AVSOFT ATHENA

Система защиты от
целенаправленных атак

О КОМПАНИИ



Компания АВ Софт была основана
в 2010 году и активно развивается
в сфере информационной безопасности.

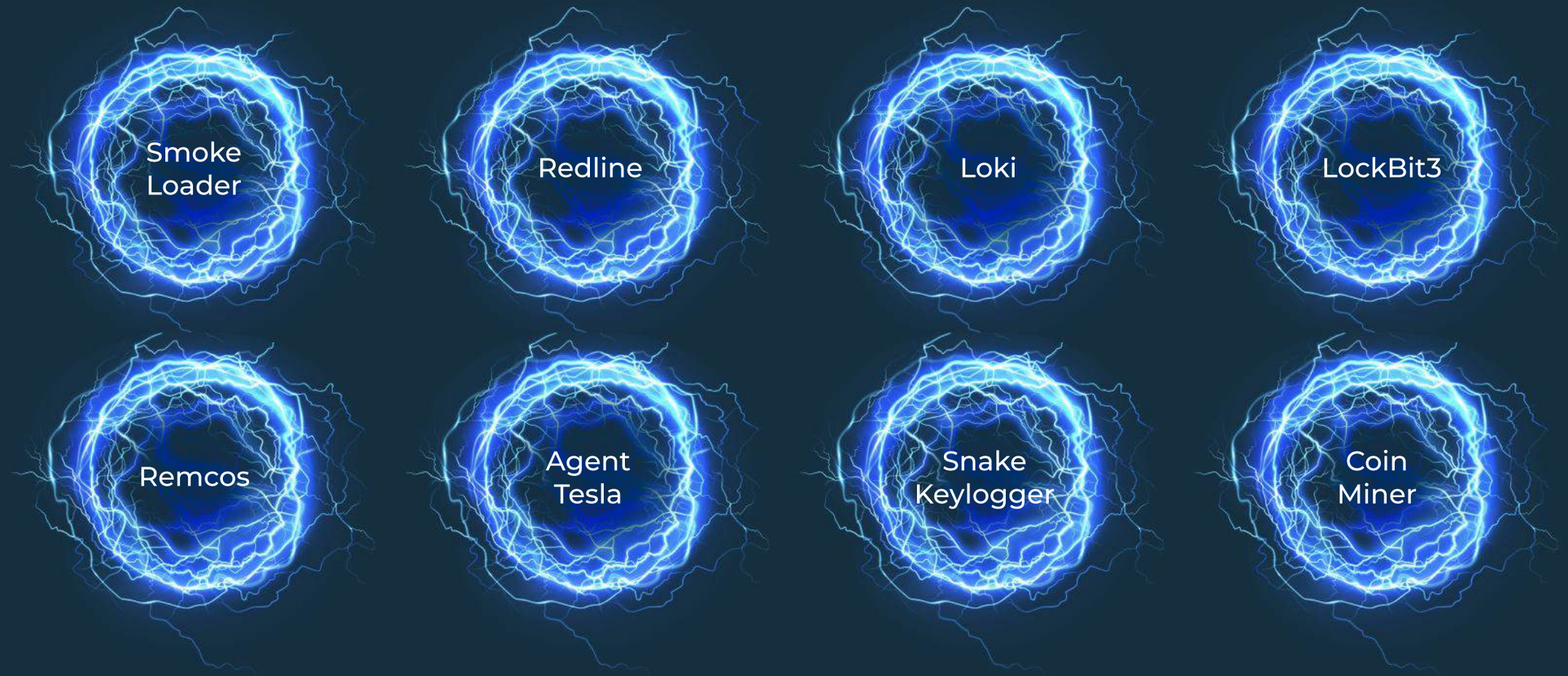
Портфель продуктов содержит решения
по защите серверов, рабочих станций,
оборудования, Интернета вещей и АСУ ТП.

- Соответствие требованиям
ФЗ, ФСБ, ФСТЭК, ISO/IEC 27000
- ИТ-консалтинг и аудит
информационной безопасности
- Расследование киберинцидентов
и анализ вирусов
- Обучение и поддержка
пользователей

