

**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



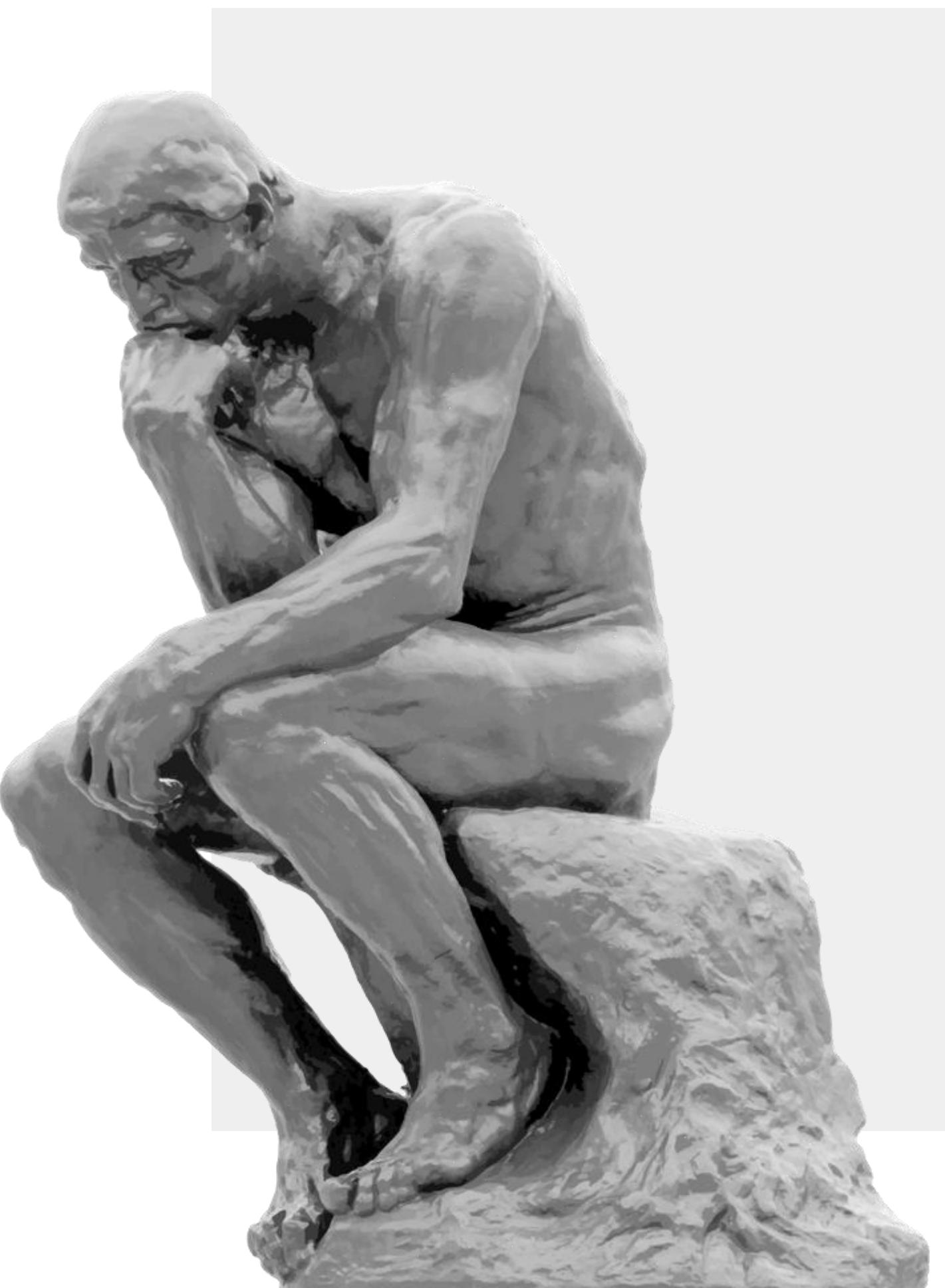
Достаточно ли регулярных пентестов?

СТАВЬ “+”, ЕСЛИ ДОСТАТОЧНО



Достаточно ли Red Team для регулярных проверок?

СТАВЬ “+”, ЕСЛИ ДОСТАТОЧНО



A photograph of a large-scale data center or server room. The perspective is looking down a long aisle between two rows of tall, grey server racks. The ceiling is high with a complex network of white steel beams and support structures. The lighting is bright, reflecting off the metallic surfaces of the racks.

ПУТЬ ОТ БЕЗОПАСНОСТИ К УСТОЙЧИВОСТИ:

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

Денис Макрушин,
Технический директор, Блок кибербезопасности, МТС

МТС



CiSO

Pentester



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.

