СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

Интеллектуальная система управления киберугрозами

Сделано в СБЕРе

SBER TIP

Интеллектуальная система управления киберугрозами: модули и функции

СБЕР КИБЕР БЕЗОПАСНОСТЬ

МОДУЛЬ ОБОГАЩЕНИЯ

Использует механизмы обогащения информации о киберугрозах из платных и открытых источников, а также из смежных систем мониторинга, учета и защиты инфраструктуры банка.

МОДУЛЬ СБОРА

Отвечает за сбор структурированных и неструктурированных данных, нормализацию и постоянную актуализацию информации о киберугрозах в сети интернет, включая теневой сегмент (DarkNet).

МОДУЛЬ BRAND MONITORING

Выявляет фишинговые ресурсы и контент, дискредитирующий бренд банка в сети интернет, включая теневой сегмент (DarkNet) с последующим оповещением CERT.

МОДУЛЬ УПРАВЛЕНИЯ СЦЕНАРИЯМИ БЕЗОПАСНОСТИ

Связывает киберугрозы со сценариями детектирования, что позволяет обнаруживать и минимизировать киберугрозы в инфраструктуре банка на разных стадиях атаки.

МОДУЛЬ АНАЛИТИКИ И ИНТЕГРАЦИЙ

Позволяет проецировать обнаруженные киберугрозы на инфраструктуру банка (индикаторы компрометации, YARA-правила, SIGMA-правила, CVE/BDU) и оценивать возможный масштаб их влияния.

Знаете ли ВЫ, что произойдет завтра? МЫ – знаем!

МОДУЛЬ АДМИНИСТРИРОВАНИЯ

Позволяет управлять ролевой моделью, словарями для хранения описаний разных сущностей, либо настройками системы.

МОДУЛЬ ВИЗУАЛИЗАЦИИ

Создает оперативные виджеты на основании хранимых атрибутов описания киберугроз либо результатов их анализа.

МОДУЛЬ «GRAPH»

Позволяет проводить аналитику с использованием интерактивного графа, выявляя в автоматическом режиме неявные связи между объектами киберугроз.

МОДУЛЬ УЧЁТА

Позволяет хранить информацию о результатах аналитики и атрибуты киберугроз (Case, Actor, Campaign, Malware, Vulnerability, TTP, IOC, DataLeaked, Phishing и др.).

МОДУЛЬ УПРАВЛЕНИЯ СКАНИРОВАНИЕМ

Отвечает за полную автоматизацию процесса сканирования элементов инфраструктуры в режиме Vulnerability и Compliance и последующую обработку полученных результатов.

МОДУЛЬ УПРАВЛЕНИЯ РИСКАМ

Позволяет автоматизировать работу с рисками: заведение рисков в учетной системе HPSM, расчет рейтинга риска, обновление полей риска, связь риска с уязвимыми элементами, контроль исполнения риска по данным сканирования.

Преимущества продукта:

- Использование ML-подходов для анализа и приоритезации киберугроз.
- Реализация полного цикла работы с киберугрозами от обнаружения, расширенного анализа и проецирования на ИТ-инфраструктуру, до последующей оценки влияния и создания сценариев реагирования.
- Встроенный модуль управления уязвимостями, содержащий полную информацию об элементах ИТ-инфраструктуры, позволяющий в автоматическом режиме определить векторы.
- Возможность работы со структурированной и не структурированной информацией за счет поддержки известных форматов (STIX/TAXII, JSON, XML и др.), а также механизмов нормализации.
- Гибкость разработанного продукта для расширения функциональных возможностей существующих модулей
- Независимость от конкретных коммерческих решений: реализовано большое количество универсальных коннекторов для подключения.
- Отсутствие аналога разработанной системы анализа киберугроз, которая в одной платформе объединяла бы в себе совокупность созданных модулей и аналитических алгоритмов.
- Система обладает патентом на территории РФ.

