УТВЕРЖДАЮ

И.о. директора Департамента цифровой трансформации и проектного менеджмента ГУ «Министерство культуры и информации Республики Казахстан»
_____ Сыздыгалин Н.Н.
«____» _____2026 г.

МП

УТВЕРЖДАЮ

Директор
ТОО «ALAN TECHNOLOGY GROUP»
_____Айгайбекова Ж.К.
«____» _____ 2026 г.

МП

ОТЧЁТ ОБ ОКАЗАНИИ УСЛУГ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

за март 2026 года, к договору № 161040017107/260055/00 от 19.03.2026 года

СОГЛАСОВАНО

Начальник ОЦИБ
ТОО «ALAN TECHNOLOGY GROUP»
_____ Серік Д.Т.
«____»_____ 2026 г.

г. Астана

ЛИСТ СОГЛАСОВАНИЯ

ГУ «Министерство культуры и информации Республики Казахстан»

№ п\п	ФИО	Должность	Подпись
1	Блялова Ә.Қ	Руководитель управления электронного архива Департамента цифровой трансформации и проектного менеджмента	
2			
3			

ТОО «ALAN TECHNOLOGY GROUP»

№ п\п	ФИО	Должность	Подпись
1	Айгайбекова Ж.К.	Директор	
2	Серік Д.Т.	Начальник ОЦИБ	
3			
4			
5			
6			
7			

Содержание

1. Введение 4
2. Определения 5
3. Услуга ситуационного центра (SOC) 6
4. Рекомендации для организации: 13
5. Рекомендации для пользователей: 14
6. Актуальные контакты специалистов 15

1. Введение

На основании технической спецификации к договору №161040017107/260055/00 от 18.03.2026 года, заключенного между Государственным учреждением «Министерство культуры и информации Республики Казахстан» (далее — Заказчик) и ТОО «ALAN TECHNOLOGY GROUP» (далее — Исполнитель), в марте 2026 года Исполнителем были выполнены следующие работы в рамках оказания услуг по мониторингу событий информационной безопасности (далее — ИБ):

В рамках выполнения мероприятий по развертыванию системы мониторинга обеспечено подключение источников событий: **18** узлов в защищенном сегменте ЕТС ГО и **6** узлов во внешнем сетевом контуре.

На текущий момент реализован сбор и индексация телеметрии, система осуществляет регистрацию событий информационной безопасности в режиме реального времени.

Настроены дашборды в Elastic / Kibana, обеспечивающие визуализацию и анализ событий по типам (auditd, system.auth), а также мониторинг действий пользователей и выявление аномальной активности.

Указанные результаты подтверждают корректную интеграцию агентов мониторинга с инфраструктурой Заказчика.

2. Определения

В настоящем документе использованы следующие определения:

Информационная безопасность (ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Оперативный центр информационной безопасности (ОЦИБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.

Источник событий ИБ – устройства, генерирующие события (операционные системы, базы данных, прикладное программное обеспечение, средства защиты информации, сетевое и серверное оборудование).

Событие ИБ – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации.

Security Information and Event Management (SIEM) – система мониторинга и управления событиями ИБ.

Инцидент ИБ – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов.

IP-адрес – уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.

Malware Information Sharing Platform (MISP) — платформа с открытым исходным кодом для обмена информацией об угрозах ИБ.

Инструментальный пентест (сканирование) – методика проведения тестирования на проникновение, в ходе которой используются автоматизированные инструменты для обнаружения уязвимостей, анализа сетевой инфраструктуры, веб-приложений или других компонентов ИТ-системы.

3. УСЛУГА СИТУАЦИОННОГО ЦЕНТРА (SOC)

В отчетный период работы по подключению источников к SIEM продолжаются. Получен доступ к выделенному серверу с развернутым коллектором, обеспечивающим централизованный сбор и передачу журналов событий. Сотрудникам Заказчика направлены инструкции по установке и настройке агентов, проведена практическая демонстрация совместно со специалистами ОЦИБ.

