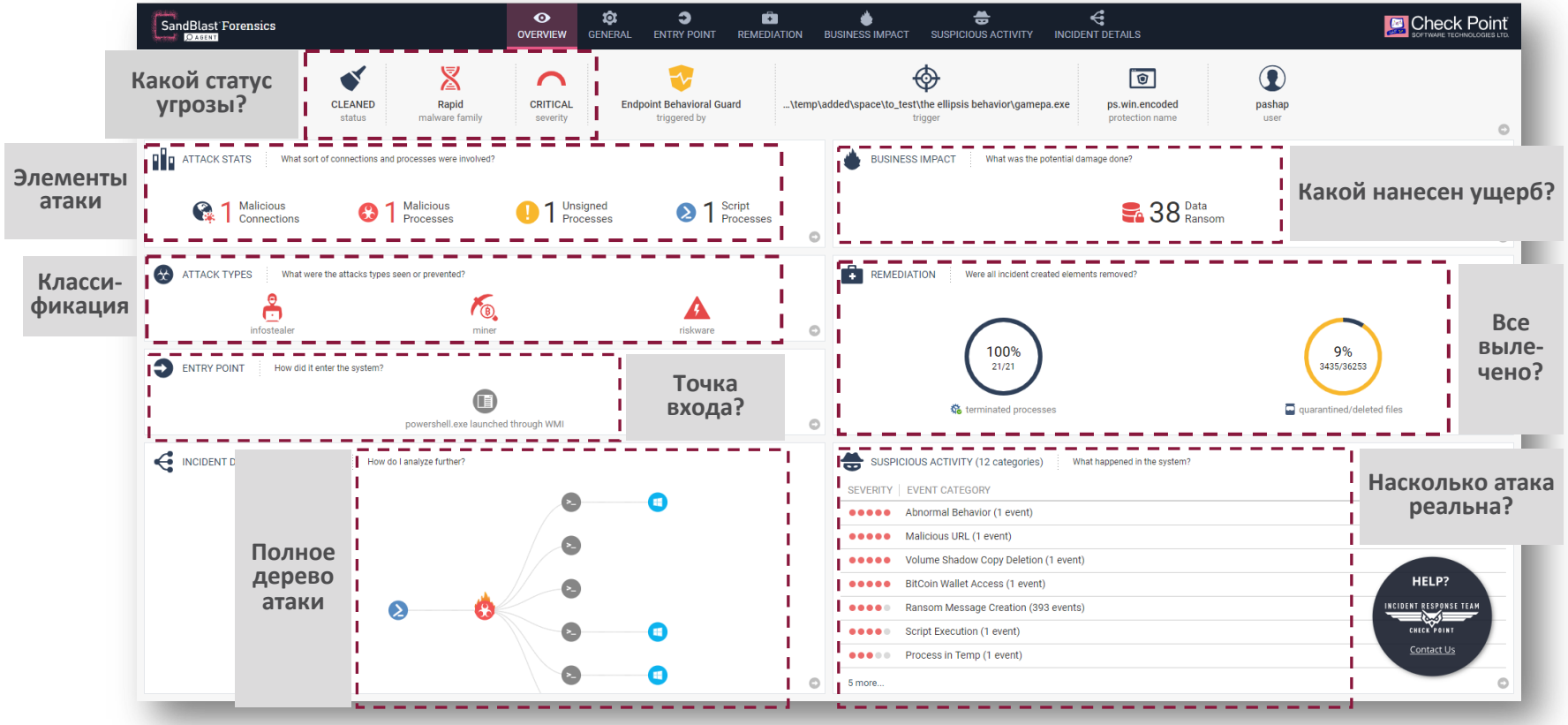
Другие решения: удаляют только то, на что среагировали

Угроза может вернуться!

Полное устранение всех последствий атаки!



Детальные отчеты Forensic



Комплексная защита от новых кибер-атак и сокращение издержек SoC

Check Point SandBlast™

NSS LABS RECOMMENDED

Сеть

Check Point SandBlast™ AGENT

NSS LABS RECOMMENDED

ПК, Mac

Check Point SandBlast™ MOBILE

IDC Analyze the Future

MTM Leader

Android, iOS

Предотвращение в реальном времени: знаем, умеем, практикуем!

Check Point
SOFTWARE TECHNOLOGIES LTD

СПАСИБО!

Check Point

Денисов Валерий | Инженер, Check Point
vdenisov@checkpoint.com
t.me/chkpstar