ПРОБЛЕМА

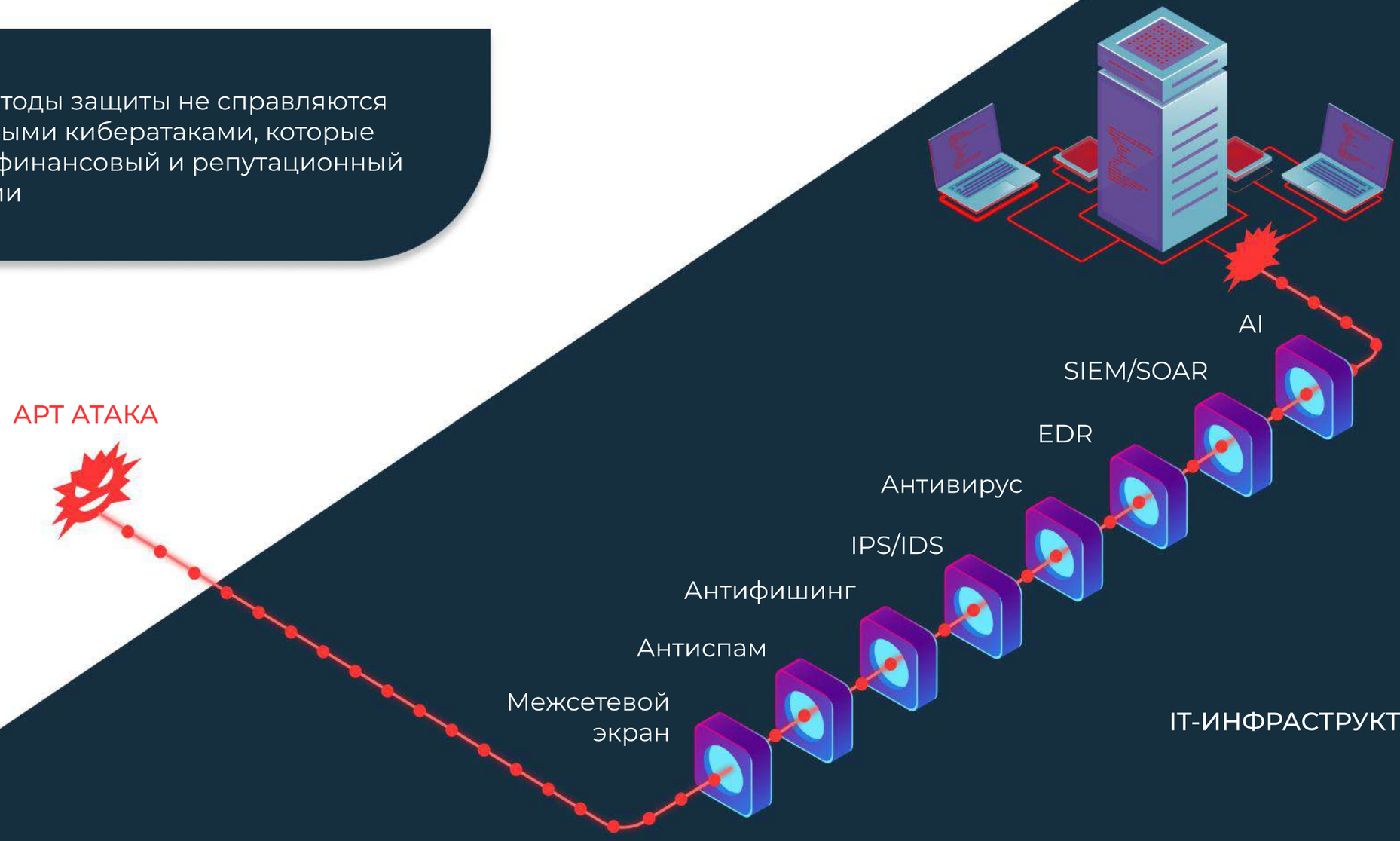
Целенаправленные кибератаки (APT) совершенствуются уже более 20 лет. Они стараются нарушить работу компаний, занимаются промышленным шпионажем, вымогают финансовые средства, могут оставаться в инфраструктуре продолжительное время и обходить все современные средства защиты.

- Loader
- Stealer
- RAT
- Ransomware
- Trojan
- Installer
- Keylogger
- Backdoor



МЕТОДЫ ЗАЩИТЫ

Существующие методы защиты не справляются с целенаправленными кибератаками, которые наносят большой финансовый и репутационный ущерб организации



AVSOFT ATHENA

Система защиты от целенаправленных атак **AVSOFT ATHENA** - антивирусный мультисканер и песочница в одной системе для защиты от известных и новых вирусов

Запись в реестре отечественного программного обеспечения
№3762 от 23.07.2017

НАДЕЖНАЯ ЗАЩИТА

- Веб-трафик
- Почтовый трафик
- Сетевой трафик
- Файловые хранилища



ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ

- ICAP
- SMTP
- Syslog
- API
- SFTP
- AD/LDAP
- FTP (S)
- SMB
- NFS
- S3

СХЕМА РАБОТЫ

ИСТОЧНИКИ ДАННЫХ

- Межсетевой экран
- NDR
- Корпоративный прокси
- Почтовый трафик
- Файловое хранилище
- Веб-трафик
- Агенты на рабочие места
- Мессенджеры
- Ручная загрузка