В отчетный период зафиксировано **164.441** событий (Counts of Events) в ЕТС ГО сегменте.

Counts of Events (Records) — это метрика, используемая в системах мониторинга и анализа, которая отображает общее количество зарегистрированных событий за определённый период времени.

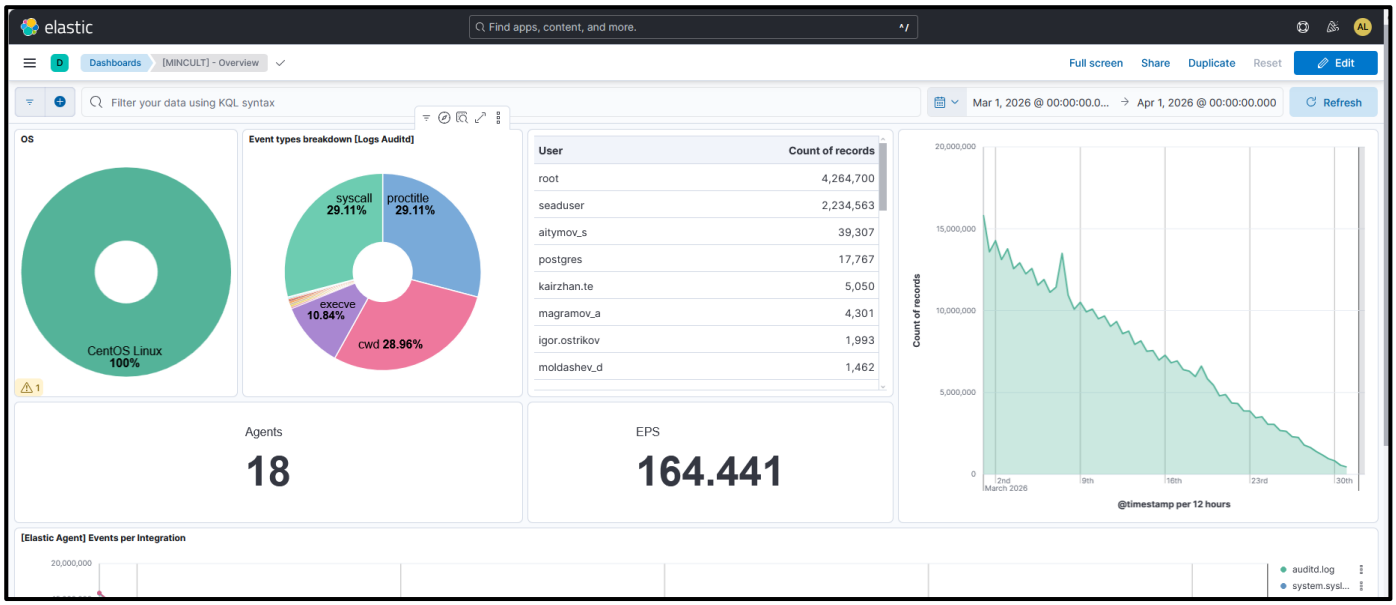

Рисунок 1. Обзор состояния инфраструктуры и инцидентов в Elastic в ЕТС ГО сегменте

Данные представлены за отчетный период. Основные показатели инфраструктуры:

Мониторинг осуществляется на **18** агентах, все узлы функционируют под управлением CentOS Linux (100%).

Структура событий аудита (Auditd): наибольшая доля событий приходится на категории proctitle (29,11%), cwd (28,96%) и syscall (29,11%), что свидетельствует о преобладании операций, связанных с выполнением процессов и системными вызовами. Доля событий execve составляет 10,84%, тогда как прочие типы занимают незначительную часть и носят вспомогательный характер.

Активность пользователей: основной объем записей сформирован системной учетной записью root (4 264 700 событий), а также пользователями seaduser (2 234 563), aitmov_s (39 307), postgres (17 767), kaizhan.te (5 050) и magramova_a (4 301).

Прочие учетные записи (включая igor.ostrikov и moldashev_d) демонстрируют низкий уровень активности.

