



SOWA

Роль API Gateway и WAF в защите АСУ ТП

Дмитрий Вандышев

Владелец продукта Platform V SOWA, СберТех

В чем проблема — ложное ощущение безопасности



Приложения, написанные для АСУ ТП используются десятилетиями



Отсутствие поддержки вендора или самого вендора ☹



Потенциальная возможность удаленной блокировки импортного оборудования в случае его доступности из сети Интернет с использованием каких-либо недеklarированных возможностей



Внешние и внутренние сети небезопасны

Потребности



Безопасная интеграция
корпоративной сетью



Административные
доступы



Интерфейсы удаленного
подключения внешней поддержки



Безопасность
внутренних систем

Потребности



Безопасная интеграция
корпоративной сетью



Административные
доступы



Интерфейсы удаленного
подключения внешней поддержки



Безопасность
внутренних систем

Zero Trust

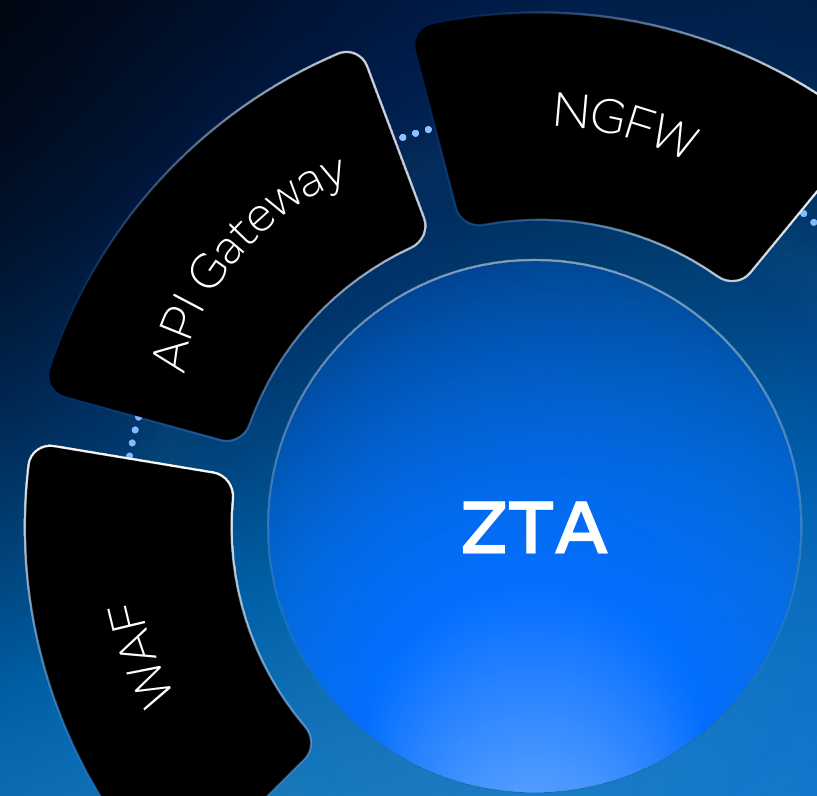
Почему Zero Trust?

Угрозы всегда присутствуют как извне, так и внутри

Каждый запрос должен быть аутентифицирован и авторизован

Внутренняя сеть не является доверенной

Сетевой трафик всегда несет угрозу



Чем полезен API Gateway и WAF в реализации концепции Zero Trust

01

API Gateway

позитивная модель безопасности
допускает только заведомо хорошее

-
- Единая точка входа и контроля API-запросов.
А также применение единой политики безопасности
 - Микросегментация сети, политики минимальных привилегий
 - Защита от угроз, снижает риски OWASP TOP 10 API
 - Аутентификация и авторизация

