

Штабные киберучения

Дмитрий Кузнецов

Positive Technologies





Коротко обо мне

Окончил Московский Государственный Университет, в информационной безопасности с 1999 г.. Последние 13 лет работаю в Positive Technologies, представляю компанию в экспертных группах ФСТЭК, ФСБ, Банка России

Активно консультирую коллег в профильных Telegram-каналах:

- «КИИ 187-ФЗ» (<https://t.me/KII187FZ>)
- «Все ФЗ» (<https://t.me/vseFZ>)
- «ИБ в Финсекторе» (<https://t.me/FinSecurity>)

Подготовка

Группа реагирования на инциденты

Мы создаем в подразделении ИБ
группу реагирования на инциденты
кибербезопасности

С чего начнем?



Первый подход к снаряду

Инцидент на химическом производстве



12:00 - Включились сирены
локальной системы оповещения о ЧС
12:30 - Ответственный по
гражданской обороне сообщил, что
включение сирен было
самопроизвольным

Инцидент или нет?

Если инцидент, то что делаем?

Типичные ошибки

- Не знаем заранее, считать ли событие инцидентом
- Не знаем объект, на котором произошло событие
- Не знаем, к чему может привести событие
- Не имеем готового плана действий

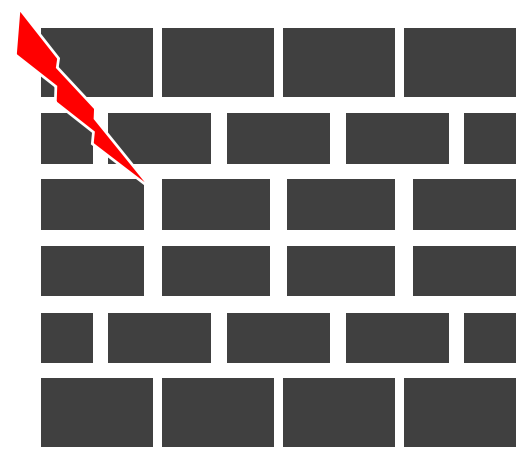


Недопустимые события

ВСЕГДА ЕСТЬ СОБЫТИЯ, КОТОРЫЕ НЕДОПУСТИМЫ ДЛЯ ПРЕДПРИЯТИЯ

делающие **невозможным достижение** операционных и стратегических **целей** или приводящие к **длительному нарушению** его основной деятельности, в том числе в результате кибератак

Выполняет все свои функции

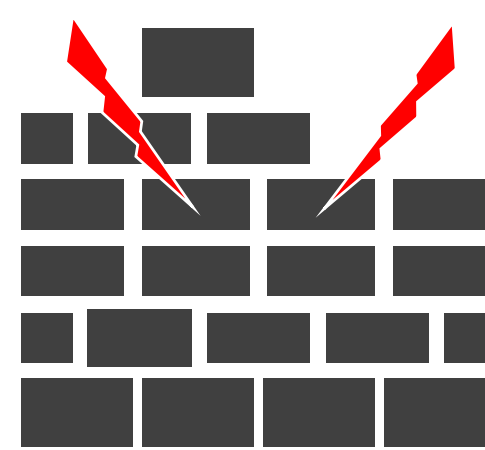


допустимый ущерб



ПУБЛИЧНЫЕ СУДЕБНЫЕ РАЗБИРАТЕЛЬСТВА

Выполняет свои функции частично



значительный ущерб



СРЫВ КОНТРАКТНЫХ ОБЯЗАТЕЛЬСТВ

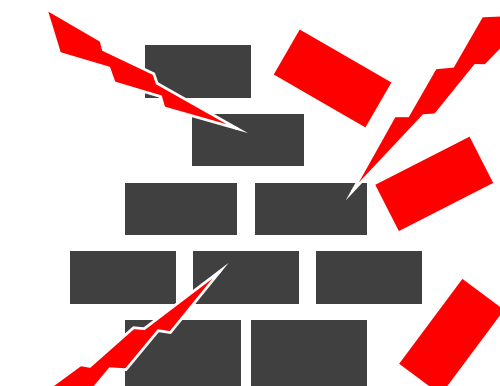


КРУПНЫЕ ФИНАНСОВЫЕ ПОТЕРИ



ПОТЕРЯ ДОЛИ РЫНКА

Не выполняет свои функции



недопустимый ущерб



ОСТАНОВКА ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ



06.05.2021 – обнаружена
подозрительная активность
07.05.2021 – коллапс IT-
инфраструктуры, остановлена
прокачка нефтепродуктов
08.05.2021 – уплачен выкуп
12.05.2021 – возобновление работы
трубопровода