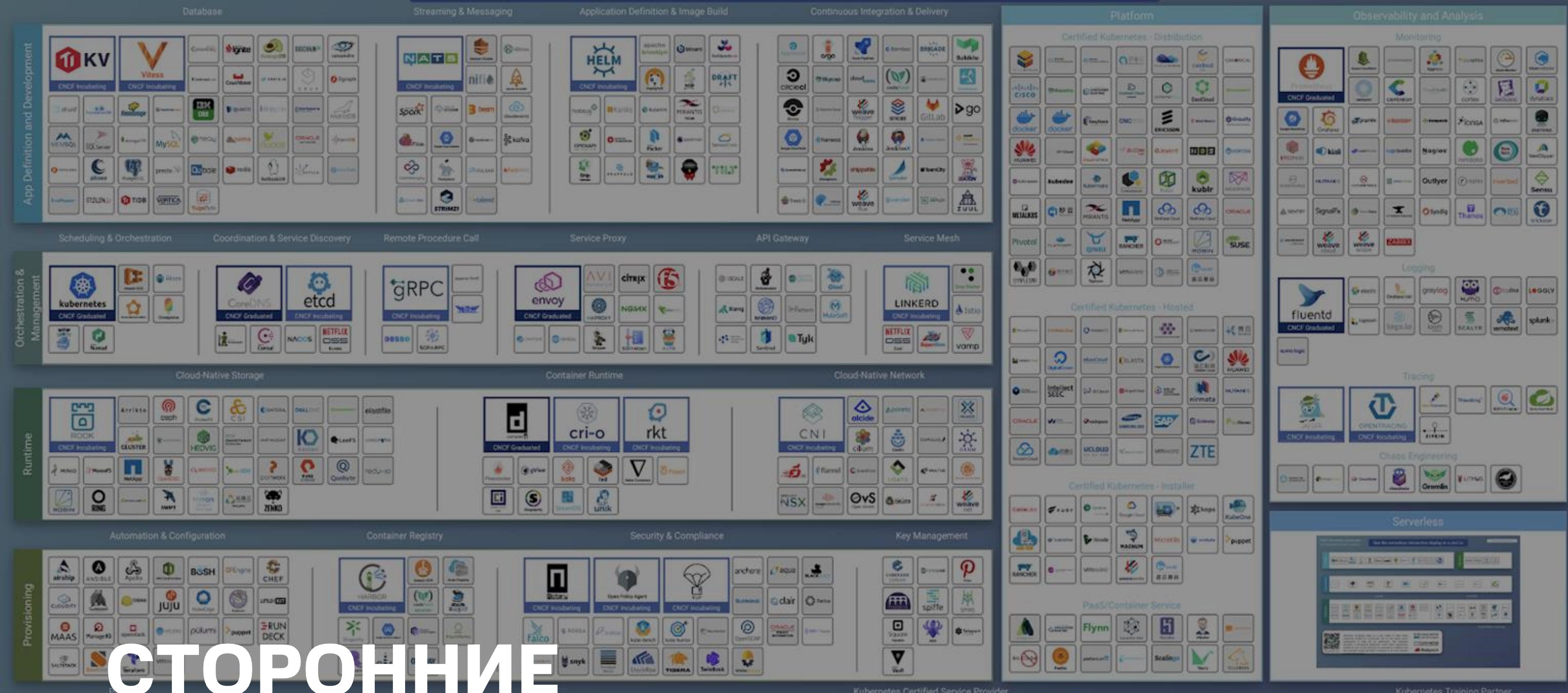
Follow

⌚ This article is more than 4 years old.



