SQUAD

Как защитить API сервисы в рамках цифровой трансформации

Нагин Павел, руководитель по развитию продукта

www.squadsec.ru

SQUAD

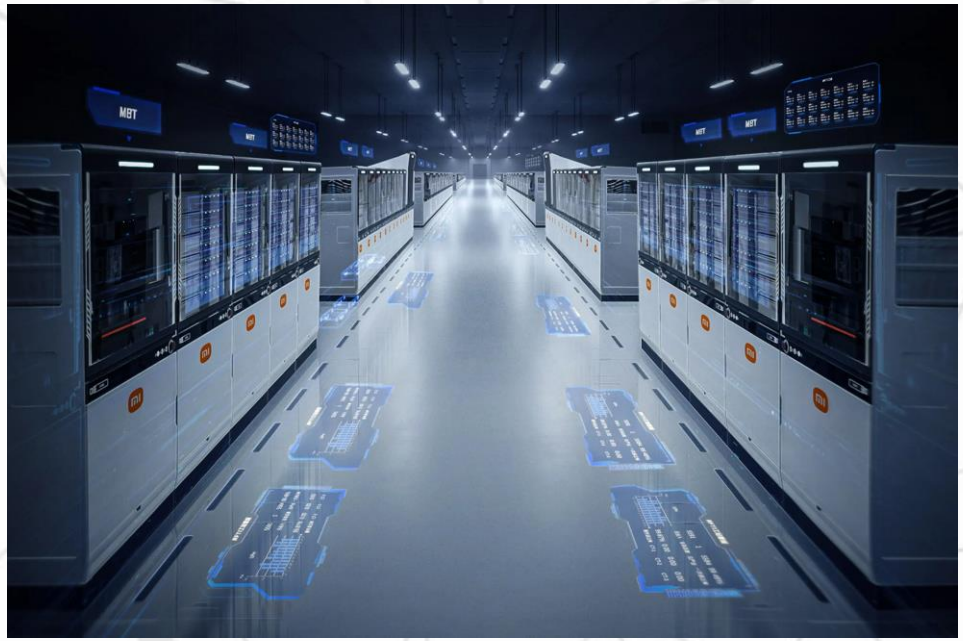
Использование API в индустриальном секторе

Области применения:

- Идустриальный Интернет Вещей (Industrial IOT)
- Интеграция производственных процессов с бизнес ИТ-системами
- Сбор метрик и повышение эффективности производства
- Контроль качества
- Взаимодействие с партнерами

Построение цифровых заводов предполагает активное использование API:

1. Siemens - Catalogue of Industrial APIs and SDKs https://developer.siemens.com/apis.html
2. General Electric - Plant Applications: https://www.ge.com/digital/documentation/proficy-plant-applications/

