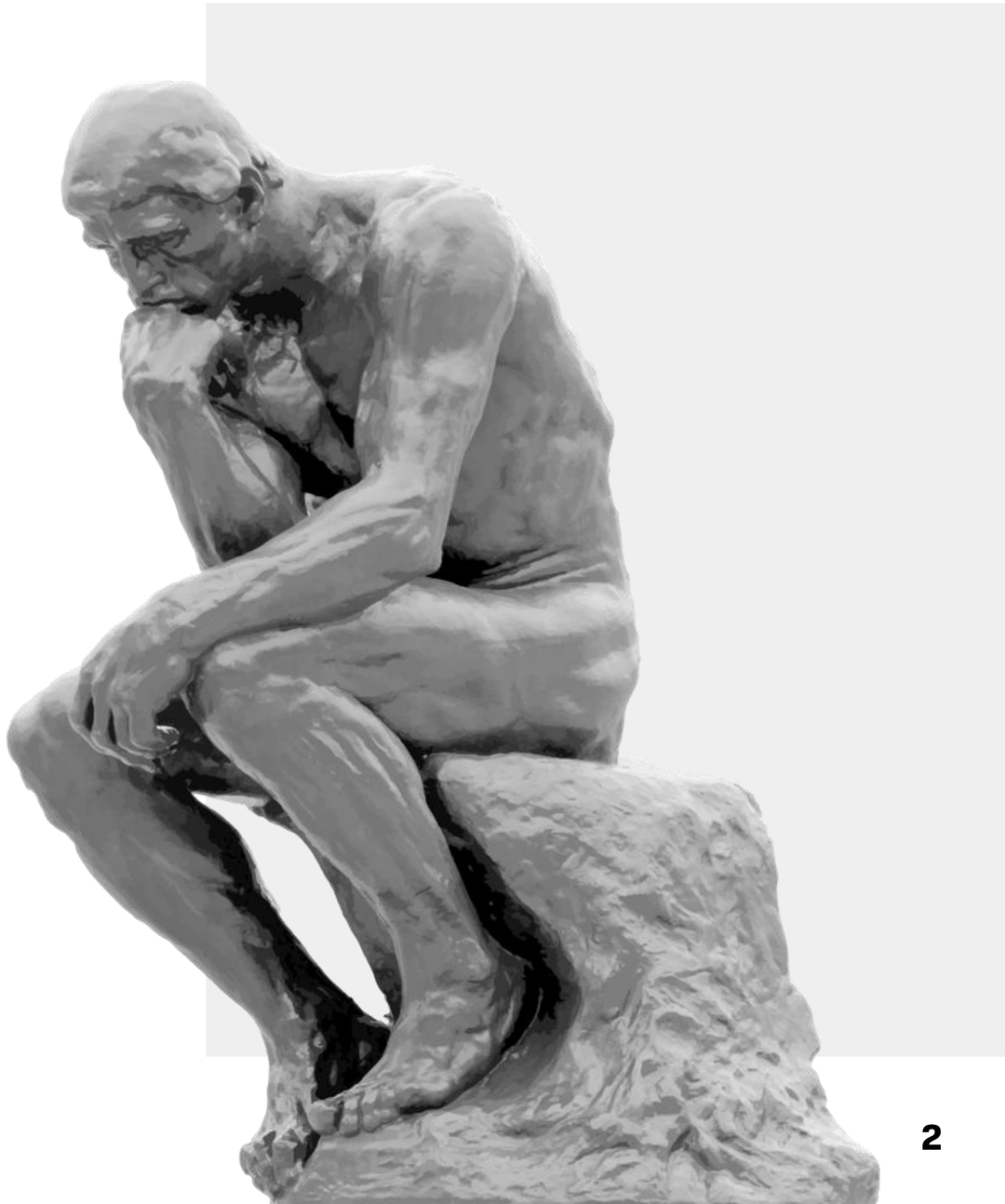
СУЩЕСТВУЕТ ТОЛЬКО ДВА ТИПА КОМПАНИЙ:

те, которые были взломаны,
и те, которые будут взломаны

Роберт Мюллер

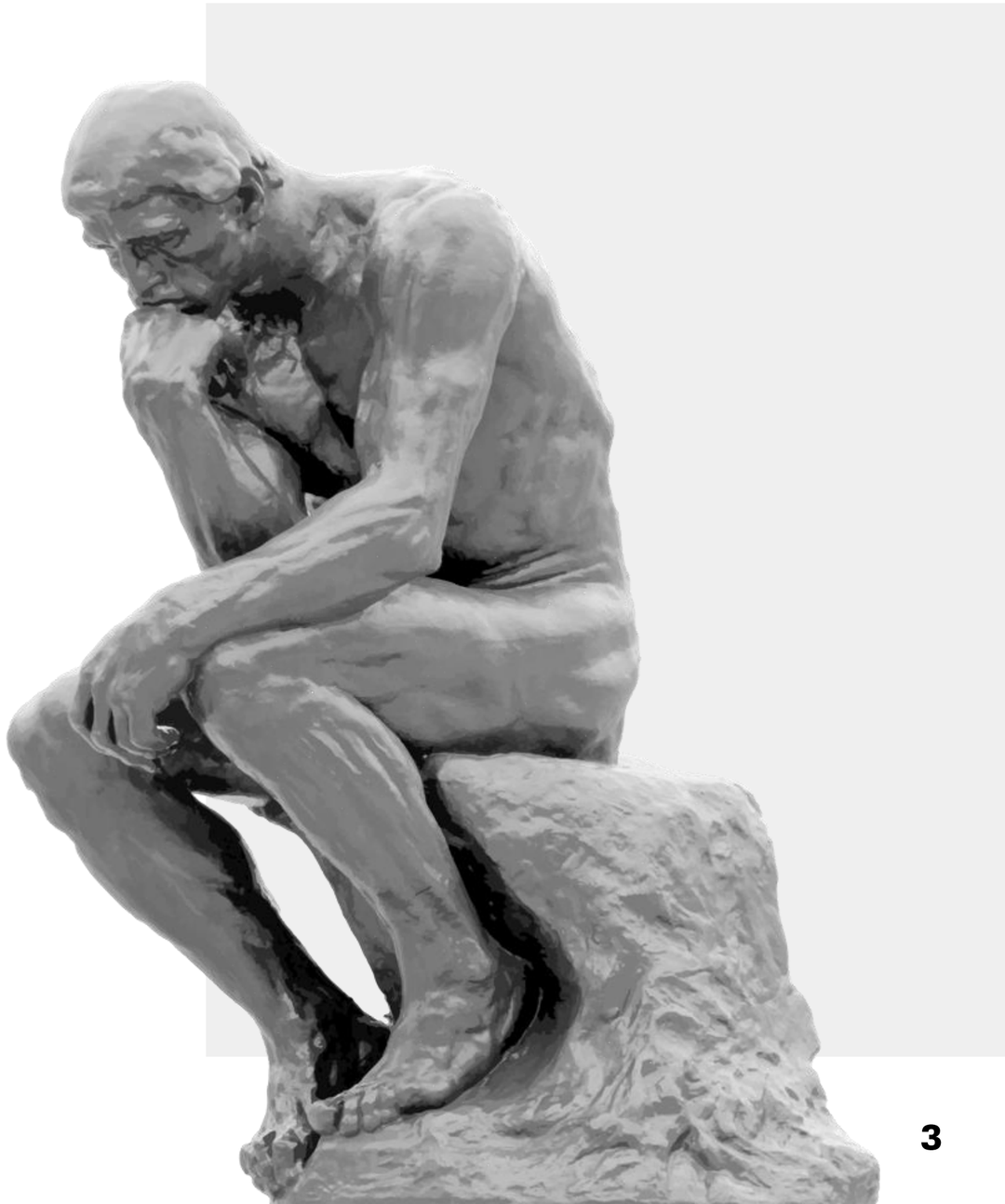
Системы мониторинга
и реагирования настроены

