

BI.ZONE

Что делать, если кибератака все уничтожила и как этого избежать

Антон Степанов

Ведущий специалист по компьютерной криминалистике,
BI.ZONE DFIR



О спикере

BI.ZONE



Опыт

- В ИБ с 2006
- 8 лет проводил компьютерные экспертизы
- Расследую кибератаки о которых вы точно слышали и видели последствия
- Соавтор и преподаватель курса по Linux Forensics в академии INSECA
- Спикер профильных конференций (Positive Hack Days, OFFZONE, SOCTech, SOCForum и других)
- Сертифицированный специалист по компьютерной криминалистике

E-mail: **an.stepanov@bi.zone**

BI.ZONE — компания по управлению цифровыми рисками

От корпорации до стартапа, мы помогаем
организациям по всему миру безопасно
развивать бизнес в киберпространстве



1600+

реализованных
проектов



800+

защищенных
клиентов

О чем поговорим?

О чем поговорим?

BI.ZONE

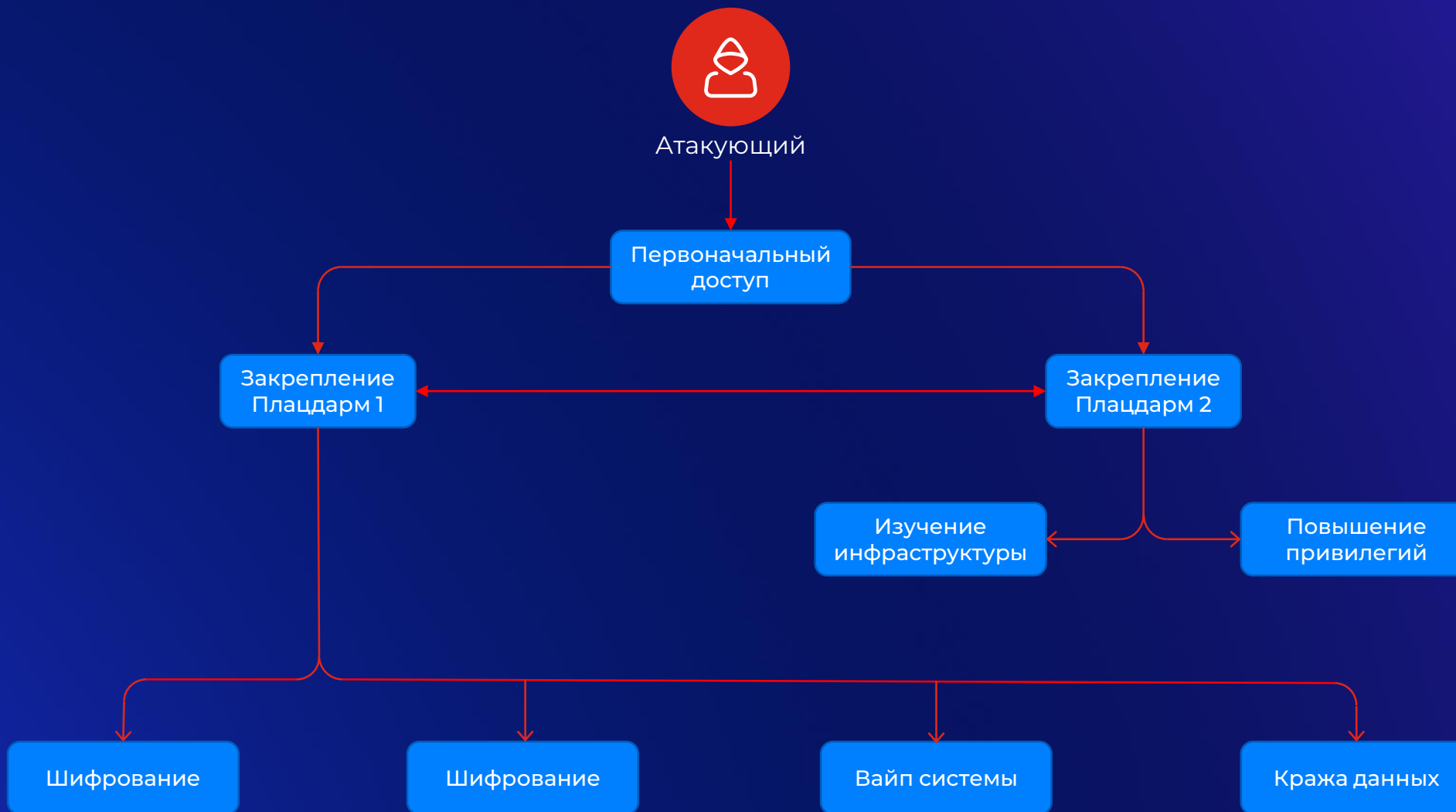
→ Что такое атака и как она происходит?

→ Мотивация атакующих

→ Как атака расследуется и для чего нужно расследование?

→ Как восстановиться и что требовать от внешнего вендора?

→ Что делать для предотвращения атак?



