



Check Point
SOFTWARE TECHNOLOGIES LTD

КАК ПРЕВЕНТИВНАЯ БЕЗОПАСНОСТЬ УПРОЩАЕТ ЖИЗНЬ SOC

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

WELCOME TO THE FUTURE OF
CYBER SECURITY

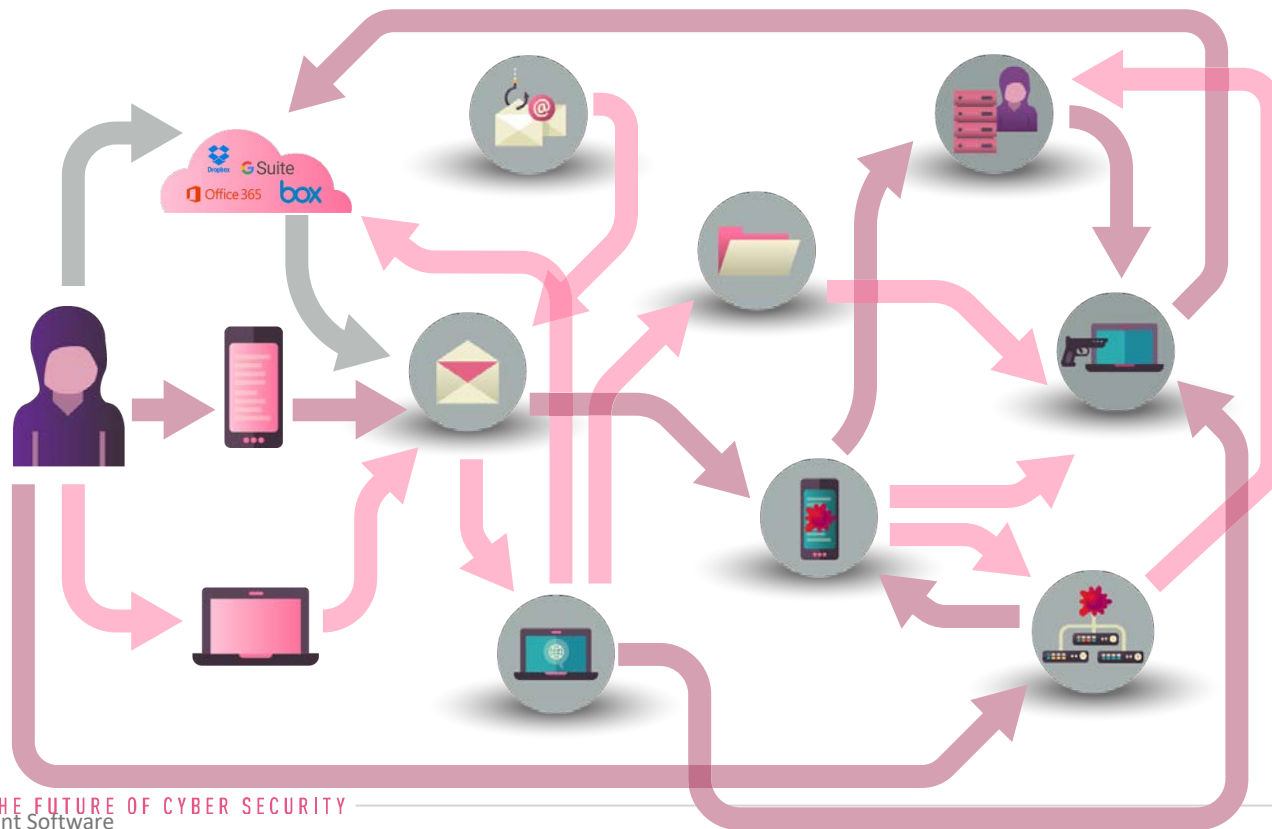
POWERED BY  CHECK POINT
INFINITY

CLOUD • MOBILE • THREAT PREVENTION



Множество сервисов и устройств

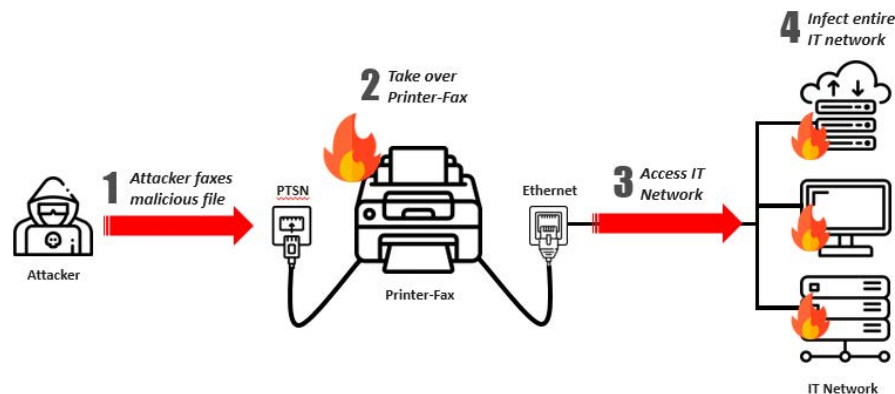
Множество векторов и комбинаций для атаки



Новый неожиданный вектор атак



Check Point
SOFTWARE TECHNOLOGIES LTD



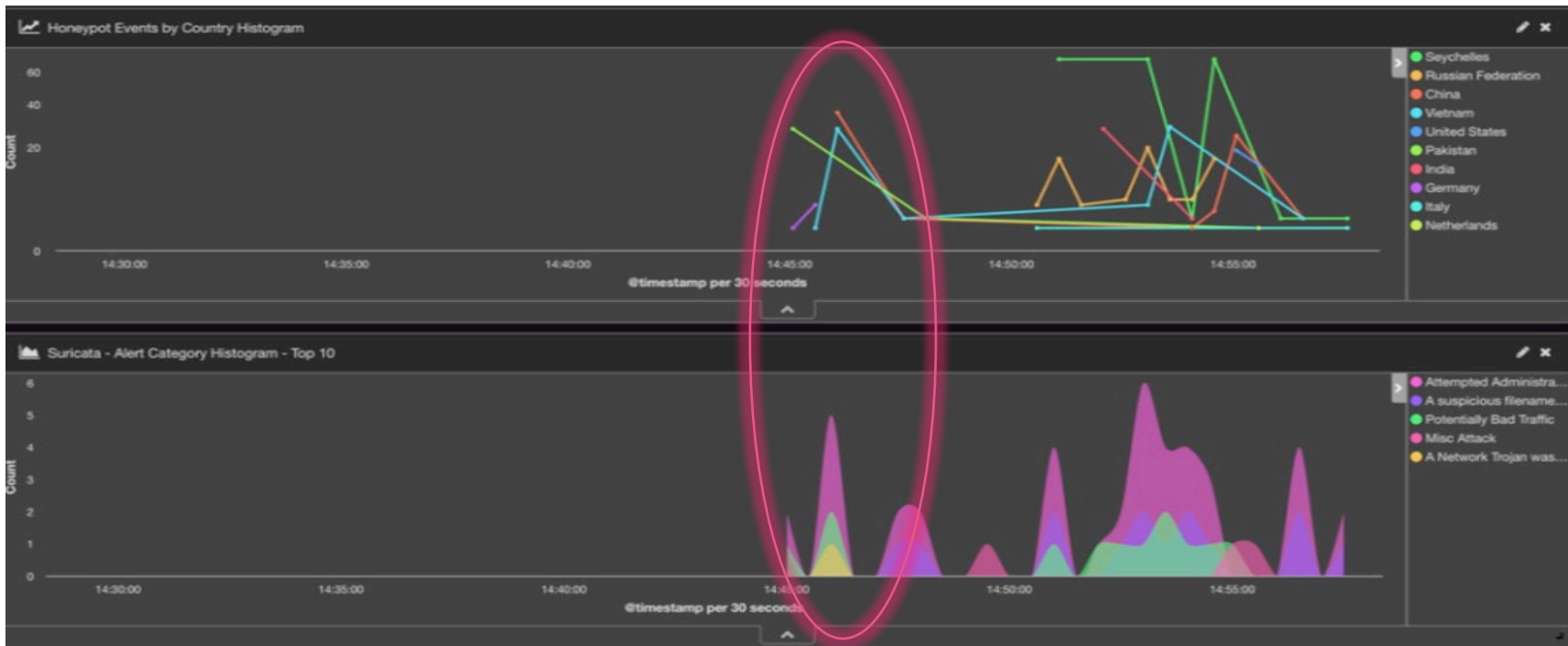
Еще больше причин для внутренней сегментации
и защиты конечных станций

