

# 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



Расследование киберинцидентов  
и анализ вирусов



ИТ-консалтинг и аудит  
информационной безопасности

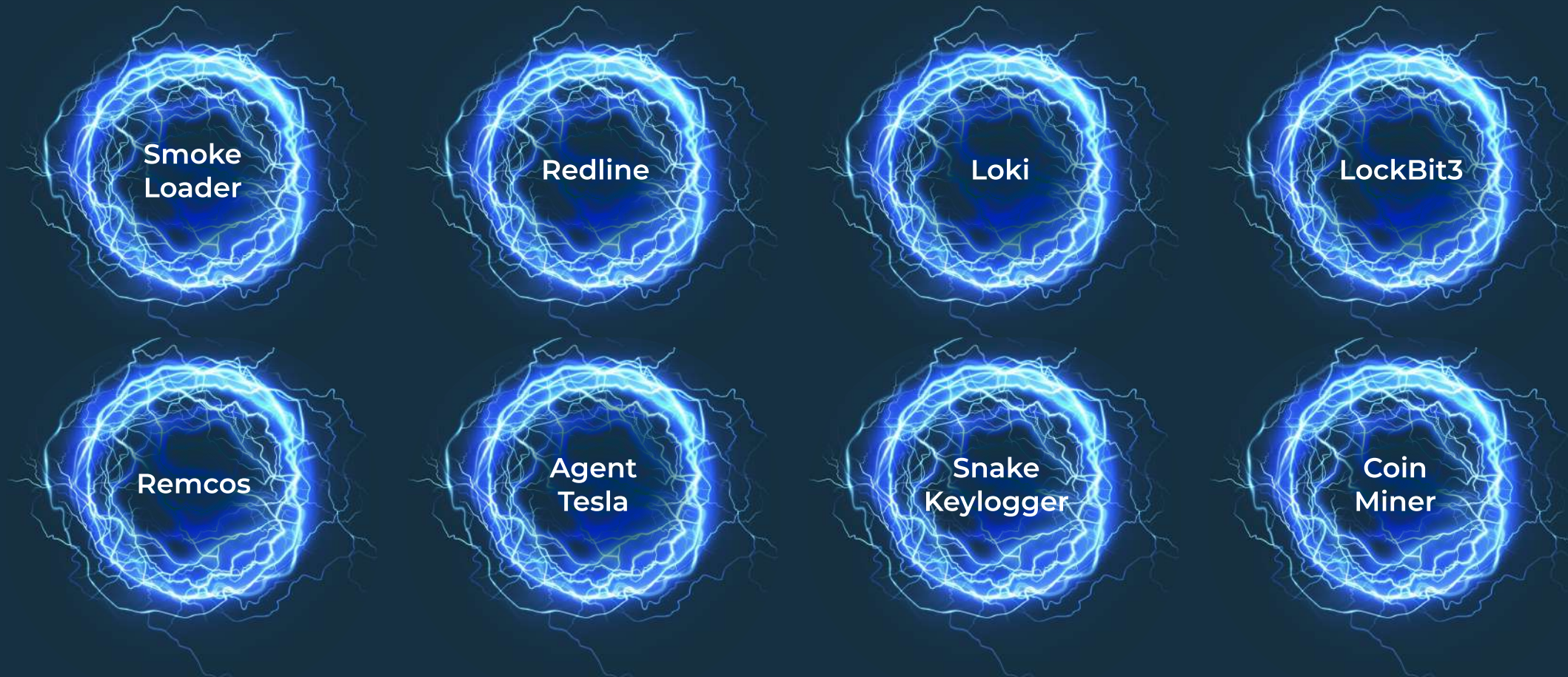


Обучение и поддержка  
пользователей

# 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.

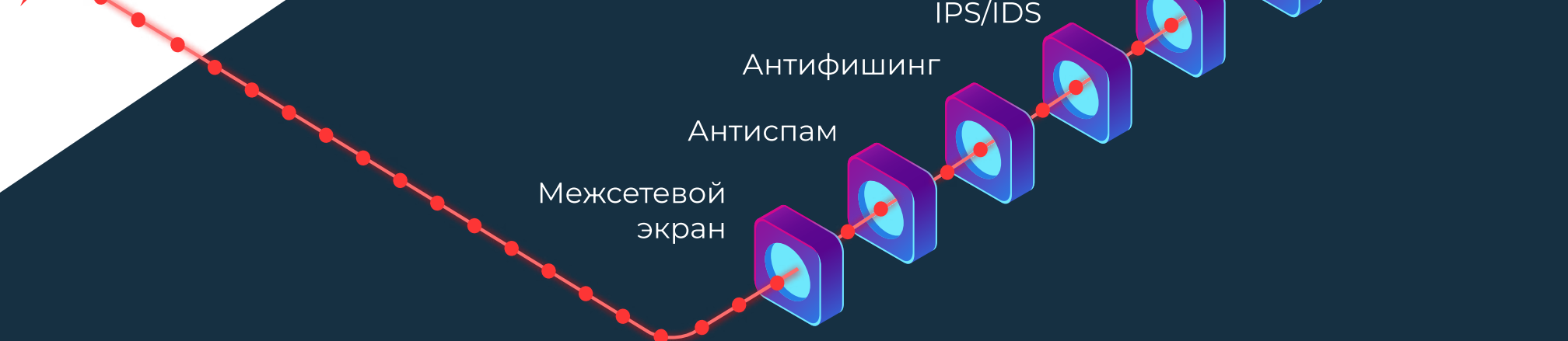
- Loader
- Stealer
- RAT
- Ransomware
- Trojan
- Installer
- Keylogger
- Backdoor



