AV SOFT

Система защиты ИТ-инфраструктуры от кибератак на базе технологии Deception

Функционально-технические требования

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5
Тел.: +7 (495) 988-92-25
E-mail: office@avsw.ru
www.avsw.ru/about/contacts

Авторское право

Версия документа

Февраль 28, 2023.
Функционально-технические требования v1.0

СОДЕРЖАНИЕ

1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
1.	Deception	Технология имитации ложных целей для привлечения к ним кибератак и защиты реальных устройств.
2.	Ловушка	Цифровая копия реального сервиса или устройства в ИТ-инфраструктуре организации.
3.	Приманка	Значимые для злоумышленника данные на рабочем месте пользователя, которые он может использовать для атаки на ловушку.
4.	Сенсор	Модуль сканирования и развертывания ловушек в подсети ИТ-инфраструктуры.

2 Сокращения

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Перечень сокращений

№	Сокращение	Значение
1.	AD	Active Directory
2.	API	Application programming interface
3.	REST	Representational state transfer
4.	SIEM	Security information and event management
5.	АРМ	Автоматизированное рабочее место
6.	ОС	Операционная система
7.	ПО	Программное обеспечение
8.	СУБД	Система управления базами данных

3 Общие положения

3.1 Определение

Система защиты ИТ-инфраструктуры на базе технологии Deception AVSOFT LOKI (далее – Система LOKI) предназначена для распространения ловушек и приманок в подсетях организации с целью привлечения к ним кибератак злоумышленника.

3.2 Назначение

Система предназначена для выполнения следующих задач:

- мониторинг кибератак в подсетях организации
- распространение приманок на рабочие места пользователей
- блокировка распространения кибератак в ИТ-инфраструктуре
- взаимодействие с злоумышленником и сбор информации
- оповещение службы информационной безопасности
- проверка и анализ собранных артефактов

4 Функциональные требования

4.1 Приманки

4.1.1 Система должна поддерживать автоматическое распространение приманок на АРМ и серверы под управлением ОС Windows с помощью смежных систем: Active Directory.

4.1.2 Система должна поддерживать механизмы ручного распространения приманок на хосты под управлением ОС Windows с использованием подготовленных администратором системы дистрибутивов (exe, msi).

4.1.3 Система должна поддерживать механизмы ручного распространения приманок на хосты под управлением ОС Linux с использованием подготовленных администратором системы дистрибутивов.

4.1.4 Система должна обеспечивать функционирование приманок, содержащих сохраненные данные подключения к следующим сервисам:

- СУБД
- браузеры
- веб-сервисам (HTTP, HTTPS)
- сервисам удаленного управления (SSH)
- службам удаленных рабочих столов (RDP)

4.1.5 Система должна обеспечивать функционирование следующих типов приманок, содержащих сохраненные данные на рабочих станциях и серверах с ОС Microsoft Windows:

- в файлах конфигурации службы подключения к удаленному рабочему столу Microsoft Windows (.rdp)
- в текстовых файлах
- в системном реестре
- в скриптах bash (.sh)

4.1.6 Система должна обеспечивать функционирование следующих приманок, содержащих сохраненные данные на рабочих станциях и серверах с ОС Linux:

- в виде истории SSH-, FTP-, HTTP-подключений
- в файлах

4.1.7 Система должна поддерживать расписание обновления приманок.

4.2 Ловушки

4.2.1 Система должна поддерживать конфигурирование ловушек из единой консоли.

4.2.2 Сервер-ловушки должны эмулировать следующие типы ловушек:

- Файловый сервер
- IoT/IIoT девайсы
- Принтер
- Устройства IP телефонии
- IP – камеры
- Операционную систему Windows
- Операционную систему Linux
- СУБД MS SQL
- СУБД Mongo DB

4.2.3 Система должна обеспечивать функционирование на серверах ловушках следующих типов протоколов:

- SSH
- RDP
- HTTP
- HTTPS (SSL/TLS)

- FTP
- IMAP
- SMTP
- POP3
- SNMP
- NTP
- Telnet

4.2.4 Система должна обеспечить возможность настройки следующих параметров для ловушки «DataBase»:

- тип базы данных
- порт подключения
- возможность добавления учетных данных для аутентификации на ловушки

4.2.5 Система должна обеспечить возможность настройки следующих параметров для ловушки «HTTP/HTTPS»:

- порт подключения
- используемый шаблон страницы
- возможность добавления учетных данных для аутентификации на ловушке

4.2.6 Система должна обеспечить возможность эмулировать наличие уязвимостей на развернутой ловушке.

4.2.7 Система должна регистрировать все попытки аутентификации на серверах-ловушках по всем типам сетевых служб и протоколов, поддерживаемых сервером-ловушкой.

4.2.8 Система должна сохранять артефакты инцидентов, происходящих на серверах-ловушках.

4.3 Единая панель управления

4.3.1 Система должна обеспечивать мониторинг состояния компонентов и централизованное управление всеми компонентами Системы LOKI.

4.3.2 Система должна обеспечивать сканирование подсетей для определения типов устройств и подбора рекомендуемых ловушек.

4.3.3 Система должна иметь возможность обеспечить перемещения злоумышленника по всей инфраструктуре ложных целей.

4.3.4 Система должна отображать последовательность взаимодействия злоумышленника с ложной инфраструктурой в хронологическом порядке (строить timeline).

4.3.5 Система должна поддерживать блокировку атак в рамках атакованной подсети при помощи системы агентов.

4.3.6 Система должна иметь REST API-интерфейс для взаимодействия с другими системами.

4.3.7 Система должна поддерживать интеграцию с системой Sandbox для передачи файлов созданных или загруженных на ловушках для проверки.

4.3.8 Система должна иметь ролевую модель с возможностью кастомизации.

4.3.9 Система должна иметь возможность интеграции со службой Microsoft Active Directory.

4.3.10 Система должна иметь возможность отправки событий метрик в SIEM системы по протоколу syslog.