ИСПОЛНИТЕЛЬ	**ЗАКАЗЧИК**
Заместитель генерального директора ТОО «MSSP.GL»	Заместитель руководителя КГУ «Управления цифровизации города Алматы»
Р.С. Джансенгиров	М.А. Дюсюков
_____	_____

Отчет об оказанных услугах по обеспечению информационной безопасности акимата города Алматы по сервисной модели информатизации

Акимат города Алматы

Отчетный период: 01.05.2026 – 31.05.2026 г.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

Оглавление

1. ОБЩАЯ ИНФОРМАЦИЯ 3
1.1. Ключевые показатели эффективности 3
2. ВВЕДЕНИЕ 3
2.1. Цель отчета 3
2.2. Область действия 3
3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 4
3.1. Состояние агентов 4
3.2 Настройка и актуализация представлений данных (Data Views) 4
3.3. Усиление мониторинга и анализа событий через SIEM-систему 5
4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6
4.1. Статистика событий безопасности 9
4.2. Система уведомлений 14
4.3 Поиск угроз 15
4.4. Доступность веб-интерфейса 15
4.5. Автоматическое реагирование на угрозы 15
5.1 Инструментальное сканирование 16
5.2 Статистика управления уязвимости 18
6.1. OpenCTI — Платформа киберразведки 20
6.2. MISP — Обмен индикаторами компрометации 21
6.3. T-Lab Sandbox — Защита от таргетированных атак 21
6.4. DLP – Предотвращение утечек данных (safetica) 26
6.4.1. Анализ веб – активности 27
6.4.2. Передачи данных 31
6.4.3. Служебные операции через интернет и внутренние сервисы 34
6.5 Checkpoint - межсетевой экран 36
7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 38
8. ВЫВОДЫ И РЕКОМЕНДАЦИИ 39
8.1. Общие выводы 39
8.2. Приоритетные планы работ 39
8.3. Рекомендации 39

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

1. ОБЩАЯ ИНФОРМАЦИЯ

Настоящий отчет представляет результаты оказания услуг по обеспечению информационной безопасности для Акимата города Алматы (далее - Заказчик) за отчетный период 01.05.2026 – 31.05.2026 года. Услуги предоставлялись в рамках комплексного подхода к защите информационной инфраструктуры Заказчика с использованием передовых технологий мониторинга, обнаружения и реагирования на угрозы информационной безопасности.

1.1. Ключевые показатели эффективности

В отчётном периоде в SIEM зарегистрировано 7266 событий безопасности, по которым обработано 18 кейсов. Защита конечных точек обеспечивалась на 196 узлах, средствами EDR предотвращено 63 вредоносных действий. Через T-Lab Sandbox проверено 9266 файлов/объектов, выявлено 153 угроз. По результатам сканирования Nessus обнаружено 42 критических и 165 высоких уязвимостей. В системе Safetica зафиксировано 206774 DLP-событий. Средствами Check Point выполнено 12679246 блокировок.

2. ВВЕДЕНИЕ

Настоящий отчет подготовлен в соответствии с пунктом 4.5 технической спецификации на услуги по обеспечению информационной безопасности и охватывает период 01.05.2026 – 31.05.2026 года.

2.1. Цель отчета

Целью настоящего отчета является предоставление Заказчику комплексной информации о:

- Текущем состоянии систем мониторинга и защиты информационной безопасности;
- Выявленных инцидентах безопасности и принятых мерах реагирования;
- Результатах проведенного тестирования и сканирования на уязвимости;
- Статистике обработанных событий и уведомлений;
- Рекомендациях по повышению уровня защищенности инфраструктуры.

2.2. Область действия

Услуги по обеспечению информационной безопасности предоставляются для всех структурных подразделений Акимата города Алматы, включая:

- Аппарат акима города;
- 24 управлений акимата;
- Территориальные подразделения (районные акиматы).

Общий объем защищаемых объектов включает более 1000 рабочих станций, 15 серверов, 205 сетевых устройств и 12 межсетевых экранов, распределенных по 12 территориально удаленным площадкам Заказчика.

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

3. АНАЛИЗ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С момента заключения договора Поставщиком проведена комплексная инвентаризация агентов системы управления событиями информационной безопасности (SIEM), системы обнаружения и реагирования на угрозы (EDR), а также дополнительных средств защиты, установленных на рабочих станциях и серверах Заказчика. Помимо EDR-агентов, на части инфраструктуры также развернуты и используются агенты DLP и Sysmon, обеспечивающие расширенный контроль утечек данных и детализацию событий безопасности.

3.1. Состояние агентов

В отчётном периоде контроль состояния агентов EDR осуществлялся на 621 узлах, из которых защита была активна на 296 (47.67%). Выявлено 40 узлов с признаками некорректной работы агентов и 245 узлов, находившихся вне связи. Статусы агентов: healthy - 296, inactive - 40, offline - 245, unhealthy - 40. Наиболее затронутые хосты: fins-pc-0042, medu-pc-0077, sprt-pc-0014. Под мониторингом находилось 617 узлов; offline - 357, нестабильных/требующих проверки - 31.

Следует учитывать, что полное агентное покрытие всех рабочих станций ограничено рядом инфраструктурных факторов. В части подразделений эксплуатируются устаревшие операционные системы, на которых установка или стабильная работа EDR-агента невозможна. Также выявляется организационный фактор: после переустановки операционной системы отдельные рабочие станции не всегда своевременно вводятся в домен, вследствие чего они не попадают в централизованный контур управления и мониторинга. Указанные причины влияют на долю offline-узлов и требуют совместной отработки с ответственными системными администраторами.

3.2 Настройка и актуализация представлений данных (Data Views)

В отчётном периоде представления данных Elastic использовались в штатном режиме; целевые изменения состава Data Views не выполнялись. Состояние источников данных и представлений в SIEM оценено как стабильное. В рабочем пространстве подтверждена доступность 11 Data Views; ключевые представления: case*, logs-elastic_agent-akimat_almaty, metrics-*, logs-windows.sysmon_operational-akimat, logs-*, logs-*, logs-*, *akimat,.alerts-security.alerts-akimat. Через указанные представления обеспечивался анализ событий по 47 правилам корреляции, 497 хостам и 180 учетным записям пользователей.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

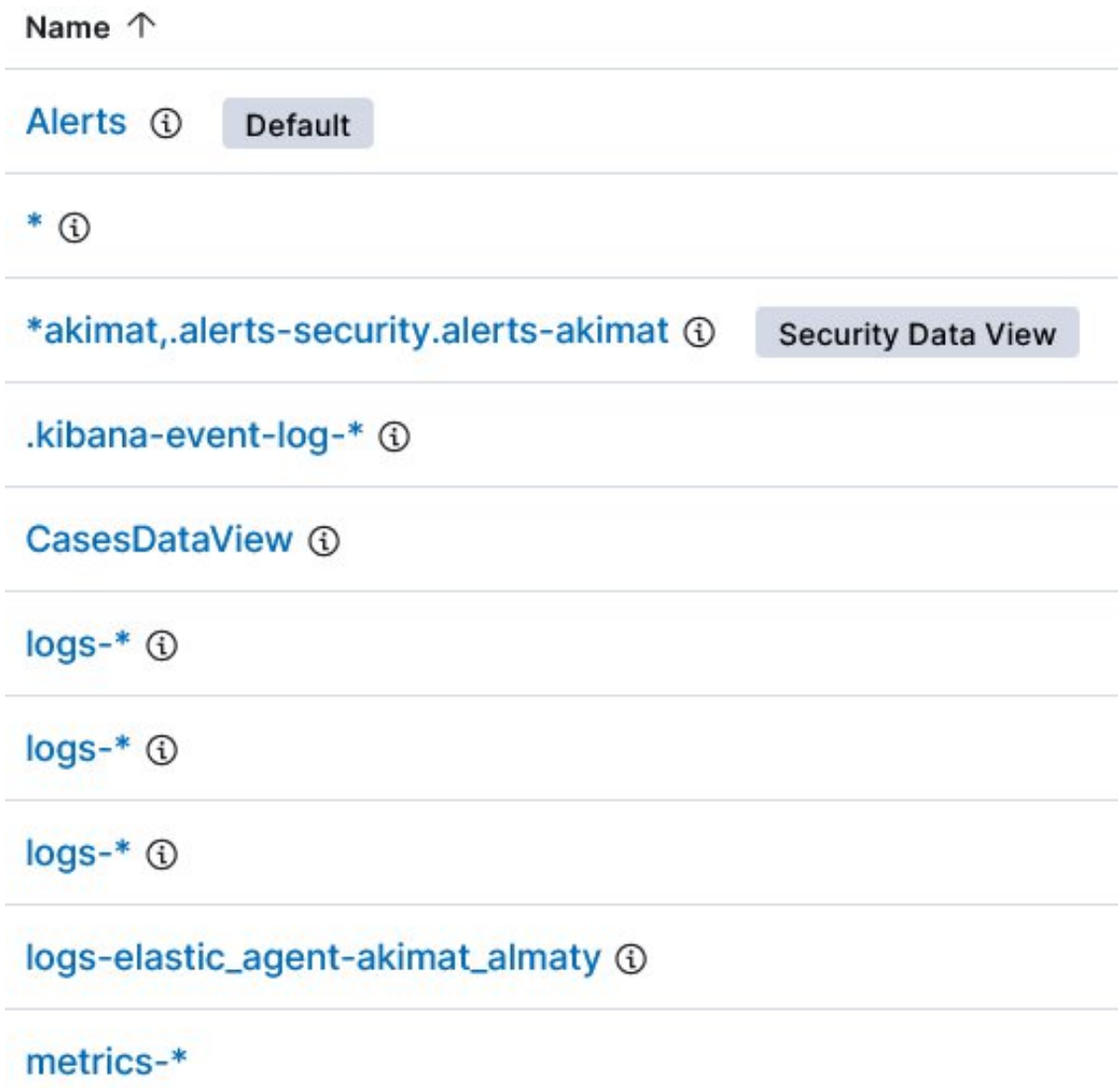


Рисунок 1. Состав представлений данных и рабочих источников Elastic

На рисунке показан состав представлений данных Elastic, задействованных в отчетном периоде. В сводном блоке указано количество Data Views - 11, а также состояние источников: стабильное. В правой части рисунка перечислены ключевые представления данных, включая: case*, logs-elastic_agent-akimat_almaty, metrics-*, logs-windows.sysmon_operational-akimat. Рисунок фиксирует, какие рабочие источники использовались для построения разделов SIEM, EDR, кейсов реагирования и аналитических выборок отчета.

3.3. Усиление мониторинга и анализа событий через SIEM-систему

За отчётный период в системе мониторинга обработано 7266 событий безопасности, в том числе critical - 19, high - 557, medium - 2853, low - 3837. Наиболее часто события фиксировались по правилам: First Time Seen Removable Device, Process Termination followed by Deletion, Potential Process Injection from Malicious Document. Всего в отчётном периоде срабатывания пришлись на 47 правил, 497 хостов и 180 пользователей. Наиболее затронутые хосты: asst-pc-0011, fins-pc-0042, medu-pc-0077; пользователи: СИСТЕМА, LOCAL SERVICE, administrator. Детализация по ключевым правилам

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z12026000019602BFD1E3

корреляции показывает следующее: «First Time Seen Removable Device» - 1 538 срабатываний (21.17%); Правило фиксирует подключение или первое обнаружение съемных носителей и применяется для контроля несанкционированного переноса данных. «Process Termination followed by Deletion» - 693 срабатываний (9.54%); Правило отражает попытки сокрытия следов или нарушения штатной работы защитных механизмов на конечной точке. «Potential Process Injection from Malicious Document» - 678 срабатываний (9.33%); Правило «Potential Process Injection from Malicious Document» используется для выявления событий, соответствующих его корреляционной логике; в отчете отражено количество таких срабатываний за период. «High Number of Process and/or Service Terminations» - 669 срабатываний (9.21%); Правило отражает попытки сокрытия следов или нарушения штатной работы защитных механизмов на конечной точке. «Privileged Account Brute Force» - 492 срабатываний (6.77%); Правило выявляет повторяющиеся неуспешные попытки аутентификации и используется для раннего обнаружения перебора учетных данных.

4. МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

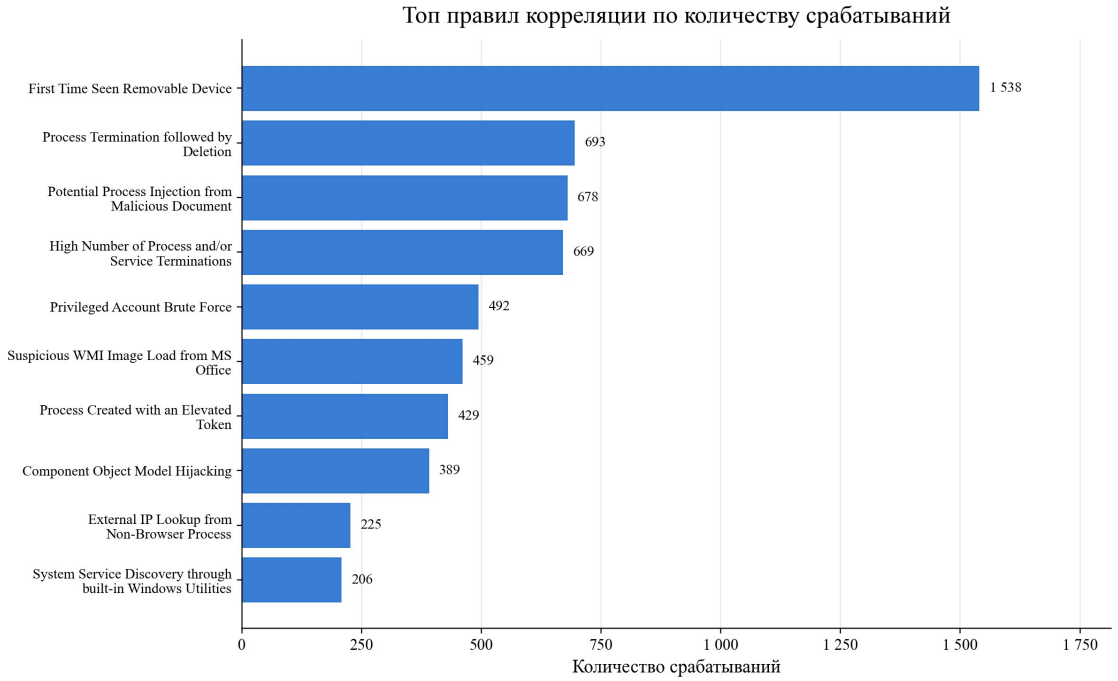


Рисунок 2. Топ правил корреляции по количеству срабатываний

На рисунке показаны корреляционные правила Elastic с наибольшим количеством срабатываний за отчетный период. Верхняя строка диаграммы соответствует правилу «First Time Seen Removable Device» с количеством срабатываний 1 538. Всего в периоде срабатывания пришлись на 47 правил, а на рисунке отображена верхняя часть выборки по количеству событий. Длина каждой полосы пропорциональна числу срабатываний соответствующего

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

правила, поэтому диаграмма показывает распределение нагрузки между наиболее активными корреляционными сценариями.

Числовая расшифровка содержит правила корреляции, представленные в разделе статистики событий. В колонках указаны порядковый номер, название правила, количество срабатываний и доля от общего числа событий. Наибольшая доля в таблице относится к правилу «First Time Seen Removable Device» - 21.17%. Табличный формат дополняет диаграмму тем, что позволяет видеть точные значения и процентный вклад каждого правила без визуальной оценки длины полос.

Таблица 1. Правила корреляции

№	Название правила	Количество	Доля
1	First Time Seen Removable Device	1 538	21.17%
2	Process Termination followed by Deletion	693	9.54%
3	Potential Process Injection from Malicious Document	678	9.33%
4	High Number of Process and/or Service Terminations	669	9.21%
5	Privileged Account Brute Force	492	6.77%
6	Suspicious WMI Image Load from MS Office	459	6.32%
7	Process Created with an Elevated	429	5.90%

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

	Token		
8	Component Object Model Hijacking	389	5.35%
9	External IP Lookup from Non-Browser Process	225	3.10%
10	System Service Discovery through built-in Windows Utilities	206	2.84%
11	Unusual Parent-Child Relationship	202	2.78%
12	Persistence via a Windows Installer	159	2.19%
13	Unusual Persistence via Services Registry	147	2.02%
14	Browser Extension Install	120	1.65%
15	LSASS Process Access via Windows API	115	1.58%

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

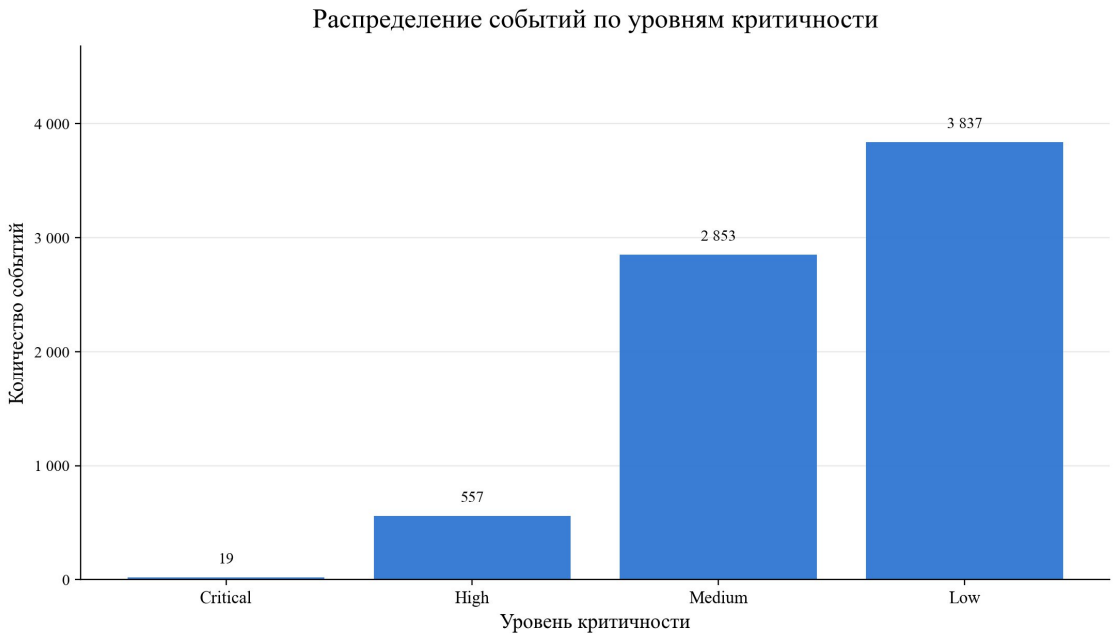


Рисунок 3. Распределение событий по уровням критичности

На рисунке показано распределение событий безопасности по уровням критичности: critical - 19, high - 557, medium - 2 853, low - 3 837. Суммарно по этим уровням отражено 7 266 событий. По горизонтальной оси указаны уровни критичности, по вертикальной - количество событий в каждой категории. Диаграмма используется как визуальная сводка структуры событий по severity и показывает, какие уровни сформировали основную часть зарегистрированной активности.

4.1. Статистика событий безопасности

В рамках мониторинга системы обнаружения и предотвращения угроз за отчётный период было зарегистрировано 7266 событий безопасности. Распределение по уровням критичности составило: critical - 19, high - 557, medium - 2853, low - 3837. Наиболее заметная активность наблюдалась по правилам First Time Seen Removable Device, Process Termination followed by Deletion, Potential Process Injection from Malicious Document, а также на узлах asst-pc-0011, fins-pc-0042, medu-pc-0077. Статусы кейсов за период: closed - 3, in-progress - 13, open - 2. Основной объем срабатываний пришелся на сценарии, связанные с контролем внешних носителей, попытками перебора привилегированных учетных записей и разведывательной активностью внутри операционной системы.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

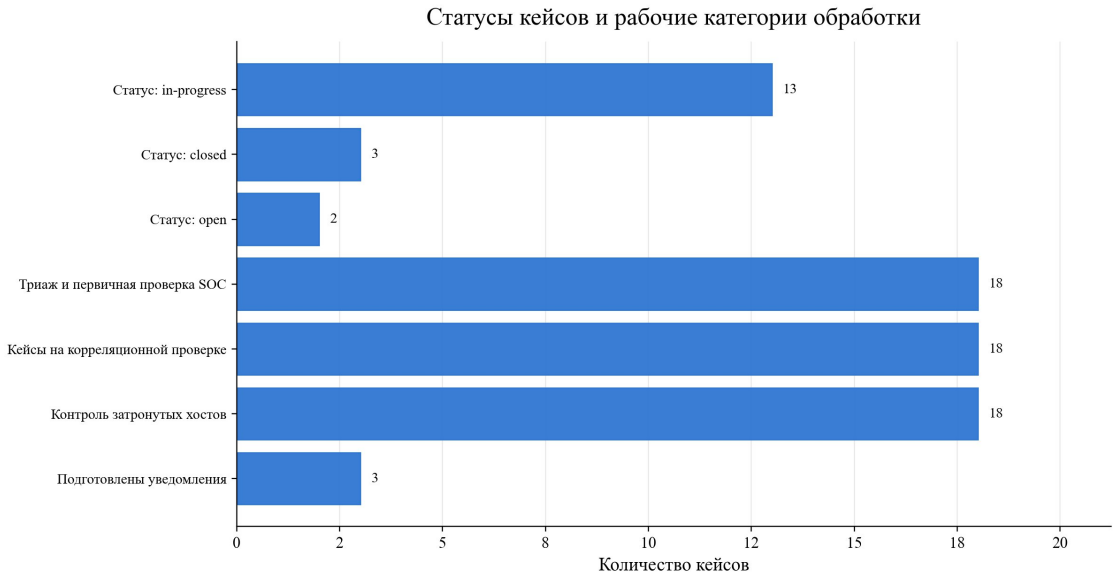


Рисунок 4. Статусы кейсов и уведомлений

На рисунке показано распределение кейсов и рабочих категорий обработки за отчетный период. Наиболее крупная категория на диаграмме: «Статус: in-progress» - 13. Общее количество кейсов в данных Elastic Cases составляет 18, количество направленных уведомлений - 3. Диаграмма объединяет фактические статусы кейсов и рабочие категории, использованные для отображения процесса обработки в отчете.

Строковая расшифровка раскрывает данные по кейсам и содержит 7 записей. В колонках указаны порядковый номер, статус или категория обработки, количество и текстовый комментарий. Строки со статусами отражают значения из Elastic Cases, а дополнительные рабочие категории показывают, как эти кейсы представлены в отчетном разделе. Таблица дополняет диаграмму тем, что фиксирует точные числа и пояснения к каждой категории.

Таблица 2. Статусы и категории обработки кейсов

№	Статус/категория	Количество	Комментарий
1	Статус: in-progress	13	Фактический статус из Elastic Cases.
2	Статус: closed	3	Фактический статус из Elastic Cases.
3	Статус: open	2	Фактический статус из Elastic Cases.

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z12026000019602BFD1E3

4	Триаж и первичная проверка SOC	18	Кейсы приняты в аналитическую обработку.
5	Кейсы на корреляционной проверке	18	Проверка связей с правилами корреляции и повторяющимися сценариями.
6	Контроль затронутых хостов	18	Сопоставление кейсов с endpoint- и host-телеметрией.
7	Подготовлены уведомления	3	Уведомления, направленные по результатам обработки.