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

Уязвимые сервисы взламывают за минуты

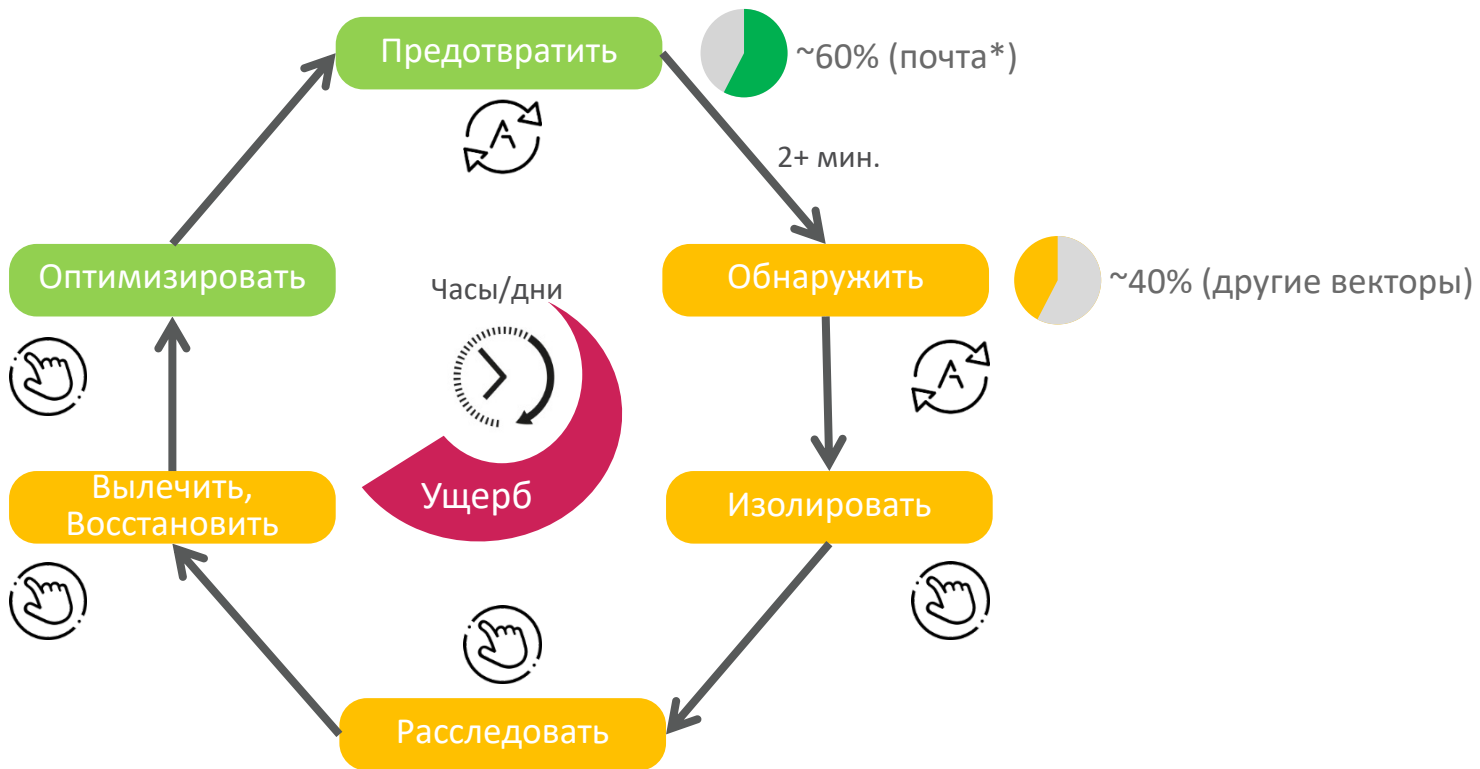


Check Point
SOFTWARE TECHNOLOGIES LTD





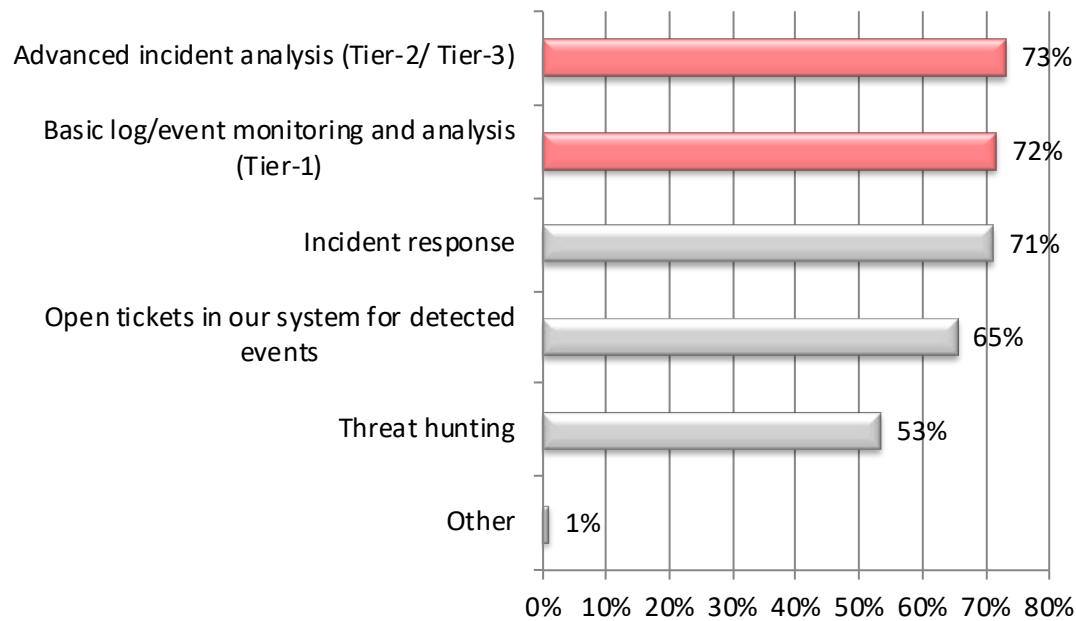
Классический подход к защите от новых угроз