02

WAF

негативная модель безопасности
блокирует только заведомо плохое

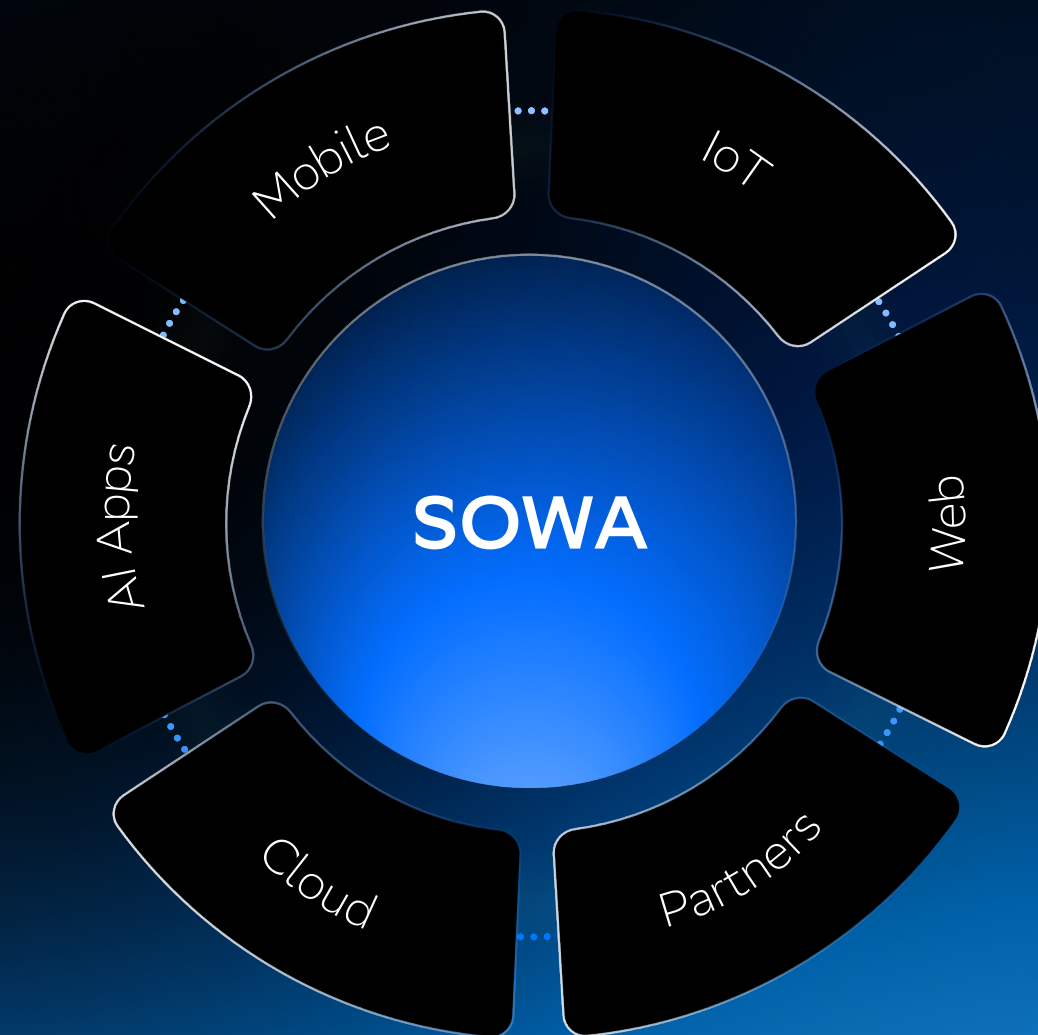
-
- Выявление угроз и блокировка атак
 - Мониторинг и журналирование
 - Глубокий анализ трафика
 - Фокусируется на OWASP Top 10



Platform V SOWA

Что такое Platform V SOWA

API Security Gateway, который обеспечивает безопасность и интеграцию API в различных сегментах сети и каналах обслуживания