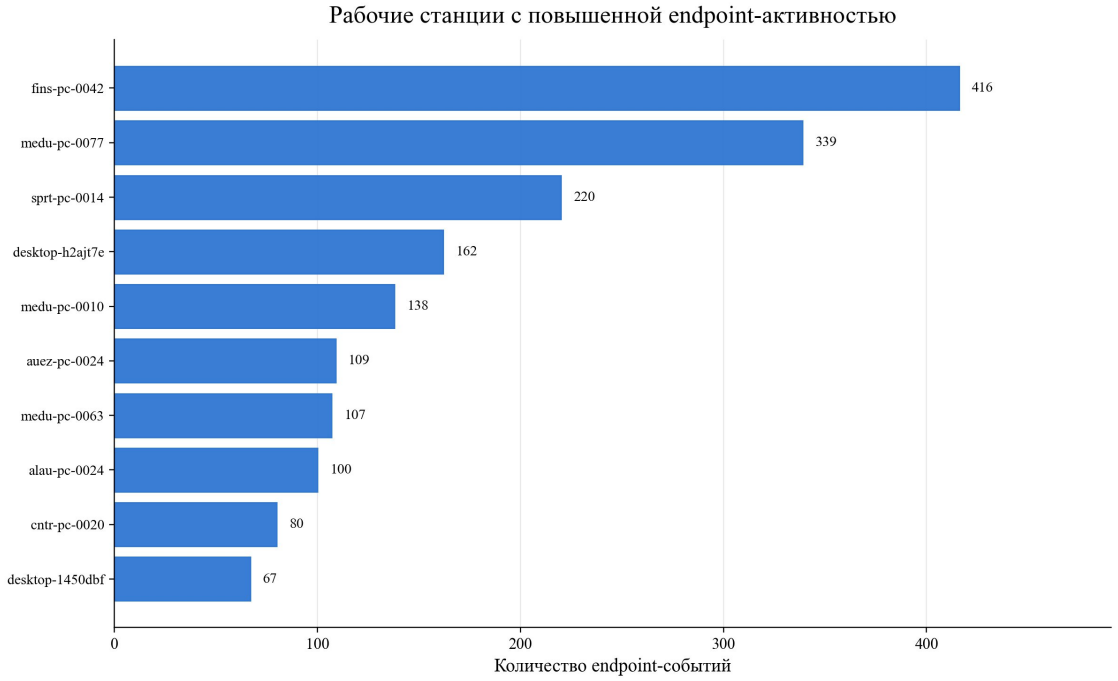


Рисунок 5. Рабочие станции с повышенной активностью

На рисунке показаны рабочие станции с наибольшим количеством endpoint-событий за отчетный период. Первое место в выборке занимает хост fins-pc-0042 с количеством событий 416. Каждая полоса соответствует отдельной рабочей станции, а ее длина отражает количество зафиксированных endpoint-событий. Рисунок отображает верхнюю часть выборки по хостам и

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

используется как визуальное дополнение к разделу обработки кейсов и активности конечных точек.

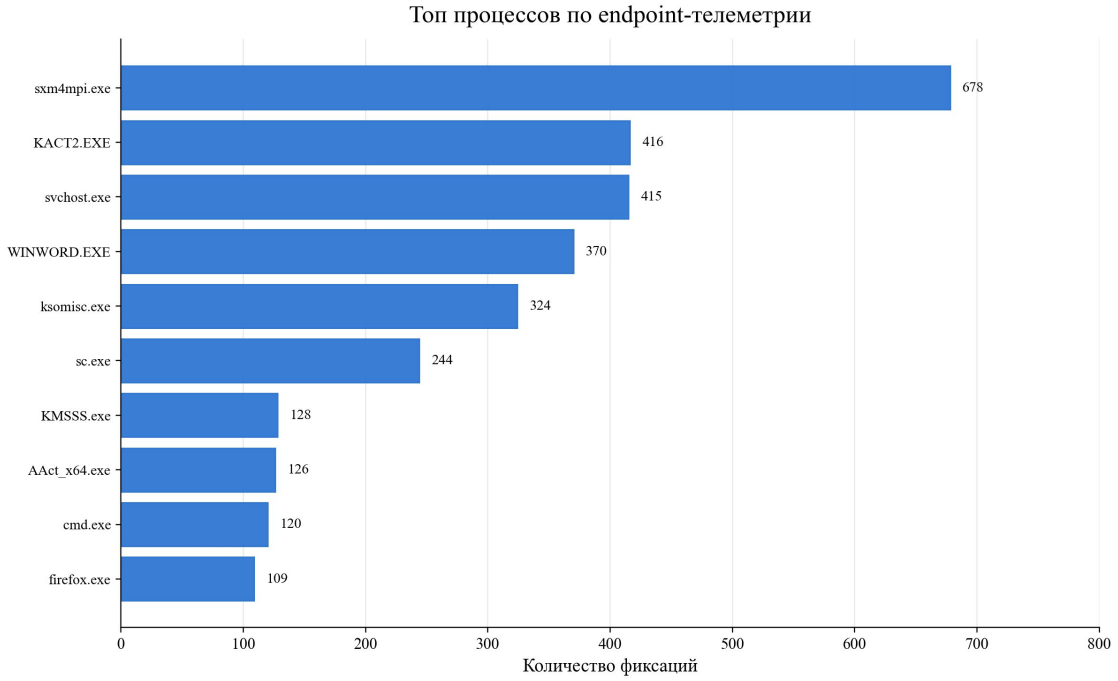


Рисунок 6. Топ процессов по endpoint-телеметрии

На рисунке показаны процессы, которые чаще всего встречались в endpoint-телеметрии за отчетный период. Верхняя строка диаграммы соответствует процессу sxm4mpi.exe с количеством фиксаций 678. По вертикальной оси перечислены имена процессов, по горизонтальной - количество фиксаций. Диаграмма показывает частотное распределение процессов и связана с таблицей ниже, где дополнительно приведено сравнение текущего и прошлого периодов.

Строковая детализация содержит процессы с изменением профиля активности относительно прошлого периода. В колонках указаны имя процесса, количество фиксаций в текущем периоде, значение прошлого периода, абсолютное изменение и комментарий из нормализованной выгрузки. Первая строка таблицы относится к процессу WINWORD.EXE. Таблица дополняет диаграмму процессов тем, что показывает не только текущую частоту, но и изменение относительно предыдущего отчетного периода.

Таблица 3. Процессы с изменением профиля активности

№	Процесс	Текущий период	Прошлый период	Δ	Комментарий
1	WINWORD.EXE	370	184	+186	рост активности относительно прошлого

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

					периода
2	rsDNSResolver.exe	108	7	+101	рост активности относительно прошлого периода
3	ksomisc.exe	324	272	+52	рост активности относительно прошлого периода
4	EXCEL.EXE	83	33	+50	рост активности относительно прошлого периода
5	upfc.exe	86	52	+34	рост активности относительно прошлого периода
6	KMSAuto++.exe	17	0	+17	новый или единичный в прошлом периоде
7	icarus.exe	30	15	+15	рост активности относительно прошлого периода
8	WhatsApp Installer (1).exe	13	2	+11	новый или единичный в прошлом периоде

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

9	whoami.exe	13	2	+11	новый или единичный в прошлом периоде
10	fver.exe	12	2	+10	новый или единичный в прошлом периоде
11	YandexDisk30Setup_x64.exe	10	0	+10	новый или единичный в прошлом периоде
12	NETSTAT.EXE	16	8	+8	рост активности относительно прошлого периода
13	KMSTools.exe	12	4	+8	рост активности относительно прошлого периода
14	setup.exe	10	3	+7	новый или единичный в прошлом периоде
15	HPScan.exe	24	18	+6	рост активности относительно прошлого периода

4.2. Система уведомлений

По событиям безопасности за отчётный период заведено и обработано 18 кейсов. Количество направленных уведомлений составило 15. Распределение кейсов по статусам: closed - 3, in-progress - 13, open - 2.

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

Дополнительно кейсы рассматривались через рабочие категории обработки: первичный триаж SOC, корреляционная проверка сработавших правил и контроль затронутых хостов по endpoint-телеметрии. Наиболее характерные заголовки кейсов: Svchost spawning Cmd | hpatchmonTask.cmd, arp -a | DrWeb, LightShot PUA | auez-0117. За отчетный период зарегистрировано 576 событий уровня high/critical; основной вклад внесло правило «First Time Seen Removable Device».

4.3 Поиск угроз

В рамках проактивного поиска угроз отдельные находки Threat Hunting по выделенному признаку не зафиксированы. При этом в отчётном периоде аналитическая обработка выполнялась на фоне 576 событий уровня high/critical с основной концентрацией по правилам First Time Seen Removable Device, Process Termination followed by Deletion, Potential Process Injection from Malicious Document. За отчетный период зарегистрировано 576 событий уровня high/critical; основной вклад внесло правило «First Time Seen Removable Device».

4.4. Доступность веб-интерфейса

В отчётном периоде веб-интерфейс SIEM функционировал в штатном режиме и оставался доступным для выполнения задач мониторинга, анализа событий и сопровождения кейсов. Существенных перебоев, препятствующих работе операторов и аналитиков, не зафиксировано. Доступность интерфейса позволяла своевременно просматривать корреляционные события, контролировать статус инцидентов и выполнять необходимые действия по сопровождению расследований. Работа с панелями, представлениями данных и карточками событий осуществлялась в обычном рабочем порядке на протяжении отчётного периода.

4.5. Автоматическое реагирование на угрозы

Средствами EDR за отчётный период заблокировано 63 вредоносных действий и 25 запусков подозрительных объектов. Дополнительно по телеметрии конечных точек выделены процессы с аномальным ростом активности относительно прошлого периода: WINWORD.EXE - 370 запусков за текущий период против 184 ранее (Δ +186); рост активности относительно прошлого периода rsDNSResolver.exe - 108 запусков за текущий период против 7 ранее (Δ +101); рост активности относительно прошлого периода ksomisc.exe - 324 запусков за текущий период против 272 ранее (Δ +52); рост активности относительно прошлого периода EXCEL.EXE - 83 запусков за текущий период против 33 ранее (Δ +50); рост активности относительно прошлого периода

По операционным сообщениям за май дополнительно выполнялись меры локализации и реагирования: изоляция или подготовка к изоляции хостов при недоступности агента, проверка и очистка зараженных рабочих

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

станций, перевод хостов на release/разблокировку после устранения угрозы, а также блокировка C2-адресов и доменов на уровне Check Point.

Ключевые действия реагирования по операционным сообщениям за период: 12.05.2026 на хосте gos1 выявлен MicrosoftHost.exe с признаками XMRig/CoinMiner; репутационная проверка показала 58/71 срабатываний, хост был изолирован для локализации угрозы; 18.05.2026 при повторной C2-активности по адресам 80.66.84.6:3333 и 91.184.248.11:8080 запрошена ручная изоляция хоста из-за недоступности Elastic Defend и блокировка адресов на Check Point; 19.05.2026 по хосту desktop-5bmr3bn обработана цепочка T-Lab/EDR: вредоносное вложение, AAct_x64.exe, DVDSetup.exe и подозрительные процессы; выполнены анализ, изоляция, очистка ПК и последующая разблокировка; 21.05.2026 по JETS-PC-0051 выявлен DriveMgr.exe с признаками крипто-клиппера, сетевого червя и Downloader, C2 185.215.113.93; рекомендованы остановка процесса, сброс и временная блокировка учетной записи, ограничение USB-носителей; 25-26.05.2026 по jets-pc-0051 и auez-pc-0109 обработаны повторные сценарии Phorpiex/DriveMgr.exe со съемных носителей; выданы рекомендации по удалению закрепления, очистке зараженных флеш-накопителей и проверке автозагрузки; 26-28.05.2026 по LightShot PUA и сетевым аномалиям выполнены проверки и блокировки на NGFW, включая домен prnt.sc и подтвержденную административную активность arp -a; 29.05.2026 по nauz-pc-0043 зафиксирован Malware Prevention Alert по Pyskpa/Chydo; вредоносные файлы помещены в карантин, рекомендованы полное внеплановое сканирование и проверка ключей автозагрузки; 29.05.2026 после очистки HEAL-PC-0060 выполнено действие на разблокировку; снятие изоляции ожидалось после выхода хоста online.

