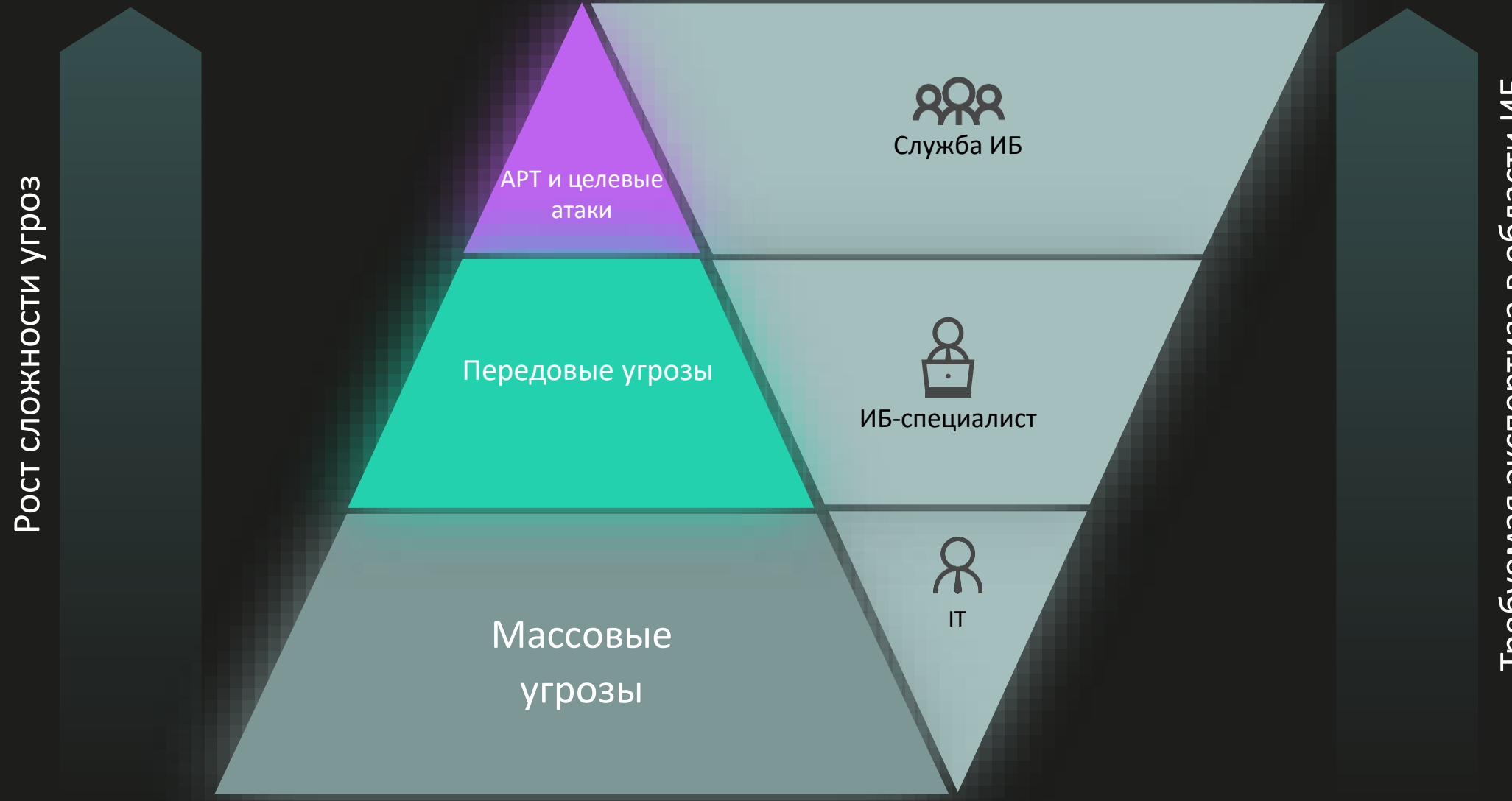
Импортозамещение с Kaspersky

kaspersky 25 лет

Краткий план презентации

1. Трехступенчатый подход ЛК
2. Kaspersky Symphony
3. Импортозамещение продуктами ЛК
4. Ресурсы и сервисы

