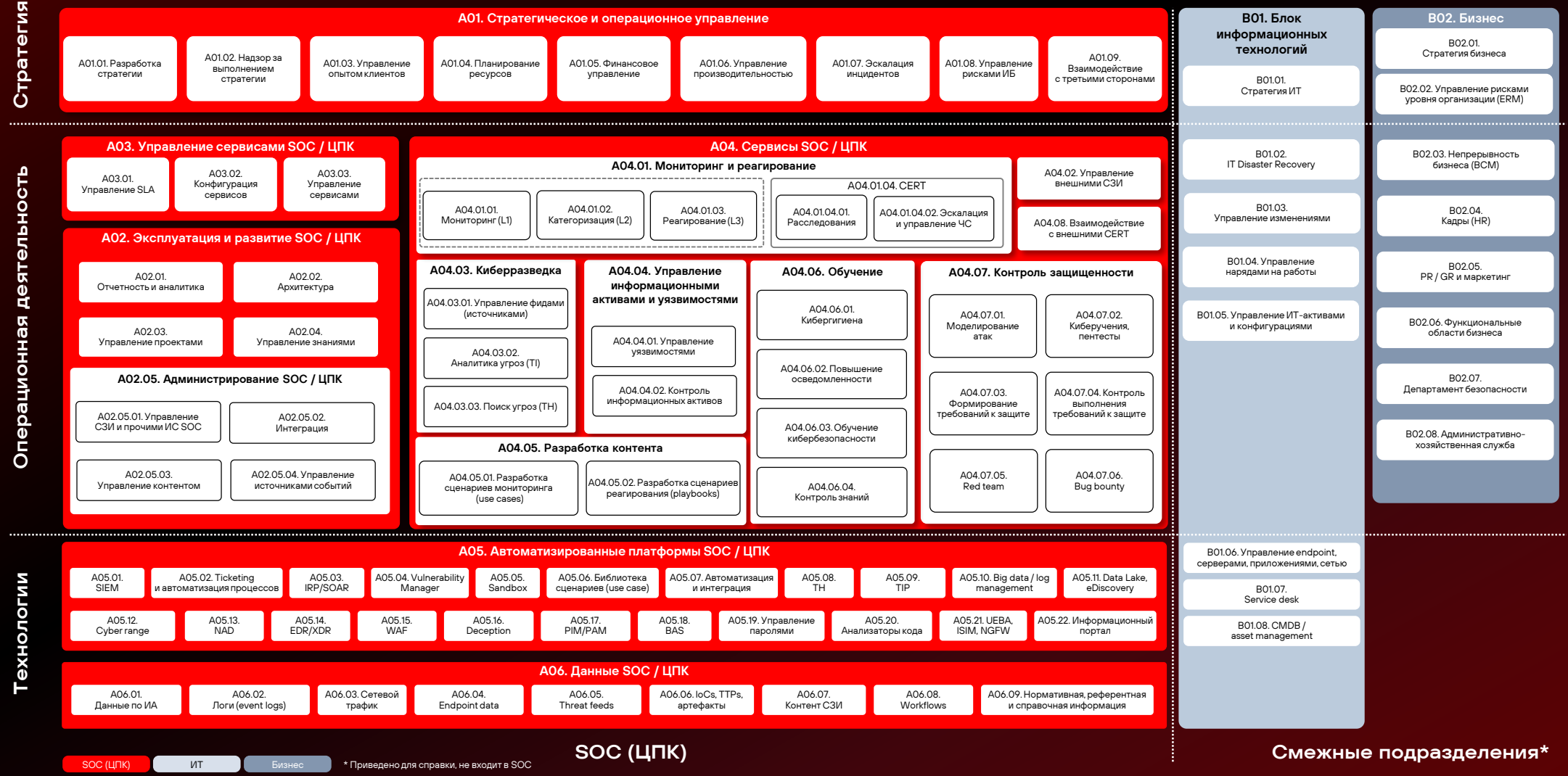
Архитектура сетевой безопасности современного предприятия – былое и думы

Михаил Кадер

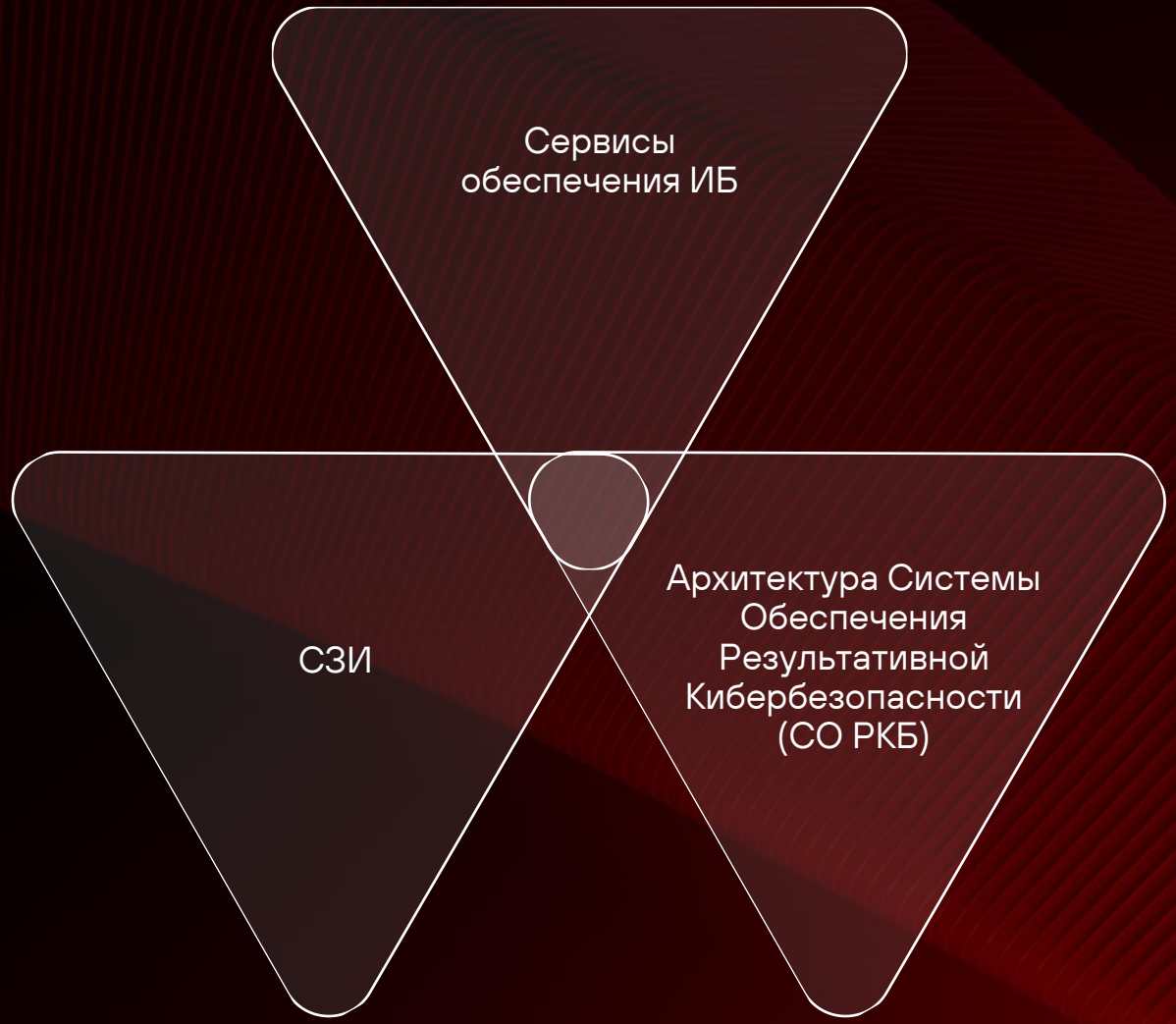
Архитектор решений по информационной безопасности

