10 YEARS JETSECURITY CONFERENCE 2019

Если Вас взломали, то что делать до, во время и после инцидента?

Денис Батранков
консультант по информационной безопасности, CISSP, PCNSE
Palo Alto Networks, Москва, Россия и СНГ
denis@paloaltonetworks.com
twitter: @batrankov

Хакеры продолжают проникать в сети компаний и скрыто вести активность.

Об угрозах не знают из-за неэффективности средств мониторинга безопасности и корреляции событий безопасности.

Основные каналы заражения для компании:

- Зашифрованные каналы:

  нельзя расшифровать SSL Pinning, мессенджеры, TOR, IPSEC, туннели

- USB flash drive

  продукты для контроля USB не помогают

Взлом производится стандартными утилитами

РАЗРОЗНЕННЫЕ УТИЛИТЫ ТОЛЬКО ЗАМЕДЛЯЮТ РАССЛЕДОВАНИЕ & РЕАГИРОВАНИЕ

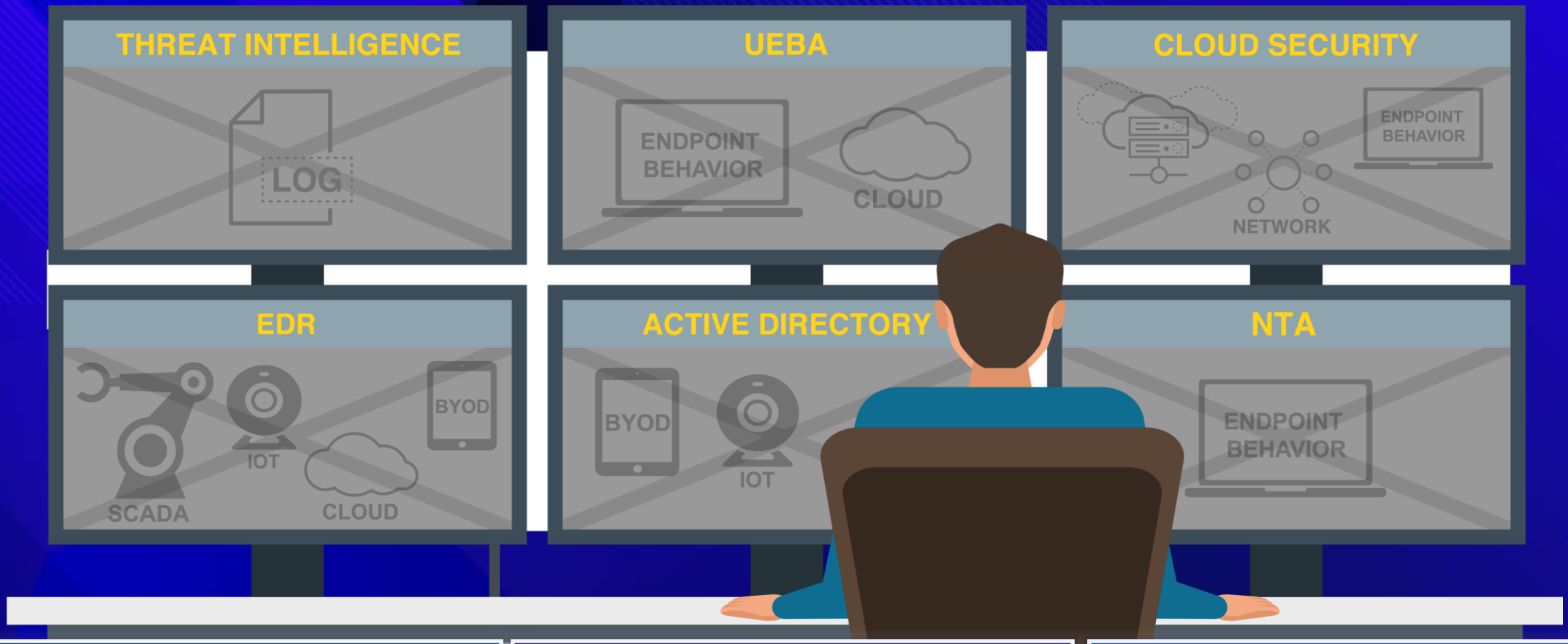
Да, они создают миллионы событий, но не останавливают атаки

