УДК 004.056.5

Дмитро ПІДЛИСЬКИЙ

Західноукраїнський національний університет

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ПЛАГІНУ KIBANA ДЛЯ РОЗВІДКИ КІБЕРЗАГРОЗ

Вступ. У сучасному інформаційному середовищі об'єктів корпоративної та державної безпеки важливість систем раннього виявлення й реагування на кіберзагрози зростає. Підходи типу розвідки загроз (Threat Intelligence) дедалі більше інтегруються у рішення з моніторингу, аналізу та візуалізації даних. У цьому контексті платформа Kibana, як компонент ELK-стеку набуває особливого значення завдяки своїм можливостям інтеграції даних, візуалізації та побудови дашбордів [1-4].

Метою є: аналіз плагіну Kibana, що дозволяє розширити її функціонал для безпекового моніторингу та розвідки загроз та оцінка практичних можливостей побудови платформи розвідки загроз на основі цього плагіну, включно з інтеграцією індикаторів, створенням правил виявлення та побудовою аналітики загроз.

1. Аналіз плагіну Kibana

Плагін Kibana створює доповнення до основного інструментарію візуалізації даних, дозволяючи розширити можливості у сфері безпеки та розвідки загроз. Він формує додатковий функціонал, наприклад: нові аплікації, модулі візуалізації, інтеграцію з даними індикаторів загроз, спеціалізовані дашборди та правила.

Згідно з офіційною документацією, Kibana [1] підтримує встановлення плагінів, що додають власну функціональність. Наприклад, існує пакет «Threat Intelligence Utilities», який включає дашборд для огляду даних зі всіх підключених TI-джерел (рисунок 1) [2].

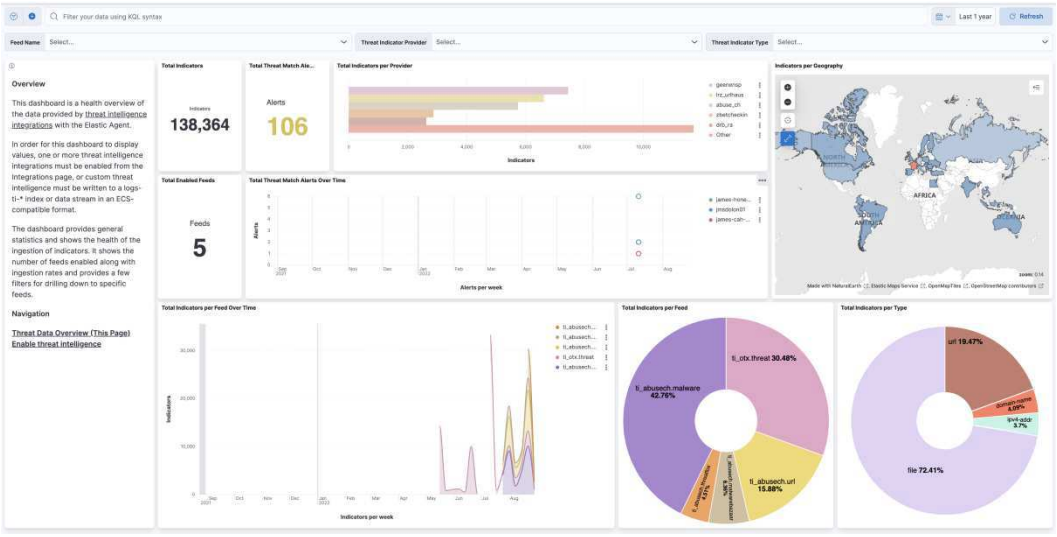

Рисунок 1 – Приклад відображення даних

Ключові можливості включають:

– підключення модулю TI (Threat Intelligence) через агент Elastic Agent або

Filebeat для збору індикаторів (IP, домени, хеші) та їх індексації.

– створення дашбордів у Kibana для візуалізації, фільтрації та кореляції даних індикаторів та подій.

– використання правил «Indicator Match», коли індикатор TI збігається з логом в середовищі, що дозволяє генерувати попередження. leveleffect.

Проведений аналіз дозволяє визначити ряд переваг застосування плагіну. Основними з них є можливість інтеграції з екосистемою Elastic, зокрема використовуючи Elasticsearch, Logstash і Kibana, організація може об'єднати збір логів, індексацію, пошук і візуалізацію в єдиний процес. Також варто зазначити гнучкість візуалізації, оскільки Kibana дозволяє створювати власні дашборди, фільтри, використовувати Lens, ES|QL запити для глибшого аналізу.