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

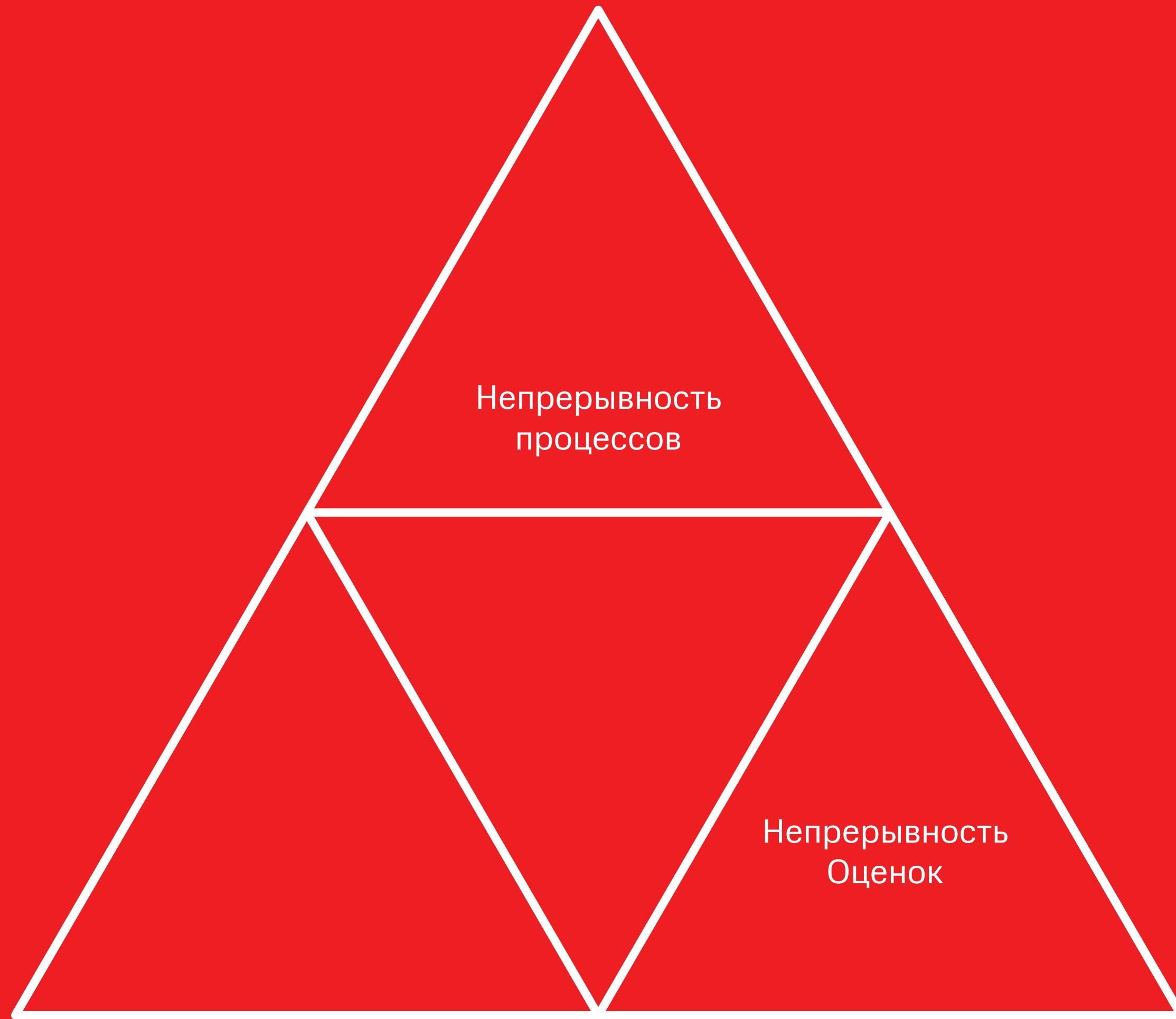
Equifax's terse explanation for its mega-breach in which 143 million Americans' information was put at risk was depressingly predictable: a vulnerability in a piece of web software. What was most depressing, though, was that the flaw was patched back in March.