РАЗРОЗНЕННЫЕ УТИЛИТЫ ТОЛЬКО ЗАМЕДЛЯЮТ РАССЛЕДОВАНИЕ & РЕАГИРОВАНИЕ

Да, они создают миллионы событий, но не останавливают атаки

Аналитики вручную собирают и коррелируют данные

РАЗРОЗНЕННЫЕ УТИЛИТЫ ТОЛЬКО ЗАМЕДЛЯЮТ РАССЛЕДОВАНИЕ & РЕАГИРОВАНИЕ



Да, они создают миллионы событий, но не останавливают атаки

Аналитики вручную собирают и коррелируют данные

Часто данные собираются постфактум и уже много слепых пятен

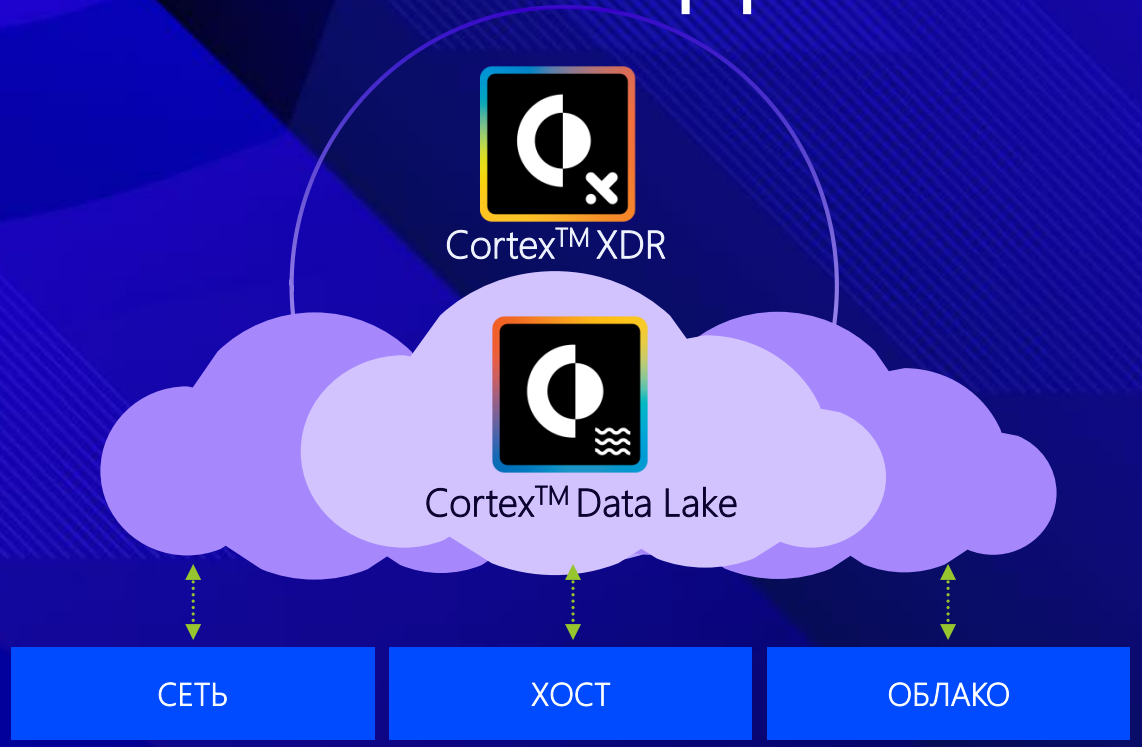
КРИТЕРИЙ ЭФФЕКТИВНОСТИ SOC: EVENT PER ANALYST HOUR (EPAH)