Динамика событий: графики демонстрируют пик нагрузки в середине отчетного периода с последующим планомерным снижением количества событий, что соответствует штатной работе инфраструктуры и отсутствию признаков инцидентов.

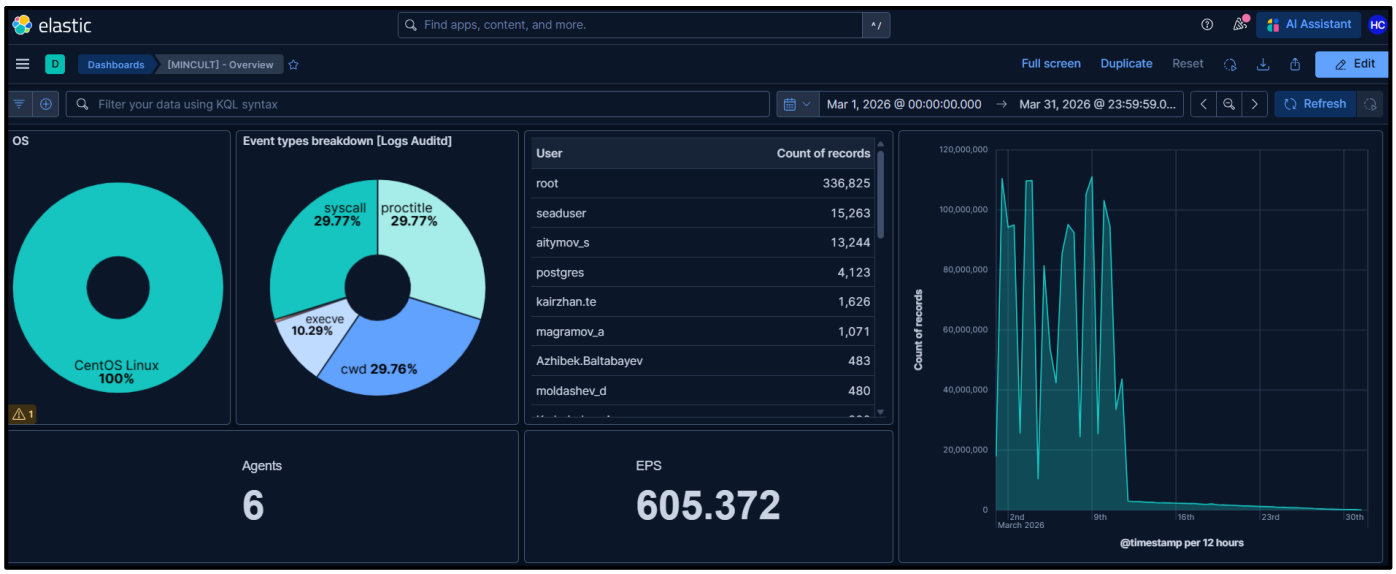

Рисунок 2. Обзор состояния инфраструктуры и инцидентов в Elastic во внешнем сегменте

Мониторинг во внешнем сегменте осуществляется на **6** агентах, все узлы функционируют под управлением CentOS Linux (100%). Средняя интенсивность событий составляет **605,372** EPS, что указывает на высокую нагрузку в отдельные периоды с последующим снижением активности к концу отчетного интервала.

Аудит и системная активность (Auditd): структура событий распределена равномерно между основными типами — syscall (29,77%), proctitle (29,77%) и cwd (29,76%), что отражает интенсивную работу процессов, системных вызовов и операций с файловой системой. Доля событий execve составляет 10,29% и соответствует нормальной активности запуска процессов.

Активность учетных записей: наибольшее количество событий инициировано учетной записью root (336 825), что типично для серверной инфраструктуры с административной нагрузкой. Также зафиксирована активность пользователей seaduser (15 263), aiymov_s (13 244), postgres (4 123), kazhan.te (1 626) и magramova_a (1 071). Прочие учетные записи (включая Azhibek.Baltabayev и moldashev_d) демонстрируют низкую активность.

