ViPNet Network Security Platform (NSP) - угрозоцентрическая архитектура продуктов ViPNet

Алексей Данилов
Руководитель продуктового направления

Риск-ориентированная модель

Все бритвы решают задачу, но какой ценой!

Опасные **Безопасные** **Электрические** **Механические**

Опасная бритва – не порежешься, но нельзя провозить в багаже (холодное оружие)
Безопасная бритва – можно порезаться, но нельзя нанести вред окружающим
Электрическая бритва – проблемы с инфраструктурой, перевозкой в самолете
Механическая бритва – плюсы/минусы неизвестны, так как не продается ☺

Угрозоцентрическая модель

7 главных причин использования опасной бритвы

- Непередаваемые ощущения, как от процесса, так и от результата
- Более чистое и гладкое бритье
- Меньше раздражения на лице
- Больший контроль над процессом
- Филигранная четкость в создании контура бороды
- Экономичность в долгосрочной перспективе
- Забота об окружающей среде

Осталось только выбрать тип лезвия

Модели сетевой безопасности

«Риск-ориентированная модель»:

Риски – это потенциальные последствия, с которыми сталкиваются организации в случае использования уязвимостей, что в итоге приводит к финансовым последствиям (утечка данных, сбои в работе, репутационные потери)

Риск-ориентированный подход фокусируется на более широком ландшафте потенциальных уязвимостей и вероятности их использования, определяя приоритетность мер по их снижению в зависимости от того, какое влияние они могут оказать на деятельность организации

«Угрозоцентрическая модель»:

Ориентированный на угрозы подход нацелен на выявление и защиту от конкретных угроз, адаптируя средства защиты по мере развития угроз

Модели на примере Ransomware

«Риск-ориентированная модель»:

Атака удаленного филиала. Дешевле купить страховку, покрывающую ущерб в случаи атаки, чем содержать парк ИБ-оборудования

«Угрозоцентрическая модель»:

Подход, ориентированный на угрозы, предполагает активный мониторинг и предотвращение или быстрое реагирование на признаки активности Ransomware с помощью защиты конечных точек и управляемых служб обнаружения и реагирования (MDR)