Platform V SOWA API Security Gateway

с 2017 года

в промышленной
эксплуатации

99,99%

отказоустойчивость*

17 000+

постоянно действующих
виртуальных машин

50 000+

транзакций в секунду
в рамках одной инсталляции

24/7

без перерыва
на обслуживание

Безопасность корпоративного уровня

Ключевые сервисы Сбера уже более 7 лет используют Platform V SOWA для обеспечения безопасности API и защиты критичной информации

Сбербанк Онлайн

sberbank.ru

СБЕР Бизнес

Кредитный конвейер

РРПО

Platform V SOWA включен
в РРПО и не использует в составе
коммерческих лицензий

Проверено профессионалами

Тестирование на проникновение RedTeam
компании Bi.Zone

*Максимальная доступность клиентских систем на уровне программного обеспечения, достигаемая в зависимости от используемой инфраструктуры развертывания платформы

Функции Platform V SOWA

Безопасность

- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Security Engine



Функции Platform V SOWA

Безопасность

- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Security Engine

SOWA

Интеграция

- Поддержка множества прикладных протоколов (включая IoT-протоколы)
- Конвертация прикладных протоколов
- Подключение протокола, разработанного клиентом
- Реализация концепции Open API
- Интеграция с облачными сервисами

Функции Platform V SOWA

Безопасность

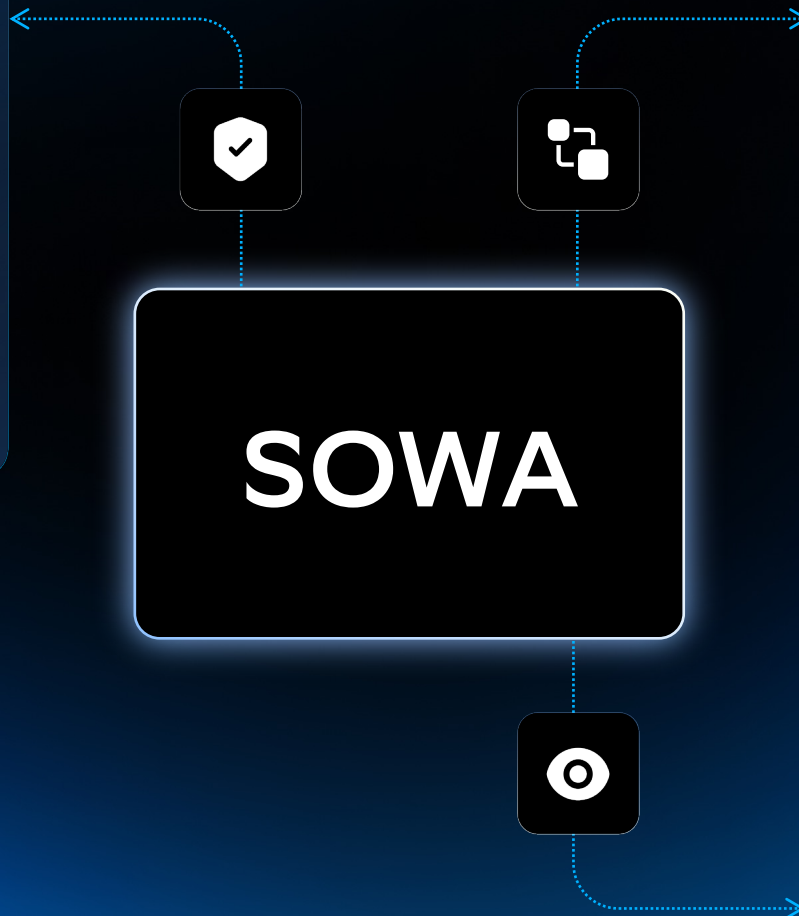
- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Security Engine

Интеграция

- Поддержка множества прикладных протоколов (включая IoT-протоколы)
- Конвертация прикладных протоколов
- Подключение протокола, разработанного клиентом
- Реализация концепции Open API
- Интеграция с облачными сервисами

Контроль

- Лимитирование запросов
- Whitelist/Blacklist
- Логирование и аудит
- Трассировка OpenTelemetry
- Маршрутизация контента
- Интеграция с системами мониторинга Zabbix, Prometheus и др.