Операционная модель ИБ

(один из возможных вариантов)



Основные составляющие



Архитектура – это не ново ☺

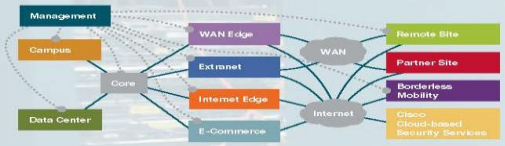
pt

The Cisco **SAFE Security** Reference Architecture

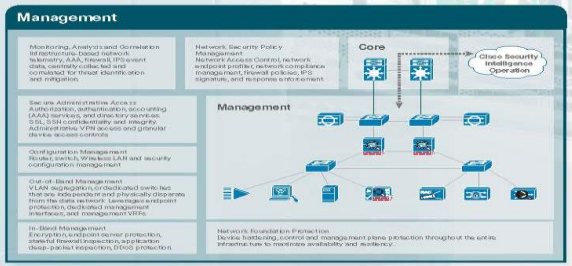
The Foundation for Secure Borderless Networks

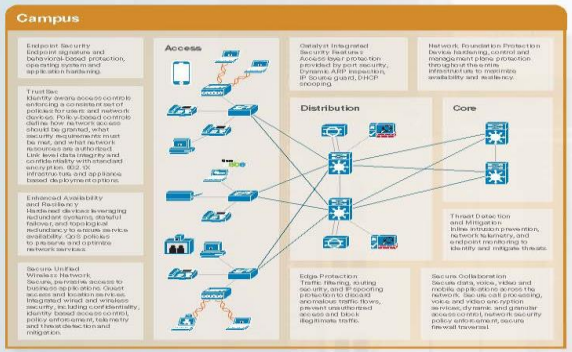
Cisco® SAFE is a security reference architecture that provides detailed design and implementation guidelines to assist organizations looking to build highly secure and reliable networks. SAFE's modular designs take advantage of cross-platform network intelligence and collaboration between Cisco security and network devices, to better address the unique security requirements of every part of the network. The SAFE designs also integrate Cisco cloud-based security services, offering flexible deployment options, as well as global threat correlation and response. The result is persistent protection and the consistent enforcement of context-aware security policies for all types of users. This provides greater visibility into device and network security events, and enhanced control of users, devices, and traffic for coordinated threat response. SAFE's comprehensive security strategy improves an organization's ability to identify, prevent, and respond to threats, and securely deploy critical business applications and services.

