BI.ZONE
Cybersecurity

DATASHEET

TI.SENSORS

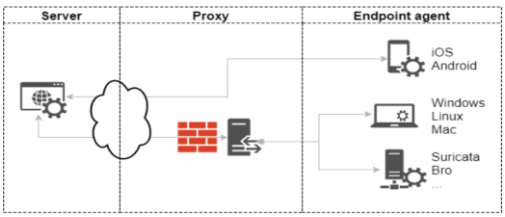
Платформа взаимодействия с конечными устройствами

Обнаружение угроз безопасности

Инвентаризация агентских устройств

Расследование инцидентов

Управление средствами защиты



Платформа **TI.SENSORS** предназначена для обеспечения безопасности рабочих станций, серверов и мобильных устройств. Система состоит из двух основных компонентов:

- Сервер управления, который установлен в защищенном контуре сети;
- Агенты, которые установлены на конечных устройствах (ПК с операционными системами **Windows, Linux, MacOS;** мобильные устройства).

Функциональность системы

Система позволяет динамически управлять функциональными модулями, установленными на конечных устройствах, а также доставлять на агенты собственные (разработанные специалистами клиента) модули.
Платформа **TI.SENSORS** способна выполнять следующие основные задачи:

- **Инвентаризация.** Модуль предназначен для сбора инвентаризационной информации об агенте и его окружении (установленное оборудование, сетевые интерфейсы, программное обеспечение и т.д.).
- **Скриптинг.** Модуль позволяет выполнять команды на удаленном устройстве. Поддерживаются скрипты **CMD, Scheme, JavaScript, Python.**
- **Поиск идентификаторов компрометации.** Модуль позволяет производить удаленный поиск идентификаторов компрометации в файлах, процессах и реестре **Windows** с использованием алгоритмов нечеткого хэширования и **YARA**-правил.
- **Мониторинг WinAPI.** Модуль позволяет отслеживать все запускаемые **Windows API** функции и может быть использован для обнаружения возможного заражения конечного устройства.
- **Мониторинг изменения объектов файловой системы.** Модуль дает возможность отслеживать все изменения объектов файловой системы (копирование, удаление, изменение, создание).
- **Мониторинг сетевых подключений.** Модуль позволяет производить мониторинг всех устанавливаемых сетевых подключений с дообогащением информации по данным соединениям.
- **Мониторинг процессов.** Модуль позволяет отслеживать все возникающие в системе процессы с указанием дополнительной информации по инициаторам процесса, исполняемому файлу и т.д.
- **Мониторинг изменений объектов реестра.** Модуль позволяет производить мониторинг всех изменений объектов реестра с получением дополнительной информации относительно данных изменений.

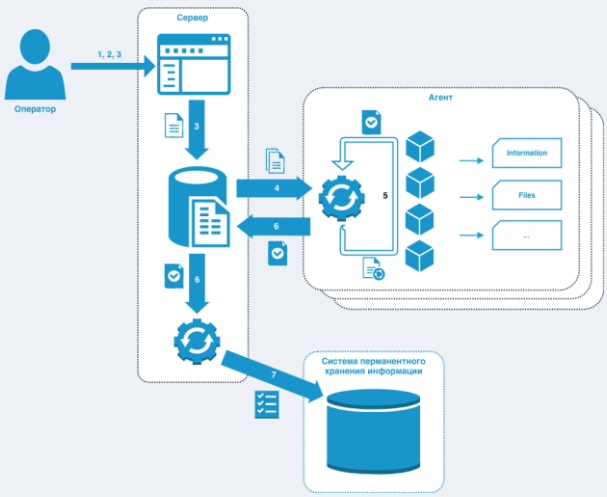
Требования к агентам

Операционная система	Windows, Linux, MacOS, Android, IOS
Оперативная память	Не менее 70Мб
Процессор	Без ограничений
Сетевое подключение	Без ограничений
Место на диске	Не менее 50Мб

Требования к серверу (из расчета на поддержку **10 000** агентов)

Операционная система	CentOS | RHEL
Кол-во ядер	4 и более
ОЗУ	32 Гб и более
Дисковое пространство	1 Тб и более
СУБД	Oracle DB | PostgreSQL

Описание процесса работы с системой



1. Оператор открывает в браузере интерфейс управления инфраструктурой.
2. Оператор просматривает текущее состояние инфраструктуры, в том числе:
   - перечень доступных агентов;
   - исполняемые и выполненные задачи;
   - Предупреждения системы уведомлений.
3. Оператор создает новые задачи, в частности:
   - выбирает требуемую категорию и тип задачи;
   - настраивает параметры работы;
   - назначает задачу на агента или группу агентов.
4. Сервер по защищенным каналам передает задачу агентам.
5. Агенты запускают полученную задачу и возвращают результаты работы (промежуточные или полные).
6. Сервер анализирует результаты, используя правила формирования уведомлений.
7. Внешняя система перманентного хранения информации получает результаты от сервера.