Функции Platform V SOWA

Безопасность

- Аутентификация, авторизация
- Трансляция токенов безопасности
- Валидация сообщений по схеме
- Фильтрация сообщений
- Шифрование канала
- Интеграция с антивирусным ПО, DLP, SOC/SIEM
- Security Engine

Интеграция

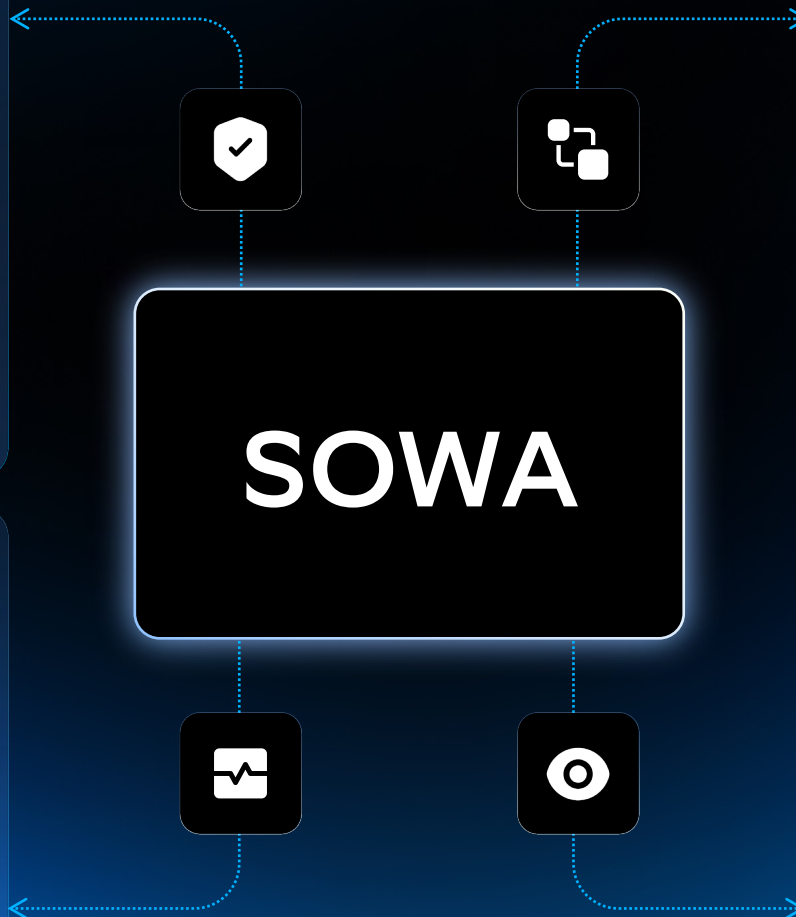
- Поддержка множества прикладных протоколов (включая IoT-протоколы)
- Конвертация прикладных протоколов
- Подключение протокола, разработанного клиентом
- Реализация концепции Open API
- Интеграция с облачными сервисами

Оптимизация

- Терминация SSL-/TLS-сессий
- Кеширование данных
- Различные стратегии балансировки нагрузки, Sticky session, Dynamic resolve DNS

Контроль

- Лимитирование запросов
- Whitelist/Blacklist
- Логирование и аудит
- Трассировка OpenTelemetry
- Маршрутизация контента
- Интеграция с системами мониторинга Zabbix, Prometheus и др.