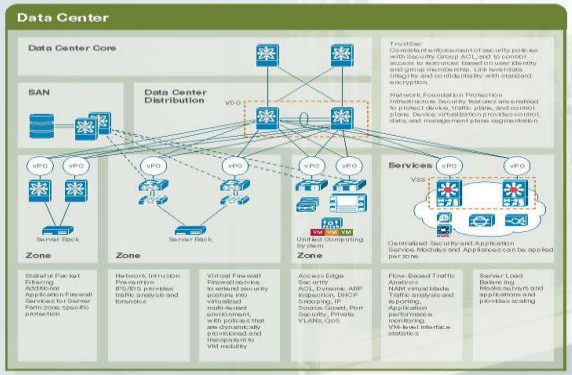
High-Level View

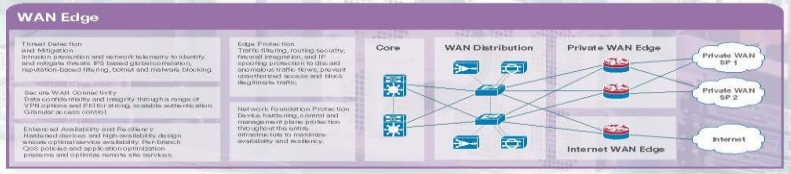


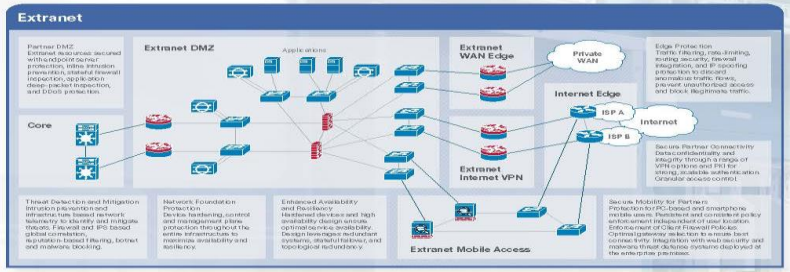
Icon Key

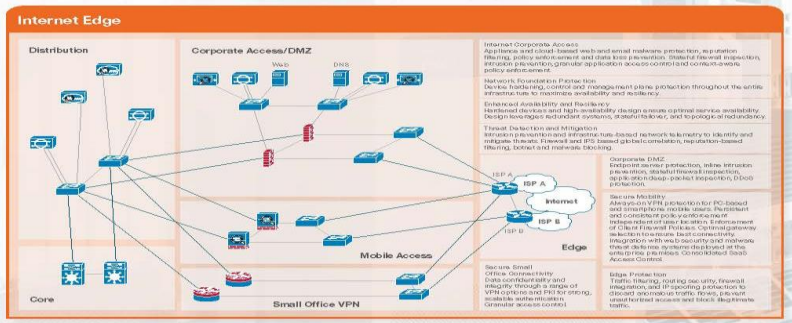


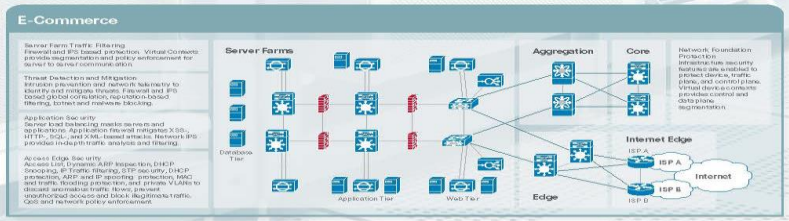




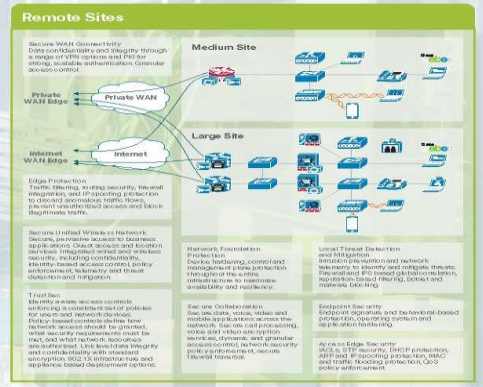


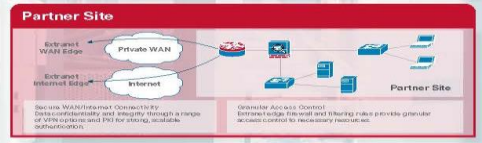


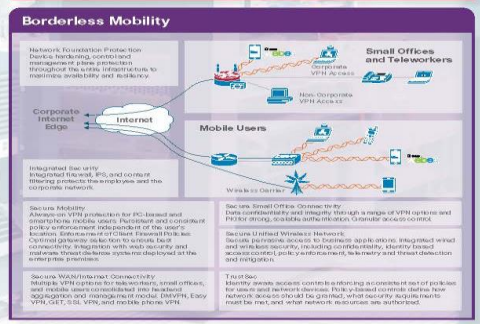


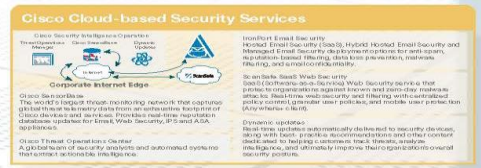


For More Information
› cisco.com/go/safe › cisco.com/go/security









Целеполагание СО РКБ

Обнаружить

- Увидеть
- Понять
- Проанализировать

Остановить

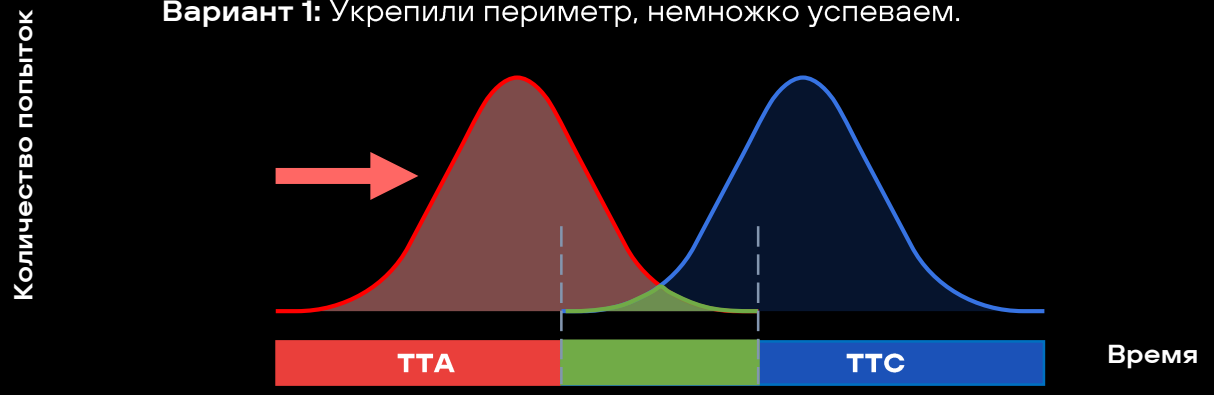
- Реагировать
- Взаимодействовать
- Уведомлять

Немного о метриках

Исходный случай: всегда опаздываем.

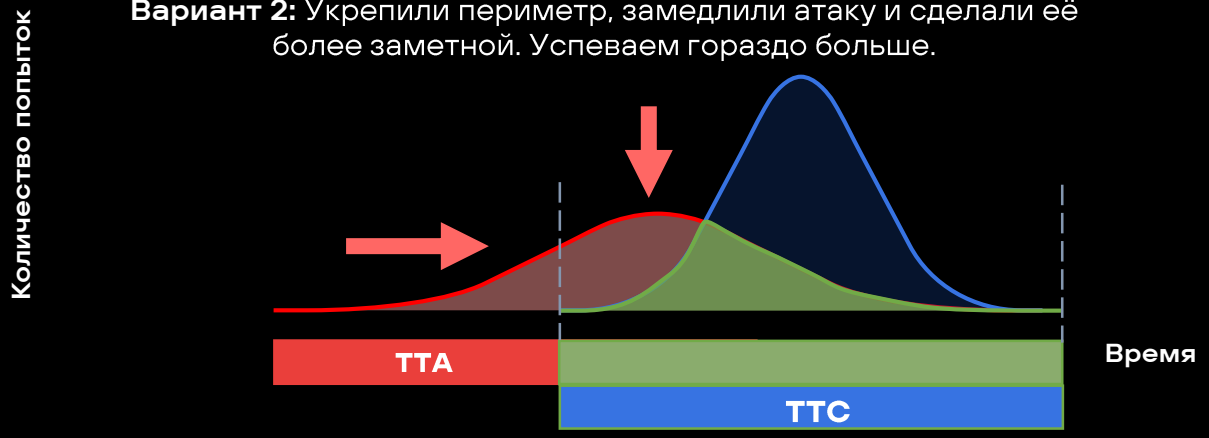
Атакующий всегда достигает своей цели, реагирование происходит слишком поздно.