Начало атаки

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

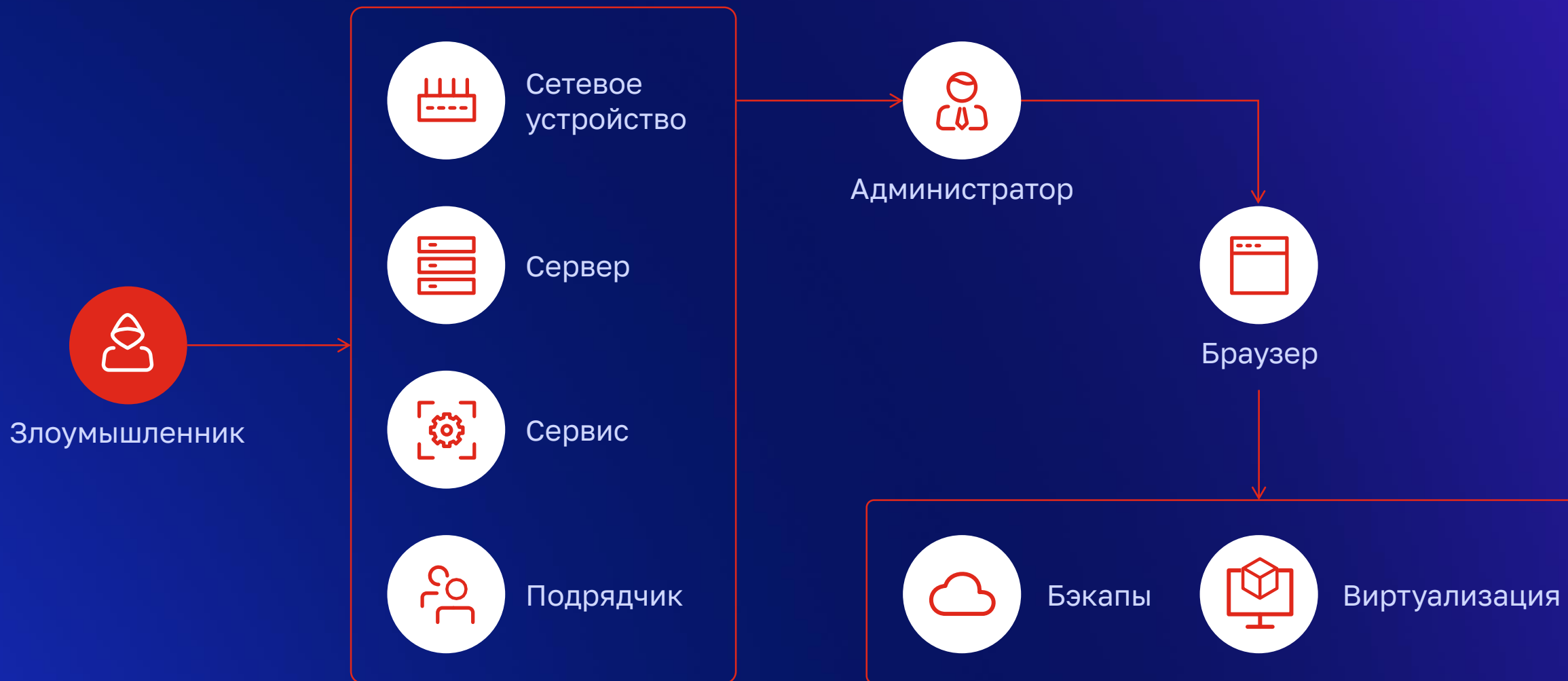
Конец атаки

Reconnaissance 12 techniques	Resource Development 9 techniques	Initial Access 11 techniques	Execution 20 techniques	Persistence 22 techniques	Privilege Escalation 13 techniques	Stealth 30 techniques	Defense Impairment 18 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (3)	Acquire Access	Content Injection	BITS Jobs	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Access Token Manipulation (5)	Disable or Modify System Firewall (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Cloud Administration Command	BITS Jobs	Access Token Manipulation (5)	BITS Jobs	Disable or Modify Tools (6)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Command and Scripting Interpreter (13)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Domain or Tenant Policy Modification (2)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (6)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Delay Execution	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Defacement (2)	Disruption of Service (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	ESXi Administration Command	Compromise Host Software Binary	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	File and Directory Permissions Modification (2)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Disk Wipe (2)	Email Bombing
Query Public AI Services	Generate Content (2)	Replication Through Removable Media	Exploitation for Client Execution	Create Account (3)	Create or Modify System Process (5)	Direct Volume Access	Modify Authentication Process (3)	Forge Web Credentials (2)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Endpoint Denial of Service (4)	Financial Theft
Search Closed Sources (2)	Obtain Capabilities (7)	Supply Chain Compromise (3)	Hijack Execution Flow (12)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Execution Guardrails (2)	Modify Cloud Compute Infrastructure (5)	Multi-Factor Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Inter-Process Communication (3)	Event Triggered Execution (18)	Escape to Host	Hide Artifacts (14)	Modify Cloud Resource Hierarchy	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (6)	Hide Infrastructure	Exfiltration Over Web Service (4)	Inhibit System Recovery
Search Open Websites/Domains (3)		Valid Accounts (4)	Input Injection	Exclusive Control	Event Triggered Execution (18)	Hijack Execution Flow (12)	Masquerading (12)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Network Denial of Service (2)
Search Threat Vendor Data		Wi-Fi Networks	Inter-Process Communication (3)	External Remote Services	Event Triggered Execution (18)	Indicator Removal (8)	Modify System Image (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Resource Hijacking (4)
Search Victim-Owned Websites			Native API	Implant Internal Image	Exploitation for Privilege Escalation	Indirect Command Execution	Obfuscated Files or Information (18)		File and Directory Discovery		Proxy (4)	Non-Application Layer Protocol		Service Stop
			Poisoned Pipeline Execution		Process Injection (12)	Masquerading (12)			Group Policy Discovery			Non-Standard Port		System
			Scheduled Task/Job (4)		Scheduled	Obfuscated Files or Information (18)			Local Storage Discovery			Protocol Tunneling		

