



**СБЕР**  
КИБЕР  
БЕЗОПАСНОСТЬ

# Интеллектуальная система управления киберугрозами

Сделано в СБЕРЕ



# Интеллектуальная система управления киберугрозами: модули и функции

## 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 АДМИНИСТРИРОВАНИЯ

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

## 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.

## 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.

## МОДУЛЬ ВИЗУАЛИЗАЦИИ


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

## Преимущества продукта:

- Использование ML-подходов для анализа и приоритизации 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 времени 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 приоритизацию (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.



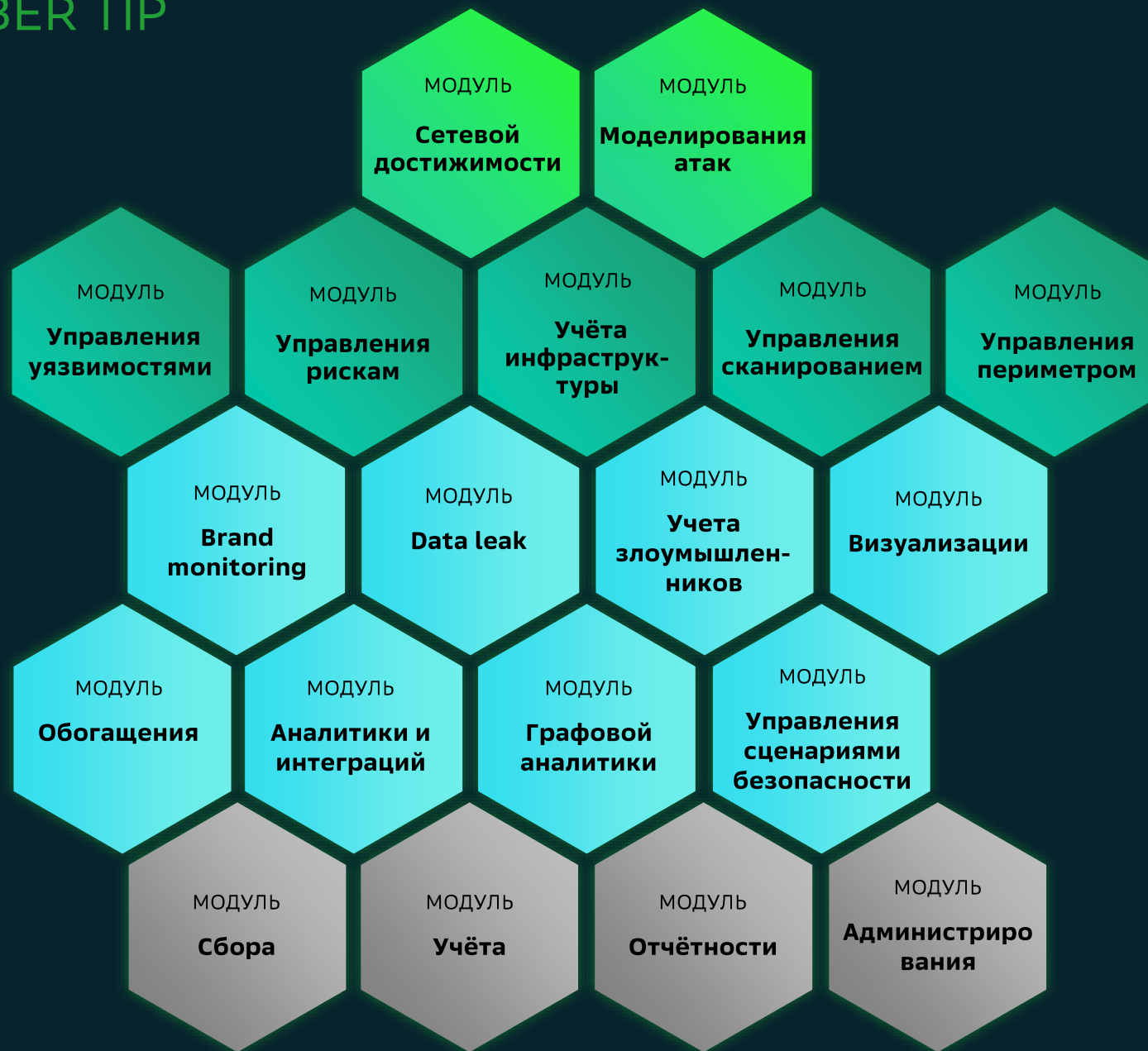
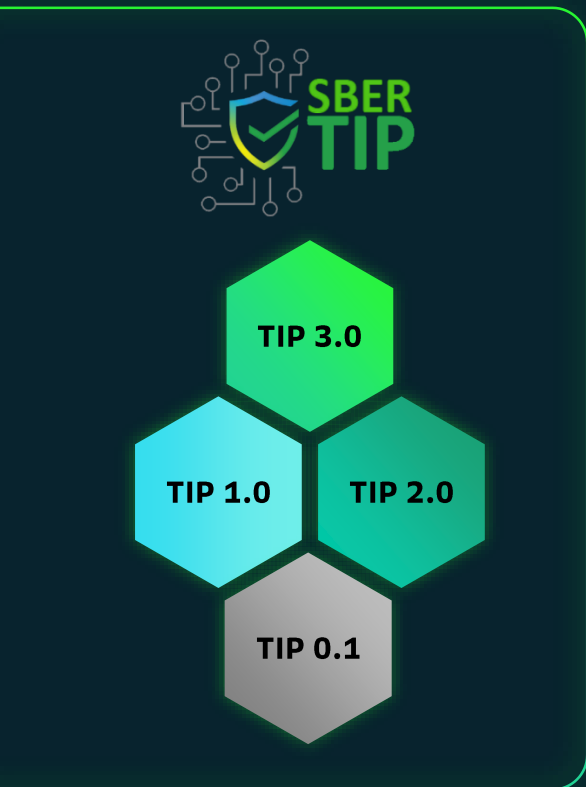
**Знаете ли Вы,  
что произойдет  
завтра? Мы – знаем!**