Вариант 1: Укрепили периметр, немножко успеваем.



Замедлили атаку на периметре (атакующему надо долго вести разведку и предпринимать неоднократные попытки проникновения).

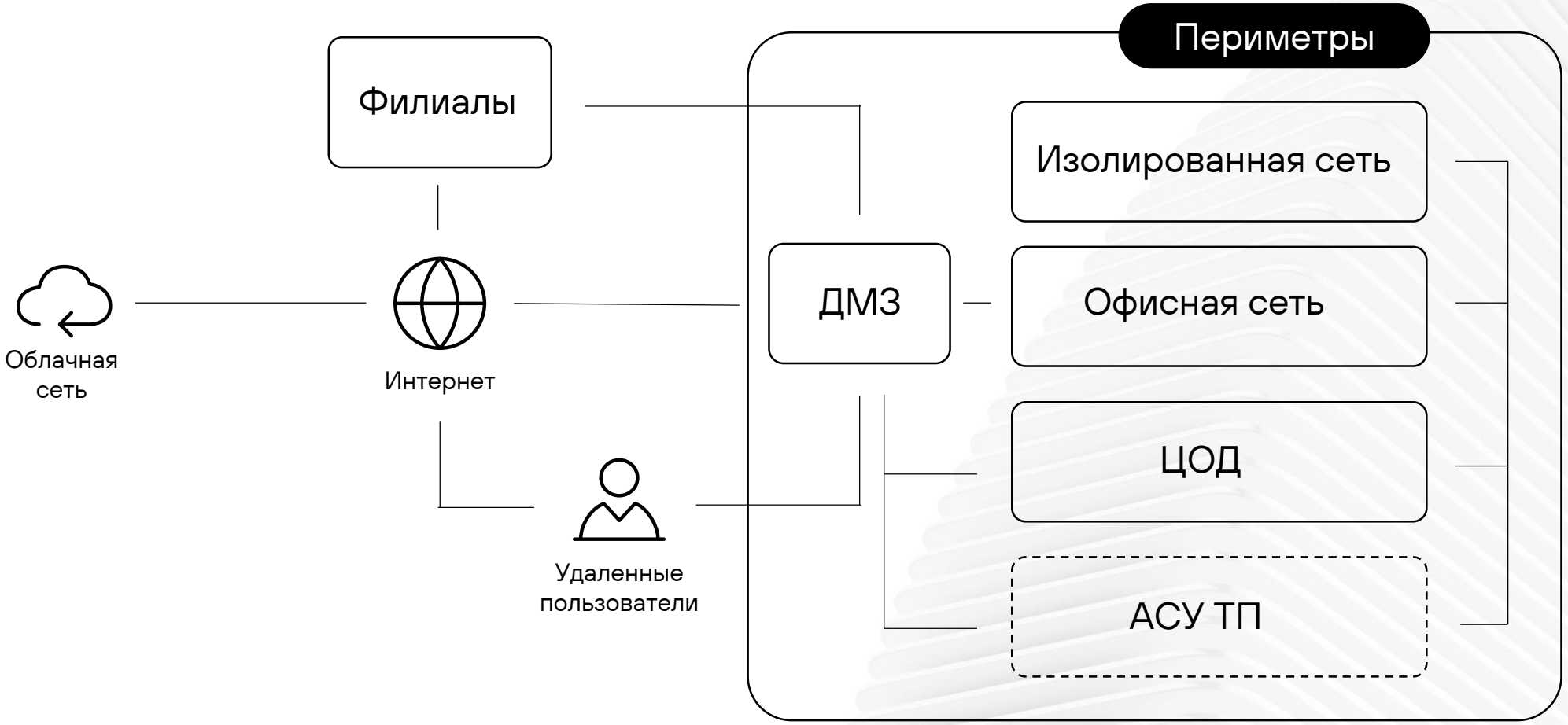
Вариант 2: Укрепили периметр, замедлили атаку и сделали её более заметной. Успеваем гораздо больше.