Security Engine

Задача

Есть сообщение

01

В сообщении
есть Multipart-Form

02

В одном из полей
ASN1-конверта лежит XML

03

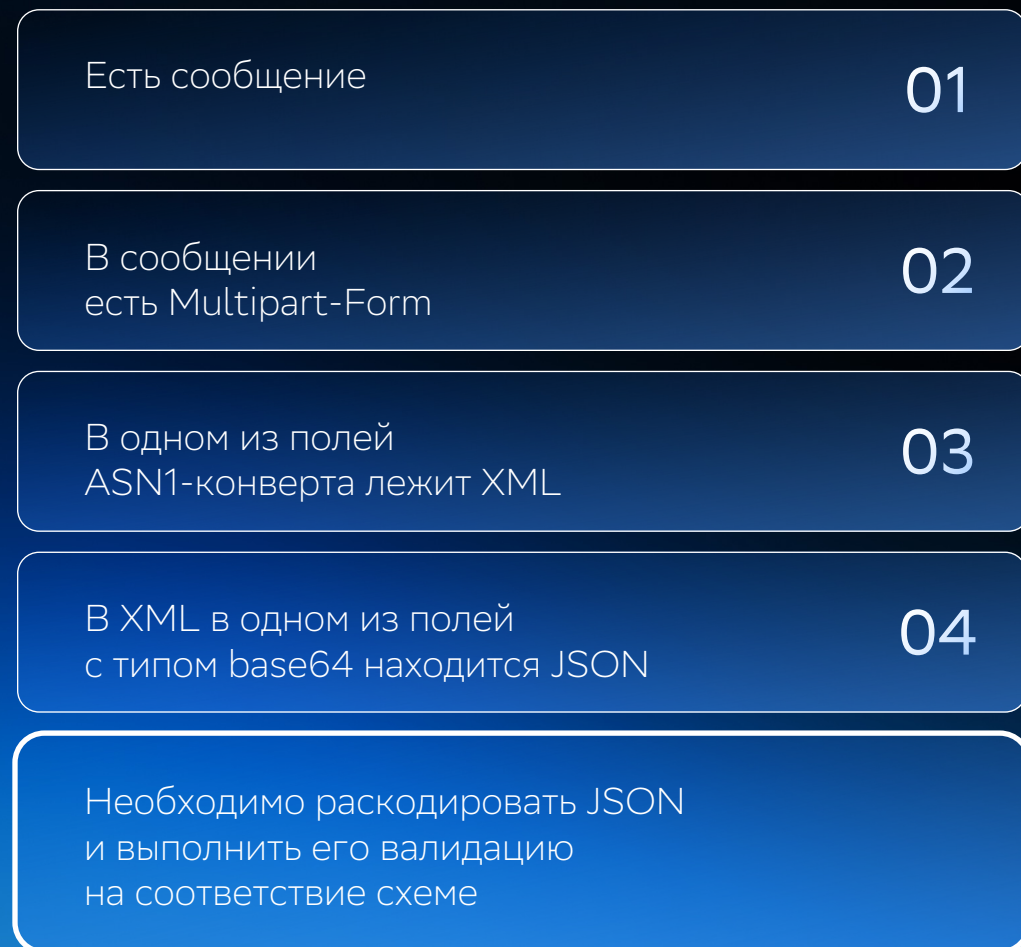
В XML в одном из полей
с типом base64 находится JSON

