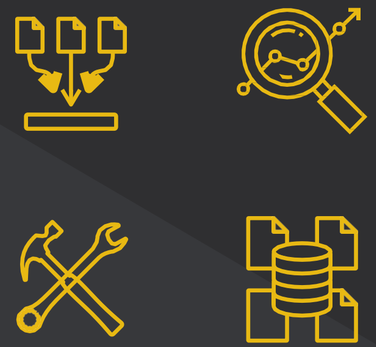
Реально ли идеальное расследование? Быстро - Качественно - Автоматизированно

Слепушенко Олег Андреевич
Ведущий аналитик RT Protect SOC



PT
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

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.

PT
Информационная безопасность

Необходимость

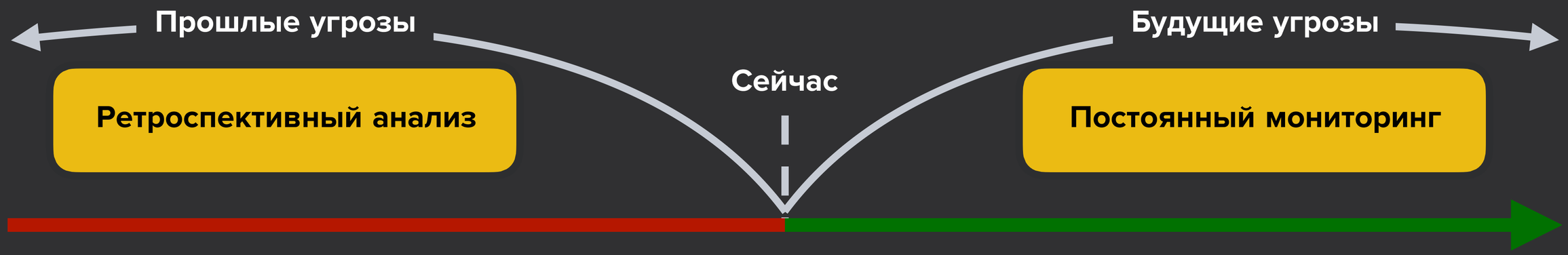
Как понять, что твоя инфраструктура взломана

- **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

PT
Информационная безопасность

Compromise Assessment vs Мониторинг

- Проактивно – EDR, Ретроспективно – CA
- Процесс анализа: сначала CA, потом мониторинг
- Использование данных об актуальных угрозах с TI



PT
Информационная безопасность

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

Оптимизация используемых инструментов в зависимости от точек сбора

Автоматизация процессов нормализации и обогащения данных

Оптимизация процесса анализа собранных данных

PT
Информационная безопасность

Классические задачи DFIR

PT Информационная безопасность

Сбор данных

- Процессы
- Файловая система
- Реестр
- Сеть
- Адреса в памяти
- Пользователи и группы
- Журналы
- Автозагрузки

...

Обнаружение

IoC / IoA

Выявление следов и TTP атакующих

Threat Intelligence Platform

Обогащение собранных данных (IP- адреса, DNS- журналы, активные соединения, Хэш-значения файлов и прочее)

Корреляция данных

Собранные данные коррелируются для выявления аномальных паттернов

Анализ

Проведение глубокой аналитики специалистами SOC

Результат

Доказательства компрометации ИС

Классические задачи DFIR

PT Информационная безопасность

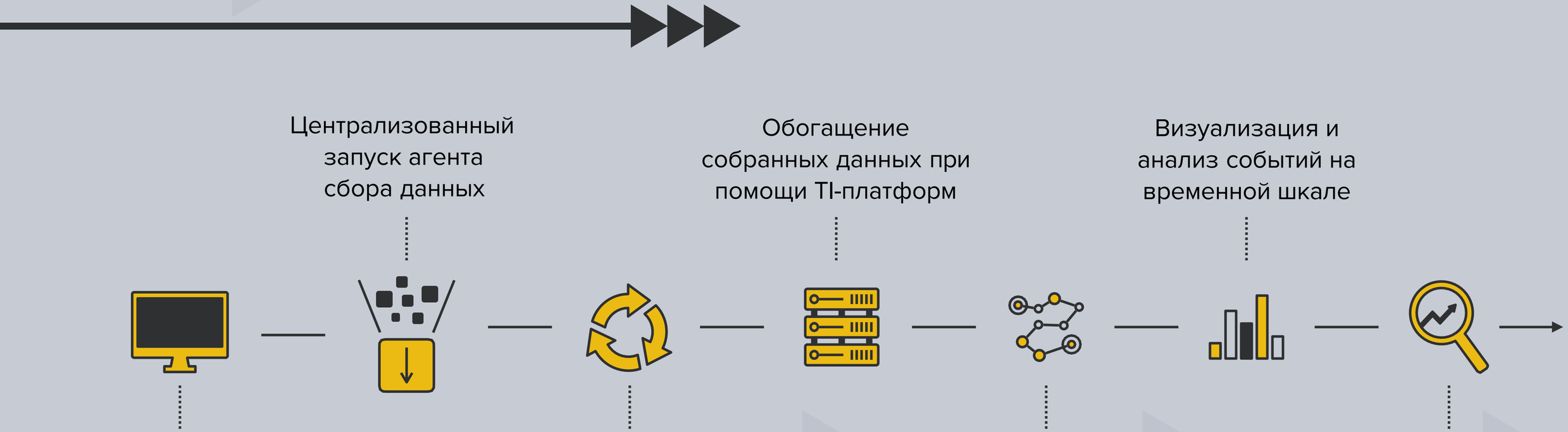
Определение используемых инструментов в зависимости от основных типов конечных систем

Формирование различных сборок инструментов извлечения данных

Проведение сбора, нормализации и анализа данных

Этапы ретроспективного анализа инфраструктуры

PT Информационная безопасность



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

PT
Информационная безопасность

Выбор инструментов

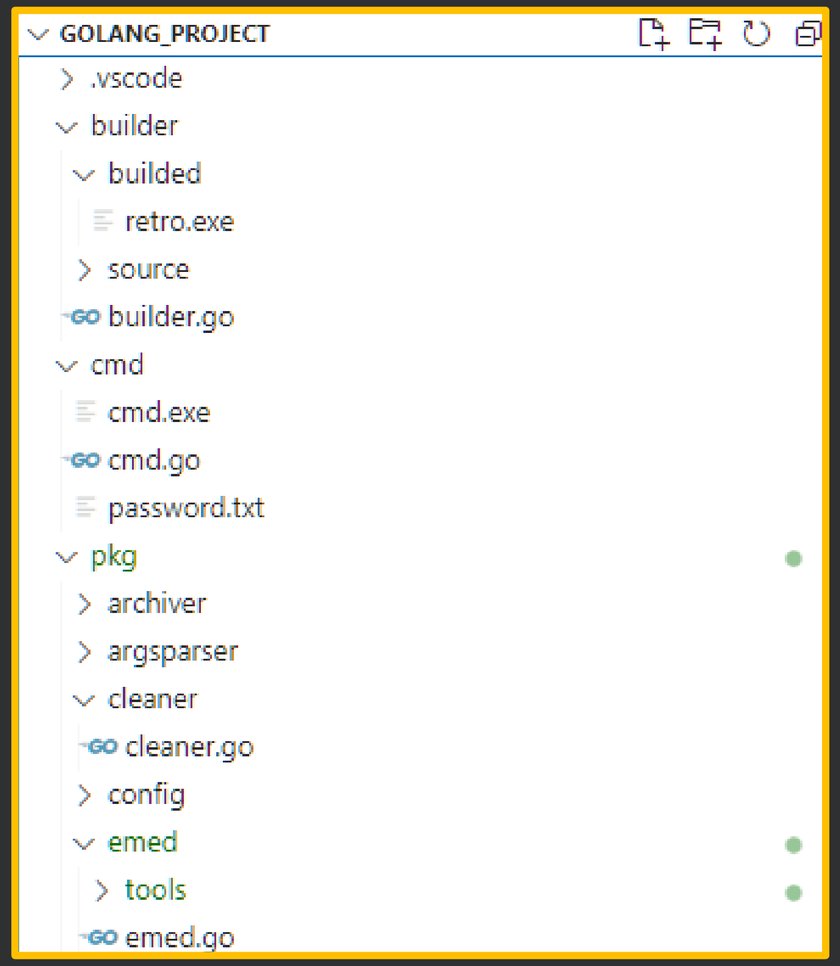
Рекомендуем ознакомиться

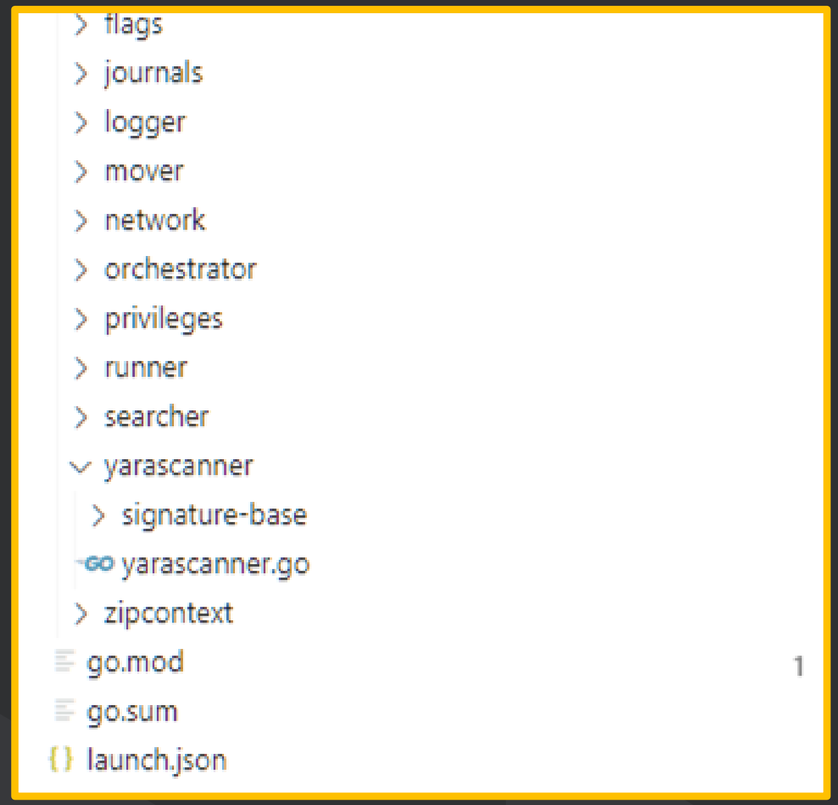
ТОР-10 криминалистических артефактов Windows при расследовании инцидентов

