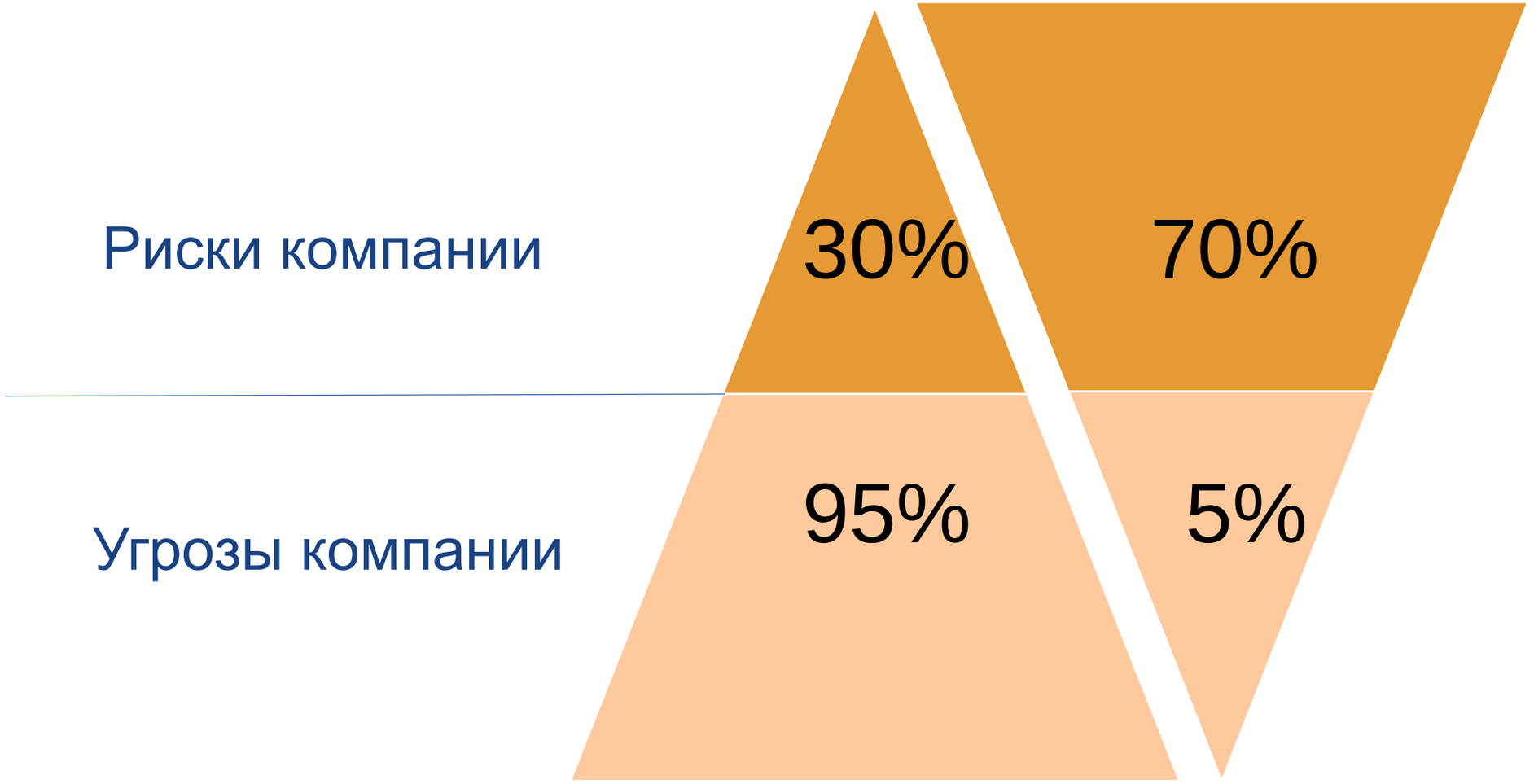
ЭР·ТЕЛЕКОМ

НАЙТИ И ОБЕЗВРЕДИТЬ

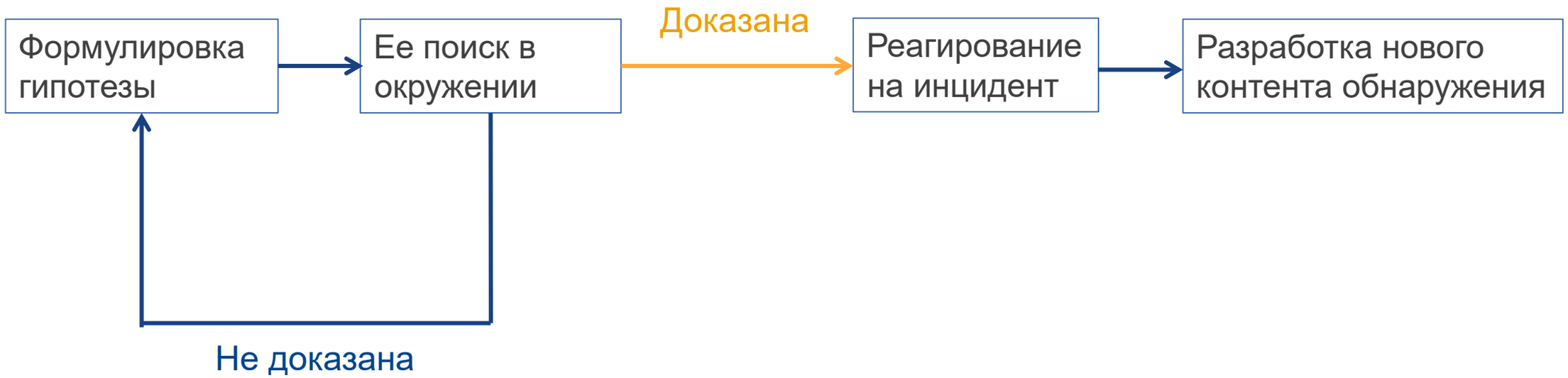
проактивый поиск угроз и злоумышленников в ИТ инфраструктуре


Риски компании
30%
70%
Угрозы компании
95%
5%

Threat Hunting- это процесс проактивного итеративного обнаружения вредоносной деятельности в компьютерных сетях

Согласно энциклопедии Касперского

Охота за угрозами



Три составляющие успешного внедрения ThreatHunting

ЭР-ТЕЛЕКОМ

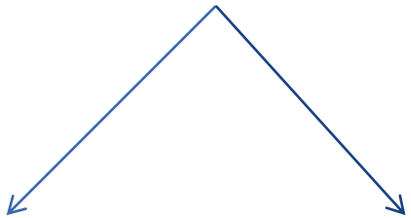
Телеметрия

Технологии

Команда

Три составляющие успешного внедрения ThreatHunting

Телеметрия Технологии Команда



Хостовая

ОС
EDR
Самописные скрипты

Сетевая

IDS
Sandbox
NGFW
WAF
Почтовые сервера

Три составляющие успешного внедрения ThreatHunting

ЭР-ТЕЛЕКОМ

Телеметрия

Технологии

Команда

Три составляющие успешного внедрения ThreatHunting

ЭР-ТЕЛЕКОМ

Телеметрия

Технологии

Команда

устройство ОС

безопасность ОС.

безопасность сетей

сетевая форензика

хостовая форензика

Threat Intelligence

MITRE ATT&CK

киберразведка

Модель зрелости использования ThreatHunting

Передовой (HMM4 — Leading)	автоматизированный метод поиска и анализа угроз
Инновационный (HMM3 — Innovative)	собственные методы поиска угроз
Процедурный (HMM2 — Procedural)	стандартные сценарии активного поиска угроз
Минимальный (HMM1 — Minimal)	сбор аналитики и данные киберразведки
Начальный (HMM0 — Initial)	традиционные системы безопасности

СОСТАВ УСЛУГИ SOC

ЭР-ТЕЛЕКОМ

24/7

Мониторинг инцидентов 24x7

- Подключение к ГосСОПКА
- Подключение к ФинЦерт
- Реагирование на инциденты
- Расследование инцидентов

По запросу

Система управления событиями безопасности (SIEM)*

- Поставка системы
- Внедрение системы
- Сопровождение системы

По запросу

Организация защищенного сетевого канала*

ГОСТ VPN

По запросу

Сопровождение*

Поддержка L1/L2/L3

По запросу

Каримов Сергей

специалист направления
информационной безопасности

7 919 499 05 41

Михаил Еловиков

менеджер по развитию
продуктов ИБ

7 912 499 94 94

Ждем вас на нашем стенде в холле

ЭР·ТЕЛЕКОМ