Результаты внедрения продукта:

- Сокращено временя сбора информации и увеличен объем обрабатываемых данных за счет средств автоматизации сбора и постоянной актуализация информации о киберугрозах.
- Сокращено время анализа обрабатываемой информации за счет автоматизации обогащения информации о киберугрозах за счет интеграции с подписками и внутренними системами защиты и мониторинга инфраструктуры.
- Сокращено время анализа на первичную обработку актуальных киберугроз из всего поступающего потока информации за счет применения ML-подходов, выполняющих приоритезацию (скоринг) поступающей информации.
- Сокращено времени анализа информации за счет централизованного учета информации о киберугрозах и гибких инструментов аналитики (неявные связи, интерактивный граф, фильтры, агрегации).
- Своевременное обнаружение и оценка масштаба влияния за счет проецирования обнаруженных киберугроз на инфраструктуру.
- Сформирован централизованный банк знаний о киберугрозах, позволяющий повышать компетенции профильных подразделений и уровень осведомленности об актуальных киберугрозах.

Интеллектуальная система управления киберугрозами в цифрах
Сентябрь 2023

СБЕР КИБЕР БЕЗОПАСНОСТЬ

66 000+
фишинговых доменов обнаружено

100+
фишинговых доменов в неделю направляется в CERT для блокировки

400 000+
сообщений в день о продаже банковской информации

100+
сообщений в день потенциально представляют угрозу для банка

