Акционерное общество «Перспективный мониторинг»

(АО «ПМ»)

**AM THREAT INTELLIGENCE PORTAL**

Функциональные характеристики AM THREAT INTELLIGENCE PORTAL

На 13 листах

Москва 2024

Аннотация

Настоящий документ описывает функциональные характеристики AM Threat Intelligence Portal (далее – AM TIP, Портал).

Содержание

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 4](#_Toc159501025)

[1 Общие сведения 5](#_Toc159501026)

[2 Функциональное назначение 6](#_Toc159501027)

[2.1 Функциональные возможности 7](#_Toc159501028)

[3 Используемые технические средства и дополнительное программное обеспечение 9](#_Toc159501029)

[4 Входные данные 11](#_Toc159501030)

[5 Выходные данные 12](#_Toc159501031)

[6 Загрузка 13](#_Toc159501032)

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

|  |  |
| --- | --- |
| АО «ПМ» | Акционерное общество «Перспективный мониторинг» |
| БРП | База данных сигнатурных правил обнаружения атак АМ Rules |
| AM TIP | AM Threat Intelligence Portal |
| СЗИ | Система защиты информации |
| ИБ | Информационная безопасность |

# Общие сведения

Основным направлением деятельности АО «ПМ» является оценка практической защищенности информационных систем, выявление их уязвимостей при помощи средств инструментального и ручного анализа, реагирование на инциденты безопасности, разработка Программного комплекса автоматизированного поиска, обработки и визуализации данных из открытых источников «Тардис» и Программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire».

Исследование угроз информационной безопасности и поставка экспертных данных в АО «ПМ» являются одними из ключевых направлений деятельности. Компания одной из первых в 2016 году стала разрабатывать собственную базу решающих правил обнаружения компьютерных атак «AM Rules», в дальнейшем расширив линейку экспертных данных TI фидами, категорированными веб-ресурсами, бюллетенями информационной безопасности.

Наименование средства – AM Threat Intelligence Portal.

Формат средства – AM Threat Intelligence Portal является веб-сервисом, обеспечивающим доступ к базе экспертных данных АО «ПМ». Портал интегрирован с внутренними и внешними сервисами экспертных данных
АО «ПМ», что позволяет оперировать всегда актуальными сведениями об угрозах в режиме реального времени.

# Функциональное назначение

AM TIP агрегирует, коррелирует и нормализует информацию об угрозах ИБ из различных открытых и закрытых источников с помощью нескольких методов и технологий предварительной обработки:

* статистические системы;
* инструменты сходства;
* «песочницы»;
* профилирование поведения;
* проверка на основе списков разрешений;
* проверка аналитики.

Каждый индикатор компрометации анализируется набором передовых технологий обнаружения:

* система киберразведки собственной разработки AM Pellonia (Свидетельство о государственной регистрации программы для ЭВМ № 2023666988 от 09.08.2023 г.);
* технологии обнаружения поведения;
* эвристический анализ;
* система срочного обнаружения;
* Sandbox.

В основе фидов – данные об угрозах, аккумулированные экспертами АО «ПМ» в ходе расследований инцидентов и изучения деятельности хакерских группировок во всем мире, а также обезличенные данные с устройств линейки ViPNet, подключенных к Центру мониторинга АО «ПМ». Это позволяет АО «ПМ» поставлять большое количество индикаторов компрометации для российского рынка ИБ.

## Функциональные возможности

К функциональным возможностям AM TIP относятся те, которые подробно описаны в тексте (Подраздел 2.1).