Топ-10 артефактов Linux для расследования инцидентов

PT
Информационная безопасность

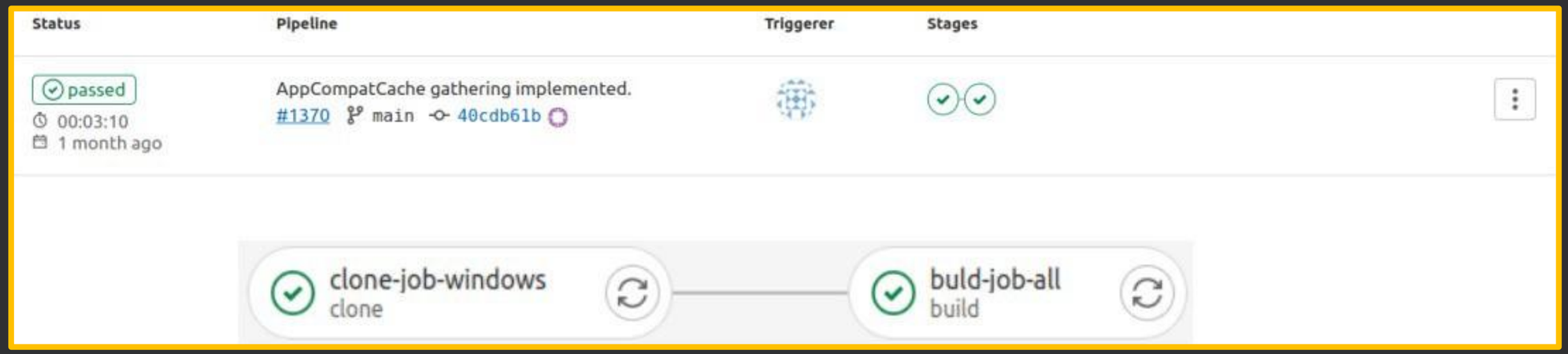
Инструмент сбора Triage





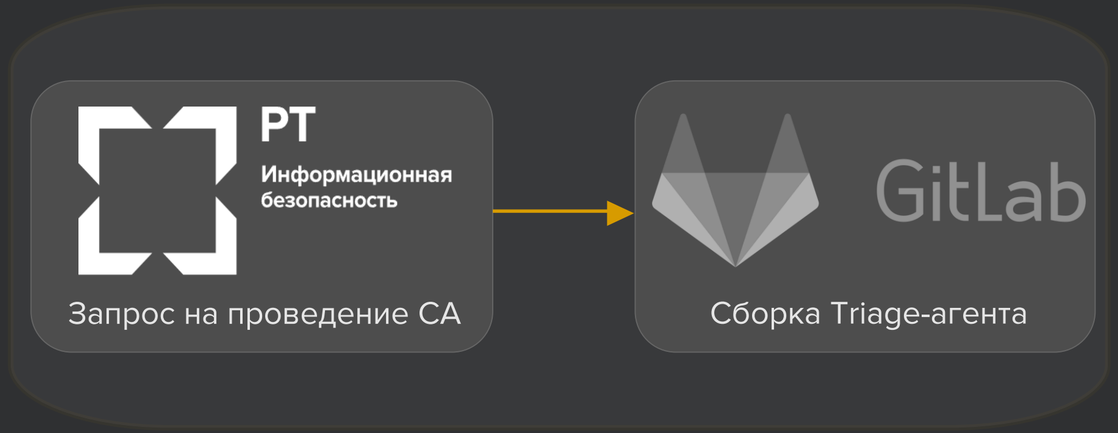
PT
Информационная безопасность

CI/CD для Triage-агента



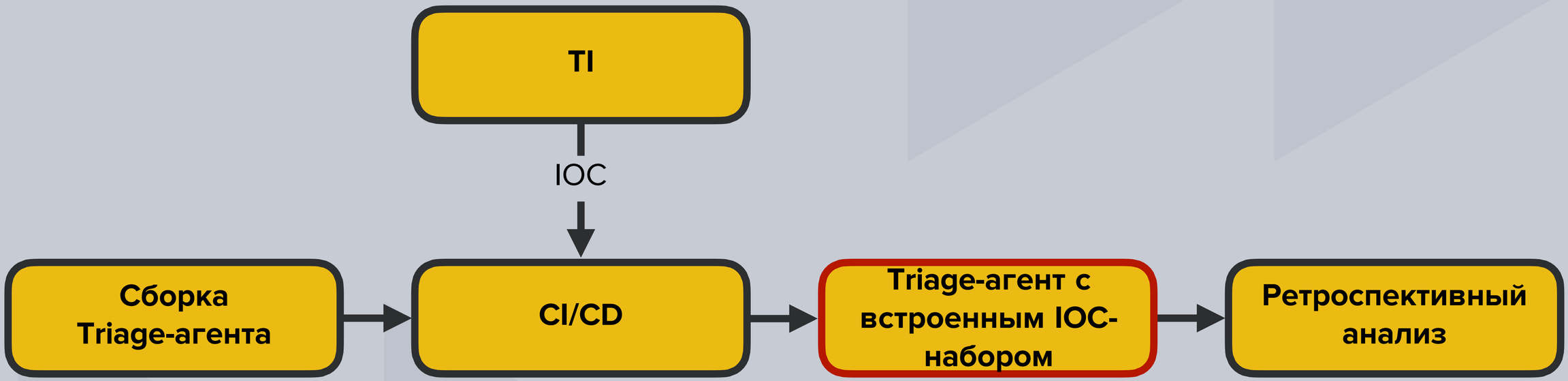
PT
Информационная безопасность

Этап подготовки



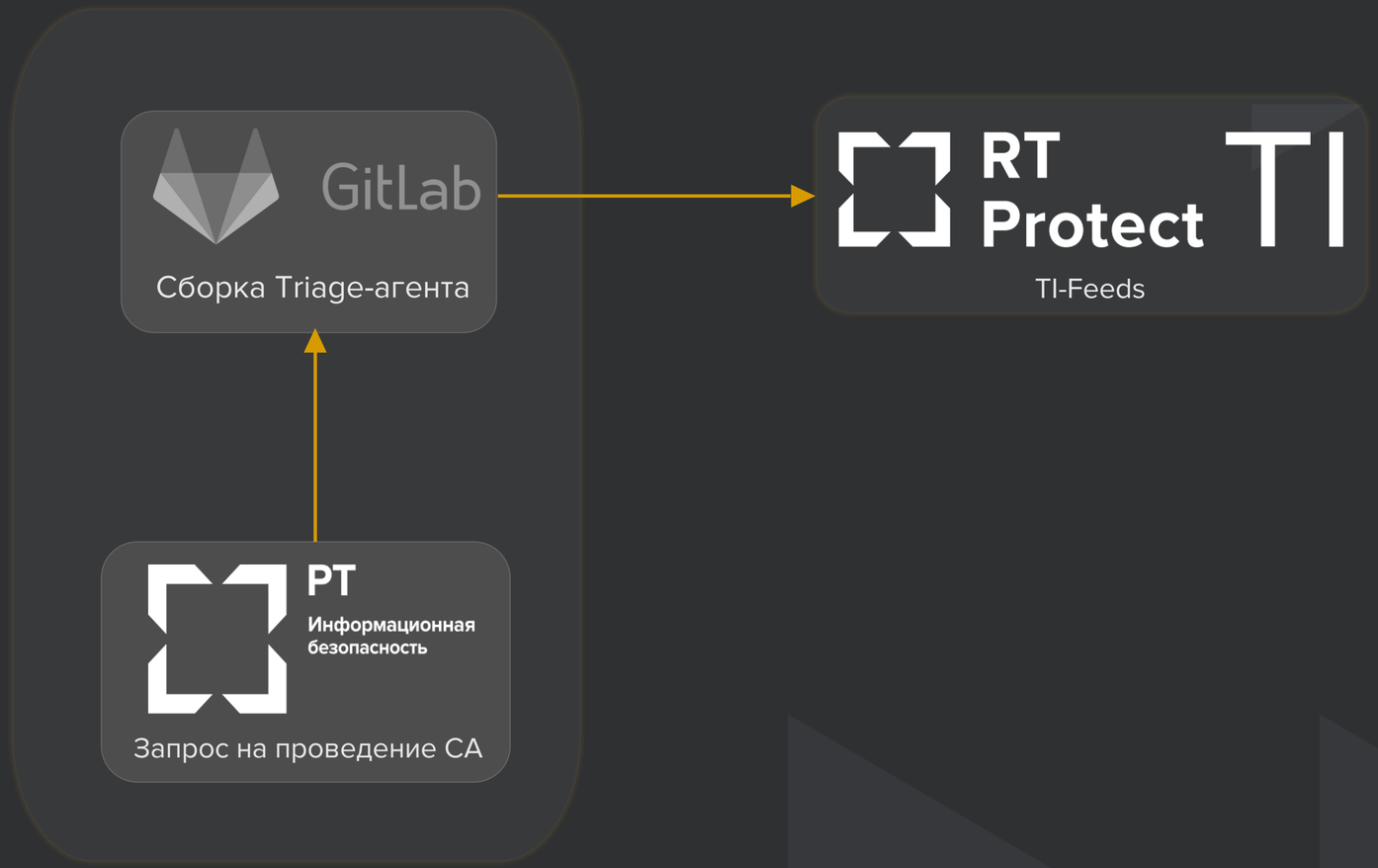
Ретроспективный анализ и Threat Intelligence