Реальная ситуация – использование всех подходов

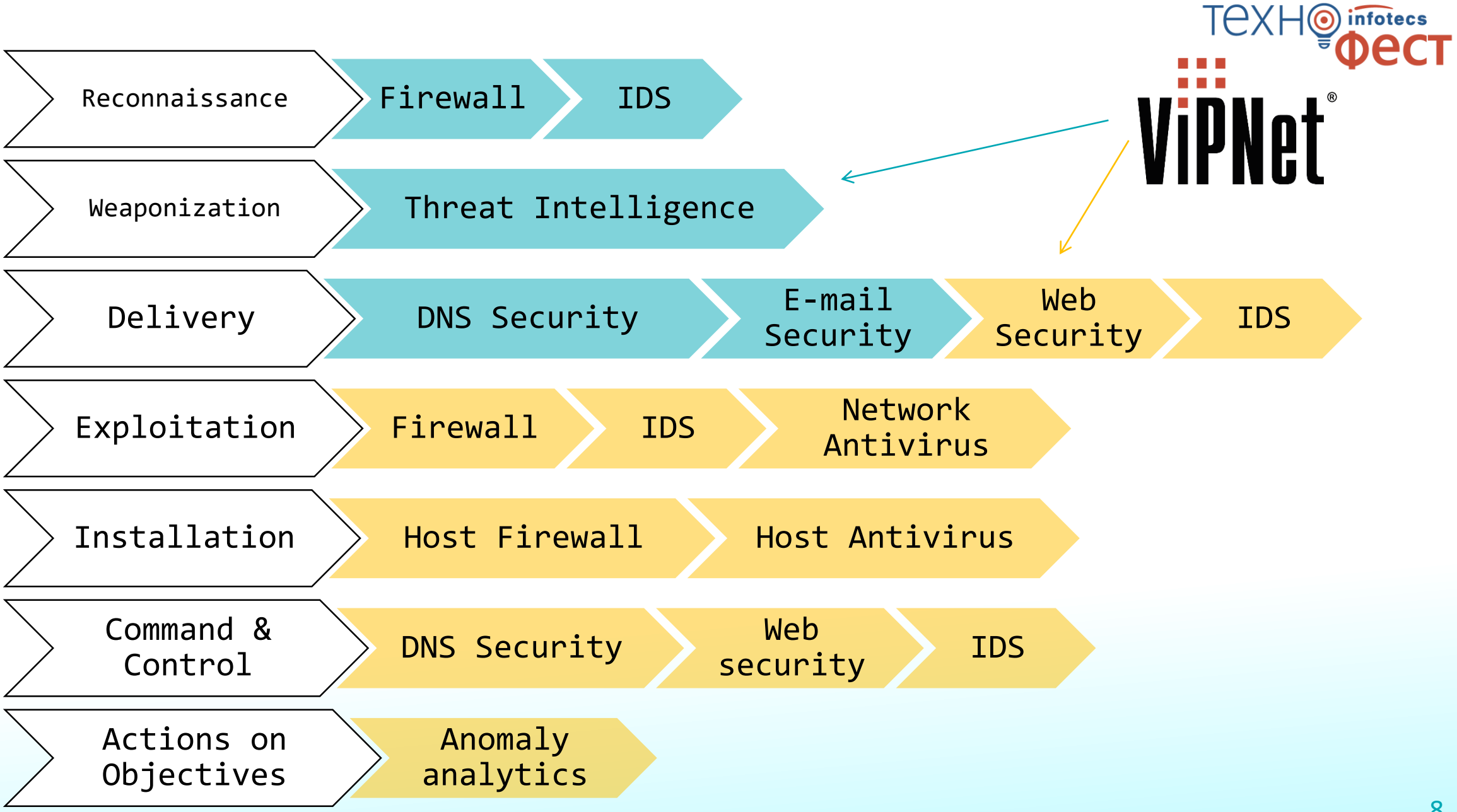
Процесс выглядит так:

- описание риск-ориентированной модели
- подбор угрозоцентрического решения (продукта)
- адаптация выбранного под риск-ориентированную модель

«Угрозоцентрическая модель» –
мы говорим об угрозоориентированных продуктах

Пример угрозо-ориентированной модели

ТЕХНО infotecs ФЕСТ


Reconnaissance
Firewall
IDS
Weaponization
Threat Intelligence
Delivery
DNS Security
E-mail Security
Web Security
IDS
Exploitation
Firewall
IDS
Network Antivirus
Installation
Host Firewall
Host Antivirus
Command & Control
DNS Security
Web security
IDS
Actions on Objectives
Anomaly analytics