У SOC множество задач



Компанией Dimensional Research был проведен опрос ИТ специалистов о задачах SOC



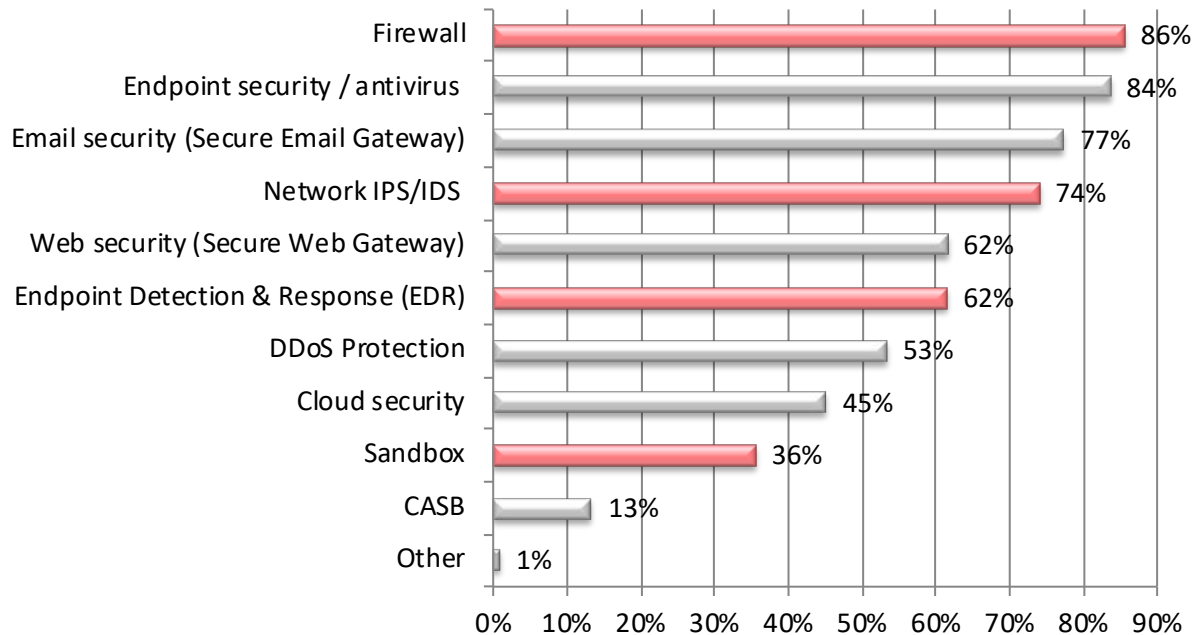
По данным Dimensional research, 2019

В SOC стекаются данные от целой плеяды средств ИБ



Check Point
SOFTWARE TECHNOLOGIES LTD

Какие средства ИБ генерируют события для SOC?



Большинство SOC борются с огромными объёмами событий и инцидентов

Какие основные трудности в работе SOC?



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

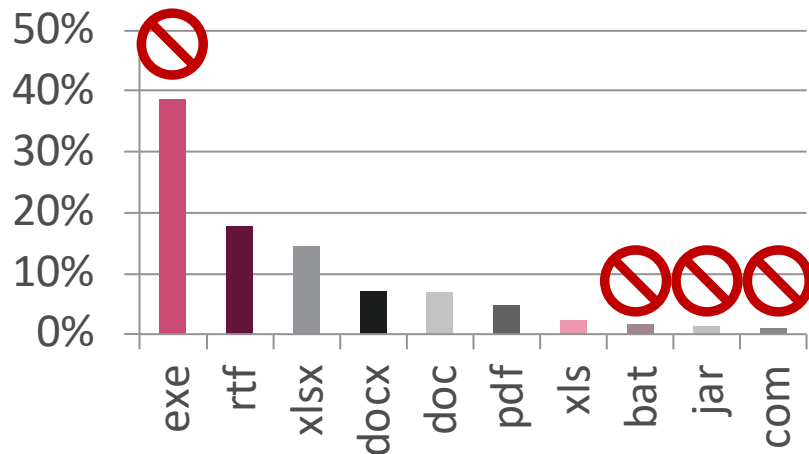
Мгновенная реакция на возникающие угрозы и атаки, включая 0-day



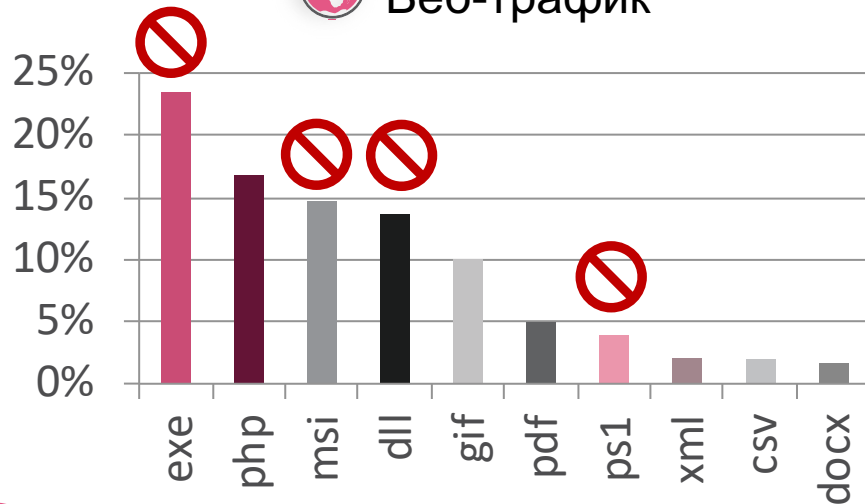
Форматы и векторы доставки вредоносных файлов в СНГ (3 мес.)