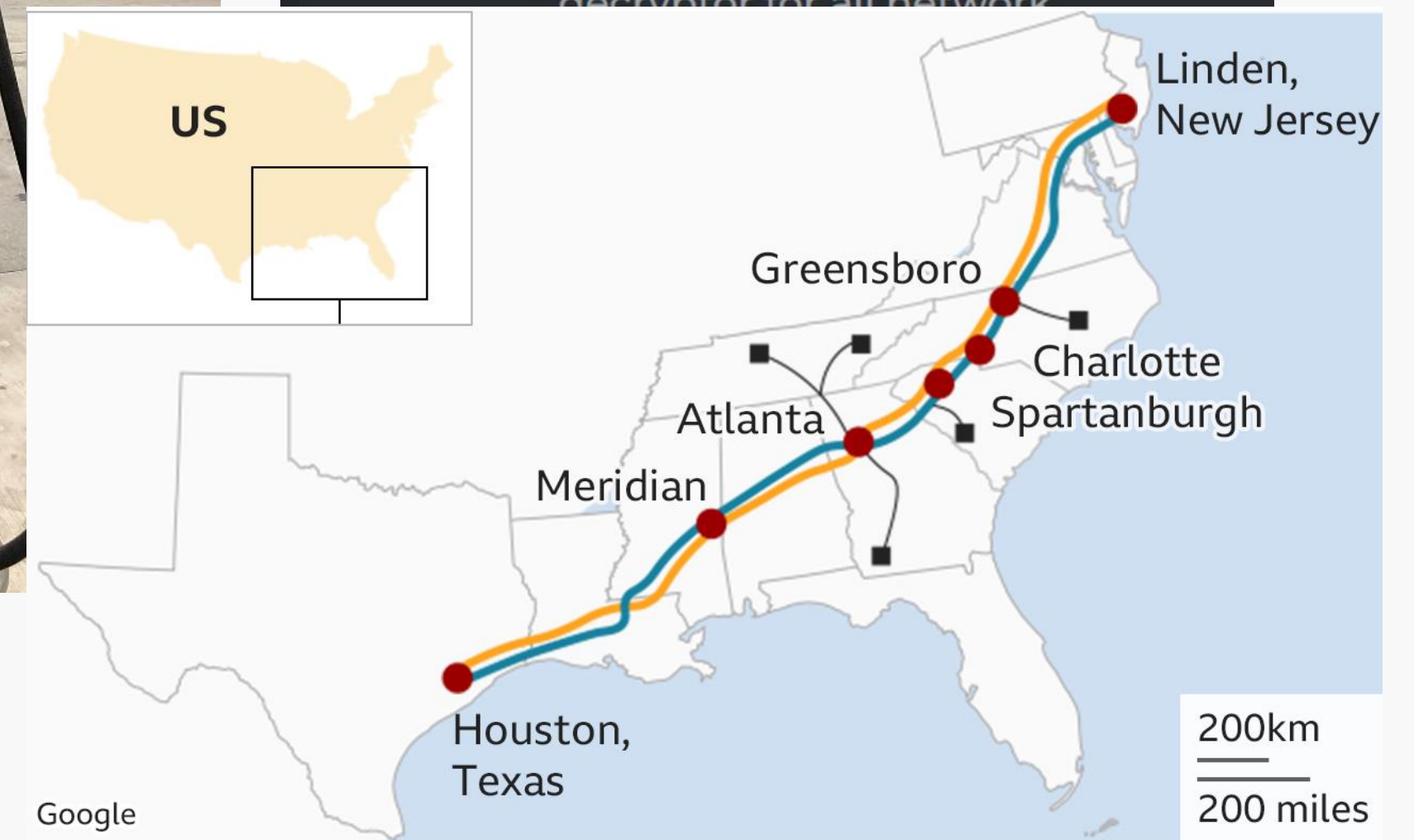
Когда инцидент произошел,
реагировать уже поздно!



