



# AVSOFT ATHENA

Система защиты от  
целенаправленных атак

# О КОМПАНИИ



**AV SOFT**

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

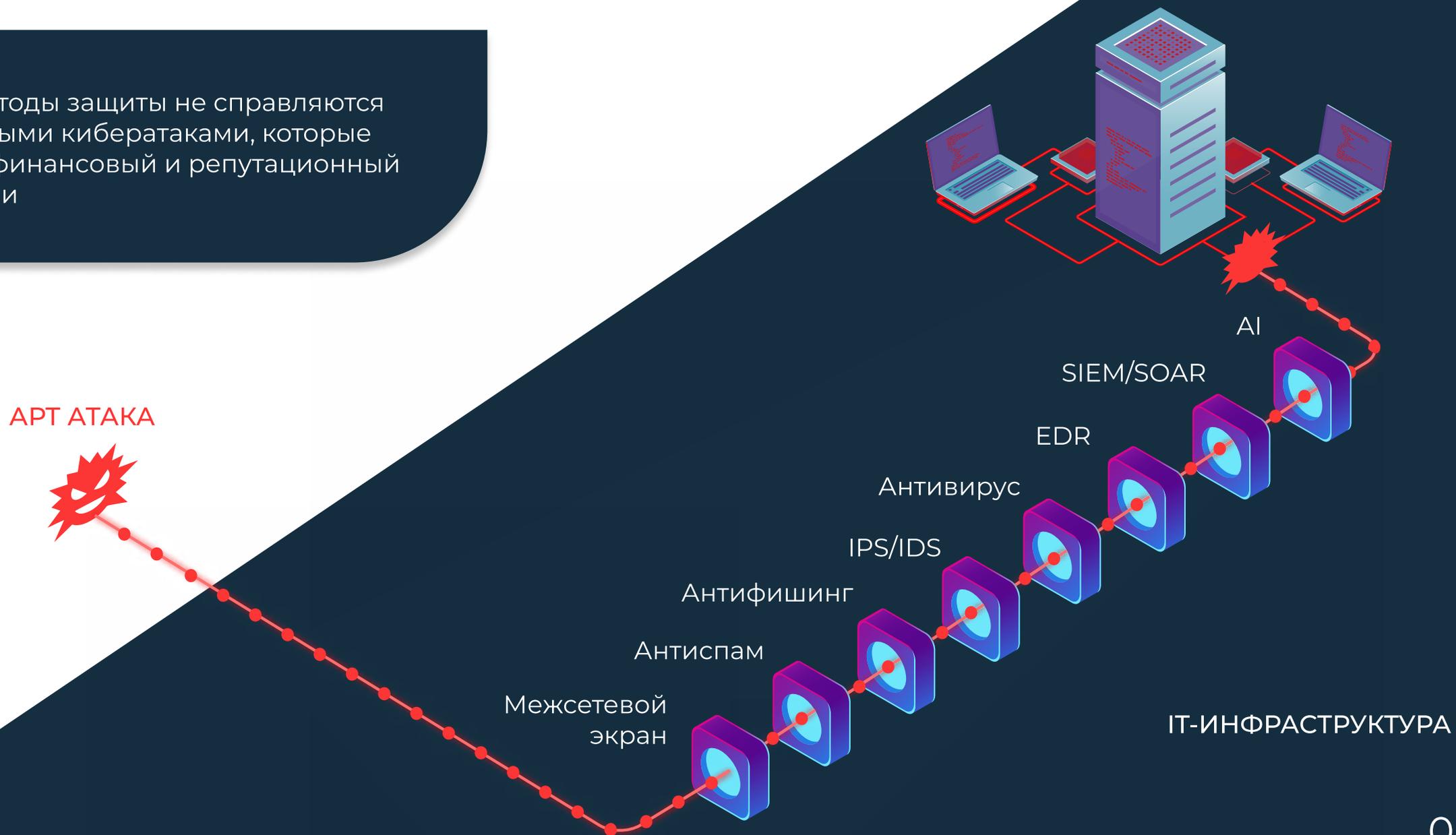
Целенаправленные кибератаки (АPT) совершенствуются уже более 20 лет. Они стараются нарушить работу компаний, занимаются промышленным шпионажем, вымогают финансовые средства, могут оставаться в инфраструктуре продолжительное время и обходить все современные средства защиты.