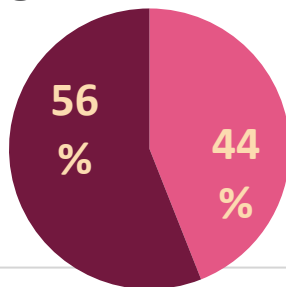
Электронная почта



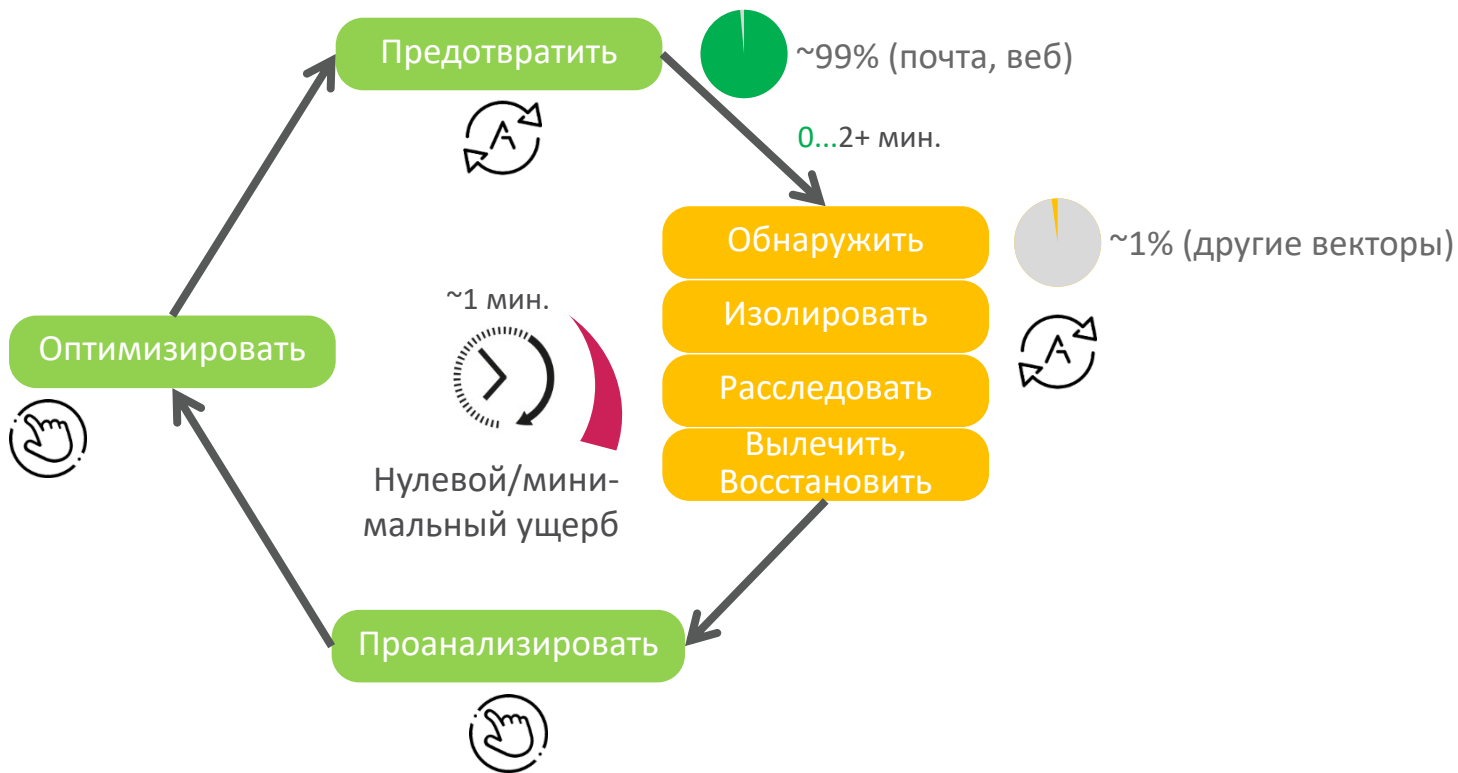
Веб-трафик

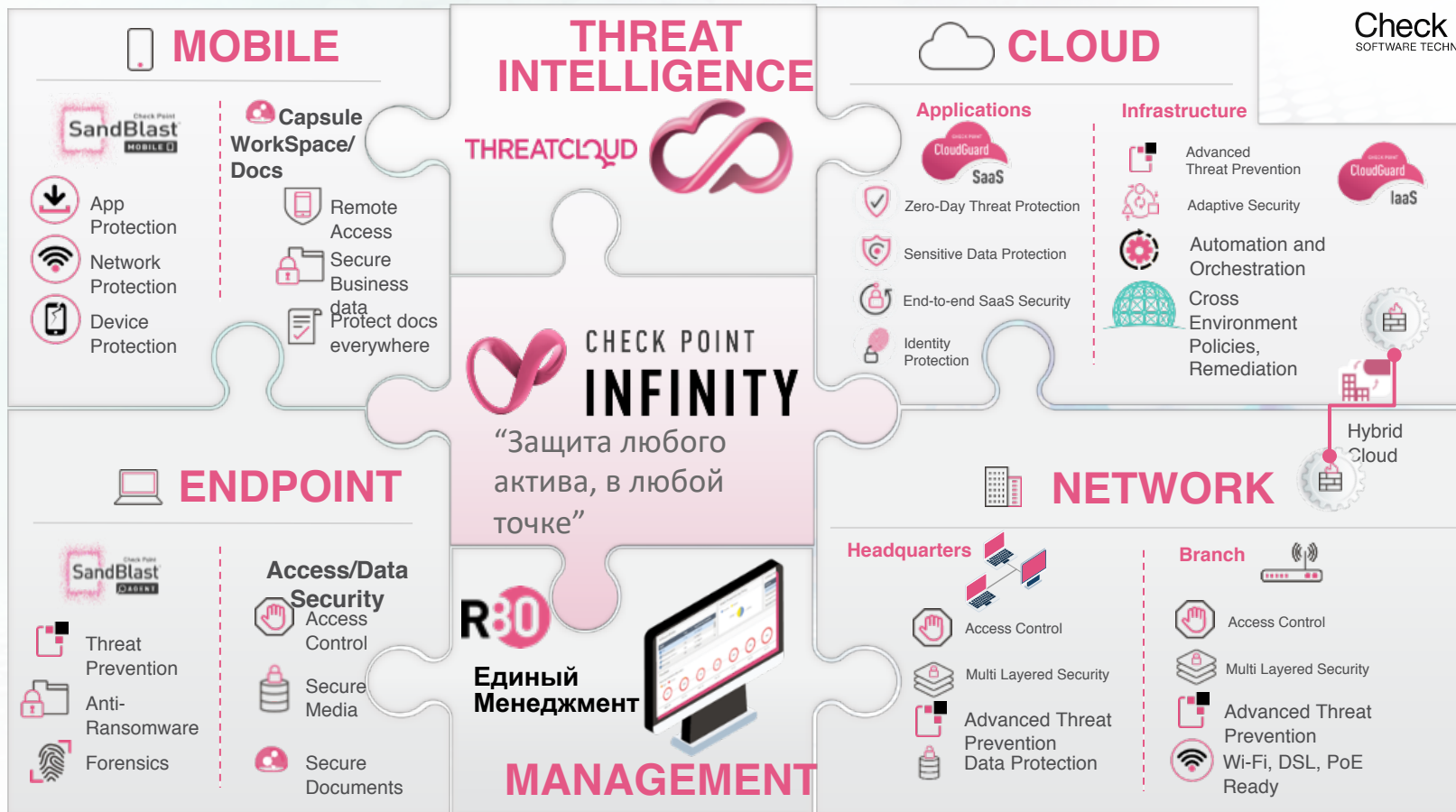


Блокируем лишнее:
Уменьшаем количество инцидентов



Подход Check Point к защите от новых угроз







THREATCLOUD



Внешние Фиды

- CERTs
- ИБ вендора



INFINITY

- Защита Мобильных устройств
- Агенты на ПК
- Ophishing
- Песочницы



Исследования

