Расследование инцидентов с MaxPatrol SIEM

быстро, эффективно, качественно

О чем сегодня поговорим

- Контекст запуска и цепочки процессов
- Отслеживание передвижения внутри сети
- Гибкое управление типом сработок и вайтлистинг

Представьте мир, где **обогащения позволяют автоматизировать плейбуки** по расследованию инцидентов

О спикерах

Кирилл Кирьянов

Руководитель группы
обнаружения атак
на конечных устройствах

Юлия Фомина

Ведущий специалист
группы обнаружения атак
на конечных устройствах

Классический плейбук

1 → **Что есть в этом событии**

Какой организации принадлежит адрес соединения?
Может, это известный IoC?

2 → **Контекст процесса**

Как этот файл появился на узле? Кем он был создан?
Кто был родителем процесса? Какой командой был запущен процесс?

3 → **Контекст пользователя**

Кто запустил процесс?
Откуда пользователь пришел на узел?

4 → **Что происходит дальше**

Полноценное расследование инцидента и реагирование

Процесс reg.exe изменил параметр holavpn ключа реестра, отвечающий за автозапуск, на значение c:\users\aamelina\desktop\calc.exe на узле aamelina.plat.form

Контекст процесса

- Как этот файл появился на узле?
- Кем он был создан?
- Кто был родителем процесса?
- Какой командой был запущен процесс?

» 12.05.2023 11:04:10

Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\aamelina\desktop\calc.exe" на узле aamelina.plat.form

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

Добавить исключение

Параметры корреляции

correlation_name	Windows_Autorun_Modification
correlation_type	event
alert.context	regex_match: \currentversion\run | app: holavpn
alert.key	c:\windows\system32\reg.exe|c:\users\aamelina\desktop\calc.exe

Категория

category.generic	Attack
category.high	Persistence
category.low	Registry Run Keys / Startup Folder

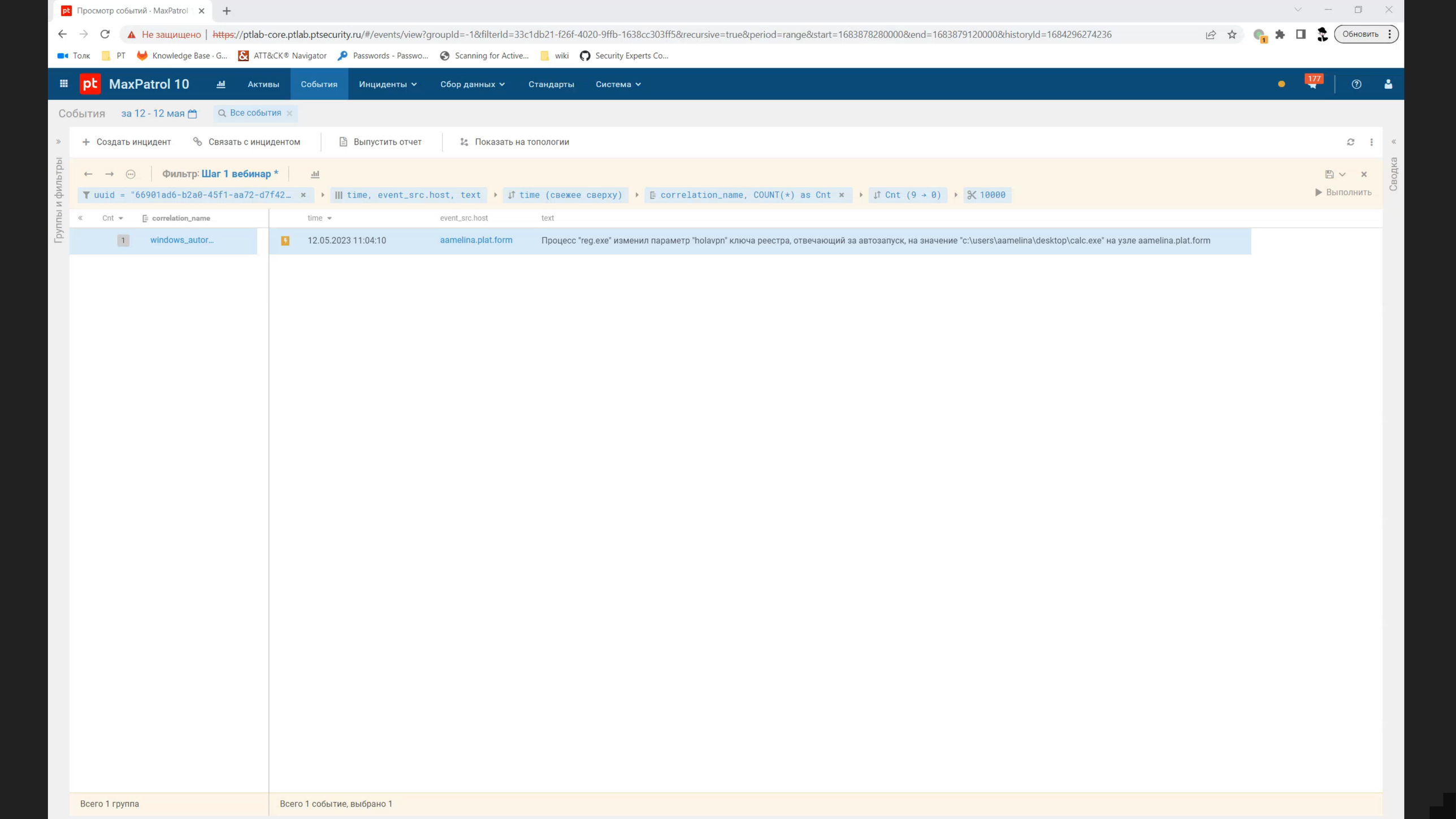
Роли во взаимодействии

Субъект

subject.process.name	reg.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\reg.exe
subject.process.guid	e5e214b7-f2fa-645d-f601-000000002600
subject.process.id	6936

Объект

object	reg_object
object.name	holavpn
object.property	value
object.value	c:\users\aamelina\desktop\calc.exe
object.type	registry run
object.path	\registry\user\s-1-5-21-1260549424-181218984-3392690056-1118\software\microsof
object.fullpath	\registry\user\s-1-5-21-1260549424-181218984-3392690056-1118\software\microsof


Просмотр событий · MaxPatrol
Не защищено | https://ptlab-core.ptlab.ptsecurity.ru/#/events/view?groupId=-1&filterId=33c1db21-f26f-4020-9ffb-1638cc303ff5&recursive=true&period=range&start=1683878280000&end=1683879120000&historyId=1684296274236
Обновить
Толк
PT
Knowledge Base · G...
ATT&CK® Navigator
Passwords - Passwo...
Scanning for Active...
wiki
Security Experts Co...
MaxPatrol 10
Активы
События
Инциденты
Сбор данных
Стандарты
Система
177
События
за 12 - 12 мая
Все события
Создать инцидент
Связать с инцидентом
Выпустить отчет
Показать на топологии
Группы и фильтры
Фильтр: Шаг 1 вебинар *
uuid = "66901ad6-b2a0-45f1-aa72-d7f42…
time, event_src.host, text
time (свежее сверху)
correlation_name, COUNT(*) as Cnt
Cnt (9 → 0)
10000
Выполнить
Сводка
Cnt
correlation_name
time
event_src.host
text
1
windows_autor…
12.05.2023 11:04:10
aamelina.plat.form
Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\aamelina\desktop\calc.exe" на узле aamelina.plat.form
Всего 1 группа
Всего 1 событие, выбрано 1

Автоматизация поиска контекста

Входы пользователей: 4624, user_start
Запуск процессов: 4688, 1
Создание файлов: 11
Миграция в процесс: 8
Удаленное подключение: VPN, RDG

Автоматизация поиска контекста

Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\aamelina\desktop\calc.exe" на узле aamelina.plat.form

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

Добавить исключение

Параметры корреляции

correlation_name	Windows_Autorun_Modification
correlation_type	event
alert.context	regex_match: \currentversion\run | app: holavpn
alert.key	c:\windows\system32\reg.exe|c:\users\aamelina\desktop\calc.exe

Категория

category.generic	Attack
category.high	Persistence
category.low	Registry Run Keys / Startup Folder

Роли во взаимодействии

Субъект

subject.process.name	reg.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\reg.exe
subject.process.guid	e5e214b7-f2fa-645d-f601-000000002600
subject.process.id	6936