4200+
исторических кейсов с описанием киберугроз

120+
сообщений о киберугрозах в день

300 000+
описаний уязвимостей

100+
уязвимостей в день

60+
Use Cases

800+
правил корреляции

Интеллектуальная система управления киберугрозами: эволюция развития SBER TIP

СБЕР КИБЕР БЕЗОПАСНОСТЬ

SBER TIP

TIP 3.0

TIP 1.0

TIP 2.0

TIP 0.1

2023

МОДУЛЬ **Сетевой достижимости**

МОДУЛЬ **Моделирования атак**

2022

МОДУЛЬ **Управления уязвимостями**

МОДУЛЬ **Управления рискам**

МОДУЛЬ **Учёта инфраструк-туры**

МОДУЛЬ **Управления сканированием**

МОДУЛЬ **Управления периметром**

2020

МОДУЛЬ **Brand monitoring**

МОДУЛЬ **Data leak**

МОДУЛЬ **Учета злоумышлен-ников**

МОДУЛЬ **Визуализации**

МОДУЛЬ **Обогащения**

МОДУЛЬ **Аналитики и интеграций**

МОДУЛЬ **Графовой аналитики**

МОДУЛЬ **Управления сценариями безопасности**

2018

МОДУЛЬ **Сбора**

МОДУЛЬ **Учёта**

МОДУЛЬ **Отчётности**

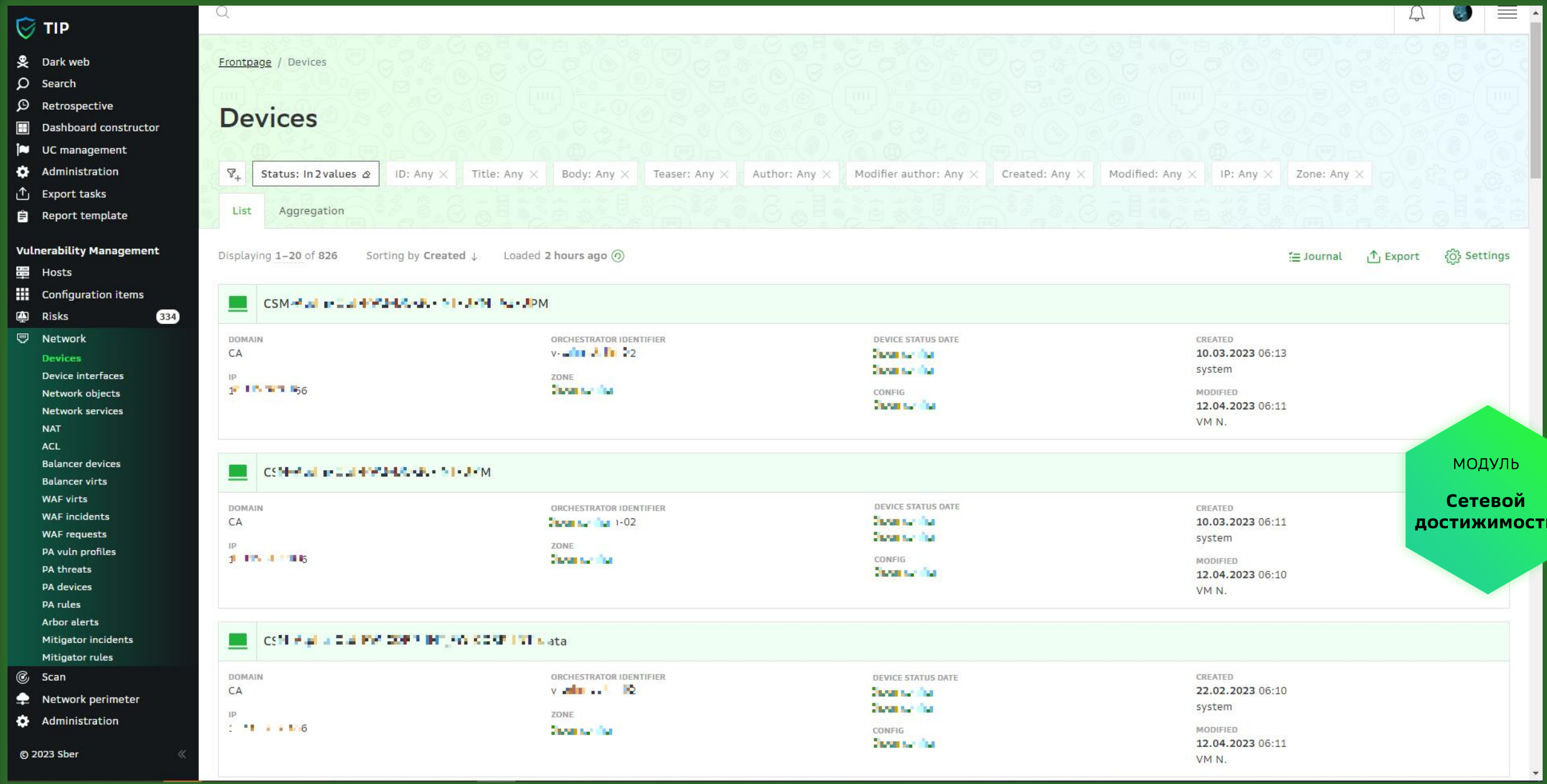
