AV SOFT


LOKI
Система мониторинга
кибератак на базе
технологии Deception
Краткое техническое
описание

LOKI

## Общая информация

AVSOFT LOKI относится к системам на базе технологии Deception. Этот класс систем используется для мониторинга и блокировки кибератак в ИТ-инфраструктуре организации.

На базе единой централизованной платформы создаются цифровые двойники «ловушки» реальных устройств, которые инициируют подключение кибератак к себе, оберегая реальные сервисы организации.

## Основные задачи

- Мониторинг кибератак на любые типы цифровых двойников
- Блокирока распространения кибератак в ИТ-инфраструктуре
- Взаимодействие с злоумышленником и сбор информации
- Оповещение службы информационной безопасности
- Проверка и анализ собранных артефактов

## Общий алгоритм работы

1

Пользователь сканирует подсети своей ИТ-инфраструктуры, где расположены датчики системы.

2

Система автоматически выбирает подходящие типы ловушек из своего каталога. Пользователь при необходимости может их изменить.

3

После выбора типов ловушек система автоматически рассчитывает их максимально допустимое количество в зависимости от количества ресурсов. Пользователь, при необходимости, может изменить его.

4

Ловушки развертываются в подсети, а затем отображаются на видеокарте в системе.

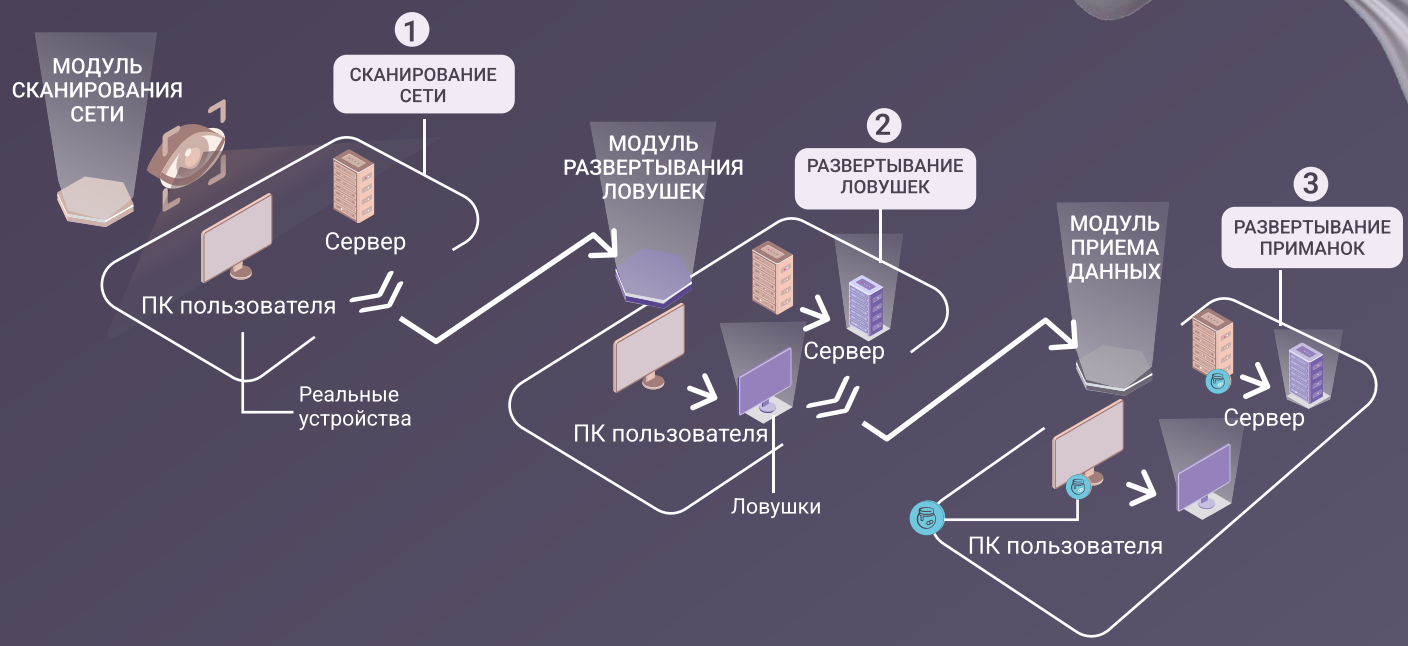
5

Идет генерация и загрузка приманок на реальные пользовательские задания.

6

Осуществляется развертывание приманок на рабочие места пользователей и отображение их на графической карте в системе

## Схема работы




## Типы ловушек

### Низкоинтерактивные

Имитируют сетевые протоколы взаимодействия устройства

### Высокоинтерактивные

Имитируют операционную систему устройства, сервисы и протоколов сетевого взаимодействия

## Виды ловушек

Ловушки могут имитировать любые объекты ИТ-инфраструктуры

- WEB-сервер
- FTP-сервер
- Почтовый сервер
- Рабочее место
- Межсетевой экран
- Маршрутизатор
- Коммутатор
- Промышленные станки
- Интернет вещей
- База данных

Для обеспечения максимального охвата поддерживаемого оборудования организации в ложной инфраструктуре ловушки поддерживают следующие архитектуры процессоров:

- Intel x86-based
- AMD64
- ARM
- MIPS
- Power System
- Эльбрус

Все ловушки осуществляют сбор сетевой телеметрии, дополнительных данных в соответствии с имитируемым протоколом:

- Исходный IP-адрес
- Исходный порт
- Порт назначения
- Протокол
- Информацию по email (адрес отправителя, адреса получателей, заголовок и текст письма, вложения)
- Информацию по HTTP/ HTTPS соединениям (тип, адрес, user-agent, данные запроса)
- Информацию по запросам к СУБД (текст запроса, ответ на запрос)
- Учетные данные при наличии в соответствующем протоколе
- Ловушки также собирают собственный сетевой трафик для последующего анализа перехваченных сетевых атак

Ловушки также осуществляют сбор собственного сетевого трафика для последующего анализа перехватываемых сетевых атак.

| Наименование протокола | Предположительный порт |
|---|---|
| SMTP | 25 |
| POP3 | 110 |
| POP3S | 995 |
| IMAP | 143 |
| IMAPS | 993 |
| HTTP | 80 |
| HTTPS | 443 |
| SSH | 22 |
| Telnet | 23 |
| RDP | 3389 |
| VNC | 5900 |
| FTP | 21 |
| TFtp | 69 |
| SMB | 139 |
| MySQL | 3306 |
| PostgreSQL | 5432 |
| MongoDB | 27017 |
| Socks5 | 27017 |
| SIP | 5060 |

## Техническая спецификация

Развертывание LOKI на нескольких виртуальных машинах

| Параметры | Минимальные требования |
|---|---|
| **Сервер** | |
| Количество ядер процессора | 4 |
| Оперативная память | 12 GB |
| Диск | 200 GB |
| Сеть | 10/100/1000 Мбит/с (2шт.) |
| **Сенсор (10 ловушек)** | |
| Количество ядер процессора | 2 |
| Оперативная память | 4 GB |
| Диск | 100 GB |
| Сеть | 10/100/1000 Мбит/с (2шт.) |

Развертывание системы LOKI можно осуществлять, как на виртуальных машинах, так и физических машинах.