- Поиск компаний
- Анализ вредоносных



ML & AI

- DGA lab
- Toctopus
- Miners



Заказчики

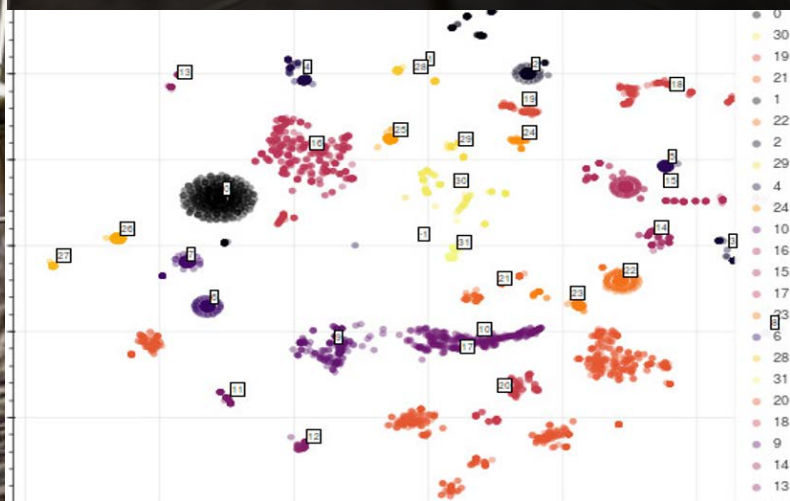
- Пилоты
- Расследование инцидентов
- Анализ событий



ПОИСК КАМПАНИЙ

ПРЕДСКАЗАНИЕ THREAT INTELLIGENCE

Кластеры семейств вредоносов



Определить “ДНК” семейства вредоносов

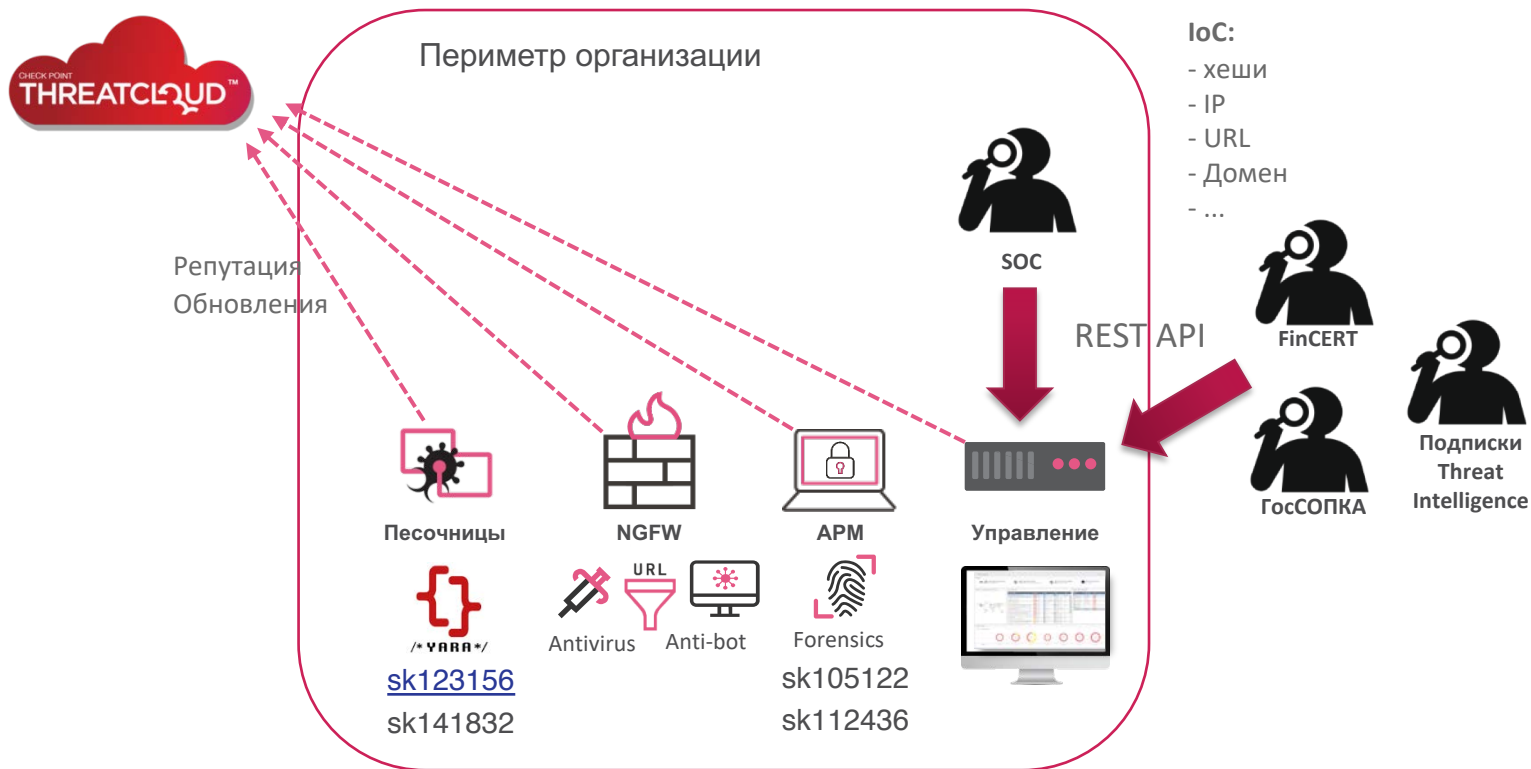
Автоматически классифицировать новые образцы

