



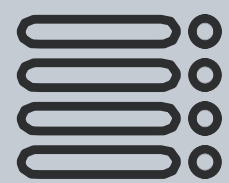
Реально ли идеальное расследование? Быстро - Качественно - Автоматизированно

Слепушенко Олег Андреевич
Ведущий аналитик RT Protect SOC



RT
Информационная
безопасность

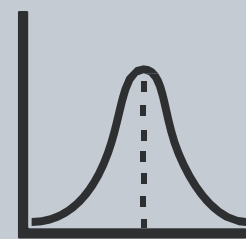
Современные тенденции



Расширение разнообразия используемых для написания ВПО языков программирования и технологий. Усложнение архитектуры



Всё более сложные социотехнические атаки, что требует повышения осведомленности об информационной безопасности обычным работникам

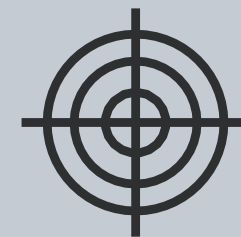


Рост активности группировок связанных с одной из сторон конфликта

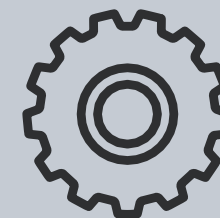


РТ

Информационная
безопасность



Эксплуатация Zero-Day уязвимостей



Повышение требований к защите конечных точек

Новейшие атаки и техники могут позволить злоумышленникам обходить современные средства защиты реального времени, пока они не станут достоянием общественности, но к тому времени будет уже поздно.

Необходимость



Как понять, что твоя
инфраструктура взломана

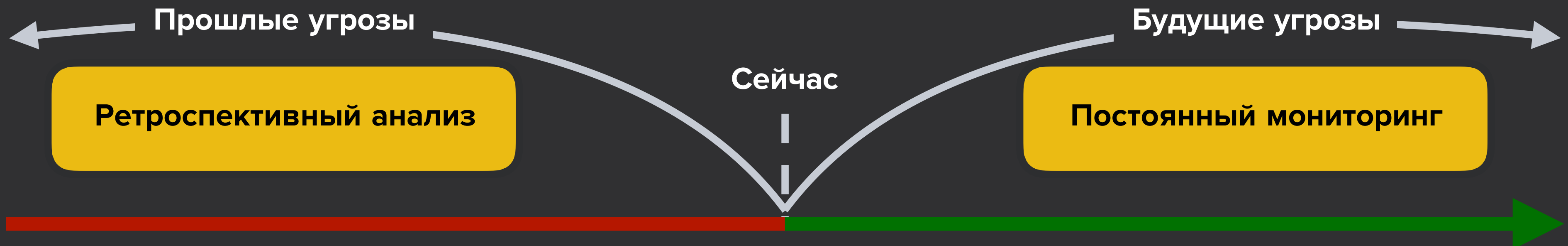
- **Указ 250:** Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры
- Поиск успешных **следов компрометации** информационной инфраструктуры злоумышленником
- **Автоматизация** процесса анализа для крупных организаций

Compromise Assessment vs Мониторинг

▶ Проактивно – EDR,
Ретроспективно – CA

▶ Процесс анализа: сначала
CA, потом мониторинг

▶ Использование данных об
актуальных угрозах с TI



Ретроспективный анализ

Compromise Assessment – ретроспективный анализ инфраструктуры на предмет компрометации

Compromise Assessment включает в себя сбор данных с конечных систем, их обработку и дальнейший анализ.

Данная процедура является очень комплексной и занимает большое количество времени и трудозатрат.

Возможно ли оптимизировать и автоматизировать данный процесс, не потеряв при этом в качестве?

Варианты решения:



Автоматизация процесса сбора данных



Автоматизация процессов нормализации и обогащения данных



Оптимизация используемых инструментов в зависимости от точек сбора



Оптимизация процесса анализа собранных данных

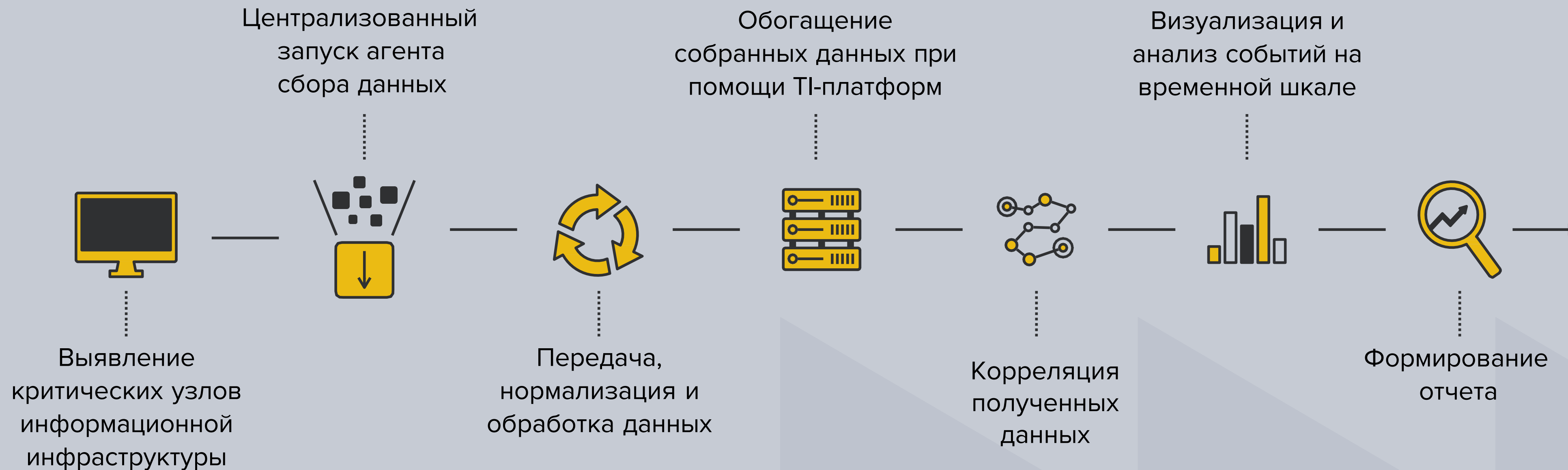
Классические задачи DFIR



Классические задачи DFIR



Этапы ретроспективного анализа инфраструктуры



Методики анализа конечных точек



Генерация инцидентов из собранных данных

- Сигнатурный анализ файловой системы и памяти процессов
- Корреляция логов
- Статистический анализ данных со всех систем, поиск аномалий
- Типичные места закрепления ВПО
- Обогащение собранных данных с помощью Threat Intelligence



Углубленный анализ конечных точек, участвующих в инцидентах

- Журналы ОС
- Информации о файловой системе
- Информация о процессах, сервисах, активных сетевых соединениях
- История активности процессов и пользовательских сессий
- Сработки с СЗИ

Выбор инструментов



Рекомендуем ознакомиться



TOP-10 криминалистических
артефактов Windows при
расследовании инцидентов

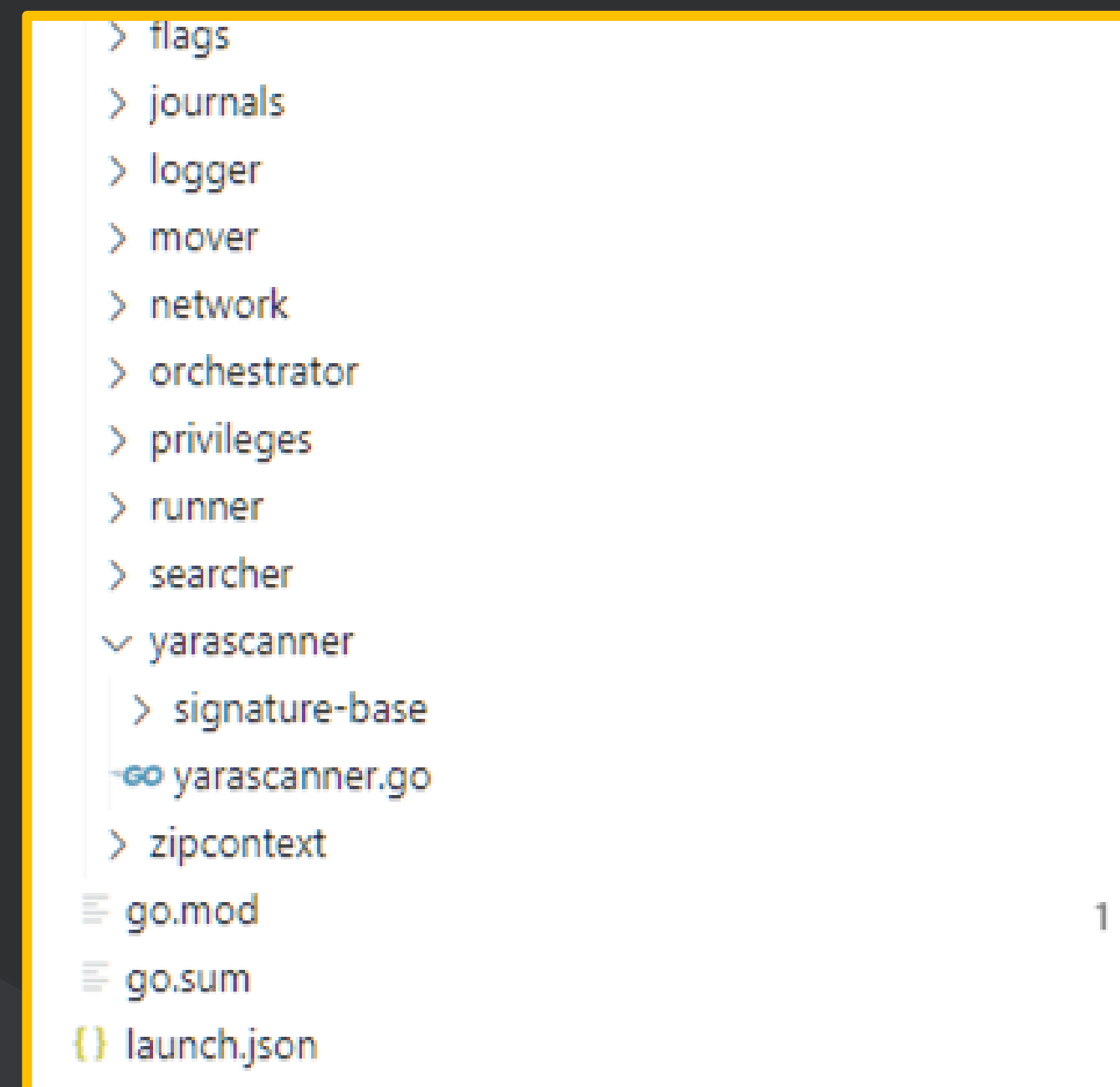
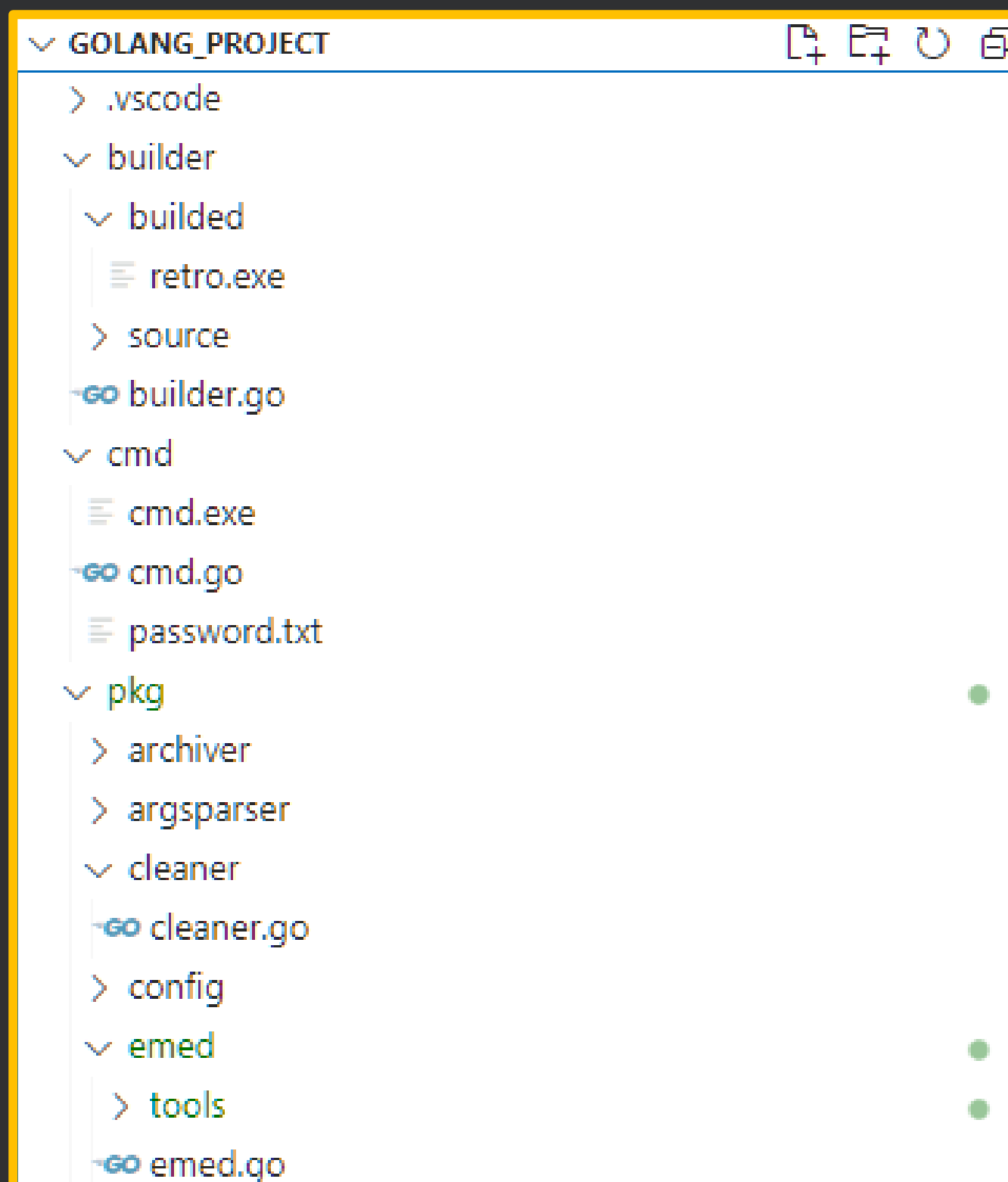