attack.mitre.org

Типовая атака

BI.ZONE



Основные способы проникновения в инфраструктуру



64%

Фишинг



18%

Службы
удаленного
доступа



9%

Подрядчики



Шпионаж

- В сети находятся настоящие джентльмены
- Как правило, не влияют на бизнес



Финансовая мотивация

- Могут использовать инфраструктуру в своих целях
- Обратимое уничтожение

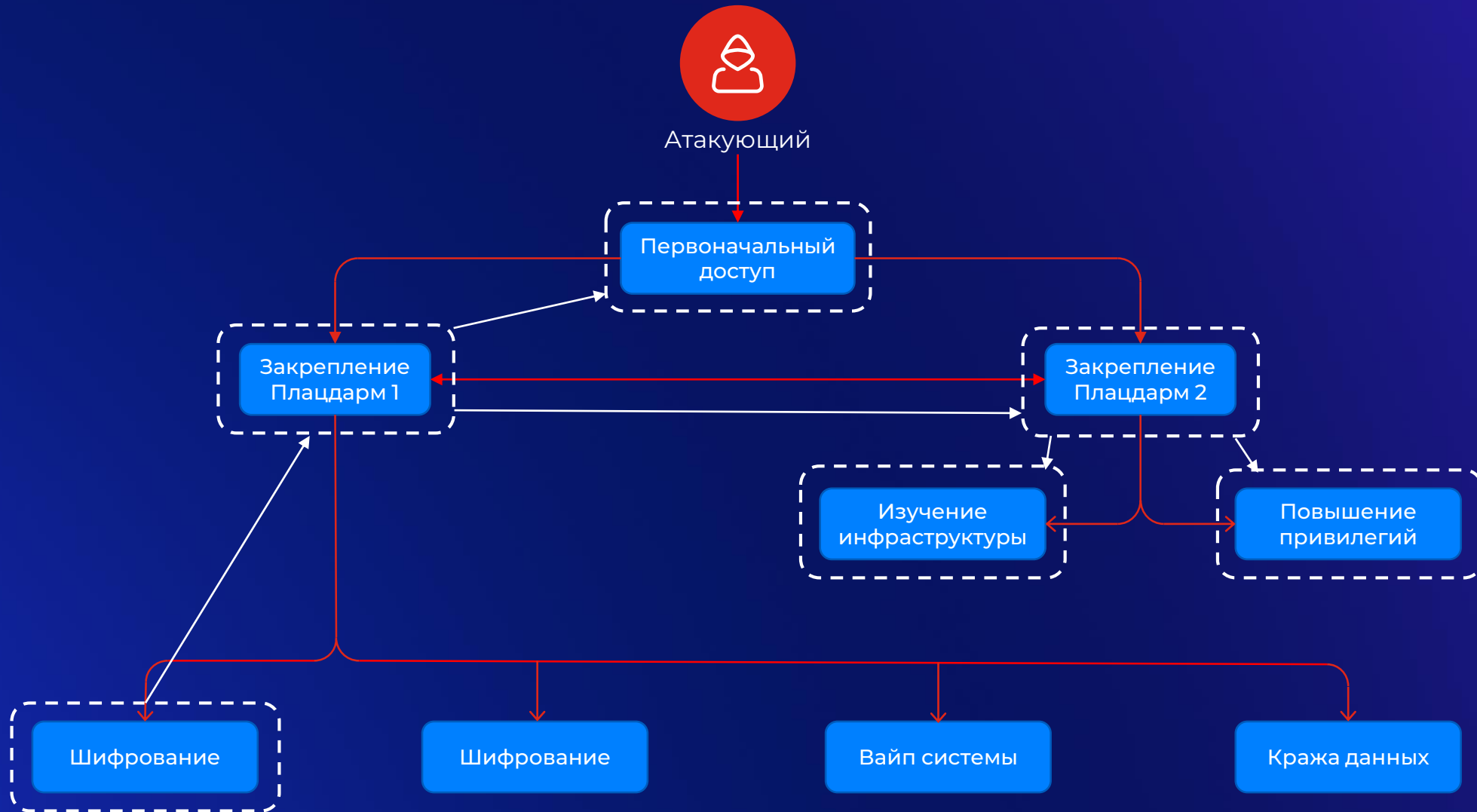


Хактивизм

- Непредсказуемы
- Могут безвозвратно уничтожить всю инфраструктуру

Платить или нет?

Как расследуют атаку?



Восстановление

Даже если у вас есть план, все пойдет не по плану

Обязательно всплывет версия с инсайдером

Будет сложно и тяжело

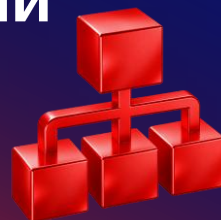
Бизнес



Проблемы

- Ничего не работает
- Оборота нет
- Клиентские системы уничтожены

Технический



Проблемы

- Инфраструктуры больше нет
- Никто точно не знает, как все работало
- Нет понимания, с чего начать

Управленческий



Проблемы

- Коллапс управления
- Нет плана
- Стресс неопределенности
- Нет лидера



Размытые роли

- Несколько конфликтующих центров принятия решений
- Бутылочные горлышки при принятии решений