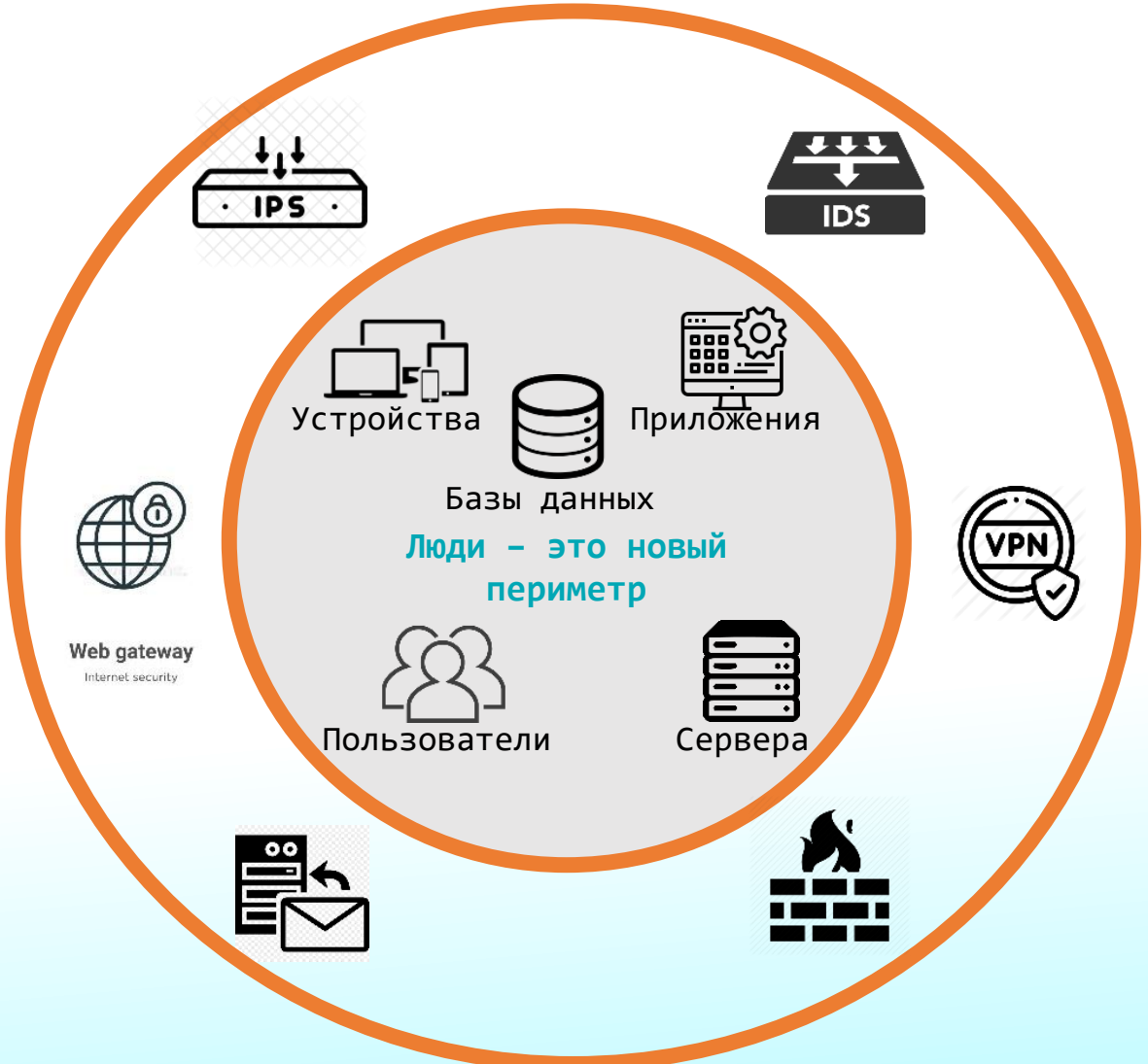
Экосистема

- **Доверие**
- **Анализ активности**
- **Сегментация подключений и защита каналов**
- **Права и политики**
- **Адаптация к предметной области**