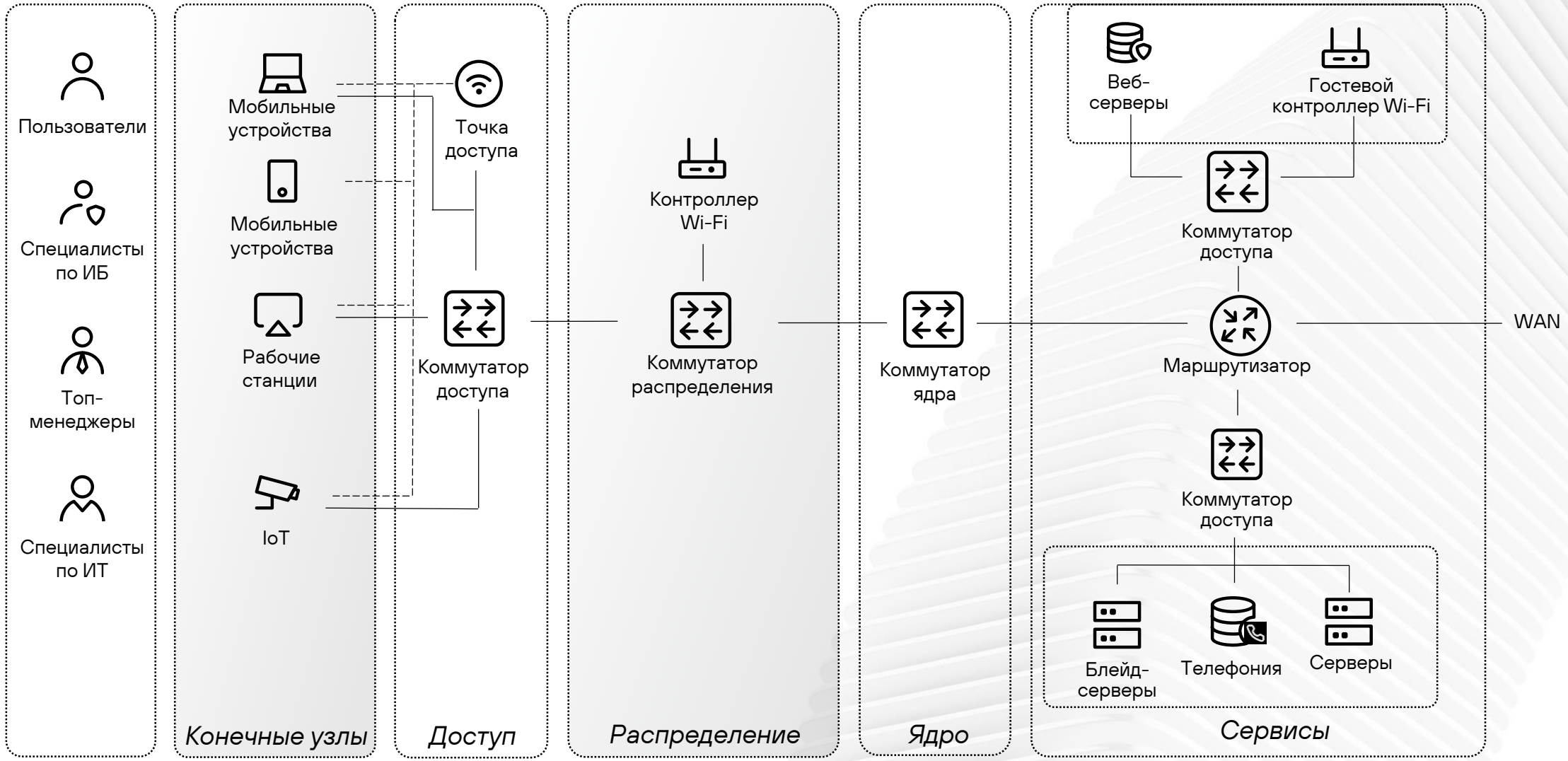
Замедлили атаку на периметре (атакующему надо долго вести разведку и предпринимать неоднократные попытки проникновения).

Задача – достижение и поддержание состояния инфраструктуры, при котором реализация недопустимого события максимально затруднена**,** а заметность атаки повышается настолько, что реагирование может быть проведено до начала реализации недопустимого события.

Основные модули инфраструктуры предприятия



Офисная сеть



Этапы атаки

Этап проникновения

- Внешняя разведка
- Взлом сервиса на периметре (эксплуатация уязвимости)
- Фишинг
- Атаки через Wi-Fi
- Получение доступа с помощью украденной или скомпрометированной учетной записи
- Компрометация цепочки поставок
- Компрометация доверенной инфраструктуры (например, VPN)

Развитие атаки

- Закрепление в инфраструктуре
- Разведка внутри инфраструктуры (как сетевой, так и доменной)
- Повышение привилегий — как локальных, так и в целом в инфраструктуре
- Передвижение по инфраструктуре
- Взлом ключевых систем

Нанесение ущерба

- Уничтожение данных и (или) систем
- Кража данных
- Взлом целевых систем (кража денег, нарушение производственного процесса и т. д.)

Тепловая карта MITRE ATT&CK

Визуализация наиболее популярных техник и подтехник, которые используют эксперты Positive Technologies.

Initial Access		Execution		Persistance		Privilege Escalation		Defense Evasion		Credential Access		Discovery		Lateral Movement		Collection		Command and Control	
Exploit Public-Facing Application		Command and Scripting Interpreter	JavaScript	Account Manipulation	SSH Authorized Keys	Abuse Elevation Control Mechanism	Sudo and Sudo Caching	Access Token Manipulation	Create Process with Token	Adversary-in-the-Middle	ARP Cache Poisoning	Account Discovery	Domain Account	Exploitation of Remote Services		Adversary-in-the-Middle	ARP Cache Poisoning	Application Layer Protocol	Web Protocols
External Remote Services			PowerShell	Create Account	Domain Account	Access Token Manipulation	Create Process with Token		SID-History Injection		LLMNR/NBT-NS Poisoning and SMB Relay		Email Account	Lateral Tool Transfer			LLMNR/NBT-NS Poisoning and SMB Relay	Data Encoding	Non-Standard Encoding
Phishing			Python		Local Account		SID-History Injection		Token Impersonation/Theft	Brute Force	Credential Stuffing		Local Account	Remote Service Session Hijacking	SSH Hijacking	Archive Collected Data	Archive via Utility		Standard Encoding
Supply Chain Compromise	Compromise Software Dependencies and Development Tools		Unix Shell	External Remote Services			Token Impersonation/Theft	Deobfuscate/Decode Files or Information			Password Cracking	Cloud Infrastructure Discovery		Remote Services	Distributed Component Object Model	Data from Configuration Repository	Network Device Configuration Dump	Encrypted Channel	Asymmetric Cryptography
Valid Accounts	Default Accounts		Windows Command Shell	Scheduled Task/Job	At	Domain Policy Modification	Group Policy Modification	Domain Policy Modification	Group Policy Modification		Password Guessing	Container and Resource Discovery				Remote Desktop Protocol		SNMP (MIB Dump)	Ingress Tool Transfer	
	Domain Accounts	Container Administration Command			Scheduled Task	Exploitation for Privilege Escalation		Exploitation for Defense Evasion			Password Spraying	Domain Trust Discovery			SMB/Windows Admin Shares	Data from Information Repositories	Code Repositories	Protocol Tunneling	
	Local Accounts	Exploitation for Client Execution		Server Software Component	Web Shell	Scheduled Task/Job	At	Impair Defenses	Disable or Modify System Firewall	Credentials from Password Stores	Password Managers	File and Directory Discovery			SSH		Confluence	Proxy	External Proxy
		Scheduled Task/Job	At	Valid Accounts	Default Accounts		Scheduled Task		Downgrade Attack	Exploitation for Credential Access		Group Policy Discovery			VNC		Sharepoint		Internal Proxy
			Scheduled Task		Domain Accounts	Valid Accounts	Default Accounts	Indicator Removal on Host	File Deletion	Forced Authentication		Network Service Discovery		Software Deployment Tools		Data from Local System		Remote Access Software	
		Software Deployment Tools			Local Accounts		Domain Accounts	Indirect Command Execution		Forge Web Credentials	Web Cookies	Network Share Discovery		Use Alternate Authentication Material	Pass the Hash				
							Local Accounts	Masquerading	Double File Extension	OS Credential Dumping	/etc/passwd and /etc/shadow	Network Sniffing			Pass the Ticket				
									Masquerade Task or Service		Cached Domain Credentials	Password Policy Discovery			Web Session Cookie				
								Modify Registry			DCSync	Permission Groups Discovery	Domain Groups						
								Use Alternate Authentication Material	Pass the Hash		LSA Secrets		Local Groups						
									Pass the Ticket		LSASS Memory	Process Discovery							
									Web Session Cookie		Security Account Manager	Query Registry							
								Valid Accounts	Default Accounts	Steal or Forge Kerberos Tickets	AS-REP Roasting	Remote System Discovery							
									Domain Accounts		Golden Ticket	Software Discovery							
									Local Accounts		Kerberoasting	System Information Discovery							
											Silver Ticket	System Network Configuration Discovery							
										Steal Web Session Cookie		System Network Connections Discovery							
										Unsecured Credentials	Bash History	System Owner/User Discovery							
											Cloud Instance Metadata API	System Service Discovery							
											Container API								
											Credentials In Files								
											Credentials in Registry								
											Private Keys								