5.1 Инструментальное сканирование

Ежемесячно проводится комплексное инструментальное сканирование внутреннего и внешнего периметра сети. Работы выполняются в строгом соответствии с технической спецификацией Акимата города Алматы и включают анализ на наличие уязвимостей, отклонений в конфигурациях и потенциальных точек компрометации. По результатам текущего цикла во внутреннем периметре выявлено Critical - 42, High - 165, Medium - 652; во внешнем периметре выявлено Critical - 0, High - 0, Medium - 0. Наибольшая событийная активность зафиксирована в подразделениях Упр. Гор. Планир. и урбан., Упр. Предприн. и инвестиций, Упр. финансов, Упр. градостроительного контроля.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

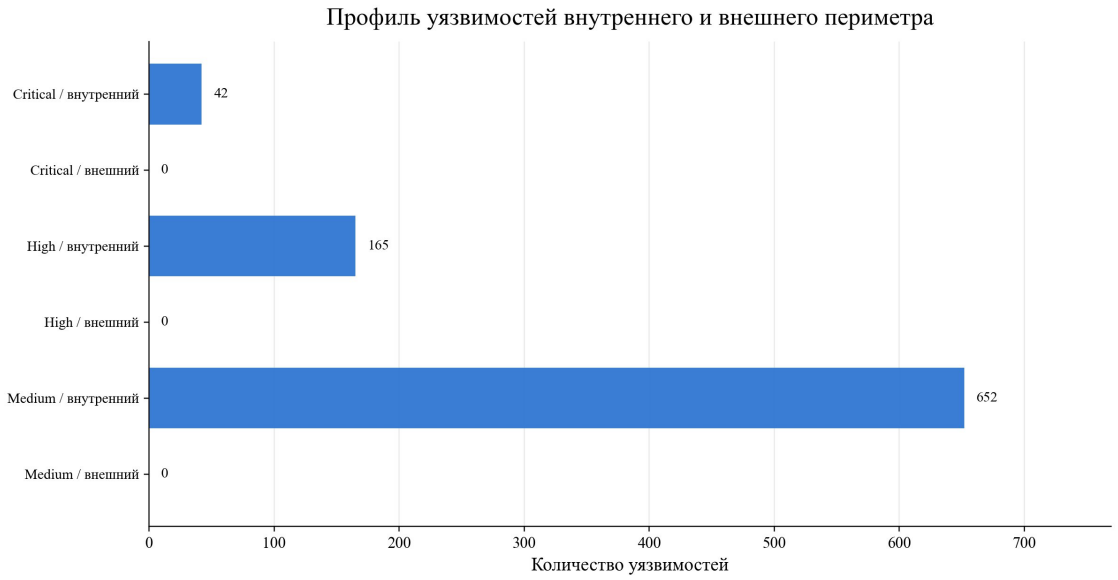


Рисунок 7. Профиль уязвимостей внутреннего и внешнего периметра

Таблица 5. Сканирование сети

№	Подразделение (объект сканирования)	Critical	High	Medium
1	Упр. Гор. Планир. и урбан.	7	8	27
2	Упр. Предприн. и инвестиций	4	42	118
3	Упр. финансов	4	7	16
4	Упр. градостроительного контроля	4	1	22
5	Аппарат Акима	3	4	9
6	Аппарат Ауэзовского района	2	17	62
7	Упр. туризма	2	9	38
8	Упр. энергетики 1	2	9	17
9	Упр. молодежной политики	2	8	16

DOC ID KZBW2Z12026000019602BFD1E3
DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

10	Упр. экологии	2	7	9

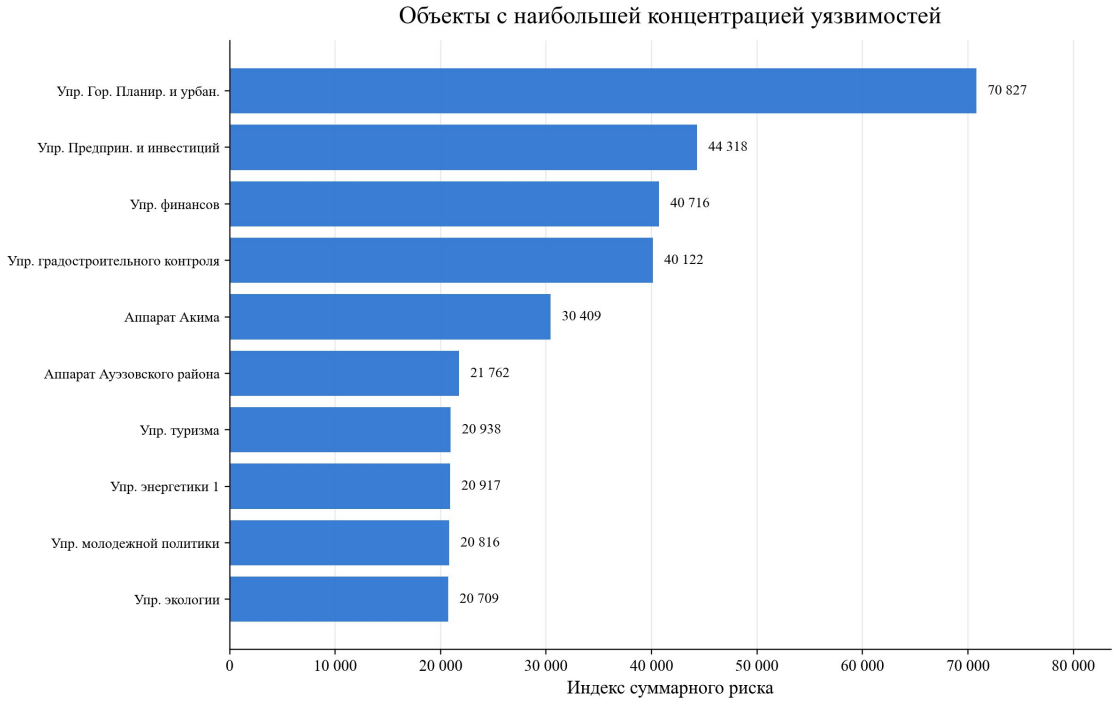


Рисунок 8. Объекты с наибольшей концентрацией уязвимостей

Примечание: Подробная информация по сканированиям сети указана в Приложениях 4, 5 и 6.

5.2 Статистика управления уязвимости

Сравнение результатов текущего и предыдущего запусков сканирования отражает динамику уязвимостей по уровням Critical, High и Medium. Последний учитываемый запуск завершен 2026-05-27T08:19:47Z, предыдущий - 2026-05-19T12:12:31Z. Изменение профиля рисков составило: ΔCritical = +40, ΔHigh = +160, ΔMedium = +640. Новых критических уязвимостей зарегистрировано 40, устранено 0.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

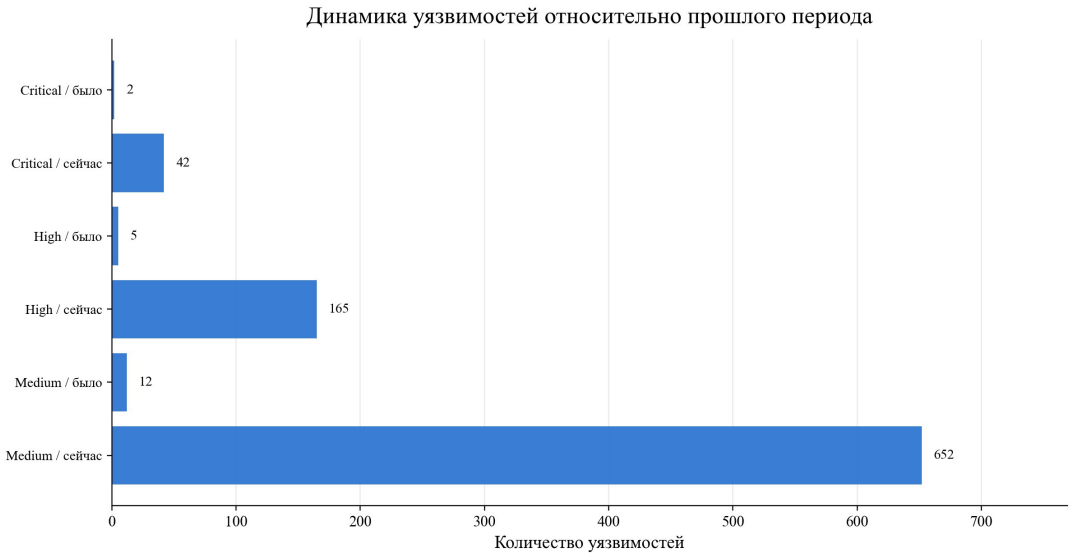


Рисунок 9. Динамика уязвимостей относительно прошлого периода

Таблица 6. Статистика управления уязвимостями

Скан	**СЕЙЧАС К/В/С**	**БЫЛО К/В/С**	**ΔК/ΔВ/ΔС**	**Новые**	**Устранены**	**Без изм.**	**Крит.↑**	**Крит.↓**	**ΔХостов**
Упр. Гор. Планир. и урбан.	7/8/27	0/0/0	+7/+8/+27	2 577	0	0	7	0	+251
Упр. Предприн. и инвестиций	4/42/118	0/0/0	+4/+42/+118	2 589	0	0	4	0	+215
Упр. финансов	4/7/16	0/0/0	+4/+7/+16	955	0	0	4	0	+256
Упр. градостроительного контроля	4/1/22	0/0/0	+4/+1/+22	1 545	0	0	4	0	+132
Аппарат Акима	3/4/9	0/0/0	+3/+4/+9	1 399	0	0	3	0	+256
Аппарат Ауэзовского района	2/17/62	0/0/0	+2/+17/+62	1 058	0	0	2	0	+35

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

Упр. туризма	2/9/38	0/0/0	+2/+9/+38	2 674	0	0	2	0	+256
Упр. энергетики 1	2/9/17	0/0/0	+2/+9/+17	478	0	0	2	0	+256
Упр. молодежной политики	2/8/16	0/0/0	+2/+8/+16	402	0	0	2	0	+256
Упр. экологии	2/7/9	0/0/0	+2/+7/+9	502	0	0	2	0	+256

Примечание: Подробная таблица по статистике управления уязвимостями приведена в Приложении 4.

6.1. OpenCTI — Платформа киберразведки

Для обеспечения проактивного подхода к выявлению и предотвращению киберугроз в инфраструктуре Заказчика используется платформа анализа угроз OpenCTI (Open Cyber Threat Intelligence Platform), развернутая по адресу 172.16.16.78:8080. Данное решение обеспечивает централизованное хранение, корреляцию и визуализацию данных об угрозах, включая:

- индикаторы компрометации (IoC);
- тактики, техники и процедуры атак в соответствии с фреймворком MITRE ATT&CK;
- информацию о киберпреступных группировках, вредоносных кампаниях и используемых инструментах.

По результатам текущего анализа и расследования инцидентов выявленные индикаторы компрометации (IP-адреса, хэши файлов, домены, URL, имена процессов и иные артефакты) были проанализированы и добавлены в базу OpenCTI, что обеспечивает их последующее использование при корреляции событий, threat hunting и автоматизированном выявлении схожих угроз в инфраструктуре.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

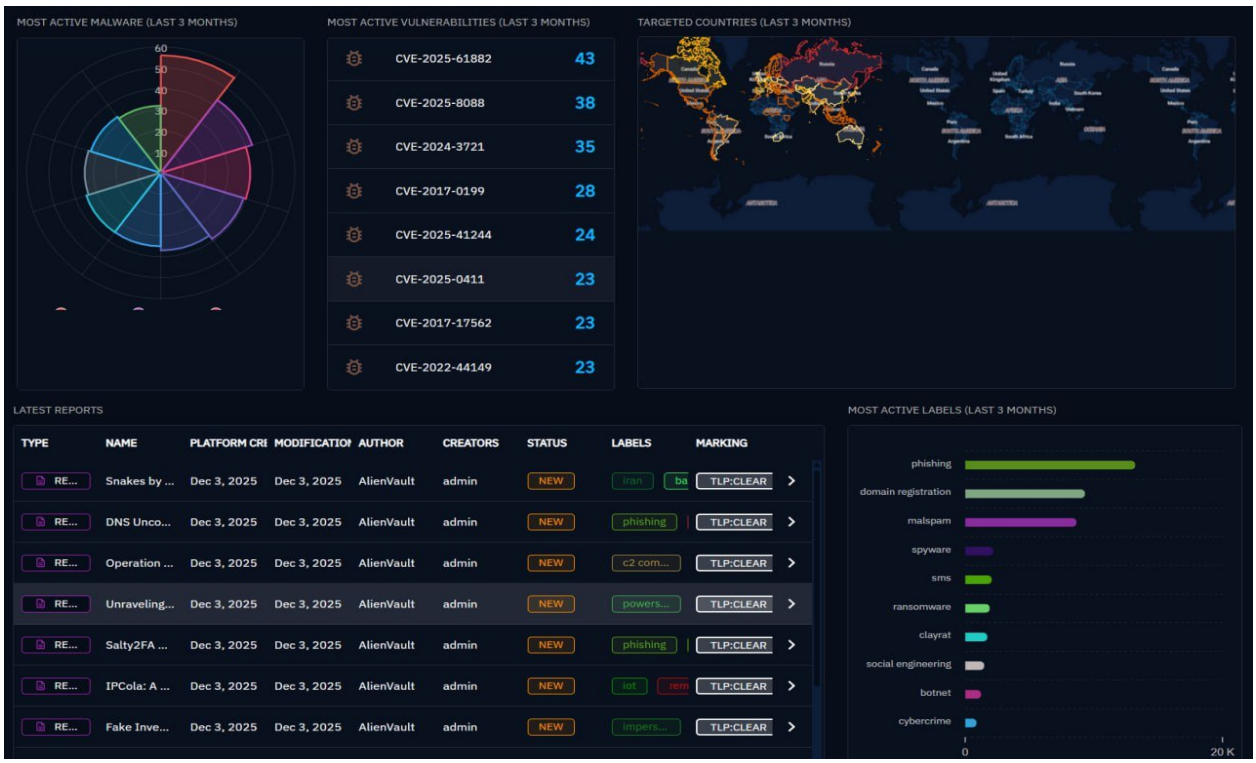


Рисунок 10. Информация с OpenCTI

Актуализация базы IoC в OpenCTI позволяет повысить эффективность мониторинга, сократить время реагирования на повторяющиеся и схожие атаки, а также обеспечивает накопление аналитической базы для последующего прогнозирования и предотвращения потенциальных киберугроз.