МОДУЛЬ **Администриро вания**

SBER TIP: информация для принятия решений всегда перед глазами

СБЕР КИБЕР БЕЗОПАСНОСТЬ

SBER TIP: модуль сетевой достижимости. Разработка 2023 года

СБЕР КИБЕР БЕЗОПАСНОСТЬ

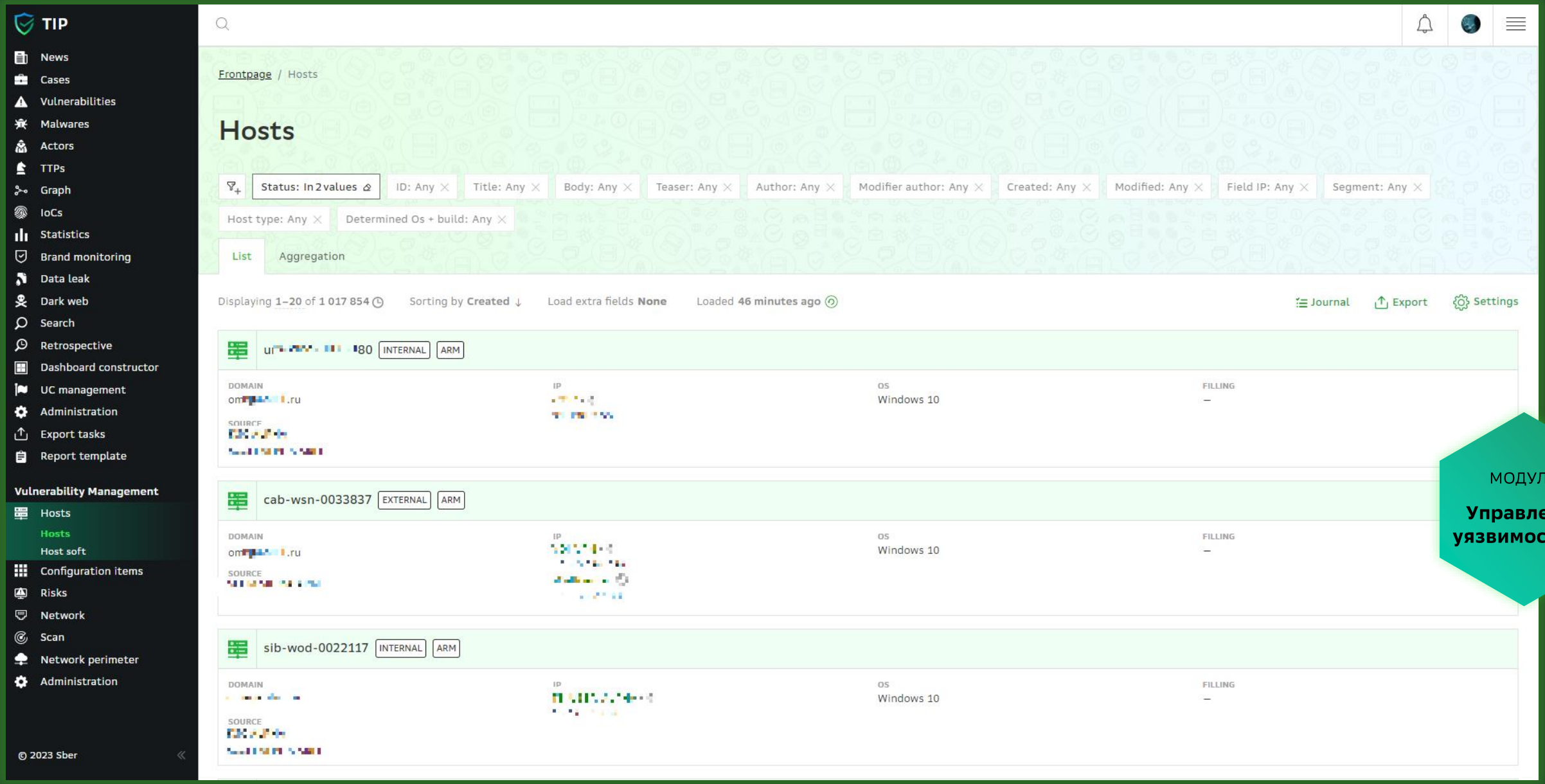


МОДУЛЬ

Сетевой достижимости

SBER TIP: ключевой модуль 2022 года – Управление уязвимостями

СБЕР КИБЕР БЕЗОПАСНОСТЬ

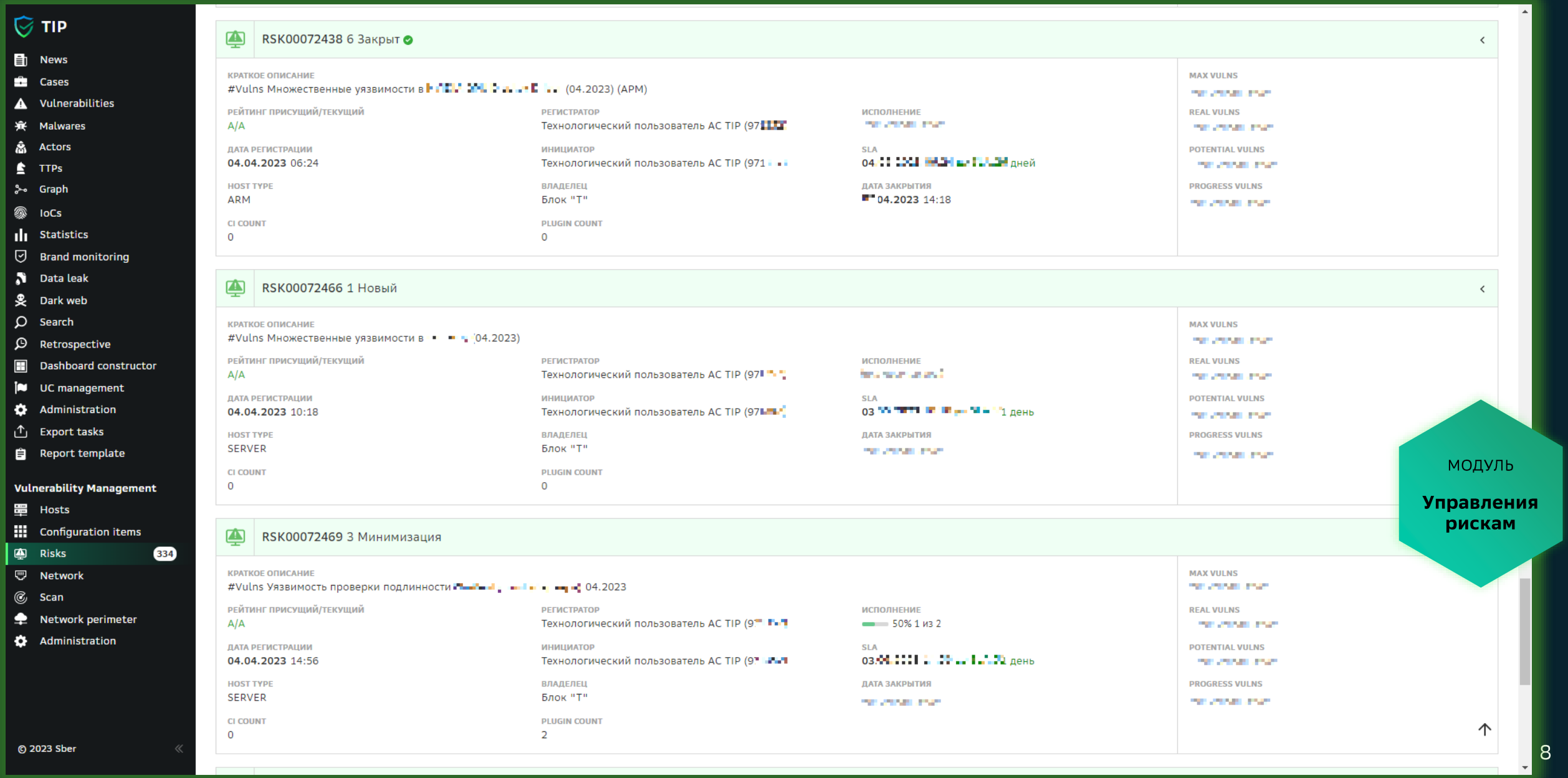


МОДУЛЬ

Управления уязвимостями