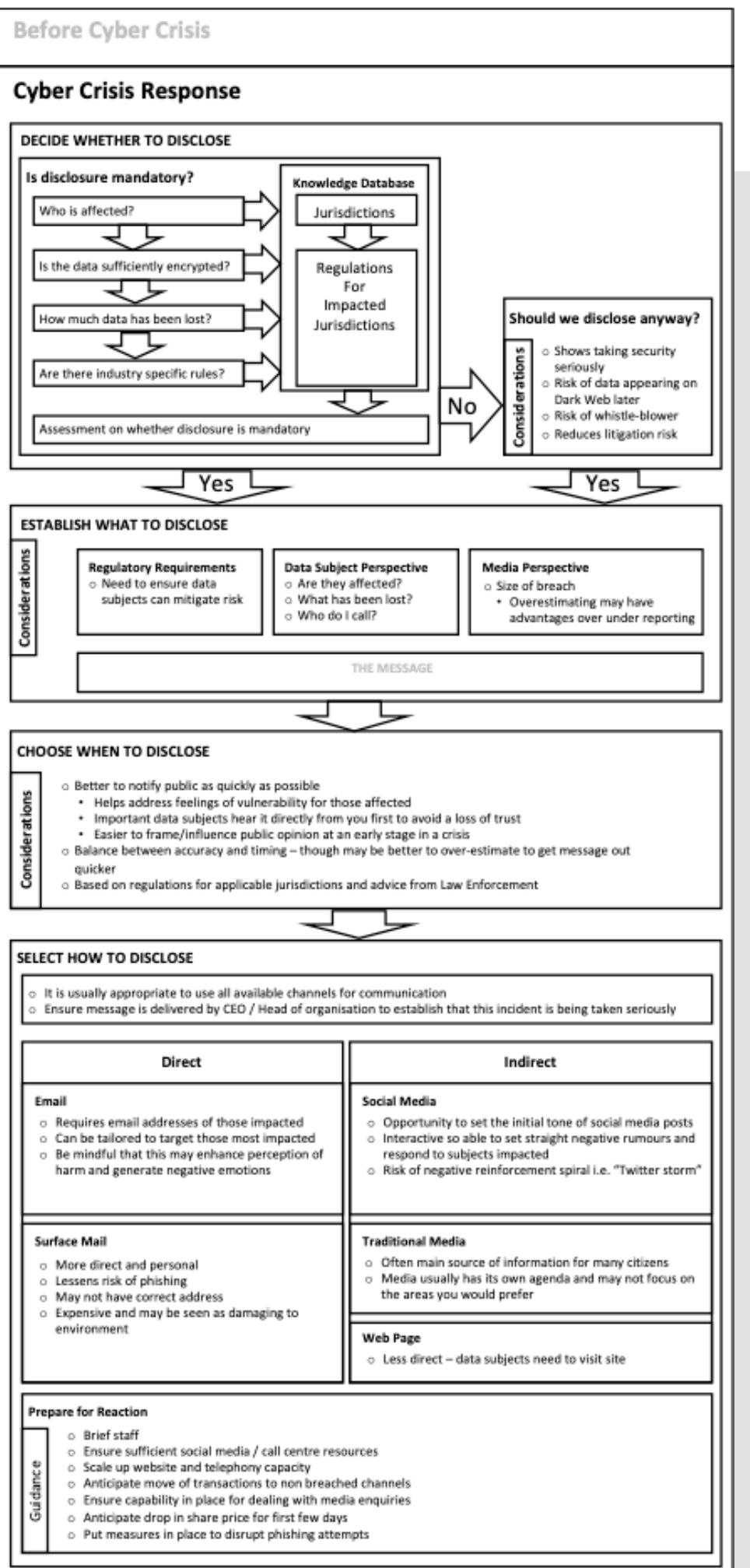


СТОРОННИЕ КОМПОНЕНТЫ В SDLC

ПРОЦЕСС РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

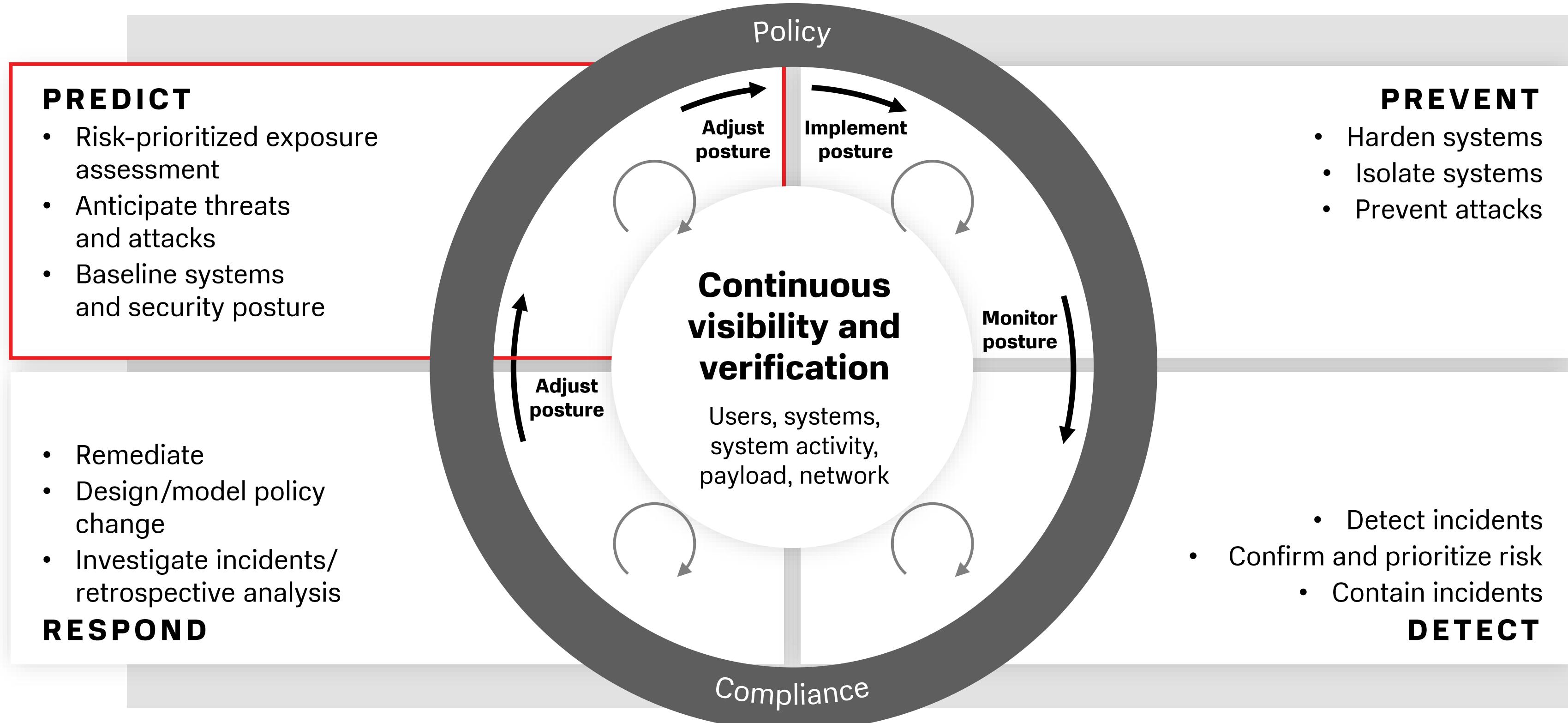