6.2. MISP — Обмен индикаторами компрометации

На стороне Поставщика функционирует и поддерживается платформа MISP, посредством которой осуществляется обмен индикаторами компрометации с АО «ГТС». Поставщиком осуществляется постоянный мониторинг и отработка поступающих запросов в рамках действующих процедур реагирования. Все обращения, поступающие через MISP, анализируются на предмет наличия вредоносной активности, проводится проверка источников угроз в соответствии с пунктом 1.1.27 технической спецификации.

За отчетный период угроз информационной безопасности не выявлено.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

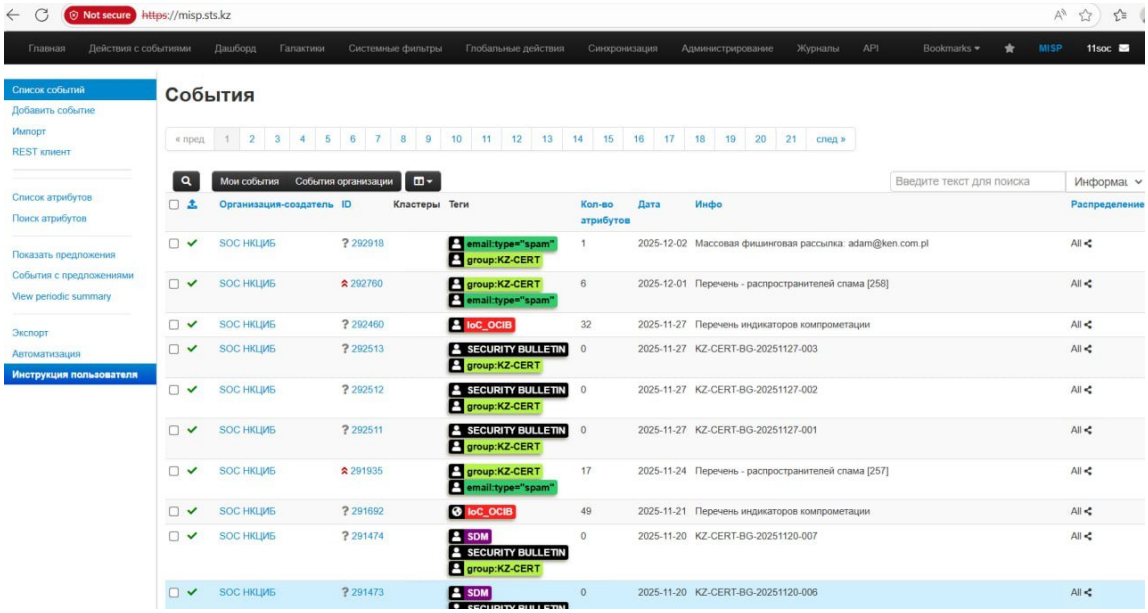


Рисунок 11. MISP

6.3. T-Lab Sandbox — Защита от таргетированных атак

Поставщиком реализованы меры защиты от таргетированных кибератак и угроз нулевого дня с использованием системы динамического и статического анализа T-Lab Sandbox, интегрированной с SIEM и EDR для централизованного мониторинга и реагирования. В отчётном периоде система анализа угроз в режиме реального времени выявила 153 угроз и 344 подозрительных объектов, при общем количестве 9266 проверенных файлов/объектов. Активность носила равномерный характер в течение месяца. Основную долю проверяемых объектов составили текстовые файлы и исполняемые файлы. В выборку отчетного периода вошло 64 отчетов T-Lab; максимальная оценка риска по статистике платформы составила 128.32, сформировано 21 SHA-256 IOC. По результатам анализа все выявленные угрозы были обработаны средствами защиты, признаки массового заражения или распространения вредоносного программного обеспечения не зафиксировано. Дополнительно выполнялась сверка результатов sandbox-анализа с SIEM/EDR для уточнения повторяющихся сценариев и приоритизации вредоносных объектов.

Сводный блок показателей фиксирует общий объем работы T-Lab за отчетный период: количество проверенных объектов - 9 266, из них 153 классифицированы как вредоносные, 344 отнесены к подозрительным, а 8 769 не имели признаков вредоносной активности. Доля вредоносных объектов составила 1.65%, доля подозрительных - 3.71%. В таблице отдельно выделены количество отчетов T-Lab, число сформированных IOC и максимальная оценка риска, что позволяет видеть одновременно объем проверок и количество технических индикаторов, сформированных по результатам анализа. Значения в таблице описывают итоговую сводку за месяц и не заменяют карточки отдельных объектов: они показывают агрегированный результат работы sandbox-контура за отчетный период. Такой формат удобен

DOC ID KZBW2Z12026000019602BFD1E3
DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

для сопоставления общего числа проверок, количества подозрительных результатов и числа IOC в одном месте без детализации по каждому отдельному файлу.

Таблица 6. Сводные показатели T-Lab Sandbox

Показатель	Значение	Комментарий
Проверено объектов	9 266	Общее количество объектов, прошедших проверку в T-Lab.
Вредоносные объекты	153	Объекты, классифицированные как вредоносные.
Подозрительные объекты	344	Объекты с подозрительным verdict в выгрузке T-Lab.
Отчетов T-Lab в периоде	64	Количество отчетов, попавших в отчетный период.
IOC SHA-256	21	Количество сформированных индикаторов компрометации.
Максимальный риск/score	128	Максимальная оценка риска по статистике T-Lab.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

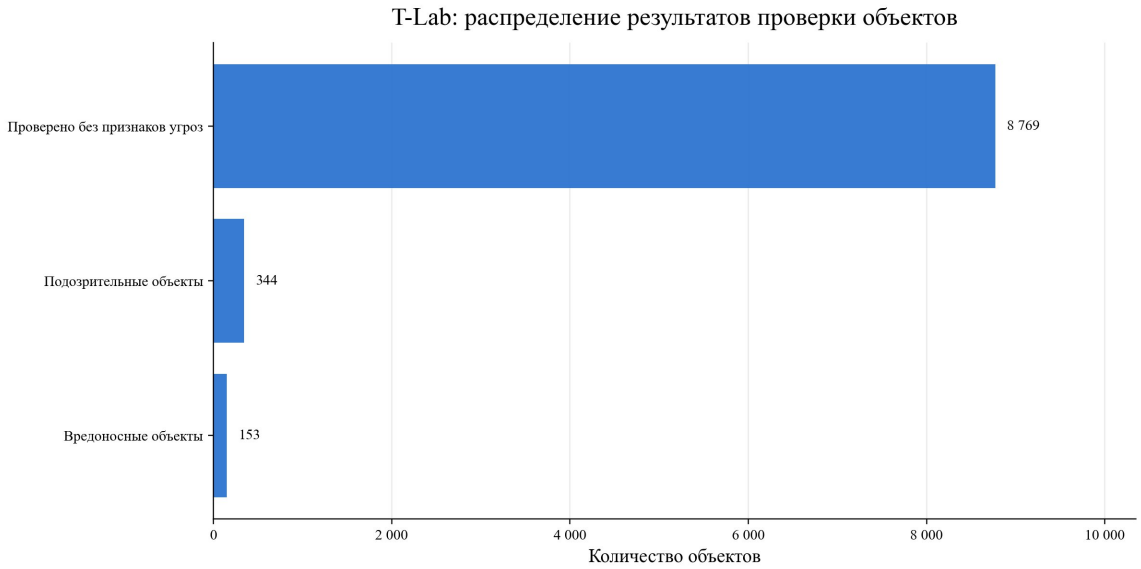


Рисунок 12. Распределение результатов проверки T-Lab

На диаграмме распределения результатов проверки показано, как общий поток из 9 266 объектов разделился по итоговым verdict-статусам T-Lab. Безопасная часть выборки составила 8 769 объектов, вредоносная - 153, подозрительная - 344. На рисунке визуально отделены объекты без признаков вредоносности от объектов, получивших вредоносный или подозрительный verdict. Размер каждого сегмента соответствует количеству объектов в соответствующей категории, поэтому по диаграмме видно соотношение основной безопасной массы и меньших групп с повышенным уровнем риска. Текстовое описание рядом с диаграммой фиксирует эти же значения числами, чтобы результат был понятен без обращения к исходной выгрузке T-Lab.

Рисунок 13. Динамика анализа объектов T-Lab по дням

На графике динамики по дням показано, как распределялась активность T-Lab внутри отчетного месяца. В исходной статистике использовано 149 временных интервалов, из которых 141 содержали фактические отчеты,

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

поэтому график отражает не единичную выгрузку, а поведение системы во времени. По горизонтальной оси отображены даты периода, по вертикальной оси - количество отчетов или объектов, пришедших на анализ в соответствующий день. Участки с более высокими значениями показывают дни, когда в T-Lab поступало больше объектов, а участки с низкими значениями отражают периоды меньшей активности. График используется как временная расшифровка месячной сводки: он показывает, распределялись ли проверки равномерно или были сконцентрированы в отдельные даты.

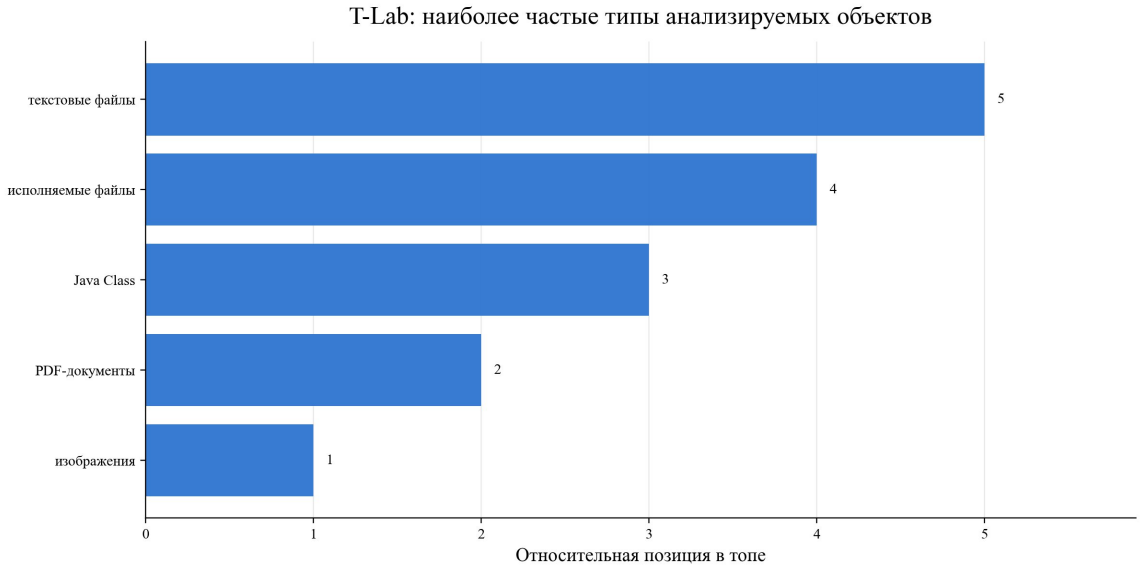


Рисунок 14. Наиболее частые типы анализируемых объектов T-Lab

На диаграмме типов объектов показано, какие форматы файлов чаще всего поступали в T-Lab на динамический или статический анализ. В текущем периоде среди наиболее частых типов указаны: текстовые файлы, исполняемые файлы, Java Class, PDF-документы, изображения. Каждая полоса диаграммы соответствует отдельному типу объекта, а ее длина отражает относительное место этого типа в выборке. Рисунок показывает структуру анализируемого потока файлов без детализации по конкретным пользователям или источникам поступления. По этой диаграмме видно, какие форматы составляют основную часть материалов, обработанных T-Lab за отчетный период.