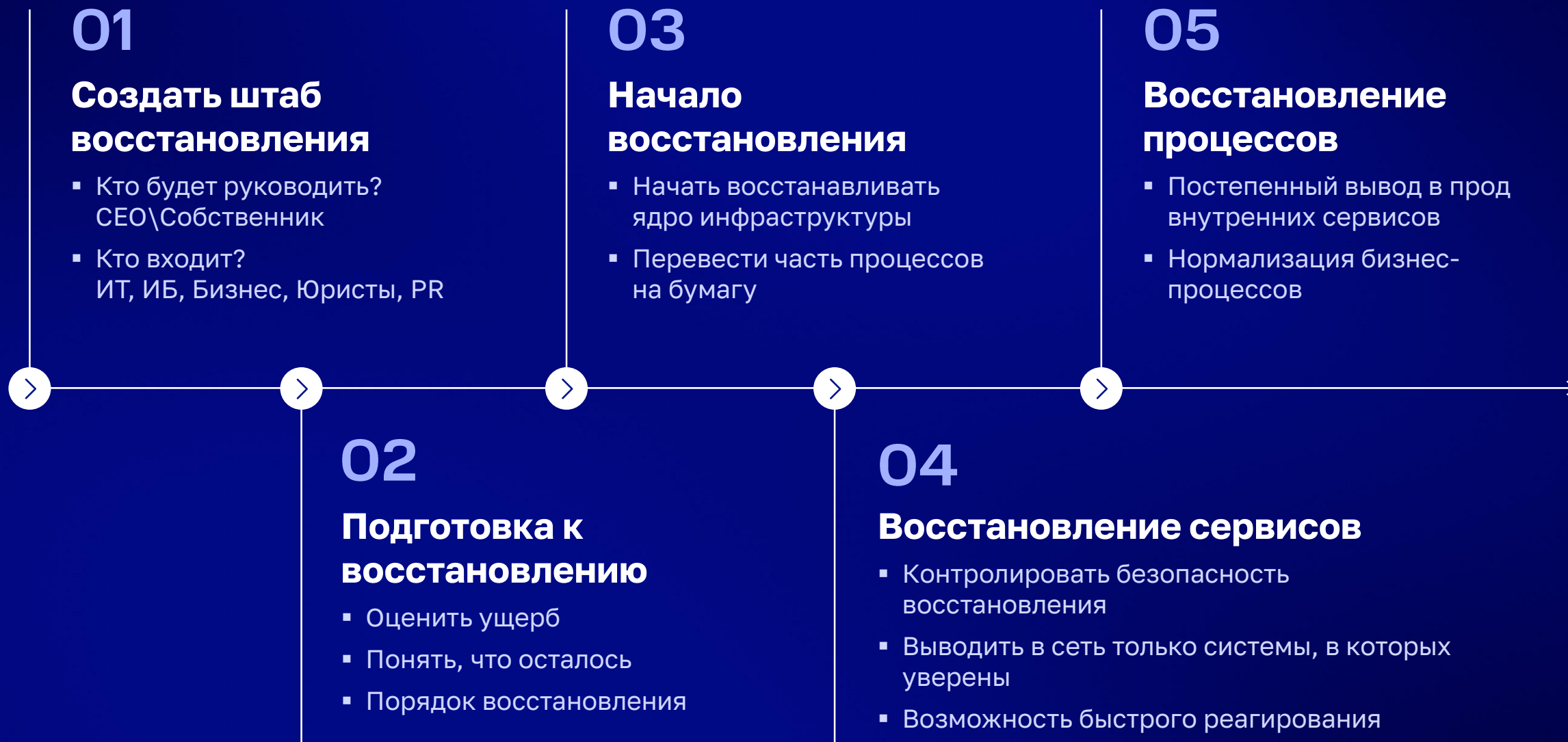
Неопределенность

- Нет полной картины
- Информация меняется каждый час (минуты)



Нехватка ресурсов

- Высокая конкуренция за ресурсы
- Неэффективный менеджмент существующих ресурсов



Организация восстановления

BI.ZONE

	Старт работ		Восстановление		Прод	
Бизнес	Определить зависимости систем	Порядок восстановления систем	Переход «на бумагу»		Восстановление процессов	
ИТ		Анализ бэкапов	Восстановление ядра	Восстановление сервисов		
ИБ			Контроль чистоты систем и МОНИТОРИНГ			
		Расследование (своими силами или внешним вендором)				
PR и юристы	Формирование PR-стратегии для взаимодействия с работниками, подрядчиками, клиентами, СМИ. Оценка и реагирование на юридические риски					