Доля компаний в которых использовались техники и подтехники:

- 66%-100%
- 41%-65%
- 21%-40%
- 1%-20%

TTP	Min	Mix
TTP1	10 мин	2 часа
TTP2	15 мин	24 часа
TTP3	30 мин	30 часов
TTP8	10 мин	12 часов

* https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/

Управление инфраструктурой и цепочками атак

Основные задачи — У4

Укрепить активы

- Инвентаризация
- Уязвимости
- Парольная политика

Уменьшить поверхность атаки

- Политики взаимодействия
- Сегментация
- Фильтрация

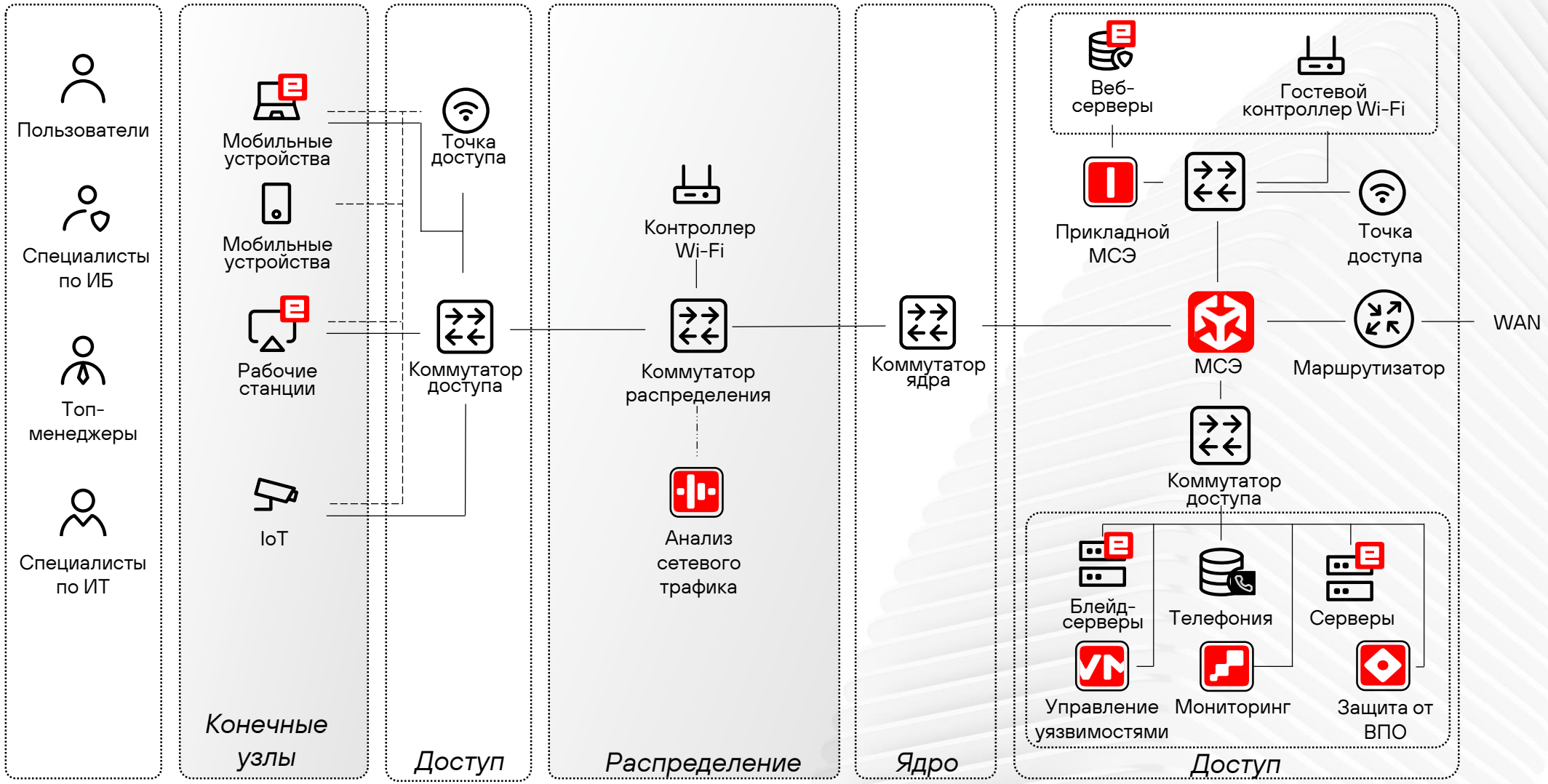