AVSOFT ATHENA

Статический анализ	Анализ ссылок	Динамический анализ
Взаимодействие с 20+ движками	Скачивание файлов	Анализ поведения
Парсинг структуры	Синтаксический анализ	Сетевая активность
Внешние источники	Внешние источники	Использование ресурсов
Машинное обучение	Машинное обучение	Аналитические ресурсы

РЕЗУЛЬТАТЫ ПРОВЕРКИ

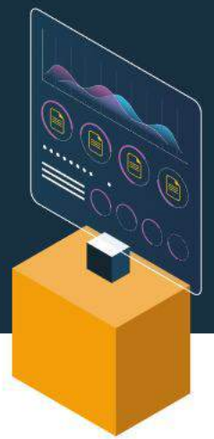
- Карантин
- Пользователь
- SIEM/SOAR

События

СТАТИЧЕСКИЙ АНАЛИЗ

ЛЮБЫЕ ТИПЫ ФАЙЛОВ

- Исполняемые
- Офисные
- Мобильные приложения
- Архивы, включая многотомные и закрытые паролем и др.



МНОГОУРОВНЕВАЯ ПРОВЕРКА

- Результаты антивирусной проверки
- Машинное обучение
- Внешние аналитические сервисы
- Анализ синтаксической структуры

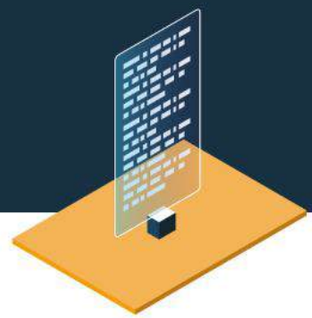


РЕЗУЛЬТАТЫ АНАЛИЗА

Активные элементы
- макросы
- скрипты
  - Visual Basic
  - Java
  - PowerShell
  - Python
  - JavaScript и др.

Атрибуты
- цифровая подпись
- упаковщики

Контент
- обфускация
- энтропия



ДИНАМИЧЕСКИЙ АНАЛИЗ

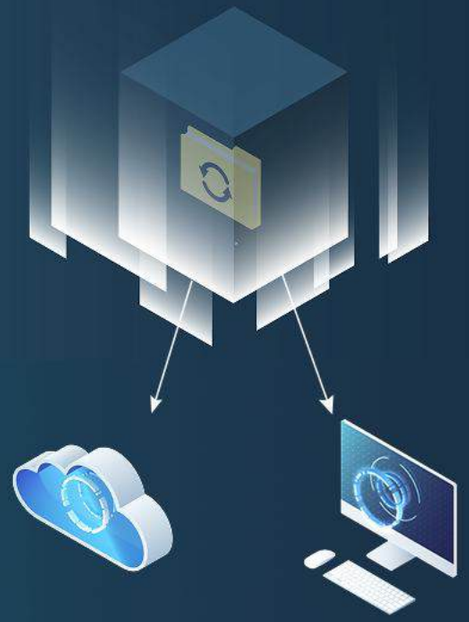
ТИПЫ ФАЙЛОВ, УКАЗАННЫЕ В СЦЕНАРИЯХ

- Исполняемые
- Офисные
- Мобильные приложения
- PKL файлы
- Архивы, включая многотомные и закрытые паролем и др.



ИССЛЕДОВАНИЕ ФАЙЛОВ В “ПЕСОЧНИЦЕ”

Sandbox



Виртуальная машина

Физическая машина (для SOC центров)

РЕЗУЛЬТАТЫ АНАЛИЗА ПОВЕДЕНИЯ

- Анализ поведения
- Запись исследования и скриншоты
- Сетевой трафик (проверка IP-адресов и доменов)



Фиксация потребляемых ресурсов (майнинг)



ПЕСОЧНИЦА


Поддержка кастомизации с возможностью установки собственного программного обеспечения
Маскировка тактовой частоты процессора, датчиков температуры, гипервизора и др.
Любая продолжительность сна заменяется на 5 секунд
Физические песочницы (для SOC центров)
Встроенная имитация действий пользователя и возможность самостоятельно совершать действия в виртуальной машине
Изменение локали (английская, русская) и учетки пользователя виртуальной машины
Изолированная среда проверки
Windows
Linux
Android

