AVSOFT ATHENA

AVSOFT ATHENA

Система выявления и анализа вредоносного программного обеспечения

О КОМПАНИИ

01

Компания «АВ Софт» существует с 2010 года.
Основными направлениями нашей деятельности являются разработка программного обеспечения и консалтинг в сфере информационной безопасности.

Консалтинг в области ИБ

Анализ вредоносного ПО

AV SOFT

Разработка ПО в области ИБ

Расследование инцидентов ИБ

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

02

Целенаправленная атака (APT) – компьютерная атака, при которой киберпреступник получает доступ к корпоративным ресурсам конкретной организации и стремиться остаться необнаруженным в течении длительного времени.

Целенаправленные атаки используют множество различных методов получения доступа к ресурсам:

- социальная инженерия;
- эксплойты «нулевого дня»;
- уязвимости в корпоративном ПО и т.д.

Традиционные технологии не могут остановить APT.

СИСТЕМА AVSOFT ATHENA

03

Система «Афина» усиливает защиту информационной инфраструктуры от целенаправленных кибератак (в т. ч. от WannaCry и Petya) путем использования двух видов анализа ПО: статического и динамического.

Статический анализ

Исследование ПО в нескольких интегрированных в систему антивирусах и во внешних ресурсах.

Динамический анализ

Параллельное исследование поведения ПО в физических и виртуальных эмулируемых средах.

ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ

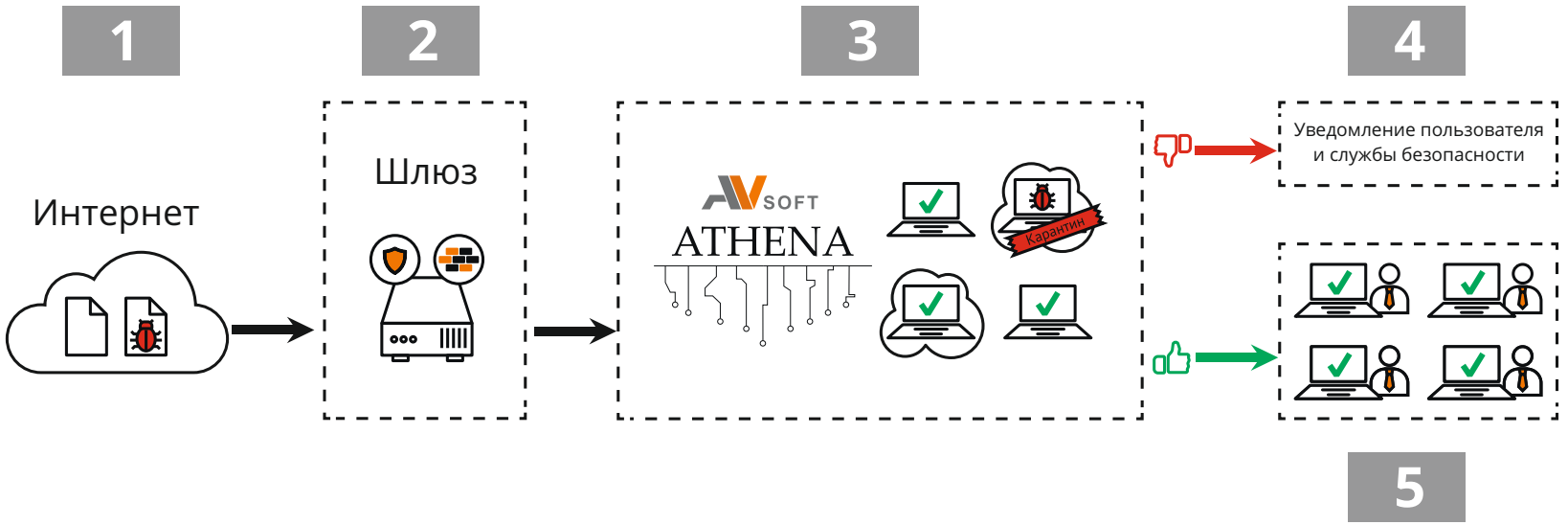
04

- Анализ содержимого почтового и интернет-трафика.
- Гибкая настройка эмулируемых сред в различных конфигурациях.
- Анализ детальной информации о поведении исследуемых файлов в виртуальных и физических эмулируемых средах.
- Управление исследованиями в экспертном режиме работы.
- Защита серверов, рабочих мест и мобильных устройств.