Дополнительно, по временной динамике наблюдается пик активности в начале отчетного периода с последующим снижением количества событий, что может быть обусловлено изменением нагрузки или завершением отдельных задач/процессов.

Признаки инцидентов информационной безопасности не выявлены.

Рисунок 3. Статистика интеграций Elastic Agent и таблица Audit Events в ЕТС ГО сегменте

На представленном дашборде (Рисунок 3) отображена динамика поступления событий от агентов Elastic Agent за отчетный период с агрегацией по 12-часовым интервалам. Визуализация демонстрирует устойчивый нисходящий тренд: максимальные значения фиксируются в начале периода (порядка 15–16 млн событий за интервал), после чего наблюдается постепенное и равномерное снижение объема поступающих событий к концу отчетного периода.

Основной вклад в общий объем телеметрии вносит журнал auditd.log, при этом события от system.syslog, system.auth и других источников занимают незначительную долю и повторяют общую динамику снижения нагрузки. Колебания в первой части периода носят незначительный характер и укладываются в рамки штатной эксплуатационной активности.

В целом, характер изменения нагрузки свидетельствует о поэтапном снижении активности систем или оптимизации объема собираемой телеметрии.

Признаки инцидентов информационной безопасности не выявлены.

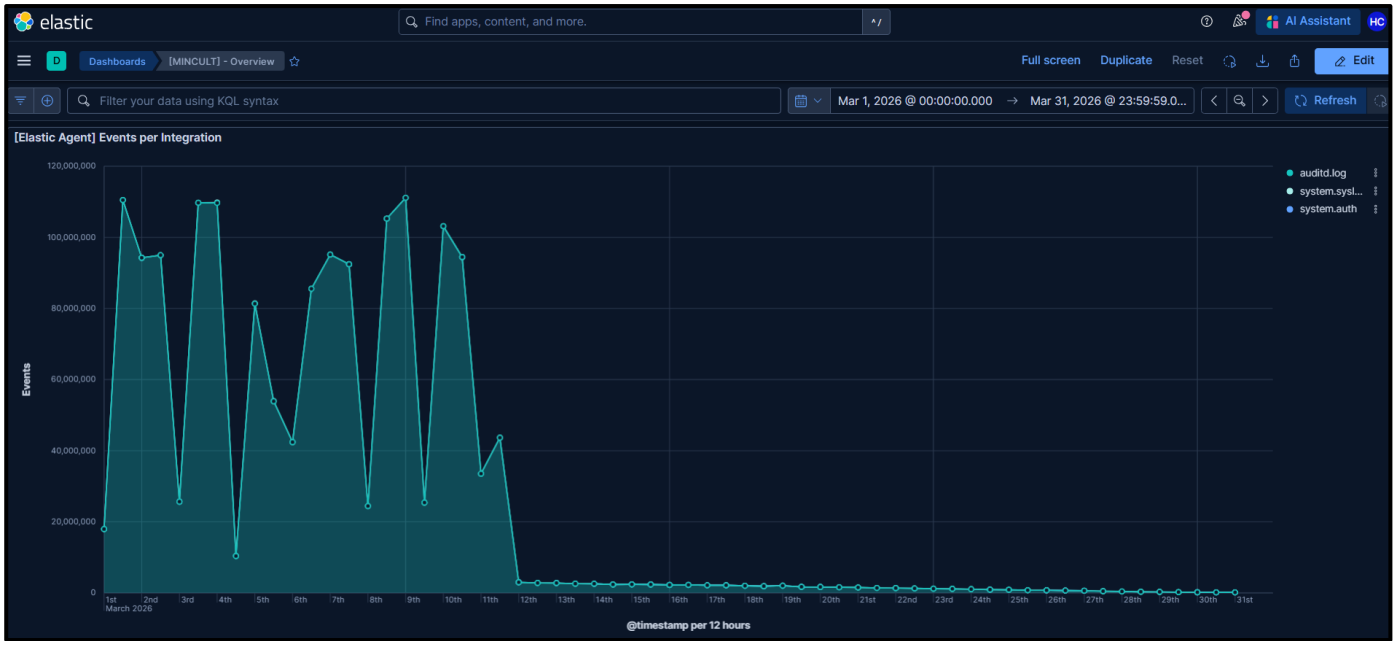

Рисунок 4. Статистика интеграций Elastic Agent и таблица Audit Events во внешнем сегменте

