

Cortex XDR

*Передовая платформа
выявления угроз*

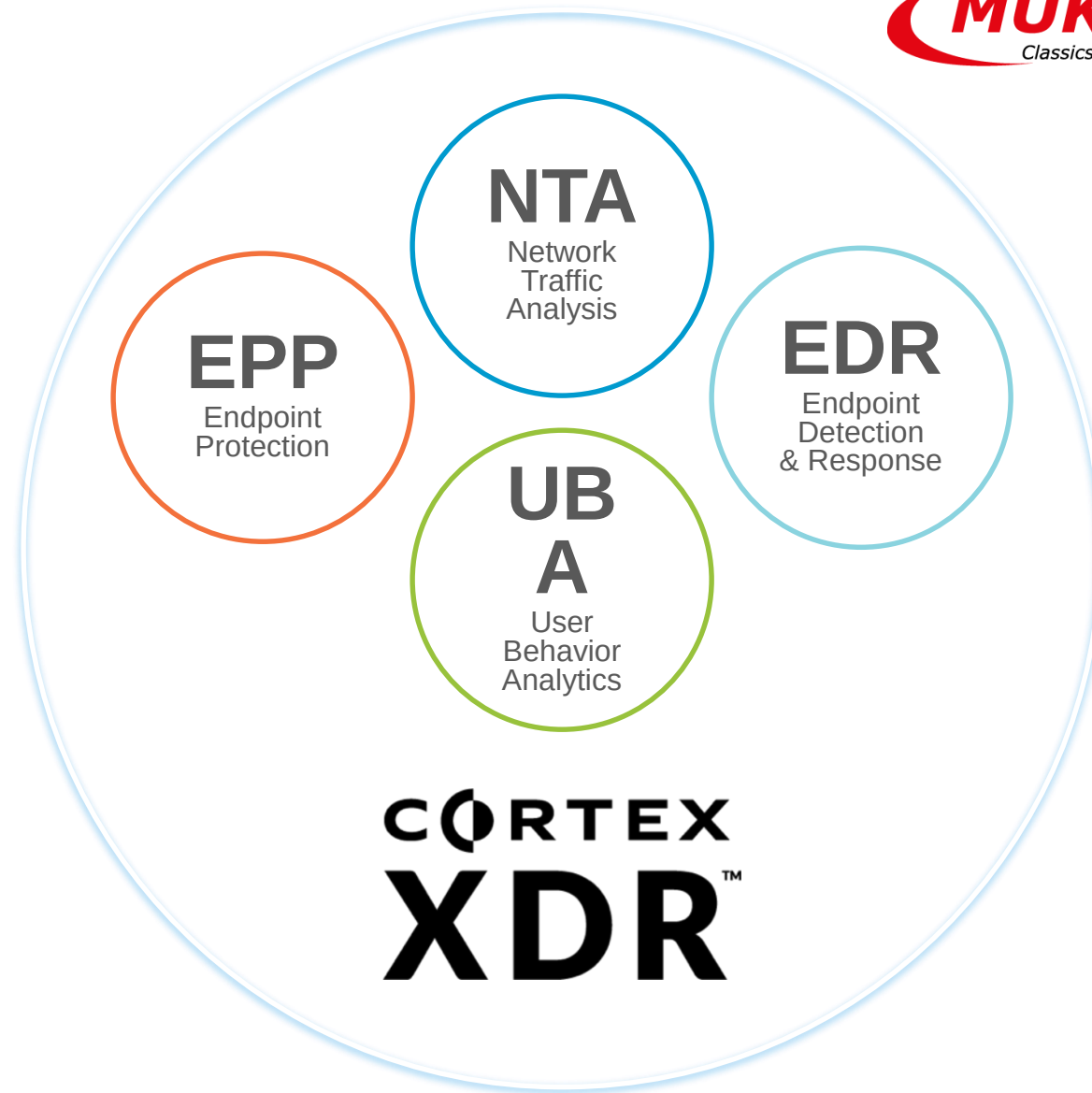
*Манушков Антон
Группа компаний MUK
Инженер Palo Alto Networks
PCNSA
CCNP Enterprise
CCNP Security*