ЧТО ДАЛЬШЕ?



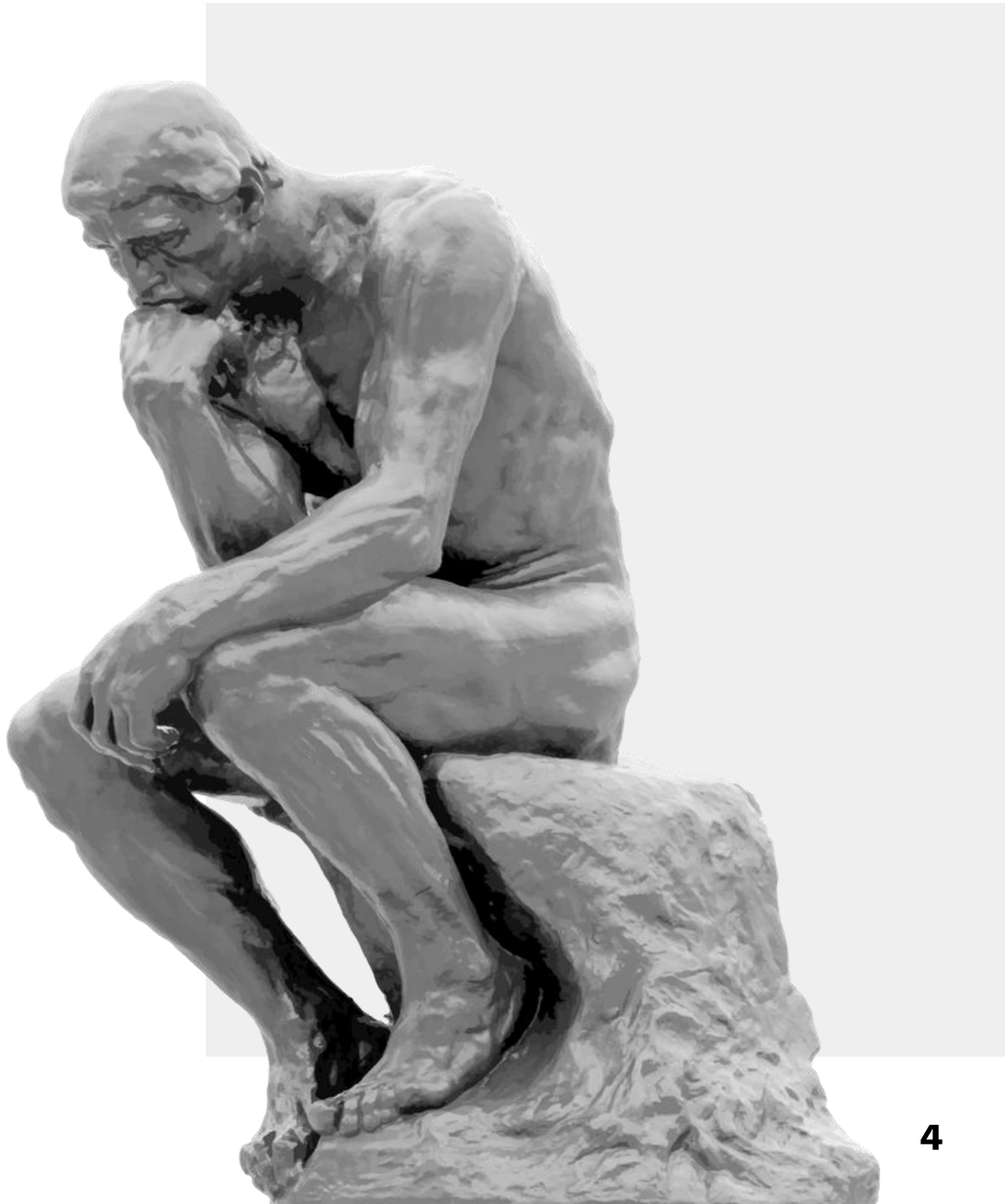
Достаточно ли установки ключевых защитных решений?

