

Непродуктивная деятельность

Внутренняя угроза

Некорректное поведение

Борьба с играми на рабочем месте

Одна из распространенных проблем компаний и боль многих руководителей — нецелевое использование рабочего времени сотрудниками. Предлагаем рассмотреть решение этой проблемы с помощью DLP-системы Falcongaze SecureTower.



Проблема

Каждый руководитель хочет быть уверенным, что сотрудник тратит свое рабочее время не напрасно и честно выполняет трудовые обязанности. К тому же, что делать, если коллектив на работу приходит вовремя, все сидят по рабочим местам, однако это не помогает — задачи решаются медленно, сроки постоянно приходится сдвигать, из-за чего компания теряет клиентов и заработок? В таком случае поможет специальное программное обеспечение, которое не только отследит время начала и окончания работы сотрудников, но и соберет подробную информацию об их цифровой активности, а также поможет обнаружить причины нарушения трудовой дисциплины.

Решение

Одна проектная организация год назад установила программный комплекс SecureTower и сразу настроила правила безопасности на отслеживание эффективности рабочего времени.

Со слов руководителя, плюсом ST является большое разнообразие отчетов, которые выгружаются за определенный период и рассылаются по установленным адресатам автоматически. Самым используемым же стал Сводный отчет по пользователям. На протяжении почти всего года показатели этого отчета не привлекали внимание руководителя. Однако за последние два месяца данные по трем сотрудникам ухудшились. Был зафиксирован рост нецелевой веб-активности, а в ТОП-3 посещенных сайтов вошли крупнейший магазин компьютерных игр Steam и платформа для онлайн-игр Yandex Games. Было принято решение исследовать инцидент подробнее.

The screenshot shows the 'Сводный отчет по подозрительным пользователям' (Summary report for suspicious users) in the SecureTower Client console. The report displays browser activity statistics for 19 users, including the number of pages visited and time spent, along with a list of the top 3 visited websites for each user.

Пользователь	Браузер-активности: количество по...		Браузер-активности: время, провед...		Top посещенных сайтов		
	Σn	n	Σn	n	1 йл.	2 йл.	3 йл.
Александр Иванов	97	24.2	01:33:34	00:23:23	mail.google...	google.ru	habrahabr.ru
Александр Иванов	55	13.8	00:57:52	00:14:28	store.steamp...	yandex.ru	visualsivn.com
Александр Иванов	56	14	01:00:38	00:15:09	stackoverflo...	visualsivn.com	about
Александр Иванов	105	26.2	01:32:47	00:23:11	store.steamp...	yandex.ru	habrahabr.ru
Александр Иванов	83	20.8	01:17:11	00:19:17	stackoverflo...	google.ru	msdn.micros...
Александр Иванов	41	10.2	00:56:59	00:14:14	multitran.ru	google.ru	habrahabr.ru
Александр Иванов	105	26.2	01:37:43	00:24:25	mail.google...	google.ru	habrahabr.ru
Александр Иванов	172	43	03:15:26	00:48:51	newtab	multitran.ru	msdn.ru
Александр Иванов	128	32	02:33:55	00:38:28	newtab	leprosorium.ru	youtube.com
Александр Иванов	96	24	01:30:54	00:23:43	store.steamp...	yandex.ru	sdma.ru
Александр Иванов	51	12.8	00:56:19	00:14:04	stackoverflo...	dyju-soft.nar...	visualsivn.com
Александр Иванов	124	31	02:37:30	00:39:22	newtab	leprosorium.ru	youtube.com
Александр Иванов	104	26	01:35:38	00:23:54	mail.google...	google.ru	sdma.ru
Александр Иванов	40	10	00:55:56	00:13:59	store.steamp...	yandex.ru	newtab
Александр Иванов	87	21.8	01:17:03	00:19:15	stackoverflo...	google.ru	b2bsky.ru
Александр Иванов	106	26.5	01:35:40	00:23:55	mail.google...	google.ru	top.rbc.ru
Александр Иванов	45	11.2	01:00:39	00:15:09	google.ru	translate.go...	lenta.ru
Александр Иванов	13	13	00:23:19	00:23:19	stackoverflo...	yandex.ru	google.ru
Александр Иванов	59	14.8	00:58:49	00:14:42	stackoverflo...	dyju-soft.nar...	visualsivn.com
Всего (19)	1 567	21.1	27:37:52	00:22:42	store.steamp...	yandex.ru	newtab

Модуль «Отчеты» (Сводный отчет)

Отследить участников и историю нарушений трудового распорядка смогли с помощью специального функционала Активность пользователя SecureTower. В отделе безопасности был запрошен более подробный отчет по интересующим сотрудникам, их веб-активности (особенно времени, проведенном на сайтах) и вовлеченности в трудовые процессы. Все доказательства нарушений трудового распорядка были зафиксированы в личных делах.

