



InfoWatch Data Access Tracker 1.0

Release Notes



Улучшенный анализ доступа и новый механизм выявления аномалий в актуальном релизе системы аудита и мониторинга InfoWatch Data Access Tracker 1.0.

В InfoWatch Data Access Tracker 1.0 (далее IW DAT) расширена функциональность в части выявления аномальной активности пользователей и анализа доступа к корпоративным ресурсам:

- новый механизм аномалий, который отображает критические отклонения количества событий на дневном отрезке;
- индекс атипичного поведения и параметров пользователей;
- карта параметров и поведения пользователей;
- улучшен анализ доступа пользователей к ресурсам компании.

Список изменений:

- **Новый механизм аномалий**

К аномальному поведению можно отнести подключение к сети в нерабочее время, попытки подключения к ресурсам, к которым пользователь не допущен по должностным обязанностям, а также массовое скачивание, удаление или изменение файлов.

Выявление отклонений от нормы поведения пользователя может являться поводом для дальнейшего расследования и фиксируется в разделе Аномалии.

Для отображения динамики аномальных активностей в Системе используется таблица критических отклонений количества событий на дневном отрезке.

Время	Количество	Среднее	Динамика	Фактор	Метод ↓
2 августа 2020 г., 00:00:00	28183	3287.48	↑ 757.28%	7.62	Z-Score Local Outlier Factor Isolation Forest ...
3 августа 2020 г., 00:00:00	28104	3287.48	↑ 754.88%	7.53	Z-Score Local Outlier Factor Isolation Forest ...
23 марта 2021 г., 00:00:00	25223	3287.48	↑ 667.24%	7.45	Z-Score Local Outlier Factor Isolation Forest ...
5 августа 2020 г., 00:00:00	32440	3287.48	↑ 886.77%	7.58	Z-Score Local Outlier Factor Isolation Forest ...
18 марта 2021 г., 00:00:00	26360	3287.48	↑ 701.83%	7.58	Z-Score Local Outlier Factor Isolation Forest ...
21 марта 2021 г., 00:00:00	37207	3287.48	↑ 1031.78%	7.74	Z-Score Local Outlier Factor Isolation Forest ...
1 августа 2020 г., 00:00:00	24668	3287.48	↑ 650.36%	7.55	Z-Score Local Outlier Factor Isolation Forest ...
4 августа 2020 г., 00:00:00	31860	3287.48	↑ 869.13%	7.62	Z-Score Local Outlier Factor Isolation Forest ...
9 апреля 2021 г., 00:00:00	19354	3287.48	↑ 488.72%	7.14	Z-Score Isolation Forest One-Class SVM
23 апреля 2021 г., 00:00:00	22608	3287.48	↑ 587.70%	7.19	Z-Score Isolation Forest One-Class SVM

Аномалии на дневном отрезке

- **Индекс атипичности**

IW DAT контролирует обращения пользователей к устройствам, файлам и почтовым ящикам. На основе полученных данных при помощи алгоритмов выявления аномалий система выстраивает индекс атипичности для каждого пользователя. Это позволяет своевременно выявить подозрительную активность и вызвать оперативную реакцию администратора.



ADMIN
I2M\pbg
Установить метки

4286 Количество входов | 133666 События | 5.37 Индекс атипичности

100 РИСК-ФАКТОР

100 Не используется настройка автоматической смены пароля

75 Аккаунт не используется 2 месяца

АНОМАЛИИ НА ЧАСОВОМ ОТРЕЗКЕ
Критические отклонения количества событий на часовом отрезке

Время	Количество
5 августа 2020 г., 07:00:00	3

ИНФОРМАЦИЯ СВЯЗИ АНАЛИЗ ФАЙЛЫ ПОЧТОВЫЕ ЯЩИКИ ПРОЦЕДУРЫ

СОБЫТИЯ ОПОВЕЩЕНИЯ СТАТИСТИКА ПОХОЖИЕ

5.37 ИНДЕКС АТИПИЧНОСТИ

- 12.89 Индекс атипичности по Local Outlier Factor (LOF)
- 4.45 Индекс атипичности по Isolation Forest
- 1.00 Индекс атипичности по One-Class SVM

Основания для решения

Параметр	Параметр
Количество входов	4286
Имеет E-Mail	Нет
Имеет телефон	Нет
Отключен	Нет
Заблокирован	Нет
Необязательный ввод пароля	Нет
Пользователь имеет пароль б...	Да
Количество почтовых ящиков	53

Индекс атипичности действий пользователя

- **Карта пользователей**

В Системе появилась карта параметров и поведения пользователей, которая отображает уровень атипичной активности. Оператор может обратить внимание на пользователей с высокой степенью атипичности и принять соответствующие меры — инициировать смену пароля для пользователя, ограничить доступ к определенным ресурсам, заблокировать пользователя и так далее.