Топ-10 артефактов Linux для
расследования инцидентов



PT
Информационная
безопасность

Инструмент сбора Triage

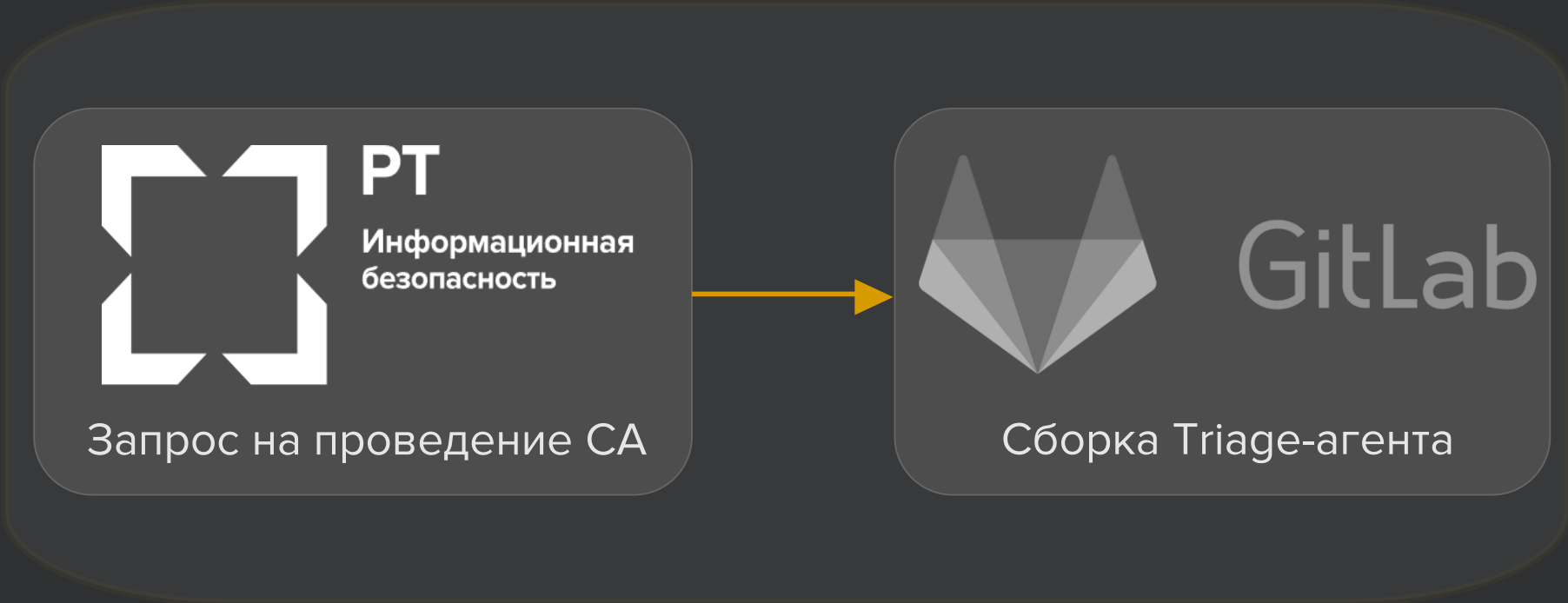


CI/CD для Triage-агента



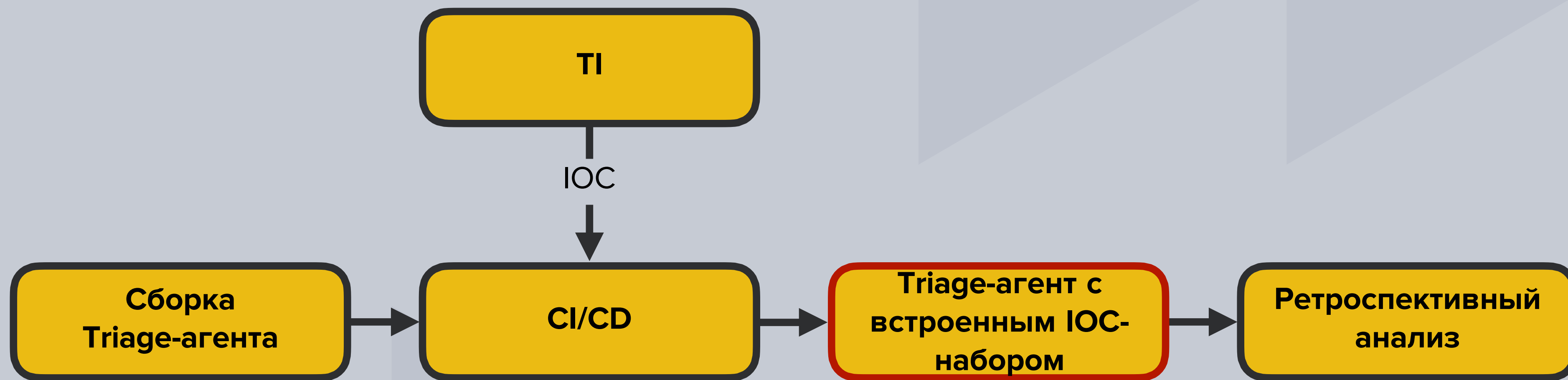
Status	Pipeline	Triggerer	Stages
passed 00:03:10 1 month ago	AppCompatCache gathering implemented. #1370 main 40cdb61b		✓ ✓ ⋮
✓ clone-job-windows clone ✓ buld-job-all build			