Поставка актуальных индикаторов
компрометации при ретроспективном анализе



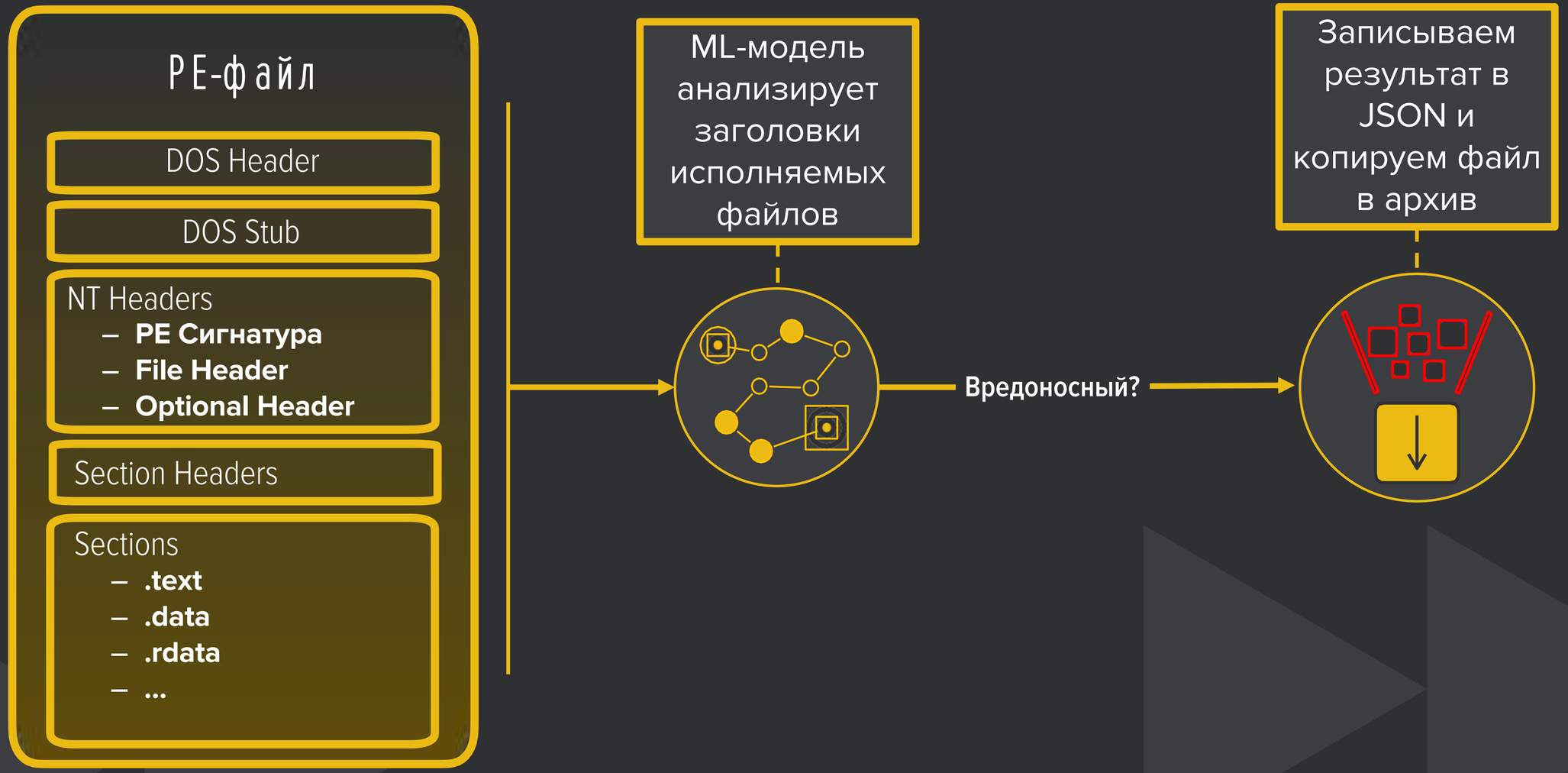
PT
Информационная безопасность

Этап подготовки

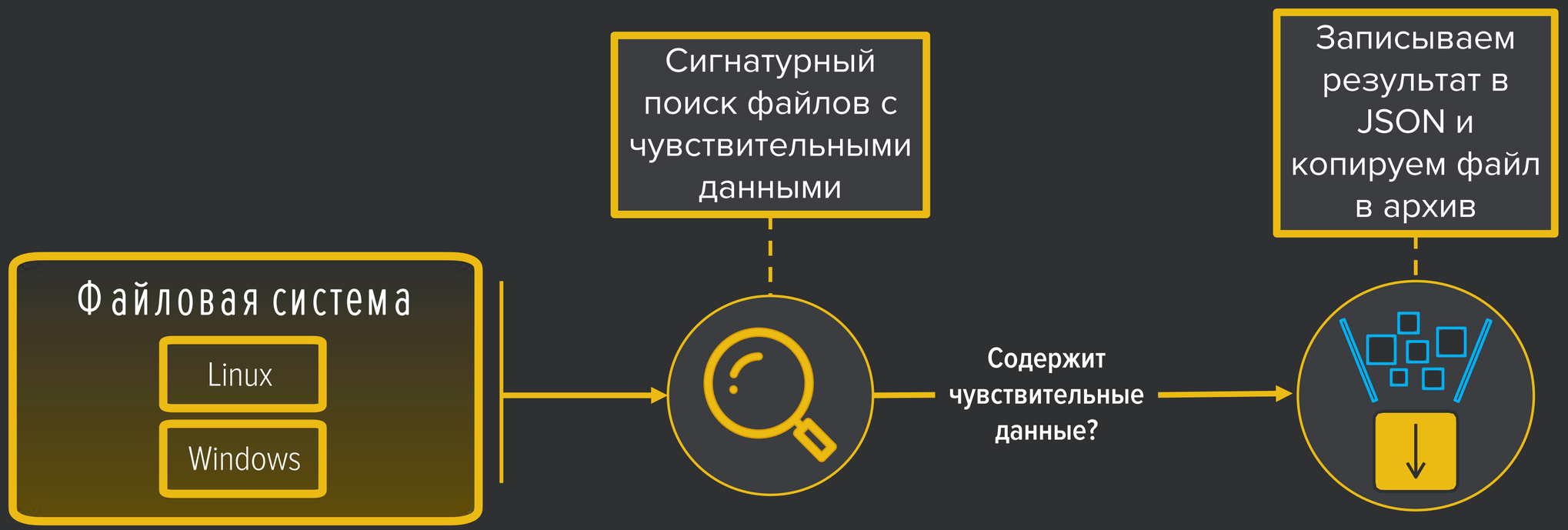


PT
Информационная безопасность

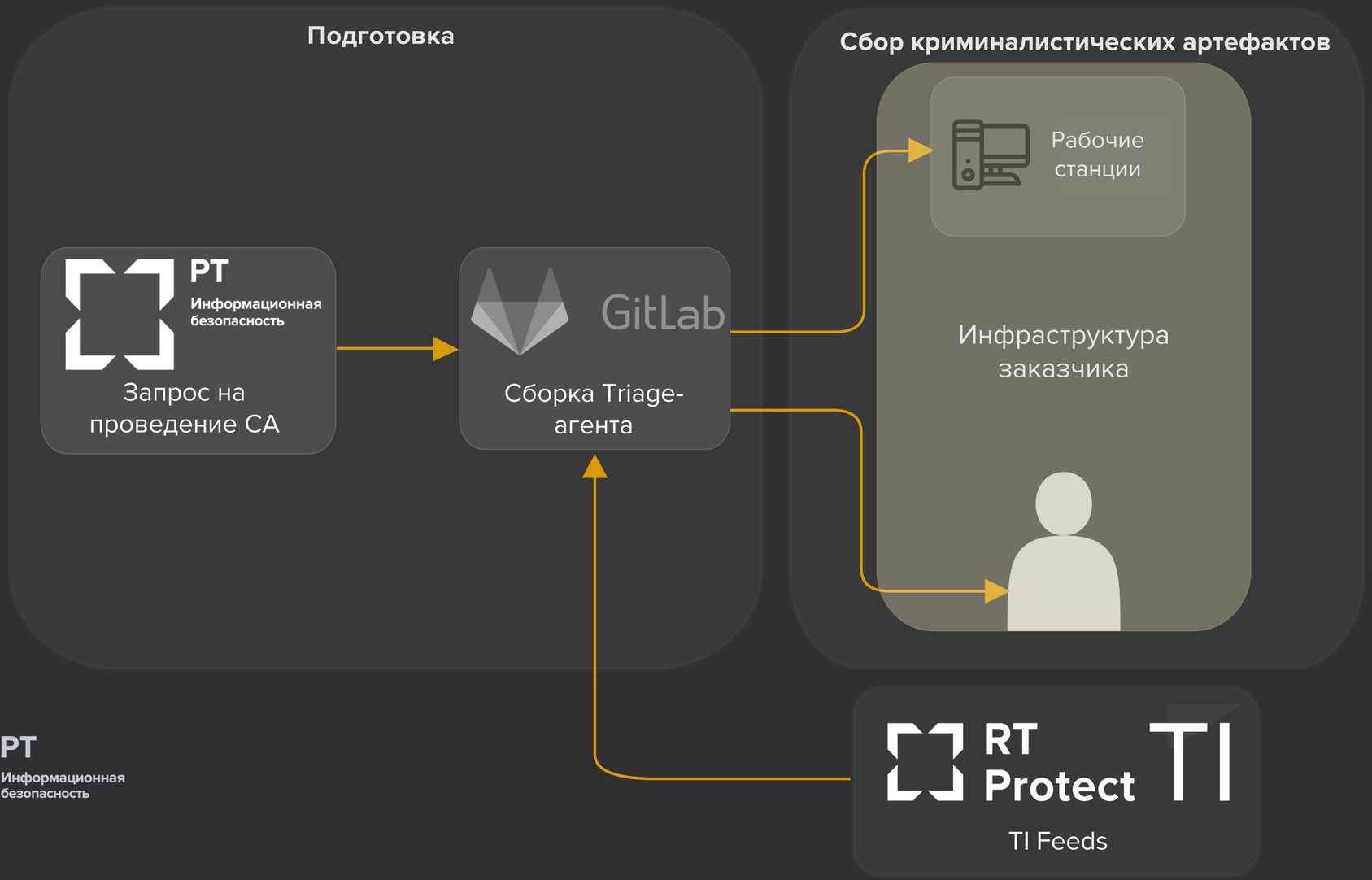
Анализ всех хэшей? Нет...



Поиск паролей в открытом виде? Да!