Взаимосвязь сложности угроз и требуемой экспертизы



Трехуровневый подход «Лаборатории Касперского» к кибербезопасности

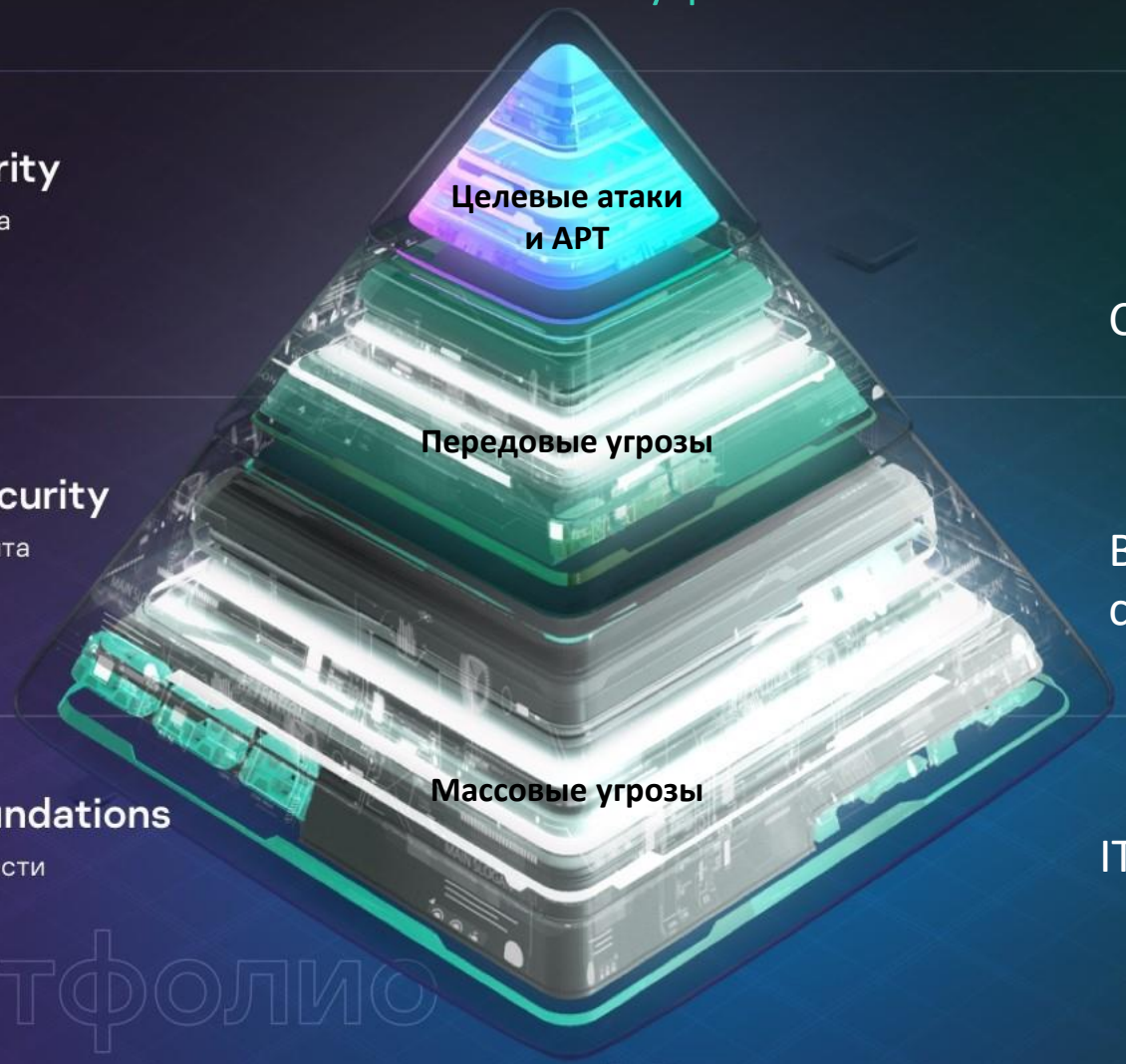
Предложение «Лаборатории Касперского»

Сложность угроз

Kaspersky Expert Security
Экспертная защита

Kaspersky Optimum Security
Оптимальная защита

Kaspersky Security Foundations
Основа безопасности



Служба ИБ

Выделенные сотрудники ИБ

IT-департамент

Зрелость команды ИБ

Портфолио «Лаборатории Касперского»

