**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
TDS Storage**

**ГТДС.00009-01**

**ОПИСАНИЕ РЕАЛИЗАЦИИ**

**СОДЕРЖАНИЕ**

[Аннотация 2](#_Toc48843630)

[1. Назначение ПО 2](#_Toc48843631)

[2. Программно-аппаратные среды функционирования ПО 2](#_Toc48843632)

[3. Общие принципы функционирования ПО 3](#_Toc48843633)

[4. Реализация ПО 5](#_Toc48843634)

# Аннотация

Настоящий документ содержит описание реализации программного обеспечения TDS Storage ГТДС.00009-01 (далее – ПО).

# Назначение ПО

ПО - комплексное решение предназначено для выявления современных высокотехнологичных атак на ранней стадии, обеспечения процесса threat hunting (охота на угрозы), оптимизации процессов реагирования на инциденты и их последующего расследования внутри корпоративной, так и технологической инфраструктуры. Оно определяет заражения, которые пропускают стандартные средства защиты: антивирусы, межсетевые экраны, системы предотвращения вторжений. Применение TDS Storage существенно снижает риски организации, помогая вовремя выявить и предотвратить хищения, финансовые мошенничества, попытки шпионажа, утечку конфиденциальной информации и другие инциденты.

# Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

1. Аппаратные среды:
	1. Сервера со следующими техническими требованиями:

Таблица 1 – Технические требования для TDS Storage

|  |  |
| --- | --- |
| **TDS Storage** |  |
| **CPU** | 3.8 GHz, 6 C (2 threads per core), 12 MB |
| **RAM, GB** | 64 GB, RDIMM |
| **HDD, GB\*\*** | 4 х 1,2Тбайт, 10000 об/мин, SAS 12 Гбит/с |
| **Network** |  |
| **Mgmt Ethernet** | 1. Ethernet
 |

1. Виртуальные среды:
	1. Hyper-V;
	2. Vmware Esxi;
	3. Qemu;
	4. Xen-server.
2. Использование браузеров для доступа к системе:
	1. Windows Internet Explorer версии 8.0 и выше;
	2. Google Chrome версии 4.0 и выше;
	3. Mozilla Firefox версии 3.5 и выше;
	4. Apple Safari версии 4.0 и выше;
	5. Opera версии 10.5 и выше;
	6. iOS Safari версии 3.2 и выше;
	7. Opera Mobile версии 11.0 и выше;
	8. Google Chrome for Android версии 11.0 и выше;
	9. Mozilla Firefox for Android версии 26.0 и выше;
	10. Windows Internet Explorer Mobile версии 10.0 и выше.

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript.

# Общие принципы функционирования ПО

На рисунке 1 изображены общие принципы функционирования ПО TDS Storage
ГТДС.00009-01 с остальными модулями TDS.



Рисунок 1. Общие принципы функционирования ПО

# Реализация ПО

**Архитектурно решение состоит из следующих модулей:**

**TDS Sensor**

Sensor предназначен для анализа входящих и исходящих пакетов данных. Он позволяет выявить взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Для работы Sensor использует собственные сигнатуры и поведенческие правила.

**Особенности системы:**

* Постоянно обновляемые базы – информация из киберразведки и системы криминалистики;
* Единый интерфейс с тикет-системой;
* Интеграция с почтой/icap;
* Анализ трафика до 20 Gb/s;
* Возможность виртуальной установки/HW Appliance;
* Интеграция с SIEM и другими системами.

**TDS Sensor Industrial**

Sensor Industrial предназначен для анализа входящих и исходящих пакетов данных. Он позволяет выявить взаимодействие зараженных устройств с командными центрами злоумышленников, общие сетевые аномалии и необычное поведение устройств. Для работы Sensor Industrial использует собственные сигнатуры и поведенческие правила.

**Особенности системы:**

* Постоянно обновляемые базы – информация из киберразведки и системы криминалистики;
* Единый интерфейс с тикет-системой;
* Интеграция с почтой/icap;
* Анализ трафика до 20 Gb/s;
* Возможность виртуальной установки/HW Appliance;
* Интеграция с SIEM и другими системами.

**TDS Polygon**

Данная система предназначена для поведенческого анализа подозрительных объектов в безопасной среде. Полученные по электронной почте или скачанные из интернета файлы проверяются до попадания на компьютеры пользователей. Применение технологий машинного обучения позволяет выявить ранее неизвестные вредоносные программы без использования сигнатур, а также блокировать их доставку пользователям.

**Особенности системы:**

* Запатентованная технология обнаружения обхода песочницы;
* Эмуляция действий пользователей;
* Специально подготовленные образы для обнаружения 0-Day уязвимостей и различного вида ВПО (вредоносного программного обеспечения);
* Анализ файлов с измененными расширениями;
* Запатентованный низкоуровневый монитор, выявляющий все возможные действия в том числе и выполнение кода на уровне CPU;
* Дешифровка запароленных архивов с паролем в теле письма/вложенном файле/по словарю;
* Ретроспективный анализ.

**TDS Huntbox**

Центр управления, мониторинга, хранения событий и обновлений, устанавливаемый внутри инфраструктуры заказчика. Huntbox интегрируется с другими компонентами комплекса
TDS (Sensor, Polygon, Huntpoint) и значительно расширяет функционал решения за счет новых возможностей:

**Особенности системы**

* Оркестрация всех компонентов TDS и управлением ими из единого интерфейса;
* Анализ больших данных, выявление новых инструментов и инфраструктуры атакующих;
* Хранение логов и аналитической информации по инцидентам;
* Визуализация инцидента на ранней стадии атаки;
* Удаленное реагирование на конечных станциях;
* Внутренний Threat Hunting (охота на угрозы) по логам;
* Сбор криминалистических данных для расследования инцидентов.

**TDS Storage**

Данная система предназначена для обеспечения гибкого масштабирования архитектуры системы для наращивания производительности в случае необходимости.