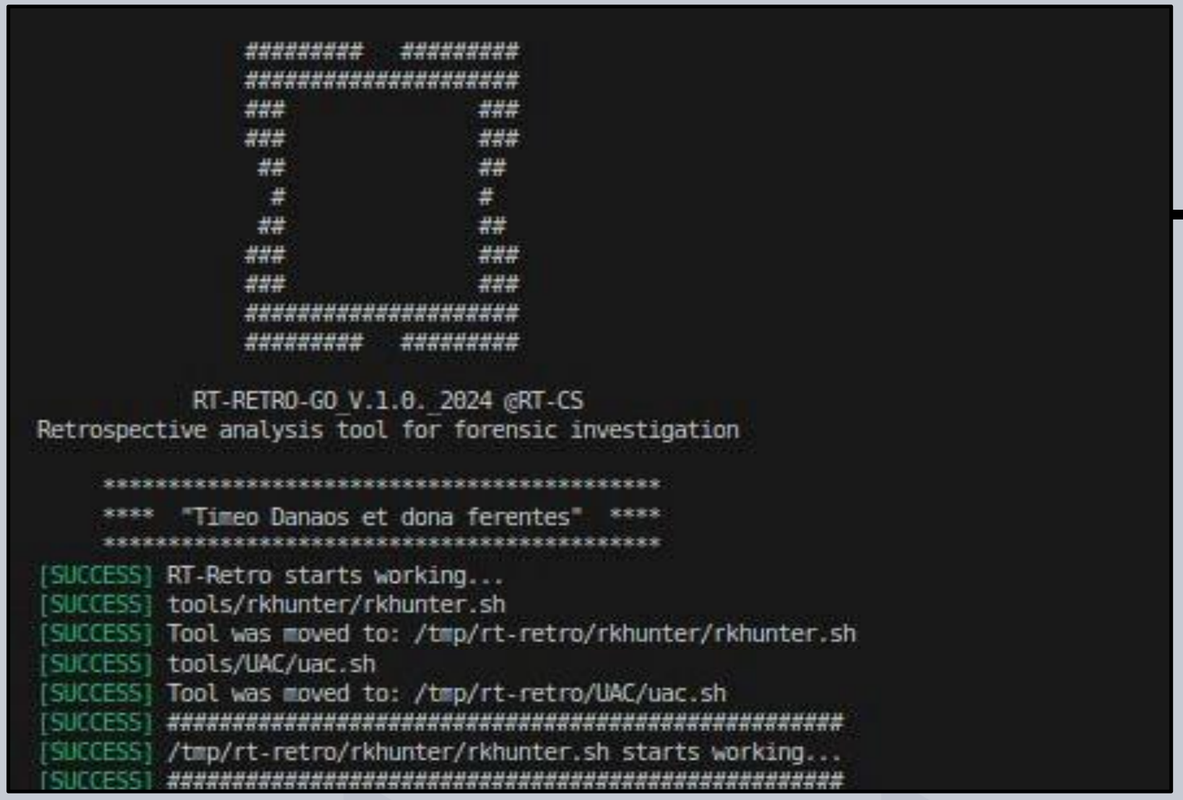


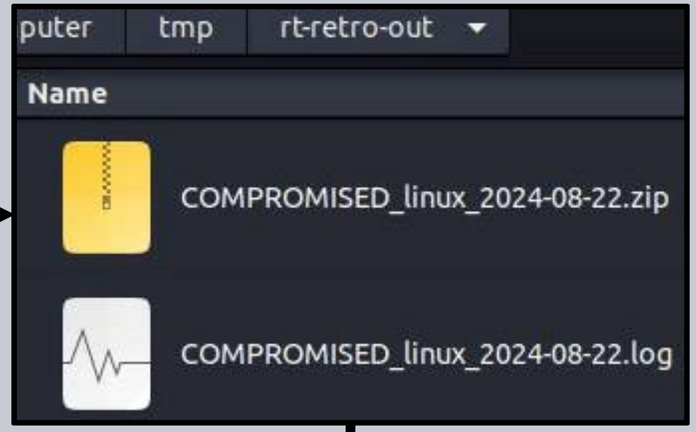
Этап сбора артефактов

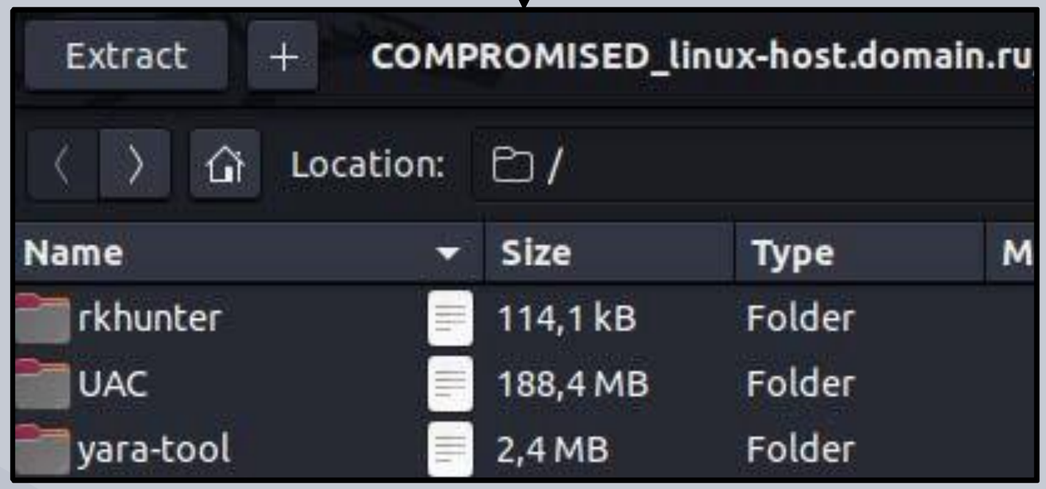


PT
Информационная безопасность

Результат работы Triage-агента на Linux

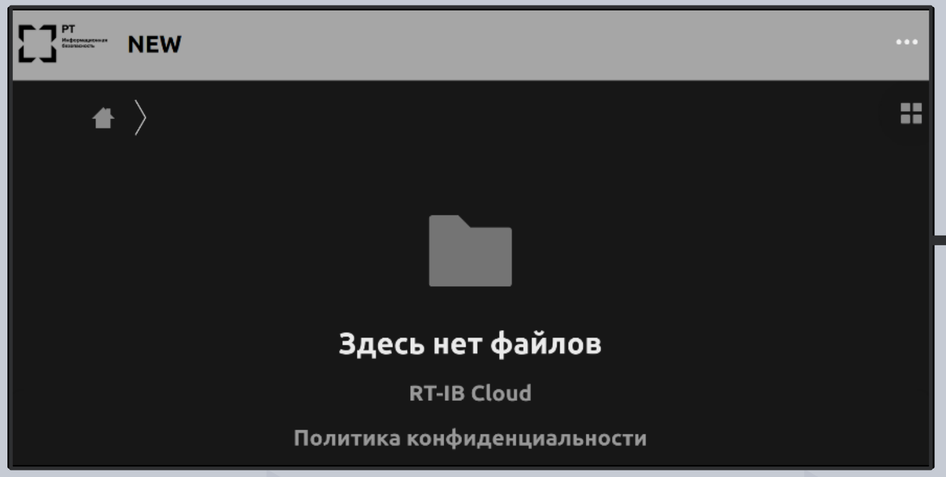


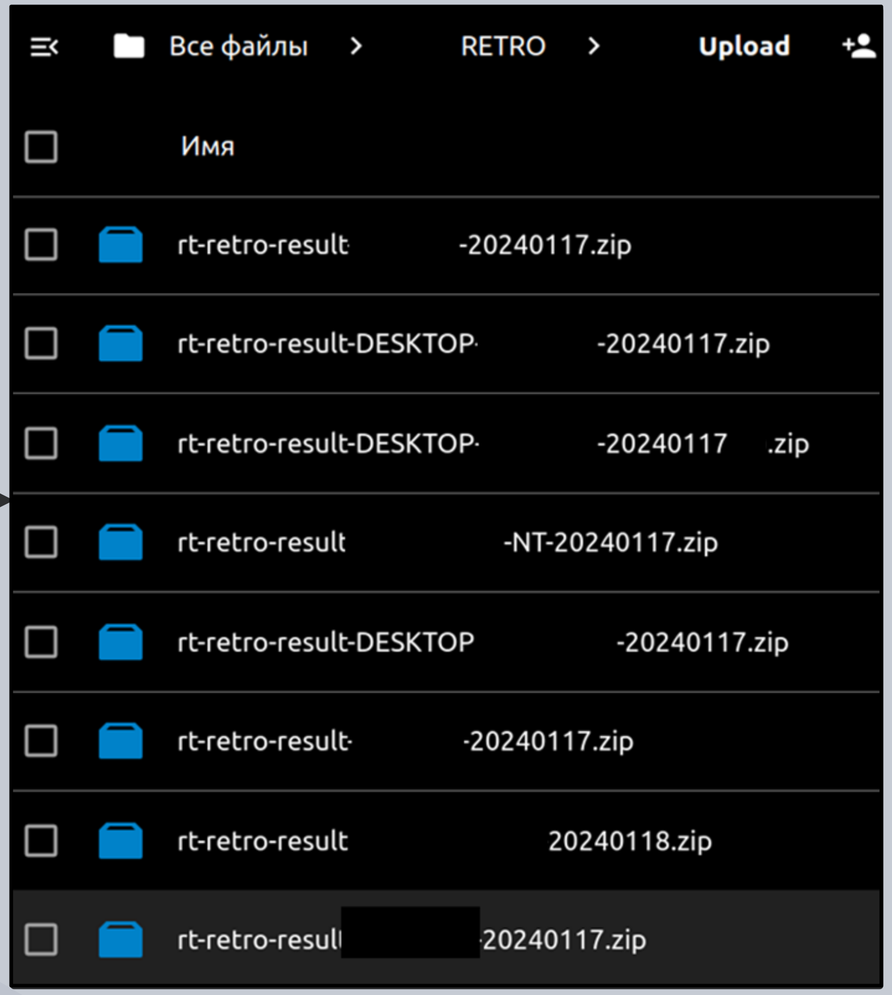




PT
Информационная безопасность

Загрузка результатов в облако через WebDAV или вручную





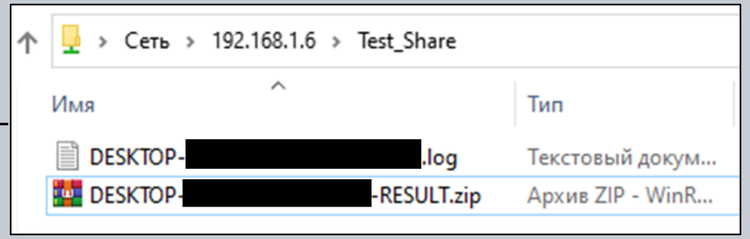
PT
Информационная безопасность

...или по SMB

DESKTOP-*.zip

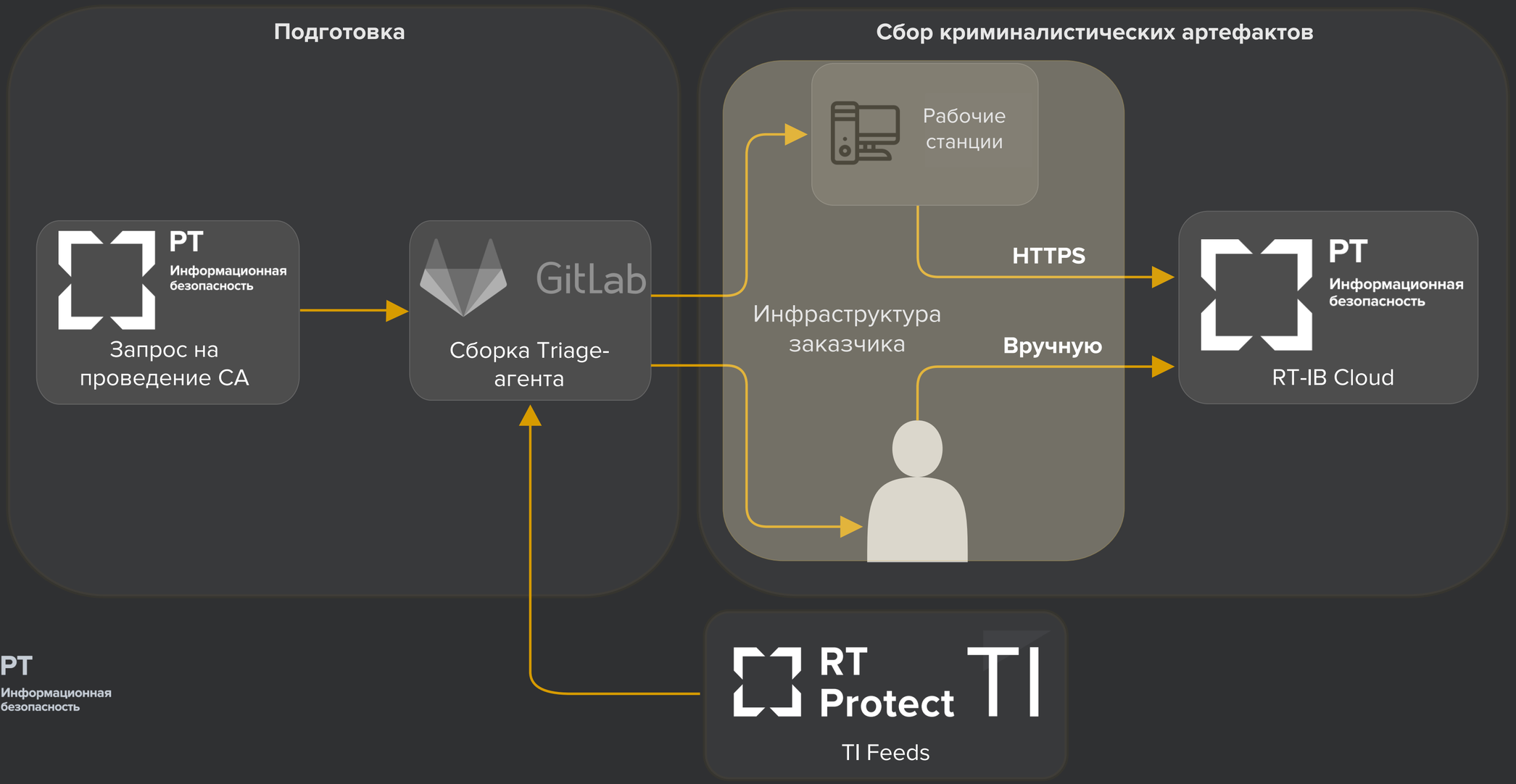
- PowerShellHistory_DESKTOP-*.zip
- xcyclopedia_DESKTOP-*.zip
- PowerHuntShares_DESKTOP-*.zip
- PersistenceSniper_DESKTOP-*.zip
- loki_DESKTOP-*.zip
- VSTriage_DESKTOP-*.zip
- hayabusa_DESKTOP-*.zip
- Collect-MemoryDump_Dumplt_DESKTOP-*.zip*
- Collect-MemoryDump_WinPMEM_DESKTOP-*.zip*
- ir-rescue_DESKTOP-*.zip*
- hollows_hunter_DESKTOP-*.zip*

