

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





SOC без иллюзий:

тренды, боли и реальность рынка

Артём Савчук

Технический директор
Перспективный мониторинг



SOC 2025-2026 в цифрах

Ampire 360°

30%

рост российского
рынка центров
мониторинга

по оценке VolgaBlob

71%

рост спроса на
экспертные
сервисы ИБ

по оценке Jet SOC

27%

рост числа
инцидентов

по оценке АО «ПМ»

40%

рост числа DDoS
на российские
ресурсы

по оценке АО «ПМ»



Главные проблемы SOC

01 Кризис скорости реагирования

Атаки становятся быстрее, злоумышленники автоматизируют атаки с помощью ИИ

03 «Усталость» от алертов

SOC получает слишком много сигналов. Чем больше средств защиты, тем сложнее найти действительно опасное событие

02 AI сам создаёт новые риски

SOC использует AI, чтобы быстрее защищать организацию, но одновременно должен защищать сам AI-контур

04 Дефицит качественных кадров

Критическая нехватка специалистов по расследованию инцидентов и форензике

Тренды SOC 2026

Ampire 360°



Автоматизация
рутины/Agentic
SOC



Фокус на Threat
Intelligence



Консолидация на
единой платформе
(Visibility Gap)



Импортозамещение

Раньше:

Чем больше
инцидентов, тем
круче!

Сейчас:

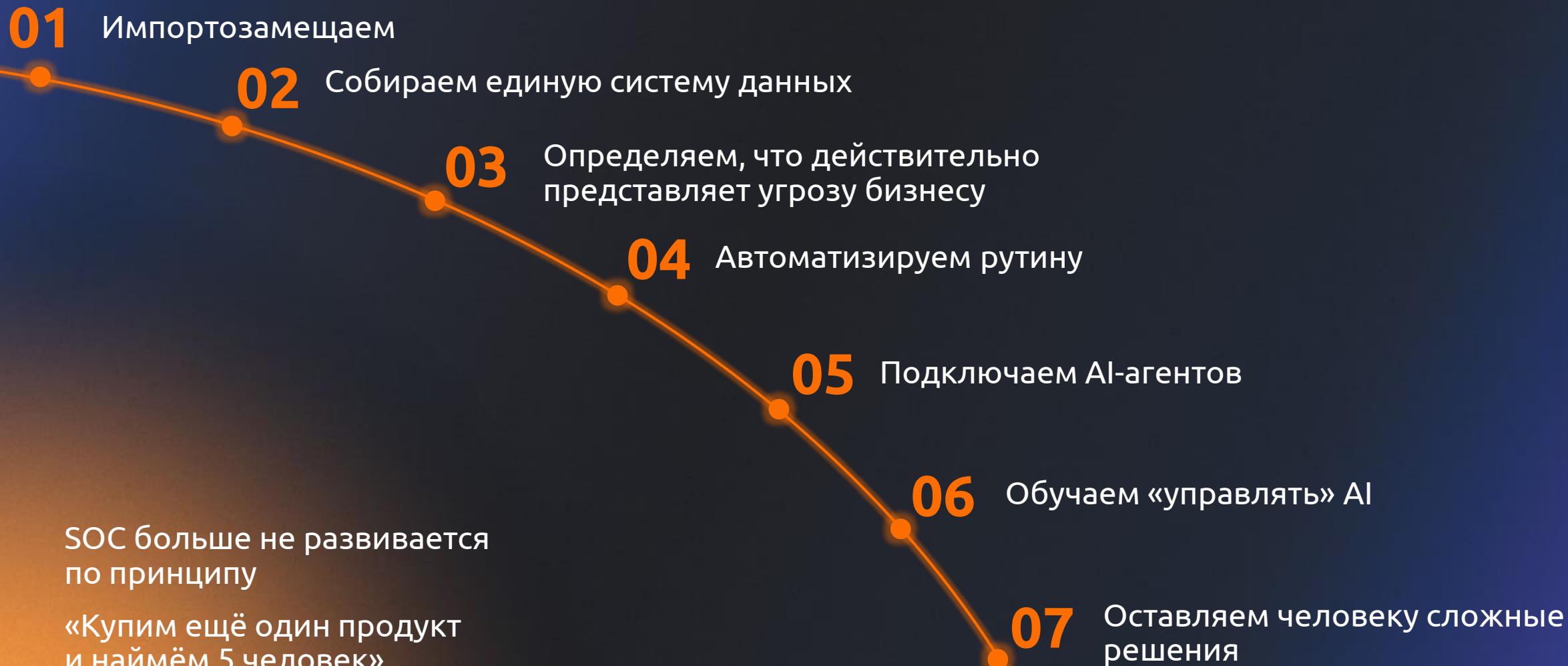
Скорость
реагирования





Построение «идеального SOC»

Ampire 360°



Главные направления атак

Фишинг и социальная инженерия

Человеческий фактор остаётся главным каналом связи между инфраструктурой и злоумышленником

Попытки эксплуатации уязвимостей

Нет ничего лучше, чем прямой путь к компрометации систем через уже существующие слабые места инфраструктуры

Компрометация учётных записей

Украденные креды позволяют злоумышленнику использовать легитимный доступ и оставаться незамеченным

Атаки на веб-ресурсы

Веб становится основным внешним периметром компаний и одним из главных каналов проникновения во внутреннюю инфраструктуру

Данные за Q3 2026 г.

Ampire 360°

Заражение ВПО

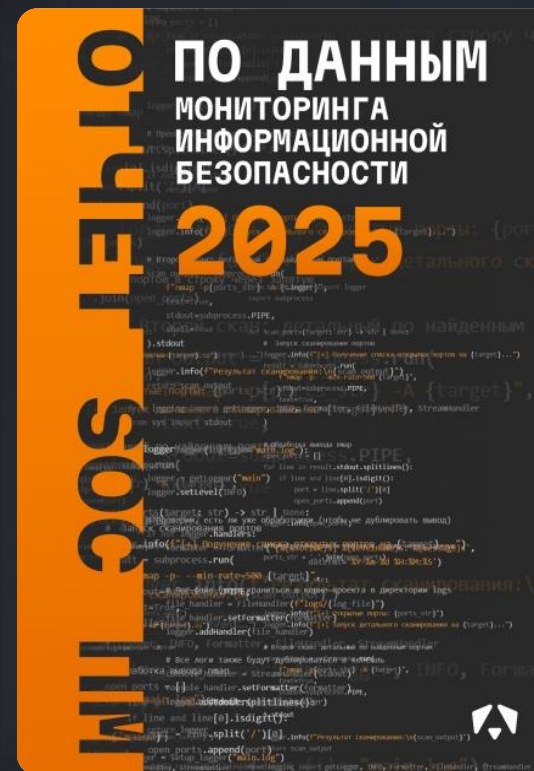
↑ **41%**

Попытки эксплуатации
уязвимостей

↑ **29%**

События по сетевому
сканированию

↑ **9%**





ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

Благодарю за внимание!

Артём Савчук

Технический директор
Перспективный мониторинг



Ampire 360°