ЧИСЛО СОБЫТИЙ КОТОРЫЕ СОТРУДНИК ОБРАБАТЫВАЕТ В ЧАС

ЗЕЛЕНАЯ ЗОНА » 75-150

XDR – АВТОМАТИЗАЦИЯ ОБНАРУЖЕНИЯ И РАССЛЕДОВАНИЯ

ГДЕ X ЭТО
- СЕТЬ,
- ХОСТЫ,
- ОБЛАКА



Автоматически обнаруживает атаки и показывает их контекст

Ускорение расследований за счет того, что данные сведены вместе сразу

Сразу посылает команды в защитные механизмы для блокирования

РЕЗУЛЬТАТ:
ВИДНА ПРИЧИНА И ПУТЬ ВЗЛОМА В ОДНОМ ОКНЕ

paloalto NETWORKS

ENV21\Sauron

1 Расследование одним кликом

2 Цепочка событий в одном окне

3 Контекст, сигналы BIOC, threat intelligence, как шло во времени

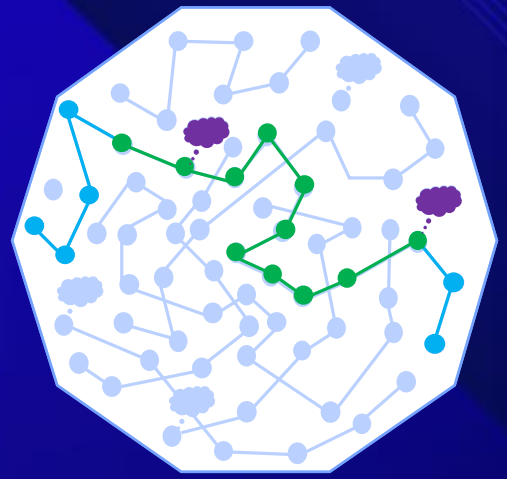
10 YEARS JETSECURITY CONFERENCE 2019

CORTEX XDR™

paloalto NETWORKS®

Обнаружить, расследовать, среагировать & поправить

1 Инцидент



Изоляция

Process creation/termination events

Черный список процессов

Registry & file modification events

Удаленный терминал (командная строка, Python, просмотр процессов, просмотр файлов)

Threat intelligence data

скачивание файлов)

Network session information

Готовые поведенческие IOC

B-IOC rules

NETWORK

GP

ENDPOINT

CLOUD

VM-Series

AP

10 YEARS JETSECURITY CONFERENCE 2019

Хакер должен найти у вас всего одну ошибку чтобы проникнуть в сеть

ХАКЕР ДОЛЖЕН СОВЕРШИТЬ ВСЕГО ОДНУ ОШИБКУ, ЧТОБЫ ВЫ УВИДЕЛИ ЕГО В СЕТИ

Ненормальное поведение обнаруживает CORTEX XDR Analytics!

МЫ СДЕЛАЛИ ДЛЯ ВАС ВСЁ, ЧТОБЫ ПРЕДОСТАВИТЬ ЛУЧШИЕ СЕНСОРЫ ДЛЯ РАЗБОРА ИНЦИДЕНТОВ

paloalto NETWORKS

Сенсорами являются лучшие мировые разработки

Хост: Traps (AEP) + SecDo (EDR) + GlobalProtect(MDM/HIP)
Сеть: NGFW + LightCyber (UEBA/NTA)
Облака (CASB): Aperture + RedLock + Evident
Автоматизация: Сотрудники всю жизнь делают Forensics + Demisto (SOAR)