Гайд BI.ZONE по коммуникациям в кризисных ситуациях



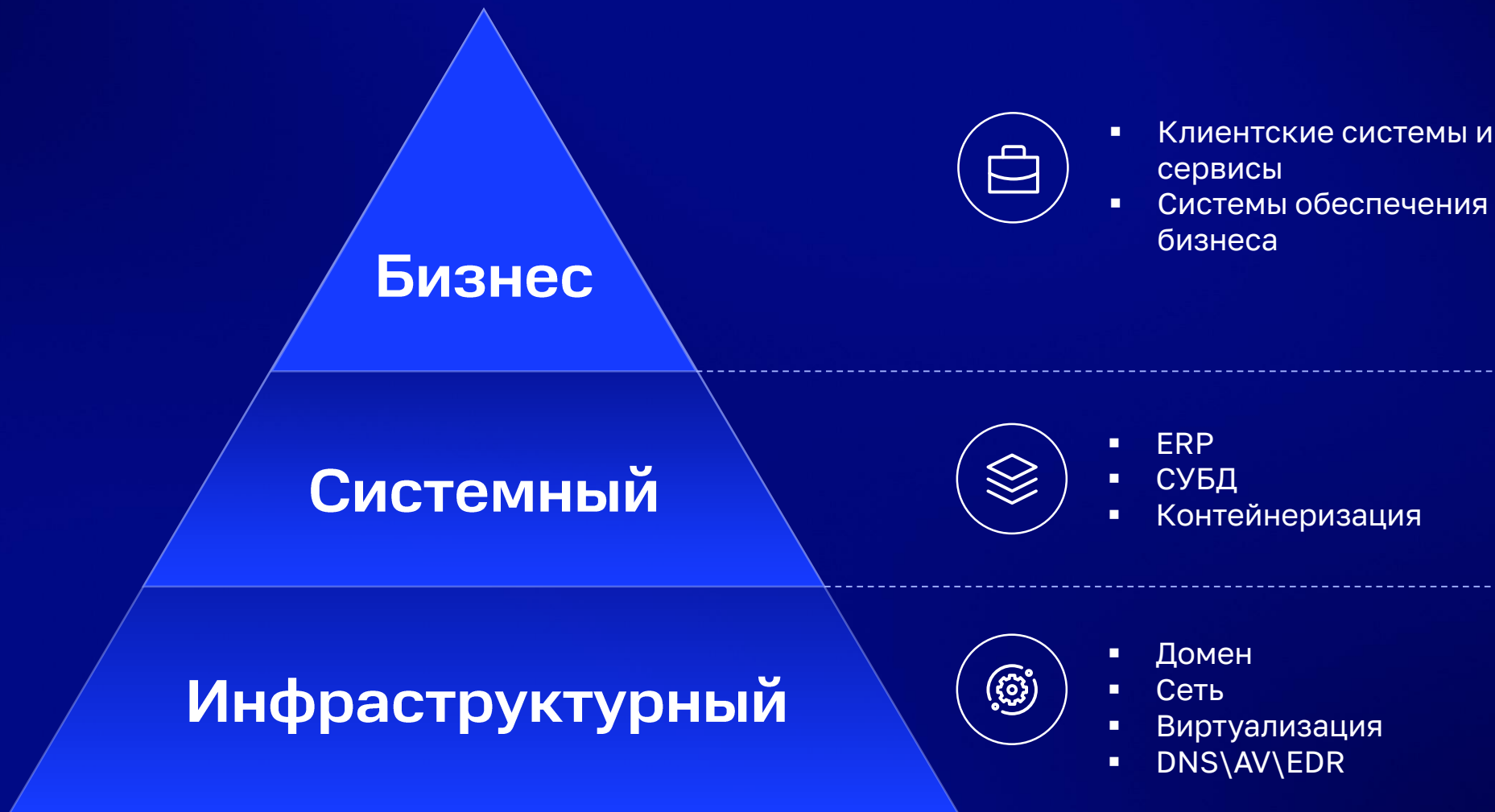
Кейс BI.ZONE. Как мы справились с негативом в публичном поле

30 апреля 2023 года в одном из телеграм-каналов появился пост с утверждением о том, что сайты некоторых публичных мероприятий BI.ZONE взломали. Мы немедленно запустили реагирование на инцидент и расследование. Анализ показал, что инцидент не стал критичным, не затронул инфраструктуру компании и клиентов.

Что мы сделали для отработки негатива в публичном поле:

- В течение двух часов после публикации выложили пост в корпоративном телеграм-канале и объяснили, что инфраструктура BI.ZONE и ее клиентов не пострадала.
- Донесли эту информацию до крупных отраслевых СМИ. Благодаря этому вышли новости с заголовками, транслирующими нашу позицию.
- В ночь с 30 апреля на 1 мая выложили в корпоративном телеграм-канале новость с обновленной информацией о ходе расследования.
- 30 апреля и 1 мая активно общались с клиентами и не зафиксировали ни одной вспышки негатива.
- 2 мая выложили результаты расследования с подробным описанием его хода на «Хабре» и итоговый пост в корпоративном [телеграм-канале](#).

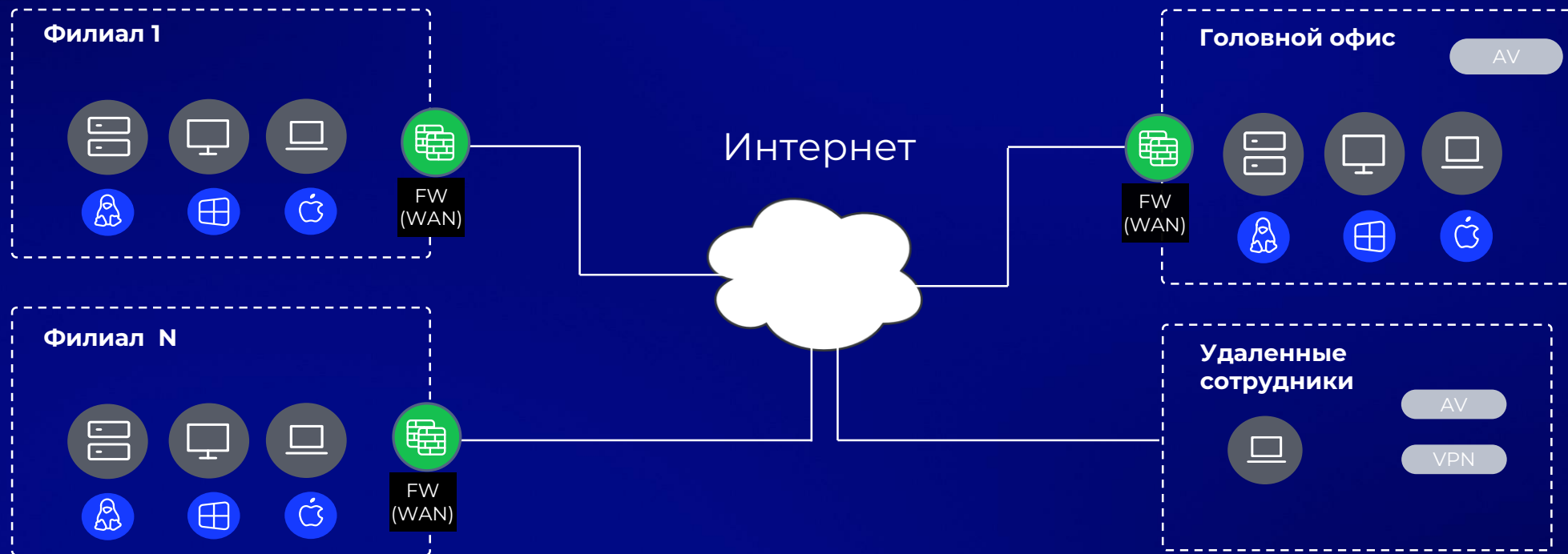
Быстрое реагирование на инцидент, открытое взаимодействие с клиентами и аудиторией позволили нам избежать неприятных последствий для репутации. Более подробно о том, что мы делали и как вели расследование, можно почитать [в нашем блоге](#).