СТАВЬ ”+”, ЕСЛИ ДОСТАТОЧНО



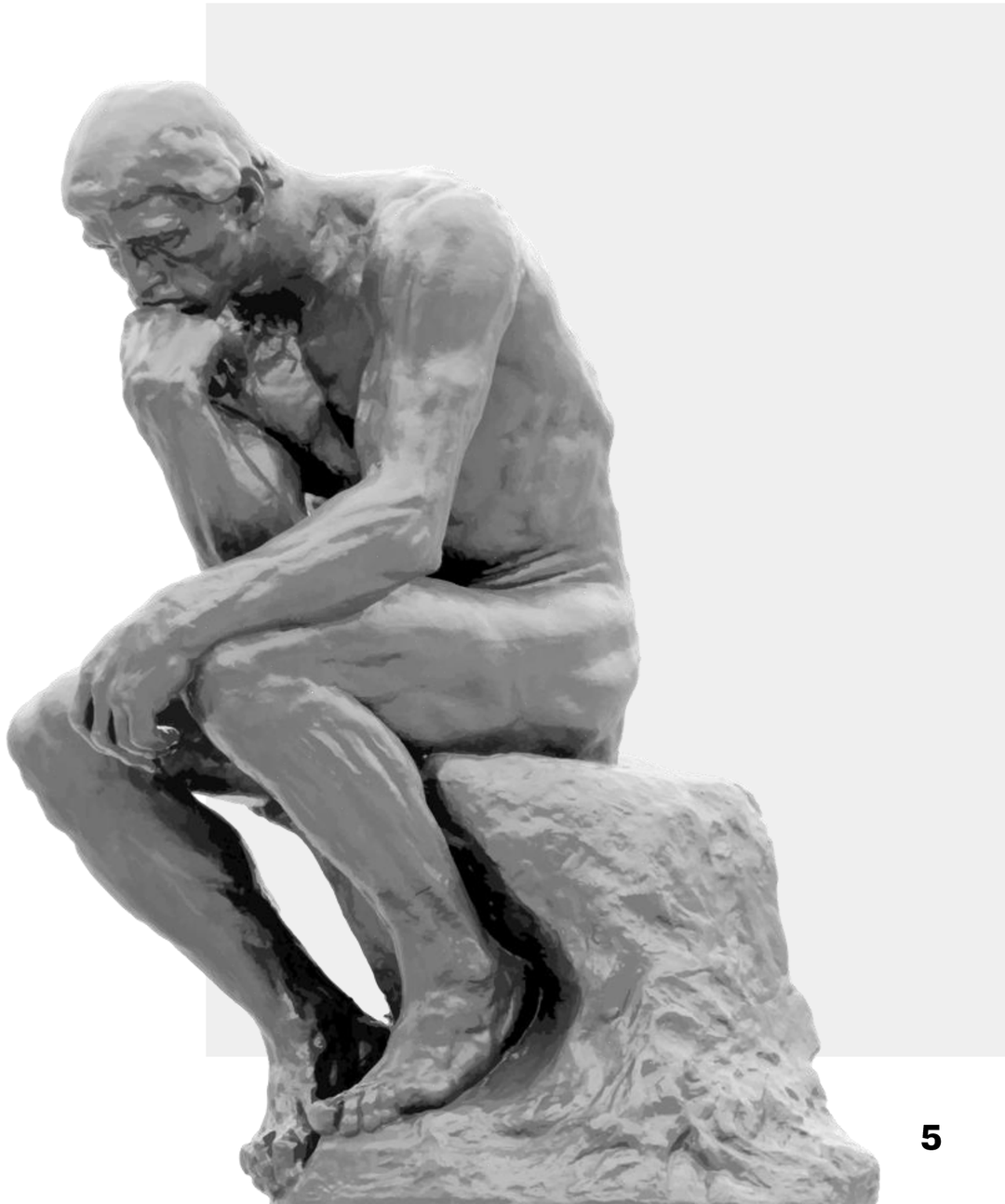
Достаточно ли регулярных пентестов?

СТАВЬ ”+”, ЕСЛИ ДОСТАТОЧНО



Достаточно ли Red Team для регулярных проверок?

СТАВЬ ”+”, ЕСЛИ ДОСТАТОЧНО



ПУТЬ ОТ БЕЗОПАСНОСТИ К УСТОЙЧИВОСТИ:

”Не важно сколько раз упал, важно, сколько раз поднялся“

Денис Макрушин,
Технический директор, Блок кибербезопасности, МТС


CiSO
Pentester

Forbes

Sep 14, 2017, 03:22am EDT

How Hackers Broke Equifax: Exploiting A Patchable Vulnerability

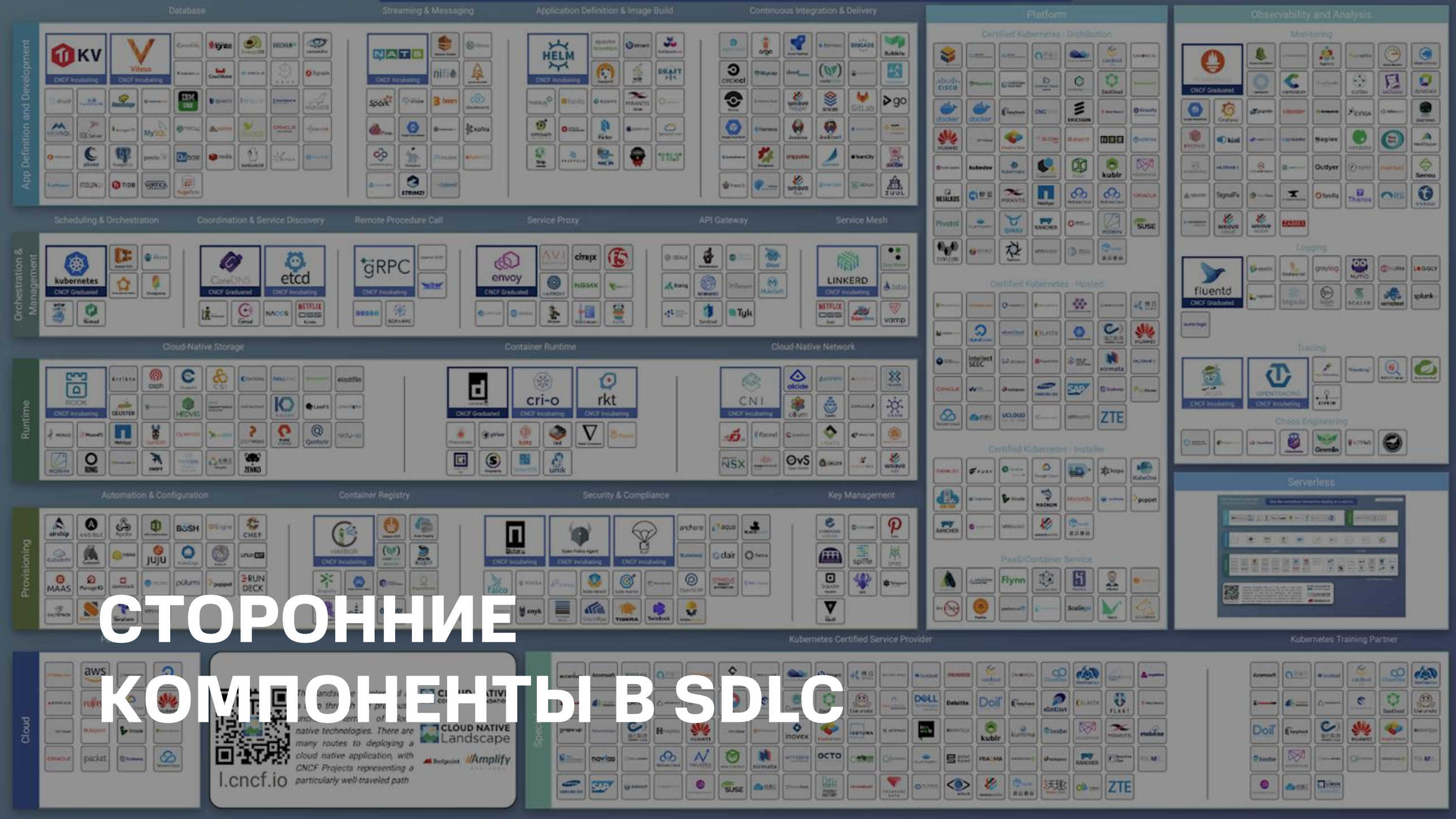
Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