1. Поиск сведений об индикаторах компрометации, которые хранятся в смежных системах, с помощью «TI LOOKUP»:
* AM Pellonia – система киберразведки, предназначенная для мониторинга, сбора, обогащения, корреляции и агрегации информации об угрозах информационной безопасности;
* СБРП – система для разработки и выпуска экспертных данных;
* TI-pipeline – система обработки образцов ВПО и PCAP'ов для автогенерации IoC;
* IP2GEO – система определения месторасположения (GeoIP).
1. Анализ индикатора компрометации с помощью графа – это инструмент для визуализации и анализа IoC и связей между объектами. Граф строится в формате STIX, который является языком описания для обмена данными TI и выводит набор объектов, а также определяет возможные типы взаимосвязей между ними. Информация STIX может быть визуально представлена для аналитика или сохранена в виде JSON для быстрого машинного чтения. Граф AM TIP является разработкой АО «ПМ», использует как общепринятые названия объектов STIX, так и введенные впервые.
2. Выгрузка отчетов по индикаторам компрометации в формате STIX и правил в формате TXT.
3. Просмотр сведений на киберкарте:
* просмотр аналитической информации по угрозам на карте мира и цветовая индикация стран в соответствии с процентом исходящих угроз по отношению к России;
* отображение ТОП 10 атакующих стран и IP-адресов;
* отображение ТОП 10 самых часто встречаемых угроз;
* отображение ТОП 10 самых часто встречаемых идентификаторов уязвимостей (CVE);
* ежедневное обновление информации и возможность выбора различных фильтров отображения информации по периоду времени.

# Используемые технические средства и дополнительное программное обеспечение

Клиентская часть – портал для пользователя функционирует в
веб-браузере. Рекомендованные веб-браузеры для использования: Яндекс.Браузер и Google Chrome.

Для входа в AM TIP компьютер пользователя должен отвечать следующим требованиям:

* 512 МБ свободного дискового пространства на жестком диске;
* стабильное соединение для работы с AM TIP в режиме онлайн;
* открытые порты 443 (HTTPS) и 80 (HTTP);
* монитор, поддерживающий разрешение экрана 1024х768;
* Intel Pentium 1 ГГц (или совместимый аналог) для 32-разрядной операционной системы;
* Intel Pentium 2 ГГц (или совместимый эквивалент) для 64-разрядной операционной системы;
* 1 ГБ свободной оперативной памяти.

Язык разработки – Python 3.10. Использованные библиотеки из официального репозитория пакетов с открытым исходным кодом ([https://pypi.org](https://pypi.org/)):

* Django ([https://pypi.org/project/Django](https://pypi.org/project/Django/));
* Django REST framework ([https://pypi.org/project/djangorestframework](https://pypi.org/project/djangorestframework/));
* Celery ([https://pypi.org/project/celery](https://pypi.org/project/celery/));
* Requests ([https://pypi.org/project/requests](https://pypi.org/project/requests/));
* Pymongo ([https://pypi.org/project/pymongo](https://pypi.org/project/pymongo/));
* Peewee ([https://pypi.org/project/peewee](https://pypi.org/project/peewee/));
* Redis ([https://pypi.org/project/redis](https://pypi.org/project/redis/)).

Язык разработки – JavaScript. Использованные библиотеки из официального репозитория пакетов с открытым исходным кодом ([https://npmjs.org](https://npmjs.org/)):

* TypeScript (<https://www.npmjs.com/package/typescript>);
* Nuxt (<https://www.npmjs.com/package/nuxt>);
* D3 (<https://www.npmjs.com/package/d3>);
* Vue (<https://www.npmjs.com/package/vue>);
* Pinia (<https://www.npmjs.com/package/pinia>).

Язык разработки – JSON, YAML.

# Входные данные

Портал используется для получения данных об угрозах в целях аналитики и оперативного обнаружения, для возможности предотвращения вредоносной активности в системах заказчика. AM TIP применяется также для получения базы решающих правил, которая в свою очередь используется для обнаружения событий в сетевом трафике, захватываемом физической или виртуальной сетевой картой с помощью сетевого интерфейса, работающего по протоколу IP и имеющего IPv4-адрес.

# Выходные данные

Портал предоставляет актуальную подробную информацию об угрозах по CVE, IP-адресам, хэшам, доменам, адресам ресурсов, правилам, техникам и тактикам, данным WHOIS и т.д. В результате пользователи и системы ИБ получают сведения о новых и возникающих угрозах, а также использование данных AM TIP в СЗИ помогают генерировать события, данные о которых могут:

1. выводиться в графический интерфейс СЗИ;
2. отправляться посредством протоколов:
* электронной почты;
* SNMP;
* Syslog;
* CEF.

# Загрузка Портала

Загрузка Портала производится согласно документу «Инструкция по установке AM TIP».