# Интеллектуальная система управления киберугрозами в цифрах

## Сентябрь 2023



# Интеллектуальная система управления киберугрозами: эволюция развития SBERTIP



2023

2022

2020

2018

- TIP - 5 ЛЕТ
- News
- Cases
- Vulnerabilities
- Malwares
- Actors
- TTPs
- Investigate
- Graph
- IoCs
- Statistics
- Brand monitoring
- Data leak
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template

## SBER THREAT INTELLIGENCE PLATFORM

4 235 CASES

↑ 14 today



### TOP-5 sectors

- Телекоммуникации
- Информационные технологии
- Промышленность и производство
- Финансовый
- Государственный

LESS MORE

Day Week Month Year

Sber Vulnerabilities  
**282 837**  
↑ 1 today

Risks  
**4 211**  
↑ 23 today

Malwares  
**2 426**  
↑ 3 today

Retrospective  
**5 751**  
↑ 13 today

TTPs  
**963**

UC Rules  
**760**  
↑ 1 today

Data leaks  
**248 946**  
↑ 358 today

Phishing domains  
**66 361**  
↑ 4 today

190 081 CYBERSECURITY NEWS

↑ 84 today

- blueteamalerts/9717: Inside the Mind of a Ransomware Operator: Ransomed ...** [Malware]  
49 SIMILAR HIGH PRIORITY 14.09.2023 19:19:33
- blueteamalerts/9693: "Building Resilience": U.S. returns from second de ...** [No Threat]  
48 SIMILAR NO PRIORITY 13.09.2023 08:19:51
- blueteamalerts/9690: Sandboxing ImageIO media parsing in macOS https:// ...** [No Threat]  
48 SIMILAR NO PRIORITY 13.09.2023 07:20:05
- blueteamalerts/9714: SaaS attack chain - The shadow workflow's evil twi ...** [TTP]  
48 SIMILAR LOW PRIORITY 14.09.2023 14:21:00