ЗАЩИТА ПОЧТОВОГО ТРАФИКА

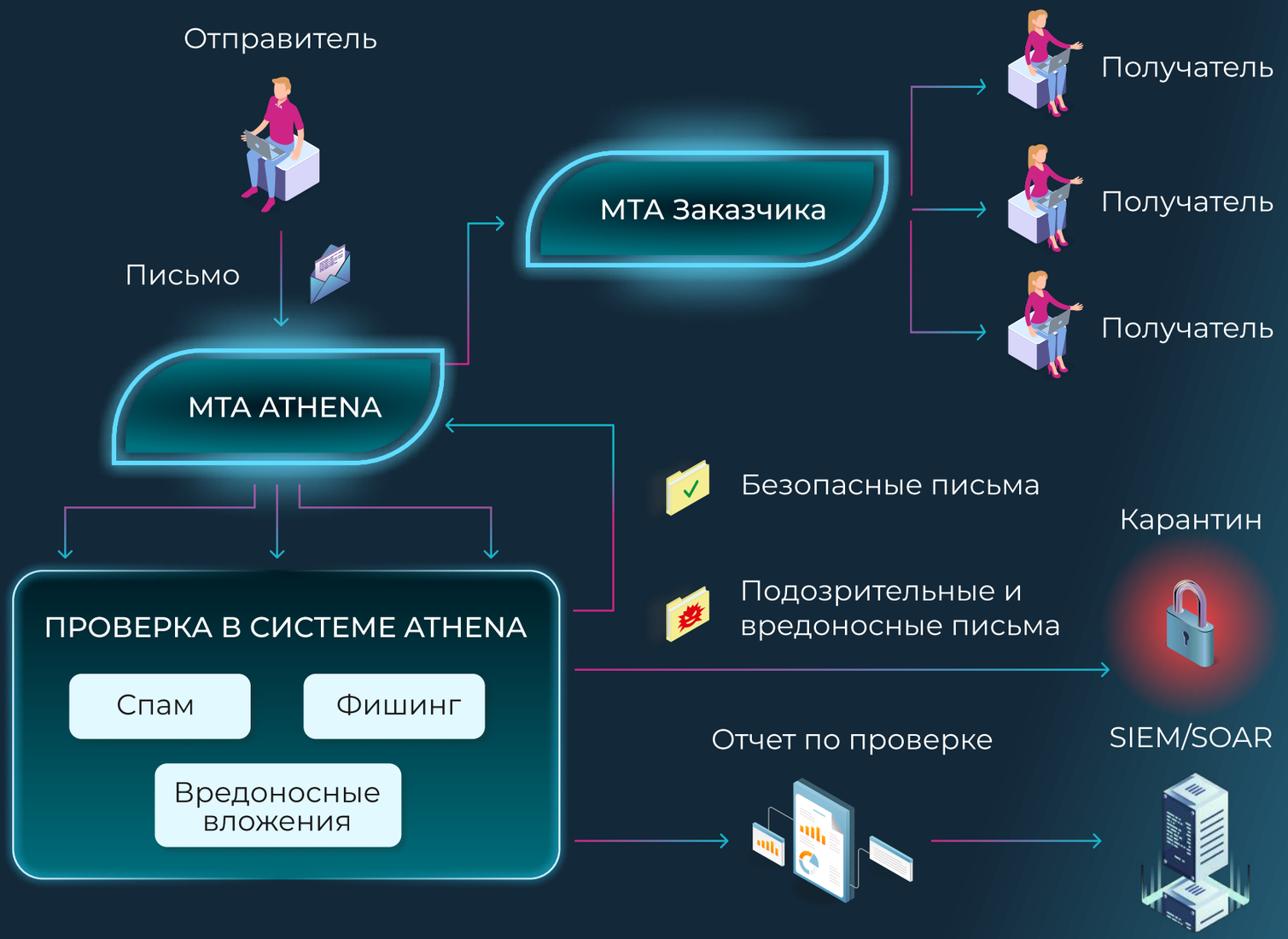
Система ATHENA осуществляет проверку входящего и исходящего почтового трафика