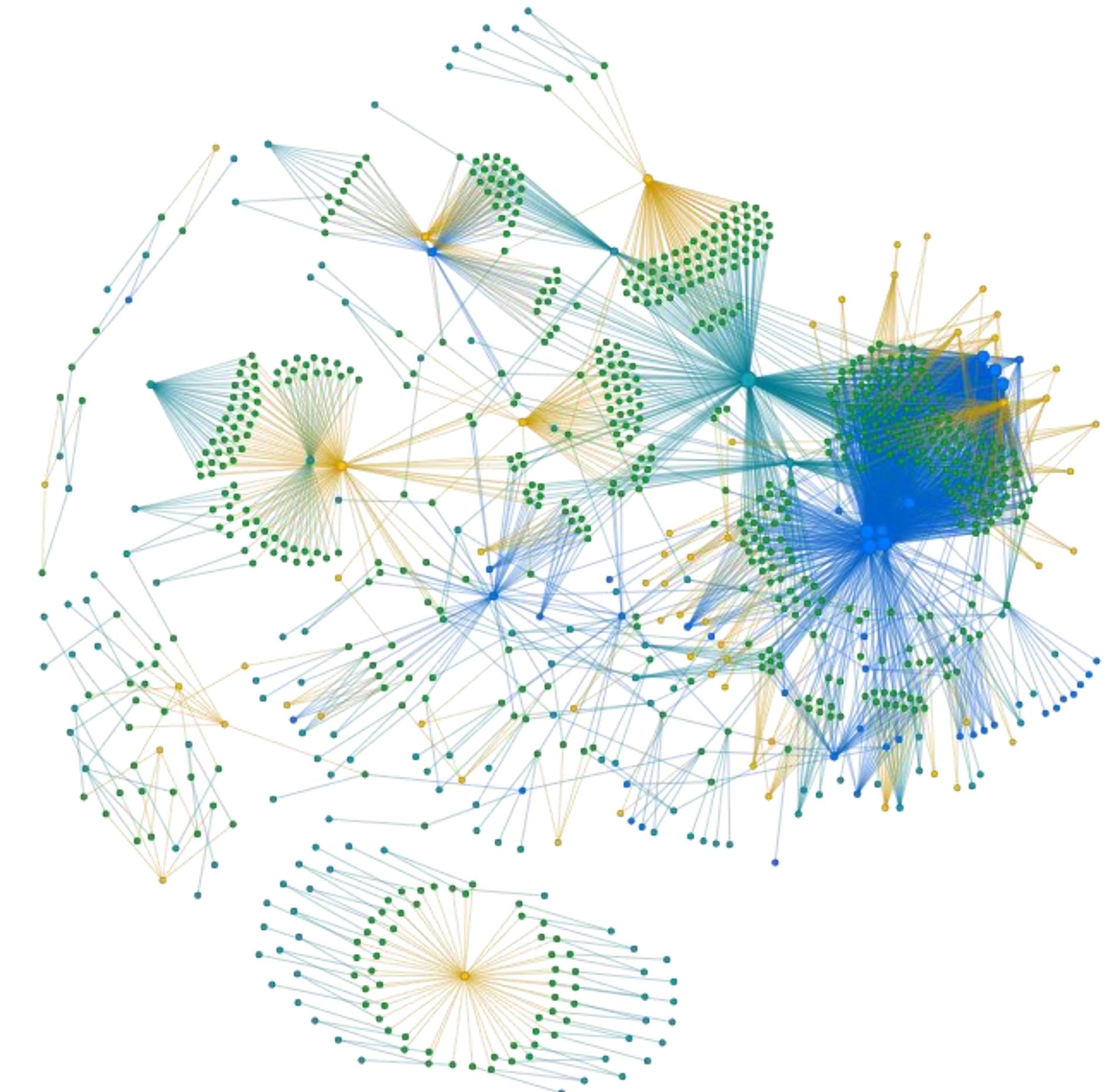


"A Framework for Effective Corporate Communication after Cyber Security Incidents", Jason R. C. Nurse