This article is more than 4 years old.

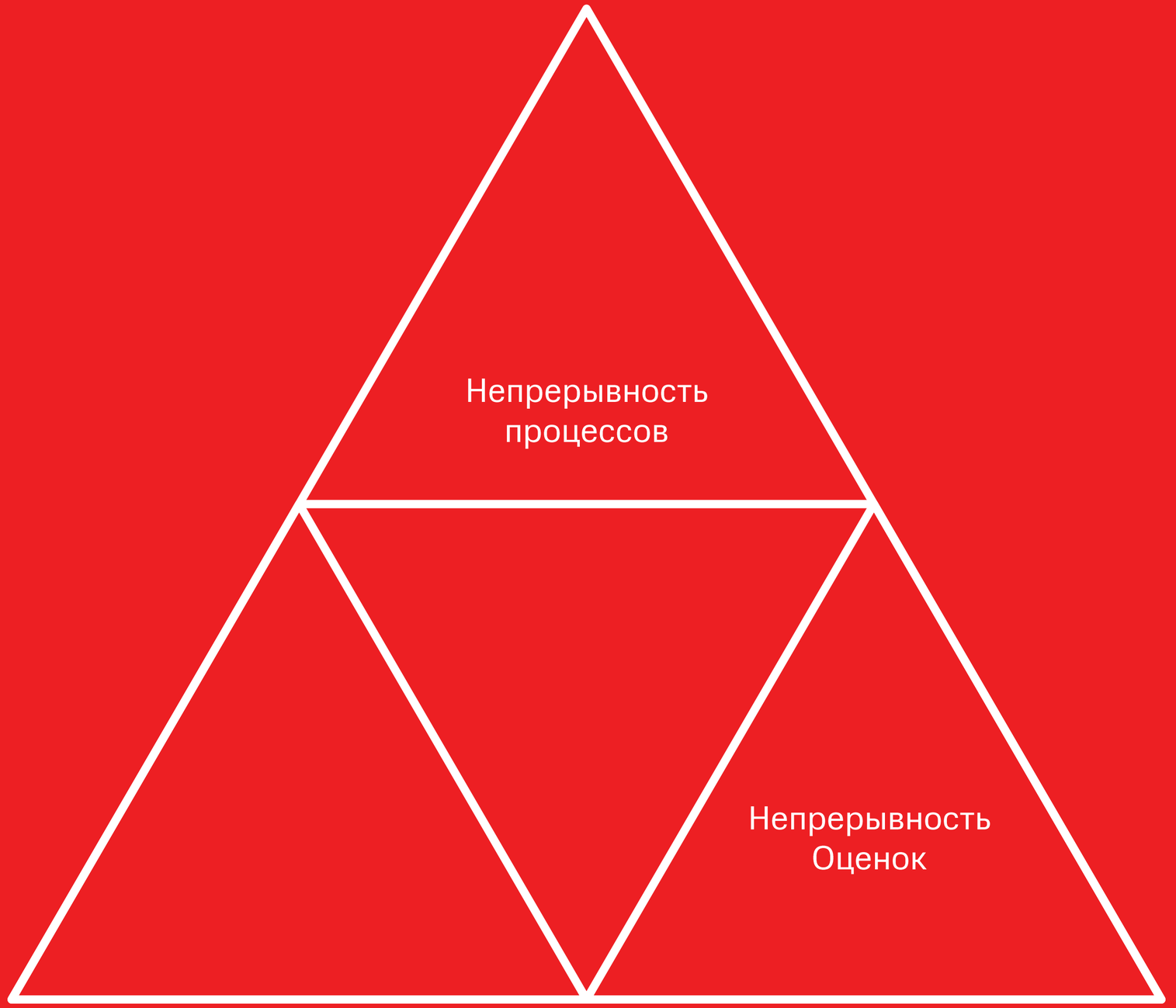
Equifax is facing a Congressional investigation, a class action lawsuit and widespread criticism... [+]

