Акционерное общество «Перспективный мониторинг»

(АО «ПМ»)

**AM THREAT INTELLIGENCE PORTAL**

На 12 листах

Москва 2024

Аннотация

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

Содержание

[ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 4](#_Toc159496363)

[1 Общие сведения 5](#_Toc159496364)

[2 Первичный вход в AM TIP 6](#_Toc159496365)

[3 Инструкция по первичной аутентификации в AM TIP 8](#_Toc159496366)

[4 Поиск IoC в AM TIP 9](#_Toc159496367)

[5 Выгрузка отчетов 12](#_Toc159496368)

[5.1 Выгрузка правил 12](#_Toc159496369)

[5.2 Выгрузка отчета по IoC 12](#_Toc159496370)

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

|  |  |
| --- | --- |
| АО «ПМ» | Акционерное общество «Перспективный мониторинг» |
| AM TIP | AM Threat Intelligence Portal |

# 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.

AM TIP 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.

# Первичный вход в AM TIP

Порядок подключения к AM TIP:

* включить компьютер;
* открыть веб-браузер (рекомендованные веб-браузеры для использования: Яндекс.Браузер и Google Chrome);
* в адресной строке веб-браузера ввести адрес AM TIP <https://amtip.ru>;
* далее отобразится главная страница Портала с киберкартой мира, на которой отображается активность компьютерных атак со всего мира на Россию. При нажатии указателя мыши на конкретную страну отображаются рейтинг угроз выбранной страны по отношению к России.

На главной странице Портала отображаются боковые панели:

* ТОП 10 атакующих IP – рейтинг атакующих IP из выбранной на карте страны по отношению к России, с выбранным периодом и источниками в процентах по убыванию;
* ТОП 10 CVE – рейтинг CVE из выбранной на карте страны по отношении к России, с выбранным периодом и источниками в процентах по убыванию, которые чаще всего встречаются в событиях безопасности клиентов Центра мониторинга АО «ПМ»;
* ТОП 10 атакующих стран – рейтинг стран, из которых приходят угрозы по отношению к России, с выбранным периодом и источниками в процентах по убыванию. При использовании фильтра по стране вкладка неактивна, так как на карте будут отображаться угрозы из выбранной страны по отношению к России. При наведении на страну в рейтинге страна выделяется в списке оранжевым цветом, территория на карте сохраняет изначальный цвет, при этом на отмеченной территории появляются прозрачные полоски;
* ТОП 10 угроз – рейтинг связанных угроз из выбранной на карте страны по отношению к России, с выбранным периодом и источниками в процентах по убыванию.

Нажимая на переключатели «Период» над киберкартой мира, можно фильтровать отображаемую информацию за определенный период: день, неделя, месяц. Ретроспективный фильтр по умолчанию находится на положении месяц. Данные для вывода на киберкарту обновляются один раз в сутки. В зависимости от выбора периода меняется киберкарта и рейтинги:

* при нажатии фильтра «День» карта и рейтинги отображают за текущие 24 часа по московскому времени;
* при нажатии фильтра «Неделя» карта и рейтинги отображают за последние 7 дней, включая сегодняшний;
* при нажатии фильтра «Месяц» карта и рейтинги отображают за последние 30 дней, включая сегодняшний.

Период можно выбрать только один.

# Инструкция по первичной аутентификации в AM TIP

Порядок первичной аутентификации в AM TIP:

* пройти аутентификацию в разделе «Логин» (Рисунок 1);