Объект

object	reg_object
object.name	holavpn
object.property	value
object.value	c:\users\aamelina\desktop\calc.exe
object.type	registry run
object.path	\registry\user\s-1-5-21-1260549424-181218984-3392690056-1118\software\microsof
object.fullpath	\registry\user\s-1-5-21-1260549424-181218984-3392690056-1118\software\microsof

Табличный список: Process_chains

host	proc_id	proc_name	subject_account	subject_session_id	object_acco...	object...	proc_meta	proc_hash	la...	parent_proc_id
rgorelov.plat.form	6936	gpupdate.exe	nt authority\system	999	nt authorit...	996	null	null	24...	1244
rkabanov.plat.form	6936	googleupdat...	nt authority\system	999	nt authorit...	999	Description:Google Installer | ...	IMPHASH:7DF1816239C5B...	59...	1132
sazanchevskij.plat.fo...	6936	culauncher.exe	nt authority\system	999	nt authorit...	999	Description:qualauncher | Pro...	IMPHASH:3121891935D13...	11...	2036
sazanchevskij.plat.fo...	6936	ngen.exe	nt authority\system	999	nt authorit...	999	null	null	95...	2252
jfomicheva.plat.form	6936	ngen.exe	nt authority\system	999	nt authorit...	999	null	null	09...	5456
sazanchevskij.plat.fo...	6936	wmiprvse.exe	nt authority\system	999	nt authorit...	999	null	null	70...	868
rkabanov.plat.form	6936	wmiprvse.exe	nt authority\system	999	nt authorit...	999	null	null	75...	836
plat-veeam-back.rf.pl...	6936	googleupdat...	nt authority\system	999	nt authorit...	999	null	null	d0...	372
aamelina.plat.form	6936	reg.exe	plat.form\aamelina	544091	plat.form\...	544091	Description:Registry Console ...	IMPHASH:BE482BE427FE2...	94...	7184
aamelina.plat.form	6936	fontdrvhost.e...	nt authority\system	999	font driver ...	7223...	Description:Usermode Font D...	IMPHASH:5E65A8FC9D3B5...	7e...	7672
db.rf.plat.form	6936	taskhostw.exe	db\administrator	7275147	db\admini...	7275...	Description:Host Process for ...	IMPHASH:1CCD2E7A159E4...	97...	1340

Принесем всю эту информацию в сработку

Контекст процесса

Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\aamelina\desktop\calc.exe" на узле aamelina.plat.form

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

Добавить исключение

Параметры корреляции

correlation_name	Windows_Autorun_Modification
correlation_type	event
alert.context	regex_match: \currentversion\run | app: holavpn
alert.key	c:\windows\system32\reg.exe|c:\users\aamelina\desktop\calc.exe

Категория

category.generic	Attack
category.high	Persistence
category.low	Registry Run Keys / Startup Folder

Роли во взаимодействии

Субъект

subject.process.name	reg.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\reg.exe
subject.process.guid	e5e214b7-f2fa-645d-f601-000000002600
subject.process.id	6936

Объект

object	reg_object
object.name	holavpn
object.property	value
object.value	c:\users\aamelina\desktop\calc.exe
object.type	registry run
object.path	\registry\user\s-1-5-21-1260549424-181218984-3392690056-1118\software\microsof
object.fullpath	\registry\user\s-1-5-21-1260549424-181218984-3392690056-1118\software\microsof

Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\aamelina\desktop\calc.exe" на узле aamelina.plat.form

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

Добавить исключение

Параметры корреляции

correlation_name	Windows_Autorun_Modification
correlation_type	event
alert.context	regex_match: \currentversion\run | app: holavpn
alert.key	c:\windows\system32\reg.exe|c:\users\aamelina\desktop\calc.exe

Категория

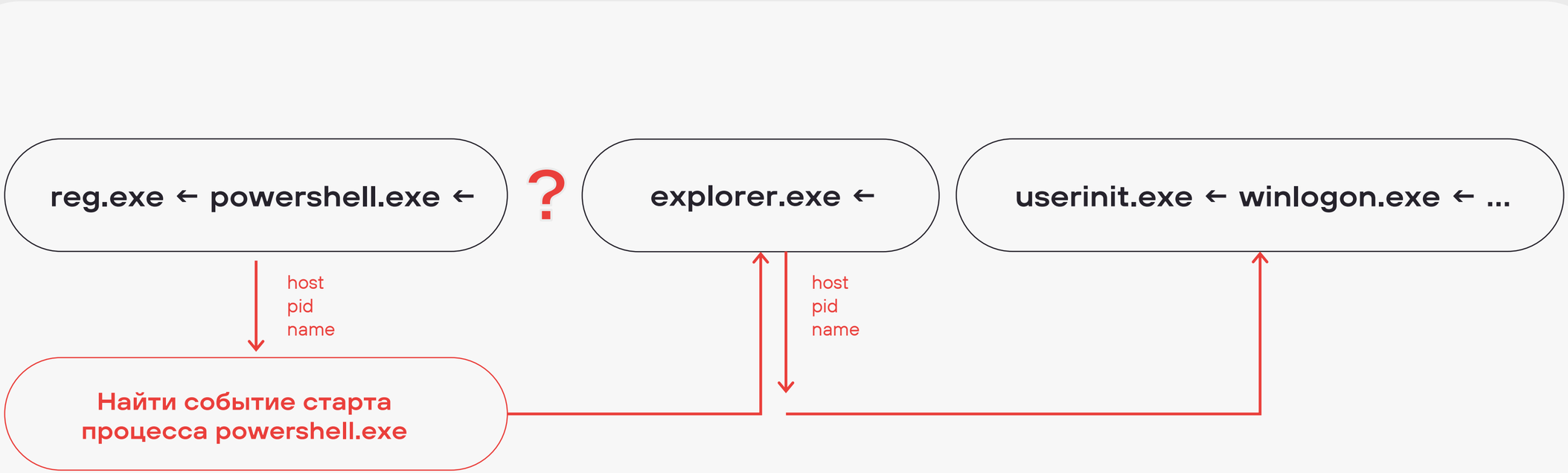
category.generic	Attack
category.high	Persistence
category.low	Registry Run Keys / Startup Folder

Роли во взаимодействии

Субъект

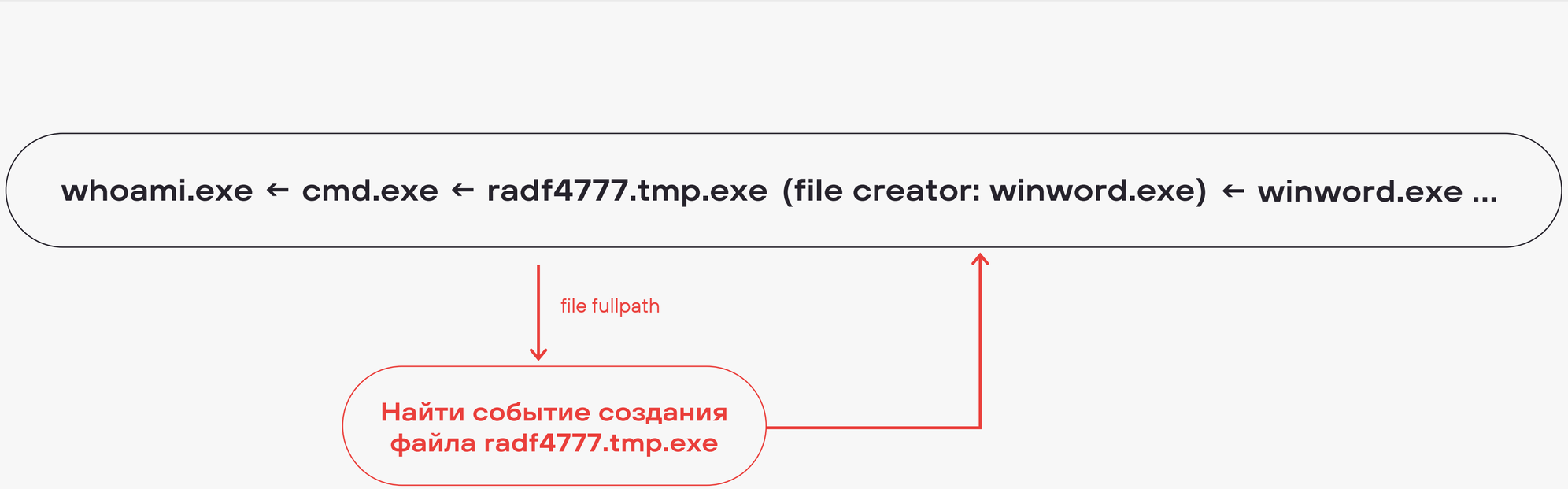
subject.account.name	aamelina
subject.account.domain	plat.form
subject.account.session_id	544091
subject.account.id	s-1-5-21-1260549424-181218984-3392690056-1118
subject.process.name	reg.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\reg.exe
subject.process.cmdline	"C:\WINDOWS\system32\reg.exe" add HKEY_CURRENT_USER\Software\Microsoft\Wi
subject.process.guid	e5e214b7-f2fa-645d-f601-000000002600
subject.process.id	6936
subject.process.parent.name	powershell.exe
subject.process.parent.id	7184
subject.process.parent.cmdline	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Родители родителей: цепочки процессов



Родители родителей: цепочки процессов

Родители родителей: цепочки процессов



Родители родителей: цепочки процессов

net.exe ← cmd.exe ← cv.docx.exe ← telegram.exe ← ...

whoami.exe ← powershell.exe ← services.exe ← ...

reg.exe ← powershell.exe ← explorer.exe ← ...