Плагін забезпечує реальне виявлення індикаторів, зокрема модуль TI дозволяє зв'язати дані індикаторів із подіями в логах, що підвищує ефективність виявлення загроз. Важливим аспектом є його масштабованість, оскільки рішення на базі Elasticsearch сімейства дозволяє обробляти великі обсяги даних з високою швидкістю індексації та пошуку.

Проте існують певні обмеження та виклики, зокрема офіційна документація вказує, що інтерфейси змінюються, і немає гарантії сумісності з новими версіями Elastic. Необхідність спеціалізованого налаштування, зокрема підключення модулю TI, налаштування індексів, правил, API-ключів тощо потребує технічної експертизи. Недоліки стосуються також продуктивності та ресурсів, оскільки активація великої кількості правил виявлення індикаторів може значно підвищити навантаження на стек. На застосування також може впливати оОбмеженість готових дашбордів, оскільки у деяких випадках потрібно створювати власні візуалізації, оскільки стандартні рішення можуть бути надто загальними.

Плагін Kibana є потужним інструментом для розширення функціональності платформи до задач безпеки і розвідки загроз. Завдяки інтеграції з Elastic Stack він дає змогу об'єднати збір, обробку, індексацію та візуалізацію даних індикаторів загроз. Проте впровадження вимагає ретельного планування, налаштування ресурсів та уваги до сумісності. Як основа платформи розвідки загроз – він має перспективу, але потребує доповнення відповідними процесами та даними.

2. Розвідка загроз на основі плагіну Kibana

Реалізація платформи розвідки загроз з використанням Kibana передбачає використаня типової архітектури (рисунок 2), що може включати наступні компоненти[1-3]:

– джерела індикаторів: відкриті TI-фіди (наприклад, AlienVault OTX, MalwareBazaar), внутрішні дані (логи, DNS-запити, мережевий трафік);

– агент або модуль збору (Filebeat, Elastic Agent) з увімкненим модулем Threat Intel;

– індексація даних у Elasticsearch: створення індексів для індикаторів (наприклад, logs-ti*) та для логів подій (logs-*);

– інтерфейс Kibana з дашбордами, фільтраціями, інструментами аналітики;

– правила виявлення (Indicator Match) - налаштування автоматичного порівняння логів і індикаторів, що дозволяє генерувати попередження.

– процес реагування – при генерації попередження , аналітик переглядає дашборд, проводить аналіз, ініціює розслідування чи заходи.

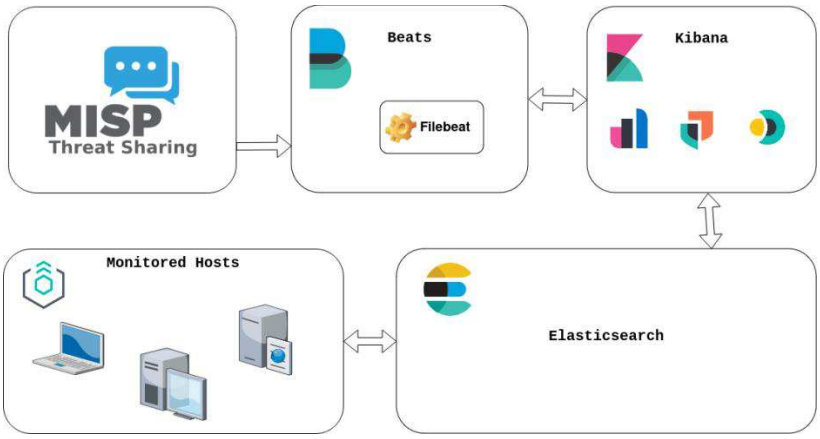

Рисунок 2 - Архітектура платформи розвідки загроз

Практичні можливості застосування використання можуть включати наступні сценарії.

– Моніторинг індикаторів у реальному часі. Плагін дозволяє візуалізувати кількість нових індикаторів, їх розподіл за типами (IP, домен, хеш), а також співставити з подіями в мережі чи кінцевих точках. Наприклад, можна побудувати дашборд із часовою серією підвищеної активності за індикаторами.

– Кореляція індикаторів з логами. Використовуючи індекси, можна створити правило, що спрацьовує коли destination.ip у логу співпадає з threatintel.indicator.ip. Це дозволяє швидко визначати події, в яких ваші системи контактували з відомим шкідливим ресурсом.