Обнаружить новые адреса и домены C&C

Пополнить базу Threat Intelligence для предотвращения кампаний




Импорт сторонних индикторов компрометации






Семейство продуктов




Шлюз на периметре,
эл. почта, ЦОД

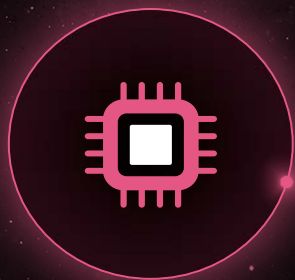

Агенты на ПК и серверах

New: CloudGuard SaaS
 Office 365  G Suite
 Dropbox  salesforce  box
servicenow

Интеграция с веб-порталами, CRM, СЭД

SANDBLAST THREAT EMULATION

Единственная песочница, защищенная от обхода



CPU-LEVEL



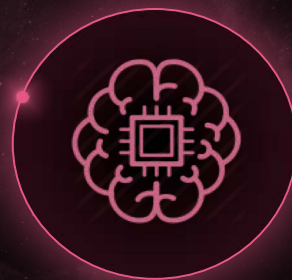
MACRO ANALYSIS & OVERRIDE



TRAPS & DECOYS



FLASH PUSH-FORWARD



MACHINE LEARNING

Human Interaction Simulator

UAC Monitor

SMEP Detector

Static Analyzer

DeepScan

Evasion Detection

FP Guard

Virtual Network Service

Icon Similarity

Link Scanner

Network Activity Monitor

Image Sanitation

DGA Generator

Dropped File Emulation

Shellcode Detector

Выявление «ДНК» новых вредонососов

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registers and in the browser settings in order to install more executable files.

Read more on Check Point ThreatGrid Intelligence

Similarity Analysis

- Similar code blocks
- Similar behavioral IOCs

Pioneer

Threat Details Report

flash_update

SIZE: 3.44 MB | TYPE: EXE | HASH: ...

Verdict: Malicious | Action: Prevent | Confidence: High | Severity: Critical | Classification: Trojan

ATTACK VECTOR | 19/12/2018 15:35

127.0.0.1 → flash_update → 127.0.0.1

```
1 {
2   "status": "success",
3   "info": {
4     "score": 21.6
5   },
6   "te_response": {
7     "status": "Ready",
8     "function": "CuckooModelPack.models.CuckooModel",
9     "confidence": "HighConfidence",
10    "statistics": {
11      "function_run_time_in_millisecond": 1
12    },
13    "perf_info": {
14      "phase": {
15        "RunSignatures": 11.118872880935669,
16        "load_signatures": 10.352633953094483,
17        "copy_and_update_analysis_dict": 9.460339069366455,
18        "signatures - on_complete": 0.9869539737701416,
19        "run_parse": 13.929502964019776,
20        "build_te_response": 9.855849027633667,
21        "BehaviorAnalysis": 2.7945871353149416,
22        "signatures - behavior processes": 10.125440835952759
23      },
24      "top_signatures": {
25        "BH_Get_Set_Thread_Context": 5.335657596588135,
26        "BH_Query_Information_On_Itself": 0.2231769561767578,
27        "bootkit": 0.08323144912719727,
28        "infostealer_ftp": 0.04895210266113281,
29        "injection_ntsetcontextthread": 0.04504585266113281,
30        "BH>Loading_Low_Level_API": 0.03670644760131836,
31        "Infostealers.Win.Generic.A": 0.12068533897399903,
32        "BH_Dynamically_Load_Function_From_Dll": 0.26926517486572268,
33        "antiv_detectreg": 0.0815737247467041,
34        "Injector.Win.RunPE.C": 0.03914022445678711
35      }
36    }
37  },
38  "model_data": {
39    "model_version": "0013b_reduced",
40    "score": 0.8478843523011203,
41    "feature_vector": [
42      2,
```

Code Block 1 of 3

Code Block ID	Verdict	Size	Context
1	Malicious	65.98 KB	dropped
2	Malicious	517.42 KB	dropped
3	Malicious	118.85 KB	dropped
4	Malicious	381.88 KB	dropped
5	Malicious	371.04 KB	dropped
6	Malicious	103.98 KB	dropped
7	Malicious	310.88 KB	dropped
8	Malicious	367.45 KB	dropped

Behavioral IOCs

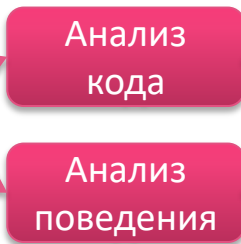
IOCI	Verdict	Size	Context
1	Malicious	65.98 KB	dropped
2	Malicious	517.42 KB	dropped
3	Malicious	118.85 KB	dropped
4	Malicious	381.88 KB	dropped
5	Malicious	371.04 KB	dropped
6	Malicious	103.98 KB	dropped
7	Malicious	310.88 KB	dropped
8	Malicious	367.45 KB	dropped