В табличной расшифровке типы объектов представлены в ранжированном виде, что удобно для последующей сверки с источниками поступления файлов и правилами обработки вложений. В первой колонке указан порядковый номер, во второй - тип объекта из нормализованной выгрузки T-Lab. Таблица повторяет содержательный смысл диаграммы, но представляет данные в текстовом виде, чтобы перечень форматов можно было прочитать без визуальной оценки длины полос. Такой формат фиксирует состав наиболее часто встречавшихся типов объектов за месяц и сохраняет его в отчете как отдельный структурированный блок.

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

Таблица 7. Наиболее частые типы анализируемых объектов T-Lab

№	Тип объекта
1	текстовые файлы
2	исполняемые файлы
3	Java Class
4	PDF-документы
5	изображения

Блок IOC содержит первые 10 SHA-256 индикаторов из 21 сформированных значений. Каждая строка таблицы представляет конкретный файловый хэш, полученный из результатов T-Lab. В первой колонке указан порядковый номер, во второй - тип индикатора, в третьей - само значение SHA-256. Таблица показывает технические индикаторы в текстовом виде и дополняет диаграммы, где отражены только агрегированные показатели по verdict-статусам, датам и типам файлов.

Таблица 8. IOC

№	Тип индикатора	Значение
1	File Hash (SHA-256)	04fbdd69924e98f46050fa77634469a3bbeffa6a8dcc0d812c62f8be9fc20aec
2	File Hash (SHA-256)	4dd9218142eef2097fa6fa2d53f69004ae1c4369e6665ce446c06496c22e5262
3	File Hash (SHA-256)	0afa4d2e6fb52cad3d4d8ed143a8b2716e9a48783c152f30ae7545e383e6fee6
4	File Hash (SHA-256)	49404f7268aa29200ed637adf43d4ca8ba83ab19be8c9d59e3b80dbc7340ba1f
5	File Hash (SHA-256)	3bcf40afbd782e814877fa22f148d343eb91f36f9842021ca3ad0fae2c74dca9

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

6	File Hash (SHA-256)	178df9fb56a11092d2dbe1936f2a366c31f91acacd2719e5172cfcb839370ce1
7	File Hash (SHA-256)	89ec2d2f9c5ccc66d1090e2b5e2df272e558db7361ab686d4d27c8648b1aa855
8	File Hash (SHA-256)	18444c3b459f6a2bf9b48463a213d4807cef573a32dcadddc408b3deb7c13dd6
9	File Hash (SHA-256)	a56d6a1fab56b787093ad771f8033acbe4fe9ac22163c429f9948526794d0b91
10	File Hash (SHA-256)	7207cbaa7b66bbf090eb45efcc55031ba9ff13ba1b6c654d273701ec85891da8

Примечание: Смотреть подробный отчет T-Lab в Приложении 7

6.4. DLP – Предотвращение утечек данных (safetica)

В ходе анализа телеметрии, поступающей с рабочих станций в систему предотвращения утечек данных Safetica, за отчётный период зафиксировано 206 774 событий контроля операций с данными. Диапазон наблюдения по выгрузке: 01.05.2026-31.05.2026. Наиболее активные пользователи: Аппарат Акима@ACER_WIN11_9, ПК@DESKTOP-P3IF86U, Ayazhan Bopan, Bekezhan Almyrza, Алма@DESKTOP-2VM9KM5. Основные приложения: Google Chrome (chrome.exe), Проводник (explorer.exe), Microsoft Word (WINWORD.EXE), Firefox (firefox.exe), Microsoft Excel (EXCEL.EXE). Совокупный объем передачи данных составил 638,9 ГБ; отдельно выделены веб-риски, операции передачи данных и служебная активность приложений. По признаку важности в выгрузке 206 774 событий отнесены к категории без установленного риска; объекты среднего и высокого приоритета в разделе рассматриваются как кандидаты на ручную проверку, а не как подтвержденные факты утечки. Основная веб-активность пришлась на ресурсы web.whatsapp.com, almaty.qujat.gov.kz, eotinish.gov.kz. Наибольший объем передачи данных сформирован приложением Проводник (explorer.exe). Объекты среднего и высокого приоритета вынесены в отдельную таблицу для дополнительной проверки DLP-политик. Подробная выгрузка Safetica приведена в Приложении 8.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

6.4.1. Анализ веб – активности

В отчётном периоде по направлению веб-активности выделено 20 объектов среднего и высокого приоритета для дополнительной проверки. Преобладающие категории веб-ресурсов: Не установлено, Бизнес, ИТ, Досуг, Наука и образование. Наибольшая активность наблюдалась по ресурсам web.whatsapp.com, almaty.qujat.gov.kz, eotinish.gov.kz, 10.61.140.66, youtube.com. В перечень объектов, требующих дополнительной проверки, вошли веб-ресурсы almaty.qujat.gov.kz, eotinish.gov.kz, chatgpt.com и приложения Solitaire.exe, dota2.exe, cs2.exe, Half-Life Launcher (hl.exe), AnyDesk (AnyDesk.exe). Отдельного внимания требуют категории инструментов ИИ, мессенджеров, игровых приложений и средств удаленного доступа: часть такой активности может быть рабочей, но для DLP-контроля она должна быть сопоставлена с должностными задачами пользователя и разрешенными бизнес-сценариями. Такая детализация используется для разграничения штатной веб-активности, облачных сервисов и ресурсов с повышенным DLP-риск-профилем.

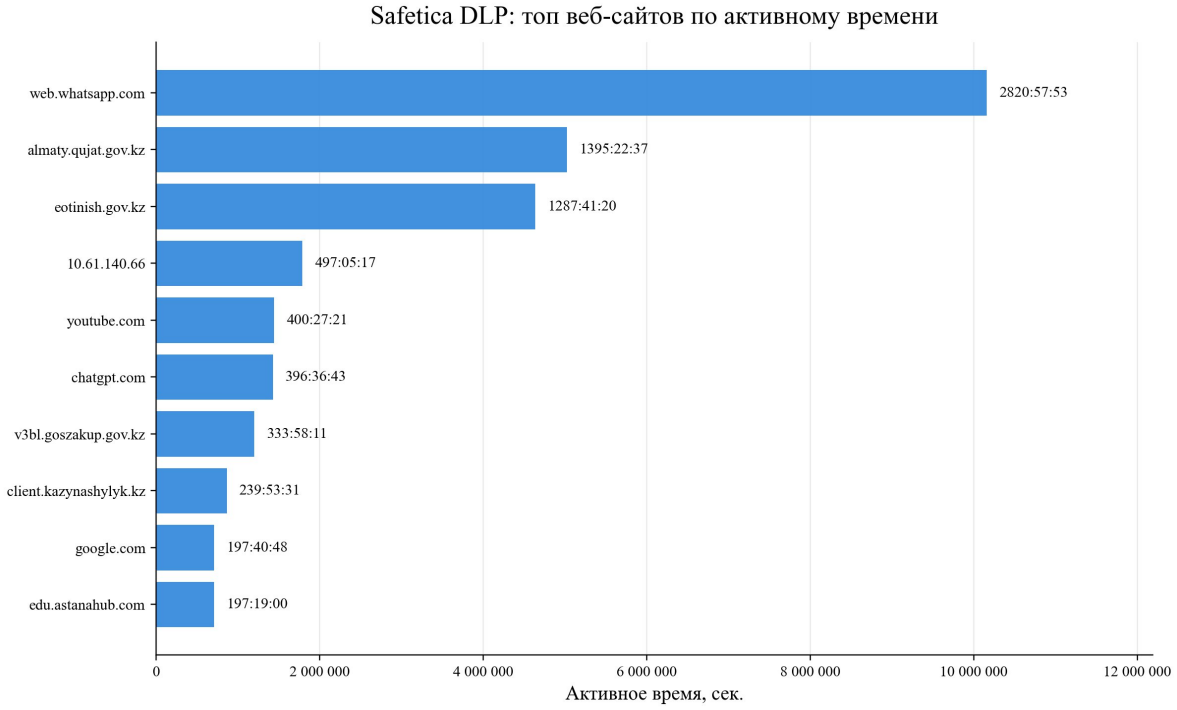


Рисунок 15. Веб-сайты

На диаграмме веб-активности показаны ресурсы, на которых пользователи провели наибольшее суммарное активное время в течение отчетного периода. Лидирующий ресурс: web.whatsapp.com с активным временем 2820:57:53 и охватом 318 пользователей. Также в верхней части выборки представлены almaty.qujat.gov.kz и eotinish.gov.kz, что позволяет увидеть не только единичный максимум, но и общий профиль наиболее используемых веб-направлений. Длина полосы отражает суммарное активное время по ресурсу, а подписи рядом с элементами диаграммы показывают конкретные значения времени. Рисунок отображает верхнюю часть выборки

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business
DOC ID KZBW2Z12026000019602BFD1E3

Safetica по веб-активности и не включает все посещенные ресурсы за месяц. Данные на рисунке связаны с таблицей ниже: диаграмма дает визуальное сравнение, а таблица раскрывает категории и количество пользователей по тем же объектам.

В числовой расшифровке веб-ресурсы представлены в виде рабочего перечня для анализа: указаны название ресурса, категория, суммарное активное время и количество пользователей. Категория помогает понять функциональный тип ресурса, активное время показывает интенсивность использования, а количество пользователей позволяет отличать массовую активность от индивидуальных отклонений. Порядок строк соответствует убыванию активности: в верхней части находятся ресурсы с наибольшим активным временем. В отличие от диаграммы, таблица содержит не только название ресурса и время, но и дополнительный контекст по категории и охвату пользователей. Такая структура показывает, какие веб-ресурсы сформировали основную часть наблюдаемой веб-активности в Safetica за отчетный период.

Таблица 9. Топ веб-ресурсов по активному времени пользователей

№	Веб-ресурс	Категория	Активное время	Пользователи
1	web.whatsapp.com	Веб-приложения для мгновенных сообщений	2820:57:53	318
2	almaty.qujat.gov.kz	Веб-порталы	1395:22:37	170
3	eotinish.gov.kz	Веб-порталы	1287:41:20	138
4	10.61.140.66	Внутренняя сеть	497:05:17	77
5	youtube.com	Досуг	400:27:21	181
6	chatgpt.com	Инструменты ИИ	396:36:43	251
7	v3bl.goszakup.gov.kz	Правительство, закон и религия	333:58:11	74
8	client.kazynashylyk.kz	Не установлено	239:53:31	27

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

9	google.com	Поисковые системы	197:40:48	311
10	edu.astanahub.com	Бизнес	197:19:00	162

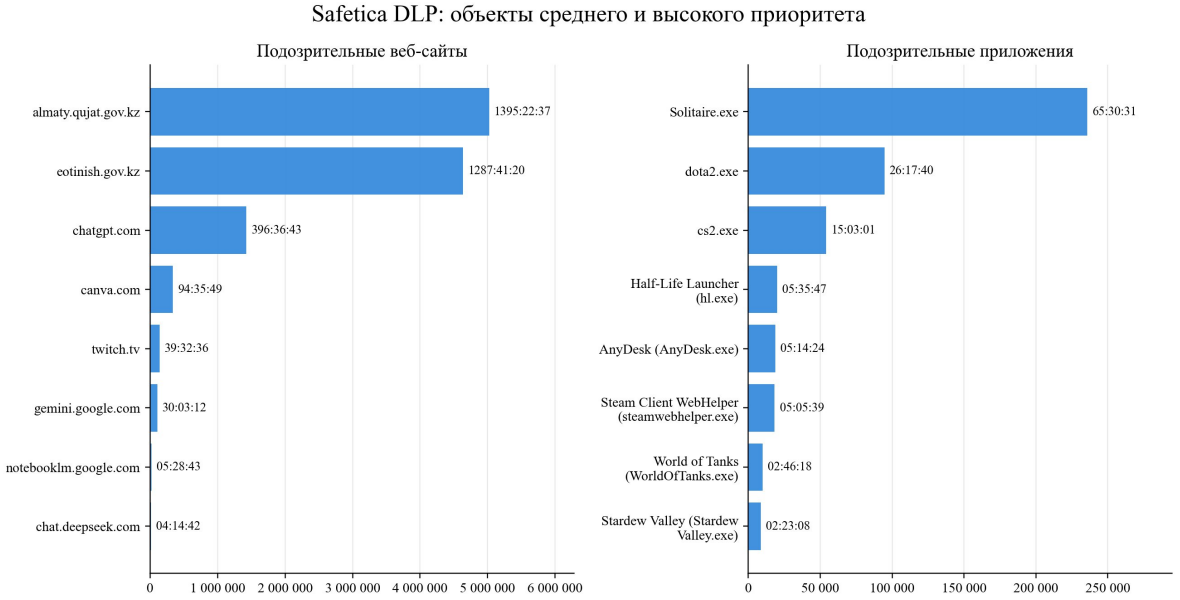


Рисунок 16. Объекты Safetica средней и высокой степени важности

На диаграмме средней и высокой степени важности объединены веб-сайты и приложения, которые Safetica отнесла к соответствующим категориям в выгрузке. Наиболее заметные объекты в текущей выборке: веб-ресурс almaty.qujat.gov.kz и приложение Solitaire.exe. В левой части рисунка представлены подозрительные веб-сайты, в правой части - подозрительные приложения. Для каждого объекта отображается активное время, а также дополнительная информация о категории и количестве пользователей, если она присутствует в выгрузке. Диаграмма показывает верхнюю часть списка объектов средней и высокой степени важности и используется в отчете как визуальная сводка по наиболее заметным элементам этого раздела.