ZTNA как угрозоцентрическая модель сетевой защиты

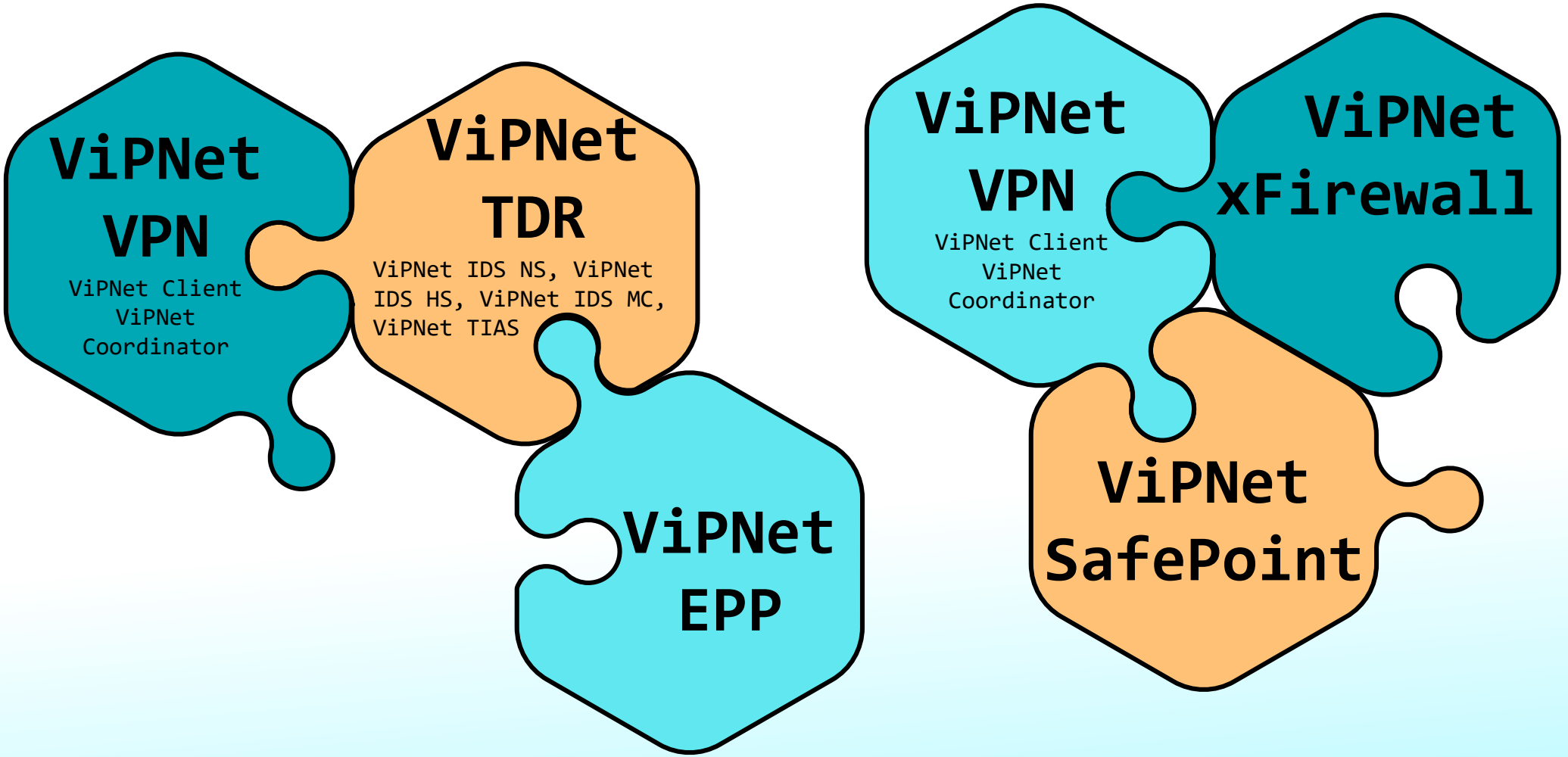
ТЕХНО infotecs ФЕСТ

Мир стремительно меняется, периметр меняется вместе с ним



	ViPNet Client	ViPNet Coordinator	ViPNet xFirewall	ViPNet SafePoint	ViPNet EPP	ViPNet TDR
Identity and Access Management (IAM)				☑		
Многофакторная аутентификация (MFA)	☑			☑		
Защита EndPoint (микроперимметры)	☑			☑	☑	
Микросегментация	☑	☑	☑	☑	☑	
Zero Trust Network Access (ZTNA)	☑	☑	☑	☑	☑	
Мониторинг и аналитика			☑	☑	☑	☑