Подробнее
о расследовании атак
с использованием
цепочек процессов

subject.process.fullpath	c:\windows\system32\reg.exe
subject.process.cmdline	"C:\WINDOWS\system32\reg.exe" add HKEY_CURRENT_USER\Software\Microsoft\Win
subject.process.chain	reg.exe ← powershell.exe ← explorer.exe ← userinit.exe ← winlogon.exe ← smss.exe ←
subject.process.id	8596
subject.process.parent.name	powershell.exe

Цепочка процессов в MaxPatrol SIEM

Классический плейбук

1 →

Что есть в этом событии

Какой организации принадлежит адрес соединения?
Может, это известный IoC?

2 →

Контекст процесса

Как этот файл появился на узле? Кем он был создан?
Кто был родителем процесса? Какой командой был запущен процесс?

3 →

Контекст пользователя

Кто запустил процесс?
Откуда пользователь пришел на узел?

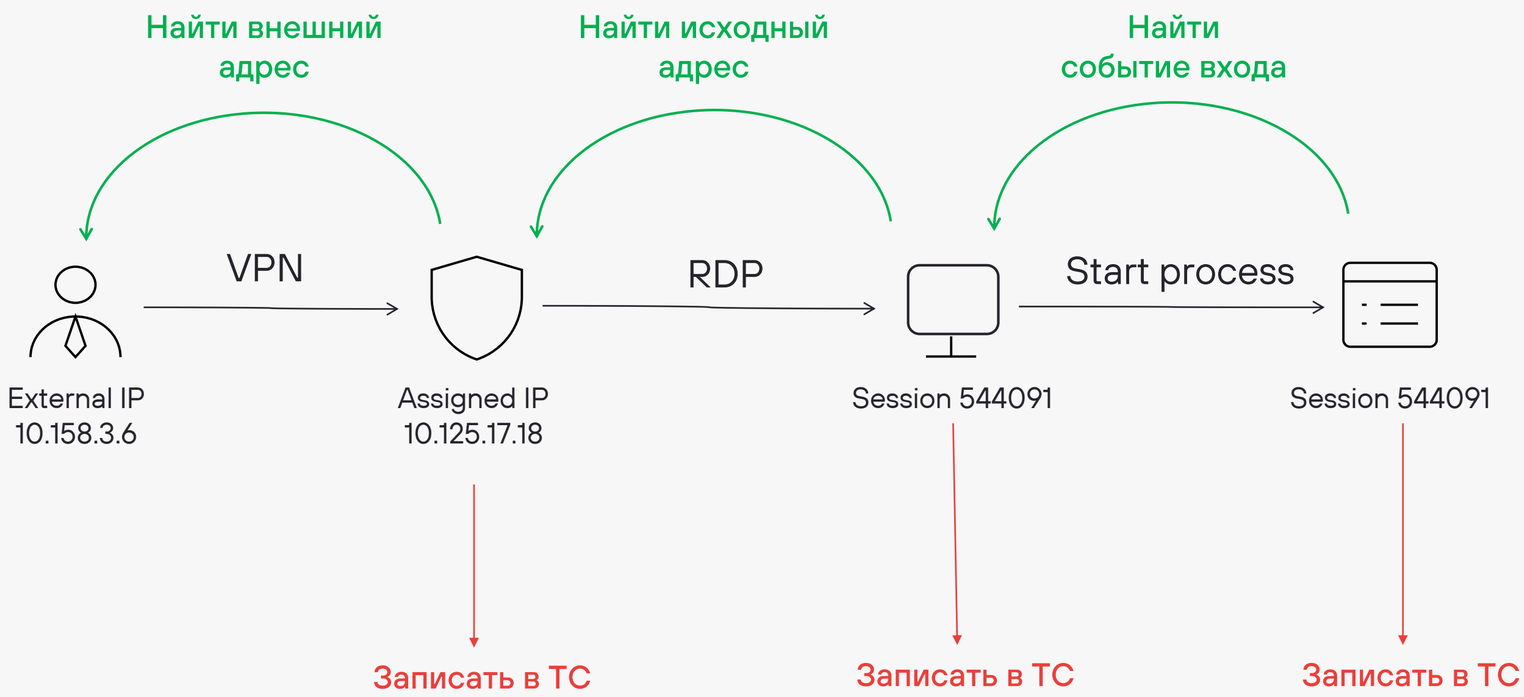
4 →

Что происходит дальше

Полноценное расследование инцидента и реагирование

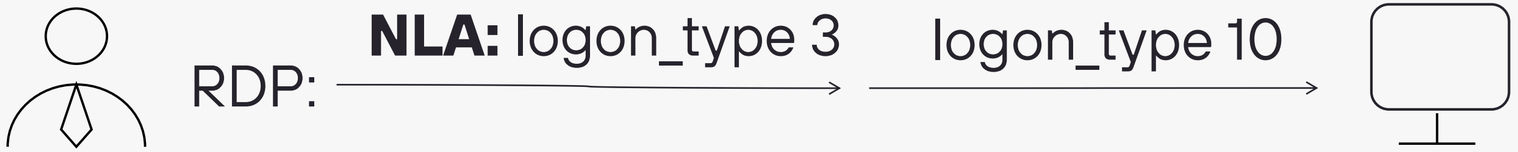
Процесс reg.exe изменил параметр holavpn ключа реестра, отвечающий за автозапуск, на значение c:\users\aamelina\desktop\calc.exe на узле aamelina.plat.form

Контекст пользователя



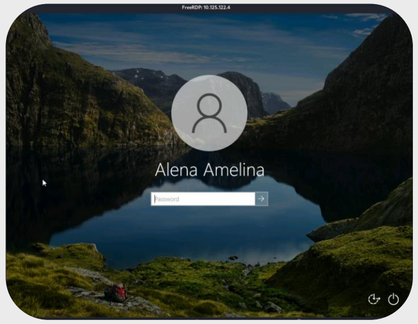
Установка RDP-соединения

Установка RDP-соединения

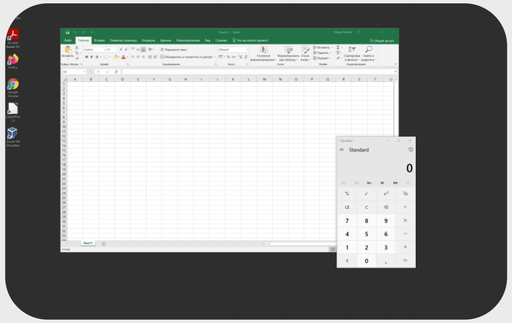


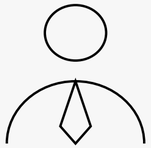
	time	event_src.host	subject.account.session_id	src.ip	text	
	15.05.2023 10:43:14	aamelina.plat.form	185117054	10.125.17.6	Пользователь aamelina осуществил успешный вход в систему на узле aamelina.plat.form	Тип входа: RemoteInteractive
	15.05.2023 10:43:06	aamelina.plat.form	185047817	10.125.17.6	Пользователь aamelina осуществил успешный вход в систему на узле aamelina.plat.form	Тип входа: Network