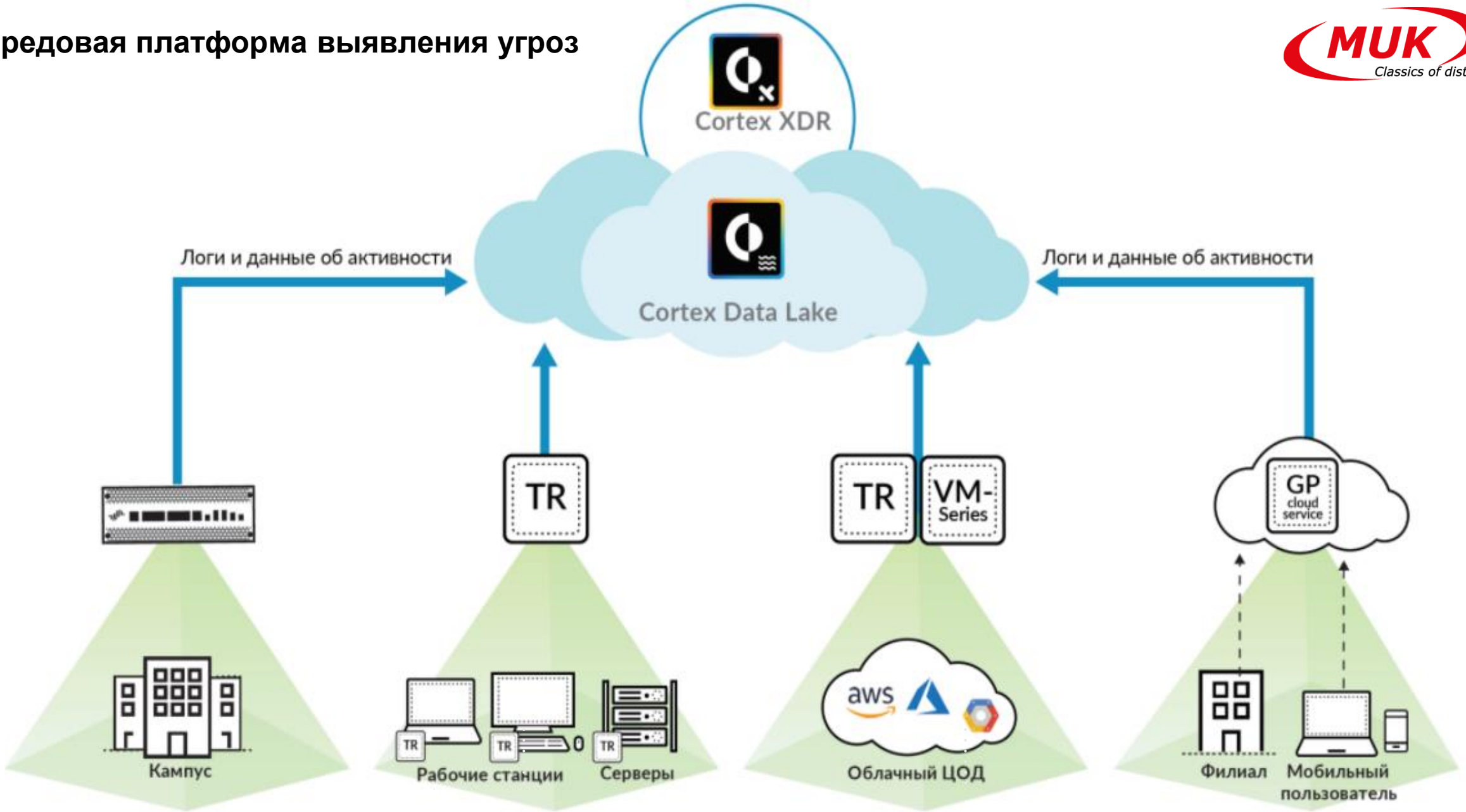
CORTEX™
BY PALO ALTO NETWORKS

- **Cortex Data Lake** – облачное хранилище логов
- **Cortex XDR** – выявление продвинутых атак (EDR, NTA, UEBA)
- **Cortex XSOAR** – оркестрация, автоматизация, реагирование для SOC (XSOAR)
- **Cortex Xpanse** – глубокая аналитика активов