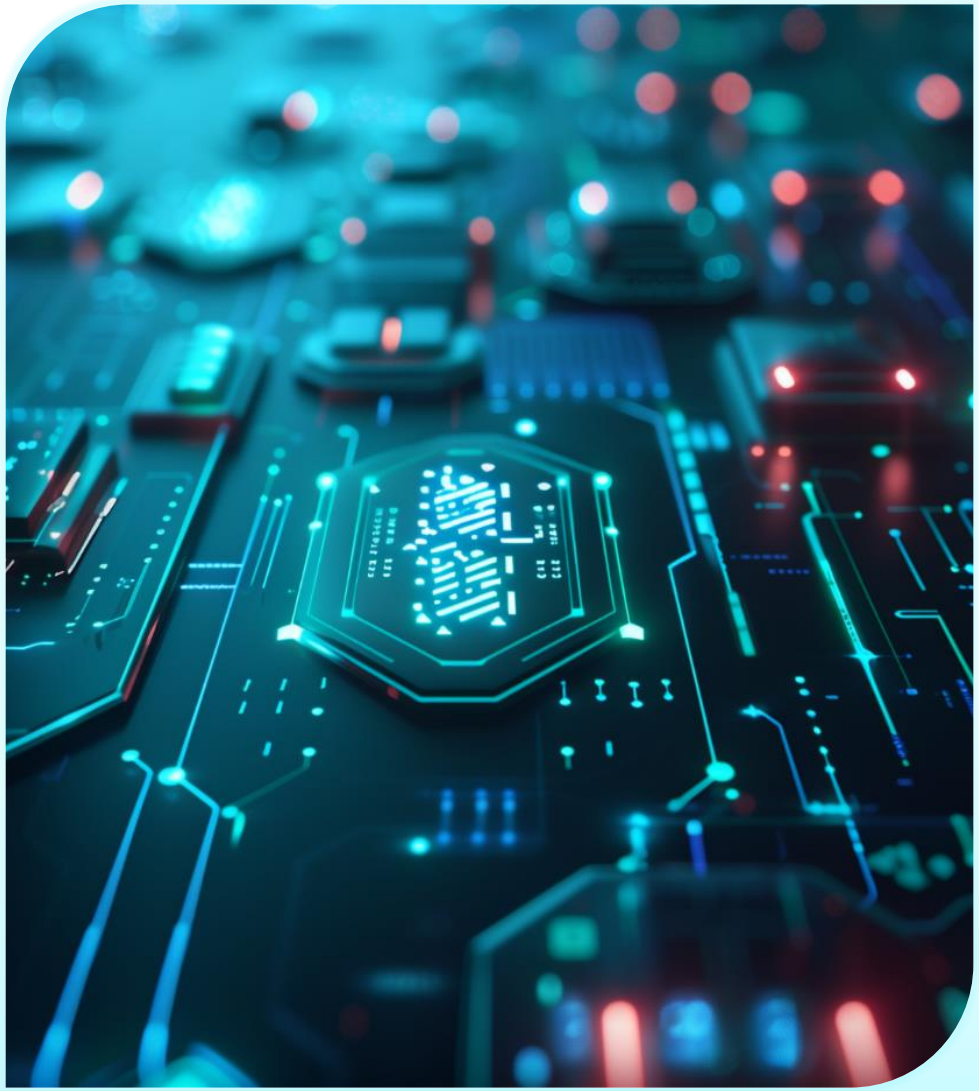
ViPNet Zero Trust как конструктор



ZTNA всем достаточно?

> Надеюсь, что да,
> но боюсь, что нет.

Жванецкий



SASE

Это ZTNA, адаптированный
для облачных сервисов

Так в чем проблема?

Убийца – дворецкий

Расследование инцидента показывает все стадии атаки, потому что оно ведется часами, а может быть даже днями

Предотвратить инцидент необходимо за миллисекунды, проведя анализ данных из десятков, сотен источников

Недостаточный уровень автоматизации

ZTNA, SASE используют RPA (Robotic Process Automation). **Несмотря на название «hands off», такие системы часто требуют от водителя держать руки на руле, как подтверждение готовности вмешаться**

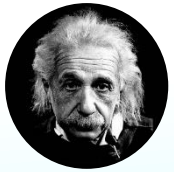
А рук катастрофически не хватает!