Удлинить цепочку атаки

- Инфраструктурные СЗИ
- Терминальные серверы
- Эшелонированная оборона

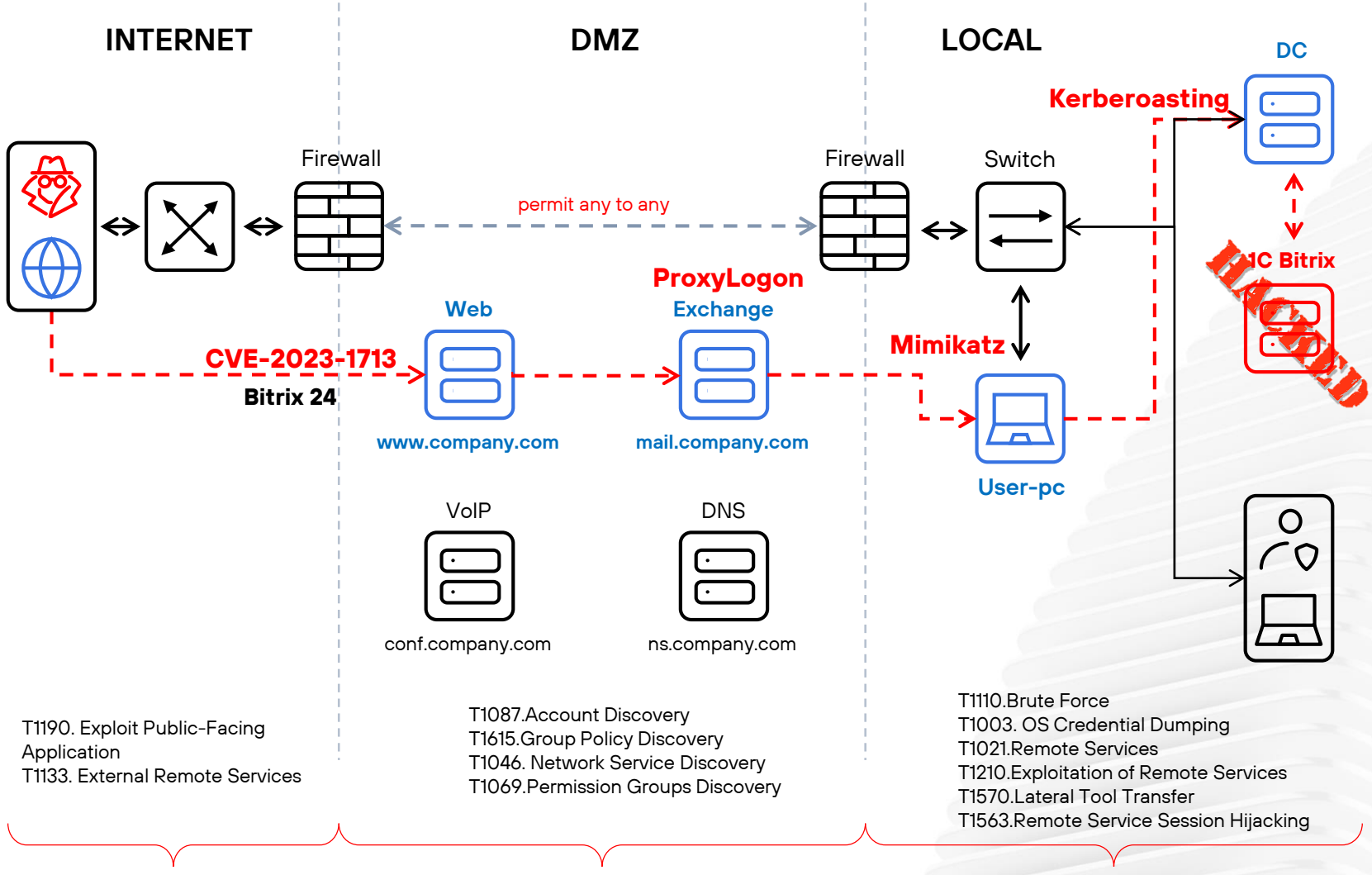
Усложнить цепочку атаки

- Защита активов
- Ложные цели

Защита офисной сети



Ключевые и целевые системы



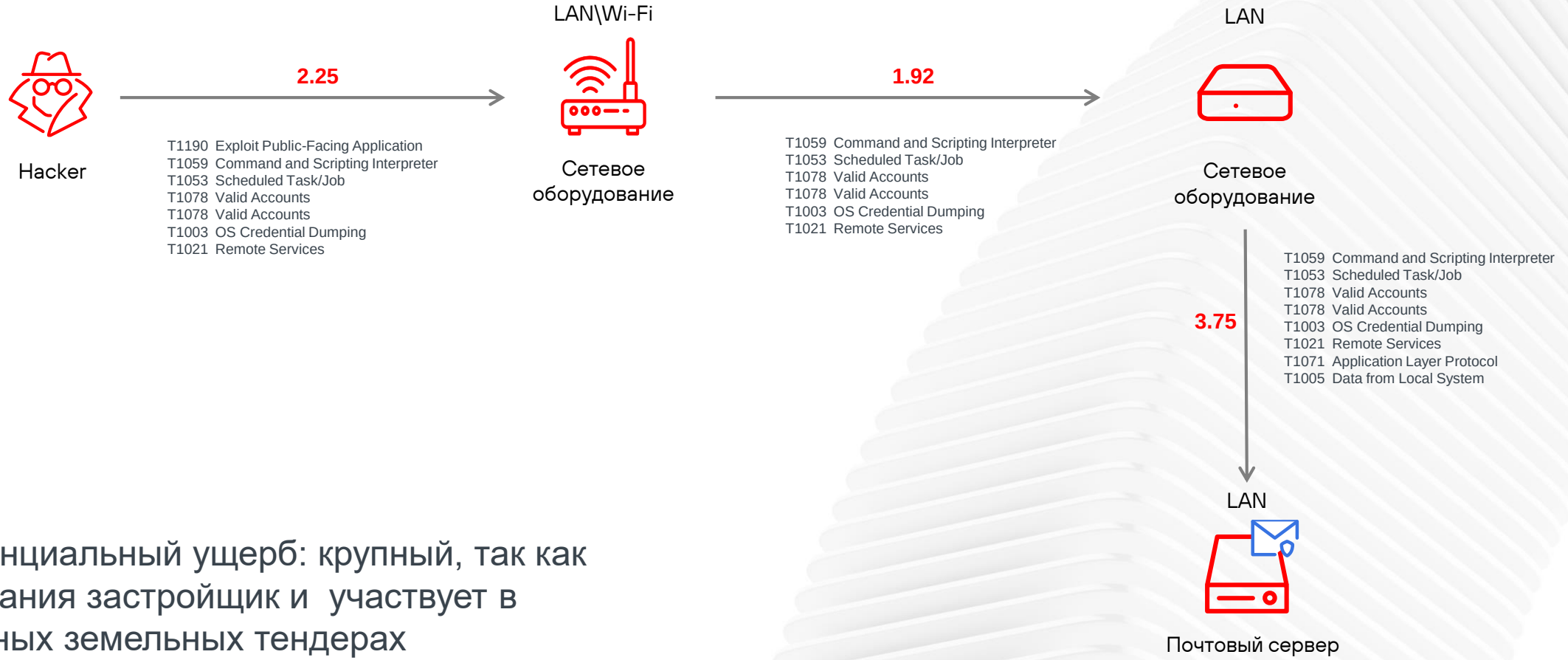
Целевая ИС – один или несколько объектов в ИТ-инфраструктуре, воздействие на которые может привести к реализации НС. Как правило объекты являются конечной целью злоумышленника при реализации НС.