Классификация с помощью обучения

Неизвестны

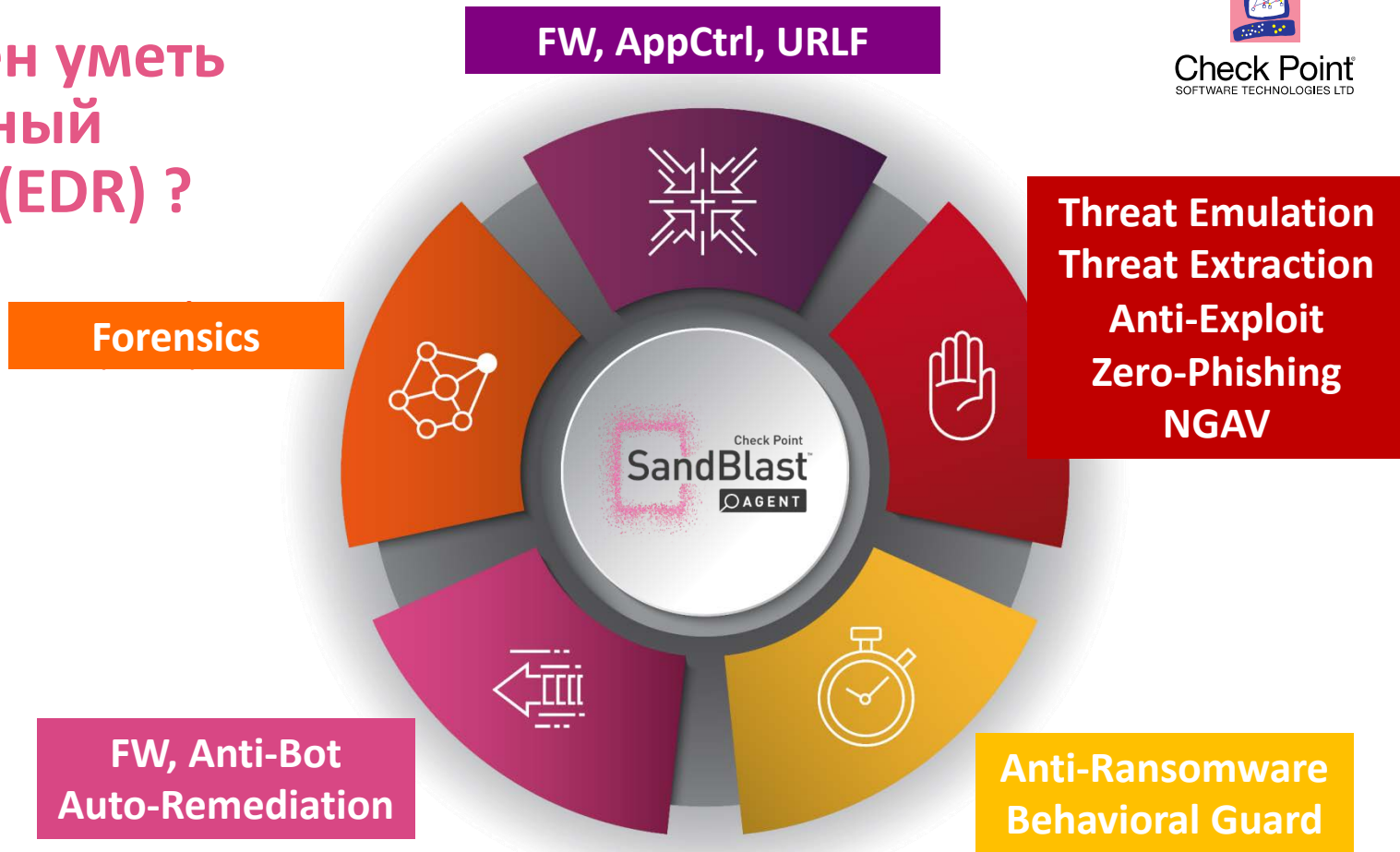


flash_update.exe

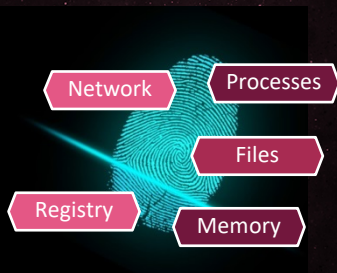


Поиск п

Что должен уметь современный endpoint (EDR) ?



Перехват угроз в реальном времени на конечной станции



Все время



В момент обнаружения



После инцидента



ANTI-RANSOMWARE



ANTI-EXPLOIT



ANTI-BOT



BEHAVIORAL GUARD

МОНИТОРИНГ И ЛОГИРОВАНИЕ АКТИВНОСТИ ПРОЦЕССОВ

Шифровальщики

Аномалии в
памяти

Трафик к C&C

Модели
поведения

Резервирование

Измененные файлы

АНАЛИЗ, КАРАНТИН, ВОССТАНОВЛЕНИЕ

Все элементы атаки на основе данных форенстики

Восстановление

Зашифрованные файлы

Остановка

Взломанный
процесс

Блокировка

Обратные каналы

Классификация

Семейство вред.

Изоляция

Процессы или станция целиком

Автоматизированное расследование инцидента

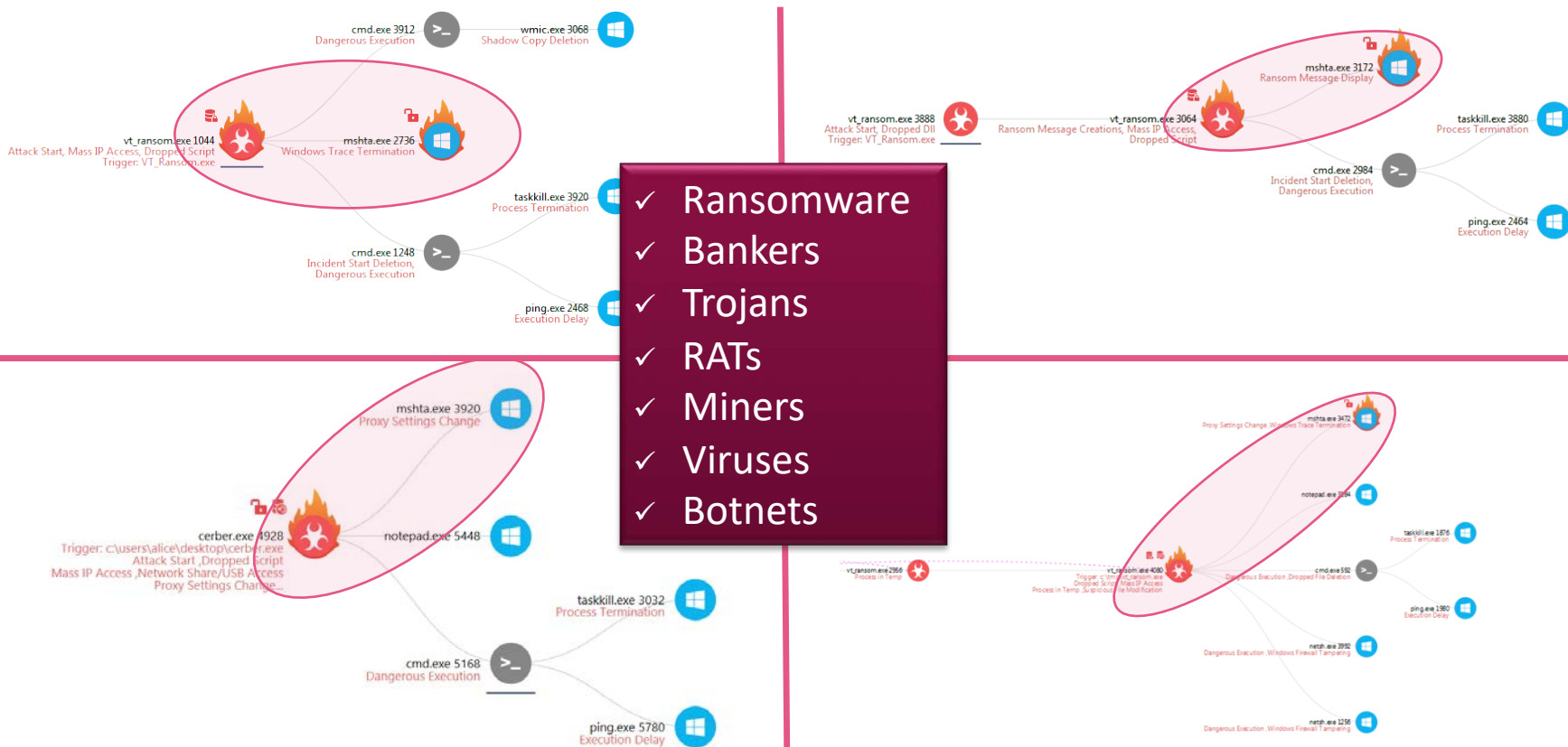
С помощью скоррелированных логов и детального отчета форенстики