НАПРАВЛЕНИЯ ЗАЩИТЫ

- Антиспам
- Антифишинг
- Вредоносные вложения

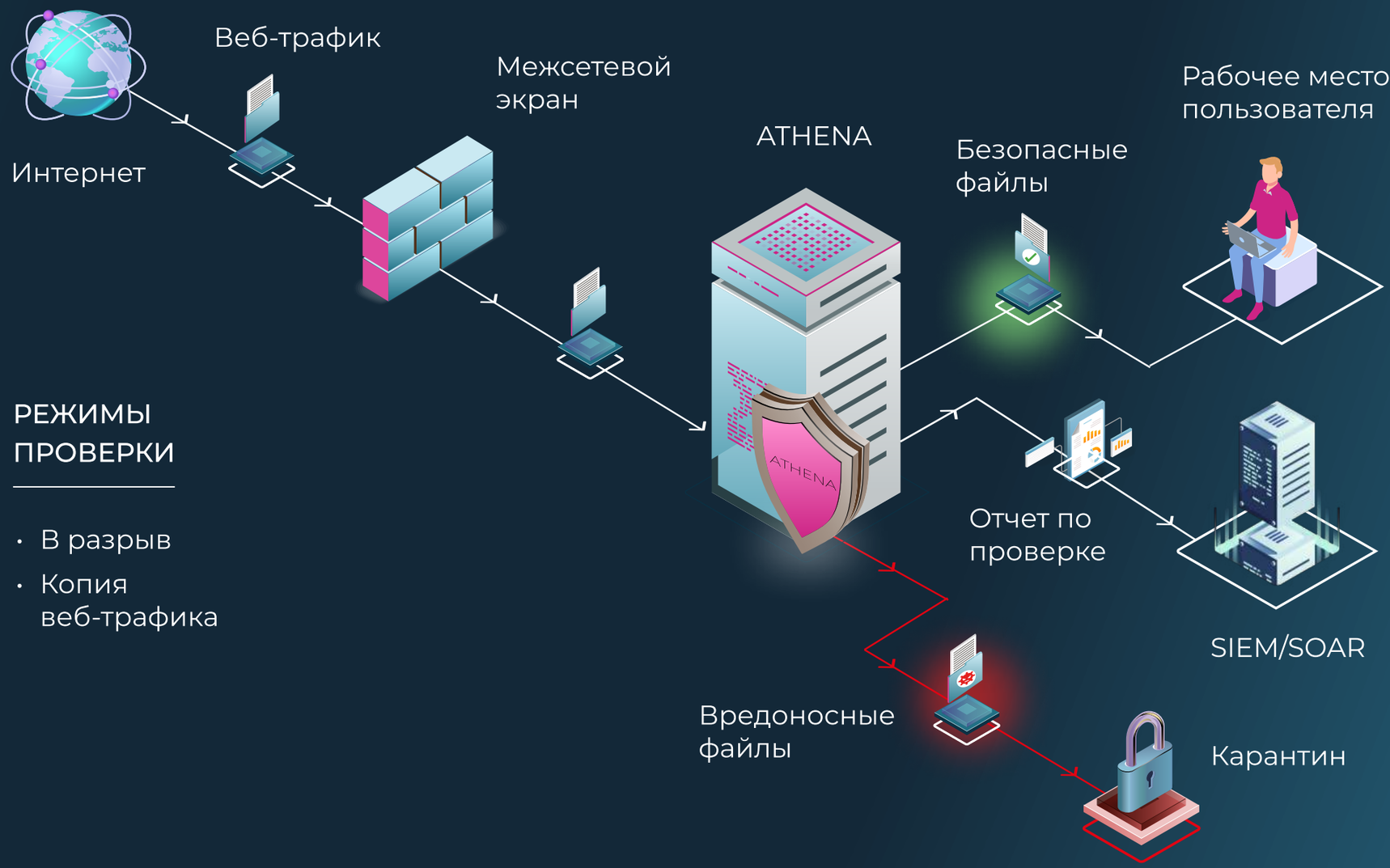
РЕЖИМЫ ПРОВЕРКИ

- В разрыв
- Архивный ящик
- Зеркальная копия (BCC)