Этап подготовки

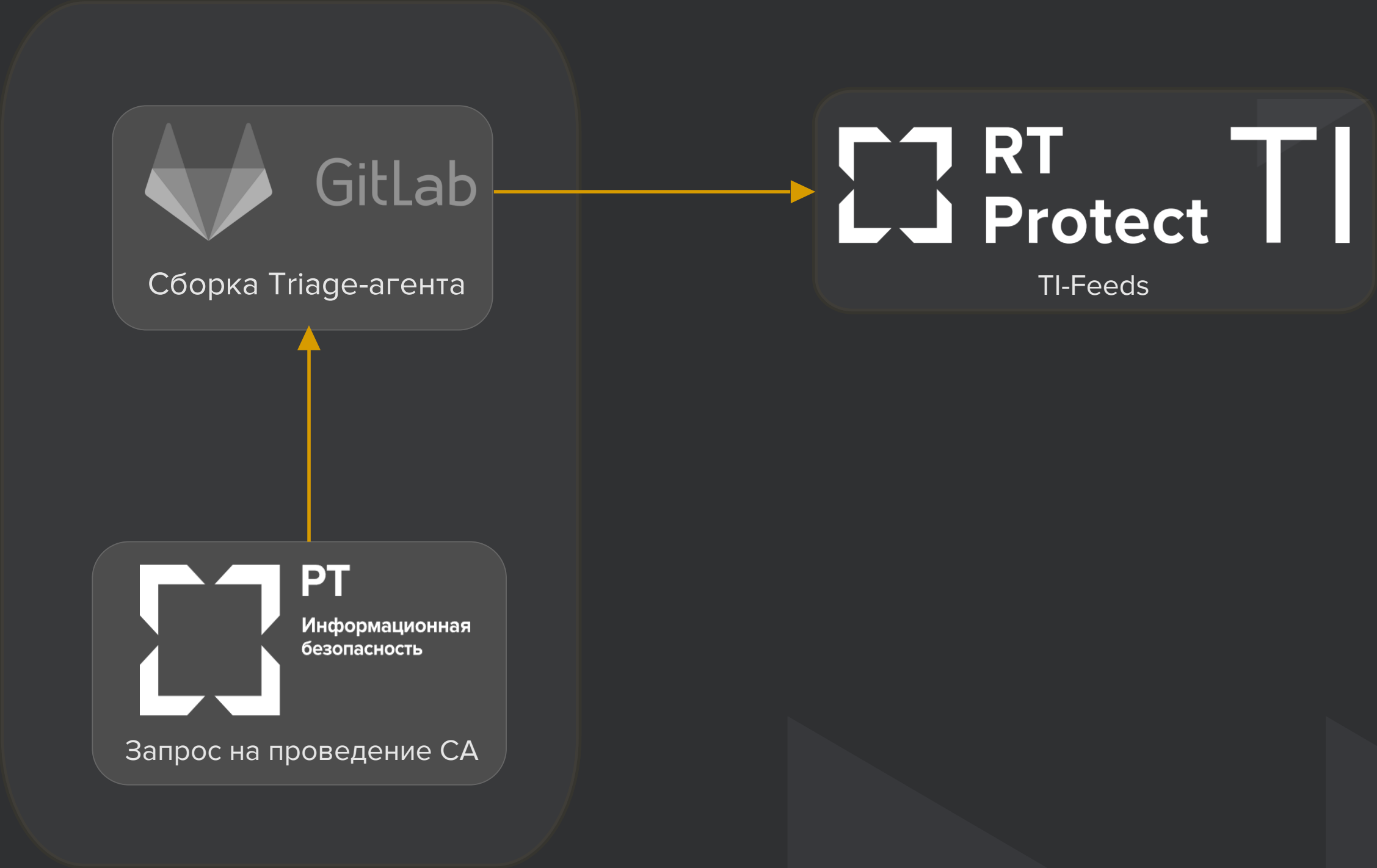


Ретроспективный анализ и Threat Intelligence

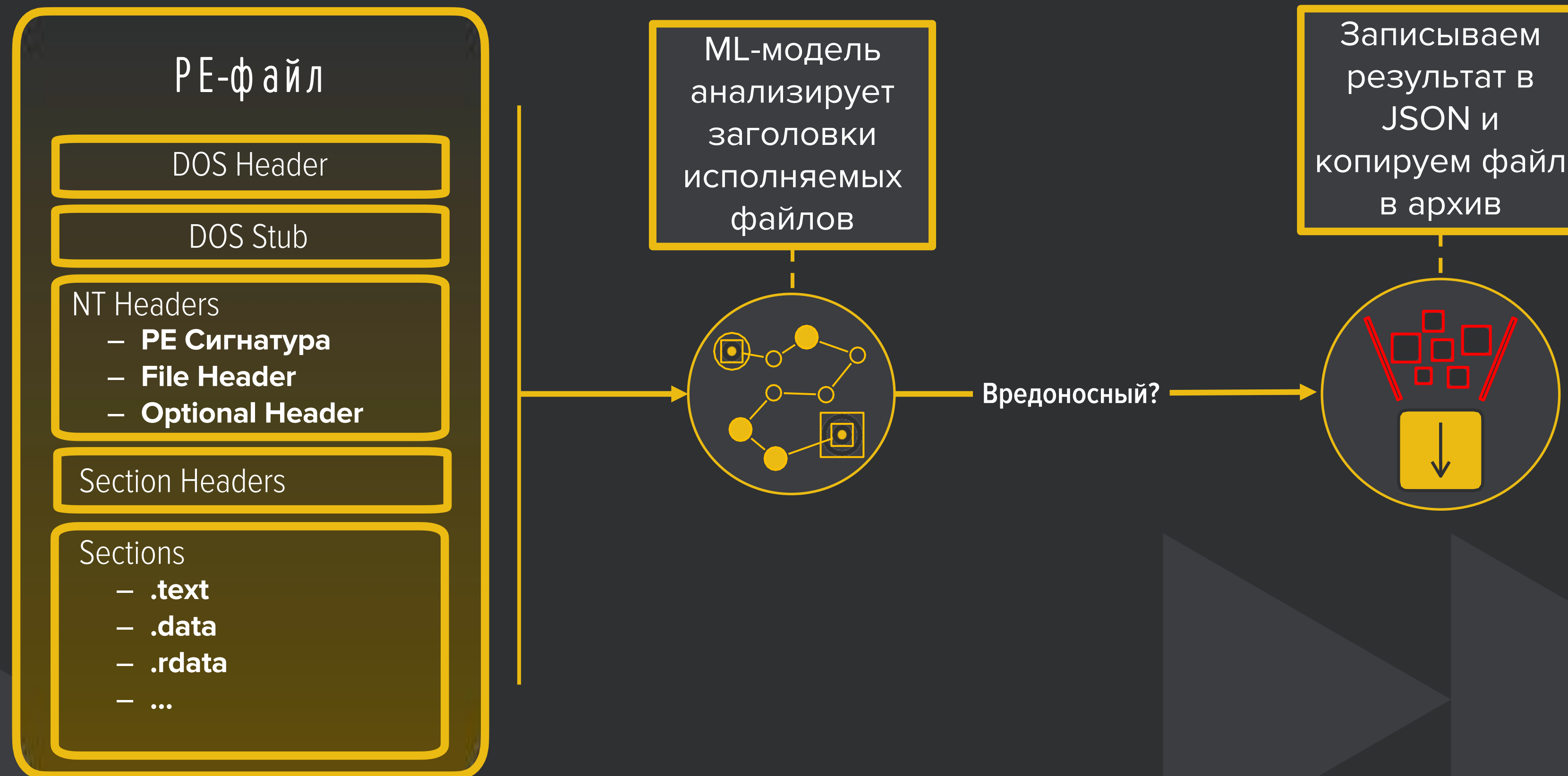
Поставка актуальных индикаторов
компрометации при ретроспективном анализе



Этап подготовки



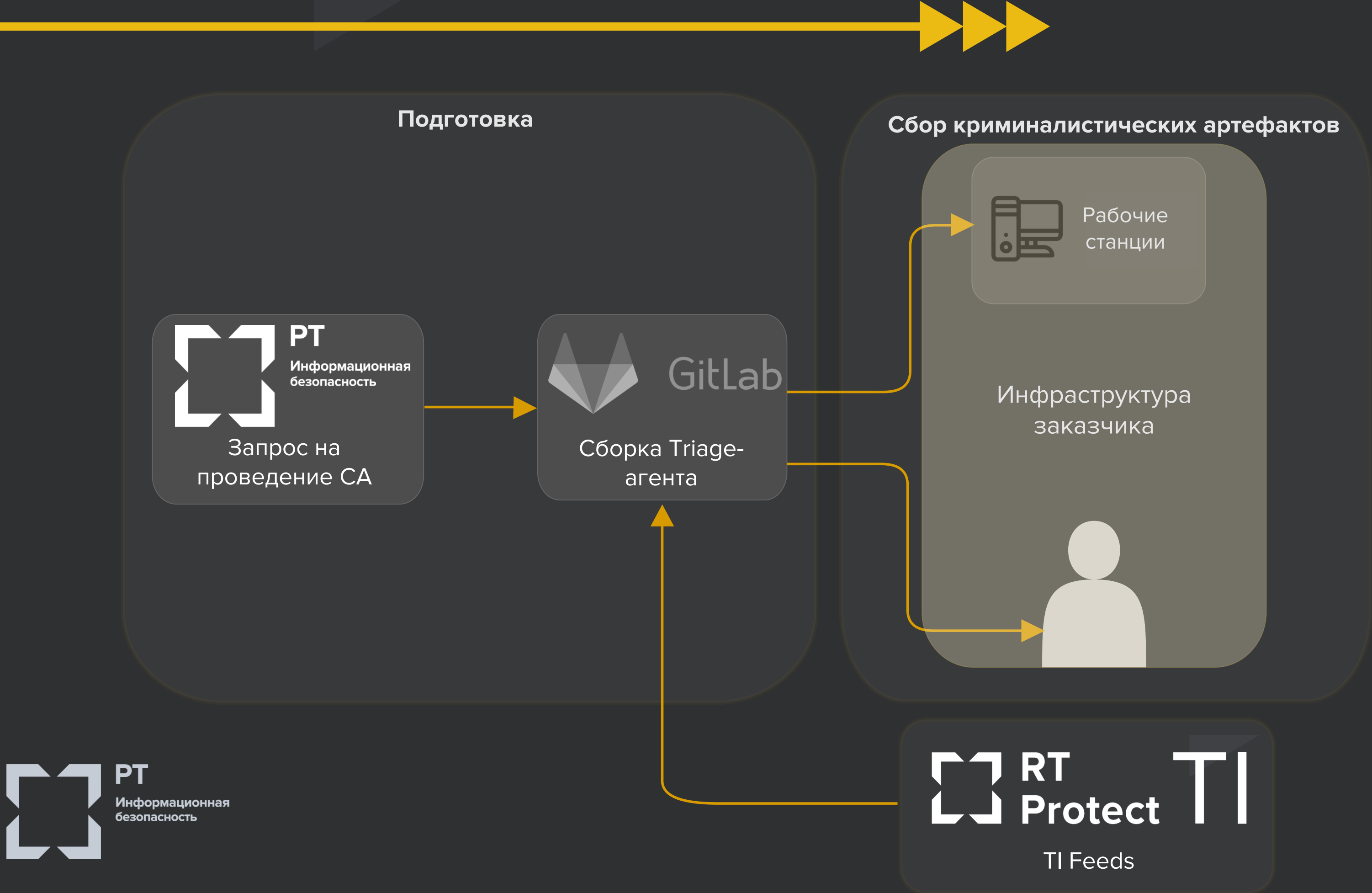
Анализ всех хэшей? Нет...



Поиск паролей в открытом виде? Да!



Этап сбора артефактов



Результат работы Triage-агента на Linux

```
#####  
#####  
#####  
###  
###  
##  
#  
##  
###  
###  
#####  
#####  
  
RT-RETRO-GO_V.1.0._2024 @RT-CS  
Retrospective analysis tool for forensic investigation  
  
*****  
**** "Timeo Danaos et dona ferentes" ****  
*****  
[SUCCESS] RT-Retro starts working...  
[SUCCESS] tools/rkhunter/rkhunter.sh  
[SUCCESS] Tool was moved to: /tmp/rt-retro/rkhunter/rkhunter.sh  
[SUCCESS] tools/UAC/uac.sh  
[SUCCESS] Tool was moved to: /tmp/rt-retro/UAC/uac.sh  
[SUCCESS] #####  
[SUCCESS] /tmp/rt-retro/rkhunter/rkhunter.sh starts working...  
[SUCCESS] #####
```