04

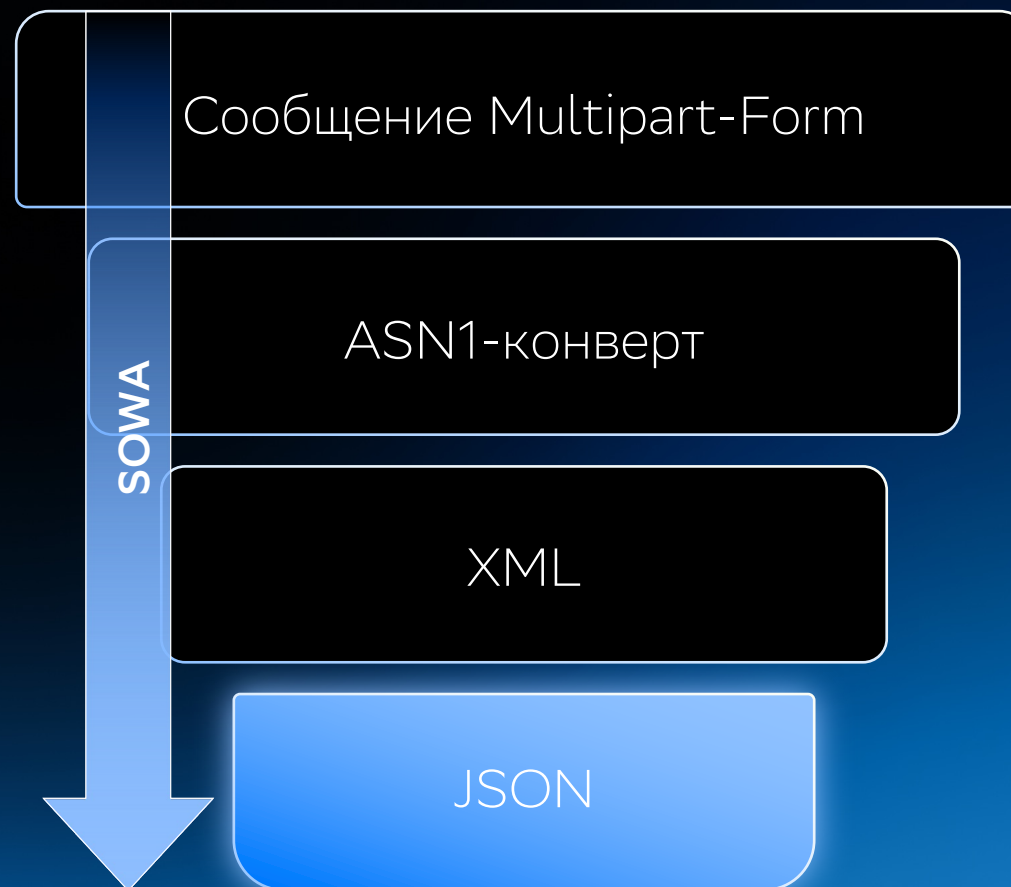
Необходимо раскодировать JSON
и выполнить его валидацию
на соответствие схеме

Security Engine

Задача



Решение



Как Platform V SOWA помогает защищать АСУ ТП

SOWA

- Интегрируется с антивирусным ПО, DLP, SIEM
- Комбинация негативной и позитивной модели безопасности для фокусной защиты (API Gateway + WAF)
- Позволяет безопасно интегрировать различные legacy-системы
- Предоставляет широкие возможности валидации контента по схеме (XML, JSON, WSDL, XSD, PROTOBUF, GraphQL, OpenAPI & Swagger)
- Поддерживает проверку широкого спектра протоколов прикладного уровня (HTTP 0.X/1.X/2.0, WebSocket, ICAP, Kafka, IBM MQ, gRPC, Artemis MQ)
- Позволяет добавить дополнительные прикладные протоколы обмена данных
- Обработывает и проверяет сложные составные сообщения

Как Platform V SOWA помогает защищать АСУ ТП

SOWA

- Интегрируется с антивирусным ПО, DLP, SIEM
- Комбинация негативной и позитивной модели безопасности для фокусной защиты (API Gateway + WAF)
- Позволяет безопасно интегрировать различные legacy-системы
- Предоставляет широкие возможности валидации контента по схеме (XML, JSON, WSDL, XSD, PROTOBUF, GraphQL, OpenAPI & Swagger)
- Поддерживает проверку широкого спектра протоколов прикладного уровня (HTTP 0.X/1.X/2.0, WebSocket, ICAP, Kafka, IBM MQ, gRPC, Artemis MQ)
- Позволяет добавить дополнительные прикладные протоколы обмена данных
- Обработывает и проверяет сложные составные сообщения

WAF + API Gateway + Security Engine



**Дмитрий
Вандышев**

Владелец продукта
Platform V SOWA

Остались вопросы?

Свяжитесь с нами любым удобным для вас способом:



Мой Telegram



Наш Сайт