Подключаем ИИ к поведенческому анализу



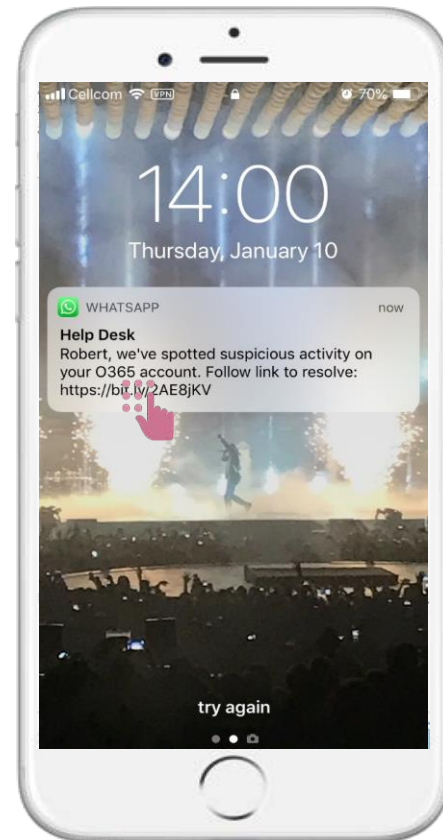
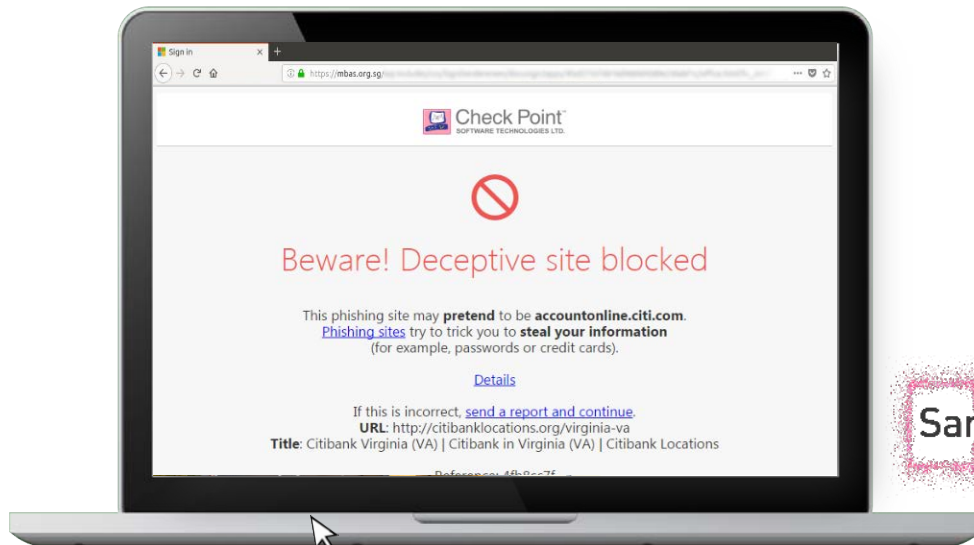
Behavioral Guard блокирует атаки по поведению



Защита от 0-day фишинговых сайтов непосредственно в браузере



Check Point
SOFTWARE TECHNOLOGIES LTD



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



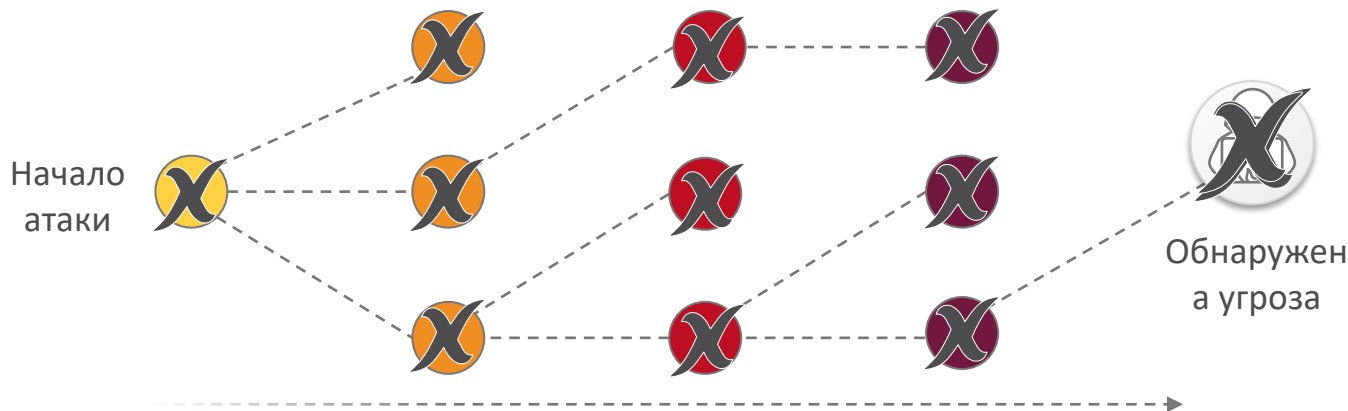
Автоматическое лечение и восстановление

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



Check Point
SOFTWARE TECHNOLOGIES LTD

SandBlast Forensics | OVERVIEW | GENERAL | ENTRY POINT | REMEDIATION | BUSINESS IMPACT | SUSPICIOUS ACTIVITY | INCIDENT DETAILS

Какой статус угрозы?

CLEANED status | Rapid malware family | CRITICAL severity | Endpoint Behavioral Guard triggered by | ...temp\added\space\to_test\the ellipsis behavior\gamepa.exe trigger | ps.win.encoded protection name | pashap user

Элементы атаки

ATTACK STATS | What sort of connections and processes were involved?

- 1 Malicious Connections
- 1 Malicious Processes
- 1 Unsigned Processes
- 1 Script Processes

BUSINESS IMPACT | What was the potential damage done?

38 Data Ransom

Классификация

ATTACK TYPES | What were the attacks types seen or prevented?

- infostealer
- miner
- riskware

ENTRY POINT | How did it enter the system?

powershell.exe launched through WMI

Точка входа?

REMIEDIATION | Were all incident created elements removed?

100% 21/21 terminated processes

9% 3435/36253 quarantined/deleted files

Все вылечено?

INCIDENT DETAILS | How do I analyze further?

Полное дерево атаки

SUSPICIOUS ACTIVITY (12 categories) | What happened in the system?

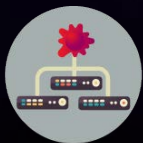
SEVERITY	EVENT CATEGORY
●●●●●	Abnormal Behavior (1 event)
●●●●●	Malicious URL (1 event)
●●●●●	Volume Shadow Copy Deletion (1 event)
●●●●●	BITCoin Wallet Access (1 event)
●●●●●	Ransom Message Creation (393 events)
●●●●●	Script Execution (1 event)
●●●●●	Process in Temp (1 event)
5 more...	

Насколько атака реальна?

HELP? INCIDENT RESPONSE TEAM CHECK POINT Contact Us

Комплексная защита от новых кибер-атак и сокращение издержек SoC

Check Point
SandBlast™

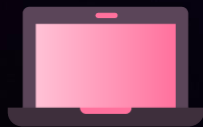


Сеть



Check Point
SandBlast™

AGENT



ПК, Mac



Check Point
SandBlast™

MOBILE



Android, iOS

IDC
Analyze the Future

MTM Leader

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



WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  **CHECK POINT
INFINITY**

CLOUD • MOBILE • THREAT PREVENTION