rt-retro-result-DESKTOP-*.log



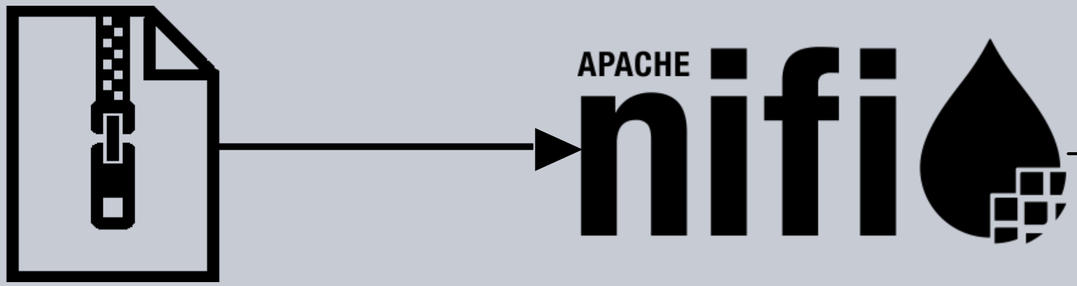
PT
Информационная безопасность

Этап сбора артефактов

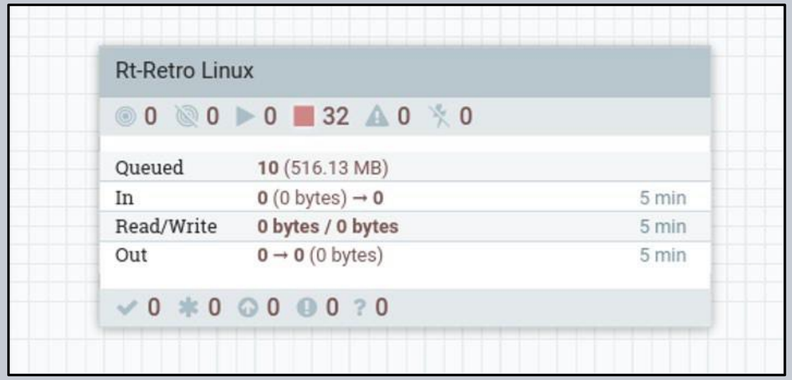


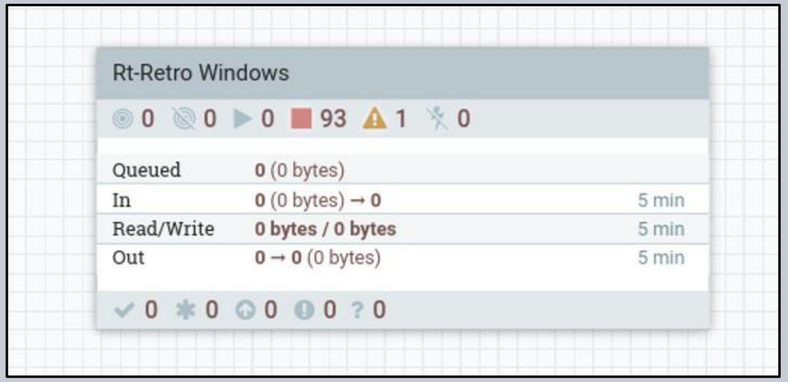
PT
Информационная безопасность

Нормализация



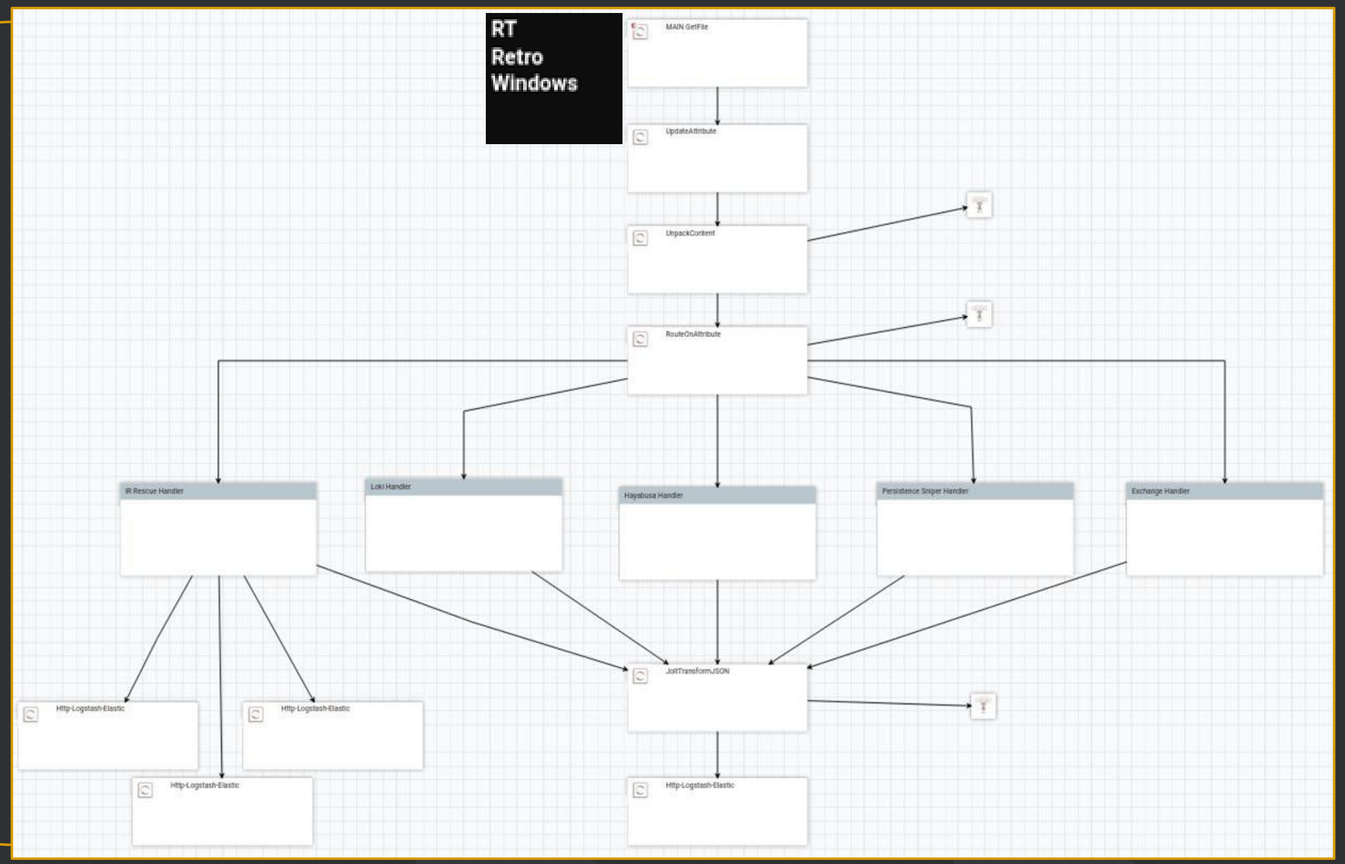
APACHE nifi





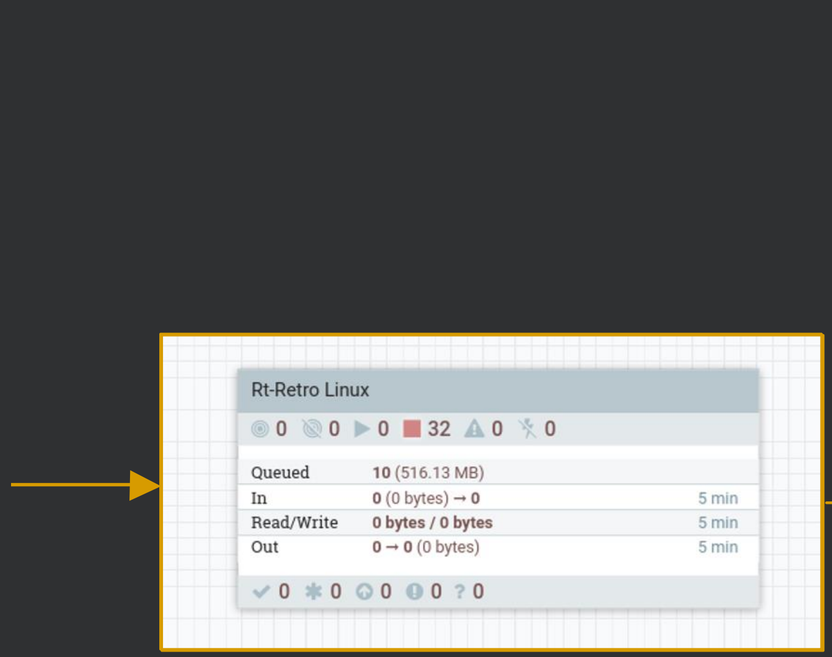
PT
Информационная безопасность

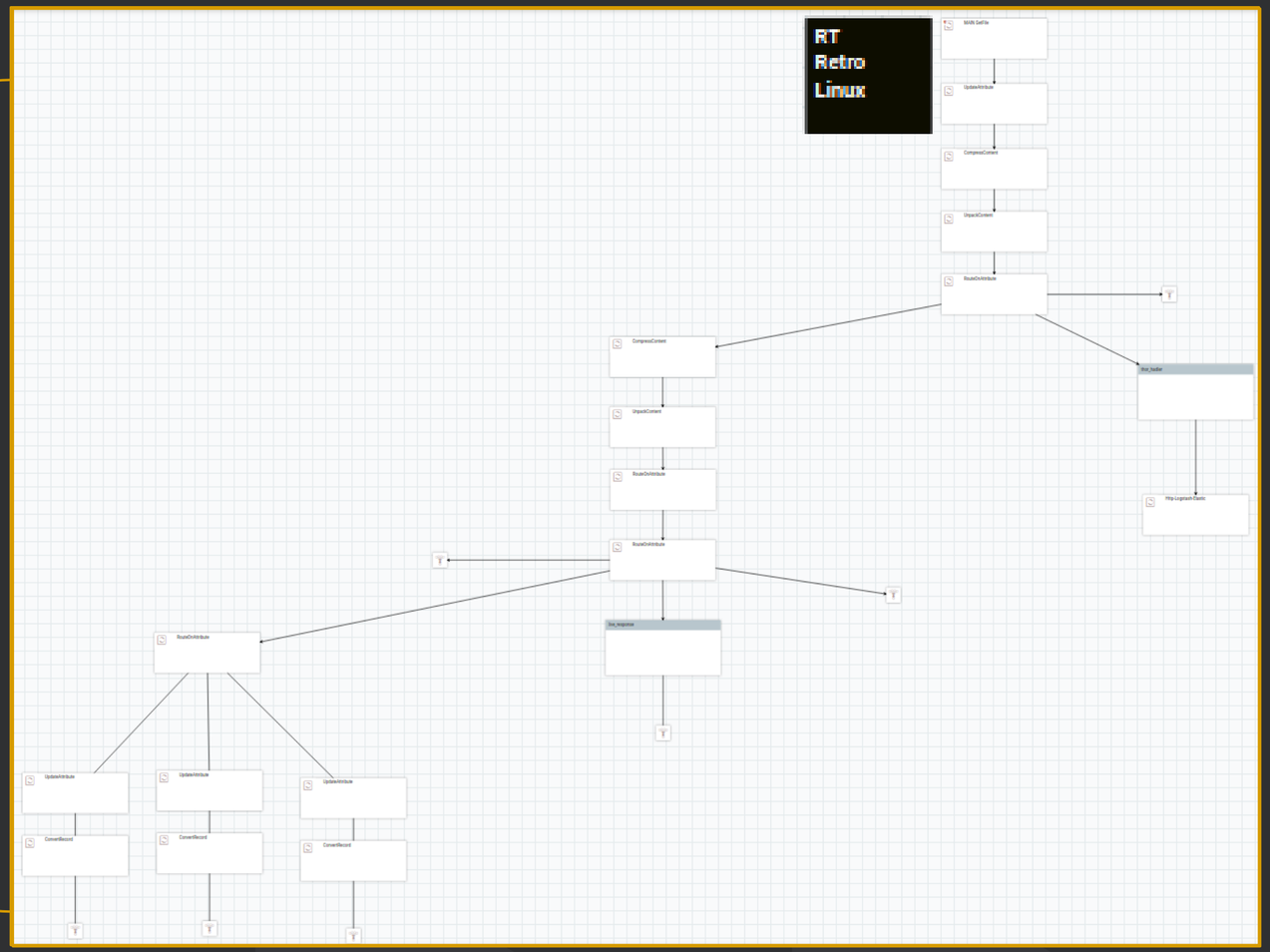
Нормализация Windows



PT
Информационная
безопасность

Нормализация Linux

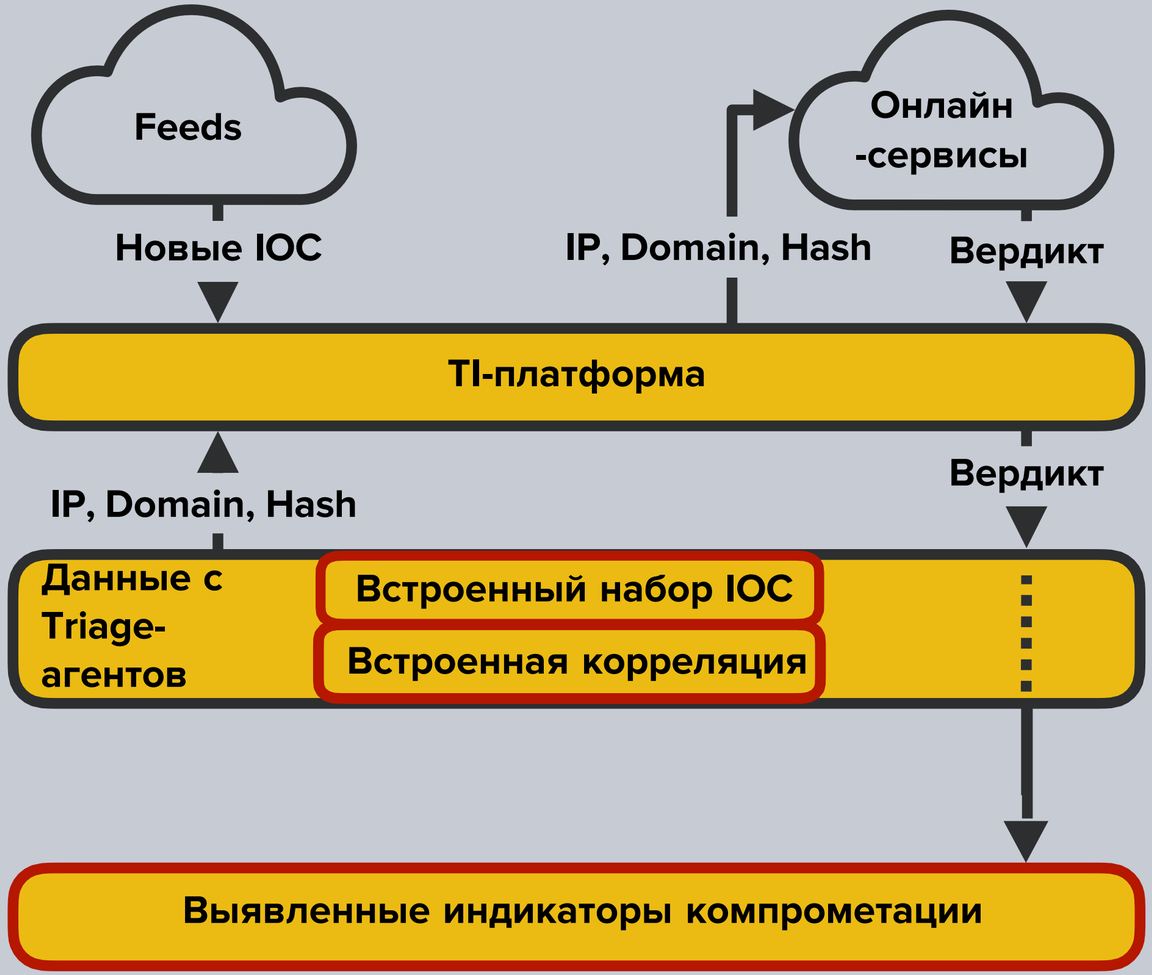




PT
Информационная
безопасность

Интеграция с TI

- Обогащение данных об артефактах, собранных с конечных точек



PT
Информационная безопасность

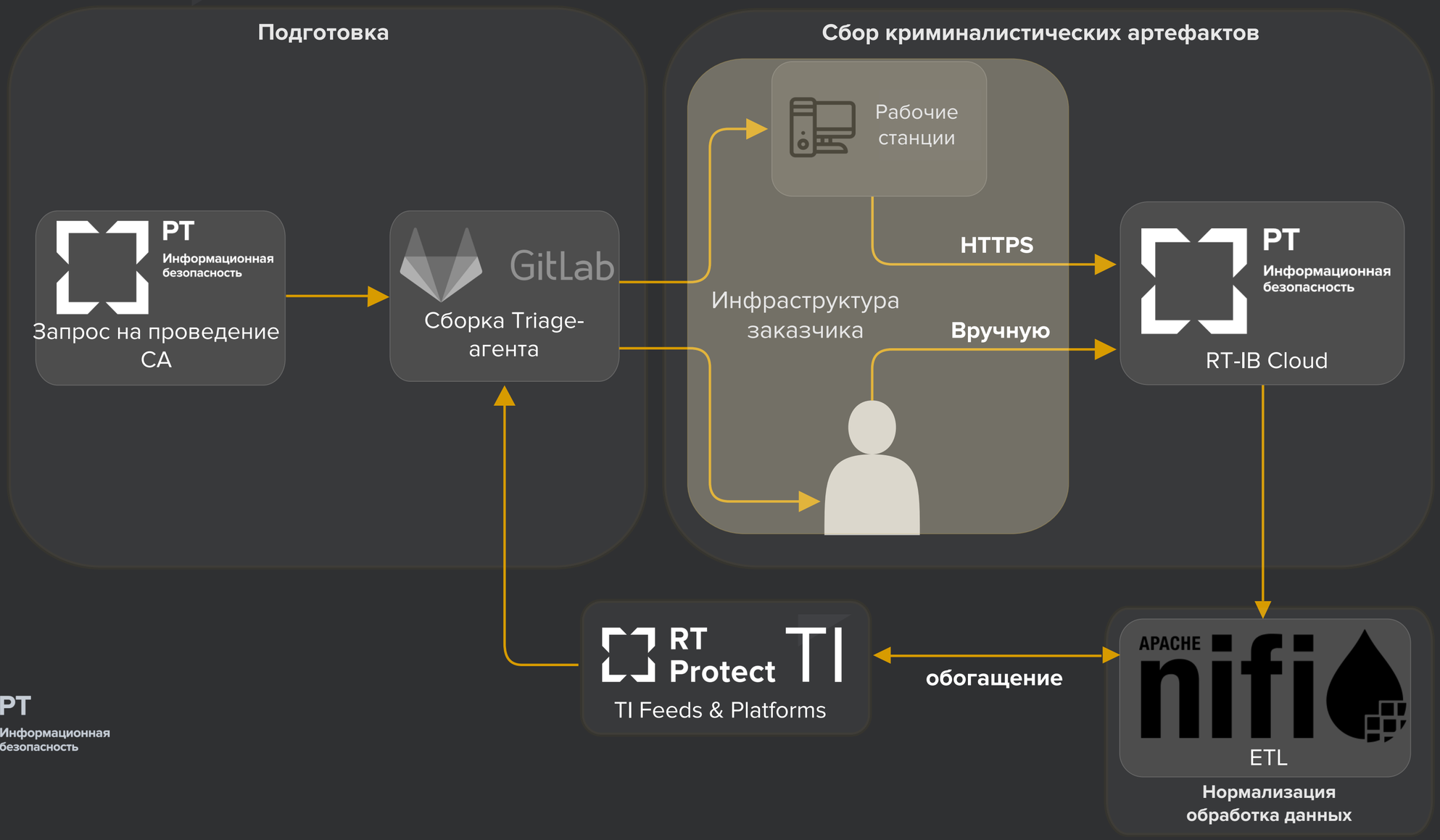
Результат обогащения артефактов

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	[redacted]
retro.investigation.mark	null
retro.org.name	[redacted]
retro.source.name	conn.txt
retro.source.path	[redacted]net/conn.txt
retro.triage.date	Aug 22, 2024 @ 03:00:00.000
retro.triage.name	[redacted]2024-08-22.zip