Your network has been locked!

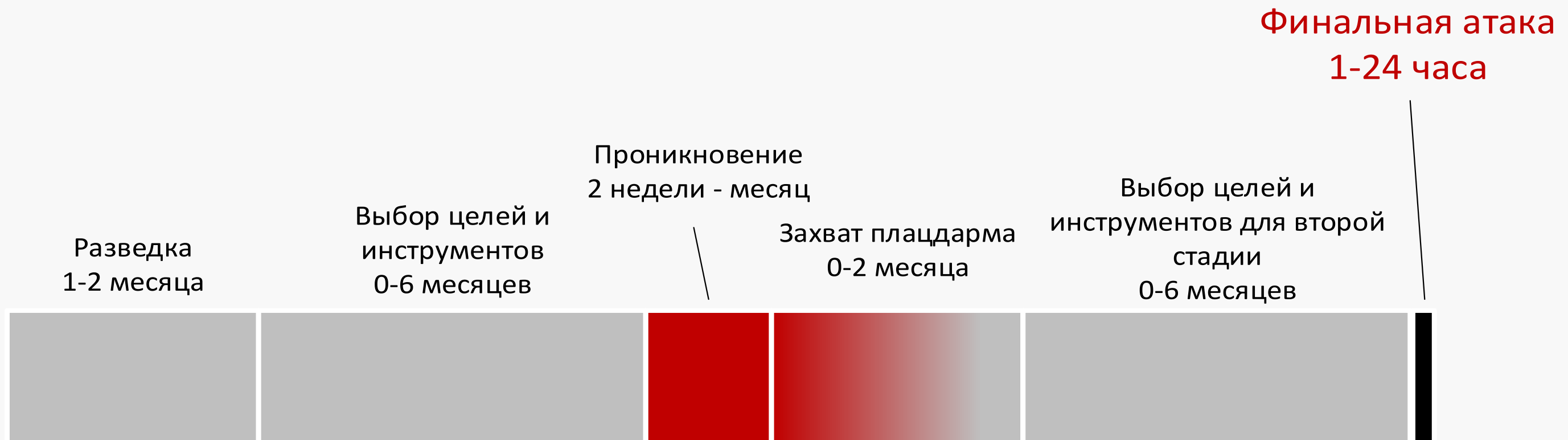
You need pay **\$ 2,000,000** now, or
190.363 BTC (+10%) - 22537.751 XMR
\$ 4,000,000 after doubled.
380.725 BTC (+10%) - 45075.501 XMR

After payment we will provide you universal
decrypter for all network



“Своевременно” – это...