puter tmp rt-retro-out

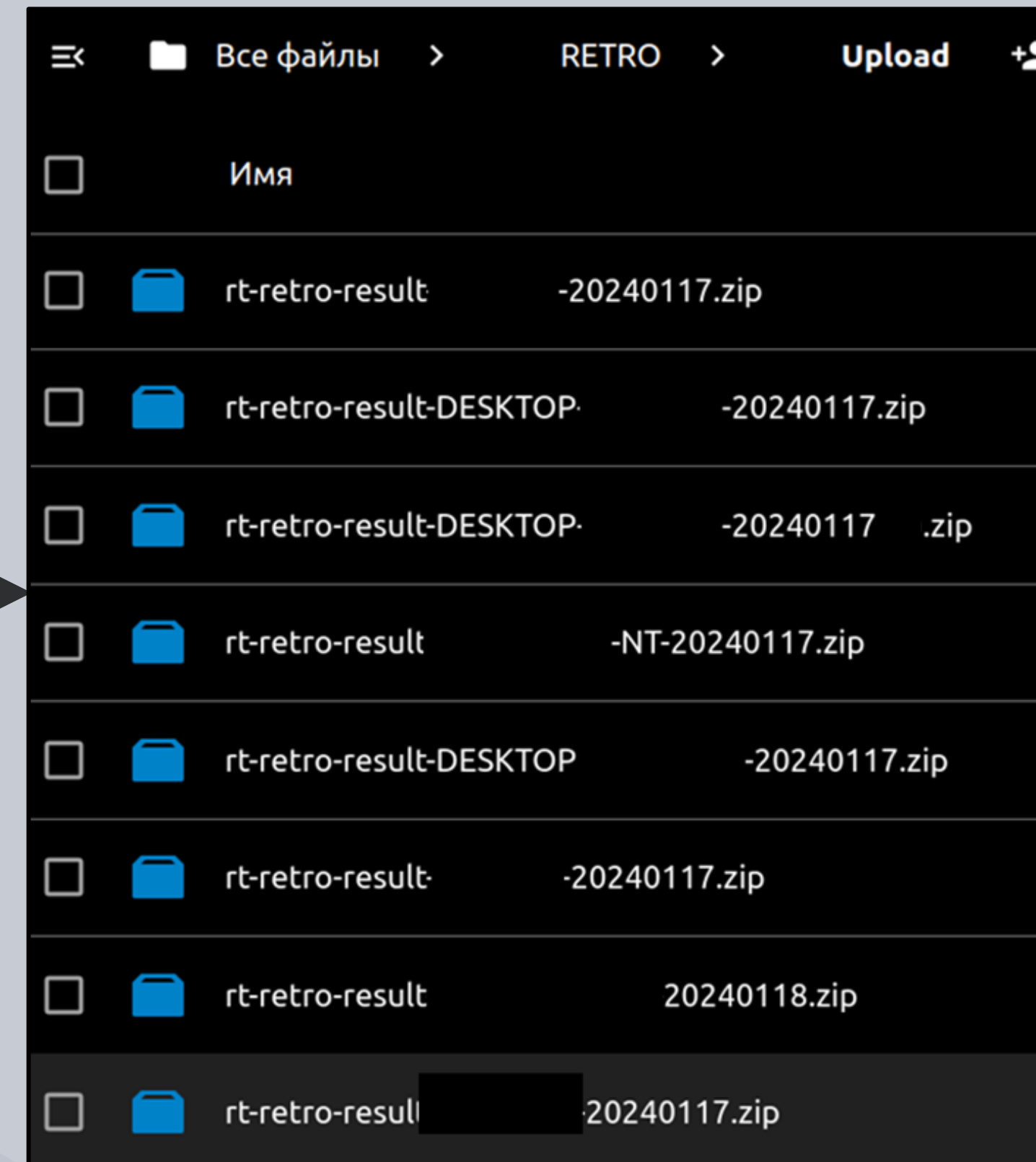
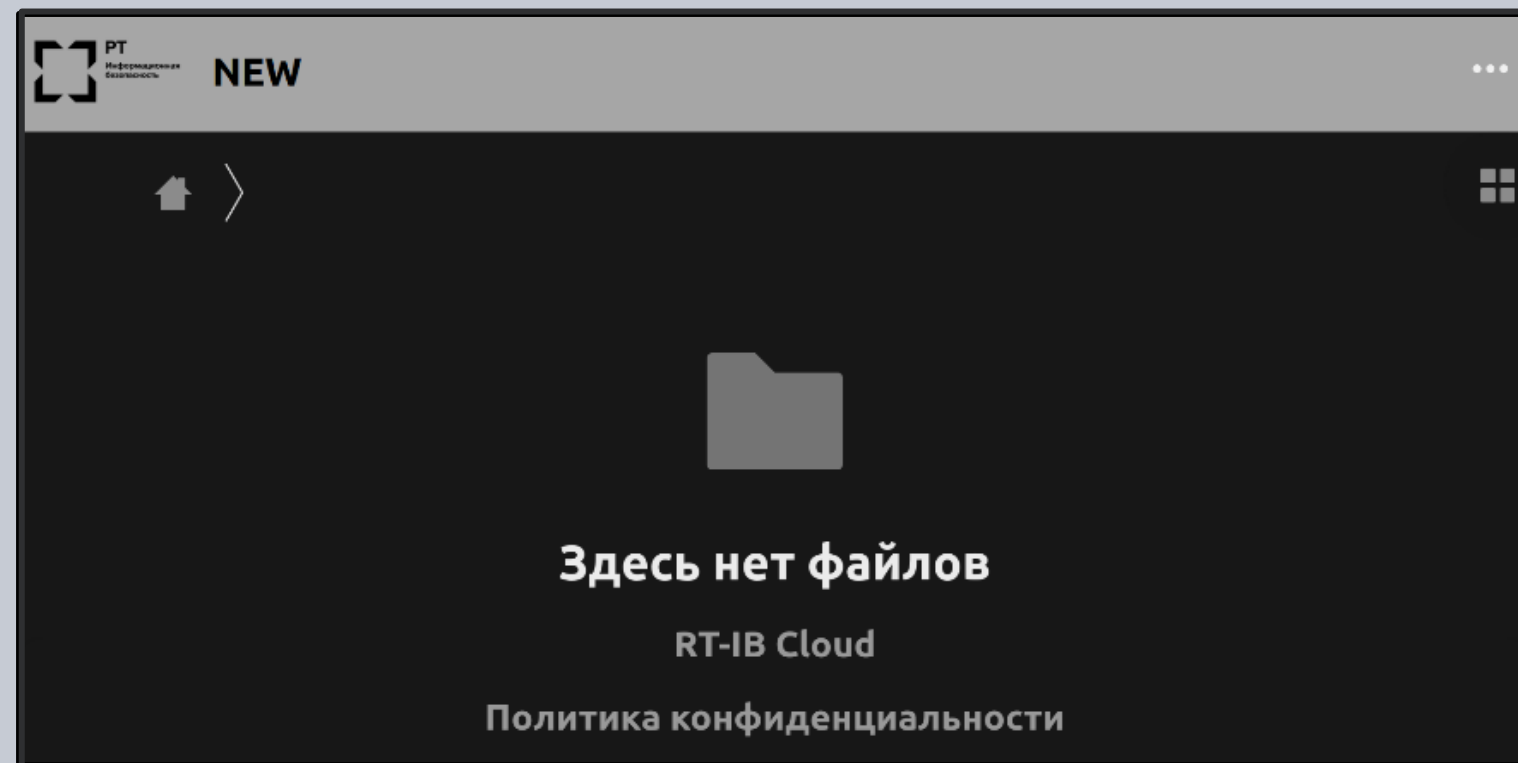
Name	
	COMPROMISED_linux_2024-08-22.zip
	COMPROMISED_linux_2024-08-22.log

Extract + COMPROMISED_linux-host.domain.ru

< > Home Location: /

Name		Size	Type	M
 rkhunter		114,1 kB	Folder	
 UAC		188,4 MB	Folder	
 yara-tool		2,4 MB	Folder	

Загрузка результатов в облако через WebDAV или вручную



...или по SMB



 DESKTOP-*.zip

 PowerShellHistory_DESKTOP-*.zip

 xcyclopedia_DESKTOP-*.zip

 PowerHuntShares_DESKTOP-*.zip

 PersistenceSniper_DESKTOP-*.zip

 loki_DESKTOP-*.zip

 VSTriage_DESKTOP-*.zip

 hayabusa_DESKTOP-*.zip

 Collect-MemoryDump_Dumplt_DESKTOP-*.zip*

 Collect-MemoryDump_WinPMEM_DESKTOP-*.zip*

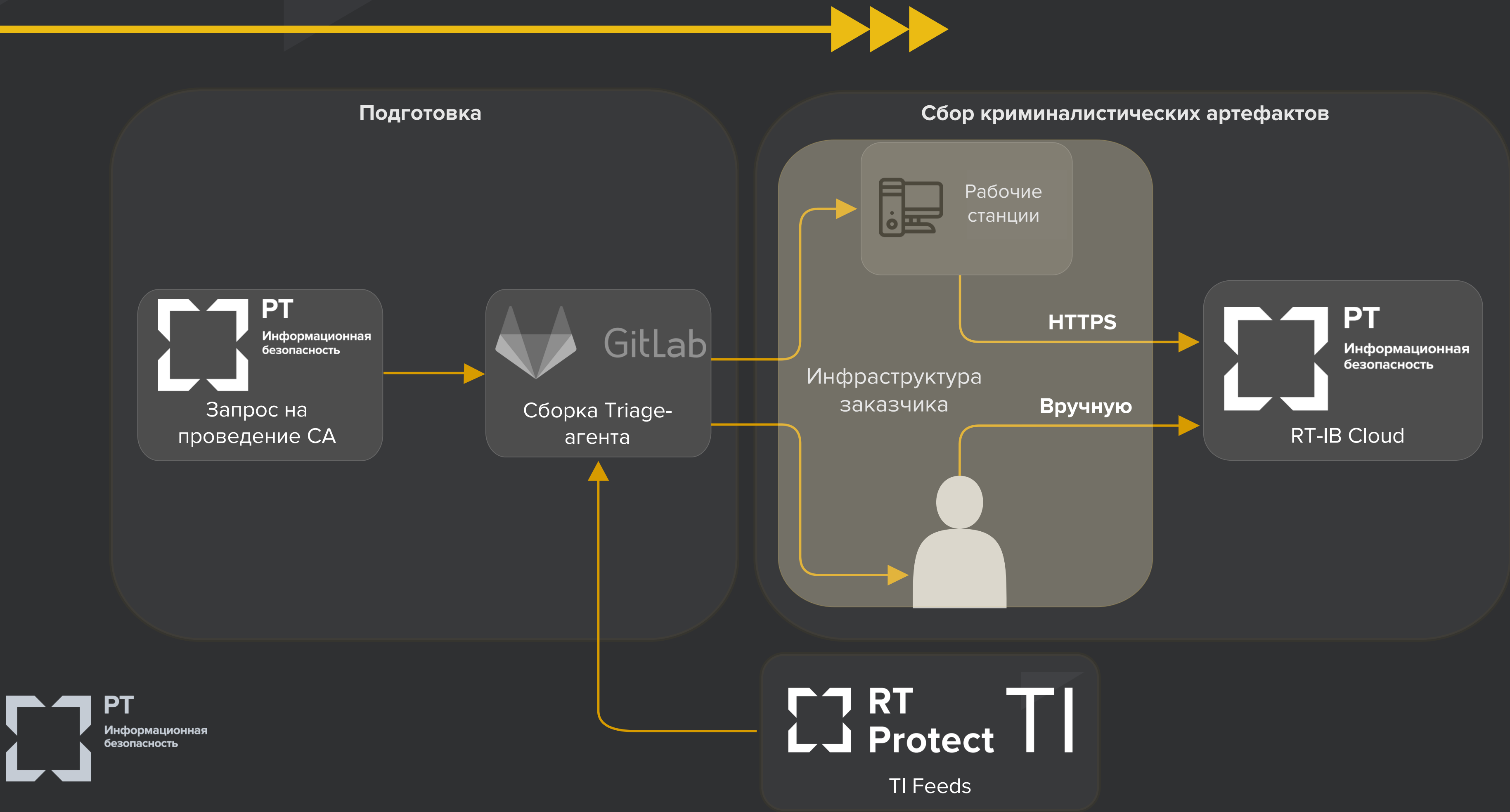
 ir-rescue_DESKTOP-*.zip*

 hollows_hunter_DESKTOP-*.zip*

 rt-retro-result-DESKTOP-*.log

↑ > Сеть > 192.168.1.6 > Test_Share		
Имя	Тип	
 DESKTOP-[REDACTED].log	Текстовый докум...	
 DESKTOP-[REDACTED]-RESULT.zip	Архив ZIP - WinR...	