Установка RDP-соединения

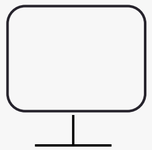


logon_type 7



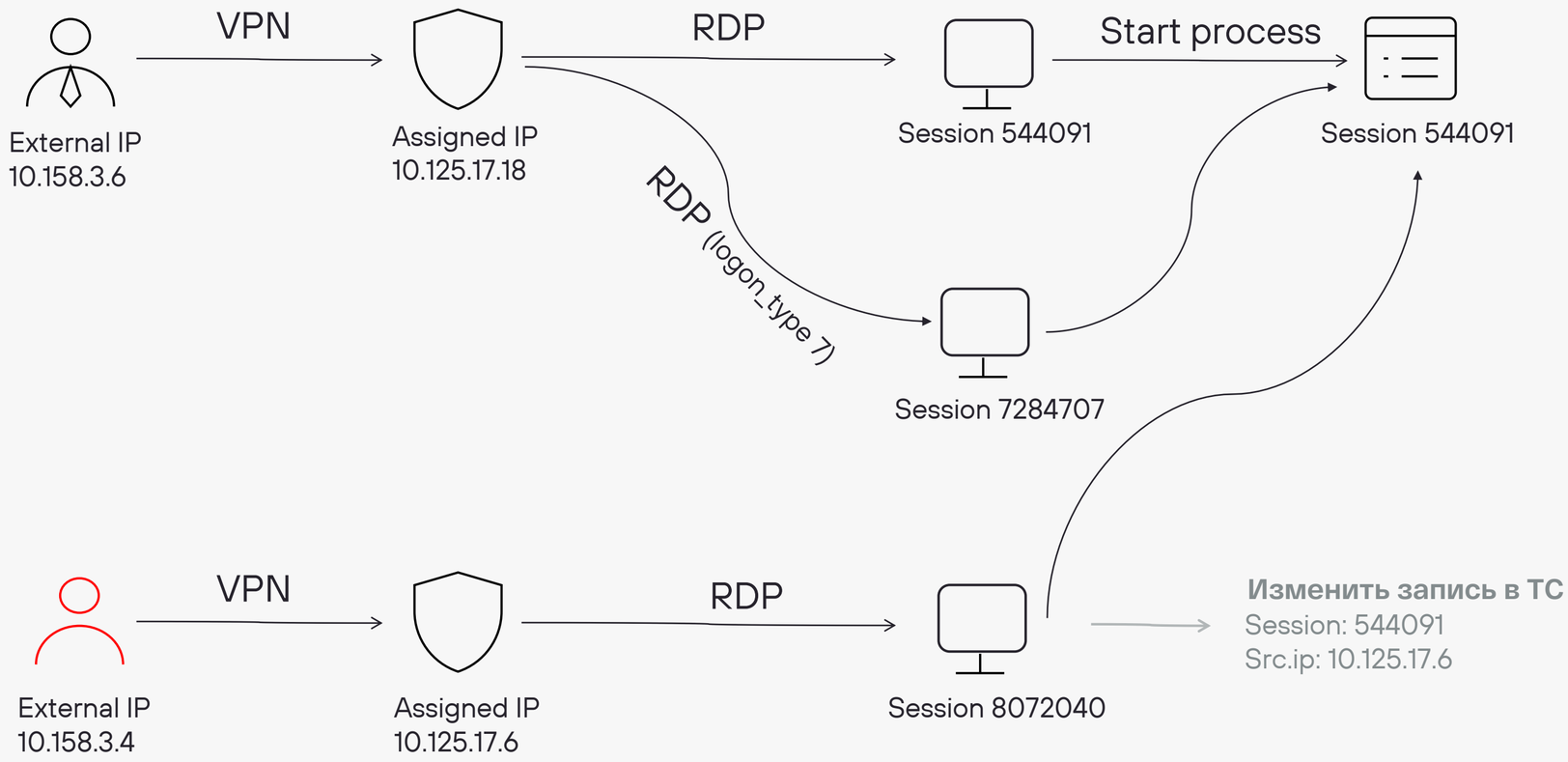


RDP: **NLA:** logon_type 3 → logon_type 10

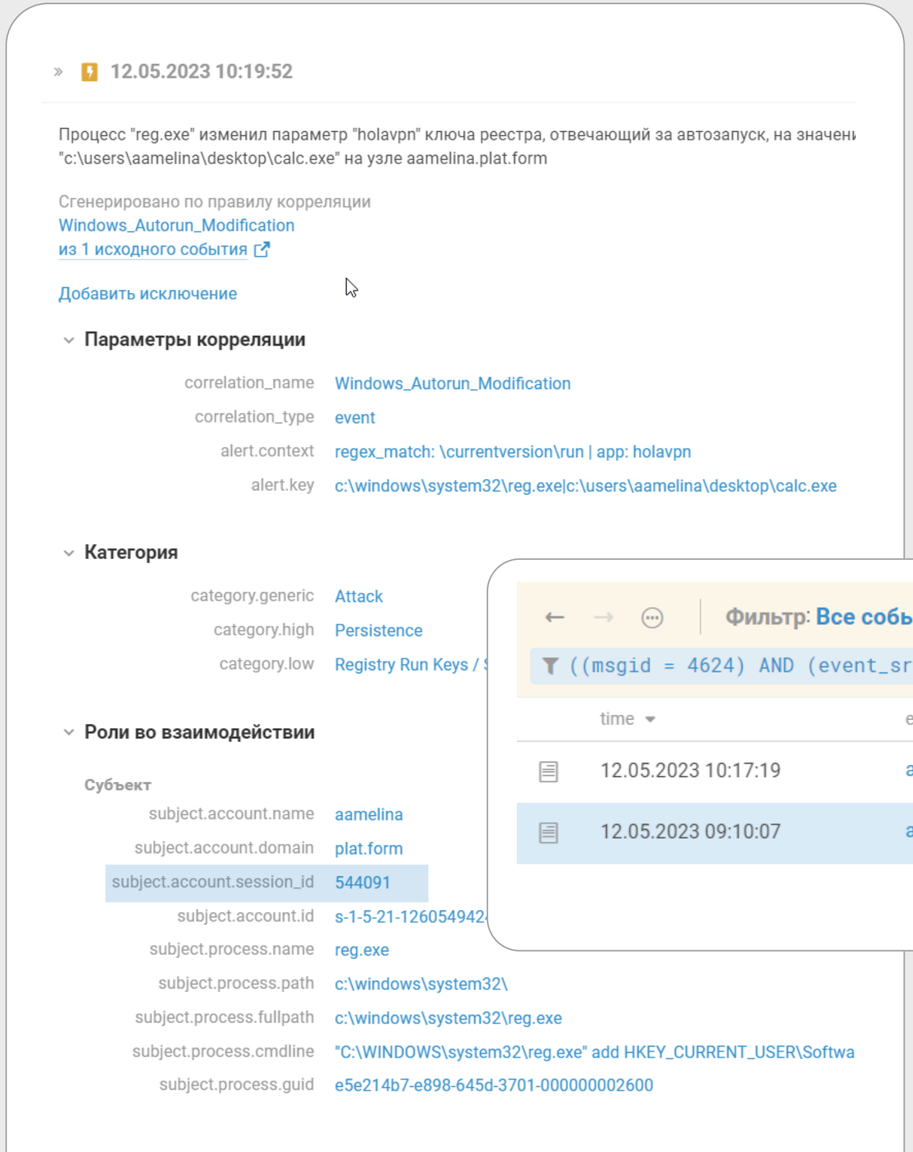


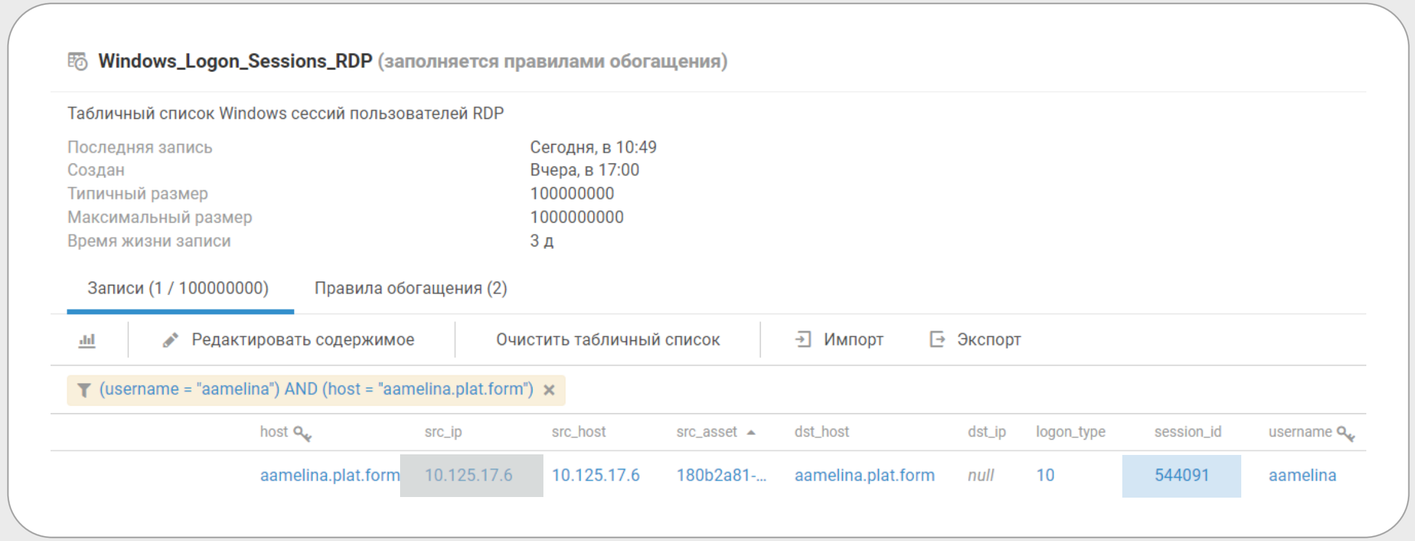
	time	event_src.host	subject.account.session_id	src.ip	text
	15.05.2023 11:48:24	aamelina.plat.form	185488856	10.125.17.6	Пользователь aamelina осуществил успешный вход в систему на узле aamelina.plat.form. Тип входа: Unlock
	15.05.2023 10:43:14	aamelina.plat.form	185117054	10.125.17.6	Пользователь aamelina осуществил успешный вход в систему на узле aamelina.plat.form. Тип входа: RemoteInteractive
	15.05.2023 10:43:06	aamelina.plat.form	185047817	10.125.17.6	Пользователь aamelina осуществил успешный вход в систему на узле aamelina.plat.form. Тип входа: Network

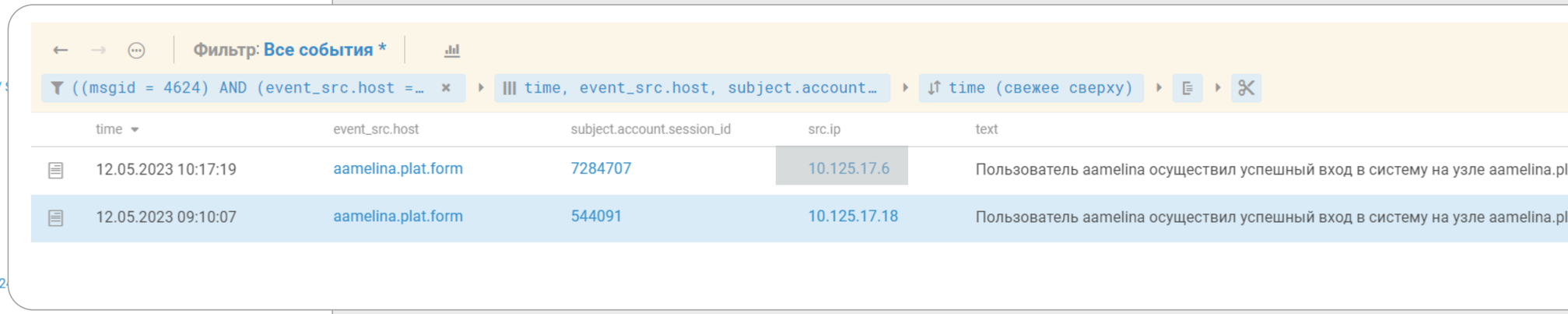
Хитрый RDP


VPN
RDP
Start process
External IP
10.158.3.6
Assigned IP
10.125.17.18
Session 544091
Session 544091
RDP (logon_type 7)
Session 7284707
VPN
RDP
External IP
10.158.3.4
Assigned IP
10.125.17.6
Session 8072040
Изменить запись в ТС
Session: 544091
Src.ip: 10.125.17.6

Контекст пользователя







Установка RDP-соединения

Пользователь aamelina осуществил успешный вход в систему на узле aamelina.plat.form. Тип входа: RemoteInteractive

Категория

Адресаты

Роли во взаимодействии

Субъект

subject	account
subject.name	aamelina
subject.domain	plat