АНАЛИЗ ВЕБ-ТРАФИКА

Проверка файлов
в веб-трафике
с возможностью
расшифровки
SSL-трафика



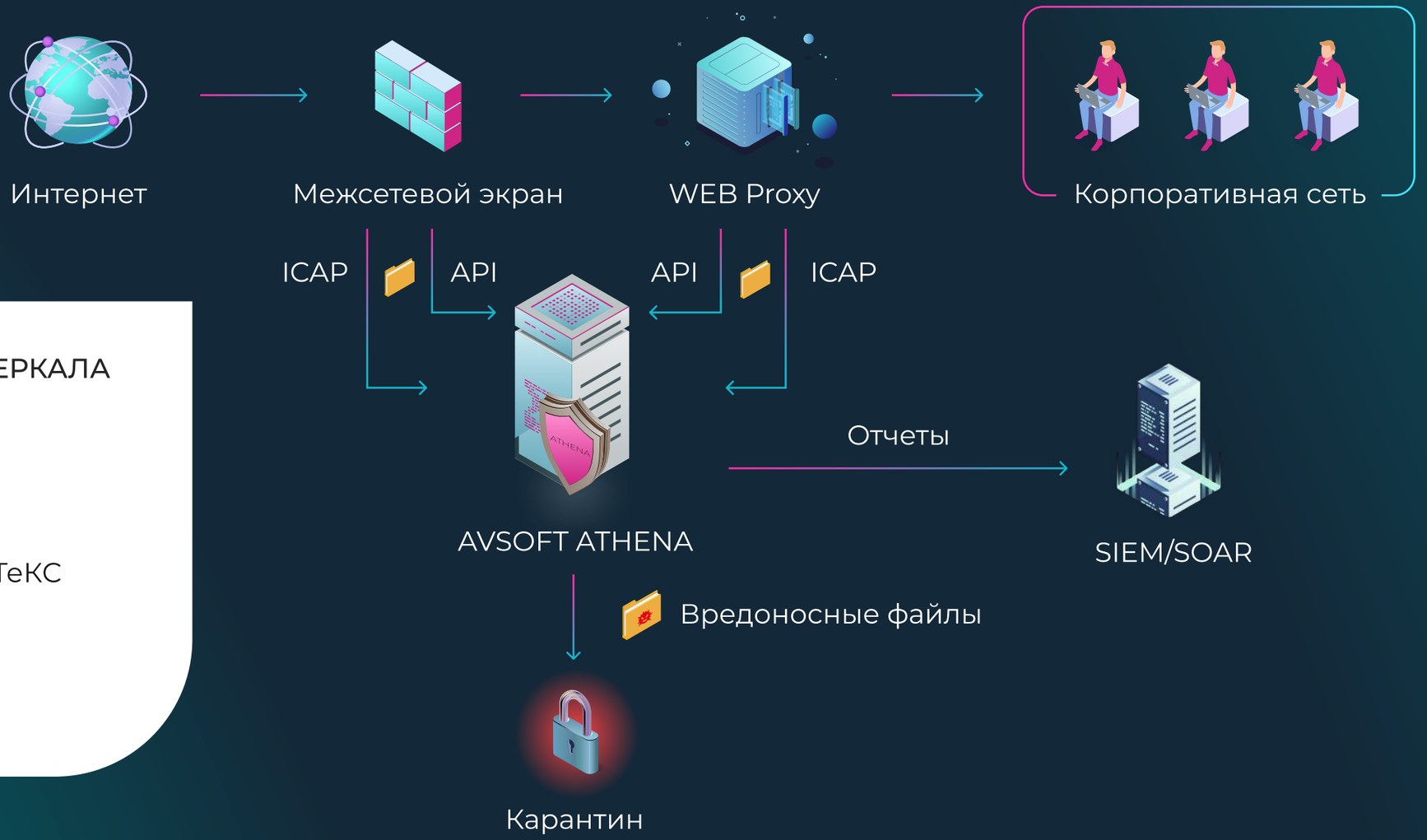
ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ

- HTTP
- HTTPS
- FTP
- FTPS

РЕЖИМЫ ПРОВЕРКИ

- В разрыв
- Копия веб-трафика

ИНТЕГРАЦИЯ С МЕЖСЕТЕВЫМИ ЭКРАНАМИ И WEB-PROXY

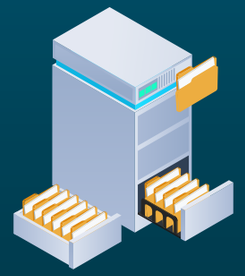


ИНТЕГРАЦИЯ В РЕЖИМЕ ЗЕРКАЛА

- CheckPoint NGFW
- InfoWatch ARMA
- UserGate NGFW
- ViPNet xFirewall 5 от ИнфоТеКС
- EtherSensor от Microlab
- Dionis DPS от Фактор-ТС
- ЦСС - Безопасность NTA

ФАЙЛОВОЕ ХРАНИЛИЩЕ

ФАЙЛОВОЕ ХРАНИЛИЩЕ



ПРОТОКОЛЫ ПРОВЕРКИ

- SFTP
- SMB
- FTP
- NFS
- S3

Поддерживается клиентская программа SSHFS

Проверка файлов и ссылок в системе ATHENA

2 РЕЖИМА

- По таймеру
- По новому файлу

ИНТЕГРАЦИЯ С ОБЛАЧНЫМИ ФАЙЛОВЫМИ ХРАНИЛИЩАМИ

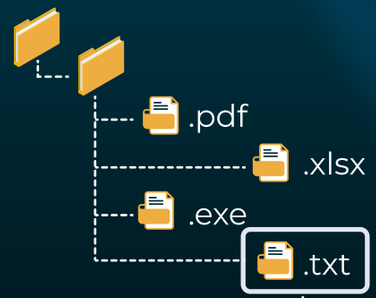
- Nextcloud (в разрыв)
- Яндекс.Диск
- Dropbox
- Google Диск

Рекурсивный обход всех поддиректорий при поиске файлов для проверки

Папка для безопасных файлов

Папка для вредоносных файлов

Сохранение структуры пути



Вредоносные файлы в структуре дерева заменяются .txt файлами, а сами файлы перемещаются в карантин

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

ПРОВЕРКА ОБНОВЛЕНИЙ И БОЛЬШИХ ФАЙЛОВ

- Дистрибутивы
- Прикладное ПО
- Системное ПО

ИНТЕГРАЦИЯ С АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ БИЗНЕСА

- Автоматизированные банковские системы
- Системы поддержки пользователей
- Системы документооборота и др.