Нападение



Защита

Нет видимых проявлений

Могли обнаружить, но не обнаружили

Убывание возможности обнаружения

Обнаружили, но не смогли помешать

Нет видимых проявлений

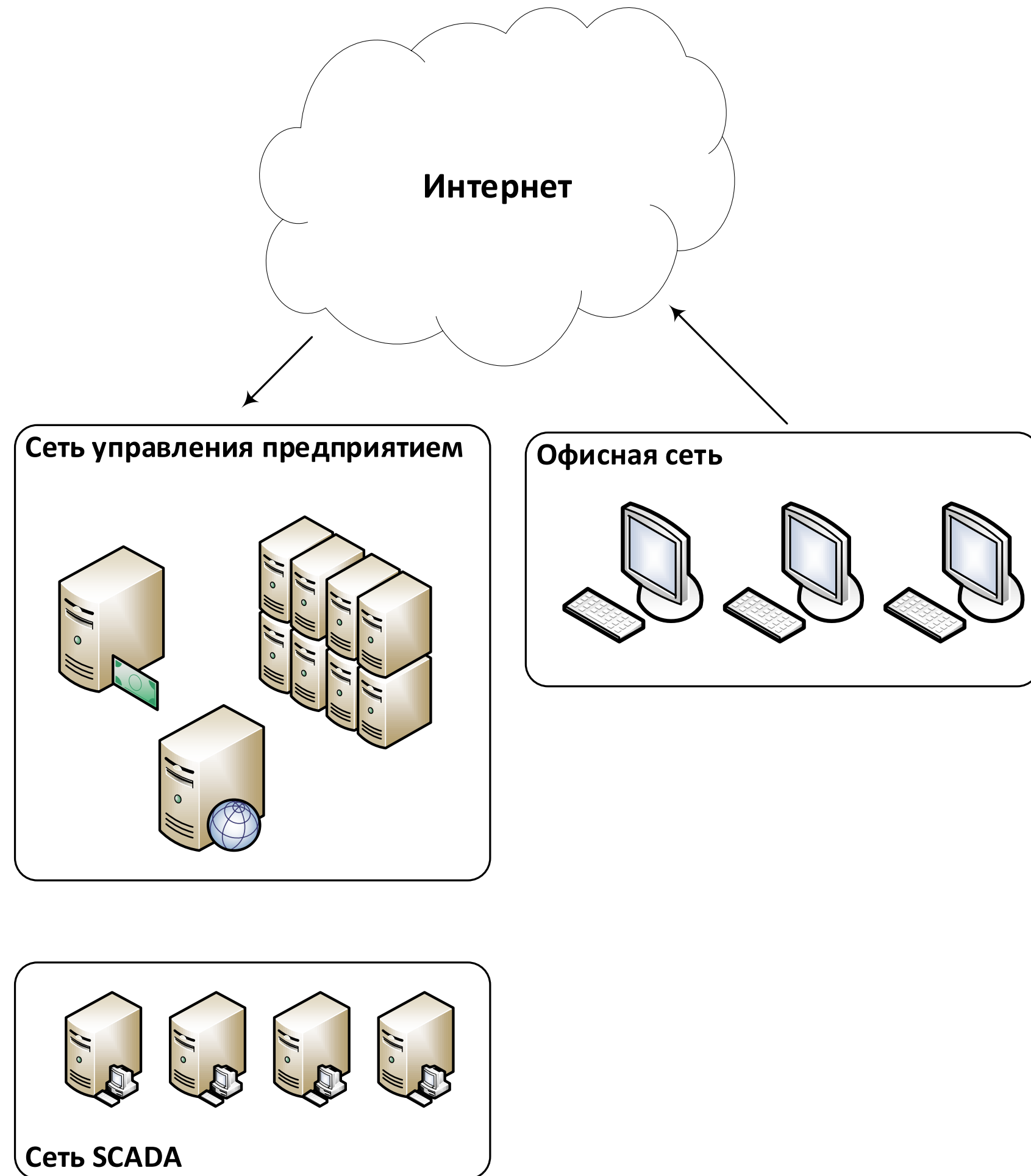
Второй подход к снаряду

Этапы реагирования

1. Признать существование проблемы
2. Локализовать проблему
3. Выяснить, что произошло
4. Устранить проблему
5. Nevermore!



Те же,
там же,
тогда же



Типичные ошибки

- Не знаем заранее, за чем наблюдать
- Не знаем заранее, как будем изолировать зону поражения
- Не имеем развернутых инструментов
- Не имеем готового плана действий



Объекты, за которыми наблюдаем

VLAN 01 (██████████)

АРМ Казначейства

АРМ сотрудников:
s██████████ (10.0.██████████)
y██████████ (10.0.██████████)

Сценарии использования системы:

- ✓ Подключение к целевым системам (1С, каталог обмена, банк-клиенты) с использованием сетевого доступа и привилегий сотрудника казначейства

АРМ руководителя казначейства

АРМ руководителя:
Ik██████████ (10.0.██████████)

Сценарии использования системы:

- ✓ Подключение к целевым системам (1С, банк-клиенты) с использованием сетевого доступа и привилегий руководителя казначейства
- ✓ Отправка ложных распоряжений от имени руководителя казначейства с его компьютера

АРМ финансового директора

АРМ директора:
a██████████ (10.0.██████████)

Сценарии использования системы:

- ✓ Подключение к целевым системам (1С, каталог обмена, банк-клиенты) с использованием сетевого доступа и привилегий финансового директора
- ✓ Отправка ложных распоряжений от имени финансового директора с его компьютера

АРМ Бухгалтерии

Сценарии использования системы:

- ✓ Подключение к целевым системам (1С, каталог обмена, банк-клиенты) с использованием сетевого доступа и

VLAN 10 (██████████)