subject.id	S-1-5-21-1260549424-181218984-3392690056-1118
subject.account.name	aamelina
subject.account.domain	plat.form
subject.account.session_id	8072040
subject.account.id	S-1-5-21-1260549424-181218984-3392690056-1118
subject.account.privileges	local user rights
subject.process.name	svchost.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\svchost.exe
subject.process.id	1908

Объект

object	system
object.property	session ID with ElevatedToken
object.value	0

Параметры взаимодействия

importance	info
logon_type	10

Пользователь aamelina_admin осуществил успешный вход в систему на узле aamelina.plat.form. Тип входа: RemoteInteracti

Категория

Адресаты

Роли во взаимодействии

Субъект

subject	account
subject.name	aamelina_admin
subject.domain	plat
subject.id	S-1-5-21-1260549424-181218984-3392690056-1114
subject.account.name	aamelina_admin
subject.account.domain	plat.form
subject.account.session_id	8072520
subject.account.id	S-1-5-21-1260549424-181218984-3392690056-1114
subject.account.privileges	local administrator rights
subject.process.name	svchost.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\svchost.exe
subject.process.id	1908

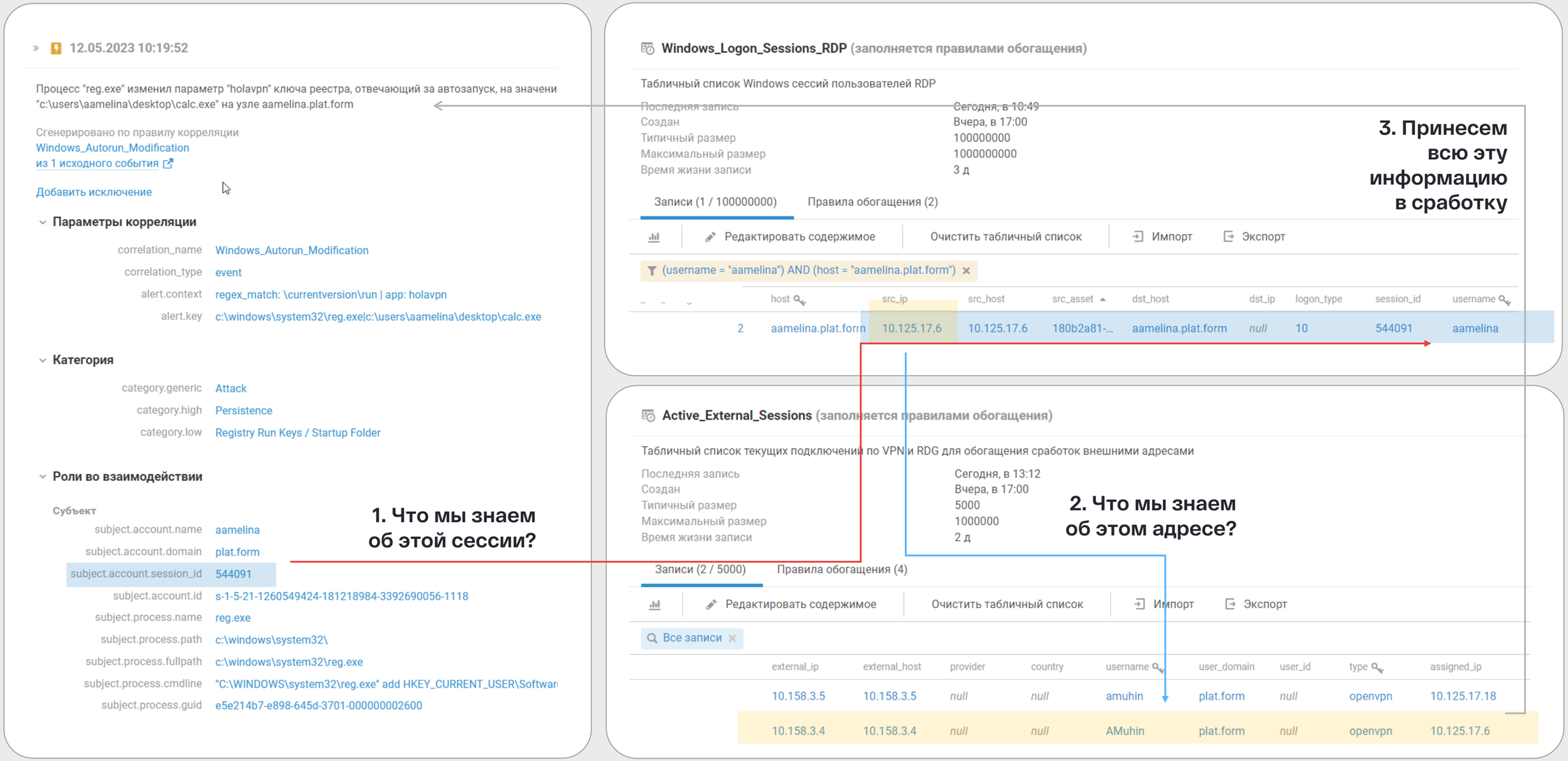
Объект

object	system
object.property	session ID with ElevatedToken
object.value	8532520

Параметры взаимодействия

importance	info
logon_type	10

Контекст пользователя



Обогащение по VPN-сессии

Active_External_Sessions (заполняется правилами обогащения)