ПРИНЦИП РАБОТЫ СИСТЕМЫ

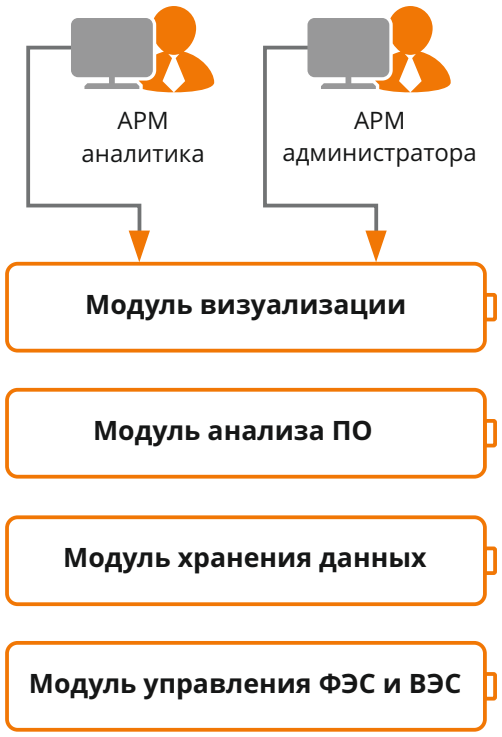
05

1. Файлы сначала проверяются антивирусным средством.
2. Веб и почтовый трафик компании фильтруется на наличие программ, офисных файлов и ссылок.
3. Отфильтрованные файлы направляются в систему для анализа их поведения.
4. При обнаружении в поведении вредоносной активности система помещает файл в карантин и направляет уведомление пользователю и службе безопасности.
5. В случае, если файл безопасен, ссылка на файл из системы передается пользователю.



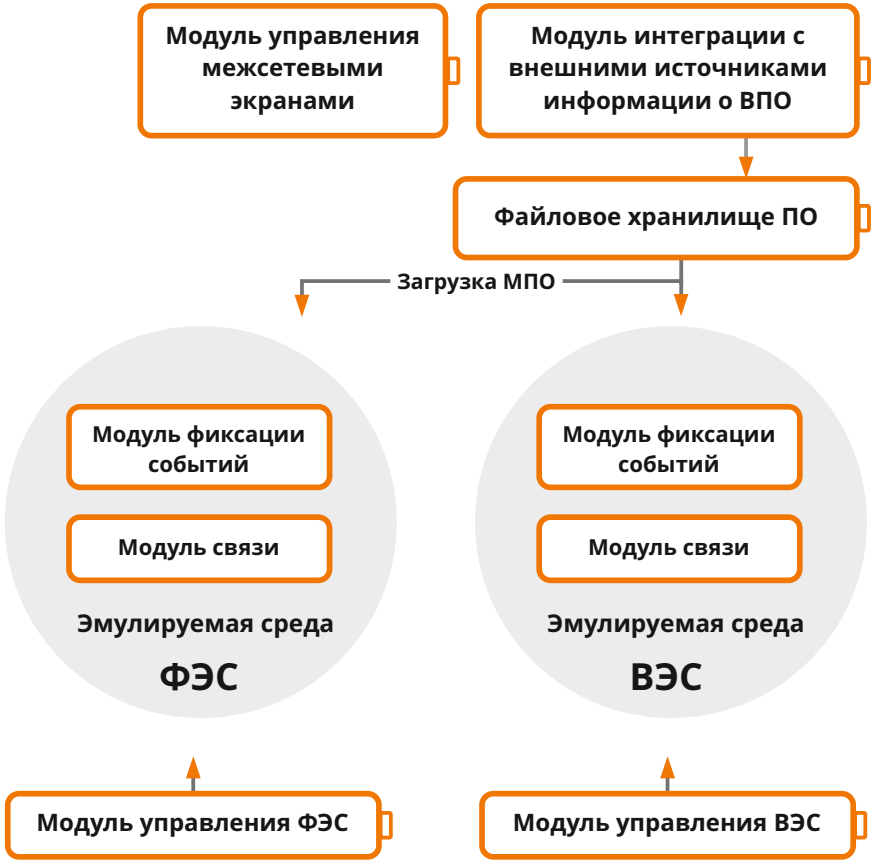
ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