Анализ PKL (.pickle) файлов и датасетов
ML форматов .h5, .hdf5, .pth, .pt

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

ССЫЛКИ

- Проверка ссылок внутри документа
- Осуществление перехода по ссылке через реальные браузеры
- Можно проверять большие объемы по API



ПОЧТОВЫЙ ТРАФИК

- Анализ заголовков
- Проверка файлов и ссылок
- Подбор пароля из темы и текста письма
- Формирование безопасной PDF версии файла



ФАЙЛЫ

- Префильтрация файлов по типам и источникам
- Проверка запароленных архивов, файлов, PDF
- Отсутствие ограничений по размерам файлов
- Проверка многотомных архивов с более 4 уровнями вложенности
- Проверка APK приложений, перехват системных вызовов и сетевого трафика



РЕЖИМ РАБОТЫ



Файл на проверку

Проверка по контрольной сумме

Вредоносный вердикт

Условия
- Нет в базе данных

Статический анализ

Вредоносный вердикт

Условия
- Безопасный вердикт
- Есть активное содержимое
  - Макросы
  - Скрипты

Динамический анализ (Виртуальные песочницы)

Вредоносный вердикт

Условия
- Подключен модуль физических машин
- Детектирование виртуальной среды
- Безопасный вердикт

Динамический анализ (Физические песочницы для SOC центров)

Вредоносный вердикт

Безопасный вердикт

Пользователь



Гибкая настройка режимов и политик проверки из различных источников

МАШИННОЕ ОБУЧЕНИЕ И БОТЫ

Использование моделей машинного обучения
для анализа различных типов файлов и фишинговых
ссылок с возможностью автоматического дообучения,
в том числе на данных клиента в закрытом контуре

- Спам
- Фишинг
- PDF
- DLL
- MS OFFICE
- APK
- EXE
- ELF

Боты в сети интернет обогащают
систему различными типами IoC
в автоматическом режиме