Трансформация модели

«Текущая модель»:

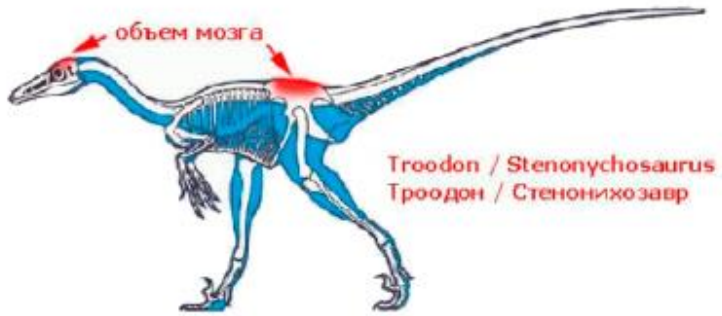
> Невозможно решить проблему на том же уровне, где она возникла. Нужно стать выше этой проблемы, поднявшись на следующий уровень

Альберт Эйнштейн



«Угрозоцентрическая модель»:

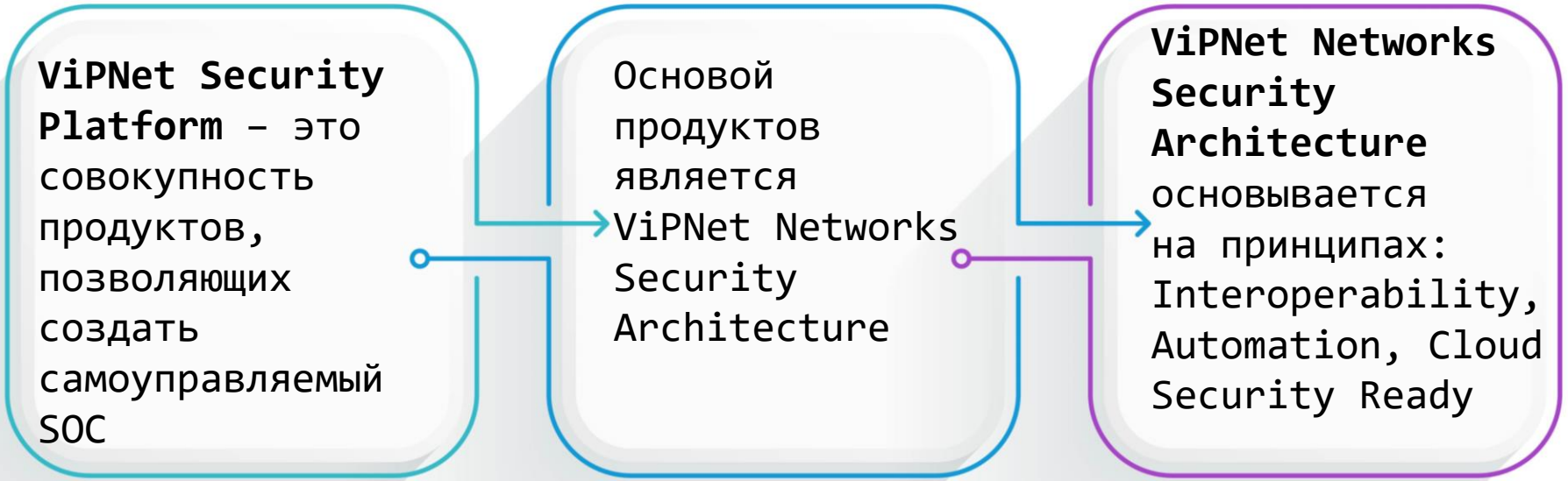
Размещение центров принятия решения максимально близко к угрозе