SBER TIP: модуль Управления рисками

СБЕР КИБЕР БЕЗОПАСНОСТЬ

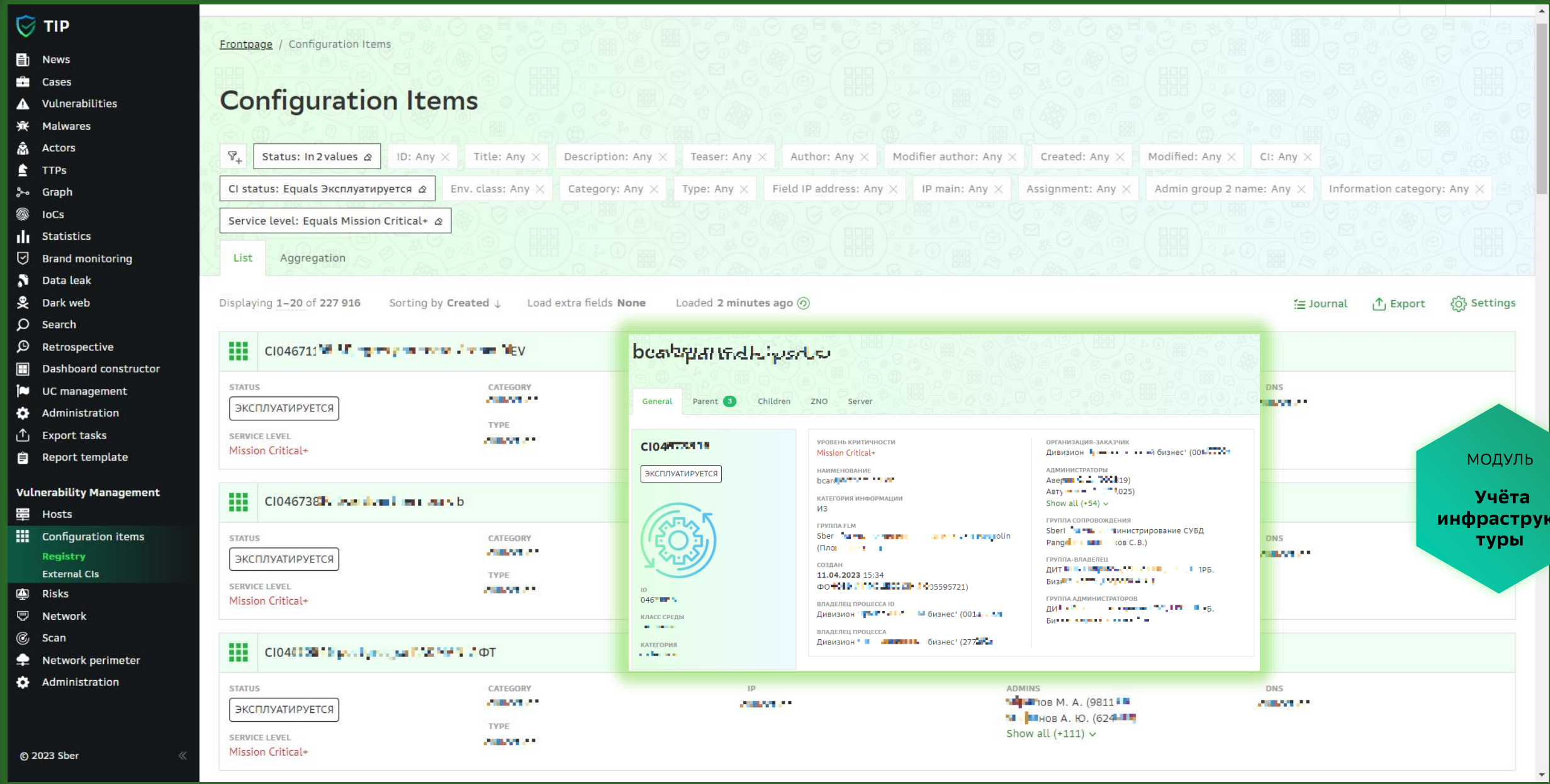


МОДУЛЬ

Управления рискам

SBER TIP: модуль Учета инфраструктуры

СБЕР КИБЕР БЕЗОПАСНОСТЬ

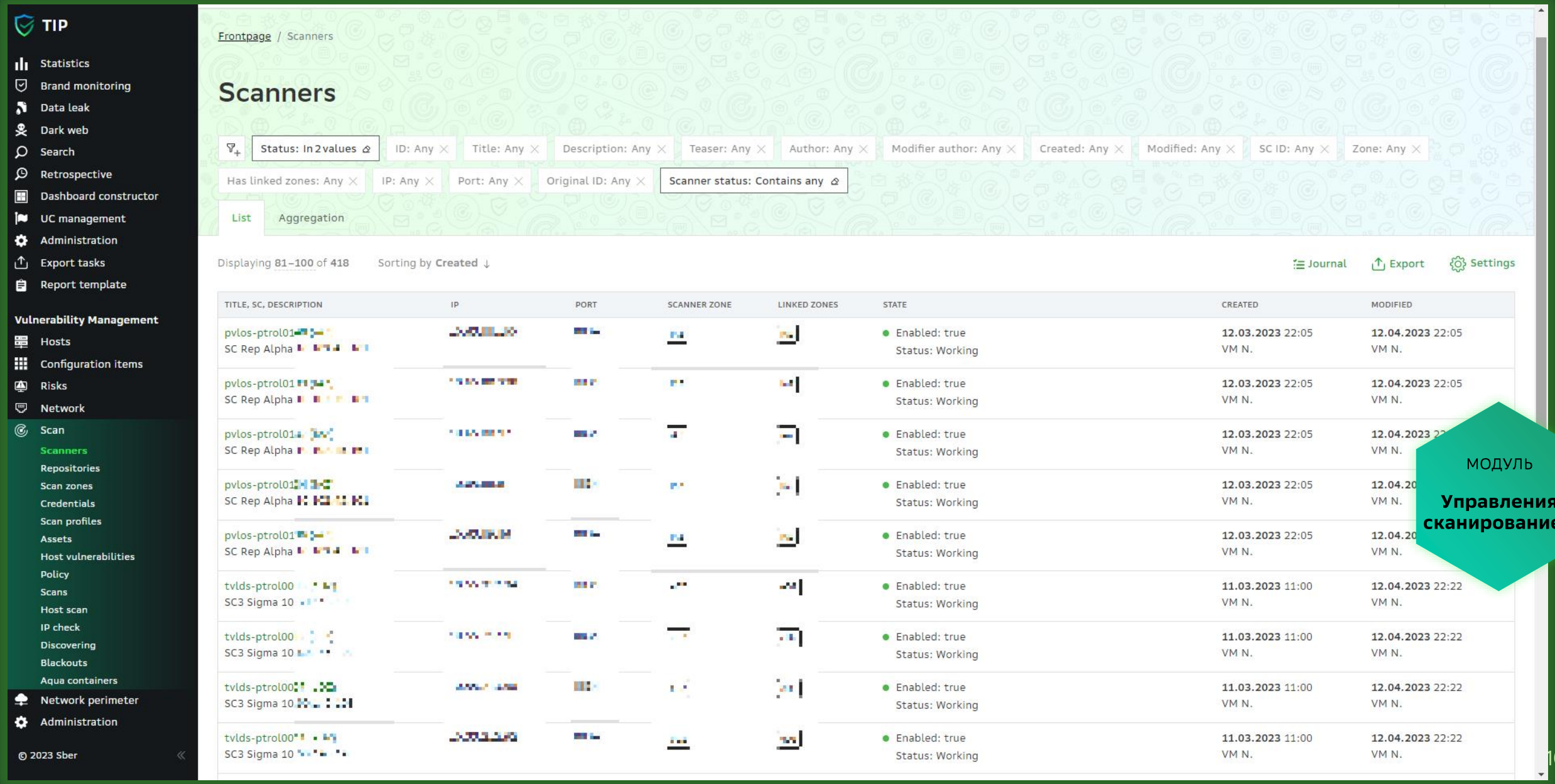


МОДУЛЬ

Учёта инфраструк-туры

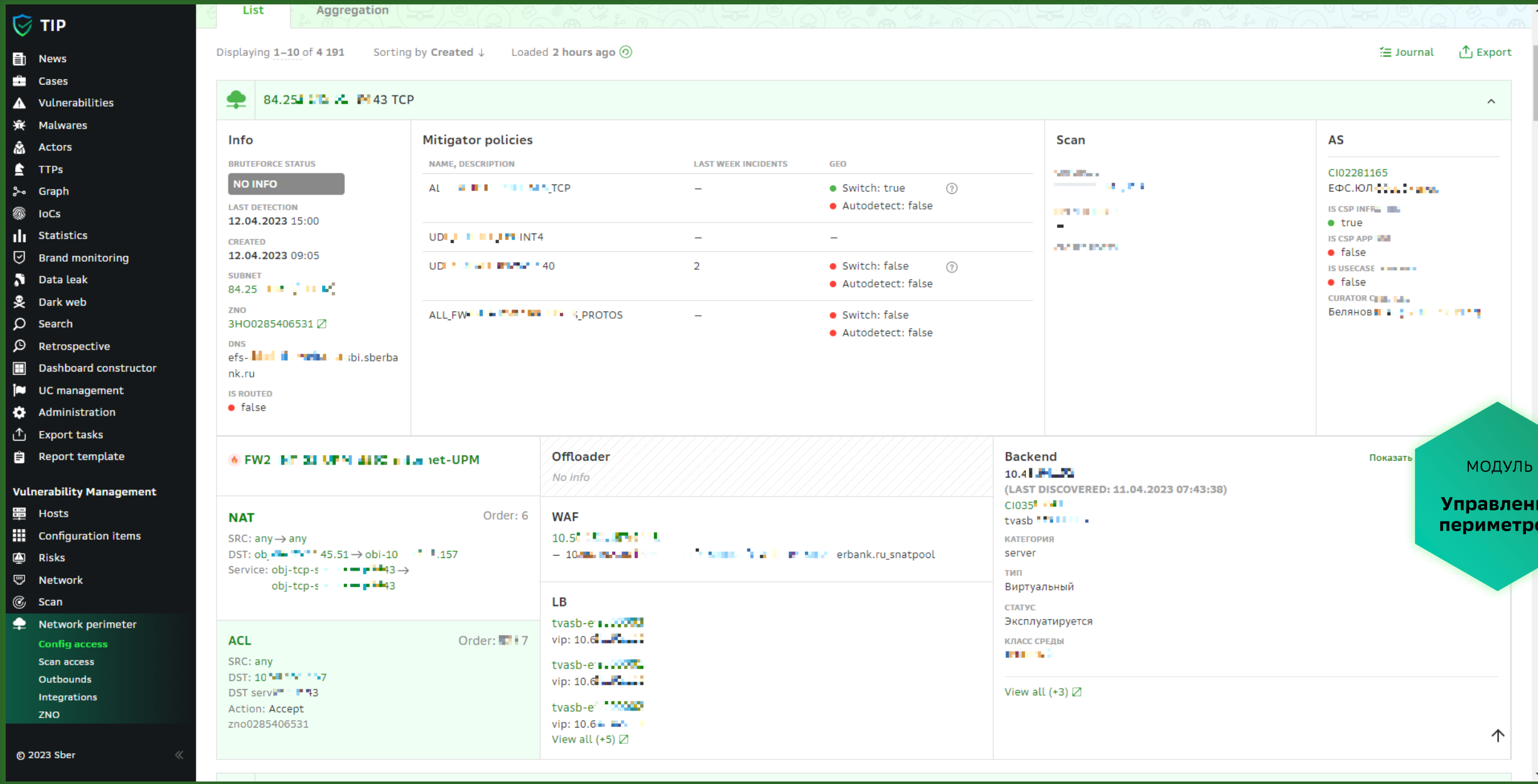
SBER TIP: модуль Управления сканированием

СБЕР КИБЕР БЕЗОПАСНОСТЬ



SBER TIP: модуль Управления периметром

СБЕР КИБЕР БЕЗОПАСНОСТЬ



МОДУЛЬ

Управления периметром