26 010 367 IOCS

TYPE	ALIVE	WHITELIST	TOTAL	TODAY
REGISTRY	39		39	
FILEPATH	448	2	450	
EMAIL	7 462	6	7 441	↑ 27
URI	2 241 276	166	2 240 533	↑ 909
DNS	2 653 103	783 685	3 436 548	↑ 238



- TIP
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template
- Vulnerability Management
  - Hosts
  - Configuration items
  - Risks 334
- Network
  - Devices
  - Device interfaces
  - Network objects
  - Network services
  - NAT
  - ACL
  - Balancer devices
  - Balancer virts
  - WAF virts
  - WAF incidents
  - WAF requests
  - PA vuln profiles
  - PA threats
  - PA devices
  - PA rules
  - Arbor alerts
  - Mitigator incidents
  - Mitigator rules
- Scan
- Network perimeter
- Administration

Frontpage / Devices

## Devices

Status: In 2 values | ID: Any | Title: Any | Body: Any | Teaser: Any | Author: Any | Modifier author: Any | Created: Any | Modified: Any | IP: Any | Zone: Any

List | Aggregation

Displaying 1-20 of 826 | Sorting by Created ↓ | Loaded 2 hours ago

Journal | Export | Settings

CSM-...			
DOMAIN CA	ORCHESTRATOR IDENTIFIER V-...	DEVICE STATUS DATE ...	CREATED 10.03.2023 06:13 system
IP ...	ZONE ...	CONFIG ...	MODIFIED 12.04.2023 06:11 VM N.
CSM-...			
DOMAIN CA	ORCHESTRATOR IDENTIFIER ...	DEVICE STATUS DATE ...	CREATED 10.03.2023 06:11 system
IP ...	ZONE ...	CONFIG ...	MODIFIED 12.04.2023 06:10 VM N.
CSM-...			
DOMAIN CA	ORCHESTRATOR IDENTIFIER V-...	DEVICE STATUS DATE ...	CREATED 22.02.2023 06:10 system
IP ...	ZONE ...	CONFIG ...	MODIFIED 12.04.2023 06:11 VM N.

МОДУЛЬ  
Сетевой  
ДОСТИЖИМОСТИ

- TIP
- News
- Cases
- Vulnerabilities
- Malwares
- Actors
- TTPs
- Graph
- IoCs
- Statistics
- Brand monitoring
- Data leak
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template
- Vulnerability Management**
  - Hosts
  - Hosts**
  - Host soft
  - Configuration items
  - Risks
  - Network
  - Scan
  - Network perimeter
  - Administration

Frontpage / Hosts

## Hosts

Status: In 2 values | ID: Any | Title: Any | Body: Any | Teaser: Any | Author: Any | Modifier author: Any | Created: Any | Modified: Any | Field IP: Any | Segment: Any

Host type: Any | Determined Os + build: Any

List | Aggregation

Displaying 1–20 of 1 017 854 | Sorting by Created | Load extra fields None | Loaded 46 minutes ago

Journal | Export | Settings

ID	INTERNAL	ARM	DOMAIN	IP	OS	FILLING
ur-180	INTERNAL	ARM	on-ru		Windows 10	—
SOURCE						
cab-wsn-0033837	EXTERNAL	ARM	on-ru		Windows 10	—
SOURCE						
sib-wod-0022117	INTERNAL	ARM			Windows 10	—
SOURCE						

МОДУЛЬ  
Управления  
уязвимостями

- TIP
- News
- Cases
- Vulnerabilities
- Malwares
- Actors
- TTPs
- Graph
- IoCs
- Statistics
- Brand monitoring
- Data leak
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template
- Vulnerability Management**
- Hosts
- Configuration items
- Risks** 334
- Network
- Scan
- Network perimeter
- Administration

**RSK00072438 6 Закрыт**

КРАТКОЕ ОПИСАНИЕ  
#Vulns Множественные уязвимости в [progress bar] (04.2023) (APM)