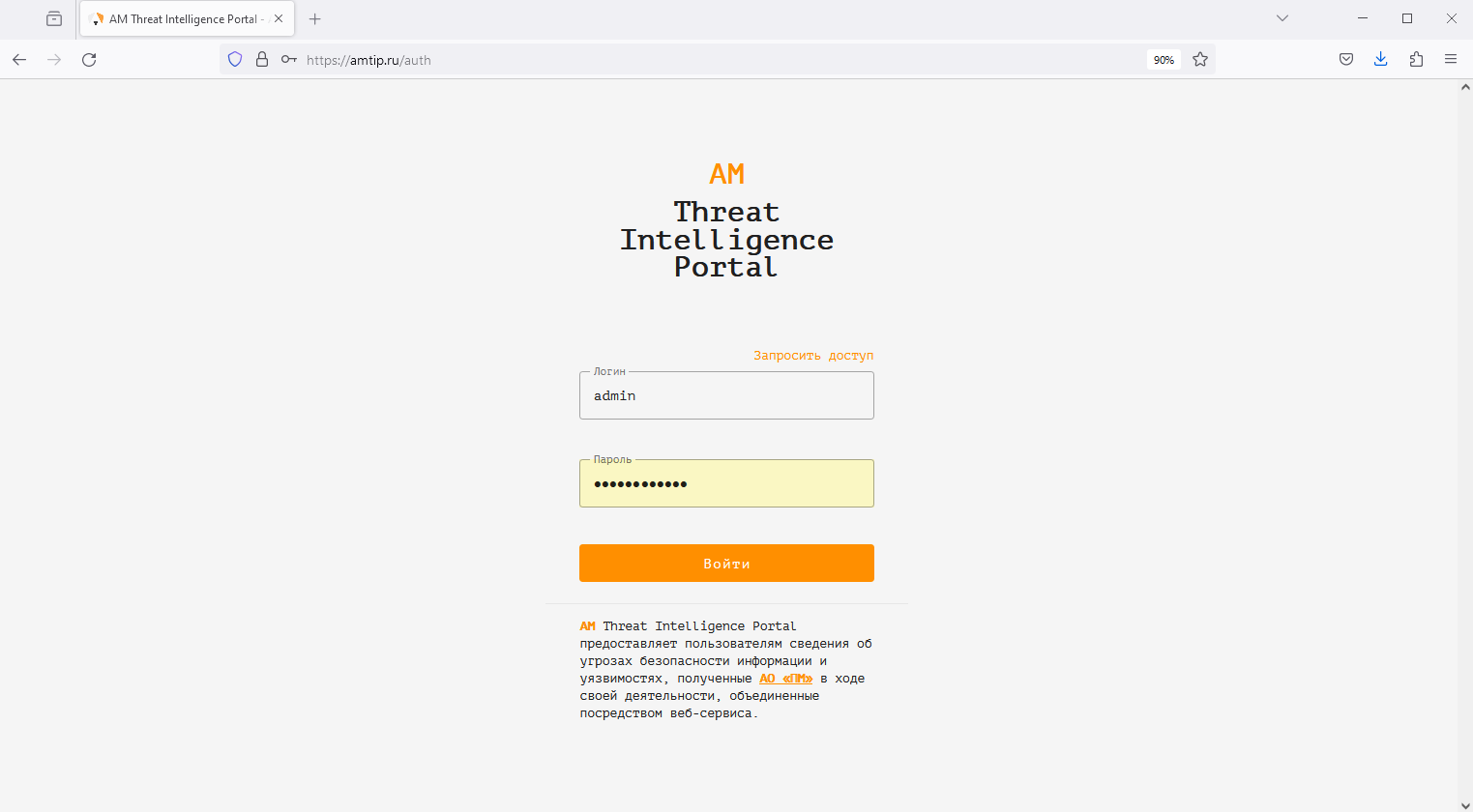


Рисунок 1 – Аутентификация в AM TIP

* в соответствующих полях ввести логин и пароль учетной записи;
* нажать «Войти»;
* при первом подключении к веб-интерфейсу после успешной авторизации имеется возможность сменить пароль. Для этого в окне «Профиль» самостоятельно задать новый пароль. В блоке «Смена пароля» необходимо ввести старый пароль, новый пароль, подтвердить новый пароль и нажать кнопку «Сохранить» (Рисунок 2).

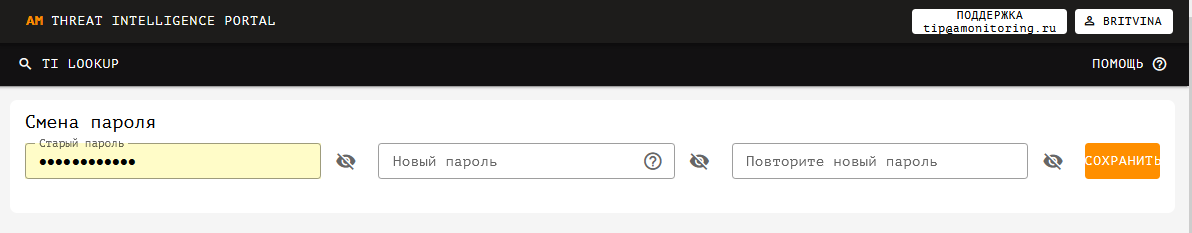


Рисунок 2 – Смена пароля

# Поиск IoC в AM TIP

Поиск по IoC в AM TIP осуществляется в разделе TI LOOKUP. После введения запроса AM TIP распознает тип запрошенного объекта и отобразит результаты расследования с IoC:

1. Обнаруженные угрозы:

* число до / указывает, какое количество антивирусов детектировало данную угрозу;
* число после / указывает, какое количество антивирусов проверяло данную угрозу.