– Аналітика тенденцій загроз. Дашборд може показати, як змінюється обсяг нових індикаторів, як часто відбуваються спрацьовування, які типи індикаторів переважають - це допомагає команді безпеки прогнозувати активність атак.

– Звітність та візуалізація для керівництва. Системи, створені на базі Kibana, можуть перетворювати технічні дані на зрозумілий дашборд для менеджменту, наприклад показуючи кількість інцидентів, ступінь ризику, тенденції.

3. Рекомендації щодо практичної реалізації платформи виявлення загроз

Для реалізації платформи розвідки загроз на основі плагіну Kibana необхідно встановити модуль Threat Intel та перевірити, що дані індикаторів коректно індексуються у відповідний індекс.

Налаштувати правила та фільтри, які мінімізують кількість хибнопозитивних спрацьовувань, наприклад, відфільтрувати внутрішні IP-адреси чи низькоризикові індикатори.

Важливим аспектом є планування ресурсів, оскільки великі обсяги даних індикаторів та логів могуть потребувати масштабування Elasticsearch і оптимізації запитів. Необхідно підготувати шаблони дашбордів, зокрема одразу створити набір базових візуалізацій, наприклад кількість індикаторів за типами, співставлення з подіями, карта геолокацій тощо.

Наступним кроком є вровадження процес реагування: алерт -> аналіз -> реакція (рисунок 3).

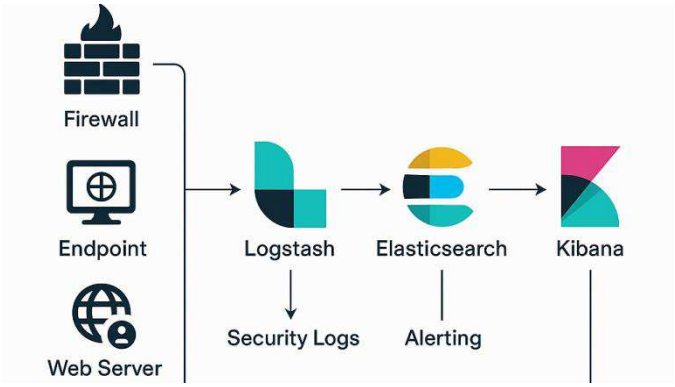

Рисунок 3 – Реагування на загрози

Дашборд Kibana повинен бути інтегрований в процес реагування на загрози. Тому потрібно періодично оцінювати ефективність, зокрема визначити як часто алерти на основі індикаторів перетворюються на реальні інциденти Це допоможе скоригувати правила та пріоритизацію.

При реалізації платформи виявленя загроз важливо враховувати певні ризики та функціональні обмеження, зокрема індикатори TI не гарантують, що подія є атакою, тому потрібно розглядати її у контексті. Також великі обсяги індикаторів можуть створювати «шум» й приводити до перевантаження аналітиків. У випадках, коли система не налаштована належним чином, можливі затримки індексації або пропущені події. Надмірне фокусування лише на індикаторах загроз може ігнорувати поведінкові або аналітичні детекції, тому рішення має бути мультиаспектним.

Висновок. Побудова платформи розвідки загроз на базі плагіну Kibana є актуальною задачею, яка дозволяє об'єднати індикатори загроз, логи подій і візуалізацію в одному середовищі. При правильній архітектурі, налаштуванні та процесах така платформа може значно підвищити видимість загроз і скоротити час реагування. Водночас вона потребує фокусування не лише на технологіях, але й на процесах і людському факторі.

Перелік використаних джерел.

1. Kibana plugins. [Електронний ресурс].- Режим доступу: https://www.elastic.co/docs/reference/kibana/kibana-plugins

2. Threat Intelligence Utilities. [Електронний ресурс].- Режим доступу: https://www.elastic.co/docs/reference/integrations/ti_util

3. Building Effective Dashboards for Threat Intelligence with Kibana and Grafana. [Електронний ресурс].- Режим доступу: https://thinkcloudly.com/blog/building-effective-dashboards-for-threat-intelligence-with-kibana-and-grafana

4. Home Lab: Enabling and Configuring Threat Intelligence and Detections. [Електронний ресурс].- Режим доступу: https://www.leveleffect.com/blog/home-lab-enabling-and-configuring-threat-intelligence-and-detections