Этап сбора артефактов



Нормализация

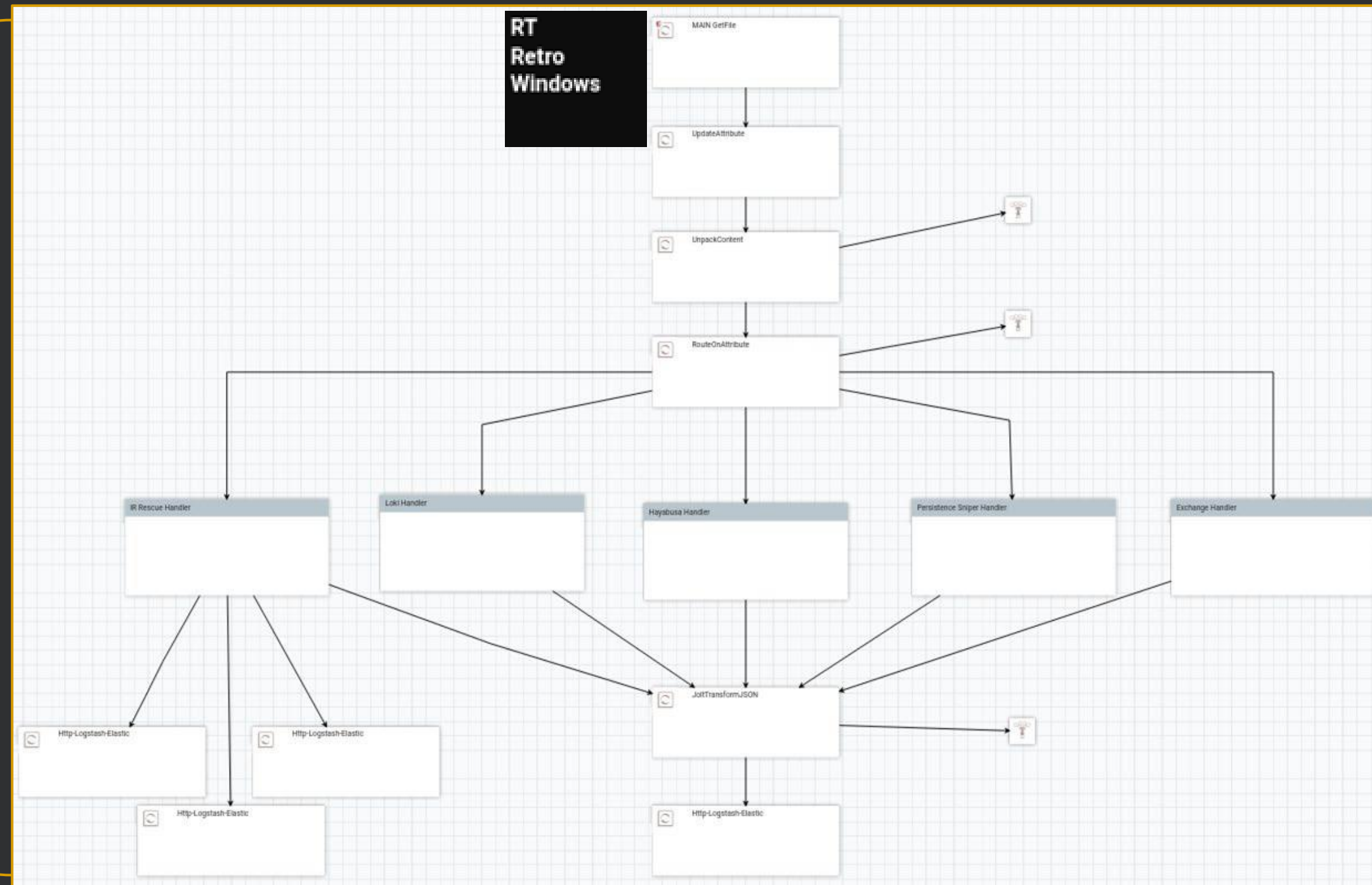


Rt-Retro Linux					
	0		0		0
	32		0		0
Queued	10 (516.13 MB)				
In	0 (0 bytes) → 0				5 min
Read/Write	0 bytes / 0 bytes				5 min
Out	0 → 0 (0 bytes)				5 min
	0		0		0
	0		0		0

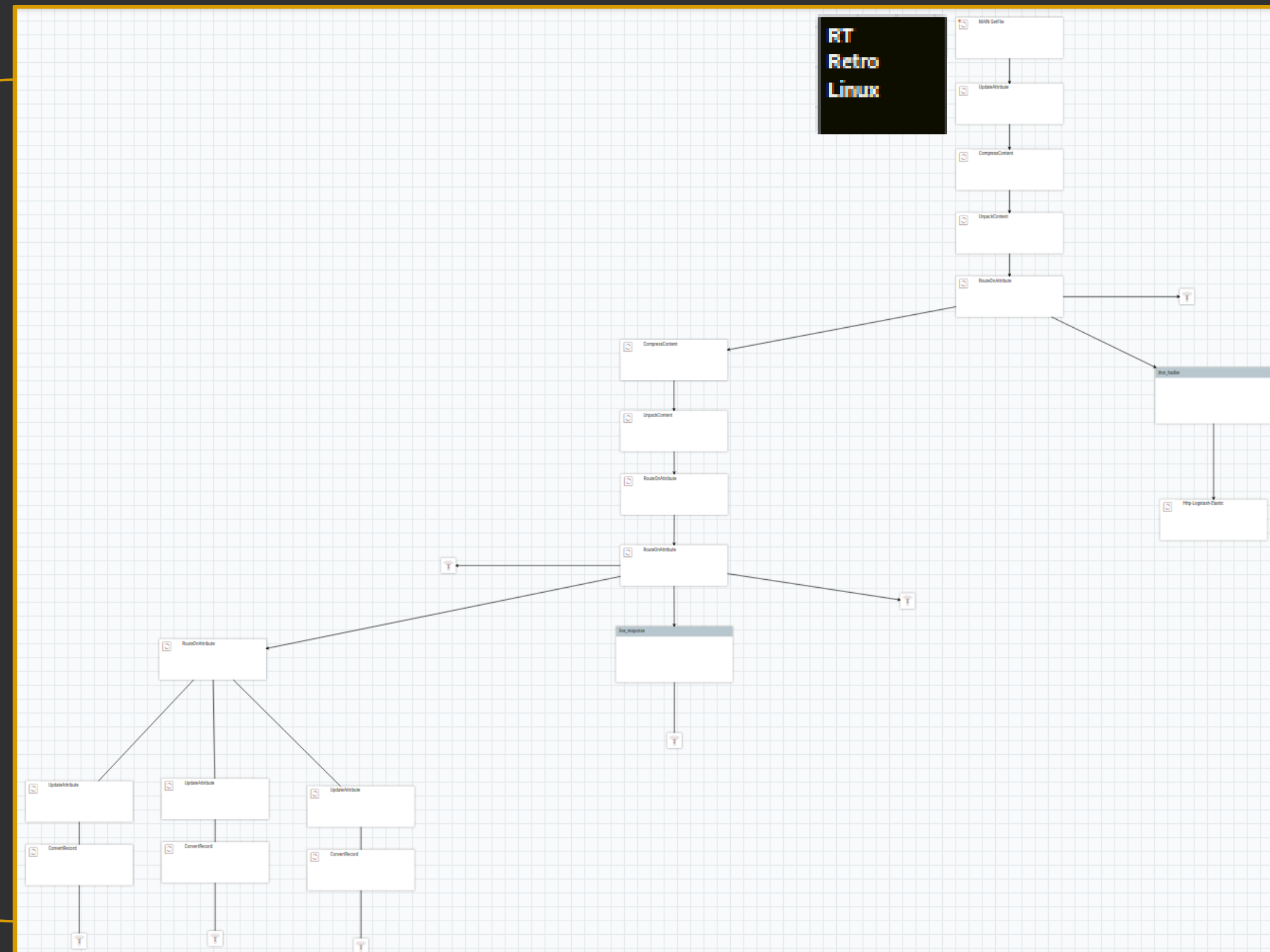
Rt-Retro Windows					
	0		0		0
	93		1		0
Queued	0 (0 bytes)				
In	0 (0 bytes) → 0				5 min
Read/Write	0 bytes / 0 bytes				5 min
Out	0 → 0 (0 bytes)				5 min
	0		0		0
	0		0		0