10 YEARS JETSECURITY CONFERENCE 2019

АНАЛИТИКА НА ОСНОВЕ СОБРАННЫХ ДАННЫХ

Поведенческий анализ и машинное обучение

Данные автоматически связываются друг с другом для разбора причин

Traps предотвращает неизвестные атаки

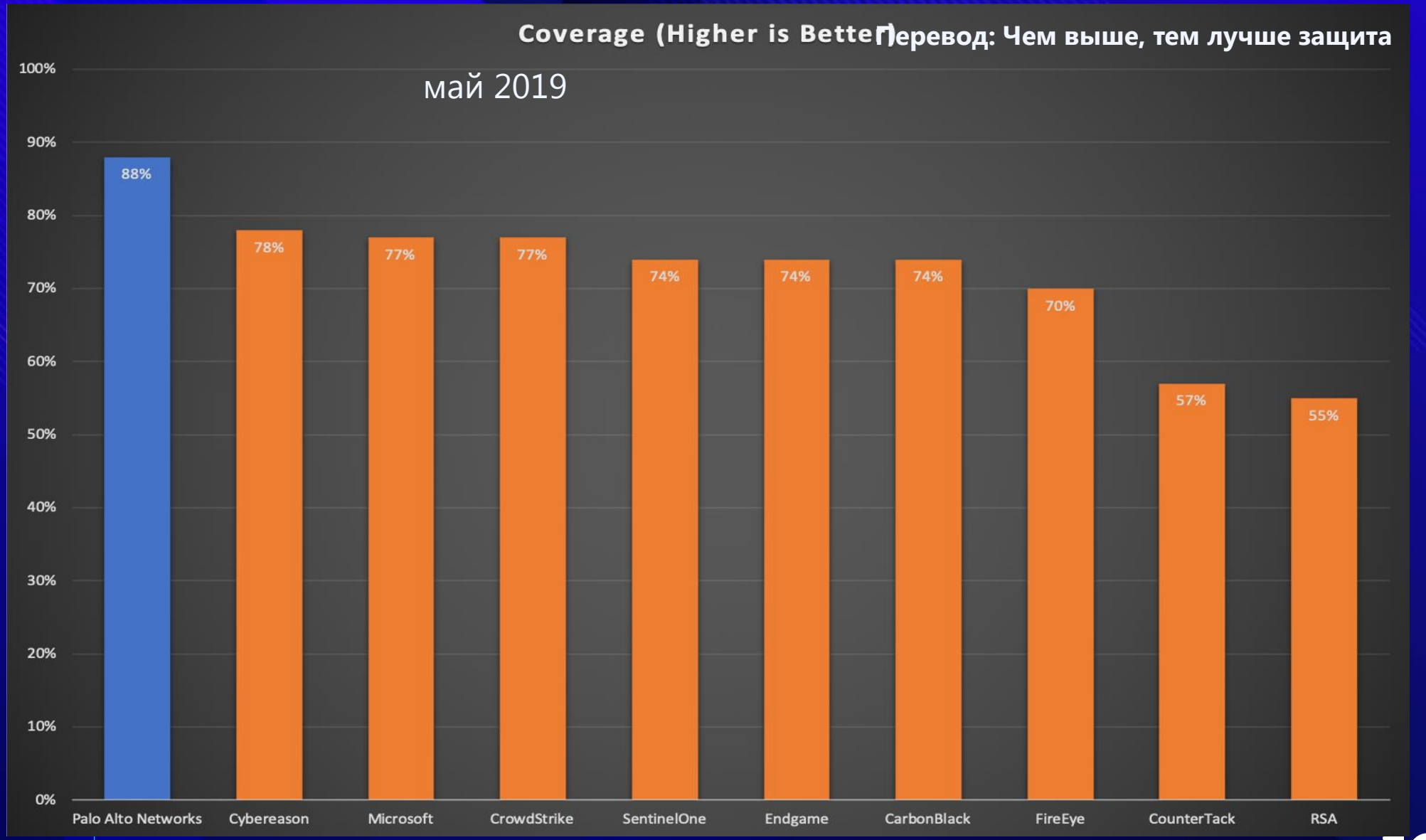
- Без сигнатур
- Без обновлений
- Без знаний об уязвимостях