- 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

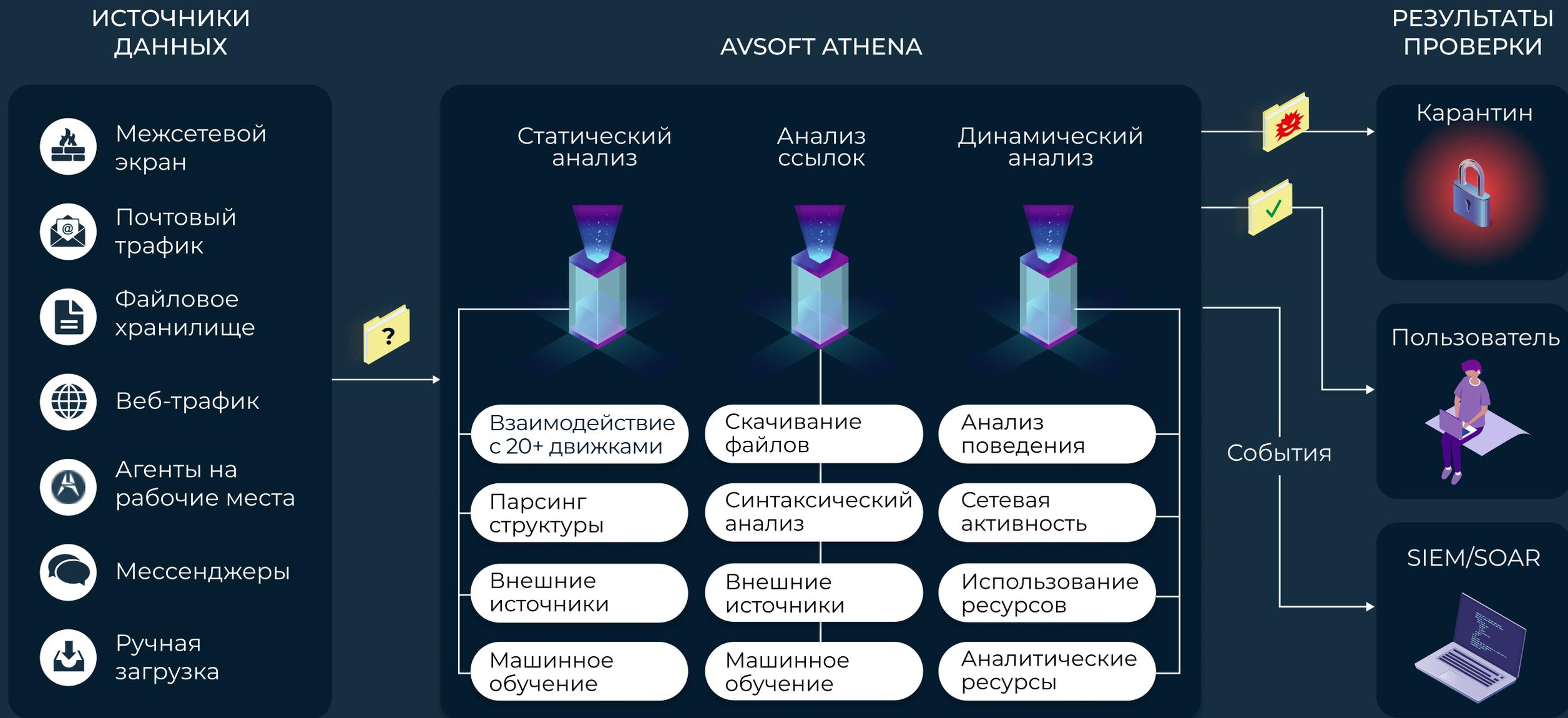
-  Веб-трафик
-  Почтовый трафик
-  Сетевой трафик
-  Файловые хранилища



## ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ

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

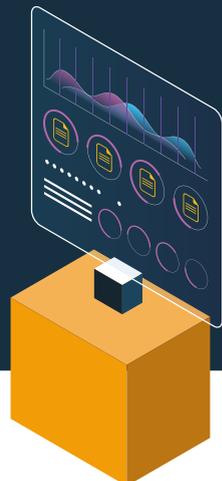
# СХЕМА РАБОТЫ



# 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
- RKL файлы
- Архивы, включая многотомные и закрытые паролем и др.



## ИССЛЕДОВАНИЕ ФАЙЛОВ В "ПЕСОЧНИЦЕ"



## РЕЗУЛЬТАТЫ АНАЛИЗА ПОВЕДЕНИЯ

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



Фиксация потребляемых ресурсов (майнинг)



# ПЕСОЧНИЦА



# ЗАЩИТА ПОЧТОВОГО ТРАФИКА

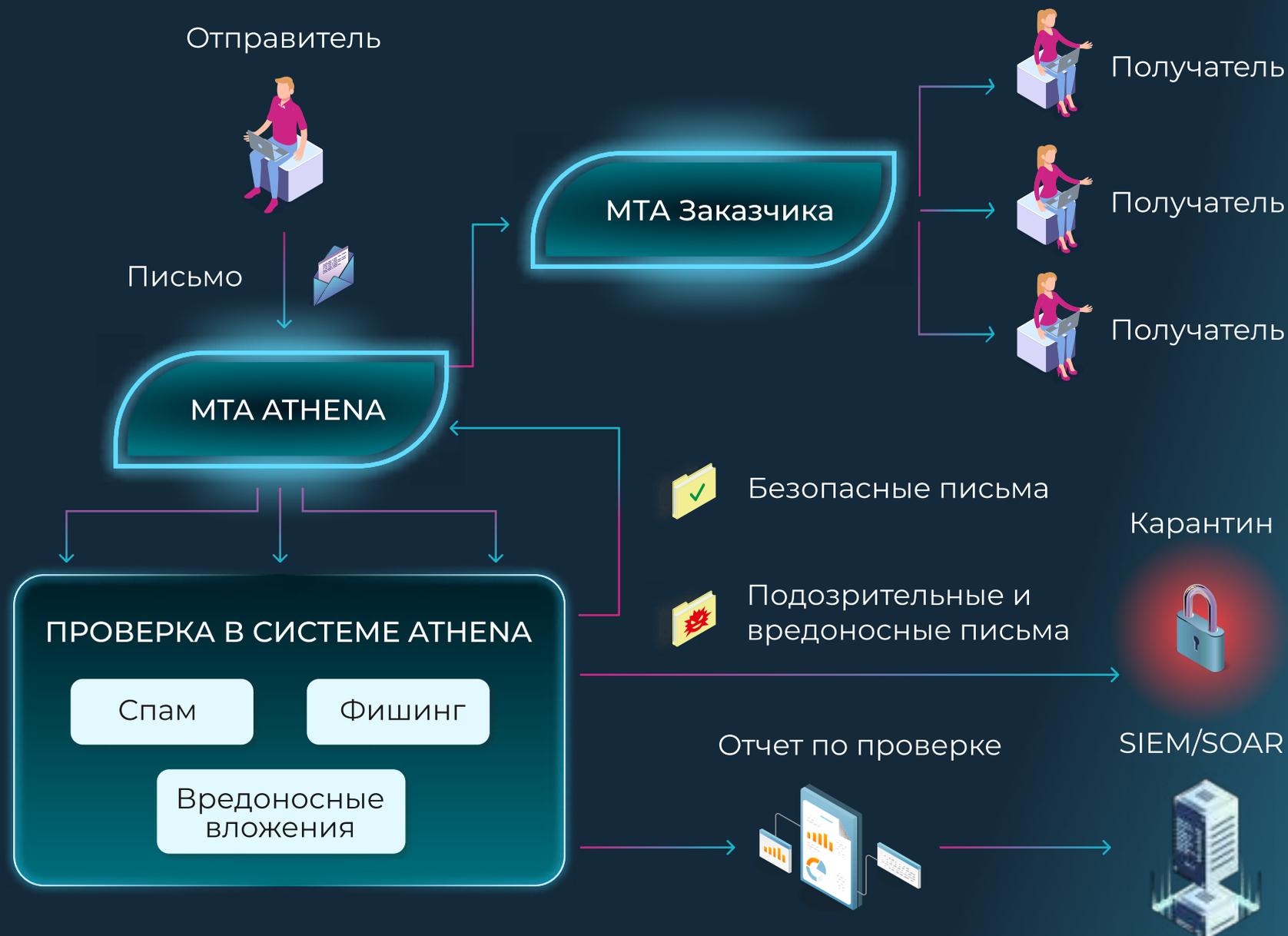
Система ATHENA осуществляет проверку входящего и исходящего почтового трафика