# МЕТОДЫ ЗАЩИТЫ

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

APT атака



IT-инфраструктура





# 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
-  Рабочие места и сервера



## ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ

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

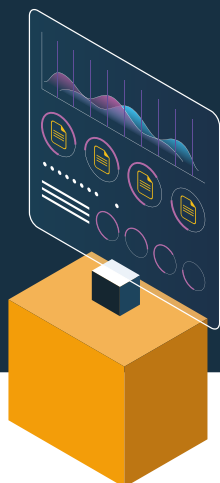
# СХЕМА РАБОТЫ



# СТАТИЧЕСКИЙ АНАЛИЗ

## Любые типы файлов

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



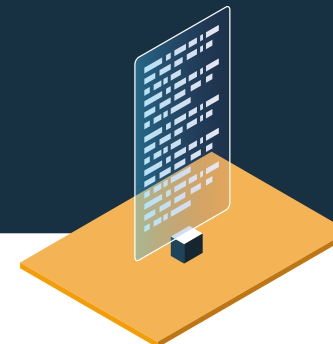
## Многоуровневая проверка

- 20 антивирусов
- 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



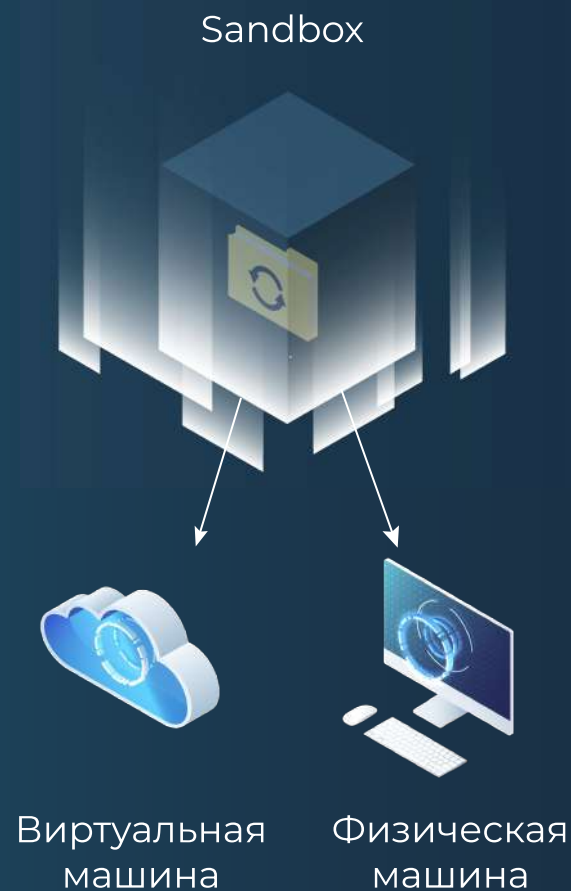
# ДИНАМИЧЕСКИЙ АНАЛИЗ

## 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

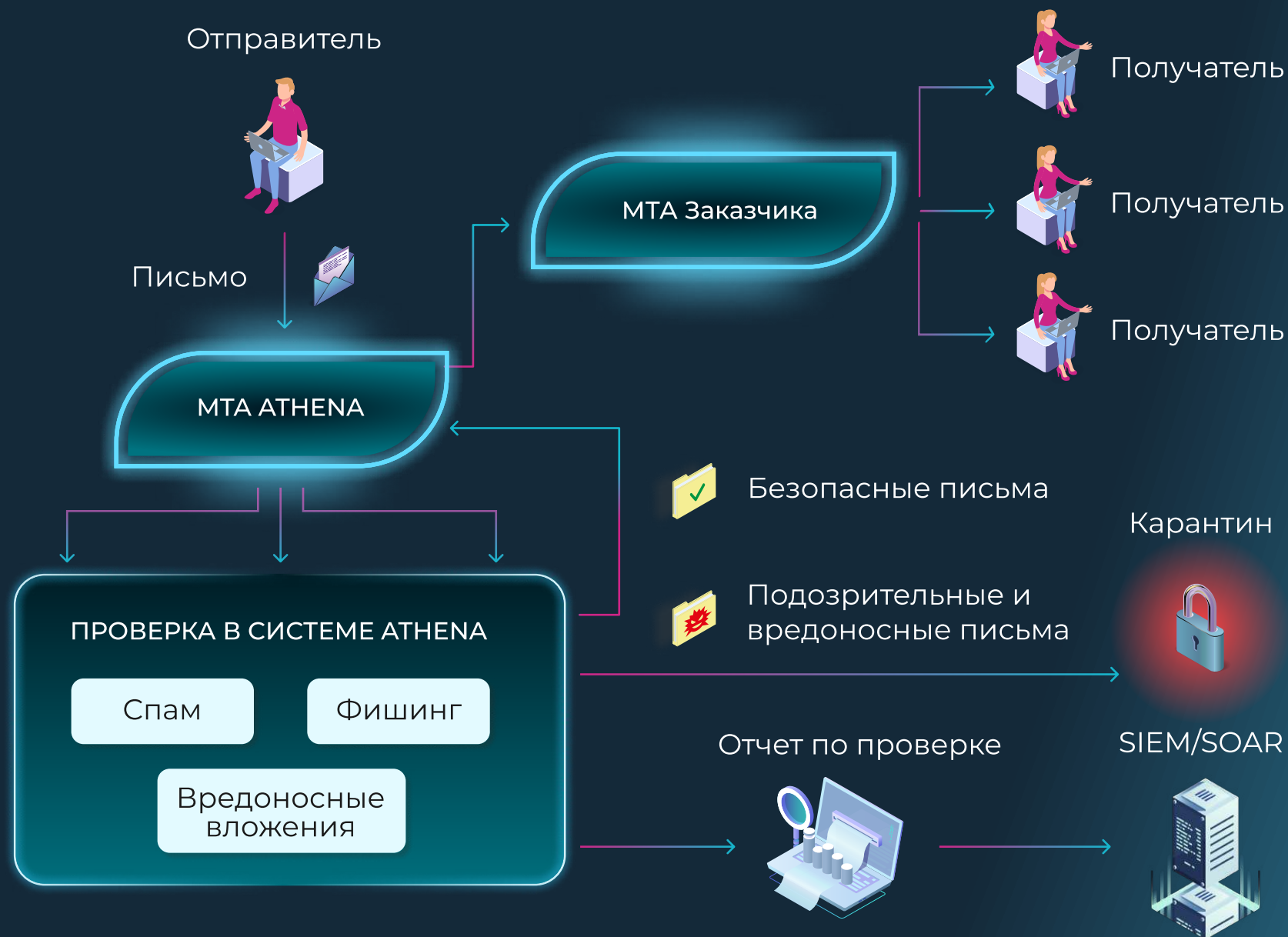
Система ATHENA осуществляет проверку почтового трафика по протоколу SMTP