На представленном дашборде (Рисунок 4) отображена статистика поступления событий от агентов Elastic Agent за отчетный период с агрегацией по 12-часовым интервалам. В начале периода наблюдается высокая и неравномерная интенсивность телеметрии с выраженными пиковыми значениями (до ~110–115 млн событий за интервал), после чего фиксируется резкое снижение нагрузки — начиная с середины периода объем поступающих событий снижается практически до фоновых значений и остается на низком уровне до конца отчетного периода.

Основной вклад в общий поток данных формирует журнал auditd.log, тогда как события system.syslog и system.auth занимают незначительную долю и повторяют общую динамику изменения нагрузки. Существенные колебания в первой части периода могут быть обусловлены пиковыми операциями или задачами, после завершения которых наблюдается стабилизация.

В целом зафиксированная динамика указывает на изменение характера нагрузки (резкое снижение активности после пикового периода) и соответствует штатной эксплуатации систем, не демонстрируя признаков инцидентов информационной безопасности.

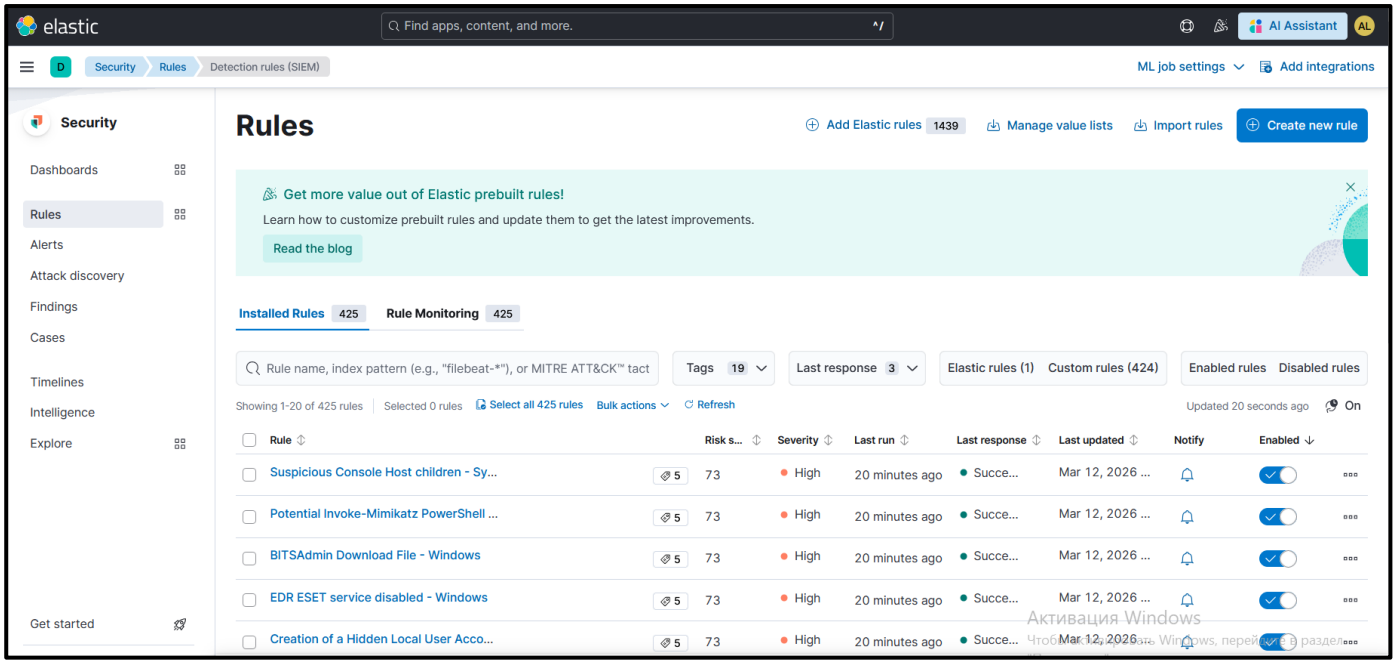

Рисунок 5. Добавленные правила в SIEM

На Рисунке 5 представлено окно управления правилами, где отображаются активные правила, их уровень критичности, статус последнего срабатывания и актуальность обновления.