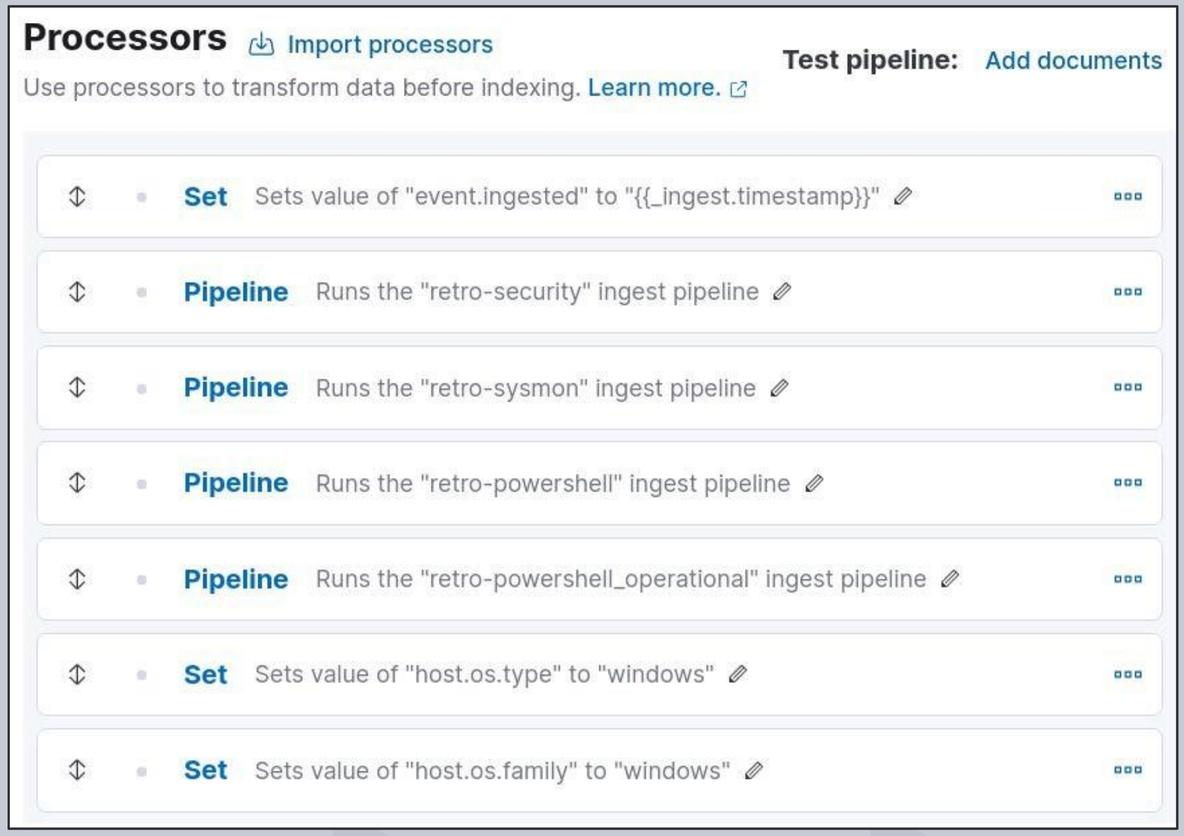
PT
Информационная безопасность

Этап нормализации



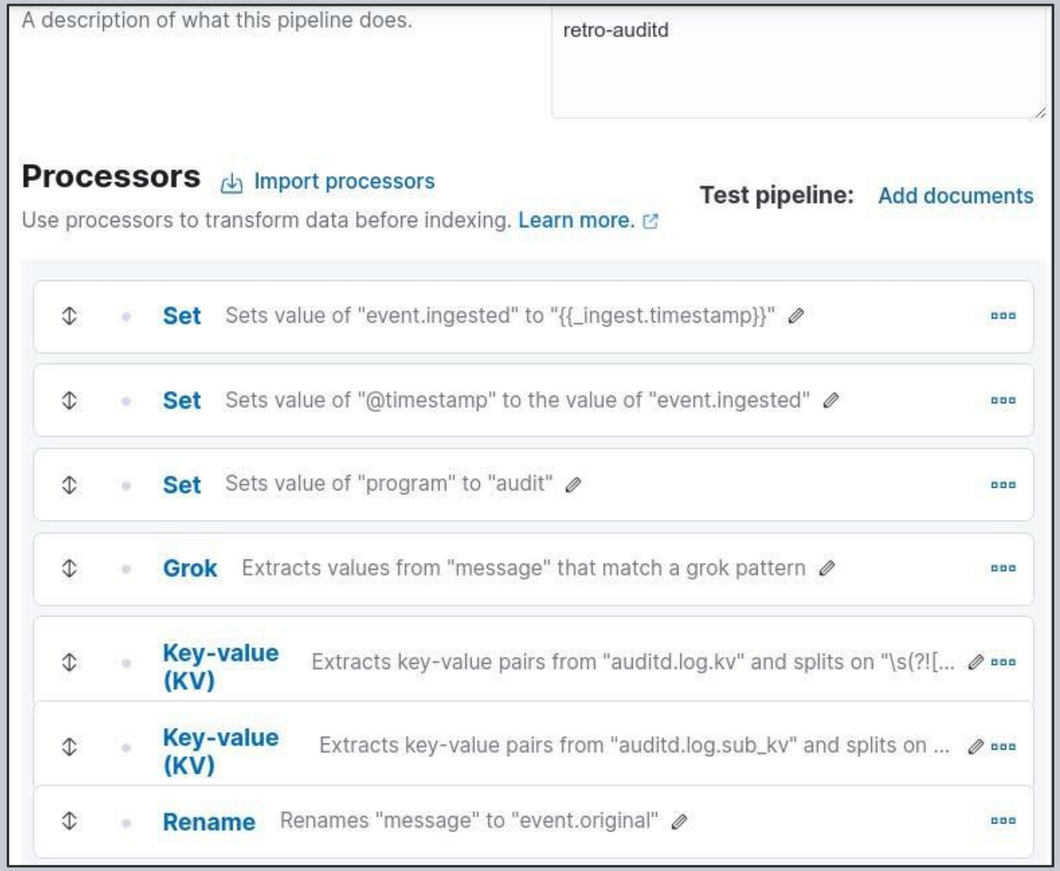
PT
Информационная безопасность

Нормализация журналов Auditd и WinEvt



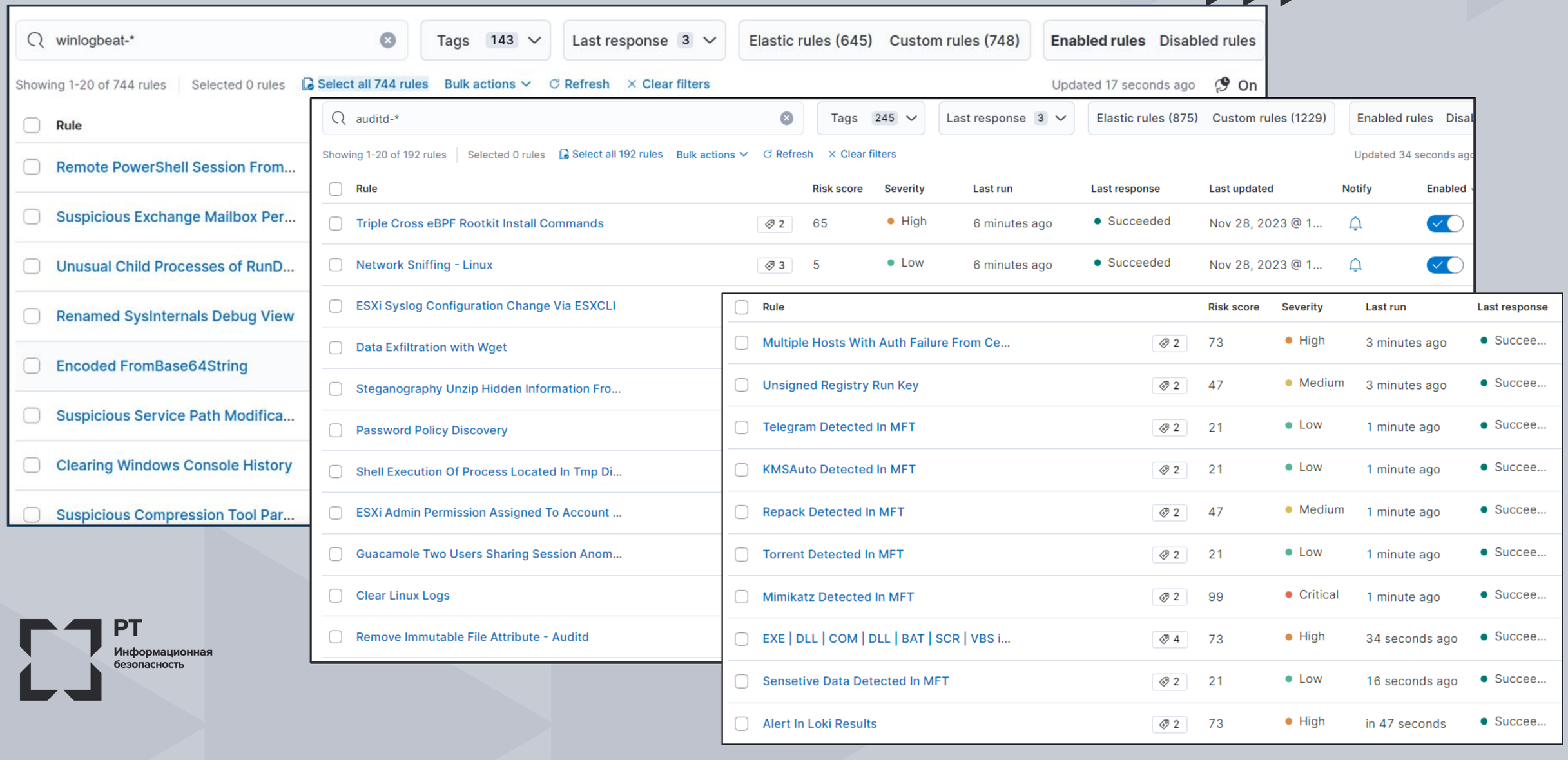
Ingest-Pipeline нормализации WinEvt

Ingest-Pipeline нормализации Auditd



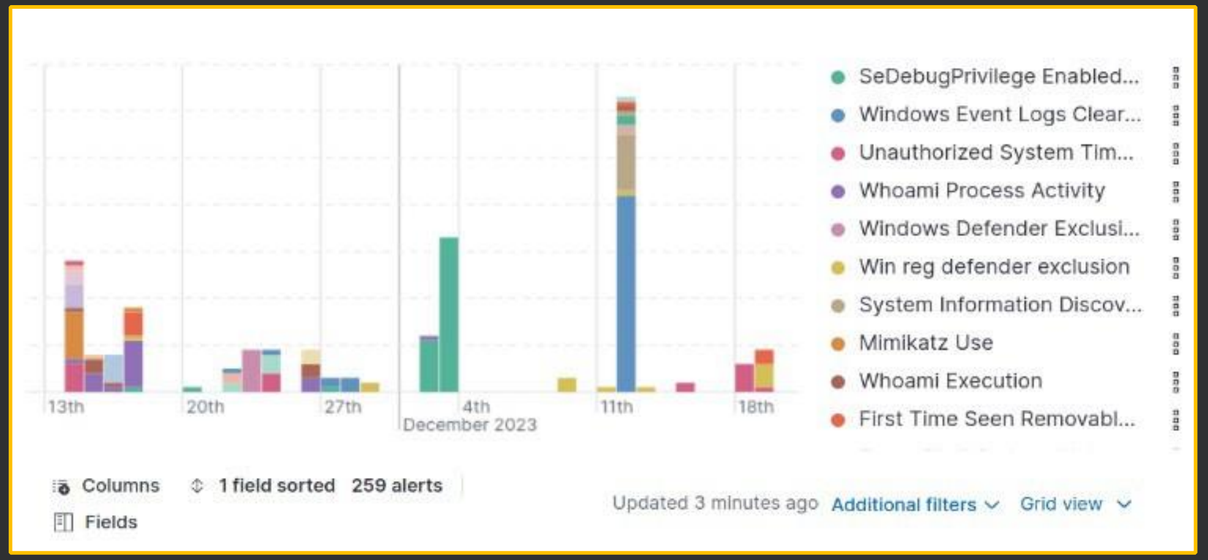
PT
Информационная безопасность

Корреляция событий всеми правилами SOC и собственной аналитикой



PT
Информационная безопасность

Проведение расследования



retro-mft-* retro-usnjrnl-* 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

t artifact.description.reason_2.matches	$lsass: 'System32\lsass.exe'
t artifact.description.reason_2.score	70
t artifact.description.reason_2.value	Yara Rule
t artifact.description.score	150
t artifact.description.sha1	ce5948945086d9761ea220f08e8c4e9c1208b928 SHA256: a90d1205b453
t artifact.severity	ALERT