МОДЕЛЬ АДАПТИВНОЙ БЕЗОПАСНОСТИ



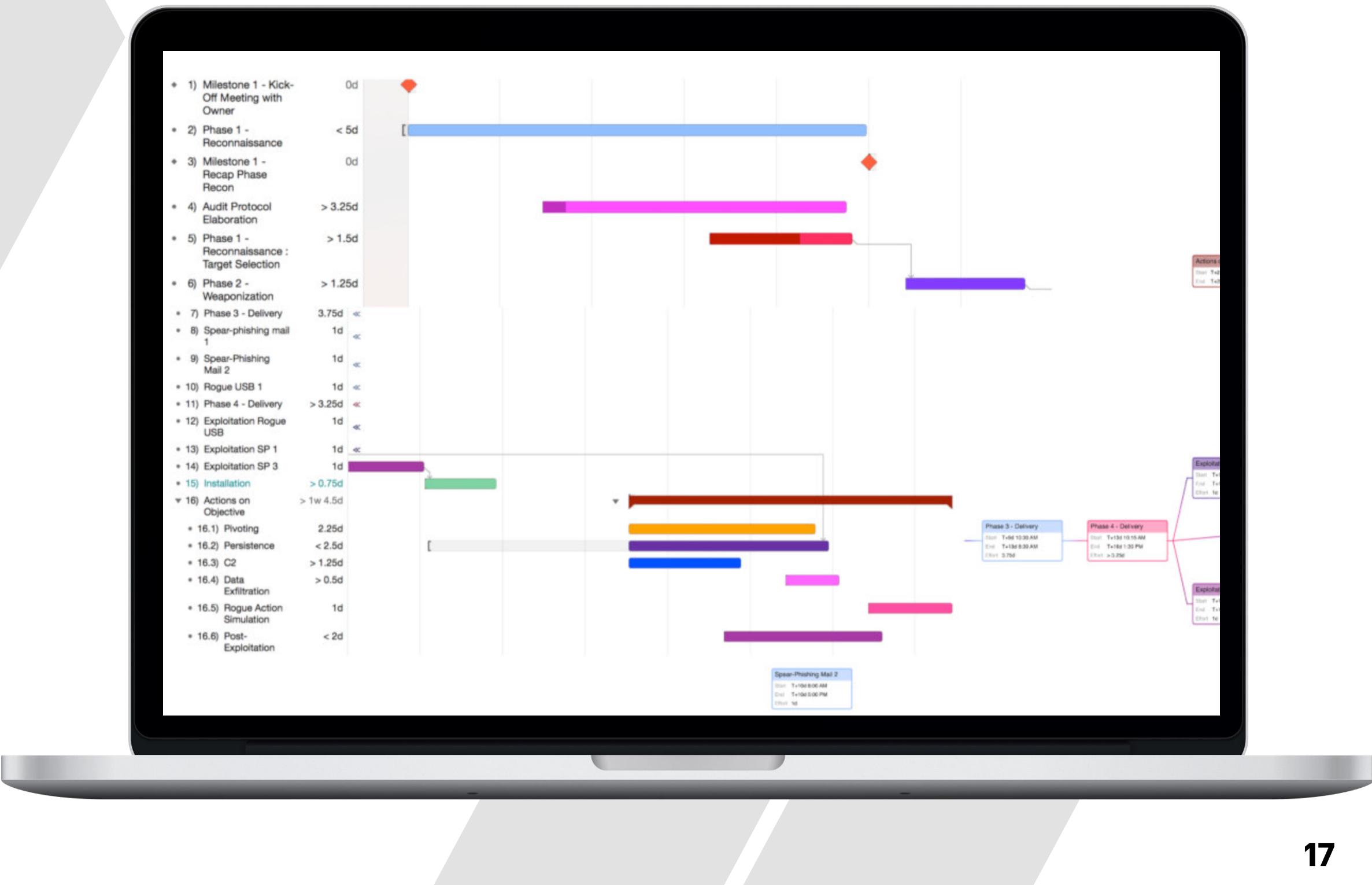
ОГРАНИЧЕНИЕ 1: ПОВЕРХНОСТЬ АТАКИ



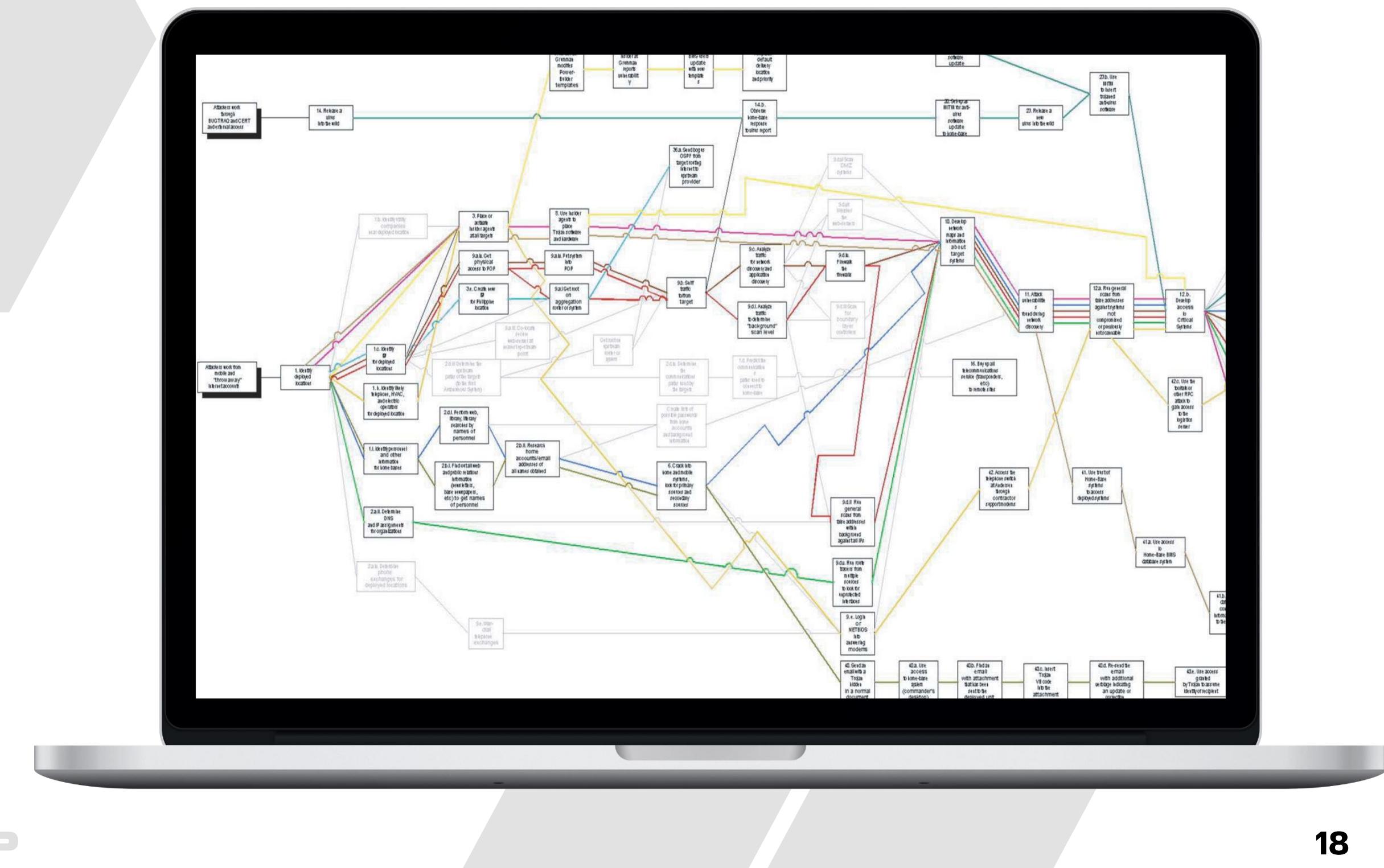
ОГРАНИЧЕНИЕ 2: РЕСУРС

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (6) Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (4) BITS Jobs Access Token Manipulation (5) Boot or Logon Autostart Execution (15) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Domain Policy Modification (2) Create or Modify System Process (4) Escape to Host Event Triggered Execution (15) External Remote Services Hijack Execution Flow (11) Implant Internal Image Modify Authentication Process (4) Office Application Startup (6) Pre-OS Boot (5) Scheduled Task/Job (6) Server Software Component (4) Traffic Signaling (1) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) BITS Jobs Access Token Manipulation (5) Boot or Logon Autostart Execution (15) Boot or Logon Initialization Scripts (5) Browser Extensions Create or Modify System Process (4) Domain Policy Modification (2) Create or Modify System Process (4) Escape to Host Event Triggered Execution (15) External Remote Services File and Directory Permissions Modification (2) Hijack Execution Flow (11) Implant Internal Image Modify Authentication Process (4) Office Application Startup (6) Pre-OS Boot (5) Scheduled Task/Job (6) Server Software Component (4) Traffic Signaling (1) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Forced Authentication Deploy Container Direct Volume Access Domain Policy Modification (2) Input Capture (4) Execution Guardrails (1) Exploitation for Defense Evasion Network Sniffing OS Credential Dumping (8) Hide Artifacts (9) Steal Application Access Token Steal or Forge Kerberos Tickets (4) Impair Defenses (9) Indicator Removal on Host (6) Valid Accounts (4) Indirect Command Execution Masquerading (7) Modify Authentication Process (4) Scheduled Task/Job (6) Server Software Component (4) Traffic Signaling (1) Valid Accounts (4) Unsecured Credentials (7) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (6) Pre-OS Boot (5) Process Injection (11) Reflective Code Loading