РЕЙТИНГ ПРИСУЩИЙ/ТЕКУЩИЙ A/A	РЕГИСТРАТОР Технологический пользователь AC TIP (97 [progress bar])	ИСПОЛНЕНИЕ [progress bar]
ДАТА РЕГИСТРАЦИИ 04.04.2023 06:24	ИНИЦИАТОР Технологический пользователь AC TIP (97 [progress bar])	SLA 04 [progress bar] дней
HOST TYPE ARM	ВЛАДЕЛЕЦ Блок "Т"	ДАТА ЗАКРЫТИЯ 04.2023 14:18
CI COUNT 0	PLUGIN COUNT 0	

MAX VULNS [progress bar]  
REAL VULNS [progress bar]  
POTENTIAL VULNS [progress bar]  
PROGRESS VULNS [progress bar]

**RSK00072466 1 Новый**

КРАТКОЕ ОПИСАНИЕ  
#Vulns Множественные уязвимости в [progress bar] (04.2023)

РЕЙТИНГ ПРИСУЩИЙ/ТЕКУЩИЙ A/A	РЕГИСТРАТОР Технологический пользователь AC TIP (97 [progress bar])	ИСПОЛНЕНИЕ [progress bar]
ДАТА РЕГИСТРАЦИИ 04.04.2023 10:18	ИНИЦИАТОР Технологический пользователь AC TIP (97 [progress bar])	SLA 03 [progress bar] 1 день
HOST TYPE SERVER	ВЛАДЕЛЕЦ Блок "Т"	ДАТА ЗАКРЫТИЯ [progress bar]
CI COUNT 0	PLUGIN COUNT 0	

MAX VULNS [progress bar]  
REAL VULNS [progress bar]  
POTENTIAL VULNS [progress bar]  
PROGRESS VULNS [progress bar]

**RSK00072469 3 Минимизация**

КРАТКОЕ ОПИСАНИЕ  
#Vulns Уязвимость проверки подлинности [progress bar] 04.2023

РЕЙТИНГ ПРИСУЩИЙ/ТЕКУЩИЙ A/A	РЕГИСТРАТОР Технологический пользователь AC TIP (9 [progress bar])	ИСПОЛНЕНИЕ 50% 1 из 2
ДАТА РЕГИСТРАЦИИ 04.04.2023 14:56	ИНИЦИАТОР Технологический пользователь AC TIP (9 [progress bar])	SLA 03 [progress bar] день
HOST TYPE SERVER	ВЛАДЕЛЕЦ Блок "Т"	ДАТА ЗАКРЫТИЯ [progress bar]
CI COUNT 0	PLUGIN COUNT 2	

MAX VULNS [progress bar]  
REAL VULNS [progress bar]  
POTENTIAL VULNS [progress bar]  
PROGRESS VULNS [progress bar]

МОДУЛЬ  
Управления  
рискам



- TIP
- News
- Cases
- Vulnerabilities
- Malwares
- Actors
- TTPs
- Graph
- IoCs
- Statistics
- Brand monitoring
- Data leak
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template
- Vulnerability Management**
- Hosts
- Configuration items**
- Registry
- External CIs
- Risks
- Network
- Scan
- Network perimeter
- Administration

Frontpage / Configuration Items

## Configuration Items

Filtering options: Status: In 2 values, ID: Any, Title: Any, Description: Any, Teaser: Any, Author: Any, Modifier author: Any, Created: Any, Modified: Any, CI: Any, CI status: Equals Эксплуатируется, Env. class: Any, Category: Any, Type: Any, Field IP address: Any, IP main: Any, Assignment: Any, Admin group 2 name: Any, Information category: Any, Service level: Equals Mission Critical+

List Aggregation

Displaying 1-20 of 227 916 | Sorting by Created ↓ | Load extra fields None | Loaded 2 minutes ago