t artifact.type	FileScan
t retro.host.name	DESKTOP_INFECTED
t retro.investigation.mark	null
t retro.org.name	Organization_name
t retro.source.name	loki_DESKTOP_INFECTED_2023-09-14_17-36-51.log
t retro.source.path	rt-retro-result-DESKTOP_INFECTED-20230914/loki_DESKTOP_INFE
t retro.triage.name	rt-retro-result-Organization name -DESKTOP_INFECTED-20230914.zip

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

PT
Информационная безопасность

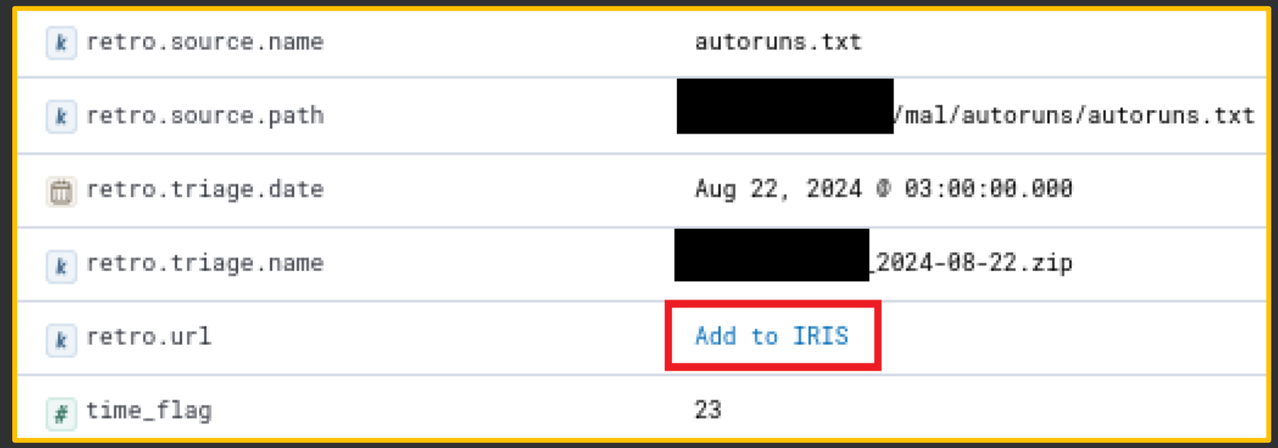
Этап корреляции и анализа

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



Результат: в кейс расследования добавлен артефакт из Kibana

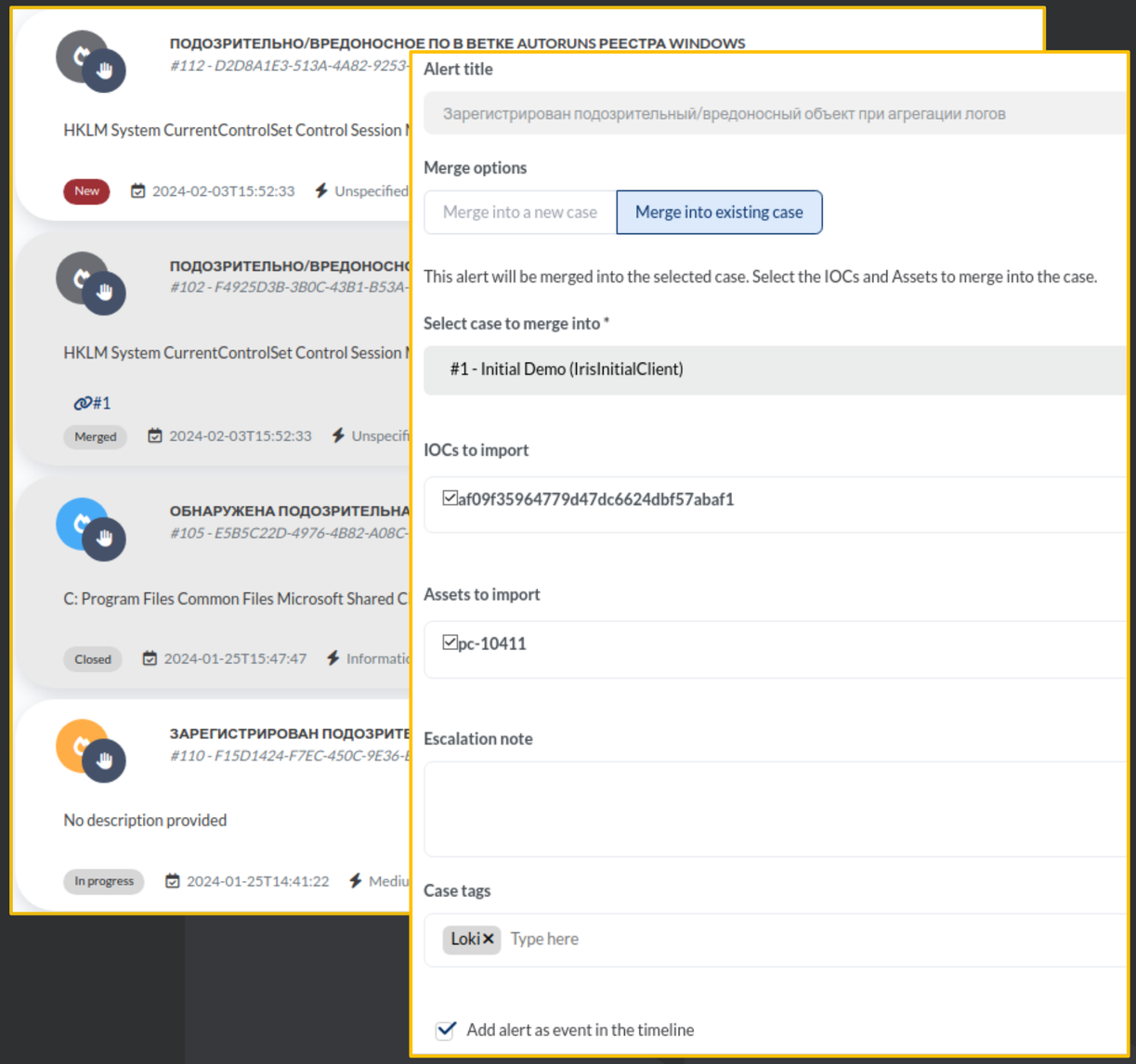
PT
Информационная безопасность

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

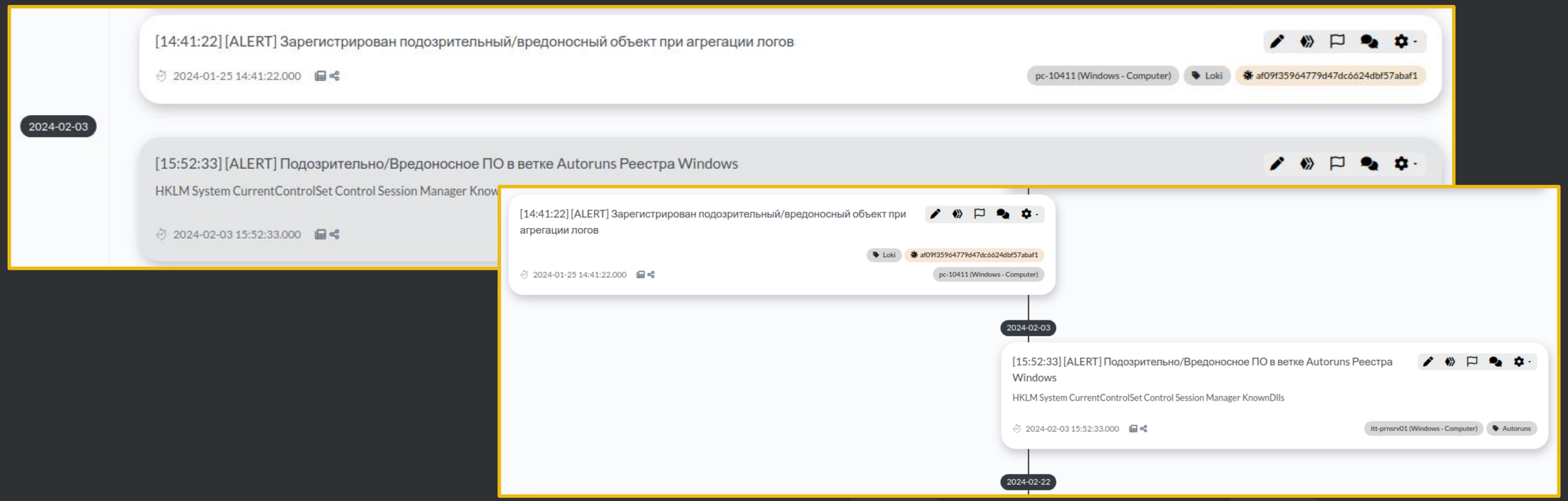
Аналитики L2-L3 подключаются для анализа событий в IRIS после их первичной обработки на L1