TRAPS - серьезное препятствие для хакеров

Защита от эксплойта сработала ловушкой техники эксплуатации

Traps блокирует Zer0-Day и неизвестные эксплойты

TRAPS И XDR ЛИДЕРЫ ПО ТЕСТАМ MITRE



L7 FIREWALL КАК СЕНСОР СЕТИ

slideshare-uploading
application function

PowerPoint
file type

slideshare
application

“Конфиденциально”
content

marketing
group

HTTP
protocol

file-sharing
URL category

rivanov
user

SSL
protocol

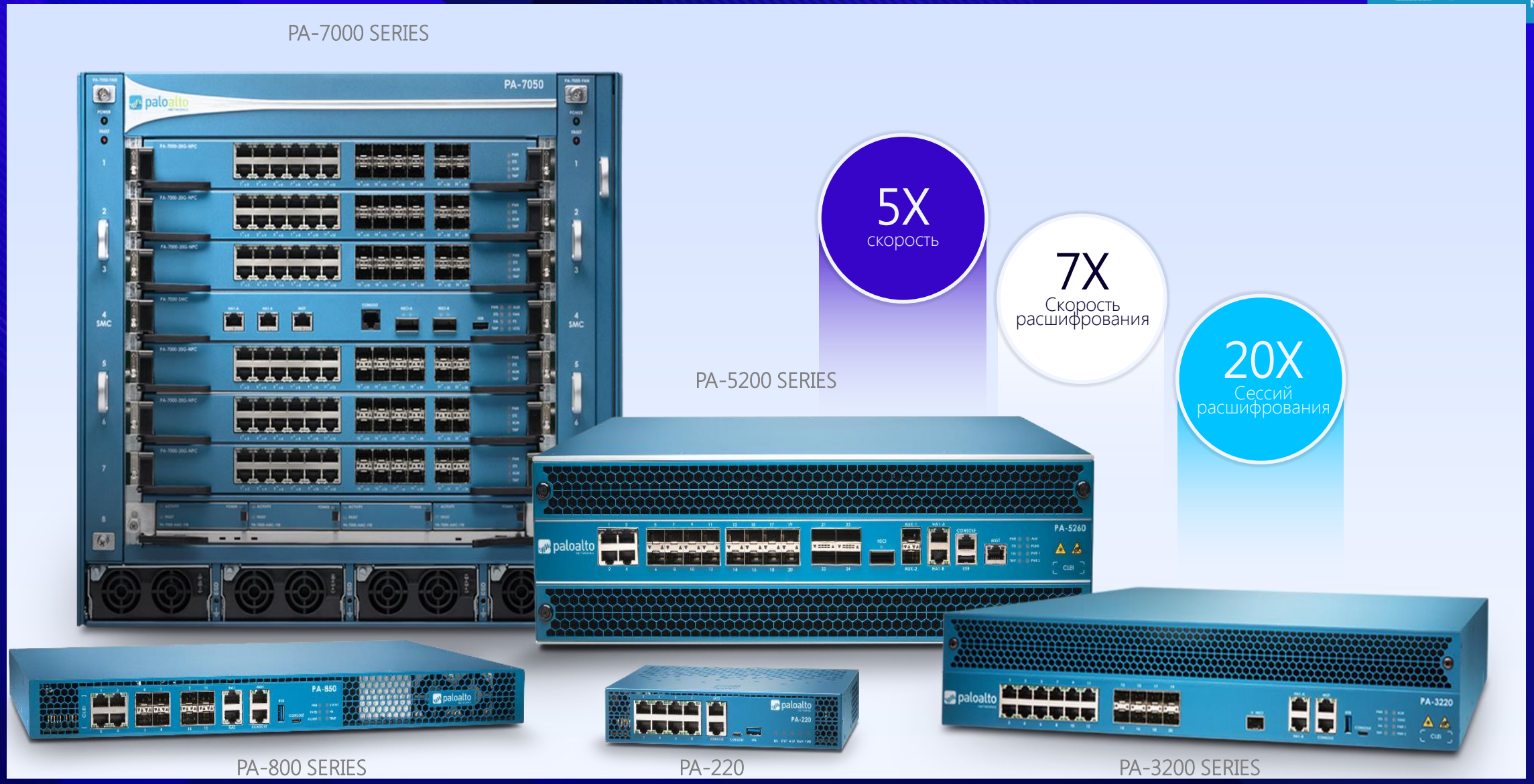
canada
destination country

172.16.1.10
source IP

TCP/443
destination port

64.81.2.23
destination IP

ЗА ВАМИ ПРАВИЛЬНЫЙ ВЫБОР NGFW



CORTEX XDR ОТЛИЧАЕТСЯ ОТ SIEM

- **Больше данных:** Cortex XDR собирает события с сетевых и хостовых сенсоров и облаков и реализует EDR и NTA.
  - SIEM собирает журналы событий; очень редко те же самые события, что собирает EDR или NTA идут в SIEM из-за стоимости масштабирования и ограничения визуализации
- **Автоматически связаны:** Cortex XDR сразу связывает активности в сети, на хосте и в облаке, использует данные ML и ставит целью простое расследование