Journal Export Settings

ID	STATUS	CATEGORY	TYPE	SERVICE LEVEL
CI046711	ЭКСПЛУАТИРУЕТСЯ			Mission Critical+
CI046738	ЭКСПЛУАТИРУЕТСЯ			Mission Critical+
CI046739	ЭКСПЛУАТИРУЕТСЯ			Mission Critical+

### beabpauwldhispwlo

General Parent 3 Children ZNO Server

**CI046711**  
ЭКСПЛУАТИРУЕТСЯ

**УРОВЕНЬ КРИТИЧНОСТИ**  
Mission Critical+

**НАИМЕНОВАНИЕ**  
bsar

**КАТЕГОРИЯ ИНФОРМАЦИИ**  
ИЗ

**ГРУППА FLM**  
Sber (Пло

**СОЗДАН**  
11.04.2023 15:34  
ФО

**ВЛАДЕЛЕЦ ПРОЦЕССА ID**  
Дивизион бизнес' (001

**ВЛАДЕЛЕЦ ПРОЦЕССА**  
Дивизион бизнес' (277

**ОРГАНИЗАЦИЯ-ЗАКАЗЧИК**  
Дивизион бизнес' (00

**АДМИНИСТРАТОРЫ**  
Авер (19)  
Авту (025)  
Show all (+54)

**ГРУППА Сопровождения**  
Sber (министрирование СУБД  
Pang (ков С.В.)

**ГРУППА-ВЛАДЕЛЕЦ**  
ДИТ IP6.  
Биз

**ГРУППА АДМИНИСТРАТОРОВ**  
Ди .6.  
Би

МОДУЛЬ  
Учёта  
инфраструк-  
туры

- TIP
- Statistics
- Brand monitoring
- Data leak
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template

- Vulnerability Management
  - Hosts
  - Configuration items
  - Risks
  - Network
  - Scan
    - Scanners**
    - Repositories
    - Scan zones
    - Credentials
    - Scan profiles
    - Assets
    - Host vulnerabilities
    - Policy
    - Scans
    - Host scan
    - IP check
    - Discovering
    - Blackouts
    - Aqua containers
  - Network perimeter
  - Administration

Frontpage / Scanners

## Scanners

List Aggregation

Displaying 81–100 of 418

Sorting by Created ↓

Journal

Export

Settings

TITLE, SC, DESCRIPTION	IP	PORT	SCANNER ZONE	LINKED ZONES	STATE	CREATED	MODIFIED
pvlos-ptrol01 SC Rep Alpha					● Enabled: true Status: Working	12.03.2023 22:05 VM N.	12.04.2023 22:05 VM N.
pvlos-ptrol01 SC Rep Alpha					● Enabled: true Status: Working	12.03.2023 22:05 VM N.	12.04.2023 22:05 VM N.
pvlos-ptrol01 SC Rep Alpha					● Enabled: true Status: Working	12.03.2023 22:05 VM N.	12.04.2023 22:05 VM N.
pvlos-ptrol01 SC Rep Alpha					● Enabled: true Status: Working	12.03.2023 22:05 VM N.	12.04.2023 22:05 VM N.
pvlos-ptrol01 SC Rep Alpha					● Enabled: true Status: Working	12.03.2023 22:05 VM N.	12.04.2023 22:05 VM N.
tvlds-ptrol00 SC3 Sigma 10					● Enabled: true Status: Working	11.03.2023 11:00 VM N.	12.04.2023 22:22 VM N.
tvlds-ptrol00 SC3 Sigma 10					● Enabled: true Status: Working	11.03.2023 11:00 VM N.	12.04.2023 22:22 VM N.
tvlds-ptrol00 SC3 Sigma 10					● Enabled: true Status: Working	11.03.2023 11:00 VM N.	12.04.2023 22:22 VM N.
tvlds-ptrol00 SC3 Sigma 10					● Enabled: true Status: Working	11.03.2023 11:00 VM N.	12.04.2023 22:22 VM N.