1. Оценка (AM SCORE) окрашивается в один из следующих цветов:

* красный – исследуемый объект может быть классифицирован как вредоносный;
* зеленый – исследуемый объект не может быть классифицирован как вредоносный;
* оранжевый – исследуемый объект имеет статус «недоверенный», содержит рекламу или другие нежелательные материалы.

AM SCORE – шкала для оценки риска:

* AM SCORE < 0.3 зеленый;
* AM SCORE >= 0.3 < 0.7 желтый;
* AM SCORE >= 0.7 красный.

1. Результаты:

* домен верхнего уровня (TLD – Top Level Domain) – это доменные имена верхнего уровня, которые идут сразу после корневого домена (root domain);
* местоположение – местоположение домена;
* метки образца – метки угрозы домена;
* черные списки – черные списки домена;
* категории – категории риска домена из категоризатора;
* связанные IP-адреса – IP-адреса, связанные с доменом;
* поддомены – это отдельные домены, являются частью домена более высокого уровня. Чаще всего поддоменом называют домен третьего уровня.

1. Правила/Сигнатуры:

* sid – уникальный идентификатор правила;
* время изменения – дата последнего изменения правила;
* название – названия правила;
* группы – группы правил;
* TTP – техники и тактики MITRE ATT&CK.

По стрелке в конце строки открывается описание правила:

* краткое описание – краткое описание правила;
* полное описание – полное описание правила;
* критичность – градация критичности правила;
* типы атаки – тип атаки (например, спам, вредоносное ПО, атака на трафик);
* платформы – используемые платформы: Linux, Windows, any;
* исходный текст – отображение текста правила: SNORT, [SURICATA](https://testing.tip.am.int/help/glossary/suricata), [YARA](https://testing.tip.am.int/help/glossary/yara), [OSSEC](https://testing.tip.am.int/help/glossary/ossec).

1. Обзор:

* Whois – полная информация о регистрации домена;
* связанные IP-адреса;
* поддомены.

1. Ресурсные записи DNS (для домена):

* блок содержит типы ресурсных записей, значение и ttl (время кэширования данных другими DNS-серверами).

1. Связи:

* каждый связанный IoC содержит дату и количество антивирусов, нашедших данную угрозу/количество антивирусов, проверивших данную угрозу.

1. Загрузки:

* правила обнаружения угроз [SNORT](https://testing.tip.am.int/help/glossary/snort), [SURICATA](https://testing.tip.am.int/help/glossary/suricata), [YARA](https://testing.tip.am.int/help/glossary/yara), [OSSEC](https://testing.tip.am.int/help/glossary/ossec);
* отчет по IoC=ip-адрес в формате [STIX](https://testing.tip.am.int/help/glossary/stix). Файл STIX содержит всю информацию о IoC, включенную в Граф.

1. Граф:

* построен в формате STIX, который является языком описания для обмена данными TI и выводит набор сущностей, а также определяет возможные типы взаимосвязей между ними.

# Выгрузка отчетов

## Выгрузка правил

Для выгрузки правил из базы решающих правил форматов Snort, Suricata, YARA, OSSEC в формате TXT необходимо:

* произвести поиск по IoC в AM TIP в разделе TI LOOKUP;
* AM TIP распознает тип запрошенного объекта и отобразит результаты расследования с IoC;
* появится блок «Загрузки», в котором нужно выбрать интересующий формат правила и нажать на TXT.

## Выгрузка отчета по IoC

Для выгрузки отчета по IoC в формате STIX нужно:

* произвести поиск по IoC в AM TIP в разделе TI LOOKUP;
* AM TIP распознает тип запрошенного объекта и отобразит результаты расследования с IoC;
* появится блок «Загрузки», в котором нужно выбрать IoC правила и нажать на STIX.