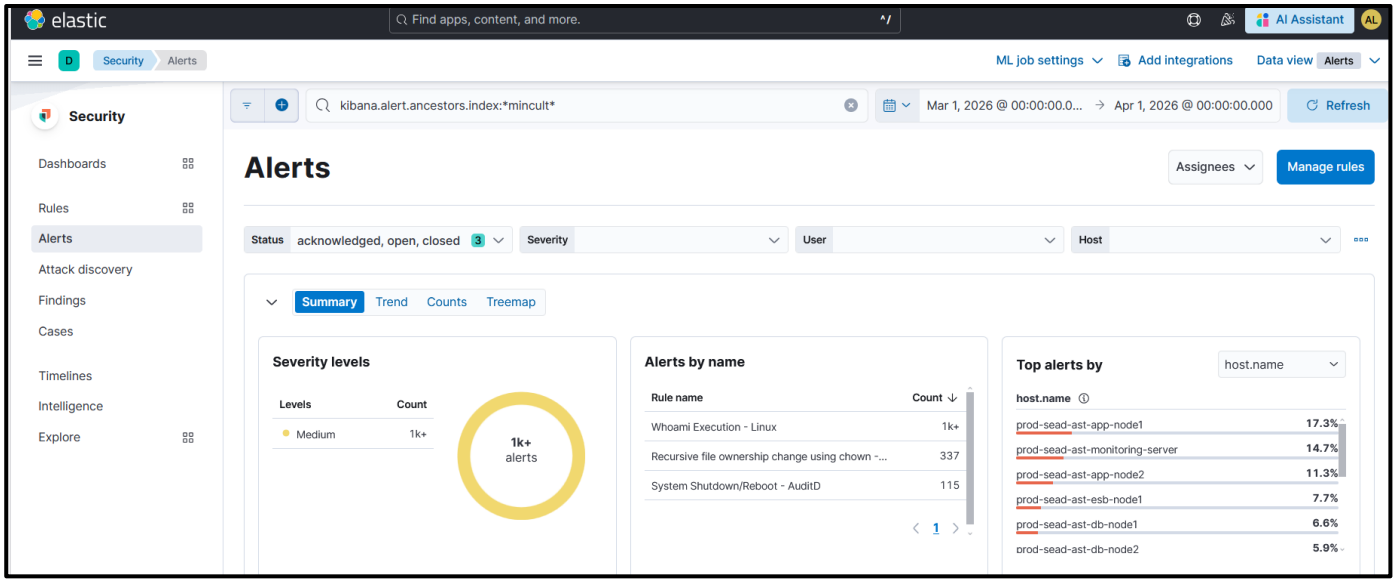

Рисунок 6. Сводная панель оповещений Elastic SIEM (Alerts Dashboard) в ETC ГО сегменте