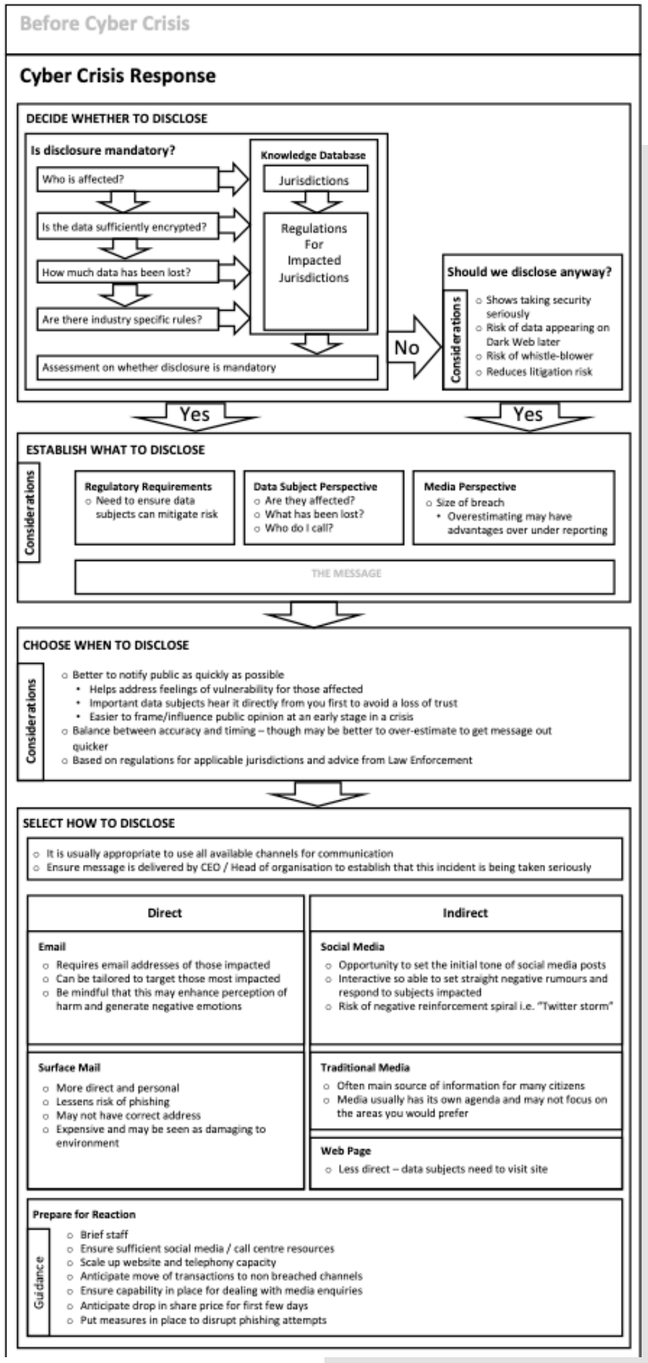
Equifax's terse explanation for its mega-breach in which 143 million Americans' information was put at risk was depressingly predictable: a vulnerability in a piece of web software. What was most depressing, though, was that the flaw was patched back in March.



СТОРОННИЕ КОМПОНЕНТЫ В SDLC

ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ


Непрерывность
процессов
Непрерывность
Оценок

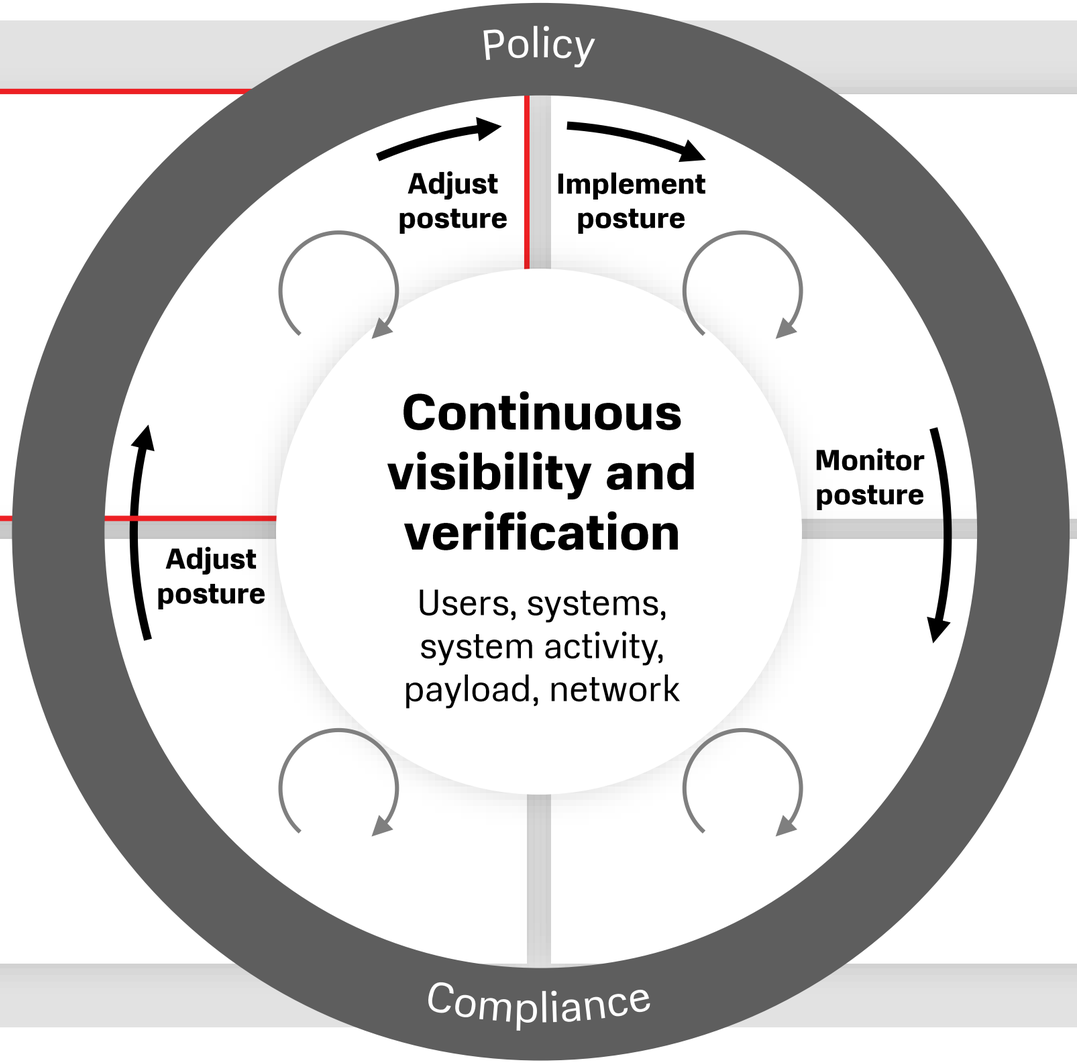


"A Framework for Effective Corporate Communication after Cyber Security Incidents", Jason R. C. Nurse