Kaspersky Security Foundations

- Основа построения безопасности
- Фундамент ИБ для всех компаний
- Использование превентивных технологий (почта, сеть, конечные точки)
- Автоматическая блокировка большого количества угроз
- Чем лучше фундамент, тем эффективнее следующие уровни защиты

Защита от массовых угроз

Kaspersky Optimum Security

Защита от передовых угроз

- Оптимальный уровень защиты для небольших компаний с базовой ИБ-экспертизой (EDR vs MDR vs всё вместе)
- Максимальный уровень автоматизации с возможностью понимания происходящего
- Фокус на самые уязвимые места: рабочие станции и люди
- Выбор технологий: Sandbox, EDR + бесплатный доступ к порталу TI
- Выбор управляемой защиты: MDR или MDR с EDR

Kaspersky Optimum Security

Собственная защита

1

Kaspersky Sandbox

Kaspersky EDR для бизнеса Оптимальный

Kaspersky Threat Intelligence Portal

И/ИЛИ

Управляемая защита

2

Kaspersky Managed Detection and Response Optimum

Фокус на особо уязвимые места

2

1

Усиление защиты рабочих мест

Рабочие станции

Люди

Повышение киберграмотности

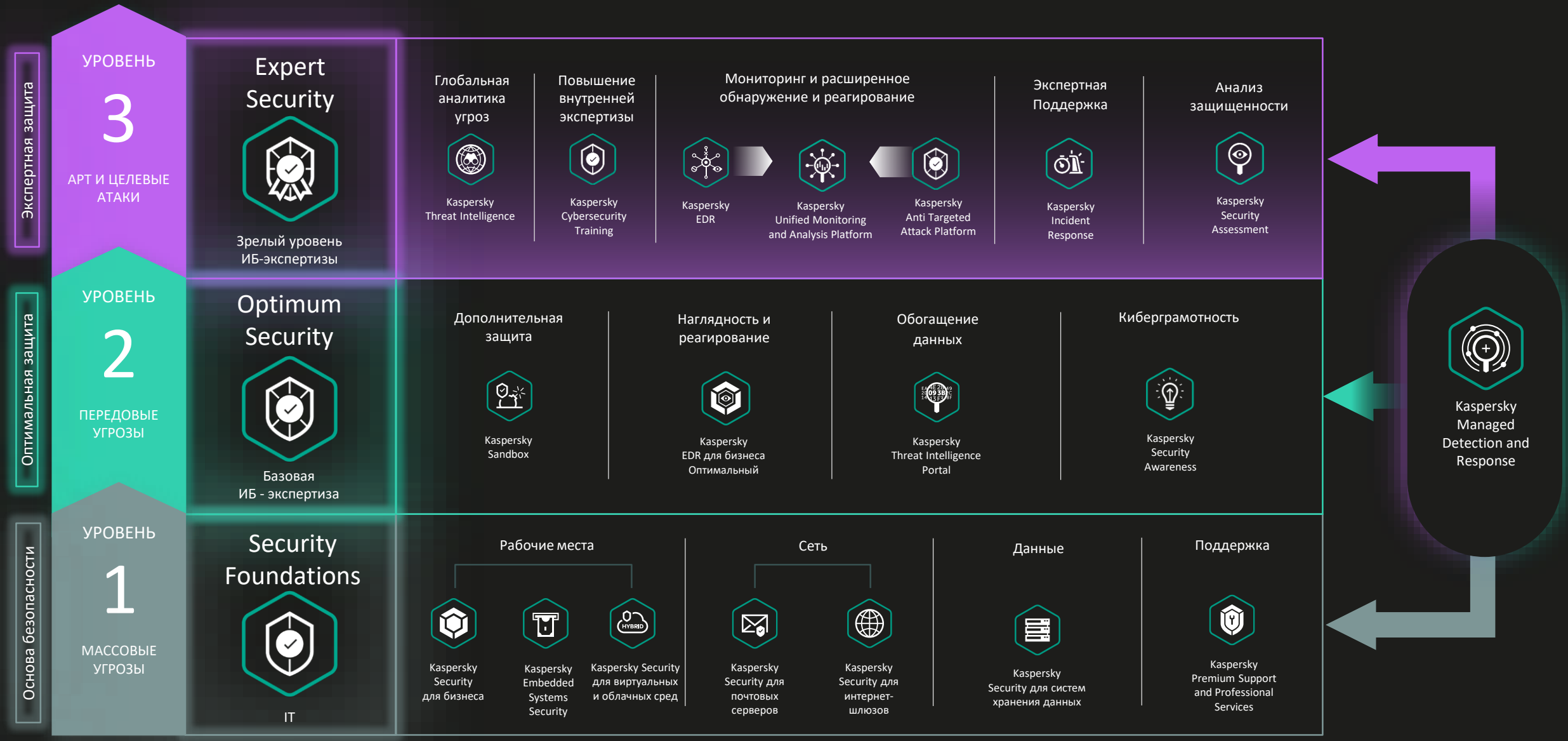
Kaspersky Security Awareness

Kaspersky Expert Security

Защита от APT и целевых атак

- Экспертная защита для средних и крупных организаций со зрелой ИБ-экспертизой
- Фокус на обеспечение всем необходимым ИБ-экспертов для противостояния самым сложным атакам
- Контроль всех популярных точек проникновения злоумышленников в инфраструктуру
- Технологии мирового уровня (EDR, XDR, SIEM), оперативные и достоверные данные об угрозах, передача знаний и всесторонняя сервисная поддержка со стороны «Лаборатории Касперского»
- Помощь в соответствии требованиям регуляторов

Портфолио «Лаборатории Касперского»



Продуктовый состав Kaspersky Symphony XDR

Kaspersky Symphony XDR: Расширенные возможности защиты