Табличный список текущих подключений по VPN и RDG для обогащения сработок внешними адресами

Последняя запись	Сегодня, в 13:12
Создан	Вчера, в 17:00
Типичный размер	5000
Максимальный размер	1000000
Время жизни записи	2 д

Записи (2 / 5000) | Правила обогащения (4)

Редактировать содержимое | Очистить табличный список | Импорт | Экспорт

	external_ip	external_host	provider	country	username	user_domain	user_id	type	assigned_ip
	10.158.3.5	10.158.3.5	*null*	*null*	amuhin	plat.form	*null*	openvpn	10.125.17.18
12.05.2023 10:48:25	10.158.3.4	10.158.3.4	*null*	*null*	AMuhin	plat.form	*null*	openvpn	10.125.17.6

OpenVPN
Cisco
Fortinet
Citrix
КриптоПро

Контекст пользователя

Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\desktop\calc.exe" на узле aamelina.plat.form

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

Добавить исключение

Параметры корреляции

correlation_name	Windows_Autorun_Modification
correlation_type	event
alert.context	regex_match: \currentversion\run | app: holavpn
alert.key	c:\windows\system32\reg.exe|c:\users\aamelina\desktop\calc.exe

Категория

category.generic	Attack
category.high	Persistence
category.low	Registry Run Keys / Startup Folder

Роли во взаимодействии

Субъект

subject.account.name	aamelina
subject.account.domain	plat.form
subject.account.session_id	544091
subject.account.id	s-1-5-21-1260549424-181218984-3392690056-1118
subject.process.name	reg.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\reg.exe
subject.process.cmdline	"C:\WINDOWS\system32\reg.exe" add HKEY_CURRENT_USER\Software\M
subject.process.guid	e5e214b7-efe3-645d-c801-000000002600
subject.process.id	796
subject.process.parent.name	powershell.exe
subject.process.parent.id	7184
subject.process.parent.cmdline	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Процесс "reg.exe" изменил параметр "holavpn" ключа реестра, отвечающий за автозапуск, на значение "c:\users\aamelina\desktop\calc.exe" на узле aamelina.plat.form

Сгенерировано по правилу корреляции
Windows_Autorun_Modification
из 1 исходного события

Добавить исключение

Параметры корреляции

correlation_name	Windows_Autorun_Modification
correlation_type	event
alert.context	regex_match: \currentversion\run | app: holavpn
alert.key	c:\windows\system32\reg.exe|c:\users\aamelina\desktop\calc.exe

Категория

Адресаты

Отправитель

external_src.host	10.158.3.4
src.host	10.125.17.6
src.ip	10.125.17.6

Роли во взаимодействии

Субъект

subject.application.account.na...	amuhin
subject.application.account.do...	plat.form
subject.account.name	aamelina
subject.account.domain	plat.form
subject.account.session_id	544091
subject.account.id	s-1-5-21-1260549424-181218984-3392690056-1118
subject.process.name	reg.exe
subject.process.path	c:\windows\system32\
subject.process.fullpath	c:\windows\system32\reg.exe

Принятие решения о реагировании

Процесс **reg.exe** изменил параметр holavpn ключа реестра, отвечающий за автозапуск, на значение **c:\users\aamelina\desktop\calc.exe** на узле **aamelina.plat.form**

Подключившись по **VPN** с использованием учетной записи **amuhin@plat.form** и тем самым получив доступ во внутреннюю сеть, атакующий осуществил интерактивный вход на узел **aamelina.plat.form**, используя учетные данные пользователя **aamelina@plat.form**. Имея интерактивный доступ к узлу, атакующий запустил **powershell.exe** и закрепился на узле, изменив параметр holavpn ключа реестра, отвечающий за автозапуск, на значение **c:\users\aamelina\desktop\calc.exe**

На какие поля обращать внимание

Поле таксономии	Какую информацию содержит
object.process.* **object.process.parent.*** **subject.process.*** **subject.process.parent.***	Информация о процессе-объекте или процессе-субъекте, если она отсутствует с исходной сработке
object.process.chain **subject.process.chain**	Информация о цепочке запуска процесса
subject.account.* **object.account.***	Информация о пользователе
src.ip **src.host**	Адрес входа на узле, если в исходной сработке поле не заполнено
logon_type	Тип входа пользователя на узел
external_src.ip **external_src.host**	Внешний адрес пользователя при подключении через средство удаленного доступа
subject.application.account.*	Исходное имя пользователя, которому был выдан адрес при подключении к инфраструктуре

Классический плейбук

1 → **Что есть в этом событии**

Какой организации принадлежит адрес соединения?
Может, это известный IoC?

✓ 2 → **Контекст процесса**

Как этот файл появился на узле? Кем он был создан?
Кто был родителем процесса? Какой командой был запущен процесс?

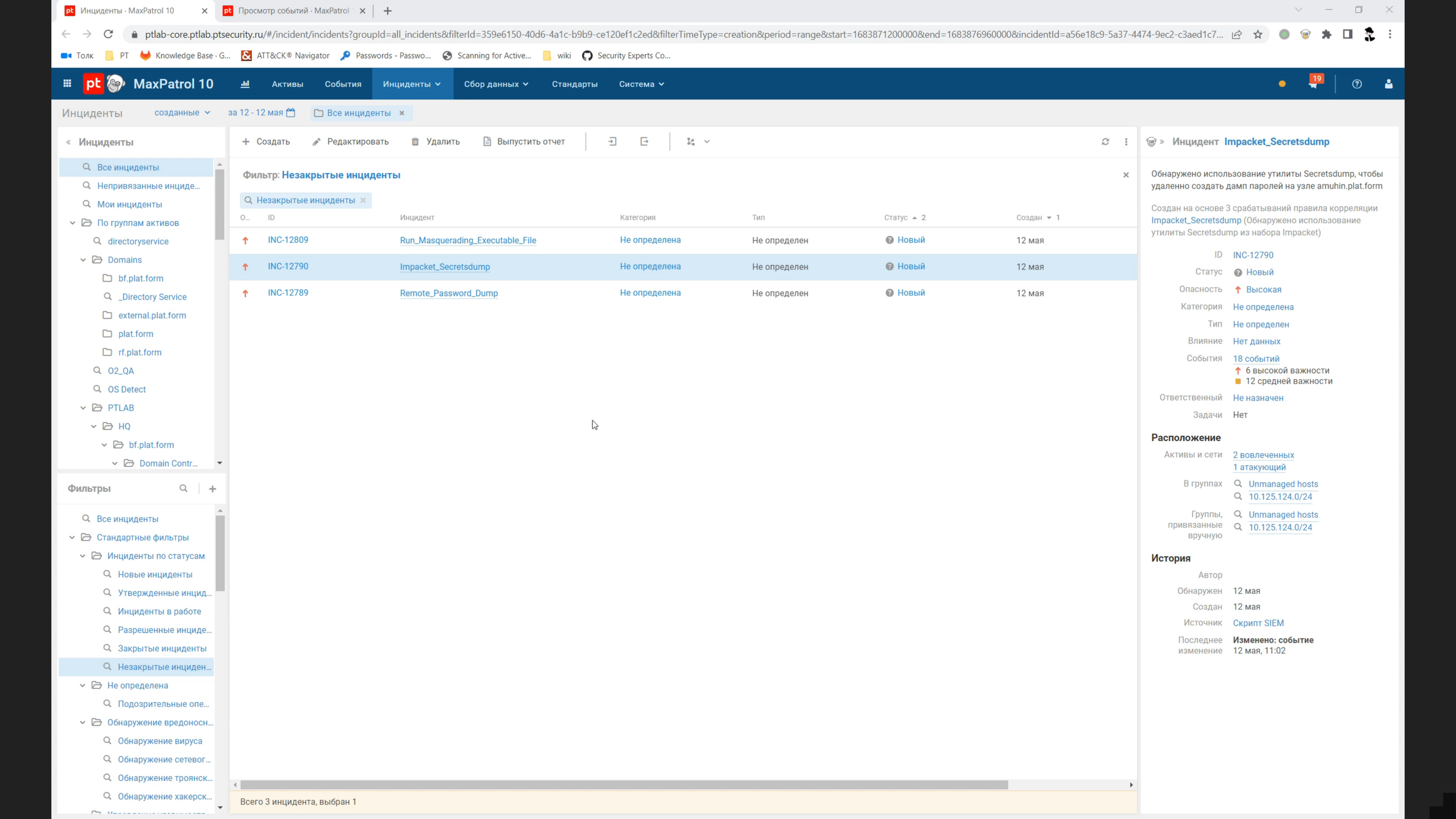
✓ 3 → **Контекст пользователя**

Кто запустил процесс?
Откуда пользователь пришел на узел?