  - SIEM предлагают корреляцию постфактум на основе запросов по логам
- **Detection, Investigation and Response:** Cortex XDR автоматически обнаруживает атаки, визуализирует причины и ход во времени атаки и предлагает усиление защиты
  - SIEMs ограничен в функциях UEBA. EDR и NTA обычно делает другой вендор, затем эти события должны быть нормализованы и обработаны.

10 YEARS JETSECURITY
CONFERENCE 2019

Подарок от российского офиса Palo Alto Networks: NGFW PA-220

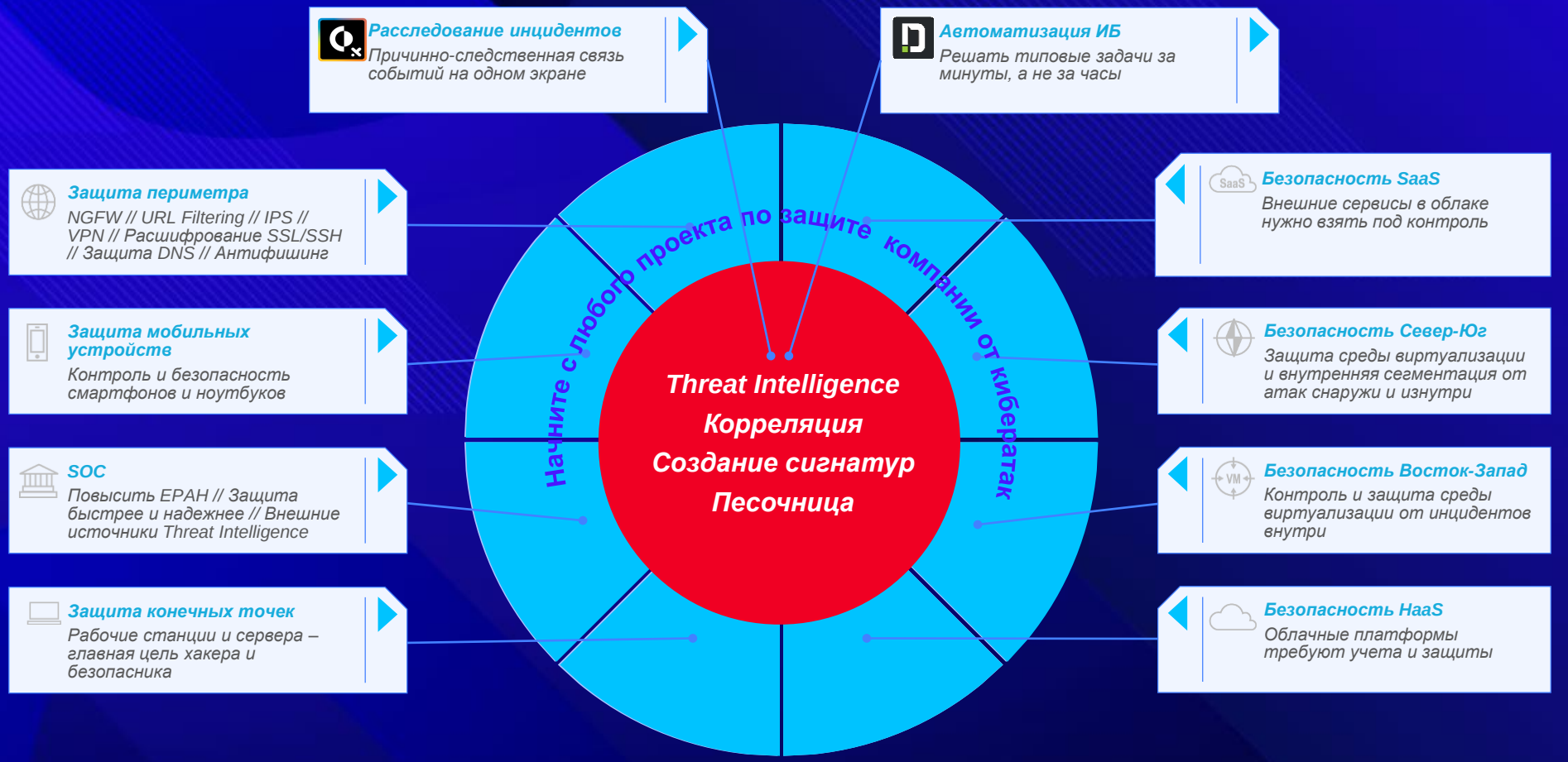
Пропускная способность при работе 100% всего функционала — **150 Мбит**
- Визуализация трафика сотрудников: приложений и файлов в сети
- URL категории, защита от фишинга и защита от сайтов 18+
- Антивирус и **песочница** для SMB, HTTP(S), FTP(S), SMTP(S), POP3(S), IMAP(
- IPS для всех приложений на любых портах
- Защита от атак внутри SSL и SSH
- Встроенный Threat Intelligence: блокировка вредоносных и C&C по IP, DNS
- DNS Sinkholing, DDoS protection
- Оптимизатор политик firewall