В перечне объектов средней и высокой степени важности данные разделены по типу объекта: отдельно отражаются веб-сайты и приложения. Для каждого объекта указаны категория, активное время и количество пользователей, поэтому таблица позволяет понять не только факт попадания в риск-зону, но и масштаб распространения активности. Колонка 'Тип' показывает, относится ли строка к веб-сайту или приложению, колонка 'Объект' содержит имя сайта или процесса, а последующие колонки раскрывают категорию, активное время и охват пользователей. Таблица дополняет диаграмму выше тем, что сохраняет значения в структурированном виде и позволяет видеть все отобранные объекты в одном списке. Содержание таблицы соответствует данным Safetica за отчетный период и не является перечнем всех событий DLP.

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

Таблица 10. Объекты Safetica среднего и высокого приоритета

№	Тип	Объект	Категория	Активное время	Пользователи
1	Веб-сайт	almaty.qujat.gov.kz	Веб-порталы	1395:22:37	170
2	Веб-сайт	eotinish.gov.kz	Веб-порталы	1287:41:20	138
3	Веб-сайт	chatgpt.com	Инструменты ИИ	396:36:43	251
4	Веб-сайт	canva.com	Инструменты ИИ	94:35:49	23
5	Веб-сайт	twitch.tv	Финансовый	39:32:36	2
6	Веб-сайт	gemini.google.com	Инструменты ИИ	30:03:12	38
7	Веб-сайт	notebooklm.google.com	Инструменты ИИ	05:28:43	2
8	Веб-сайт	chat.deepseek.com	Инструменты ИИ	04:14:42	6
9	Приложение	Solitaire.exe	Игры	65:30:31	9
10	Приложение	dota2.exe	Игры	26:17:40	2
11	Приложение	cs2.exe	Кейлоггер	15:03:01	3
12	Приложение	Half-Life Launcher (hl.exe)	Игры	05:35:47	11
13	Приложение	AnyDesk (AnyDesk.exe)	VPN клиент	05:14:24	28
14	Приложение	Steam Client WebHelper (steamwebhelper.exe	Игры	05:05:39	11

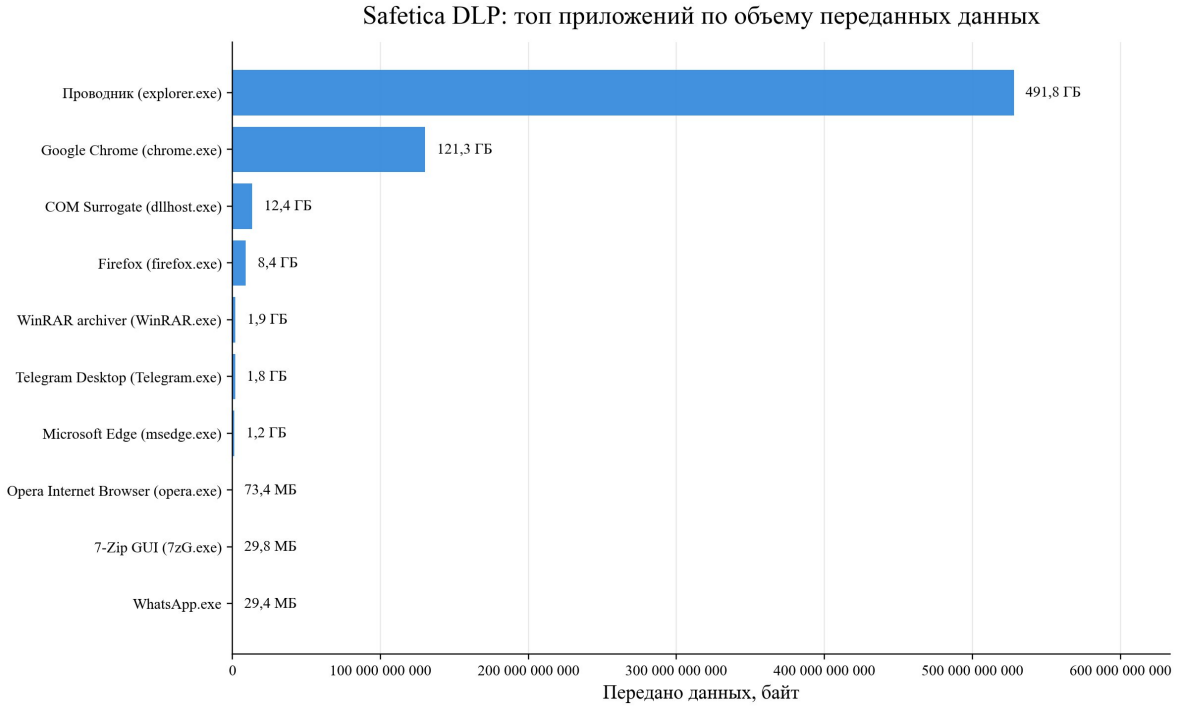
DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

		)			
15	Приложение	World of Tanks (WorldOfTanks.exe)	Игры	02:46:18	1
16	Приложение	Stardew Valley (Stardew Valley.exe)	Игры	02:23:08	1

6.4.2. Передачи данных

Диаграмма «Топ-10 приложений по объёму переданных данных» отражает распределение сетевого трафика между наиболее активно используемыми пользовательскими и системными приложениями за отчётный период. Всего по операциям передачи данных зафиксировано 324 538 событий контроля; основные каналы: Копировать, Печать, Переместить, Веб-загрузка, Отправлено через мессенджеры. Наибольший объём трафика сформирован процессом Проводник (explorer.exe) (≈491,8 ГБ), что обусловлено активной работой пользователей с файловой системой и сетевыми ресурсами. Существенную долю также занимают веб-браузеры (Google Chrome (chrome.exe), Firefox (firefox.exe) и Microsoft Edge (msedge.exe)). Использование системных и прикладных процессов (COM Surrogate (dllhost.exe) и WinRAR archiver (WinRAR.exe)) связано с обработкой и передачей документов. Высокий объем операций через Проводник и браузеры сам по себе не является инцидентом, но формирует приоритет для проверки правил копирования, печати, веб-загрузки и передачи через мессенджеры. Распределение используется для проверки DLP-политик, исключений и рабочих сценариев передачи данных; окончательная оценка допустимости операций выполняется по владельцам процессов и назначению данных.



DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

Рисунок 17. Топ-10 приложений

На диаграмме передачи данных показаны приложения, сформировавшие основной объем операций с данными в отчетном периоде. Лидирующее приложение: Проводник (explorer.exe) с объемом 491,8 ГБ; далее в верхней части выборки находятся Google Chrome (chrome.exe) и COM Surrogate (dllhost.exe). По горизонтальной оси отражен объем переданных данных, а по вертикальной - приложения из верхней части выборки. Длина полосы показывает относительный вклад приложения в общий объем передачи среди отображенных объектов. Рисунок описывает распределение объема по приложениям и связан с таблицей ниже, где для тех же приложений дополнительно указаны категория, средний объем в активный день и количество пользователей.

В детализации передачи данных диаграмма раскрывается до уровня конкретных приложений: по каждой строке указаны категория, общий объем передачи, средний объем в активный день и количество пользователей. Совокупный объем передачи за период составил 638,9 ГБ, поэтому таблица используется как основа для оценки того, какие процессы реально формируют основную нагрузку на DLP. Общий объем показывает суммарный размер операций за месяц, средний объем в активный день показывает усредненное значение только по дням активности, а количество пользователей показывает охват приложения. Таблица содержит числовую расшифровку диаграммы и позволяет видеть не только порядок приложений по объему, но и дополнительные поля, отсутствующие на рисунке. Все значения приведены в агрегированном виде по отчетному периоду.

Таблица 11. Распределение объема переданных данных по основным пользовательским и системным приложениям

№	Приложение	Категория	Объем переданных данных (итого)	Средний объем в активный день	Пользователи
1	Проводник (explorer.exe)	Windows	491,8 ГБ	15,9 ГБ	313
2	Google Chrome (chrome.exe)	Веб-браузер	121,3 ГБ	3,9 ГБ	302
3	COM Surrogate	Не указано	12,4 ГБ	409,5 МБ	39

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

	(dllhost.exe)				
4	Firefox (firefox.exe)	Веб-браузер	8,4 ГБ	276,7 МБ	77
5	WinRAR archiver (WinRAR.exe)	Не указано	1,9 ГБ	62,7 МБ	14
6	Telegram Desktop (Telegram.exe)	Не указано	1,8 ГБ	58,5 МБ	1
7	Microsoft Edge (msedge.exe)	Веб-браузер	1,2 ГБ	40,6 МБ	73
8	Opera Internet Browser (opera.exe)	Не указано	73,4 МБ	2,4 МБ	4
9	7-Zip GUI (7zG.exe)	Не указано	29,8 МБ	985,4 КБ	1
1 0	WhatsApp.exe	Мгновенны е сообщения и интернет-телефония (VOIP)	29,4 МБ	970,7 КБ	6

6.4.3. Служебные операции через интернет и внутренние сервисы

По служебным операциям и активности приложений в поведенческую выборку Safetica включено 78 пользователей. Наибольшая активность отмечалась в приложениях Google Chrome (chrome.exe), Проводник (explorer.exe), Microsoft Word (WINWORD.EXE), Firefox (firefox.exe), Microsoft Excel (EXCEL.EXE). Максимальное активное время пользователя за период: DeLux@Buh2 - 148:05:43; доля подозрительной активности по данному пользователю составила 17.7%. В отдельный список для проверки попали приложения Solitaire.exe, dota2.exe, cs2.exe, Half-Life Launcher (hl.exe), AnyDesk (AnyDesk.exe), включая игровые приложения, средства удаленного доступа или сервисы, требующие проверки на соответствие рабочему

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

профилю. Полученные значения используются для приоритизации ручной проверки пользователей, уточнения исключений DLP-политик и настройки допустимых сценариев работы с веб-сервисами, файлами и приложениями.