- Включена функциональность платформы Threat Intelligence и потоки данных об угрозах
- Включено повышение осведомленности сотрудников
- Включен модуль ГосСОПКА для автоматического взаимодействия с НКЦКИ

Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

Автоматические

- Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочницей в сетевом и почтовом трафике
- Автоматическая блокировка на уровне почтового шлюза неизвестных вредоносных объектов, обнаруженных детектирующими механизмами KATA (до доставки получателю)
- Взаимодействие веб-шлюза и KATA через API для передачи объектов из веб-трафика на проверку в песочницу и последующей их автоматической блокировки в случае выявленной вредоносной нагрузки
- Потоковое обогащение событий в KUMA, предварительно обработанных в CyberTrace
- Передача релевантных сложным атакам событий с KATA, KES, KEDR, KSMG, KWTS в KUMA для корреляции с данными от сторонних источников
- Передача сырой телеметрии с EDR в KUMA
- Реагирование через EDR на найденные угрозы в KUMA
- Автоматическое обогащение карточки инцидента в KUMA информацией об уровне осведомленности атакованного пользователя*

Полуавтоматические

- Доступ в Threat Lookup для получения дополнительного контекста для эффективного расследования
- Построение модели активов в KUMA на основании данных из KSC
- Принудительный запуск обновления баз и антивирусной проверки через KSC с карточки инцидента в KUMA
- Запуск действий по реагированию через EDR с карточки инцидента в KUMA*
- Возможность назначить обучение по повышению киберграмотности из карточки инцидента в KUMA*
- Передача информации о произошедших инцидентах в НКЦКИ, благодаря встроенному в решение модулю ГосСОПКА

*В ближайшем Roadmap

Импортозамещение

SIEM

NGFW

Инфраструктурные решения

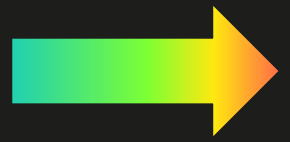
Anti-APT

NTA, EDR, Sandbox (web, email)

и т.д.