Rogue Domain Controller Rootkit Signed Binary Proxy Execution (13) Signed Script Proxy Execution (1) Subvert Trust Controls (6) Template Injection Traffic Signaling (1) Trusted Developer Utilities Proxy Execution (1) Unused/Unsupported Cloud Regions Use Alternate Authentication Material (4) Valid Accounts (4) Virtualization/Sandbox Evasion (3) Weaken Encryption (2) XSL Script Processing	Adversary-in-the-Middle (2) Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (4) Network Sniffing OS Credential Dumping (8) Hide Artifacts (9) Steal Application Access Token Steal or Forge Kerberos Tickets (4) Impair Defenses (9) Indicator Removal on Host (6) Valid Accounts (4) Indirect Command Execution Masquerading (7) Modify Authentication Process (4) Scheduled Task/Job (6) Server Software Component (4) Traffic Signaling (1) Valid Accounts (4) Two-Factor Authentication Interception Unsecured Credentials (7) Modify Cloud Compute Infrastructure (4) Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (6) Pre-OS Boot (5) Process Injection (11) Reflective Code Loading Rogue Domain Controller Rootkit Signed Binary Proxy Execution (13) Signed Script Proxy Execution (1) Subvert Trust Controls (6) Template Injection Traffic Signaling (1) Trusted Developer Utilities Proxy Execution (1) Unused/Unsupported Cloud Regions Use Alternate Authentication Material (4) Valid Accounts (4) Virtualization/Sandbox Evasion (3) Weaken Encryption (2) XSL Script Processing	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Location Discovery (1) System Network Configuration Discovery (1) System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion (3)	Exploitation of Remote Services Adversary-in-the-Middle (2) Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Clipboard Data Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4) Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Exfiltration Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (1) Web Service (3)	Automated Exfiltration Data Trans Limits Exfiltration Alternative Protocol (3) Exfiltration Network M Exfiltration Physical M Scheduled Transfer D Cloud Acc	