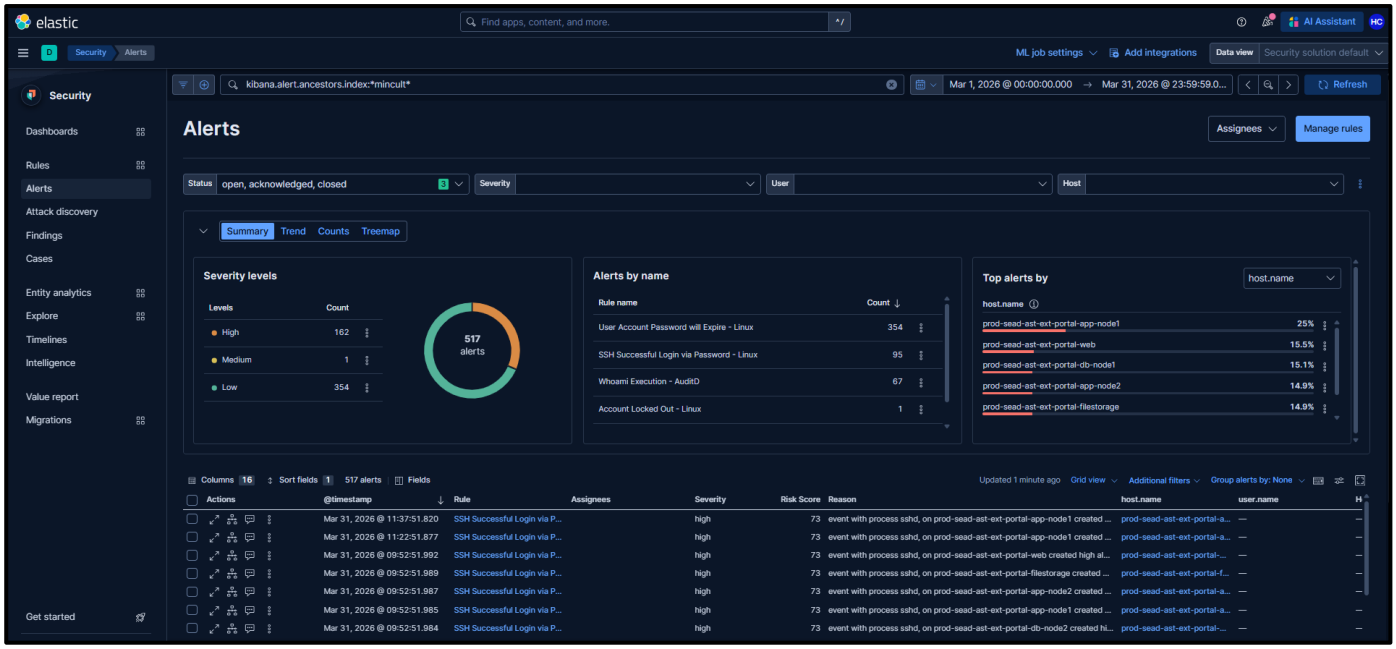

Рисунок 7. Сводная панель оповещений Elastic SIEM (Alerts Dashboard) во внешнем сегменте

В ходе мониторинга информационной безопасности в ЕТС ГО сегменте зафиксировано **18** событий среднего уровня критичности. Сводная информация по данным событиям приведена в Таблице **1**.

Таблица№1. Перечень событий ИБ в ЕТС ГО сегменте

№	_createdAt	title	severityLabel
1.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
2.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
3.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
4.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
5.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
6.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
7.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
8.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
9.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
10.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
11.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
12.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM

13.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
14.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
15.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
16.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
17.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM
18.	07.03.2026 21:43	Suspicious Internal activity, detected on - AuditD	MEDIUM

Во внешнем сегменте зафиксировано **12** событий различного уровня критичности, включая события высокого и незначительного уровня. Соответствующие данные представлены в Таблице **2**.

Таблица№2. Перечень событий ИБ во внешнем сегменте

№	_createdAt	title	severityLabel
1.	27.03.2026 8:36	Suspicious Internal activity, detected on - Linux	HIGH
2.	27.03.2026 8:36	Suspicious Internal activity, detected on - Linux	HIGH
3.	26.03.2026 19:13	Suspicious Internal activity, detected on - AuditD	HIGH
4.	26.03.2026 11:35	Suspicious Internal activity, detected on - Linux	HIGH
5.	24.03.2026 23:57	Suspicious Internal activity, detected on - AuditD	HIGH
6.	13.03.2026 8:26	Suspicious Internal activity, detected on - AuditD	HIGH
7.	13.03.2026 8:26	Suspicious Internal activity, detected on - AuditD	HIGH
8.	13.03.2026 8:26	Suspicious Internal activity, detected on - AuditD	HIGH
9.	13.03.2026 8:25	Suspicious Internal activity, detected on - AuditD	HIGH
10.	13.03.2026 8:25	Suspicious Internal activity, detected on - AuditD	HIGH
11.	03.03.2026 9:54	Suspicious External activity, detected on - Linux	LOW
12.	03.03.2026 9:54	Suspicious External activity, detected on - Linux	LOW