Внешний вендор

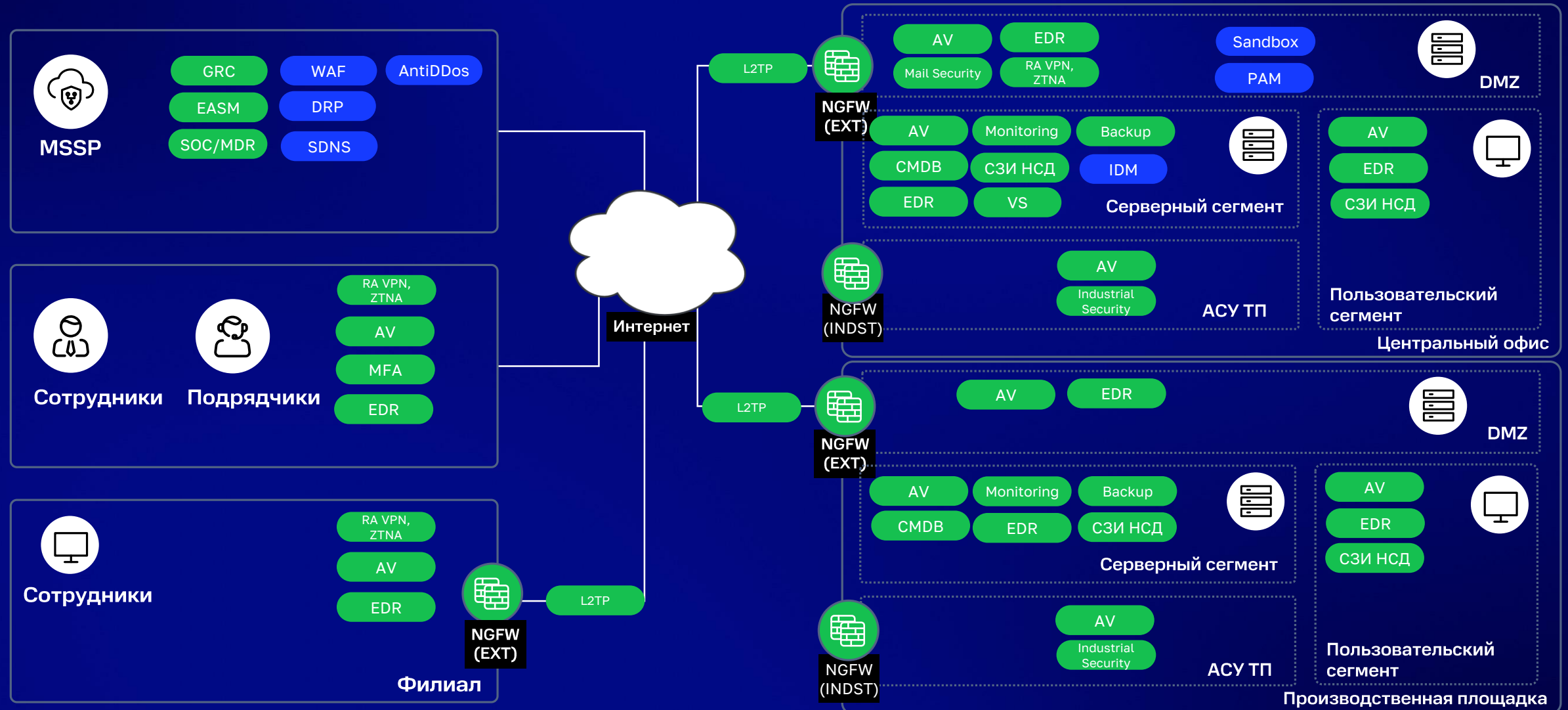
Путь от этого...

BI.ZONE



... К ЭТОМУ ...