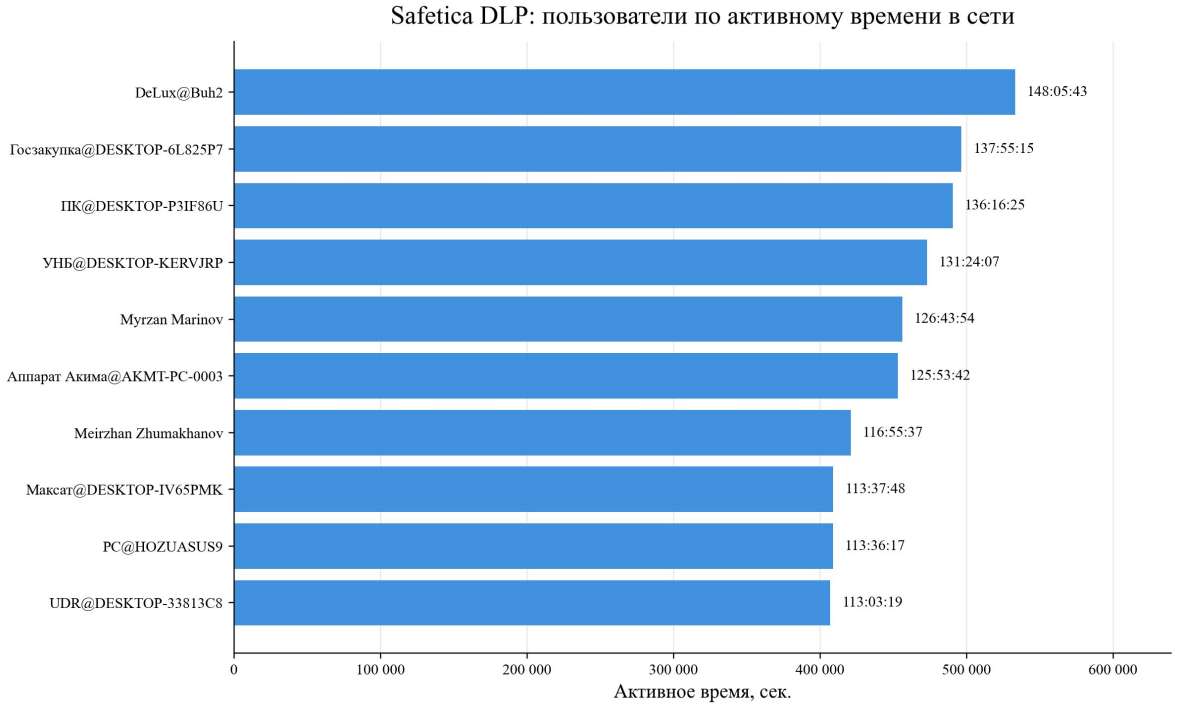


Рисунок 18. Время нахождения пользователя в сети

На диаграмме пользовательской активности показаны пользователи с максимальным суммарным временем работы в сети за отчетный период. Лидирующий пользователь: DeLux@Buh2 с активным временем 148:05:43; также в верхней части выборки находятся Госзакупка@DESKTOP-6L825P7 и ПК@DESKTOP-P3IF86U. Длина полосы соответствует общему активному времени пользователя, рассчитанному по данным Safetica. Рисунок показывает верхнюю часть выборки пользователей по сетевой активности и визуально сравнивает значения между ними. Подробные числовые значения по активным дням, подозрительной активности и доле подозрительной активности приведены в таблице ниже.

В детализации сетевой активности по пользователям приведены активные дни, общее активное время, время подозрительной активности и ее доля. Колонка 'Активные дни' показывает, в течение скольких дней пользователь был представлен в наблюдаемой активности, а колонка 'Общее активное время' отражает суммарную длительность. Отдельно показано время подозрительной активности и его процентная доля относительно общей активности пользователя. Таблица дополняет диаграмму тем, что переводит визуальное сравнение пользователей в числовой формат и показывает дополнительные показатели, которые не помещаются на рисунке.

Таблица 12. Сетевая активность пользователя

№	Пользователь	Активн	Общее	Подозритель	Доля

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

		ые дни	активное время	ная активность	подозрительной активности
1	DeLux@Buh2	23	148:05:43	26:08:57	17.7%
2	Госзакупка@DESKTOP-6L825P7	21	137:55:15	00:19:42	0.2%
3	ПК@DESKTOP-P3IF86U	17	136:16:25	00:00:10	0.0%
4	УНБ@DESKTOP-KERVJRP	17	131:24:07	00:08:40	0.1%
5	Myrzan Marinov	20	126:43:54	00:00:06	0.0%
6	Аппарат Акима@AKMT-PC-0003	18	125:53:42	00:37:55	0.5%
7	Meirzhan Zhumakhanov	18	116:55:37	00:00:51	0.0%
8	Максат@DESKTOP-IV65PMK	23	113:37:48	00:00:08	0.0%
9	PC@HOZUASUS9	17	113:36:17	00:17:50	0.3%
10	UDR@DESKTOP-33813C8	15	113:03:19	00:07:02	0.1%

6.5 Checkpoint - межсетевой экран

В отчётном периоде на шлюзах Check Point NGFW осуществлялся мониторинг сетевой активности, выявление вредоносного трафика и блокирование потенциально опасных соединений. Совокупно зарегистрировано 12 679 246 срабатываний защитных механизмов, в том числе Anti-Bot - 5 355 972, Anti-Virus - 5 977 562, IPS - 1 345 712. Наибольшая активность наблюдалась на шлюзе GW-NAURYZBAY.

Таблица 13. Зафиксированный активность в Межсетевом экране

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

№	Категория	Показатель	Значение
1	Общие события безопасности	Anti-Bot события	5 355 972
2	Общие события безопасности	Anti-Virus события	5 977 562
3	Общие события безопасности	IPS-инциденты	1 345 712

Анализ сетевой активности показывает преобладание приложений удалённого доступа, обмена файлами и проксирующих сервисов. Наиболее заметная нагрузка пришлась на приложение BitTorrent Protocol (сессии - 8 994 018, трафик - 121,4 ГБ). Основные категории сетевой активности: P2P File Sharing, Critical Risk, Remote Administration, Anonymizer, File Storage and Sharing. Указанные показатели требуют периодической проверки на предмет соответствия деловым задачам пользователей.

Таблица 14. Сетевая активность

№	Приложение	Сессии	Трафик
1	BitTorrent Protocol	8 994 018	121,4 ГБ
2	ZeroTier One	662 526	260,4 МБ
3	AnyDesk	453 991	2,6 ГБ
4	MediaGet	81 080	2,6 ГБ
5	Radmin VPN	46 485	81,7 МБ
6	uTorrent	44 349	330,7 МБ
7	TeamViewer	37 231	1,1 ГБ
8	BitTorrent Sync	13 461	16,4 МБ
9	VeePN	13 448	498,3 МБ
10	iTop VPN	1 555	4,6 МБ

Средства Anti-Bot и Anti-Virus блокировали обращения к вредоносным ресурсам и попытки загрузки/исполнения вредоносных объектов. Наиболее часто детектировались сигнатуры PUA.TC.3626Wodp, Infecting_URL.ME.RS.TC.530drvMW, Trojan.Linux.RubyMiner.B, что указывает на постоянный фон сетевых угроз в адрес инфраструктуры. Признаков массового заражения по итогам отчётного периода не выявлено.

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

Таблица 15. Заблокированный ВПО

№	Вредоносное ПО	События
1	PUA.TC.3626Wodp	962
2	Infecting_URL.ME.RS.TC.530drvMW	480
3	Trojan.Linux.RubyMiner.B	468
4	Phorpiex.TC.345agexN	430
5	Cryptominer.TC.9e2cUoIa	429
6	Phorpiex.TC.725ebNyK	425
7	Phorpiex.TC.6860TADZ	408
8	Infecting_URL.VUP.RS.TC.c5edmXPX	404
9	Swift.TC.e7e0XsOZ	305
10	Infecting_URL.VDP.RS.TC.6748Jhse	303

Система предотвращения вторжений (IPS) фиксировала и блокировала типовые сценарии сетевого воздействия и нарушений протоколов. Наиболее частыми типами событий стали TCP Segment Limit Enforcement, Max Ping Size, TCP Invalid Retransmission. Срабатывания носили превентивный характер и свидетельствуют о штатной работе защитных политик межсетевого экрана.

Таблица 16. Система предотвращения вторжений

№	Тип события	Сессии
1	TCP Segment Limit Enforcement	768 408
2	Max Ping Size	432 821
3	TCP Invalid Retransmission	102 109
4	Command Injection	13 814
5	228	12 444
6	ZMap Security Scanner	2 367
7	GnuTLS DistinguishedName	874

DOC ID KZBW2Z120260000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z120260000019602BFD1E3

	Decoding Double Free	
8	Sensitive Configuration File Disclosure	836
9	SQL Injection	818
10	Non Compliant IKE	475

7. РЕАЛИЗОВАННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с техническим заданием обеспечено функционирование и сопровождение комплекса средств защиты информации, включающего: Elastic SIEM, Elastic Defend, Nessus, T-Lab Sandbox, Safetica DLP, Check Point NGFW. Состояние систем оценивается как работоспособное; детализированный статус по внедрению и сопровождению отражается в приложениях и служебной документации.

Отдельно сформирован перечень пунктов, учтенных при корректировке отчета и комплекта подтверждающих материалов. В перечень включены замечания по полноте мониторинга, доступности MDR, управлению уязвимостями, контролю привилегированного доступа, обучению и процессам информационной безопасности. Детальная матрица замечаний, статусов и подтверждающих материалов приведена в Приложении 10.

8. ВЫВОДЫ И РЕКОМЕНДАЦИИ

8.1. Общие выводы

На отдельных шлюзах фиксировалось использование приложений удалённого доступа, VPN и P2P-обмена, включая BitTorrent Protocol, ZeroTier One, AnyDesk. Выявленные вредоносные объекты своевременно блокировались средствами Check Point; наиболее часто встречались PUA.TC.3626Wodp, Infecting_URL.ME.RS.TC.530drvMW, Trojan.Linux.RubyMiner.B. IPS фиксировала типовые сценарии сетевого воздействия, при этом признаков успешной эксплуатации уязвимостей не выявлено. Под мониторингом находилось 617 узлов; offline - 357, нестабильных/требующих проверки - 31. За отчетный период зарегистрировано 576 событий уровня high/critical; основной вклад внесло правило «First Time Seen Removable Device». По данным Nessus в отчётном периоде сохраняются 42 критические и 165 высоких уязвимостей.

8.2. Приоритетные планы работ

Продолжить актуализацию и оптимизацию правил корреляции в SIEM с учётом выявленных сценариев и особенностей инфраструктуры. Усилить контроль полноты телеметрии от агентов и качество интеграций между

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

DOC ID KZBW2Z12026000019602BFD1E3

системами защиты. Продолжить устранение критических и высоких уязвимостей по данным сканирований и перепроверку проблемных узлов. Продолжить контроль и актуализацию политик Check Point NGFW с акцентом на risky applications, VPN и P2P-категории. Перепроверить необходимость использования приложений BitTorrent Protocol, ZeroTier One, AnyDesk в инфраструктуре Заказчика.

8.3. Рекомендации

Продолжить контроль и актуализацию политик Check Point NGFW с акцентом на risky applications, VPN и P2P-категории. Перепроверить необходимость использования приложений BitTorrent Protocol, ZeroTier One, AnyDesk в инфраструктуре Заказчика. Проводить дополнительную проверку узлов и пользователей, демонстрирующих устойчивую активность по BitTorrent, AnyDesk, OpenVPN и аналогичным приложениям. Сохранять мониторинг IPS/Anti-Bot/Anti-Virus в непрерывном режиме и пересматривать исключения на шлюзах с наибольшей активностью. Проверить offline/unhealthy агенты и сверить состояние политик на проблемных хостах. Провести ревизию логики и исключений для правила «First Time Seen Removable Device».

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business

Квитанция о подписании

Основная информация

DOC ID	KZBW2Z12026000019602BFD1E3
Тип документа	Исходящее письмо
Тема	Отчет по фактически оказанным услугам за май. Ранее ошибочно было направлено сопроводительное письмо без приложений (рег. №01-01/207 от 05.06.2026г.)
Статус	Доставлен
Рег. Номер:	01-01/208
Рег. Дата:	05.06.2026
Количество страниц	0
Подписи	2

Информация об отправителе

Отправитель	ТОО "MSSP.GL"
IP-адрес	109.163.197.162

Информация о получателях

Получатель 1	Управление цифровизации города Алматы, 042000249000, Казахстан

Информация о подписантах

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Заместитель Генерального директора
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи
Подпись	MIIWlQYJ...y/1gNaQ==
Дата подписания	05.06.2026 16:24

Подписал(а)	САЛИПОВ ДАУРЕН
Компания	ТОО "MSSP.GL"
Должность	Заместитель Генерального директора
IP-адрес	109.163.197.162
Email	info@kazdream.kz
Тип ЭЦП	ЭЦП Национального удостоверяющего центра Республики Казахстан
	Первый руководитель юридического лица, имеющий право подписи

Подпись	MIIWzAYJ...HJebpkN0=
Дата подписания	05.06.2026 16:25

DOC ID KZBW2Z12026000019602BFD1E3

DOC ID KZBW2Z12026000019602BFD1E3
Электронный документ подписан в Documentolog Business