КАРТА ПОЛЬЗОВАТЕЛЕЙ
Карта параметров и поведения пользователей

Разделение по атипичности

100 75 50 25 0

0 25 50 75 100

● Прочие ● Низкая ● Средняя ● Высокая

Подробнее

Имя	Риск-фактор	Индекс атипичности
	72	0.33
	Отключен	1.66
	100	0.89
	72	
	100	

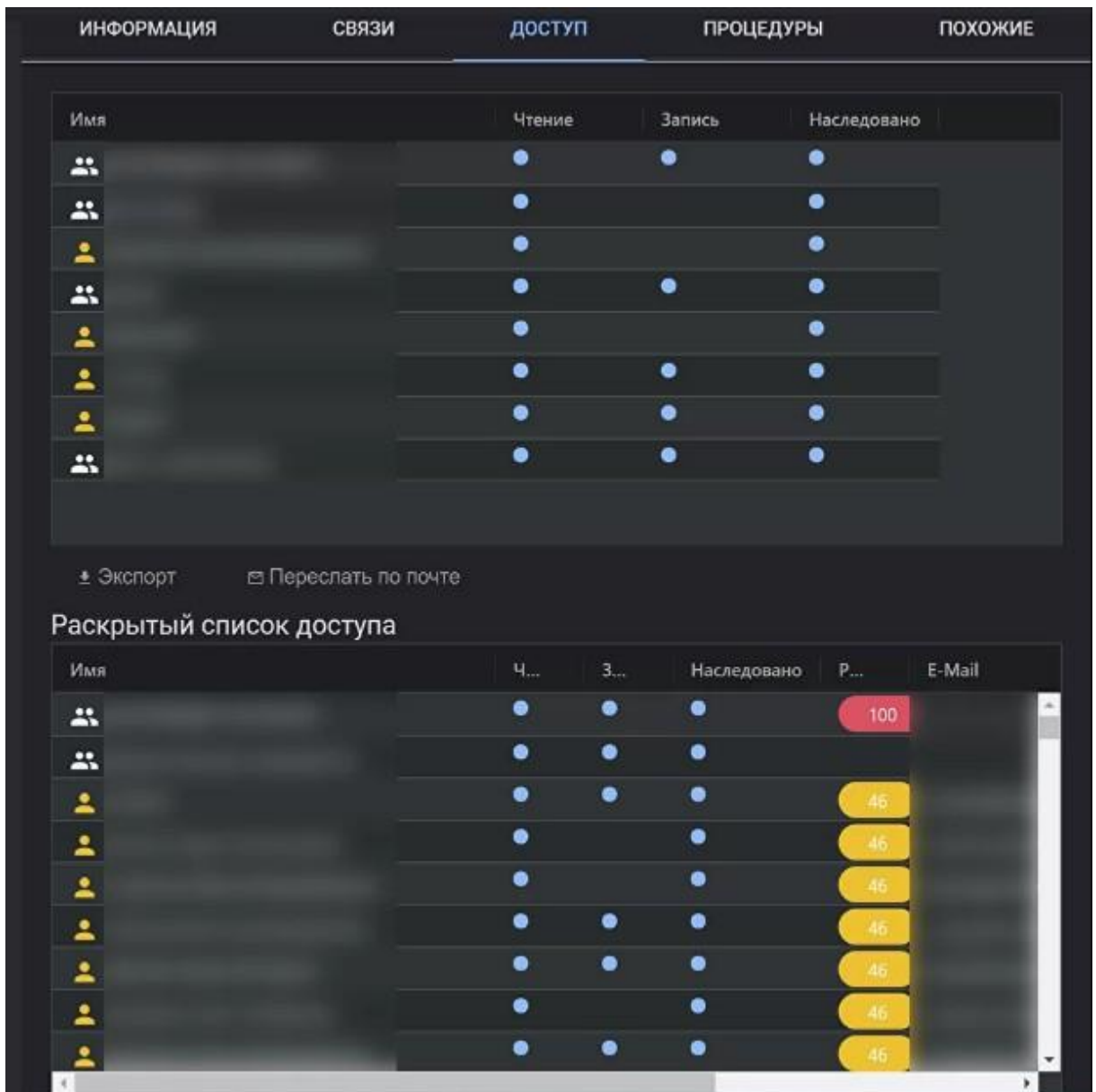
Карта параметров и поведения пользователей



- **Анализ доступа**

В IW DAT улучшен анализ доступа к определенному ресурсу — файлу или папке.

Детализированный список с настраиваемыми фильтрами, который отображает уровни доступа к конкретному файлу, наследование прав, e-mail адреса пользователей, для которых открыт доступ и риск-фактор, можно экспортировать для передачи исполнителю или отправить по e-mail прямо из консоли.



Детализация списка доступа