Ключевая ИС – объекты в ИТ- инфраструктуре, несанкционированный доступ к которым или воздействие на которые необходимы нарушителю, чтобы развить атаку на целевую систему, или система, взлом которой существенно упростит сценарий атаки.

Пример расчета цепочки атаки

Недопустимое событие: Несанкционированный доступ к корпоративному почтовому ящику тендерного отдела

Время атаки: 7.92 часа

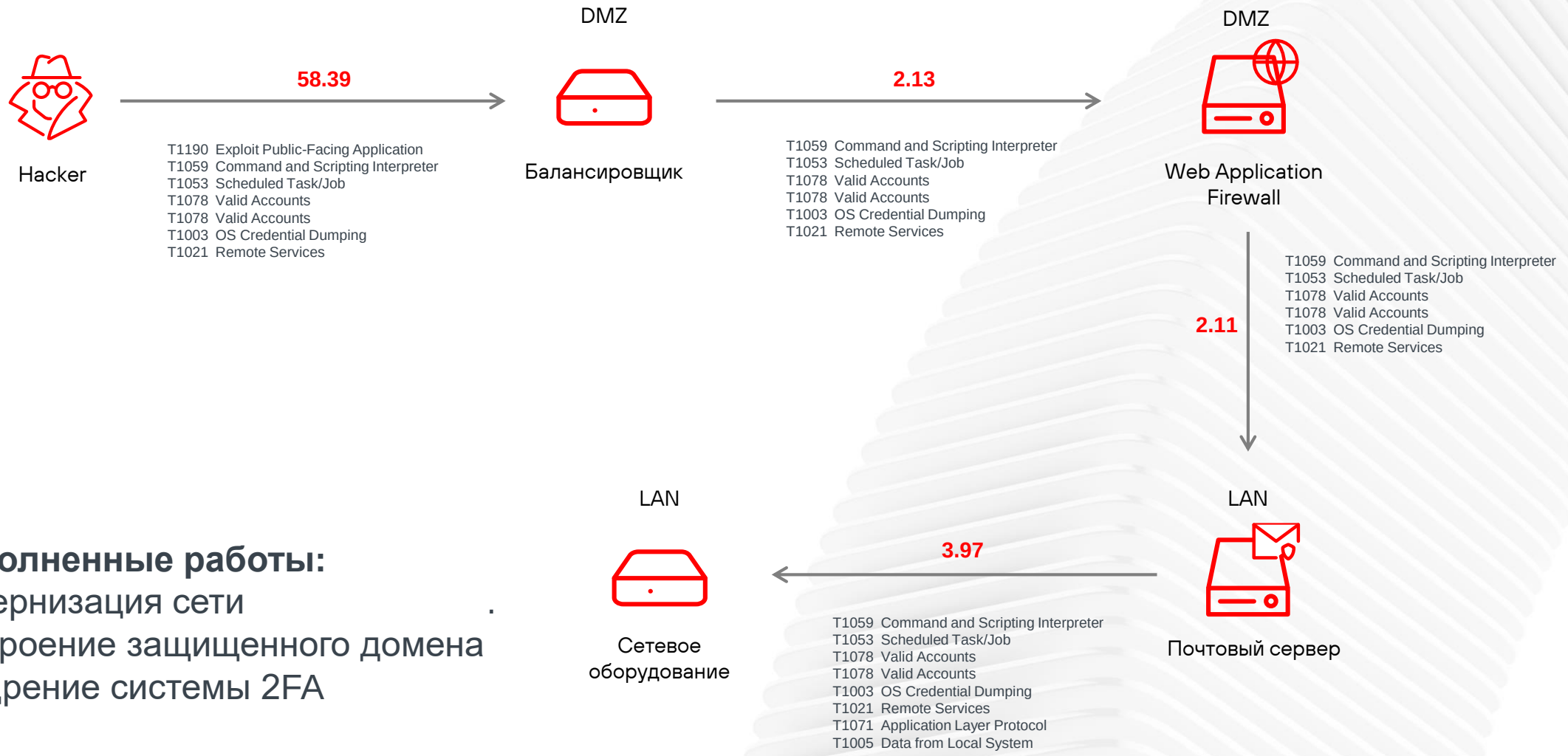


Потенциальный ущерб: крупный, так как компания застройщик и участвует в крупных земельных тендерах

Пример расчета цепочки атаки

Недопустимое событие: Несанкционированный доступ к корпоративному почтовому ящику тендерного отдела

Время атаки: 66.6 часа



Выполненные работы:

Модернизация сети

Построение защищенного домена

Внедрение системы 2FA

В заключение

Реальная архитектура СО РКБ индивидуальна для каждой организации

Укрепление и (или) подтверждение надежности ИТ-инфраструктуры является обязательным шагом

При проектировании необходимо учитывать возможные цепочки атаки:

- точки проникновения,
- топологию,
- ключевые и целевые системы

Киберучения как метод тестирования


pt
Спасибо!