## 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



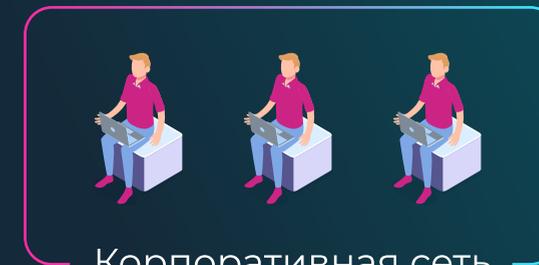
Интернет



Межсетевой экран



WEB Proxy

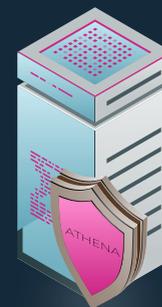


Корпоративная сеть

ICAP



API



AVSOFT ATHENA



Вредоносные файлы



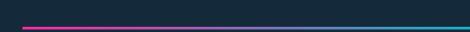
Карантин

API



ICAP

Отчеты



SIEM/SOAR

## ИНТЕГРАЦИЯ В РЕЖИМЕ ЗЕРКАЛА

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

# ФАЙЛОВОЕ ХРАНИЛИЩЕ



# 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



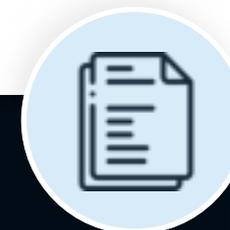
## ПОЧТОВЫЙ ТРАФИК

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



## ФАЙЛЫ

- Префилترация 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



# 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



Экстремальное усиление градиента