BI.ZONE



... нужно пройти под контролем

BI.ZONE



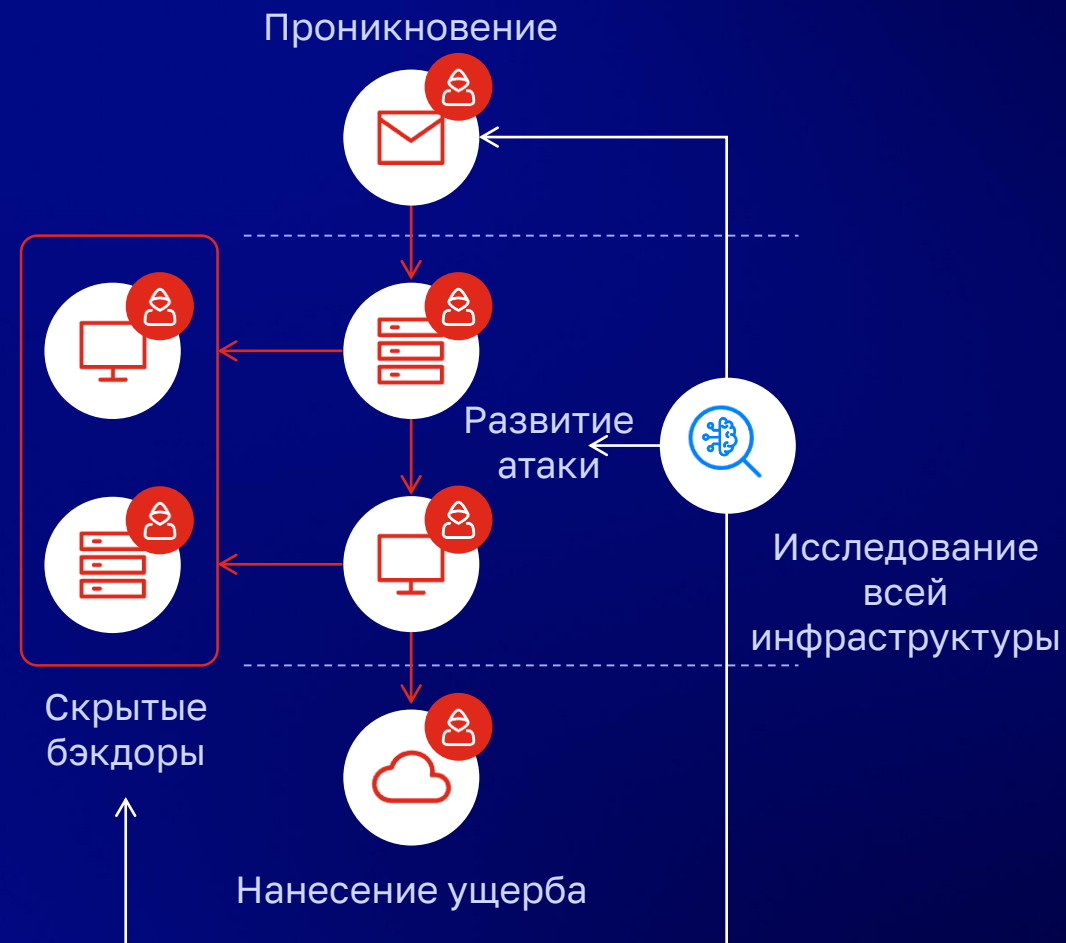
Расширенное реагирование

BI.ZONE

Классическое реагирование

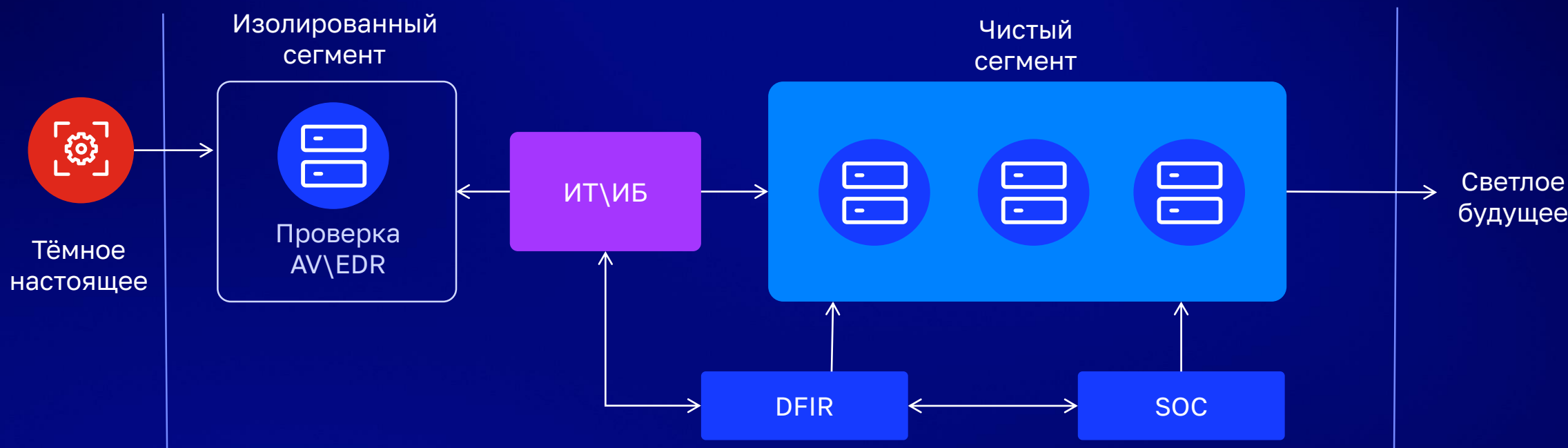


Расширенное реагирование



Роль внешнего вендора

BI.ZONE



Помощь с проверкой систем



Постоянный мониторинг



Методологическая помощь



Контроль чистоты



Реагирование



Рекомендации по защите

Рекомендации

Проанализируйте свою инфраструктуру и подготовьте план DRP

Неприятности случаются. Даже с вами. Нужно к ним подготовиться

Проведите учения

Когда план готов, проведите реальные учения по восстановлению одной или нескольких систем. В процессе появится много новых вводных для улучшения плана и процесса.