4. РЕКОМЕНДАЦИИ ДЛЯ ОРГАНИЗАЦИИ:

1. Регулярно обновлять и анализировать политики безопасности организации, учитывая изменения в угрозах и требованиях (в том числе внутренними и внешними).
2. Ежемесячно проверять эффективность мер по предотвращению атак, в том числе фишинговых, и корректировать их при необходимости.
3. Своевременно обновлять все программные и аппаратные средства, включая операционные системы, прикладное программное обеспечение и антивирусные решения.
4. Регулярно проводить тестирование на проникновение для выявления потенциальных уязвимостей в сетевой инфраструктуре и приложениях.
5. Ежеквартально анализировать и оптимизировать права доступа сотрудников, минимизируя привилегии до необходимого уровня.
6. Соблюдать принцип "принцип наименьших привилегий" при выдаче доступа к информационным ресурсам.
7. Регулярно обучать персонал основам информационной безопасности, проводить тренинги и тестирования для повышения осведомленности.
8. Своевременно реагировать на инциденты безопасности, в том числе проводить анализ инцидентов для предотвращения их повторения.
9. Проводить аудит безопасности системы управления событиями (SIEM) еженедельно для выявления аномалий и улучшения процессов мониторинга.
10. Не допускать использование нелицензионного или устаревшего программного обеспечения в организации.
11. Обеспечивать ежегодной технической поддержкой все инструменты информационной безопасности.
12. Проводить аудит IP-адресов, портов и баз данных, используемых для подключения к серверам, с целью оперативного выявления потенциальных уязвимостей и несанкционированных доступов
13. Установить Next-Generation Firewall (NGFW) на внешний контур регионов сети для повышения общей безопасности, обеспечивая эффективный контроль и защиту от современных угроз
14. Регулярно проводить аудит паролей, включая исследование их стойкости, а также систематически изучайте логи для выявления необычных активностей и оперативного реагирования на потенциальные угрозы информационной безопасности.
15. Обеспечить направление логов с критически важных источников на мониторинг ОЦИБ с целью оперативного выявления и предотвращения развития атак и инцидентов ИБ.

5. РЕКОМЕНДАЦИИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ:

1. Следите за своими учетными данными: регулярно изменяйте пароли, используйте сильные пароли и не делитесь ими с коллегами.
2. Не открывайте вложения и не переходите по ссылкам в электронных письмах от незнакомых отправителей.
3. Пользуйтесь только официальными и безопасными источниками для загрузки и установки программного обеспечения.
4. Заблокируйте свои устройства при отсутствии возможности доступа к ним и не оставляйте их без присмотра.
5. Постоянно обновляйте операционные системы, антивирусные программы и прикладное ПО на своих устройствах.
6. Поддерживайте осторожность в социальных сетях, избегая публикации личной информации и ограничив доступ к вашим профилям.
7. Следите за уведомлениями об изменениях в политиках безопасности и проходите тренинги по информационной безопасности.
8. Если вы обнаружите необычную активность или подозрительные события, немедленно сообщите об этом службе информационной безопасности.
9. Регулярно создавайте резервные копии важных данных и храните их в безопасном месте.

6. АКТУАЛЬНЫЕ КОНТАКТЫ СПЕЦИАЛИСТОВ ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.

№	ФИО	Номер телефона
1	Нигиманова Айгерим Жуматаевна	8705 5619838
2	Драбчук Богдан Александрович	8776 1242016
3	Кадринов Даулет Маулетович	8775 9745001
4	Жексенбеков Бексұлтан	8778 2663799
5	Сәндібекова Нұрдана	8707 5461251