PALITRA

Система централизованного управления и мониторинга

Функциональные характеристики

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

Март 24, 2023.
Функциональные характеристики 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.	Инсталляция	Программное обеспечение компании АВ Софт

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.	ICAP	Internet content adaptation protocol
4.	REST	Representational state transfer

3 Общие положения

3.1 Определение

Система централизованного управления и мониторинга AVSOFT PALITRA (далее – Система PALITRA) предназначена для управления отдельными инсталляциями продуктов компании АВ Софт.

3.2 Назначение

Система предназначена для выполнения следующих задач:

- Агрегация и хранение логов
- Построение отчетов
- Управление настройками
- Сбор статистической информации
- Отслеживание состояния функциональных модулей
- Отображение всех проверок в едином интерфейсе системы
- Централизованное распространение настроек на все инсталляции

4 Описание внешней информационной среды

4.1 Информационные объекты

Информационные объекты, к которым применимо разрабатываемое ПО:

- инсталляции
- системные логи
- файлы настроек

4.2 Каналы передачи данных

Система PALITRA должна взаимодействовать со следующими каналами передачи данных:

- API интерфейс

4.3 Взаимодействие с другими системами

Способы и связи для информационного обмена между подсистемами и модулями Системы PALITRA описаны в таблице 3.

Таблица 3. Протоколы взаимодействия

№	Протокол	Описание
1.	HTTPS	Подключение к интерфейсу управления системой
2.	Kerberos	Аутентификация пользователей
3.	LDAP	Аутентификация пользователей
4.	REST API	Для взаимодействия с внешними системами и сервисами.
5.	SSH	Протокол для удалённого подключения к серверу, на котором функционирует система

5 Модуль сбора и анализа логов

5.1 Подсистема должна позволять выполнять сбор системных логов.

5.2 По системным логам подсистема должна фиксировать следующие данные:

- Дата и время
- Уровень события
- Тип события

5.3 Подсистема должна отображать весь файловый поток от всех инсталляций.

5.4 По каждой проверке файла в инсталляциях должна собираться следующая информация:

- Дата и время
- Инсталляция
- Наименование файла
- Источник
- Тип источника
- IP источника
- Группа IP
- Вердикт
- Статус

6 Модуль централизованного управления настройками

6.1 Подсистема должна обеспечивать централизованное распространение настроек на отдельные инсталляции.

6.2 Подсистема должна обеспечивать управление следующими видами настроек:

- Общие
- Пользователи
- Политики
- Почтовый трафик
- ICAP
- Исследования
- Ключи API
- Серверы
- Оповещения
- SIEM
- Спутники
- Файловое хранилище

7 Единая панель управления

7.1 Подсистема должна обеспечивать мониторинг состояния компонентов и централизованное управление всеми компонентами Системы PALITRA.

7.2 Подсистема должна иметь REST API-интерфейс, позволяющий осуществлять добавление инсталляций в Систему PALITRA.

7.3 Подсистемы должна иметь ролевую модель с возможностью кастомизации.

7.4 Подсистема должна иметь возможность интеграции со службой AD.

7.5 Подсистема должна иметь возможность экспортирования и импортирования настроек Системы PALITRA.

7.6 Подсистема должна осуществлять мониторинг системных событий и состояния программных модулей.

7.7 Подсистема должна иметь журнал доступа и регистрировать все попытки авторизации в системе посредством веб-интерфейса и API ключей.