МОДЕЛЬ АДАПТИВНОЙ БЕЗОПАСНОСТИ

PREDICT
- Risk-prioritized exposure assessment
- Anticipate threats and attacks
- Baseline systems and security posture

PREVENT
- Harden systems
- Isolate systems
- Prevent attacks



- Remediate
- Design/model policy change
- Investigate incidents/ retrospective analysis

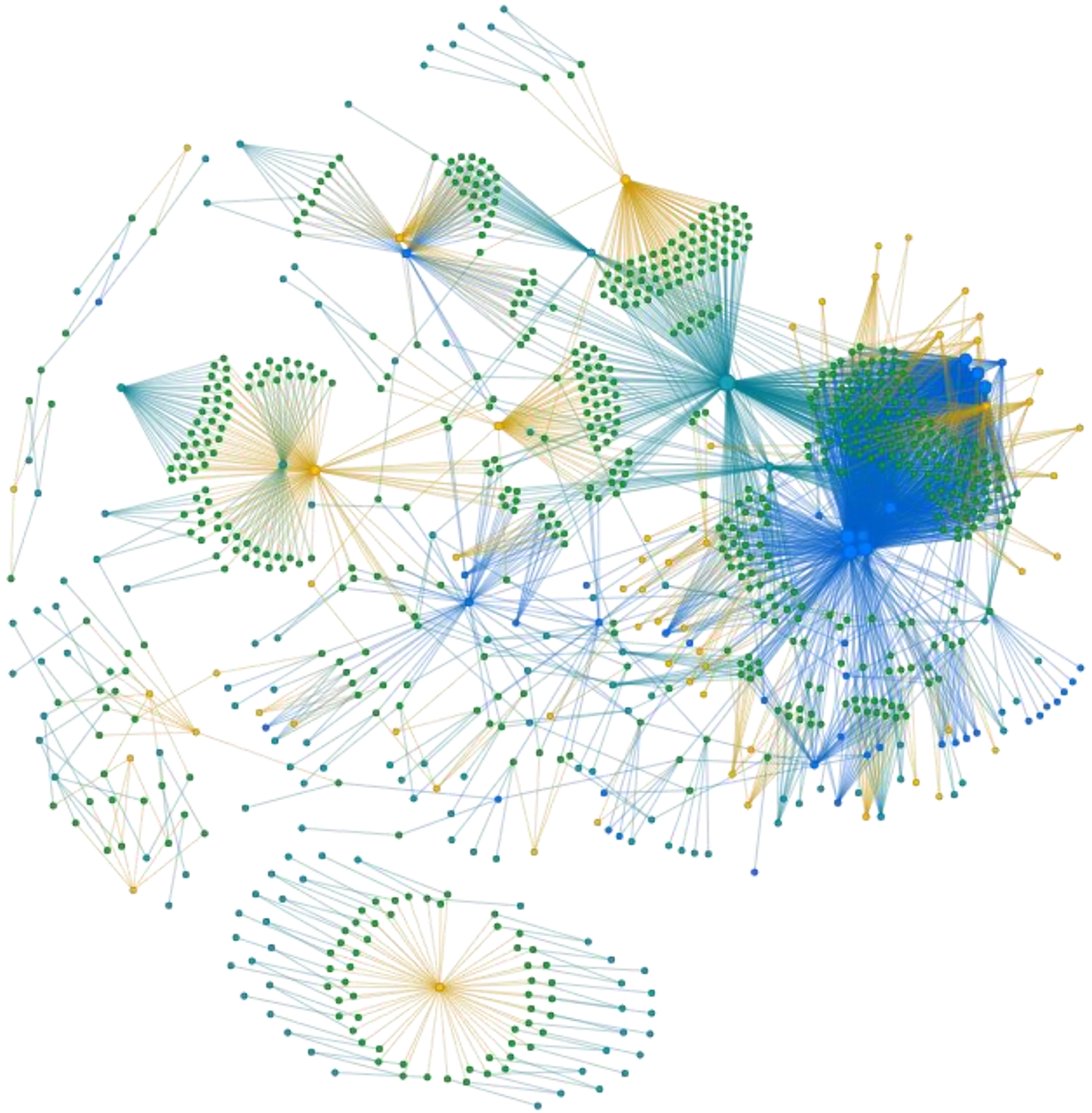
RESPOND

- Detect incidents
- Confirm and prioritize risk
- Contain incidents

DETECT

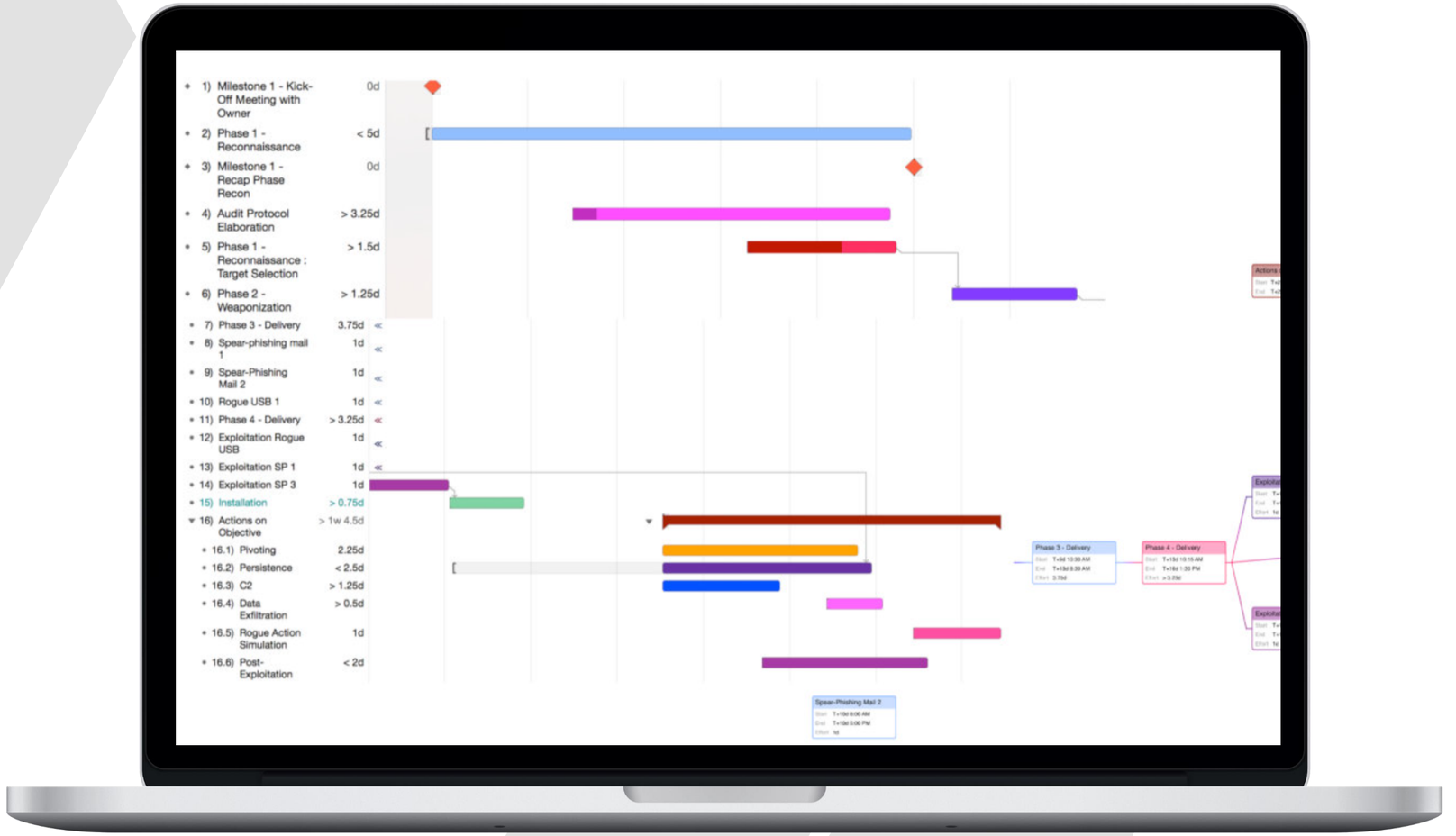
ОГРАНИЧЕНИЕ 1:

ПОВЕРХНОСТЬ АТАКИ

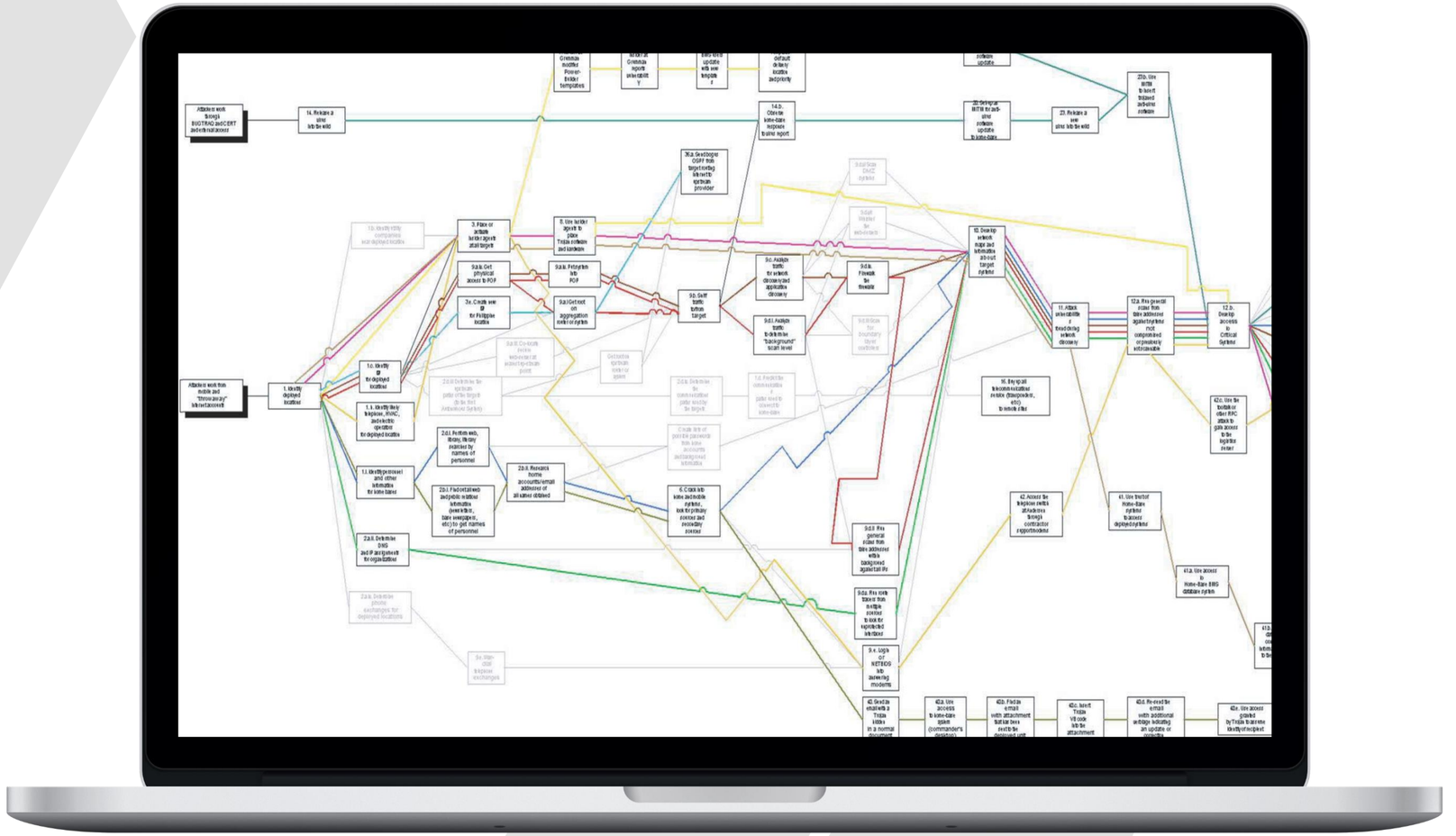


ОГРАНИЧЕНИЕ 2:
РЕСУРС

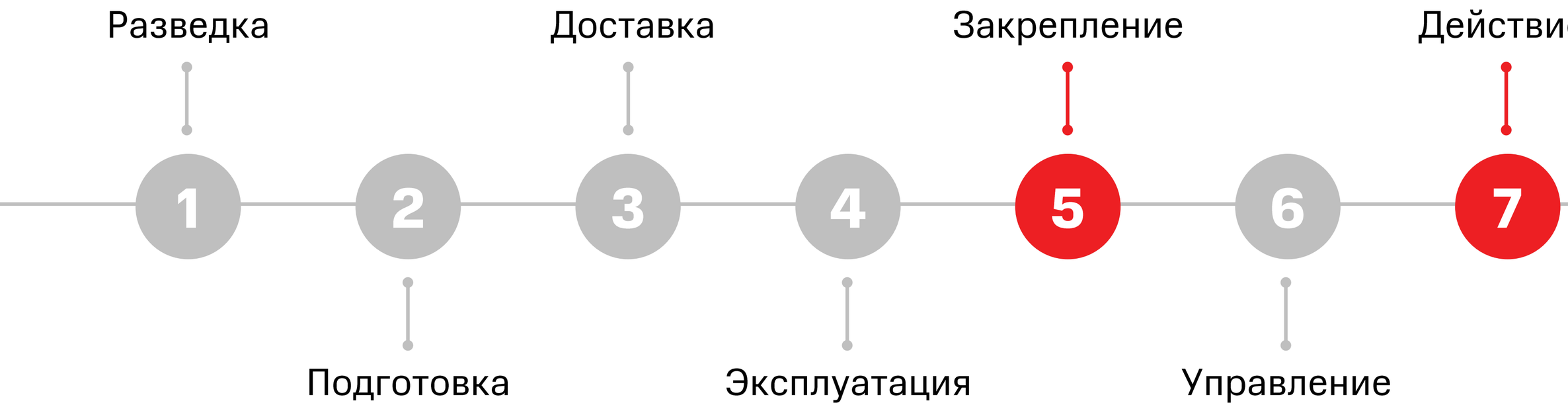
ОГРАНИЧЕНИЕ 3:
КОММУНИКАЦИЯ



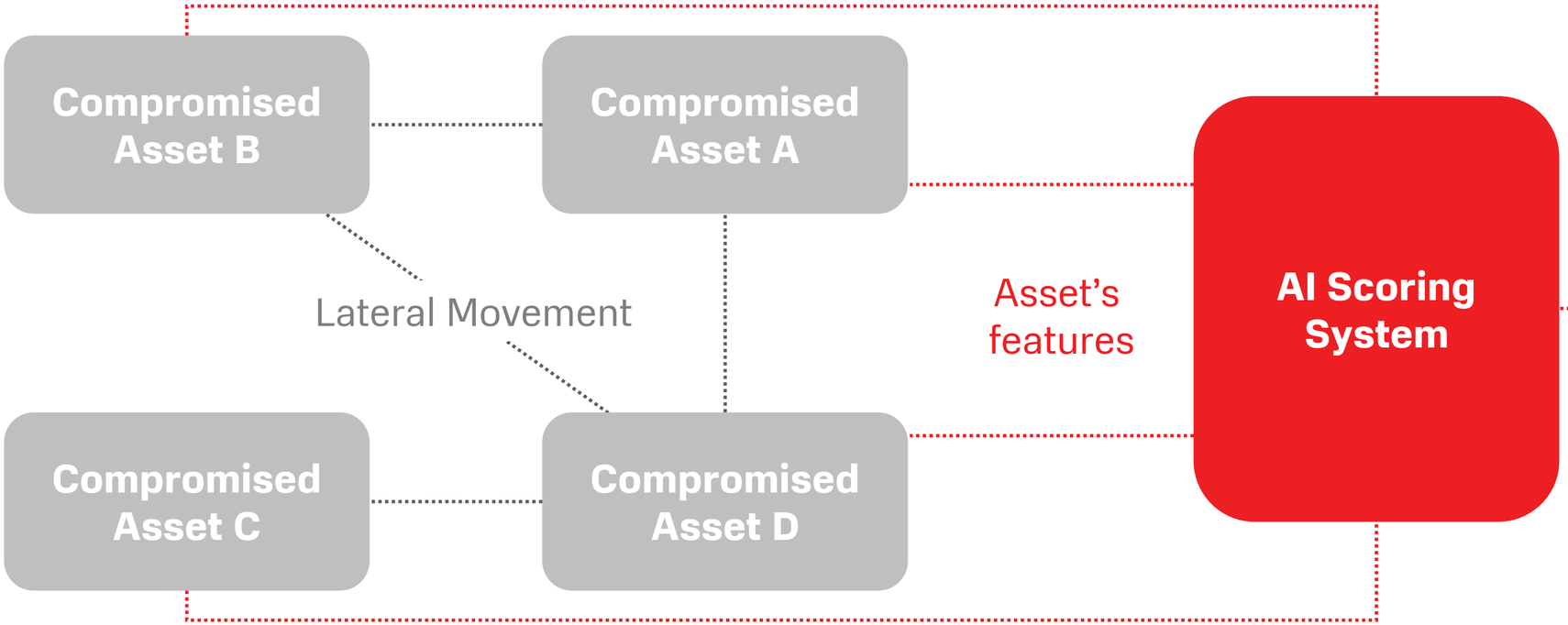
ОГРАНИЧЕНИЕ 4:
АВТОМАТИЗИРОВАННЫЙ ИНСТРУМЕНТ



ATTACK KILL CHAIN ТРЕБУЕТ ЧЕЛОВЕКА



ML ДЛЯ ОЦЕНКИ ЦЕННОСТИ РЕСУРСА



- Оценка безопасности
- Прогнозирование путей атаки
- Оценка ценности ресурсов


Непрерывность
процессов
Триада
Устойчивости
Бизнеса
Непрерывность
Проверок
Непрерывность
Оценок

ПУТЬ ОТ БЕЗОПАСНОСТИ К УСТОЙЧИВОСТИ

Задать вопрос экспертам
cybersecurity@mts.ru