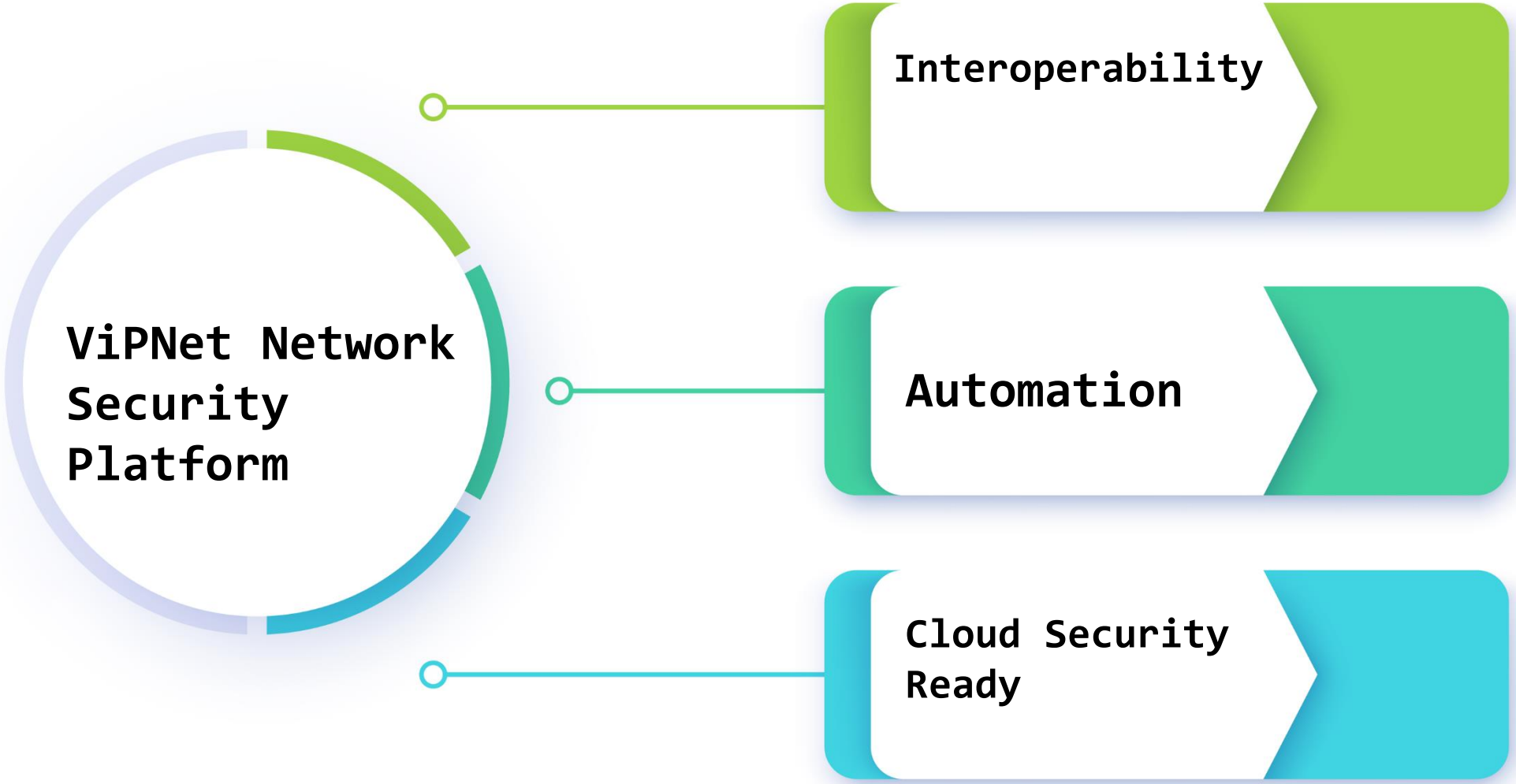
ViPNet NSP – самоуправляемый SOC

ТЕХНО infotecs ФЕСТ

ViPNet Network Security Platform



Что лежит в основе



Что это такое

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

Алексей Данилов
Руководитель продуктового направления
danilov@infotecs.ru
www.infotecs.ru