Нормализация Windows

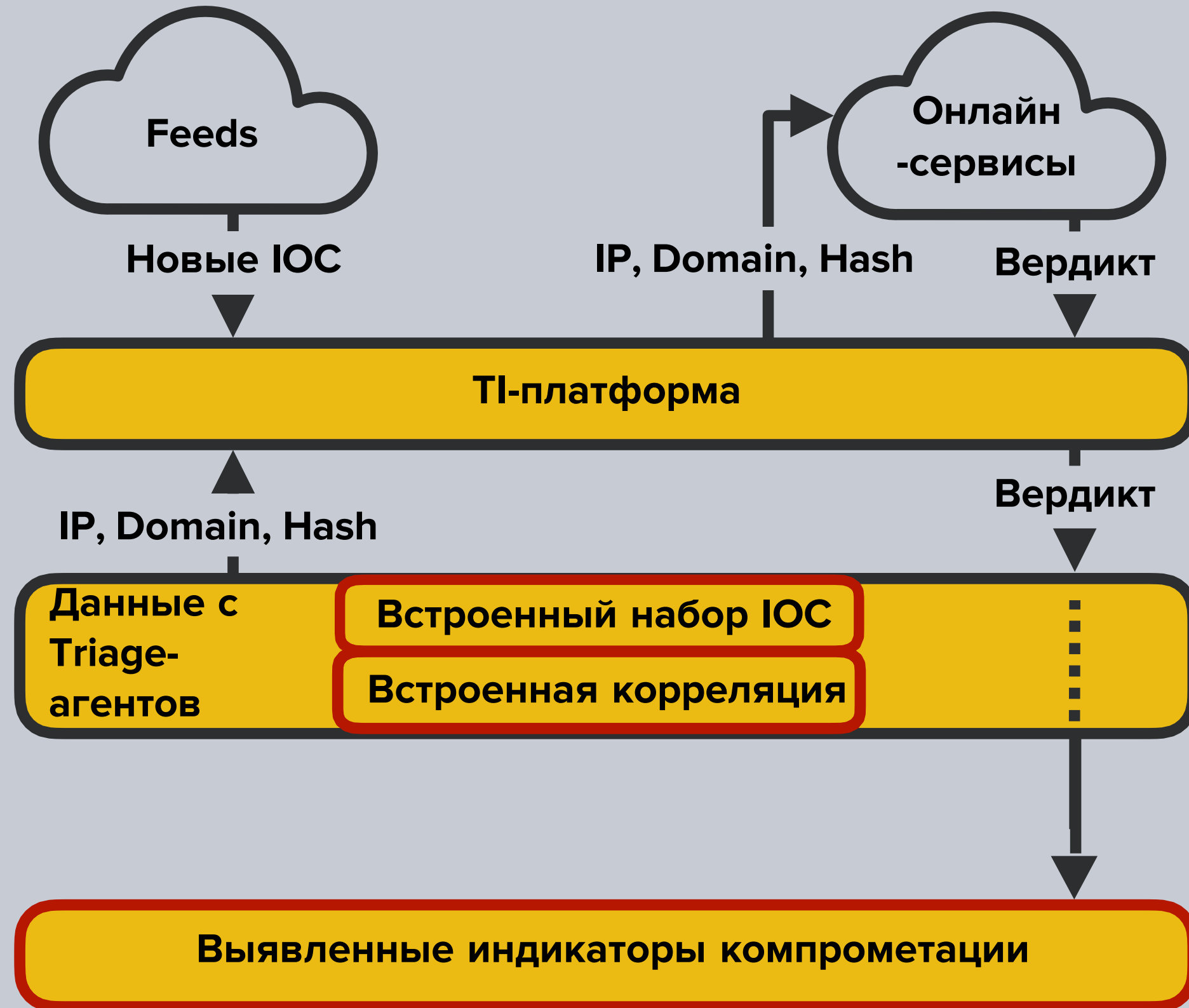


Нормализация Linux



Интеграция с TI

- Обогащение данных об артефактах, собранных с конечных точек



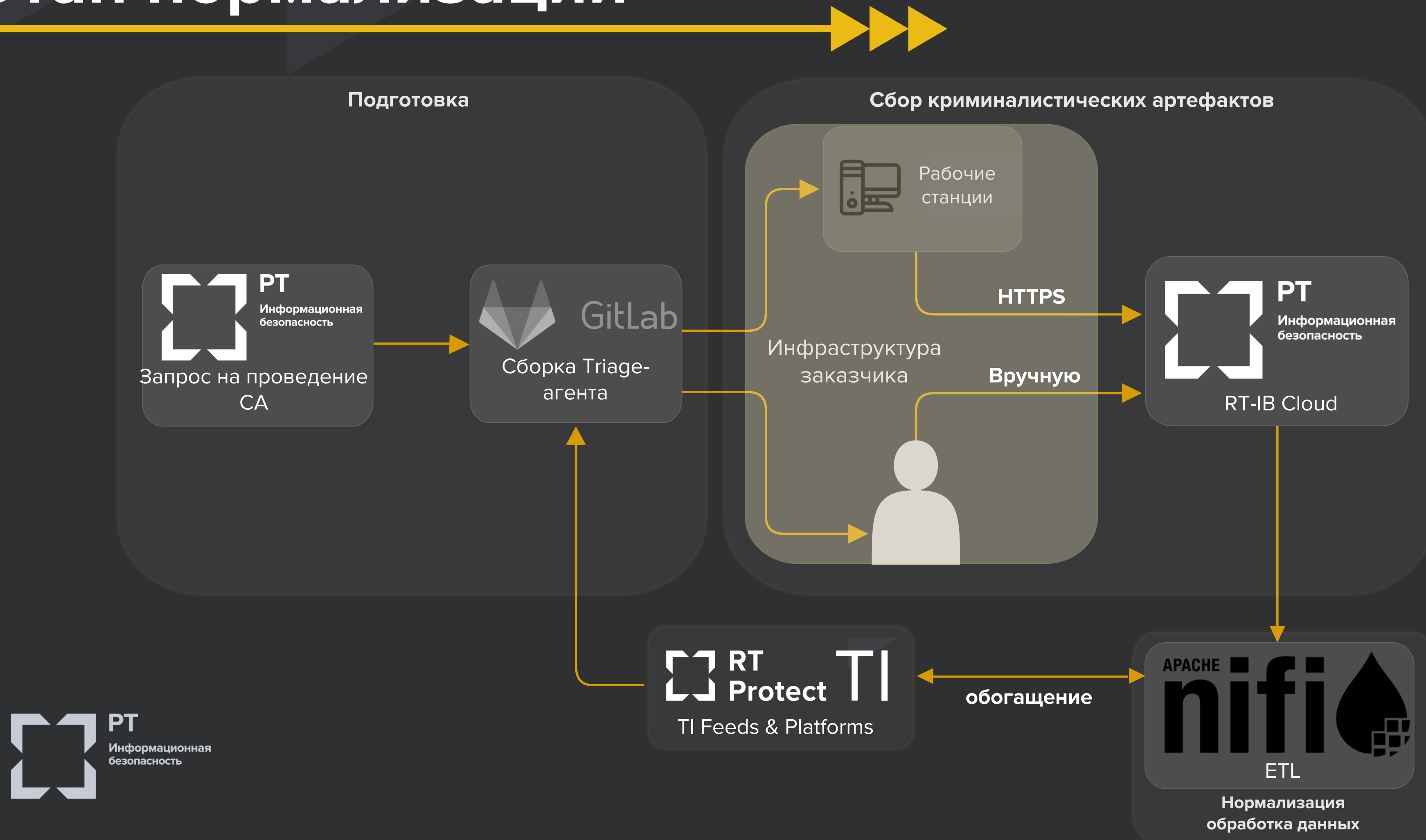
Результат обогащения артефактов



artifact.ti_url	https://ti.rt-protect.ru/artifact/ip/61.160.194.160
destination.ip	61.160.194.160
destination.port	443
dst.ip	61.160.194.160
dst.port	443
enrichment.feed	VirusTotal
enrichment.info	Информация об IP-адресе содержится в источнике данных VirusTotal
enrichment.ioc	61.160.194.160
enrichment.severity	98
enrichment.verdict	Malicious

event.status	ESTABLISHED
network.transport	TCP
process.name	firefox.exe
process.pid	8,680
retro.host.name	
retro.investigation.mark	null
retro.org.name	
retro.source.name	conn.txt
retro.source.path	net/conn.txt
retro.triage.date	Aug 22, 2024 @ 03:00:00.000
retro.triage.name	2024-08-22.zip

Этап нормализации



Нормализация журналов Auditd и WinEvt



Processors

Import processors

Test pipeline: Add documents

Use processors to transform data before indexing. Learn more.

Set

Sets value of "event.ingested" to "{_ingest.timestamp}"

...

Pipeline

Runs the "retro-security" ingest pipeline

...

Pipeline

Runs the "retro-sysmon" ingest pipeline

...

Pipeline

Runs the "retro-powershell" ingest pipeline

...

Pipeline

Runs the "retro-powershell_operational" ingest pipeline

...

Set

Sets value of "host.os.type" to "windows"

...

Set

Sets value of "host.os.family" to "windows"

...

Ingest-Pipeline нормализации Auditd

A description of what this pipeline does.

retro-auditd

Processors

Import processors

Test pipeline: Add documents

Use processors to transform data before indexing. Learn more.

Set

Sets value of "event.ingested" to "{_ingest.timestamp}"

...

Set

Sets value of "@timestamp" to the value of "event.ingested"

...

Set

Sets value of "program" to "audit"

...

Grok

Extracts values from "message" that match a grok pattern

...

Key-value (KV)

Extracts key-value pairs from "auditd.log.kv" and splits on "\s(?:[..."

...

Key-value (KV)

Extracts key-value pairs from "auditd.log.sub_kv" and splits on ...

...

Rename

Renames "message" to "event.original"

...

Ingest-Pipeline нормализации WinEvt



Корреляция событий всеми правилами SOC и собственной аналитикой

winlogbeat-*

Tags 143

Last response 3

Elastic rules (645) Custom rules (748)

Enabled rules Disabled rules

Showing 1-20 of 744 rules | Selected 0 rules | Select all 744 rules Bulk actions Refresh Clear filters Updated 17 seconds ago On

Rule

Remote PowerShell Session From...

Suspicious Exchange Mailbox Per...

Unusual Child Processes of RunD...

Renamed SysInternals Debug View

Encoded FromBase64String

Suspicious Service Path Modifica...

Clearing Windows Console History

Suspicious Compression Tool Par...

auditd-*

Tags 245

Last response 3

Elastic rules (875) Custom rules (1229)

Enabled rules Disal

Showing 1-20 of 192 rules | Selected 0 rules | Select all 192 rules Bulk actions Refresh Clear filters Updated 34 seconds ago

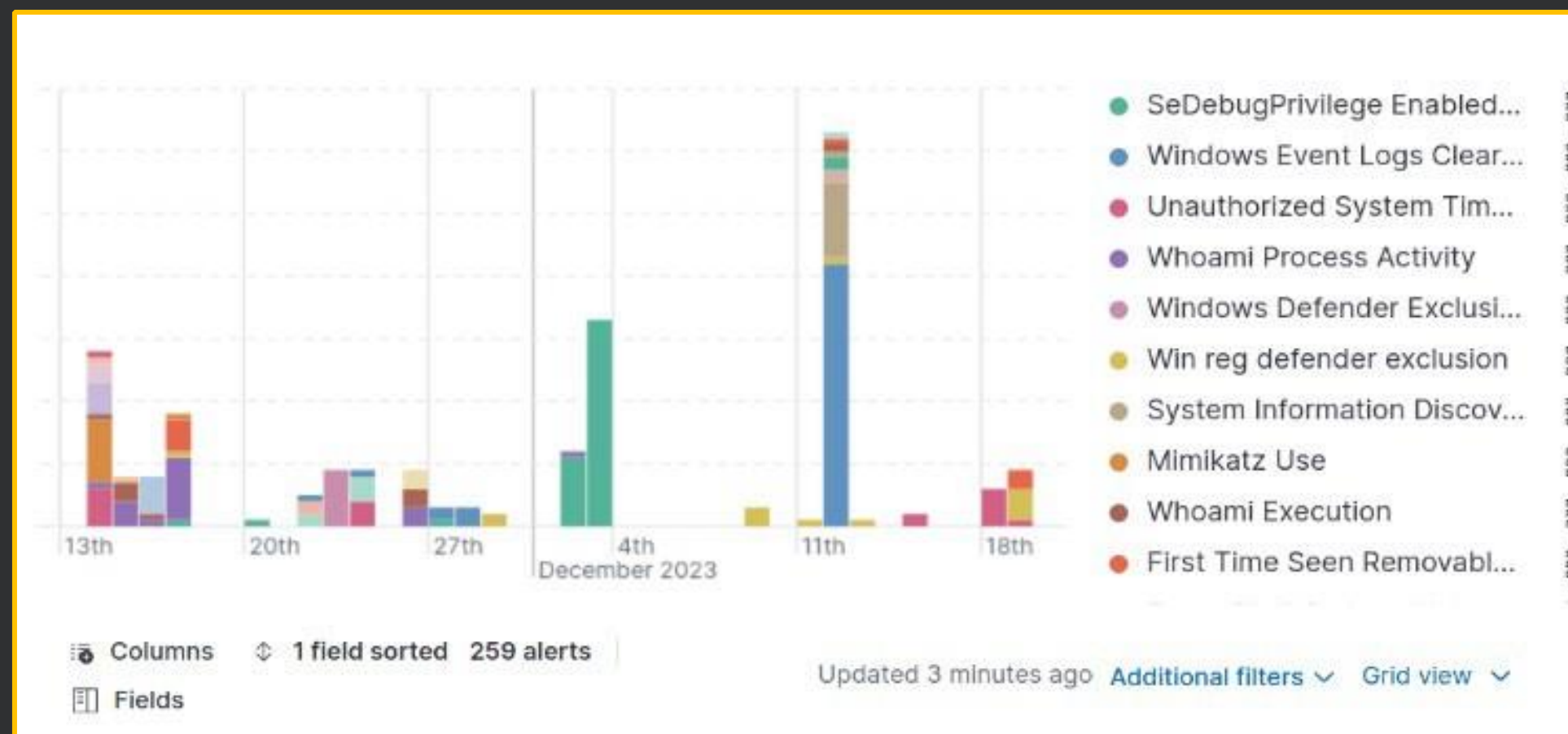
Rule		Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
Triple Cross eBPF Rootkit Install Commands	2	65	High	6 minutes ago	Succeeded	Nov 28, 2023 @ 1...		
Network Sniffing - Linux	3	5	Low	6 minutes ago	Succeeded	Nov 28, 2023 @ 1...		
ESXi Syslog Configuration Change Via ESXCLI								
Data Exfiltration with Wget								
Steganography Unzip Hidden Information Fro...								
Password Policy Discovery								
Shell Execution Of Process Located In Tmp Di...								
ESXi Admin Permission Assigned To Account ...								
Guacamole Two Users Sharing Session Anom...								
Clear Linux Logs								
Remove Immutable File Attribute - Auditd								