## НАПРАВЛЕНИЯ ЗАЩИТЫ

- Антиспам
- Антифишинг
- Вредоносные вложения

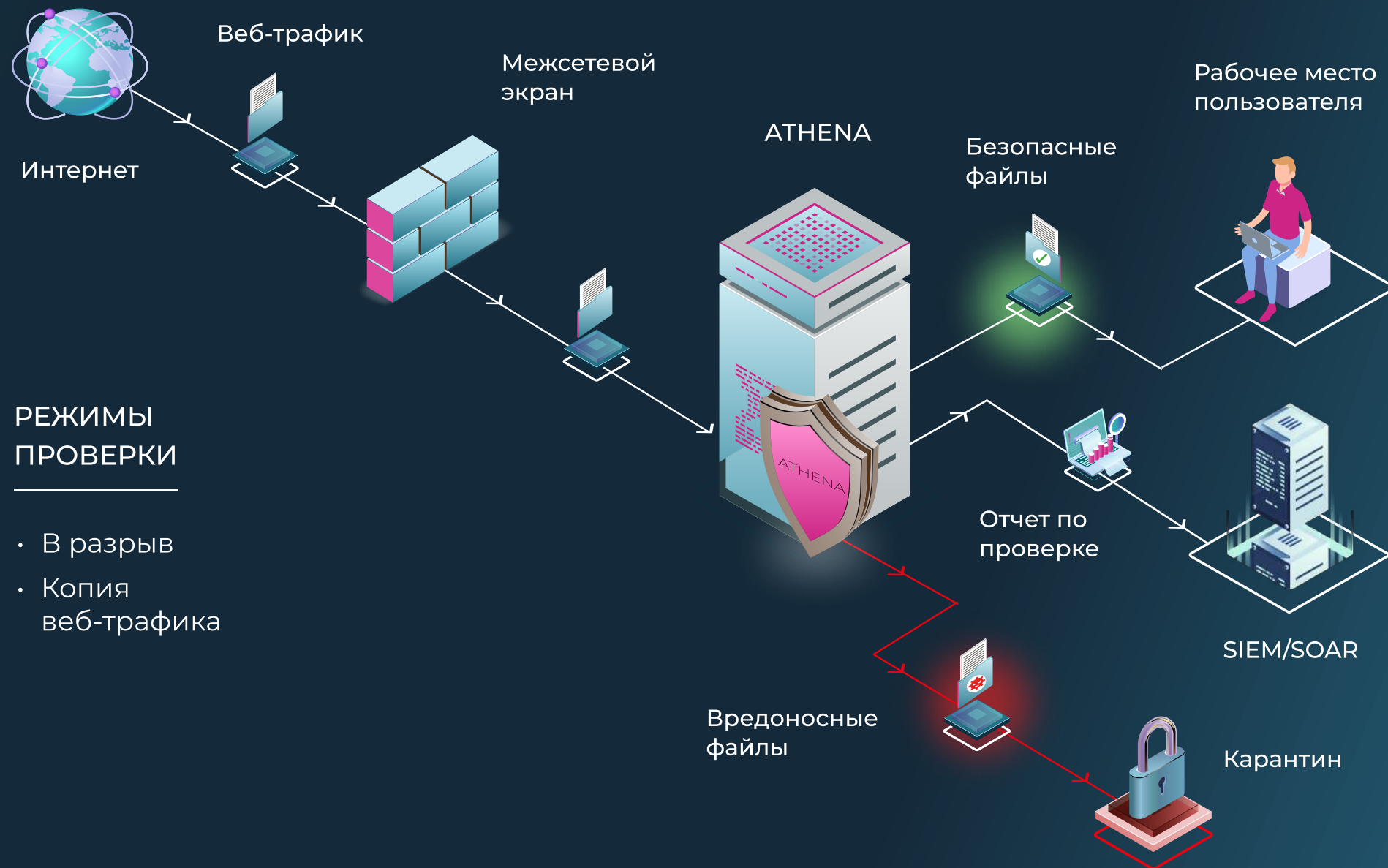
## РЕЖИМЫ ПРОВЕРКИ

- 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



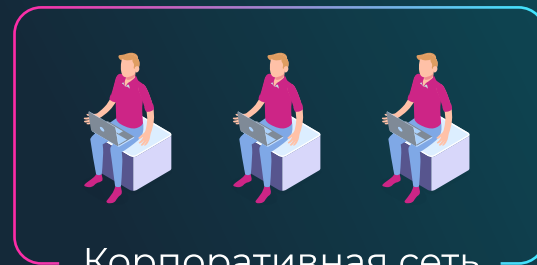
Интернет



Межсетевой экран



WEB Proxy



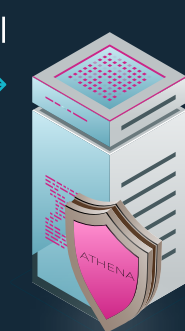
Корпоративная сеть

ICAP

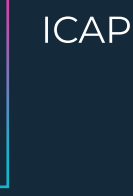
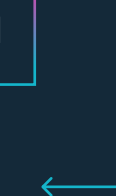
API