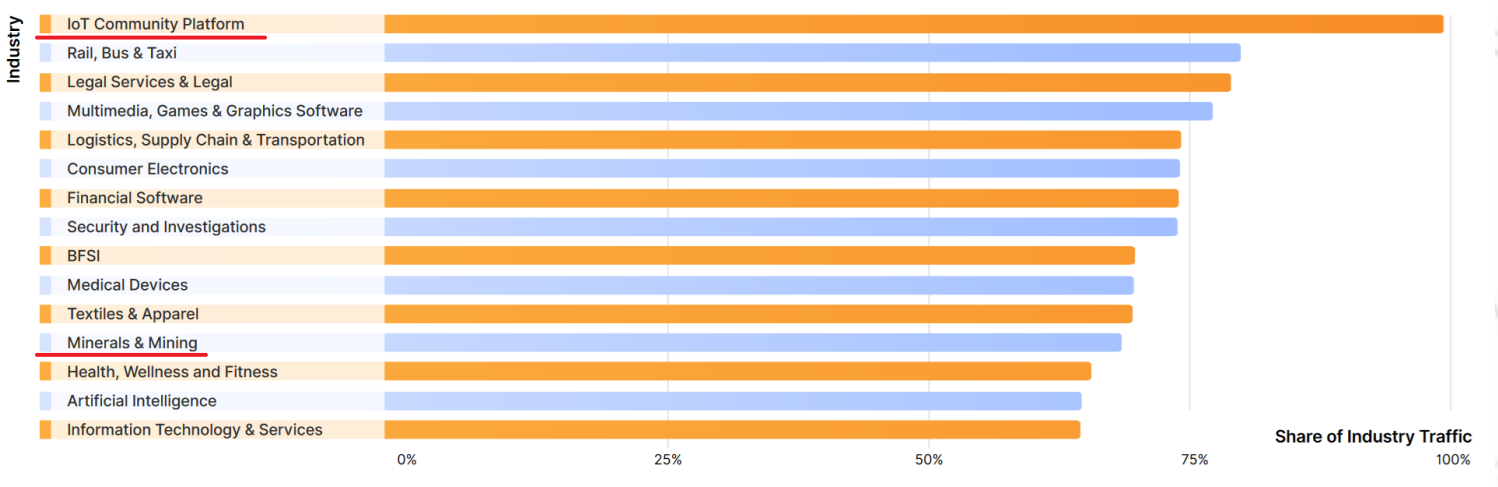


SQUAD

Трафик API

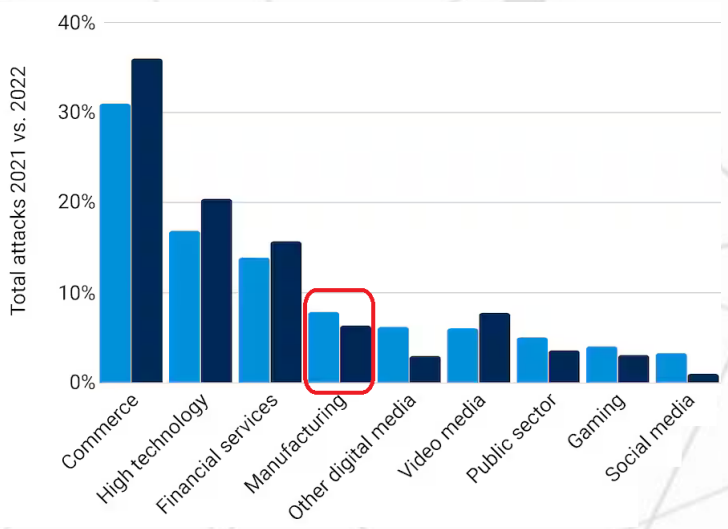
*Согласно данным **Cloudflare** с 01.10.2022 по 31.08.2023 в их глобальной сети **более 53%** динамического контента в HTTP генерировали API (контент, который изменяется в зависимости от факторов, характерных для пользователя, таких как время посещения, местоположение и устройство).*