Объединение разрозненных точечных
продуктов



Передовая платформа выявления угроз

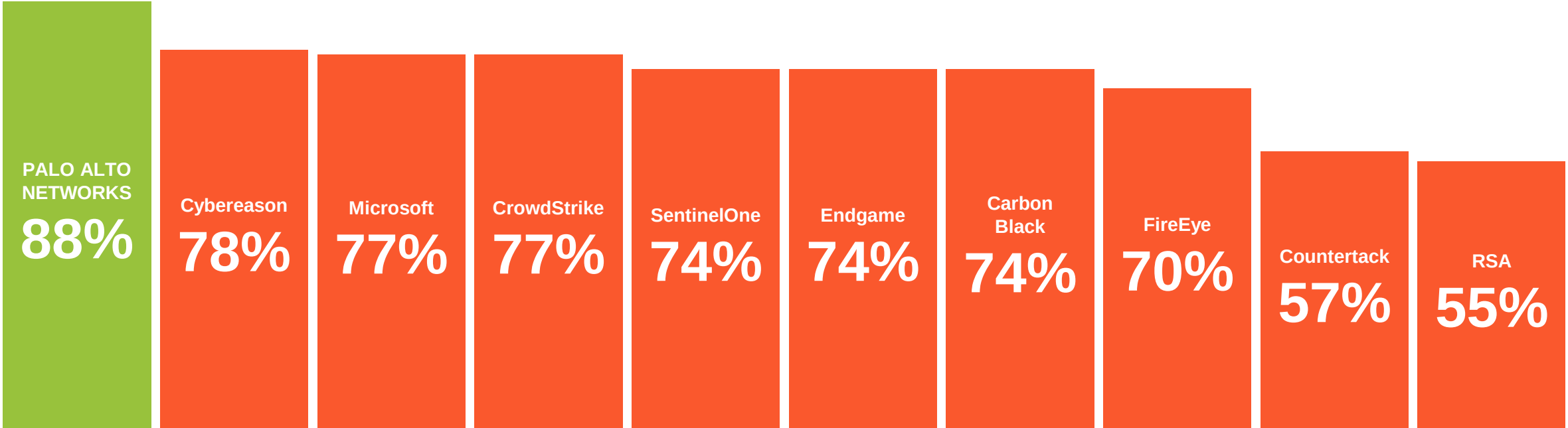


- **Автоматическое обнаружение скрытых атак:** постоянное обнаружение угроз с помощью искусственного интеллекта, поведенческого анализа и настраиваемых пользователем правил и политик детекта
- **Снижение нагрузки на персонал:** мгновенное отсеивание ложных срабатываний, повышение производительности аналитиков
- **Сокращение среднего времени обнаружения угрозы (MTTI):** сочетание точного детектирования атак с быстрой приоритизацией инцидентов существенно сокращает временные затраты
- **Сокращение среднего времени на сдерживание угроз (MTTC):** быстрое обнаружение и безошибочная реакция на внешние атаки и внутренние угрозы доступно даже младшим аналитикам
- **Быстрый возврат инвестиций:** дополнительные возможности на основе экосистемы приложений и использования существующей инфраструктуры (NGFW, хосты) в качестве точек выявления угроз и применения политик ИБ

Cortex XDR обеспечивает лучшее покрытие MITRE ATT&CK в отрасли



Наивысшая оценка
и на 93% меньше
пропусков



Покрывтие техник атак

- Cortex XDR PREVENT – лицензируется по количеству конечных точек + 30 дней логов. Минимум 200 точек;
- Cortex XDR PRO per endpoint – лицензируется по количеству конечных точек + 30 дней логов, обладает расширенным функционалом. Минимум 200 точек;
- Cortex XDR PRO per host – лицензируется по количеству конечных точек + 30 дней логов, ориентирован на защиту облачных платформ. Минимум 50 хостов;
- Cortex XDR PRO per TB – лицензируется по объему хранилища логов. Минимально доступно 5TB.

- Главная страница продукта – <https://www.paloaltonetworks.com/cortex/cortex-xdr>
- Страница лицензирования и функционала – <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/features-by-cortex-xdr-license-type.html#features-by-cortex-xdr-license-type>
- Спецификации XDR - <https://www.paloaltonetworks.com/resources/datasheets/quickstart-service-for-cortex-xdr-pro-per-tb-ds>

Спасибо за внимание