МОДУЛЬ  
Управления  
сканированием

# SBER TIP: модуль Управления периметром

- TIP
- News
- Cases
- Vulnerabilities
- Malwares
- Actors
- TTPs
- Graph
- IoCs
- Statistics
- Brand monitoring
- Data leak
- Dark web
- Search
- Retrospective
- Dashboard constructor
- UC management
- Administration
- Export tasks
- Report template
- Vulnerability Management
- Hosts
- Configuration items
- Risks
- Network
- Scan
- Network perimeter
- Config access
- Scan access
- Outbounds
- Integrations
- ZNO

List Aggregation

Displaying 1-10 of 4 191    Sorting by Created ↓    Loaded 2 hours ago

Journal    Export

**84.25** 43 TCP

Info	Mitigator policies	Scan	AS															
<p><b>BRUTEFORCE STATUS</b></p> <p>NO INFO</p> <p><b>LAST DETECTION</b> 12.04.2023 15:00</p> <p><b>CREATED</b> 12.04.2023 09:05</p> <p><b>SUBNET</b> 84.25</p> <p><b>ZNO</b> 3HO0285406531</p> <p><b>DNS</b> efs-...; ibi.sberba nk.ru</p> <p><b>IS ROUTED</b> false</p>	<table border="1"> <thead> <tr> <th>NAME, DESCRIPTION</th> <th>LAST WEEK INCIDENTS</th> <th>GEO</th> </tr> </thead> <tbody> <tr> <td>AL ..._TCP</td> <td>—</td> <td>Switch: true Autodetect: false</td> </tr> <tr> <td>UD...INT4</td> <td>—</td> <td>—</td> </tr> <tr> <td>UD...40</td> <td>2</td> <td>Switch: false Autodetect: false</td> </tr> <tr> <td>ALL_FW..._PROTOS</td> <td>—</td> <td>Switch: false Autodetect: false</td> </tr> </tbody> </table>	NAME, DESCRIPTION	LAST WEEK INCIDENTS	GEO	AL ..._TCP	—	Switch: true Autodetect: false	UD...INT4	—	—	UD...40	2	Switch: false Autodetect: false	ALL_FW..._PROTOS	—	Switch: false Autodetect: false	<p><b>Scan</b></p>	<p><b>AS</b></p> <p>CI02281165 ЕФС.ЮЛ</p> <p>IS CSP INFR true</p> <p>IS CSP APP false</p> <p>IS USECASE false</p> <p>CURATOR Белянов</p>
NAME, DESCRIPTION	LAST WEEK INCIDENTS	GEO																
AL ..._TCP	—	Switch: true Autodetect: false																
UD...INT4	—	—																
UD...40	2	Switch: false Autodetect: false																
ALL_FW..._PROTOS	—	Switch: false Autodetect: false																

**FW2** net-UPM

NAT	Offloader	Backend
<p>Order: 6</p> <p>SRC: any → any</p> <p>DST: obj-... 45.51 → obj-10... 157</p> <p>Service: obj-tcp-s → obj-tcp-s</p>	<p>No info</p>	<p>10.4</p> <p>(LAST DISCOVERED: 11.04.2023 07:43:38)</p> <p>CI035</p> <p>tvasb</p> <p>КАТЕГОРИЯ server</p> <p>ТИП Виртуальный</p> <p>СТАТУС Эксплуатируется</p> <p>КЛАСС СРЕДЫ</p> <p>View all (+3)</p>
<p><b>ACL</b> Order: 7</p> <p>SRC: any</p> <p>DST: 10...7</p> <p>DST serv...93</p> <p>Action: Accept</p> <p>zno0285406531</p>	<p><b>WAF</b></p> <p>10.5... erbank.ru_snatpool</p>	
	<p><b>LB</b></p> <p>tvasb-e vip: 10.6</p> <p>tvasb-e vip: 10.6</p> <p>tvasb-e vip: 10.6</p> <p>View all (+5)</p>	

МОДУЛЬ  
Управления  
периметром