Rule		Risk score	Severity	Last run	Last response
Multiple Hosts With Auth Failure From Ce...	2	73	High	3 minutes ago	Succee...
Unsigned Registry Run Key	2	47	Medium	3 minutes ago	Succee...
Telegram Detected In MFT	2	21	Low	1 minute ago	Succee...
KMSAuto Detected In MFT	2	21	Low	1 minute ago	Succee...
Repack Detected In MFT	2	47	Medium	1 minute ago	Succee...
Torrent Detected In MFT	2	21	Low	1 minute ago	Succee...
Mimikatz Detected In MFT	2	99	Critical	1 minute ago	Succee...
EXE DLL COM DLL BAT SCR VBS i...	4	73	High	34 seconds ago	Succee...
Sensitive Data Detected In MFT	2	21	Low	16 seconds ago	Succee...
Alert In Loki Results	2	73	High	in 47 seconds	Succee...

PT

Информационная
безопасность

Проведение расследования



retro-mft-* retro-usnrnl-* retro-logfile-*

any where (file.path like~ "*"\\AppData*\\Temp*" and
(endsWith(file.name,".exe") or endsWith(file.name,".dll")
or endsWith(file.name,".scr") or
endsWith(file.name,".vbs") or endsWith(file.name,".sys")
or endsWith(file.name,".com"))))

Event Correlation

retro-hayabusa-*

event.code:4625 AND artifact.description.subjectusername:*
AND NOT artifact.description.subjectusername:*\$ AND NOT
artifact.description.subjectusername:SYSTEM

Threshold

None

Results aggregated by retro.host.name >= 1

retro-*

artifact.ti_url:* AND NOT artifact.ti_url:"local" AND NOT event.severity: "0"

Query



PT

Информационная
безопасность

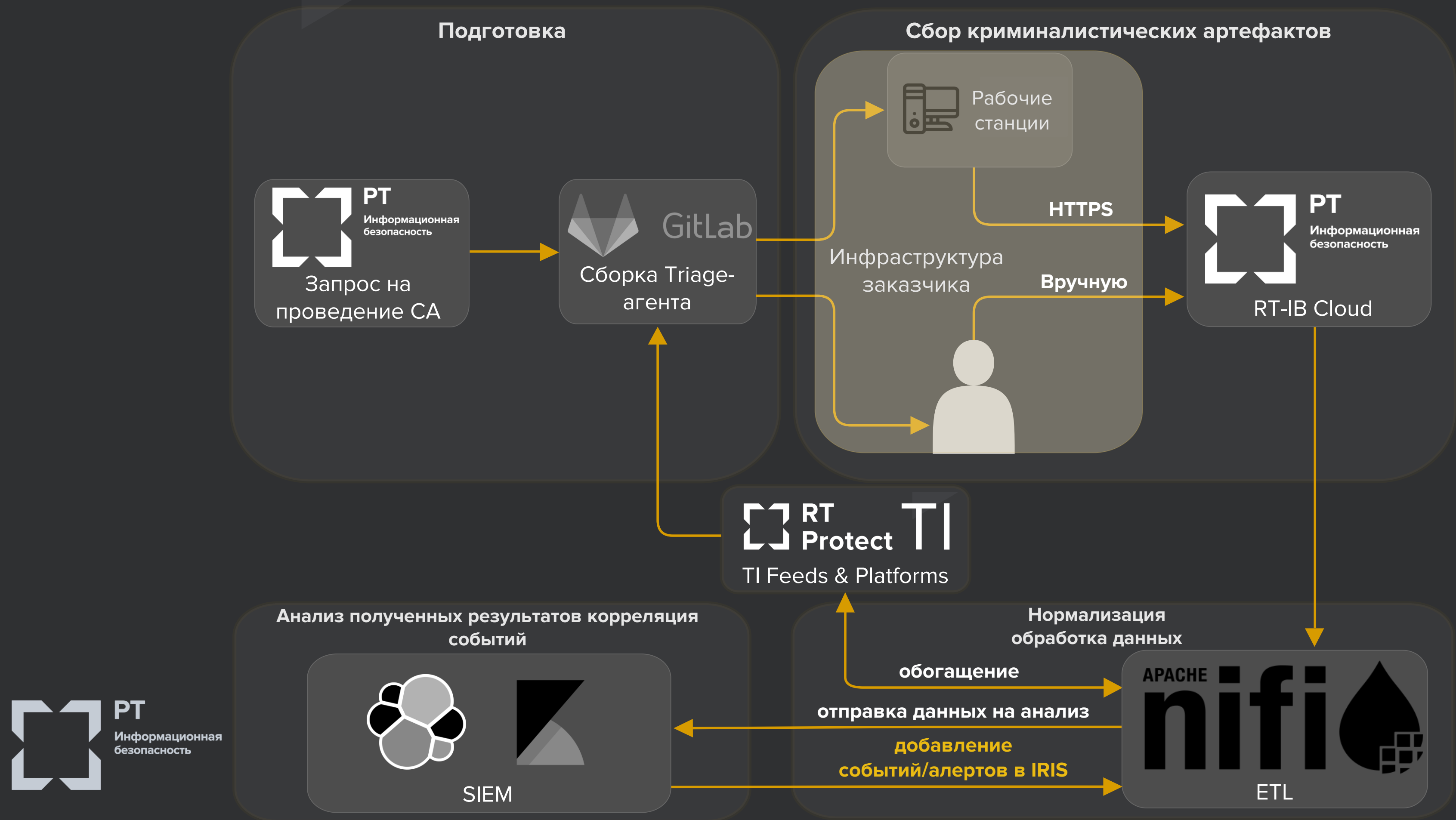
Проведение расследования



artifact.description.reason_2.matches	\$lsass: 'System32\lsass.exe'
artifact.description.reason_2.score	70
artifact.description.reason_2.value	Yara Rule
artifact.description.score	150
artifact.description.sha1	ce5948945086d9761ea220f08e8c4e9c1208b928 SHA256: a90d1205b453
artifact.severity	ALERT
artifact.type	FileScan
retro.host.name	DESKTOP_INFECTED
retro.investigation.mark	null
retro.org.name	Organization_name
retro.source.name	loki_DESKTOP_INFECTED_2023-09-14_17-36-51.log
retro.source.path	rt-retro-result-DESKTOP_INFECTED-20230914/loki_DESKTOP_INFECTED-20230914.zip
retro.triage.name	rt-retro-result-Organization name-DESKTOP_INFECTED-20230914.zip

Field	Value
_id	_43BEo0BWpg12MHDKLPZ
_index	retro-loki
_score	0
@timestamp	2023-09-14 15:35:12.000
artifact.description.accessed	Wed Sep 13 10:35:08 2023
artifact.description.file	C:\Users\pwned\AppData\Local\Temp\lsass.DMP
artifact.description.first_bytes	4d444d5093a7f1a0100000002000000000000000 / <
artifact.description.md5	fe0db2bb3933ae584da557c74c7f0c8a
artifact.description.modified	Wed Sep 13 10:35:10 2023
artifact.description.reason_1.desc	LSASS process memory dump names
artifact.description.reason_1.pattern	\\lsass\.(dmp DMP)
artifact.description.reason_1.score	80
artifact.description.reason_1.value	File Name IOC matched
artifact.description.reason_2.description	LSASS minidump file for mimikatz
artifact.description.reason_2.match	mimikatz_lsass_mdmp

Этап корреляции и анализа



Как интегрировать Kibana и IRIS?

Через Apache NiFi реализуем интеграцию с IRIS используя API

В каждом документе сформируем специальное поле с гиперссылкой на обработчик NiFi

По полученному *_id* документа заберём его из базы и направим в IRIS

retro.source.name	autoruns.txt
retro.source.path	[REDACTED]/mal/autoruns/autoruns.txt
retro.triage.date	Aug 22, 2024 @ 03:00:00.000
retro.triage.name	[REDACTED]_2024-08-22.zip
retro.url	Add to IRIS
time_flag	23

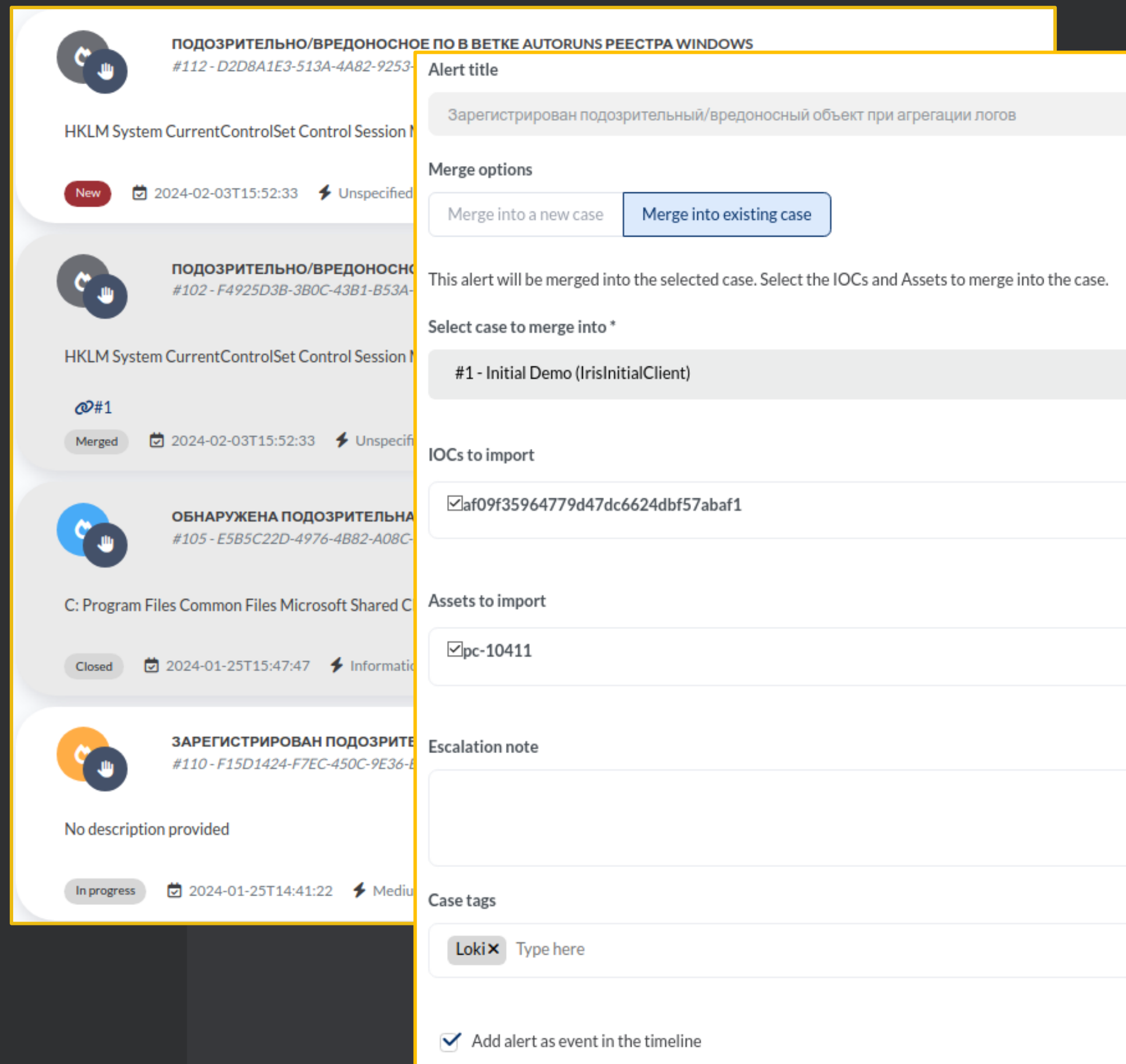
Результат: в кейс расследования добавлен артефакт из Kibana

Что это дает?