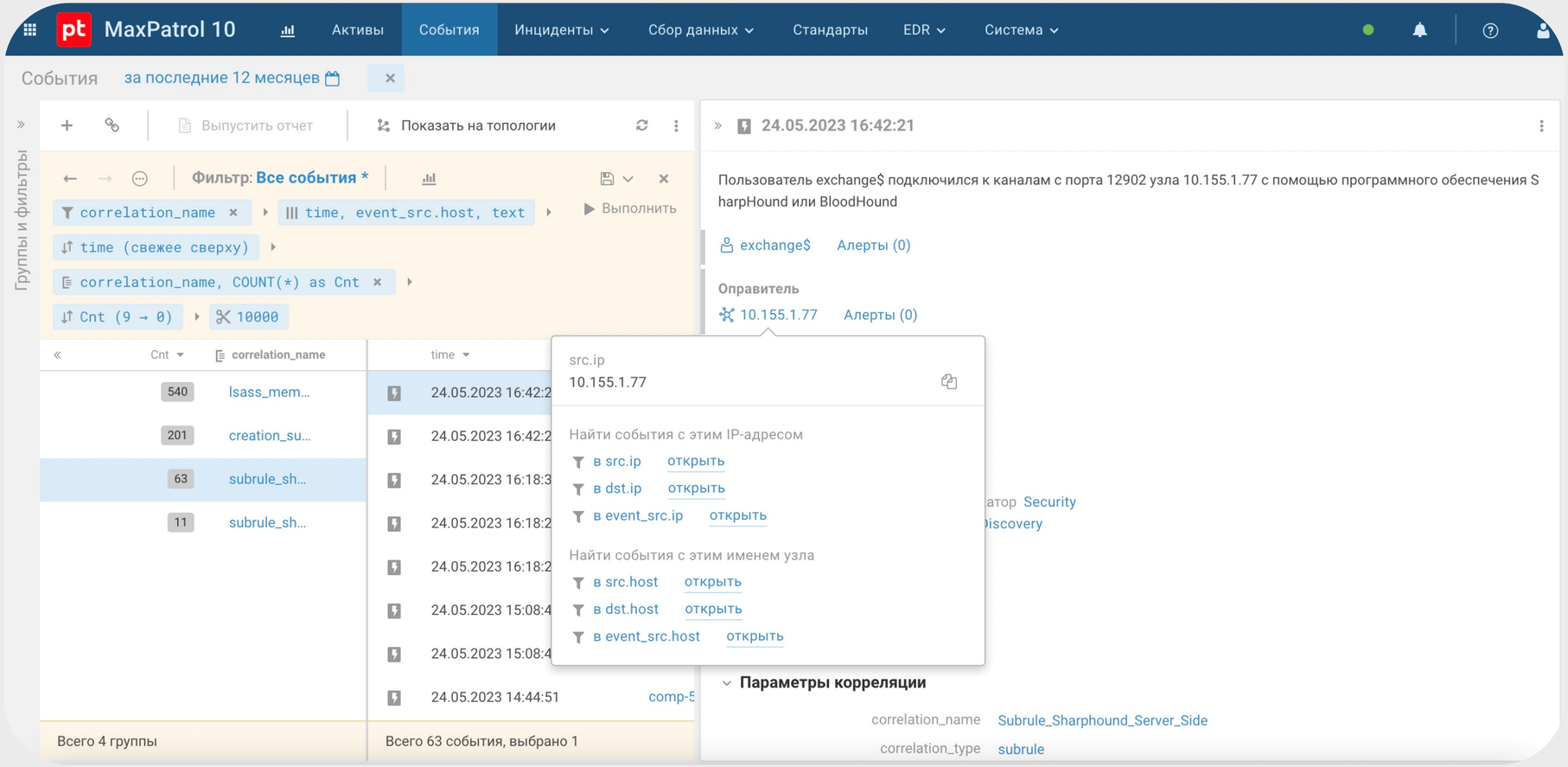
4 → **Что происходит дальше**

Полноценное расследование инцидента и реагирование

Процесс reg.exe изменил параметр holavpn ключа реестра, отвечающий за автозапуск, на значение c:\users\aamelina\desktop\calc.exe на узле aamelina.plat.form


Инциденты · MaxPatrol 10
Просмотр событий · MaxPatrol
ptlab-core.ptlab.ptsecurity.ru/#/incident/incidents?groupId=all_incidents&filterId=359e6150-40d6-4a1c-b9b9-ce120ef1c2ed&filterTimeType=creation&period=range&start=1683871200000&end=1683876960000&incidentId=a56e18c9-5a37-4474-9ec2-c3aed1c7...
Толк
PT
Knowledge Base · G...
ATT&CK® Navigator
Passwords - Passwo...
Scanning for Active...
wiki
Security Experts Co...
MaxPatrol 10
Активы
События
Инциденты
Сбор данных
Стандарты
Система
19
Инциденты
созданные
за 12 - 12 мая
Все инциденты
Инциденты
Все инциденты
Неприв язанные инциде...
Мои инциденты
По группам активов
directoryservice
Domains
bf.plat.form
_Directory Service
external.plat.form
plat.form
rf.plat.form
O2_QA
OS Detect
PTLAB
HQ
bf.plat.form
Domain Contr...
Фильтры
Все инциденты
Стандартные фильтры
Инциденты по статусам
Новые инциденты
Утвержденные инцид...
Инциденты в работе
Разрешенные инциде...
Закрытые инциденты
Незакрытые инциден...
Не определена
Подозрительные опе...
Обнаружение вредоносн...
Обнаружение вируса
Обнаружение сетевог...
Обнаружение троянск...
Обнаружение хакерск...
Создать
Редактировать
Удалить
Выпустить отчет
Фильтр: Незакрытые инциденты
Незакрытые инциденты
O...
ID
Инцидент
Категория
Тип
Статус 2
Создан 1
INC-12809
Run_Masquerading_Executable_File
Не определена
Не определен
Новый
12 мая
INC-12790
Impacket_Secretsdump
Не определена
Не определен
Новый
12 мая
INC-12789
Remote_Password_Dump
Не определена
Не определен
Новый
12 мая
Всего 3 инцидента, выбран 1
Инцидент Impacket_Secretsdump
Обнаружено использование утилиты Secretsdump, чтобы удаленно создать дамп паролей на узле amuhin.plat.form
Создан на основе 3 срабатываний правила корреляции Impacket_Secretsdump (Обнаружено использование утилиты Secretsdump из набора Impacket)
ID INC-12790
Статус Новый
Опасность Высокая
Категория Не определена
Тип Не определен
Влияние Нет данных
События 18 событий
6 высокой важности
12 средней важности
Ответственный Не назначен
Задачи Нет
Расположение
Активы и сети 2 вовлеченных
1 атакующий
В группах Unmanaged hosts
10.125.124.0/24
Группы, привязанные вручную Unmanaged hosts
10.125.124.0/24
История
Автор
Обнаружен 12 мая
Создан 12 мая
Источник Скрипт SIEM
Последнее изменение Изменено: событие
12 мая, 11:02