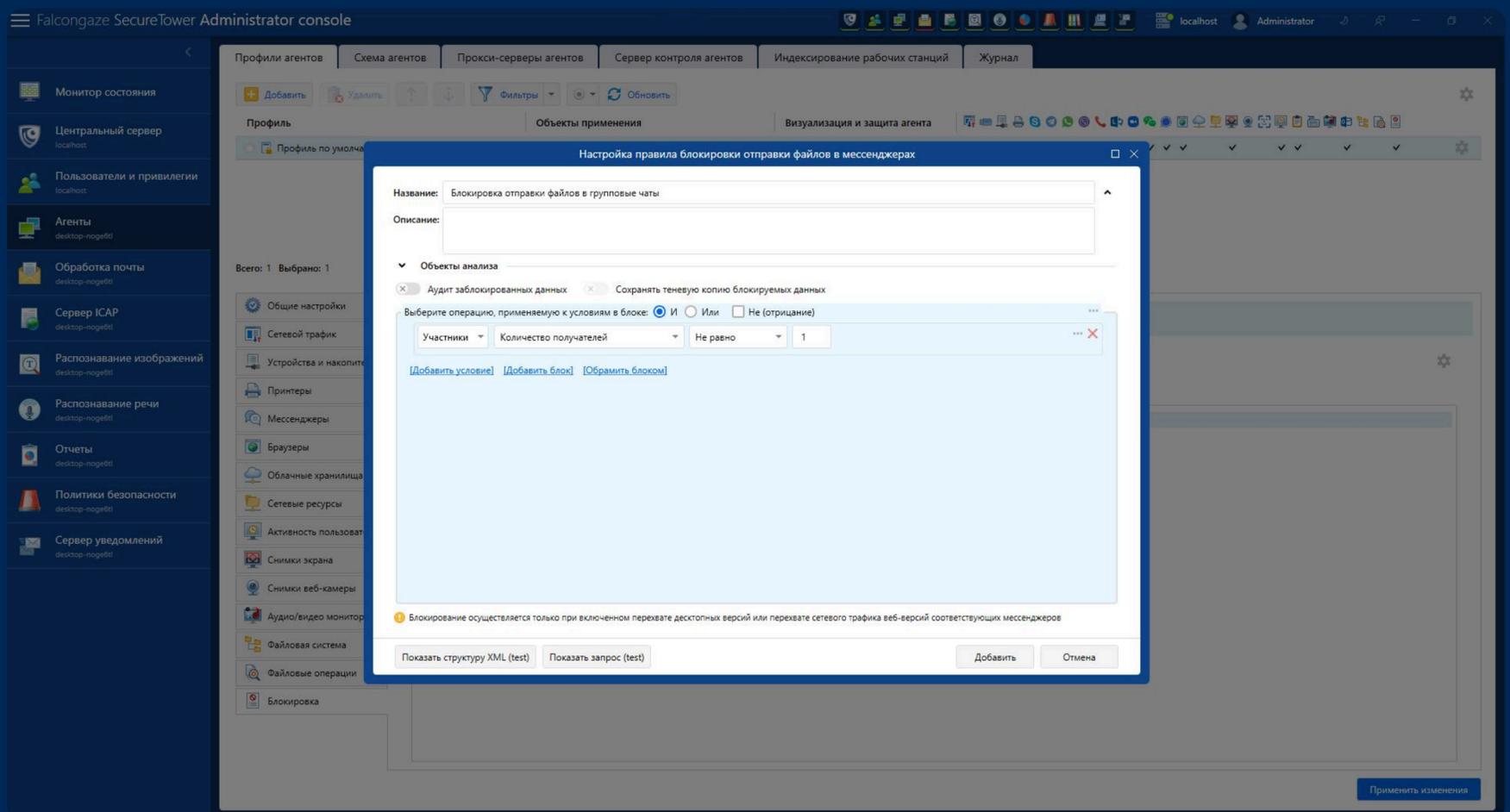
The screenshot shows the 'Нецелевое использование рабочего времени' (Non-targeted use of working time) investigation report in the SecureTower Client console. The report lists five incidents of browser activity, including the user, the type of data, the local user, the remote user, and the time of the incident.

#	Тип данных	Локальный пользователь	Удаленный пользователь	Перехвачено
1	Браузер-активность	Александр Иванов	Александр Иванов	30.11.2024 18:00:34
2	Браузер-активность	Александр Иванов	Александр Иванов	01.12.2024 16:44:24
3	Браузер-активность	Александр Иванов	Александр Иванов	02.12.2024 16:48:37
4	Браузер-активность	Александр Иванов	Александр Иванов	30.11.2024 16:35:11
5	Браузер-активность	Александр Иванов	Александр Иванов	02.12.2024 16:48:37

Модуль «Расследования»

Затем для автоматического отслеживания и пресечения подобных инцидентов в будущем были активированы политики безопасности по параметрам посещения популярных игровых ресурсов (сайты, приложения), что позволило обеспечить контроль подобных инцидентов для всего коллектива.

Параллельно с этим с профилактической целью была заблокирована возможность отправки файлов в мессенджера. Согласно информации о веб-активности пользователей, штатные игроки использовали для обсуждения игр чат в Viber, в который входили также посторонние для компании лица.



Консоль Администратора (Правило блокировки отправки файлов в мессенджерах)

Как позже показала практика, эта мера была оправдана, так как во время очередного обсуждения боев в Borderlands один из сотрудников по ошибке прикрепил технический документ к сообщению и осуществил попытку его отправки. DLP-система распознала инцидент и пресекла распространение информации.

Результат

- **Доказаны нецелевые траты рабочего времени**

Программный комплекс SecureTower помог выявить игроков в коллективе.

- **Заведены личные дела сотрудников**

Специалист отдела безопасности смог зафиксировать нарушения каждого сотрудника в личном деле, что обеспечит сохранность истории участия в инцидентах.

- **Пресечено распространение конфиденциальной информации**

Благодаря вовремя примененному правилу блокировки передачи файлов было пресечено распространение технического документа, содержавшего конфиденциальные данные о застройке жилого квартала клиентом.

С сотрудниками, которые играли в рабочее время, была проведена профилактическая беседа и вынесены устные предупреждения, а специалист отдела безопасности провел лекцию на тему безопасного обращения с цифровыми документами в компании и цифровой гигиены в целом, что поможет пресечь подобные инциденты в будущем. Также благодаря непрерывному мониторингу темы «Видеоигры» есть возможность обнаружить повторные нарушения и применить более серьезные меры наказания к сотрудникам в случае необходимости.

Модули, которые были использованы:



Политики безопасности



Отчеты



Расследования