Первичная корреляция данных правилами SOC и их обработка в Kibana позволяет подключить аналитиков 1-й линии

По одной кнопке подозрительные события направляются в IRIS

Аналитики L2-L3 подключаются для анализа событий в IRIS после их первичной обработки на L1



The screenshot displays the IRIS interface. On the left, a list of alerts is shown:

- Alert 1:** ПОДОЗРИТЕЛЬНО/ВРЕДНОСНОЕ ПО В ВЕТКЕ AUTORUNS РЕЕСТРА WINDOWS (#112 - D2D8A1E3-513A-4A82-9253-...). Status: New. Date: 2024-02-03T15:52:33. Unspecified.
- Alert 2:** ПОДОЗРИТЕЛЬНО/ВРЕДНОСНОЕ (#102 - F4925D3B-3B0C-43B1-B53A-...). Status: Merged. Date: 2024-02-03T15:52:33. Unspecified.
- Alert 3:** ОБНАРУЖЕНА ПОДОЗРИТЕЛЬНАЯ (#105 - E5B5C22D-4976-4B82-A08C-...). Status: Closed. Date: 2024-01-25T15:47:47. Informational.
- Alert 4:** ЗАРЕГИСТРИРОВАН ПОДОЗРИТЕЛЬНЫЙ (#110 - F15D1424-F7EC-450C-9E36-...). Status: In progress. Date: 2024-01-25T14:41:22. Medium.

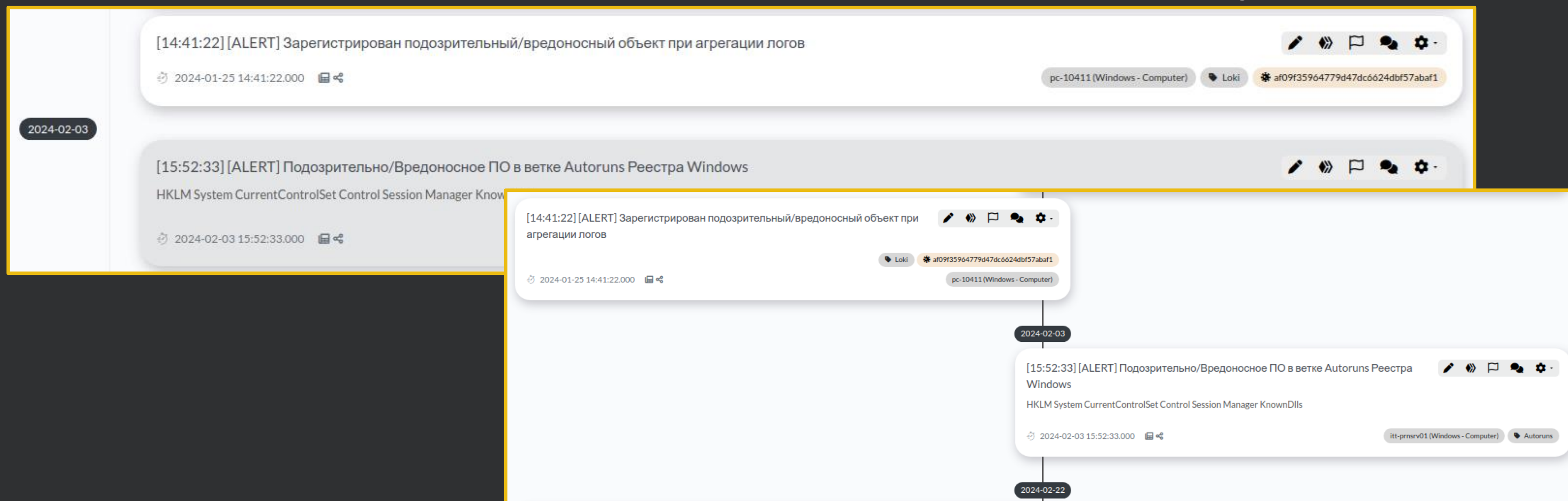
On the right, a 'Merge options' dialog is open for the first alert. It contains the following fields:

- Alert title:** Зарегистрирован подозрительный/вредоносный объект при агрегации логов
- Merge options:** Two buttons: 'Merge into a new case' and 'Merge into existing case'.
- Select case to merge into *:** A dropdown menu showing '#1 - Initial Demo (IrisInitialClient)'.
- IOCs to import:** A checkbox labeled 'af09f35964779d47dc6624dbf57abaf1' is checked.
- Assets to import:** A checkbox labeled 'pc-10411' is checked.
- Escalation note:** A text input field.
- Case tags:** A search bar with 'Loki' entered and a 'Type here' placeholder.
- Footer:** A checkbox labeled 'Add alert as event in the timeline' is checked.

Проведение расследования



Установление связей между событиями



Выстраивание таймлайна атаки

Проведение расследования



Генерация отчета по шаблону

Select report template ×

Since IRIS v2.0.0, the report generation supports images. Integration of images might fail depending on the situation.
Safe Mode can be used to generate the report without them.

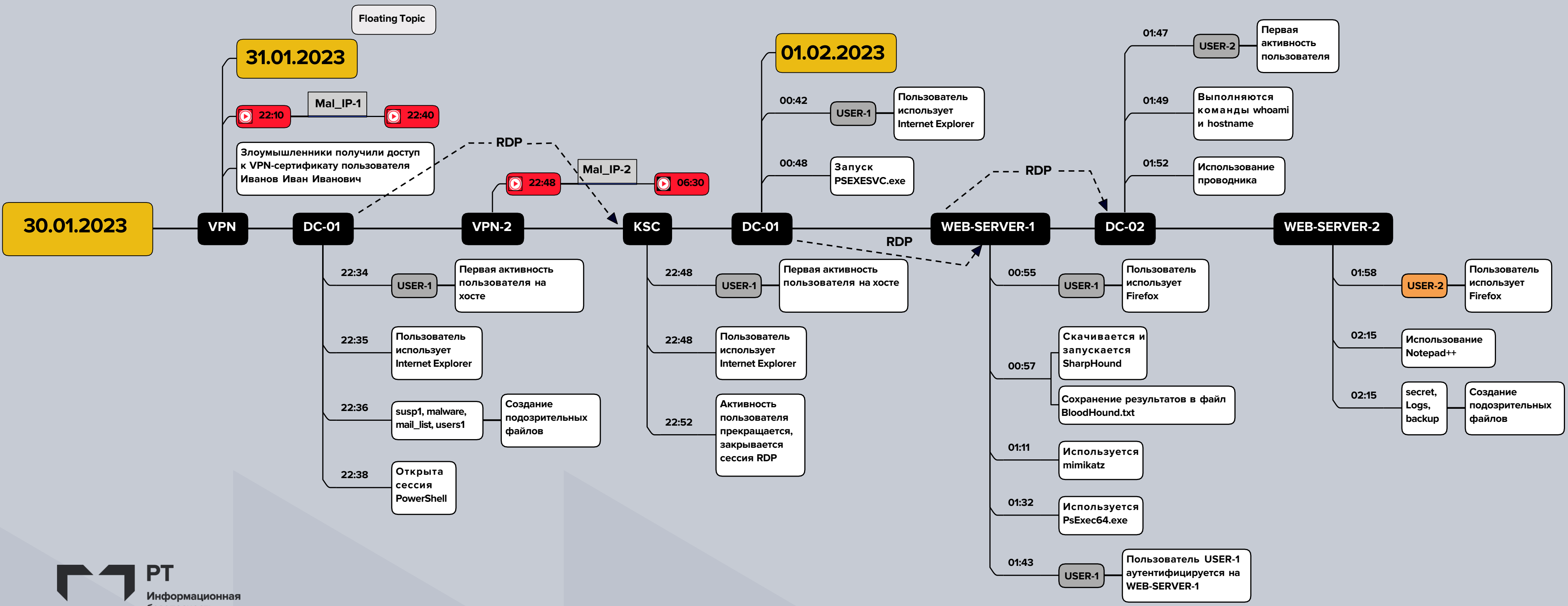
ibr6 (English) 6

Generate in Safe Mode



Формирование графа действий атакующих

Срез информационной безопасности



Подготовка



Информационная
безопасность

Запрос на
проведение СА



GitLab

Сборка Triage-
агента

Сбор криминалистических артефактов



Рабочие
станции

HTTPS

Вручную

Инфраструктура
заказчика



Информационная
безопасность

RT-IB Cloud



RT
Protect



TI-Feeds
&
Platforms

Анализ полученных результатов
корреляция событий



SIEM

Нормализация
обработка данных

обогащение

отправка данных на анализ

добавление событий/алертов
в IRIS



ETL

Сбор результатов анализа и создание отчета



Отчёт



IRIS

CIRP

Жизненный цикл автоматизированного Compromise Assessment

Что получает исполнитель?



Автоматизированный
процесс сбора данных



Автоматизированные
процессы нормализации и
обогащения данных



Автоматизированный
процесс выявления
артефактов и их анализа



Оптимизированный и
автоматизированный процесс
формирования отчета



Что получает заказчик?



Появляется возможность более оперативного реагирования на инциденты и принятия мер по локализации, ликвидации и восстановлению



Возможность своевременно принять необходимые меры по улучшению политик безопасности

Результат

- «Срез» состояния ИБ своей инфраструктуры с точки зрения наличия вредоносной активности
- Таймлайны произошедших атак с описанием обнаруженных инцидентов
- Рекомендации по реагированию на действующие, активные угрозы, а также по их недопущению в будущем



Самое интересное из мира
кибербезопасности у нас в Telegram-канале!



@RTINFOBEZ

Нам доверяют



КБП



СИБЕР



Нацимбио



НОВИКОМБАНК

Контакты

Адрес: 117587, г.

Москва, Варшавское
шоссе, дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru



РТ
Информационная
безопасность