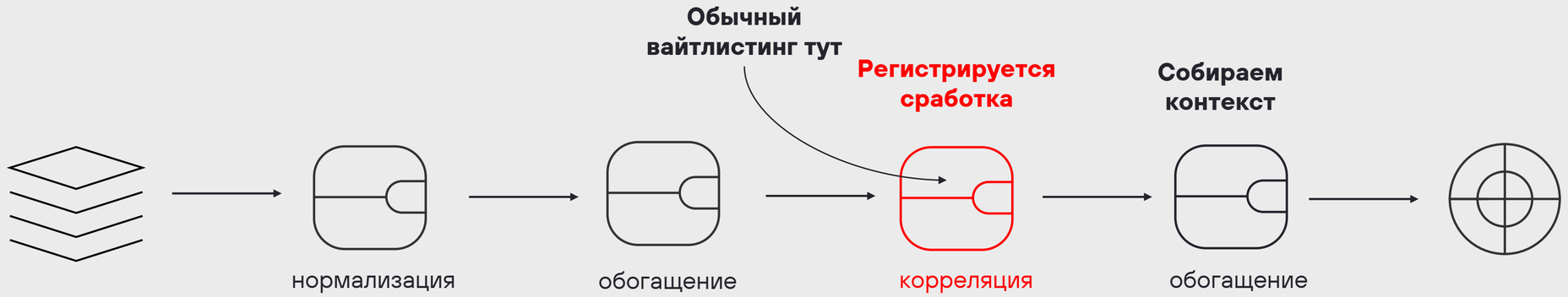
Еще проще, еще быстрее



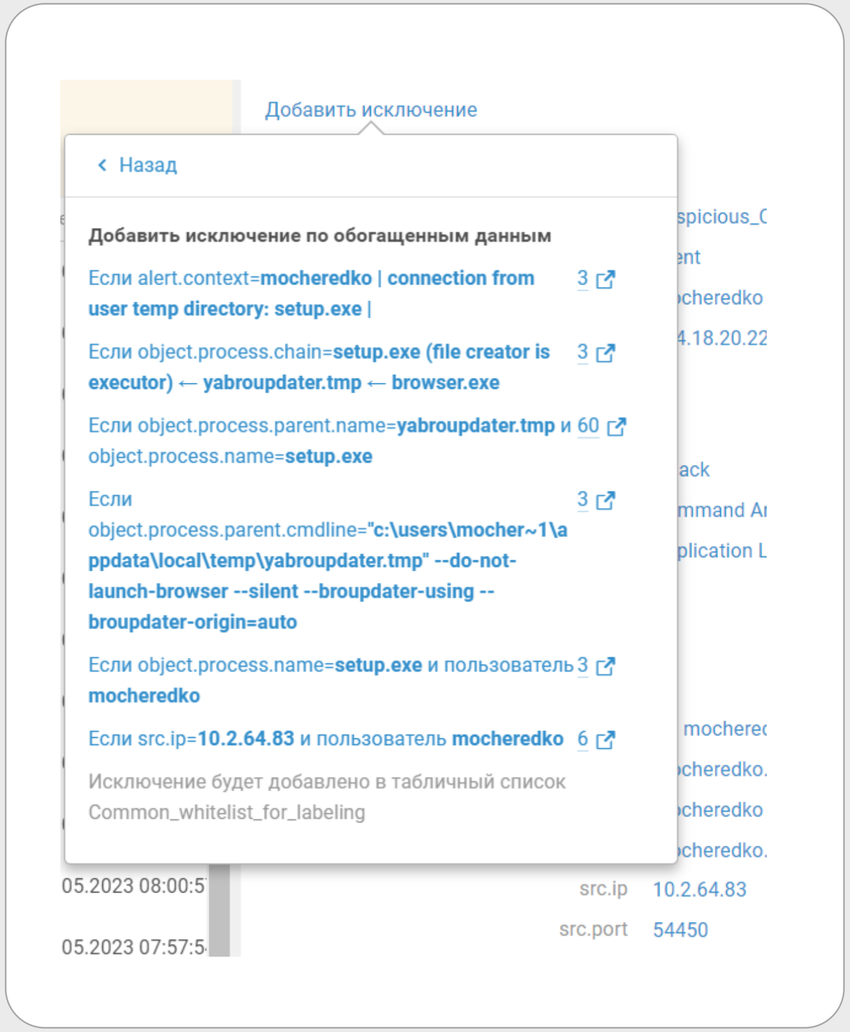
Вайтлистинг по обогащенным данным

Обнаружено сетевое обращение к узлу 104.18.20.226:80, инициированное файлом setup.exe из временной директории на узле

object.process.cmdline	"c:\users\mocher~1\appdata\local\temp\cr_a3b52.tmp\setup.exe" --install-archive="c:\users\mocher~1\appdata\local\temp\cr_a3b52.tmp\browser.packed.7z" --brand-package="c:\users\mocher~1\appdata\local\temp\cr_a3b52.tmp\brand" --partner-package="c:\users\mocher~1\appdata\local\temp\cr_a3b52.tmp\partner" --update --do-not-launch-browser --silent --broupdater-using --broupdater-origin=auto file creator is executor
object.process.chain	setup.exe (file creator is executor) ← yabroupdater.tmp ← browser.exe



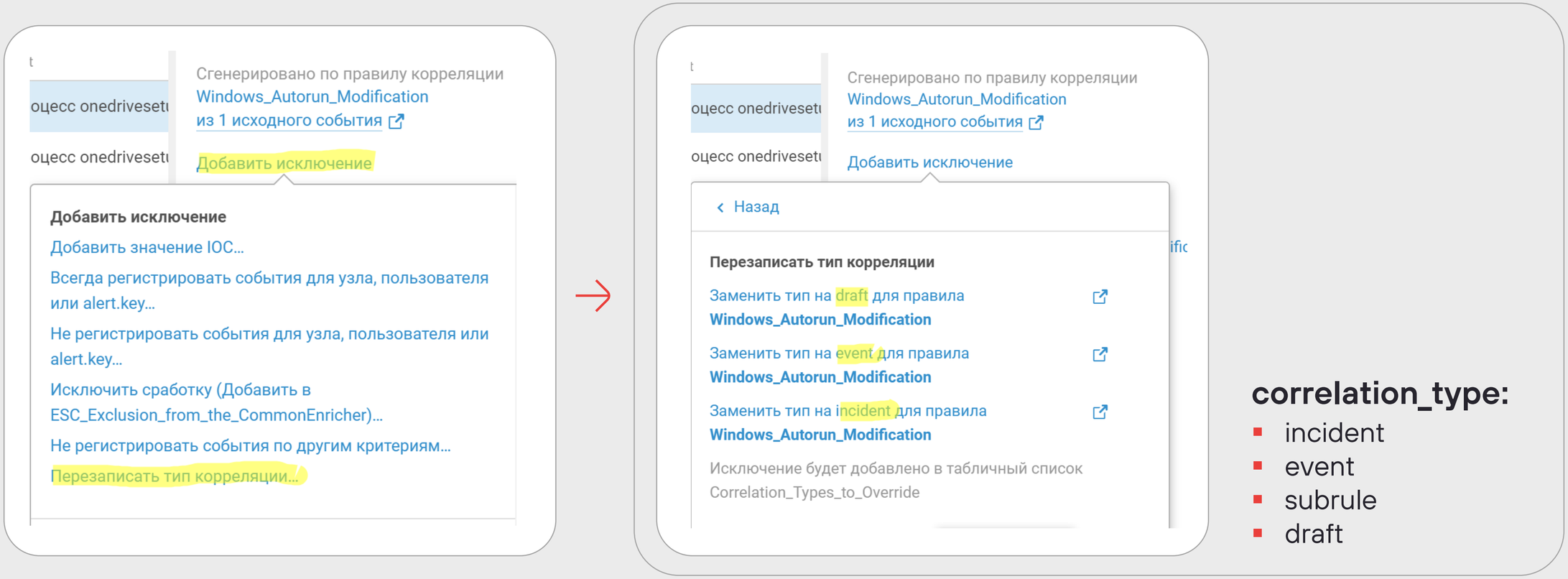
Вайтлистинг по обогащенным данным



Статья об идее вайтлистинга и обработке ложных срабатываний

Вебинар про механизмы обработки исключений в MaxPatrol SIEM

Гибкое управление типом сработки



Механизмы в цифрах

5

табличных списков

- Процессы
- Сессии пользователей
- Внешние подключения
- Созданные файлы

9

правил обогащения,

которые записывают данные в TC
и приносят данные в сработки,
чтобы упростить работу аналитику

70+

интеграционных тестов,

чтобы мы всегда могли быть
уверены в корректности работы
механизмов после любых
обновлений контента

3

команды экспертов

вели работу над разработкой

10 000+

часов тестирования

на собственной инфраструктуре,
несинтетических данных и реальном
потоке событий

1

пакет экспертизы

включающий многолетний опыт
работы экспертов PT ESC

Пакет экспертизы
«Расследование запуска процессов
и исследование сеансов»
позволяет автоматизировать
плейбуки по расследованию
инцидентов

Спасибо!