API

ICAP



AVSOFT ATHENA



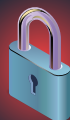
Отчеты



SIEM/SOAR



Вредоносные файлы



Карантин

## 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

- 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



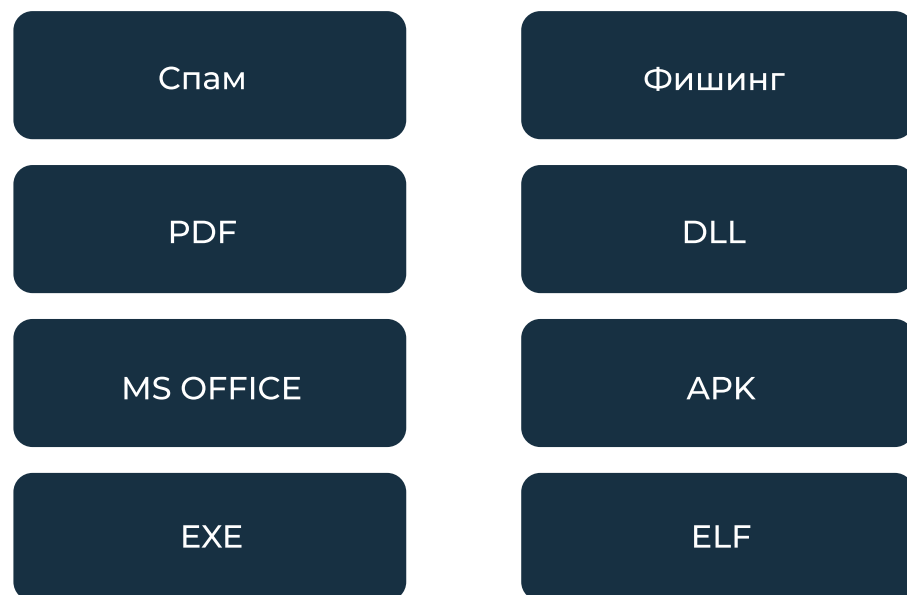
# РЕЖИМ РАБОТЫ





# 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



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



Экстремальное  
усиление  
градиента



Light Gradient  
Boosting



VGG, NasNet,  
EfficientNet



RandomFor  
estClassifier



Catboost

# РЕЗУЛЬТАТЫ АНАЛИЗА

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

**File report**  
Monero.exe  
369 KB | application/x-dosexec | \*.exe  
NF 53746 | 2/11/2020, 11:40:54 AM

Tags: non-a-win32;HTLR;RiskTool;Win32;Generic;anti-debug;anti-vn

SHA1: 95c8000972ee7c6809da11a5fd925652782e78f  
SHA256: cdcfc92e2ad53b665d6de3be2896eae0f4bb8687980327523c35749ba514a508  
MD5: 20b0c1eee0557da7b0b1d18056359a31  
SSDEEP: 6144:JUTJULKmjK3nDvgFzYF207gFuRDF6L1bz73Ktu/NbnLrkZrUSvVjv8euMKKer7km2DwZ...  
OS: Windows x64 (Version 5.2)  
Sources: Demo\_08

Static analysis | Dynamic analysis | Verdict history

ID	Created	Scenario	State	Verdict
50380	7/10/2020, 12:29 PM		Completed	Malware
50353	7/10/2020, 4:33 AM		Completed	Malware
50326	7/10/2020, 3:43 AM		Completed	Malware
50299	7/9/2020, 8:21 PM		Completed	Malware
50141	7/2/2020, 1:35 PM		Completed	Malware
40402	2/28/2020, 4:53 PM		Completed	Malware
48326	2/11/2020, 11:40 AM		Completed	Malware

**Dynamic research report**  
8485c644c0a96ff0d9256b10e2c50ee462868432080b6f27869d96ed77a7d0e  
3.37 MB | application/x-dosexec | \*.exe  
NF 84223 | 3/2/2022, 10:09:22 AM | 10 min, 53 sec. | infostealer recon stealth

State: Completed  
SHA256: 8485c644c0a96ff0d9256b10e2c50ee462868432080b6f27869d96ed77a7d0e  
Source: Водолазская Оксана