Light Gradient Boosting



VGG, NasNet, EfficientNet



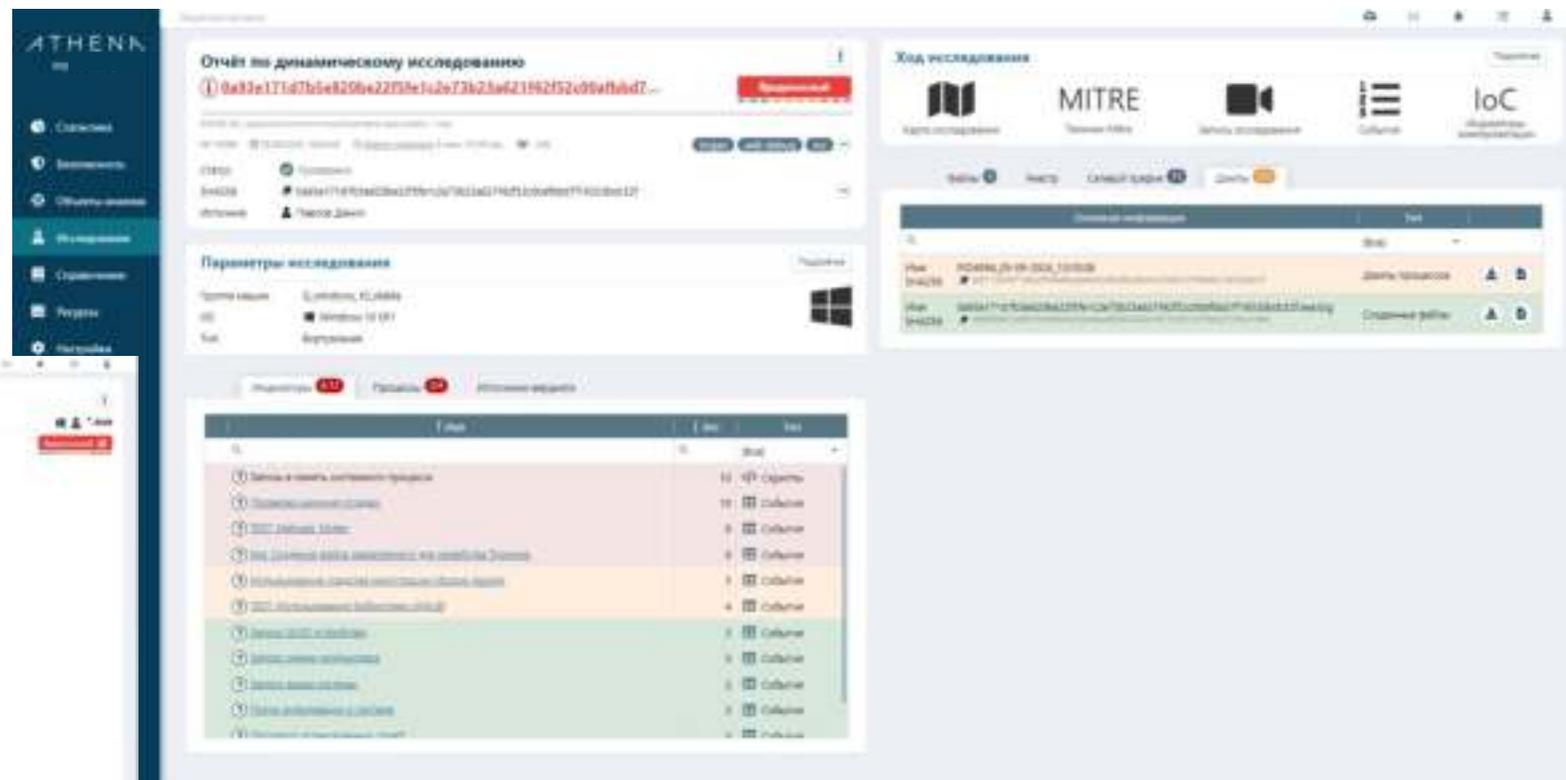
Random Forest Classifier



Catboost

# РЕЗУЛЬТАТЫ АНАЛИЗА

Система ATHENA предоставляет детальный отчет с ключевой информацией по результатам исследования файла



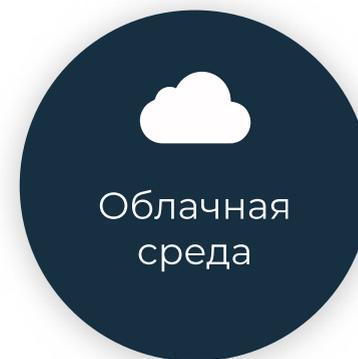
В системе присутствует версия отчетов для печати в формате PDF, которую можно кастомизировать через вендора

# ИНТЕГРАЦИЯ

## ТИПОВАЯ СХЕМА ИНТЕГРАЦИИ



## ВАРИАНТЫ РАЗВЕРТЫВАНИЯ



# ПРЕИМУЩЕСТВА



Подключение внешних  
антивирусных движков



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



Проверка  
обновлений  
и PKL файлов

# КОНТАКТЫ

Спасибо, что нашли  
время ознакомиться  
с презентацией!

ЗАПОЛНИТЬ АНКЕТУ



+7 (495) 988-92-25



office@avsw.ru



127106, г. Москва,  
ул. Гостиничная, д. 5



www.avsw.ru