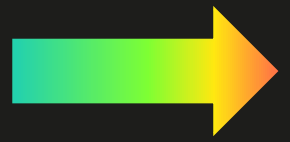
AV/EPP

ESET
TREND MICRO
McAfee
Symantec
Bitdefender



SIEM


IBM
MICRO FOCUS
McAfee
FORTINET
splunk>




Kaspersky
Unified Monitoring
and Analysis Platform

Anti-APT

NTA

Cisco
LogRhythm
riverbed
Plixer
MICRO FOCUS

EDR/XDR

TREND MICRO
FIREEYE
paloalto NETWORKS
eset
Symantec.
FORTINET

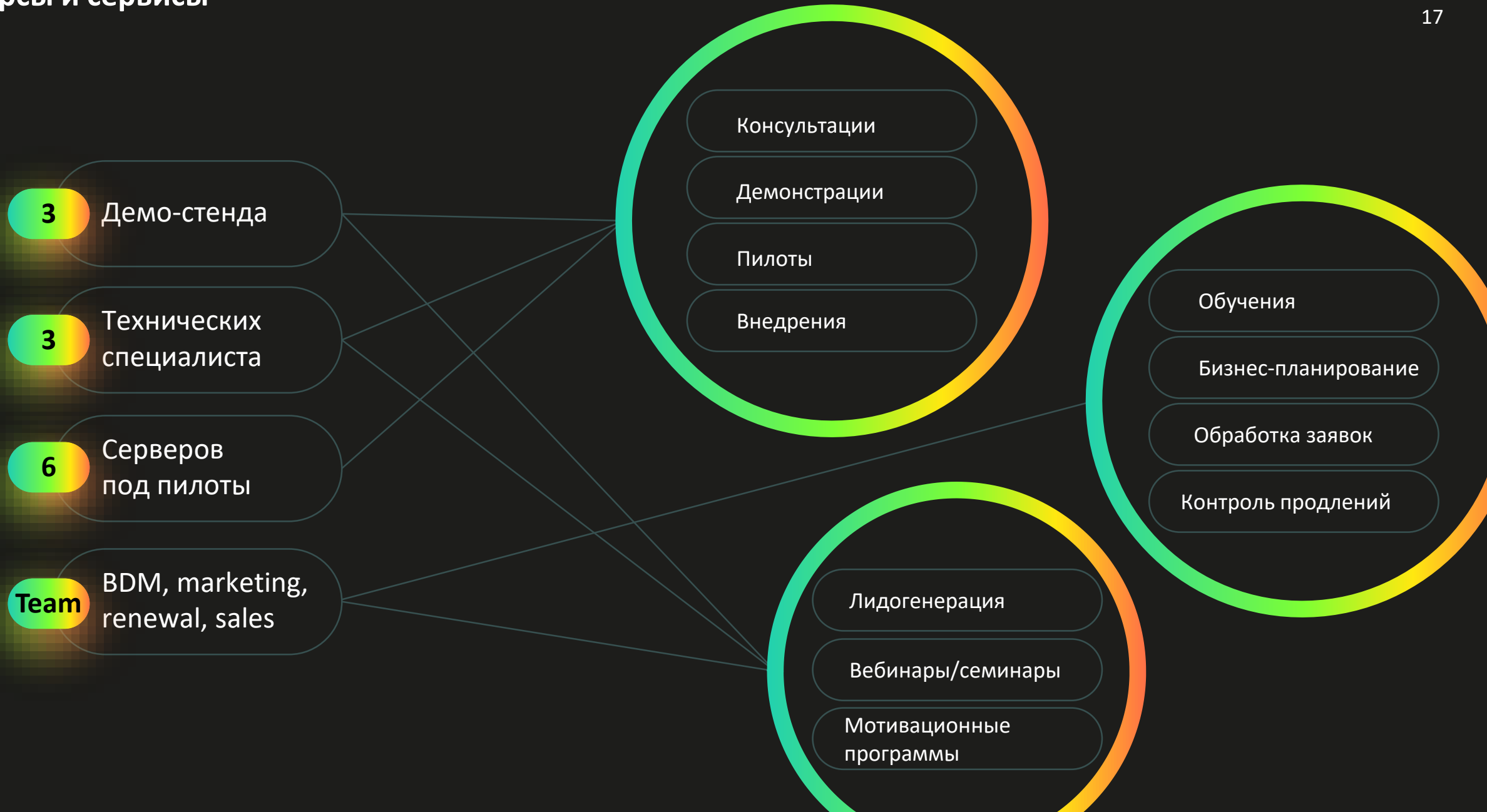
Sandbox

FORTINET
Check Point SOFTWARE TECHNOLOGIES LTD.
paloalto NETWORKS
TREND MICRO
FIREEYE

TI

CROWDSTRIKE
INTSIGHTS
Recorded Future
paloalto NETWORKS
ANOMALI
FIREEYE

Ресурсы и сервисы



Спасибо