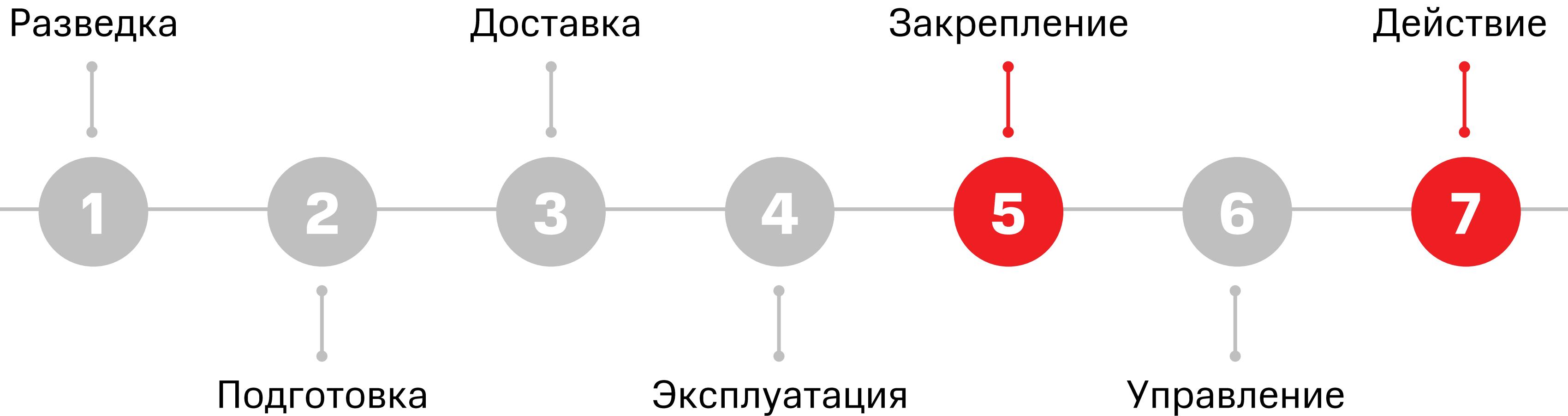
ОГРАНИЧЕНИЕ 3: КОММУНИКАЦИЯ



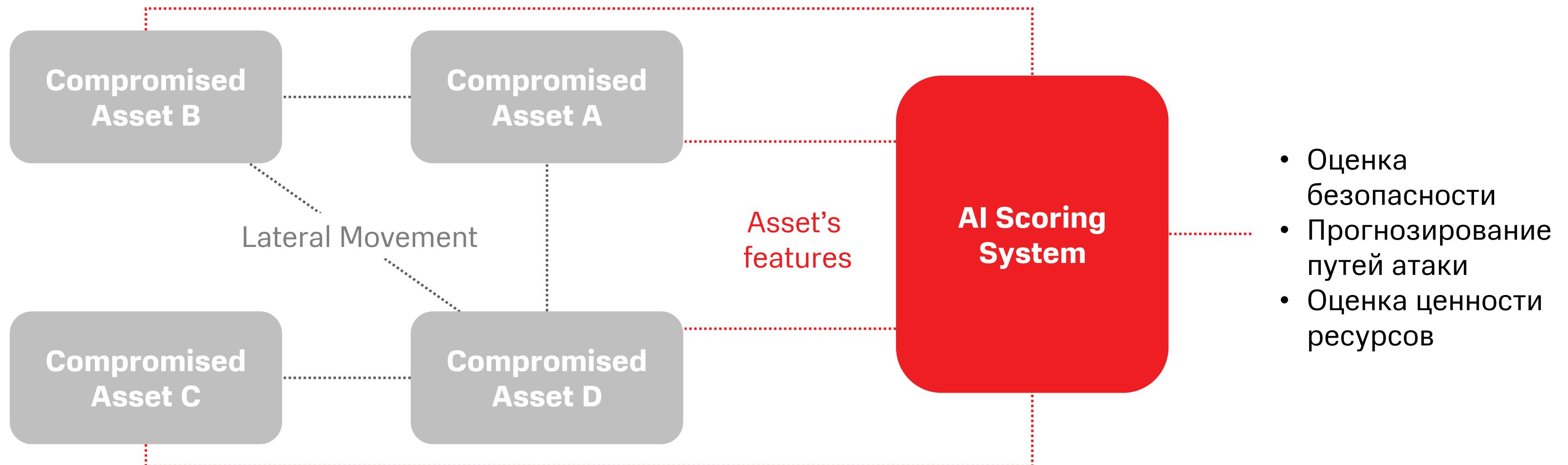
ОГРАНИЧЕНИЕ 4: АВТОМАТИЗИРОВАННЫЙ ИНСТРУМЕНТ



АТТАСК KILL CHAIN ТРЕБУЕТ ЧЕЛОВЕКА



ML ДЛЯ ОЦЕНКИ ЦЕННОСТИ РЕСУРСА









ПУТЬ ОТ БЕЗОПАСНОСТИ К УСТОЙЧИВОСТИ

**Задать вопрос экспертам
cybersecurity@mts.ru**