Учения необходимо проводить периодически, чтобы никто не забыл, как действовать

Протестируйте план «на бумаге»

Когда план готов, соберите все службы и попробуйте проговорить все действия. Скорректируйте «острые углы» и опишите новые вводные

Пока инцидент не случился, модернизируйте инфраструктуру

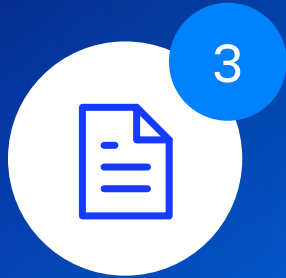
Проверьте свою инфраструктуру на соответствие требованиям ИБ и на слабые места



3-2-1

Резервное копирование «3-2-1»

BI.ZONE



Три резервные
копии данных



Два разных типа
носителя



Одна копия —
в удаленном
хранилище
(вне офиса)

01

Анализ активов и
периметра

02

Сегментация сети

03

Особое внимание
системам АВПО, РАМ,
бэкапы, виртуализация

04

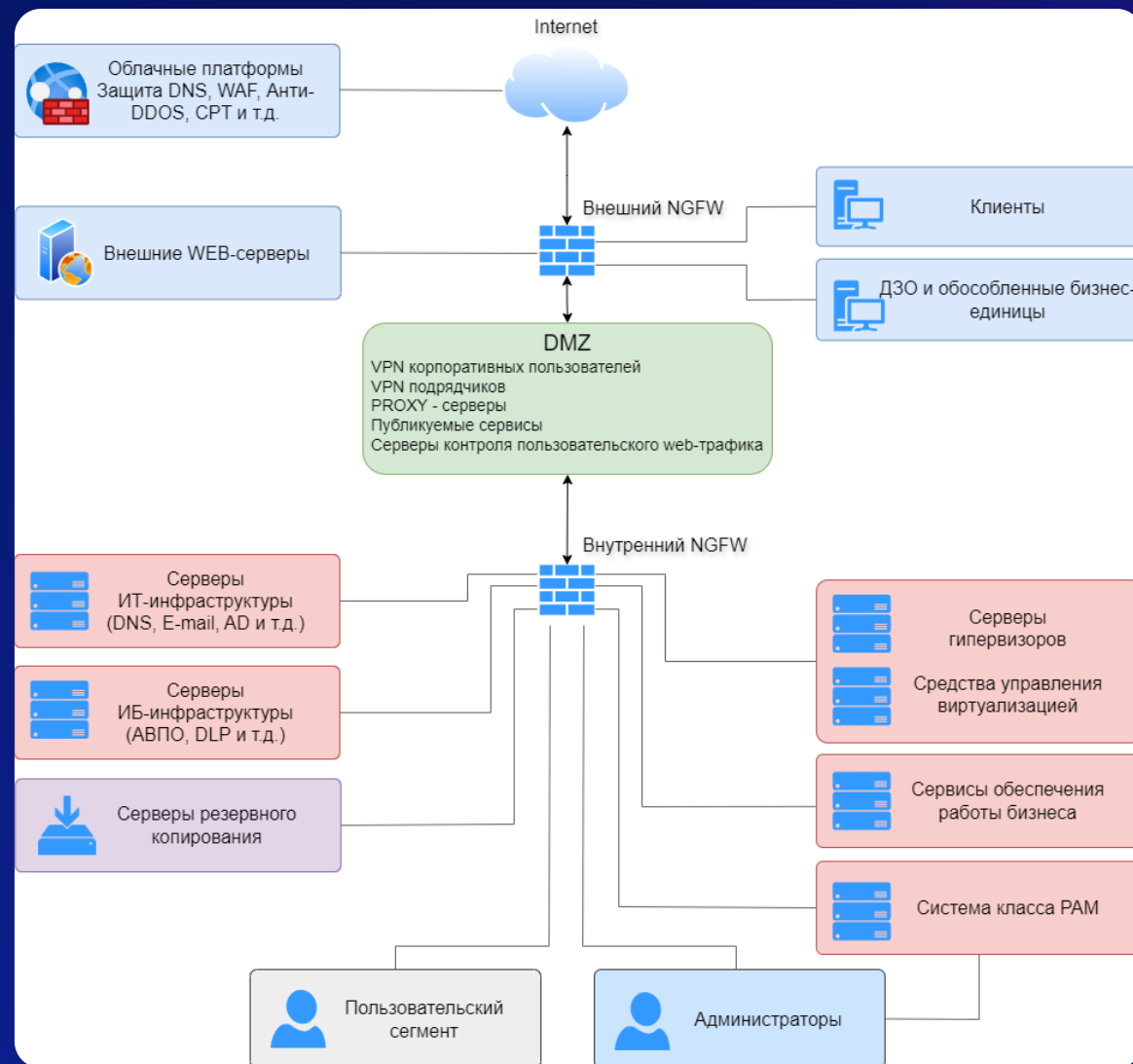
Мониторинг
инфраструктуры

05

Второй фактор везде, где
это возможно. На
периметре - обязательно

06

Контроль подрядчиков



Безопасность –

ЭТО ПРОЦЕСС,

а не состояние

BI.ZONE

Спасибо!
Вопросы?



Сервис DFIR BI.ZONE



@BI_ZONE_DFIR

Оперативный чат в
Telegram в случае
инцидента

Sale BI.ZONE: **Анна Наумочкина**

+7 916 307 9765

@AnnaNaumochkina