1С Веб-приложения **1С СУБД (MSSQL)**

Серверы 1С:
dc██████████2.ptsecurity.ru (10.10.██████████)
dc██████████3.ptsecurity.ru (10.10.██████████)

Способы реализации угроз:

- ✓ Создание ложной заявки
- ✓ Подмена реквизитов контрагента
- ✓ Создание ложного контрагента

Confluence Веб-приложение (корпоративная Wiki)

Сервер Confluence:
10.10.██████████

Сценарии использования системы:

- ✓ Получение информации о процессах, адресах и учетных записях для реализации атак на целевые и ключевые системы

1С Веб-приложения (тестовый) **1С СУБД (MSSQL) (копия)**

Сервер 1С разработчиков
dev-1-01 (10.10.██████████)

Сценарии использования системы:

- ✓ Получение информации из копии базы данных 1С
- ✓ Отработка атак на тестовом сервере перед атакой целевой системы (1С)

1С БД (резервные копии)

Сервер резервного копирования 1С
dc1-bk██████████ (10.10.██████████)

Сценарии использования системы:

- ✓ Получение информации из копии базы данных 1С

VLAN 10.52 (██████████)

Каталог обмена платежными документами:
\\ptsecurity.ru\██████████
\\ptsecurity.ru\pt██████████

Файловый сервер:
dc██████████ (10.10.██████████)

Способы реализации угроз:

- ✓ Подмена файла платежного документа
- ✓ Подмена данных в файле платежного документа

Контроллеры домена PTSECURITY

Серверы Domain Controller:
10.0.██████████, 10.0.██████████
10.10.██████████, 10.10.██████████

Сценарии использования системы:

- ✓ Получение доступа к ключевым и целевым системам (и другим компьютерам и серверам) с максимальными привилегиями в домене

Серверы корпоративной электронной почты Exchange

Серверы Exchange Mailbox:
mail.ptsecurity.com (10.10.██████████)
dc██████████01 (10.10.██████████)
dc██████████02 (10.10.██████████)
dc██████████03 (10.10.██████████)
dc██████████04 (10.10.██████████)
dc██████████05 (10.10.██████████)

Сценарии использования системы:

- ✓ Проведение атак на сотрудников с использованием методов социальной инженерии (business email compromise)

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create or Modify System Process (4)	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repository (2)	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Compromise Client Software Binary	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Local System	Encrypted Channel (2)	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create Account (3)	Escape to Host	Execution Guardrails (1)	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (2)	Use Alternate Authentication Material (4)	Data from Removable Media	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Network Service Scanning		Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
			User Execution (3)	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (7)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
			Windows Management Instrumentation	Hijack Execution Flow (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Data from Removable Media	Non-Standard Port		Service Stop
				Implant Internal Image	Scheduled Task/Job (7)	Impair Defenses (7)	Two-Factor Authentication Interception	Peripheral Device Discovery		Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
				Modify Authentication Process (4)	Valid Accounts (4)	Indicator Removal on Host (6)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Email Collection (3)	Proxy (4)		
				Office Application Startup (6)		Indirect Command Execution		Process Discovery		Input Capture (4)	Remote Access Software		
				Pre-OS Boot (5)		Masquerading (6)		Query Registry		Man in the Browser	Traffic Signaling (1)		
				Scheduled Task/Job (7)		Modify Authentication Process (4)		Remote System Discovery		Man-in-the-Middle (2)	Web Service (3)		
				Server Software Component (3)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)		Screen Capture			
				Traffic Signaling (1)		Modify Registry		System Information Discovery		Video Capture			
				Valid Accounts (4)		Modify System Image (2)		System Location Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Binary Proxy Execution (11)							
						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							

