# ВАРИАНТ ОПТИМИЗАЦИИ ПРОЦЕССА THREAT INTELLIGENCE В ЦЕНТРЕ МОНИТОРИНГА КИБЕРБЕЗОПАСНОСТИ

А.В. Макатерчик, В.В. Маликов

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Республика Беларусь*

Кибербразведка или Threat Intelligence является частью комплексного подхода по мониторингу и реагированию на современные киберугрозы. При этом организация кибербразведки в рамках современного центра мониторинга кибербезопасности сталкивается с целым рядом проблем, из которых для данного исследования выделены следующие:

Современная политическая обстановка не гарантируют стабильность доступа к источникам информации об угрозах.

Использование нескольких источников приводит к росту объемов информации требующей корреляции, обработки и фильтрации ложных данных. Что приводит к росту нагрузки на средства защиты информации и персонал.

Большое время реакции при ручной обработке инцидентов связанных с обнаружением индексов компрометации в потоках событий.

Сложность, а зачастую невозможность реализации превентивной блокировки источников угроз на средствах защиты информации, из-за существующих у них ограничений по производительности, емкости баз данных, количествуACL списков и т. п.

Решение данных проблем возможно при организации комплексного подхода, заключающегося в:

1. Организации сбора информации из нескольких источников: собственные инструменты кибербразведки, фиды и платформы от нескольких поставщиков из разных стран и сообществ.
2. Обработка их с использованием нескольких средств. Например, встроенный сервис SIEM (SOAR) и ПО Kaspersky CyberTrace.
3. Превентивную блокировку средствами защиты информации только источников угроз с высоким риском.
4. Анализ потоков событий на предмет наличия в них индексов компрометации с использованием как специально выделенных аппаратно-программных средств, например, Kaspersky CyberTrace, так и средствами, интегрированными в SIEM, SOAR и т.п.
5. При обнаружении в потоке событий индексов компрометации выполнять автоматическую блокировку источников угроз средствами защиты информации на ограниченный период времени.

Данный подход обеспечивает оптимизацию использования ресурсов средств защиты информации, уменьшение нагрузки на аналитиков безопасности, снижает количество ложно-позитивных событий.

## Список литературы

1. Threat Intelligence сейчас модный тренд. [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/phdays/articles/499145.php. – Дата доступа: 27.04.2023.