КЛАССИЧЕСКИЕ МОДЕЛИ

RandomForest, CatBoost, XGBoost,
LightGBM, KNN, K-Means

НЕЙРОННЫЕ СЕТИ

CNN, RNN, LSTM, BI-LSTM

МАШИННОЕ ЗРЕНИЕ

OpenCV

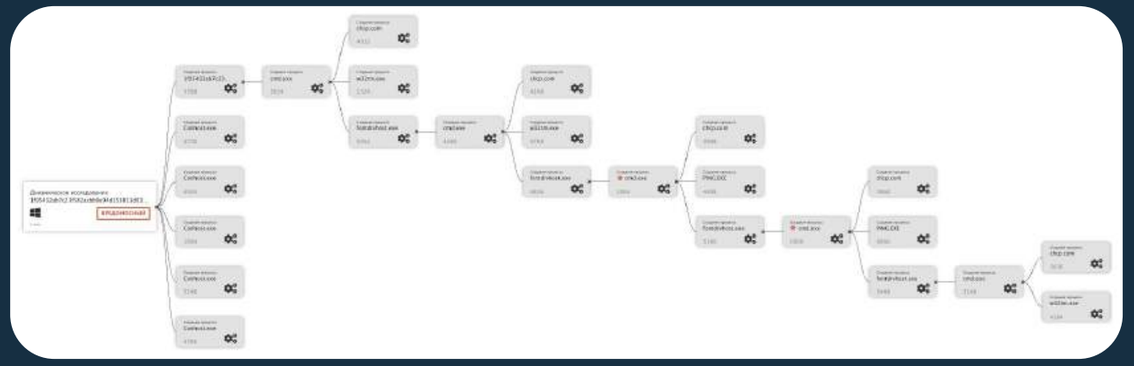
МОДЕЛИ NLP

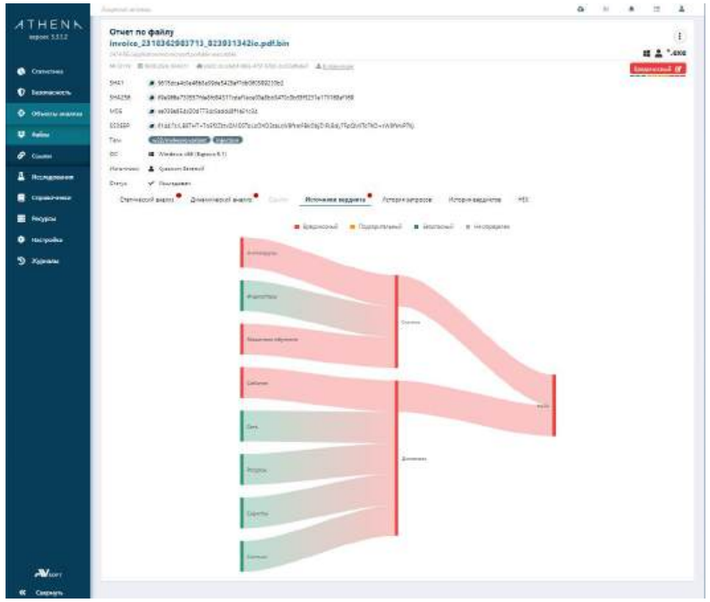
Bert, LLM

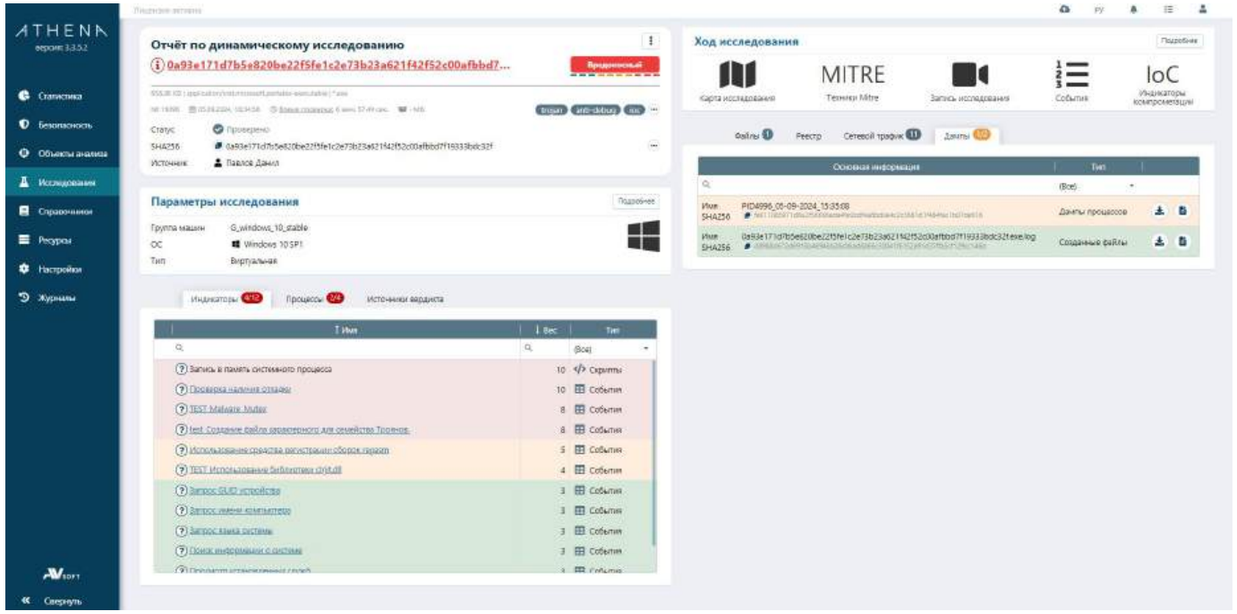
РЕЗУЛЬТАТЫ АНАЛИЗА

Система ATHENA предоставляет детальный отчет с ключевой информацией по результатам исследования файла, веб-ссылки и письма

В системе присутствует версия отчетов для печати в формате PDF, которую можно кастомизировать через вендора







УСТАНОВКА И ИНТЕГРАЦИЯ

ФИЗИЧЕСКАЯ СРЕДА

- Debian 10/12
- Astra Linux 1.7
- Ubuntu 22.0
- RHEL

ВИРТУАЛЬНАЯ СРЕДА

- WMware ESX Server от 5.5
- Microsoft Hyper-V от 2019
- KVM 1.3.1

ВНЕШНИЕ СИСТЕМЫ

- Межсетевые экраны- ICAP/API
- Служба каталогов (AP)- LDAP
- Системы сбора событий (SIEM/SOAR)-Syslog
- Почтовые сервера- SMTP

ПРЕИМУЩЕСТВА

- Взаимодействие с внешними антивирусными движками
- Модели машинного обучения
- Антивирусный мультисканер и песочница
- Проверка архивов (в т. ч. многотомных и многоуровневых)
- Боты сбора IoC в сети Интернет
- Поддержка отечественных ОС
- Интеграция с Deception
- Физические песочницы (для SOC центров)
- Проверка обновлений и PKL файлов

AV SOFT

КОНТАКТЫ

Спасибо, что нашли
время ознакомиться
с презентацией!

ЗАПОЛНИТЬ АНКЕТУ