06



Подсистема анализа и управления

Подсистема обеспечения сетевой безопасности



Подсистема исследования МПО «Песочница»

ПРЕИМУЩЕСТВА СИСТЕМЫ

07

Параметры	Check Point SandBlast	FireEye FireEye	Cisco ThreatGRID	paloalto WildFire	AV SOFT Athena
Эмуляция работы пользователя	✓	✓	✓	✗	✓
Эмуляция корпоративных приложений и данных (кастомизация «песочниц»)	✗	✗	✗	✗	✓
Экспертный режим работы с детальной настройкой эмулируемой среды	✗	✗	✓	✗	✓
Анализ файлов без отправки данных за периметр компании	✓	✓	✗	✗	✓
Отечественная разработка всех компонентов системы (оперативное реагирование)	✗	✗	✗	✗	✓
Поддерживаемые ОС	Windows XP, 7, 8.1	Windows XP, 7 Mac OS X, Android (облако), iOS (облако)	Windows XP, 7	Windows XP, 7	Windows XP /Vista / 7 / 8.1 / 10 Windows Server

БЛИЖАЙШИЕ РЕЛИЗЫ

08

Готовяться к выходу версии системы:

- IOS
- Android
- Windows Phone

ОС на базе ядра Linux, включая отечественные:

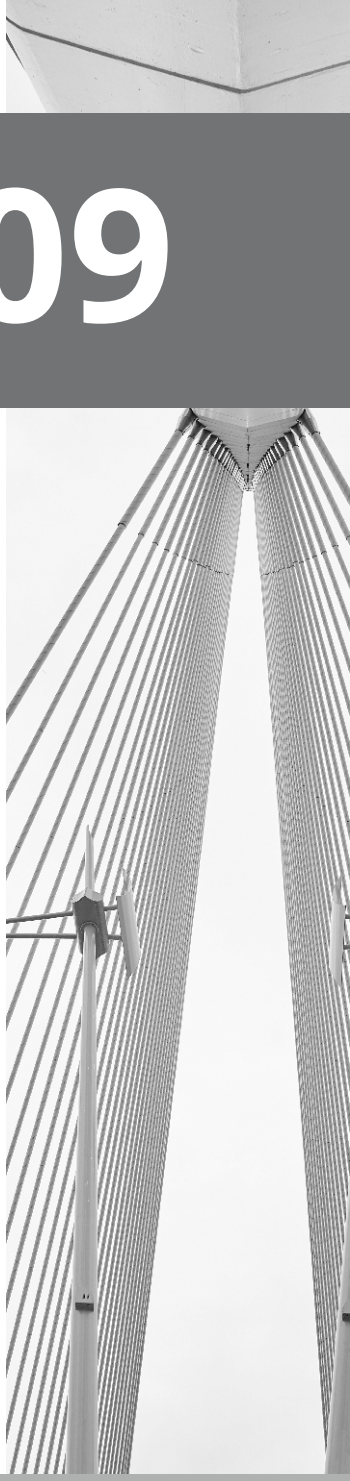
- Astra Linux
- ROSA Linux
- ALT Linux
- CentOS
- Ubuntu
- Red Hat

ЛИЦЕНЗИИ СИСТЕМЫ

09

№	Виды лицензий	Минимальные требования к установке	Рекомендованный режим использования ПК
1	Minimal (лицензия A) 6 виртуальных машин на 500 исследований в сутки	RAM 32, SSD 500 GB, CPU cores 4	Проверка в экспертном режиме Анализ только исполняемых файлов из входящего интернет трафика.
2	Advanced (лицензия B) 30 виртуальных машин на 2 500 исследований в сутки	RAM 128, SSD 2 TB, CPU cores 24	Проверка исполняемых файлов и почтовых вложений из входящего интернет трафика организации до 100 пользователей*.
3	Unlimited (лицензия C) Неограниченное количество виртуальных машин	RAM 256, SSD/RAID 10 TB, CPU cores 48	Проверка исполняемых файлов и почтовых вложений из входящего интернет трафика организации до 100 пользователей*.

* - зависит от объема входящего интернет трафика (активности пользователей в Интернете)



КОНТАКТЫ

+7 (495) 988-92-25

office@avsw.ru

127106, Москва, ул. Гостиничная, д.5

www.avsw.ru

СПАСИБО ЗА ВНИМАНИЕ!