PT
Информационная безопасность

Проведение расследования

Установление связей между событиями

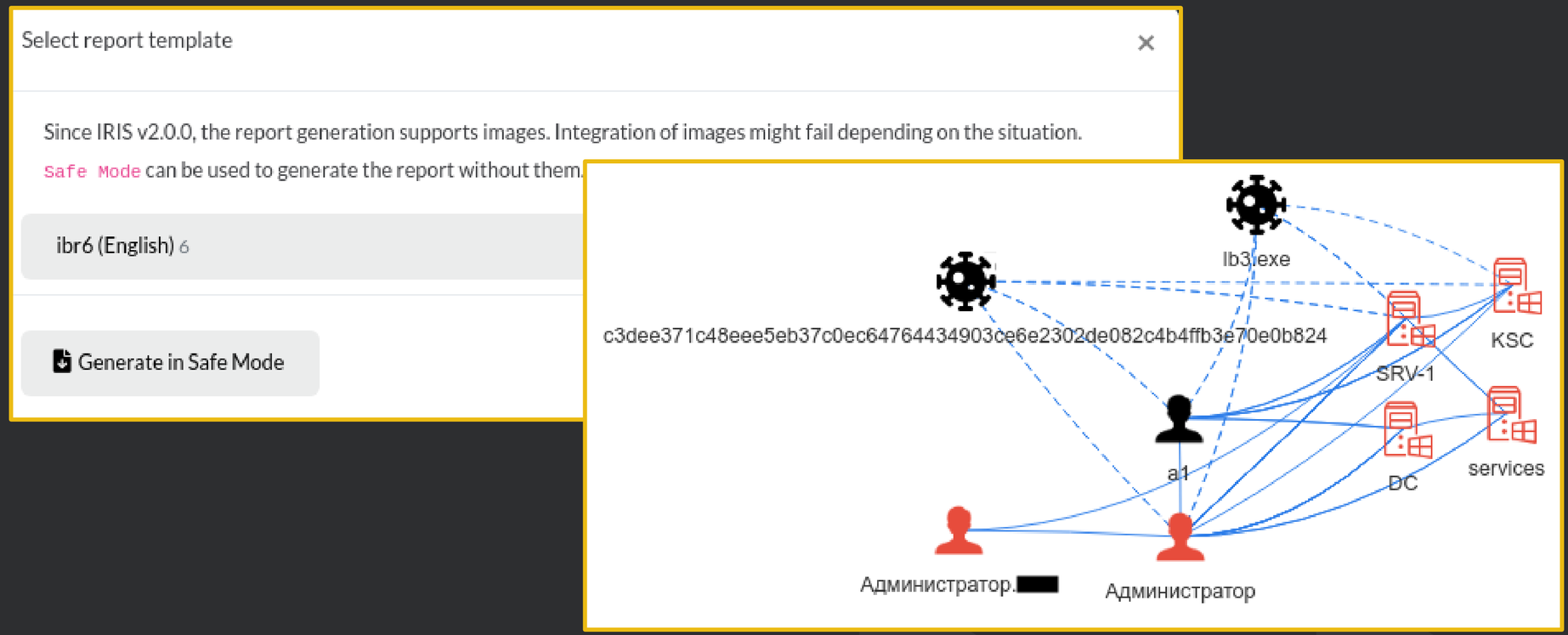


Выстраивание таймлайна атаки

PT
Информационная безопасность

Проведение расследования

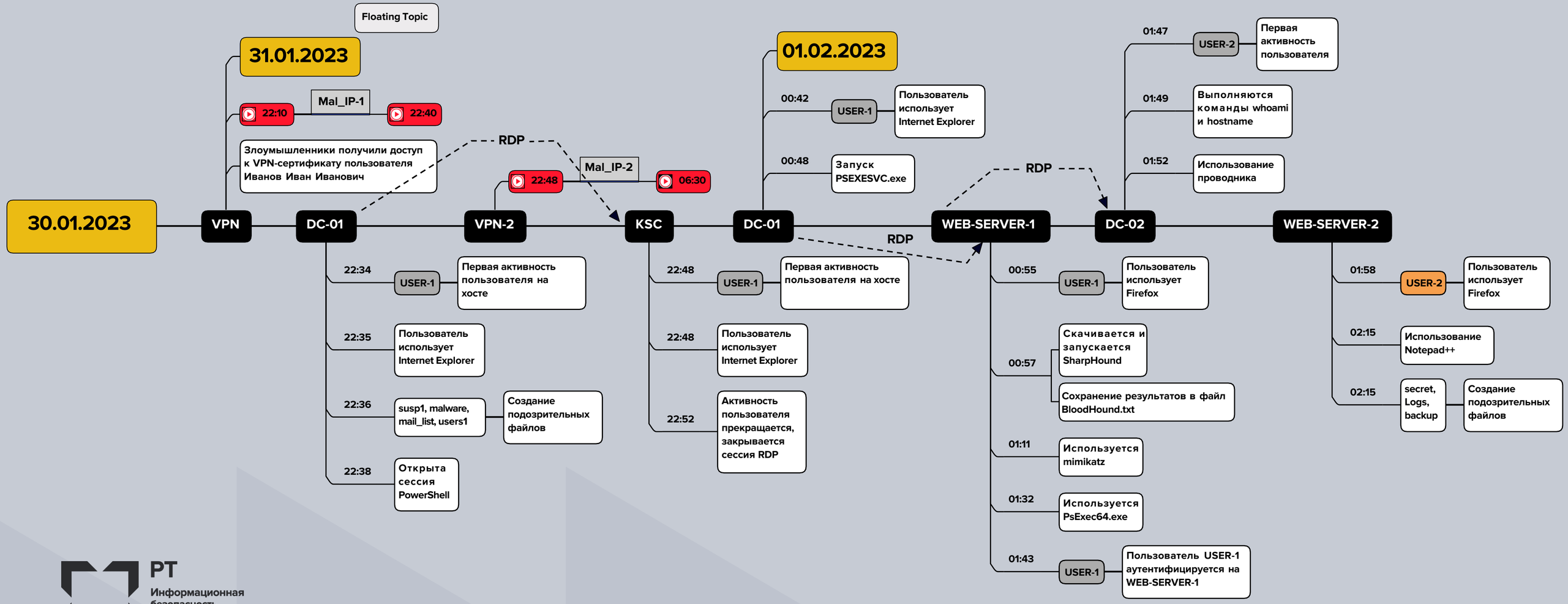
Генерация отчета по шаблону



Формирование графа действий атакующих

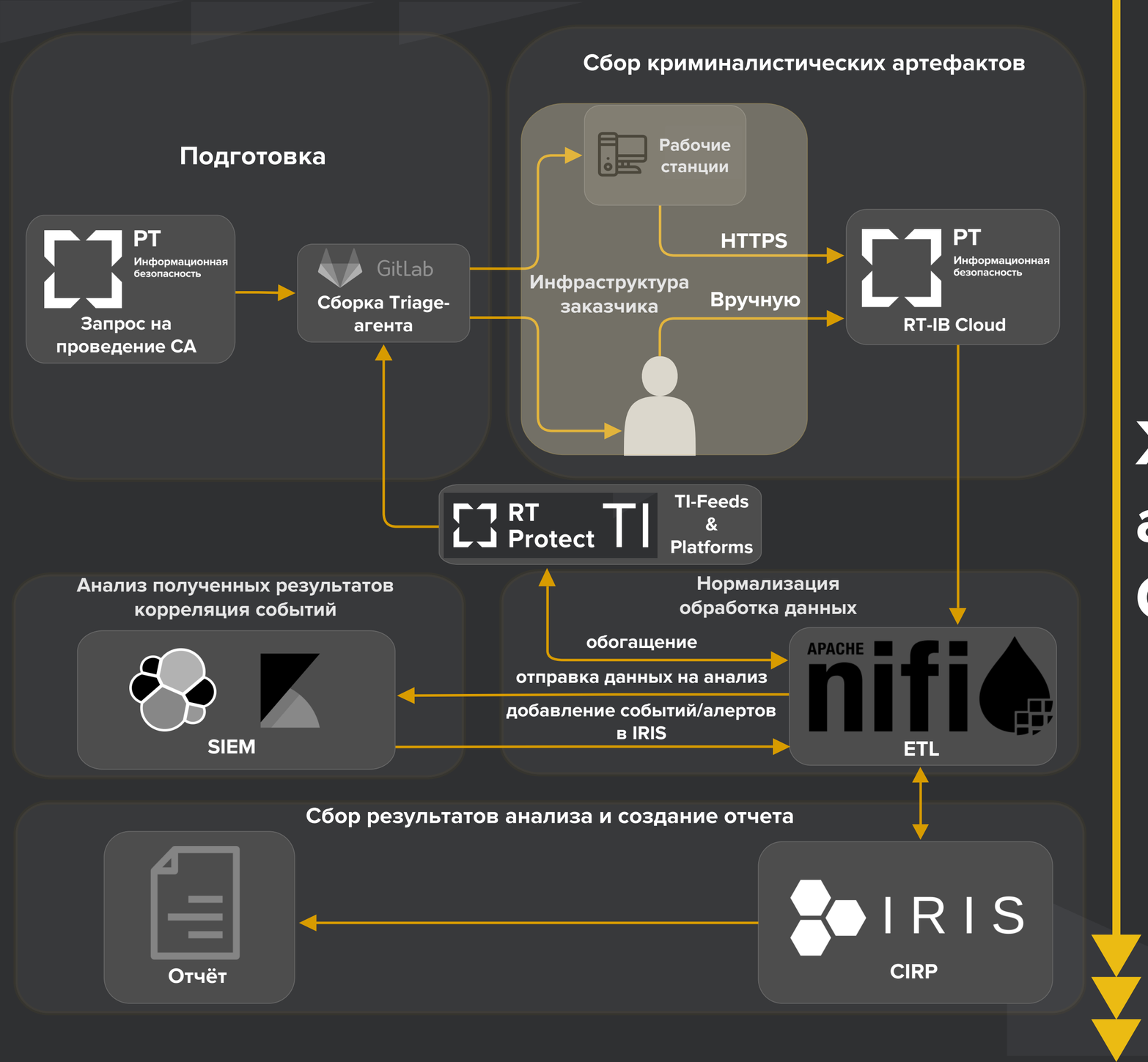
PT
Информационная безопасность

Срез информационной безопасности



PT
Информационная безопасность

Жизненный цикл автоматизированного Compromise Assessment



Что получает исполнитель?

PT Информационная безопасность

- 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?

PT Информационная безопасность

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 Telegrem-канале!

@RTINFOBEZ

Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

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