Денис Батранков
консультант по информационной безопасности, CISSP, PCNSE
Palo Alto Networks, Москва, Россия и СНГ
mail: denis@paloaltonetworks.com twitter: @batrankov

paloalto NETWORKS®

ГИБКОСТЬ, МАСШТАБИРОВАНИЕ, СООТВЕТСТВИЕ ПРИОРИТЕТАМ КОМПАНИИ

ВАЖНЫЕ ПРОЕКТЫ



ВАЖНЫЕ ПРОЕКТЫ

ВАЖНЫЕ ПРОЕКТЫ

Уже готовые видеоролики

Ответы на вопросы

Тема вебинара	Ссылка для просмотра видеозаписи
Демонстрация блокировки эксплойтов и криптолокера, используя NGFW и TRAPS	https://youtu.be/IoW8uI8-MT0
10 самых частых ошибок при защите сетей	https://youtu.be/0UkdESEgc4E
NGFW и песочницы. Какие вопросы нужно задавать при выборе.	https://youtu.be/XB8VhvF-SO4
Threat Intelligence от аналитиков Palo Alto Networks Unit42. База индикаторов компрометации Autofocus, MineMeld.	https://youtu.be/mhFAoqeKF1w
Aperture - защита облачных SaaS приложений, включая Office 365	https://youtu.be/IYG2j3QADas
Тактика и стратегия защиты сети от современных атак	https://youtu.be/8qfkDf1rg4c
Защита корпоративных и коммерческих ЦОД	https://youtu.be/JuSMcoF9E6k
Обучение настройкам NGFW	https://www.youtube.com/channel/UC6yzUQIrdNzqeCzZ4sWqtEg

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Денис Батранков
консультант по информационной безопасности, CISSP, PCNSE
Palo Alto Networks, Москва, Россия и СНГ
denis@paloaltonetworks.com
twitter: @batrankov