События, за которыми наблюдаем



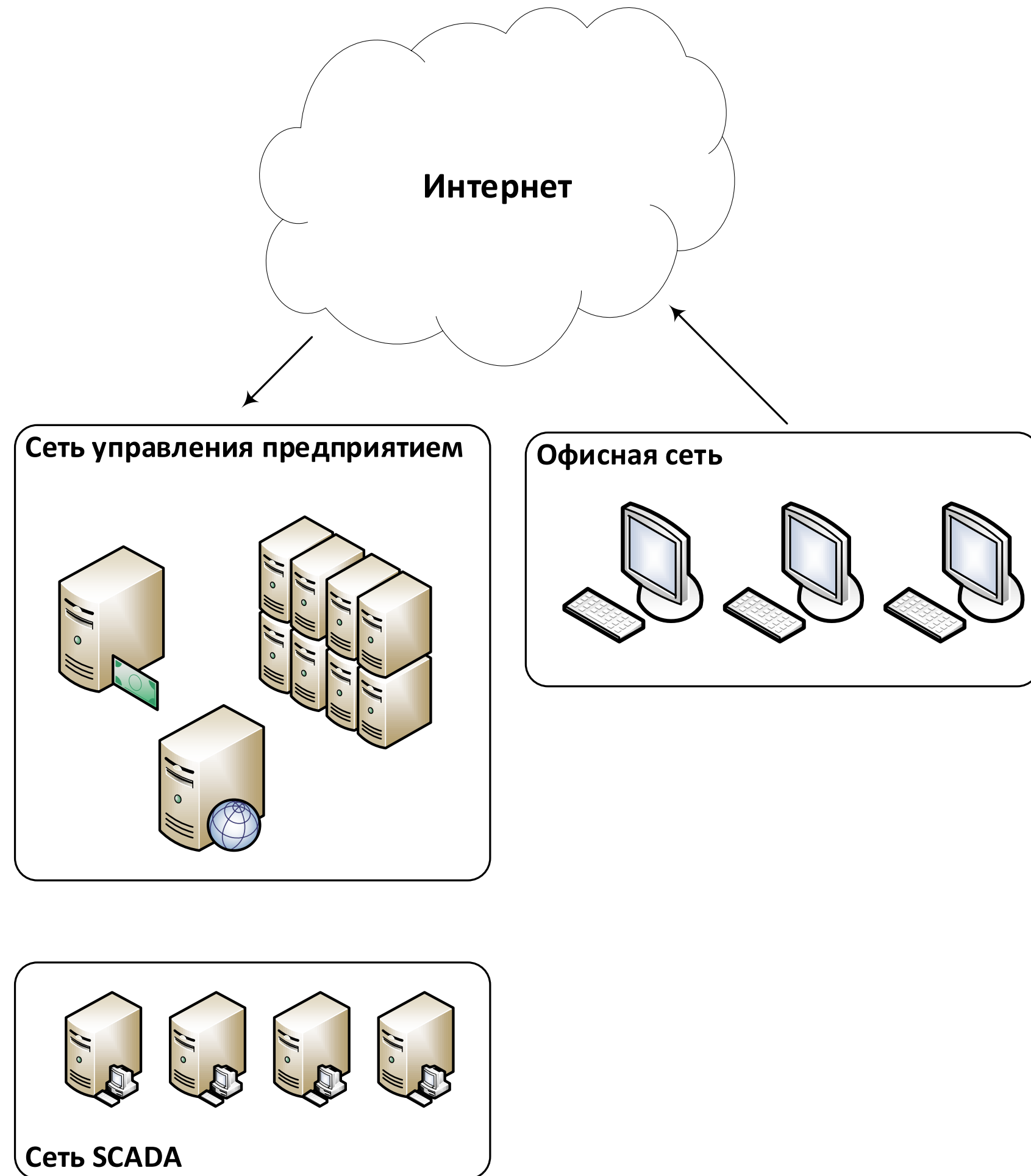
Мы реагируем не на инциденты
Мы реагируем на известные нам способы воздействия нарушителя на целевые и ключевые объекты

План реагирования



- Какие события недопустимы?
- Какие объекты являются целевыми и ключевыми?
- Какие действия нарушителя с этими объектами нужно обнаруживать?
- Чем и как эти действия обнаруживать?
- Что делать при обнаружении?

Подготовка к реагированию



Инструменты реагирования

- SIEM
- CMDB (если этого не умеет SIEM)
- Анализаторы трафика
- WAF
- Песочницы
- Базы знаний



Что в итоге

Реагирование на инциденты vs. ИБ

- Нужно знать потребности бизнеса
- Нужно знать приемы нарушителя
- Нужно ставить под сомнение собственную защищенность
- Нужен инструментарий, не предусмотренный нормативными требованиями



Готов ответить на ваши вопросы

E-mail

malotavr@gmail.com

Telegram

[@malotavr](https://www.instagram.com/malotavr)