**Research parameters**  
Machine group: G\_Windows\_10\_Stable  
OS group: Windows 10 SP1  
Type: Virtual

**Research progress**  
MITRE, Research record, Events, loC

Files 1/46, Registry 12, Network traffic 5/15, Dumps

Connections 1/8, DNS 3/6, HTTP(S) 1/1

Domain	Response	PID	SpamHaus
ip-api.com	208.95.112.1	3364	Not Found
safialinks.com			Spam
hsiens.xyz			Botnet
gheorhip.tumblr.com	74.114.154.18,74.114.154.22	3400	Not Found
iplogger.org	148.251.234.83	3320	Not Found
cdn.discordapp.com	162.159.129.233,162.159.135.233,162.159.134.23,3,162.159.133.233,162.159.130.233	1176	Not Found

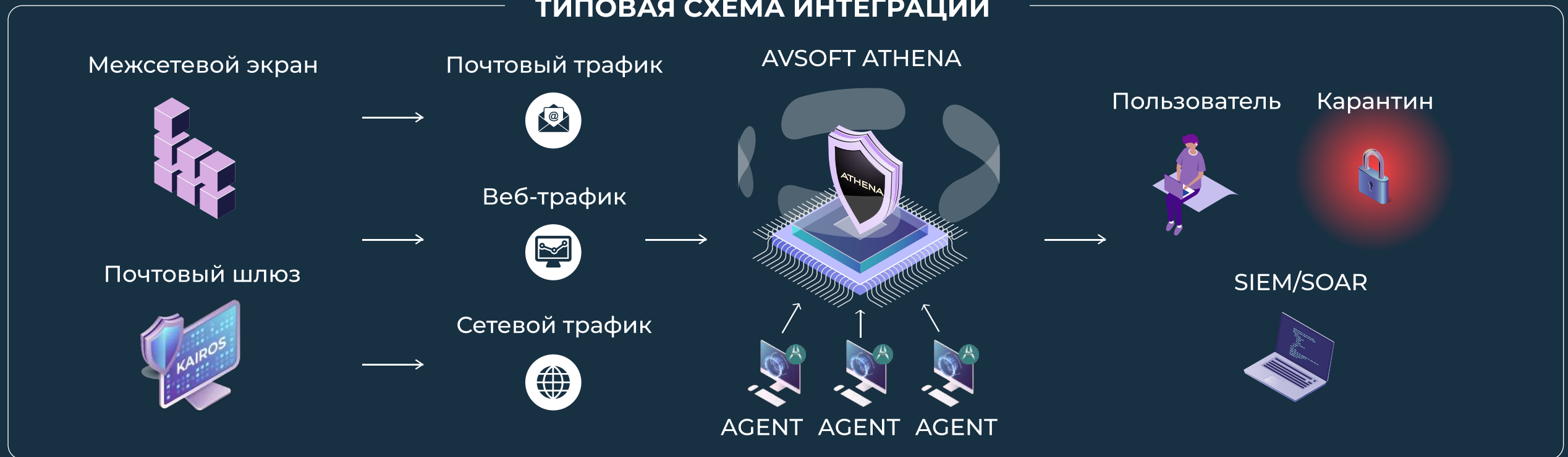
Verdict sources: HEX

Flow diagram showing verdict sources: Malware, Grayware, Benign, Undefined. Sources include Antivirus, Indicators, Links, Machine Learning, VirusTotal, YARA, Dumps, Events, Network traffic, Processes, Scripts, and Static/Dynamic analysis.

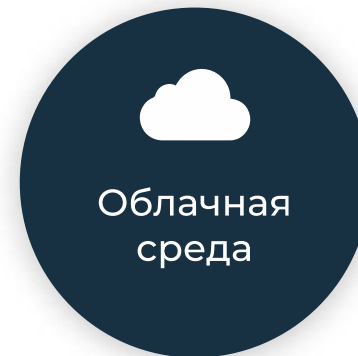
В системе присутствует версия отчетов для печати в формате PDF, которую можно кастомизировать через вендора

# ИНТЕГРАЦИЯ

## ТИПОВАЯ СХЕМА ИНТЕГРАЦИИ



## ВАРИАНТЫ РАЗВЕРТЫВАНИЯ



# ПРЕИМУЩЕСТВА



20 антивирусных движков



Модели машинного обучения



Антивирусный мультисканер и песочница



Проверка архивов (в т. ч. многотомных и многоуровневых)



Боты сбора IoT в сети Интернет



Поддержка отечественных ОС



Интеграция с Deception



Физические песочницы



Проверка обновлений и PKL файлов

# КОНТАКТЫ

Спасибо, что нашли  
время ознакомиться  
с презентацией!



+7 (495) 988-92-25



office@avsw.ru



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



www.avsw.ru