Топ 15 секторов по API трафику



***Akamai**, 2023: Атаки на API остаются критической угрозой для организаций*

Количество web-атак в 2021/2022

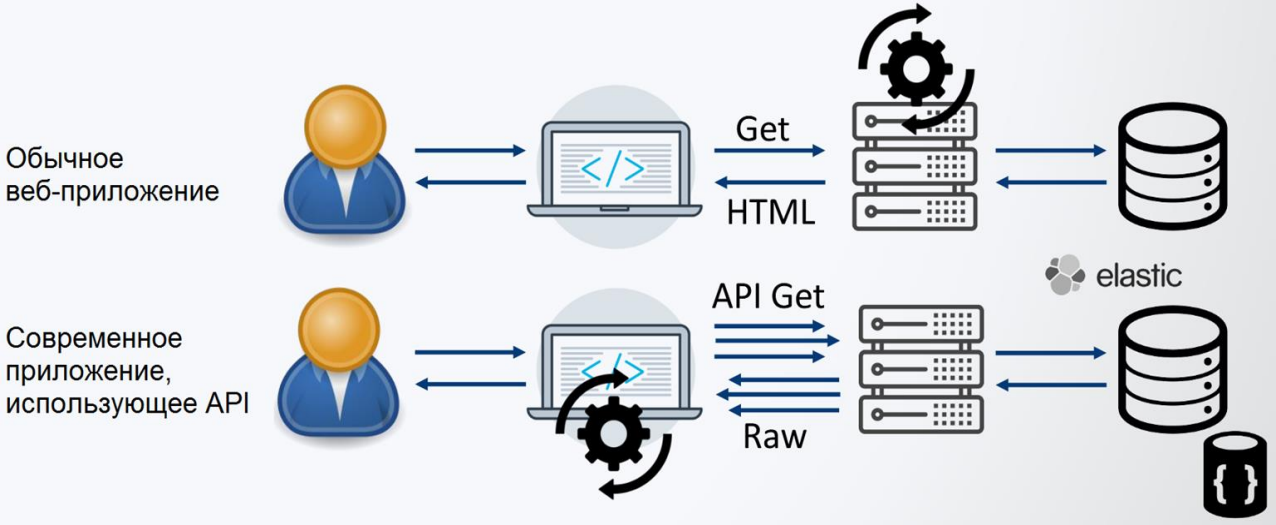


SQUAD

Отличия API от обычного веб-приложения

Ключевые отличия API от web с т.з. безопасности:

1. API раскрывают логику и особенности реализации приложения.
2. В HTTP запросах передается большее количество параметров.
3. Другая схема предоставления доступов (JWT & API Keys).
4. Растет скорость создания и изменения новых сервисов (shadow API).



SQUAD

Угрозы согласно OWASP

Top 10 **API** Security Risks

- **API1:2023** - Broken Object Level Authorization
- **API2:2023** - Broken Authentication
- **API3:2023** - Broken Object Property Level Authorization
- **API4:2023** - Unrestricted Resource Consumption
- **API5:2023** - Broken Function Level Authorization
- **API6:2023** - Unrestricted Access to Sensitive Business Flows
- **API7:2023** - Server-Side Request Forgery
- **API8:2023** - Security Misconfiguration
- **API9:2023** - Improper Inventory Management
- **API10:2023** - Unsafe Consumption of APIs

VS

Top 10 **Web Application** Security Risks

- **A01:2021** - Broken Access Control
- **A02:2021** - Cryptographic Failures
- **A03:2021** - Injection
- **A04:2021** - Insecure Design
- **A05:2021** - Security Misconfiguration
- **A06:2021** - Vulnerable and Outdated Components
- **A07:2021** - Identification and Authentication Failures
- **A08:2021** - Software and Data Integrity Failures
- **A09:2021** - Security Logging and Monitoring Failures
- **A10:2021** - Server-Side Request Forgery

SQUAD

Примеры атак

Атаки на API:

- **04.2023** - уязвимость в API "Росреестра" позволяла по кадастровому номеру получить персональные данные: https://habr.com/ru/news/726480/
- **06.2023** - стало известно об уязвимостях в API на дилерском портале Honda https://xakep.ru/2023/06/09/honda-api/
- **11.2023** - у платформы обучения duolingo через API было украдено 2.6 млн записей https://cybernews.com/security/hackers-exposed-duolingo-users-more-available-scraping/
- **05.2024** - через API были украдены 49 млн записей о клиентах Dell
- **01.2024** - API Trello использовали для выявления e-mail 15 млн учётных записей сервиса https://habr.com/ru/news/788514/
- **07.2024** - записи из API Trello выложены в свободный доступ https://habr.com/ru/posts/829482/

Атаки на промышленные предприятия:

- **02.2023** - Applied Materials потеряла $250M из-за атаки шифровальщиков: https://finance.yahoo.com/news/applied-materials-sales-shortfall-linked-225203127.html
- **08.2024 –** Halliburton, вторая по величине в мире нефтесервисная компания, расследует инцидент: https://www.bleepingcomputer.com/news/security/halliburton-cyberattack-linked-to-ransomhub-ransomware-gang/

SQUAD

Защита API

Ключевые выводы из исследования Gartner:

- API часто приводят к утечкам данных, основная причина – некорректно настроенные доступы
- Нужны дополнительные усилия по защите API таке как: rate limiting, token validation, session management and transport security
- Основные функции API защиты: discovery, security posture management and runtime protection
- Первые клиенты покупали standalone защиту API, сейчас рынок консолидируется за счет поставщиков WAAP (Web Application and API Protection), и CIPS (Cloud Infrastructure and Platform Service).

Рекомендации Gartner:

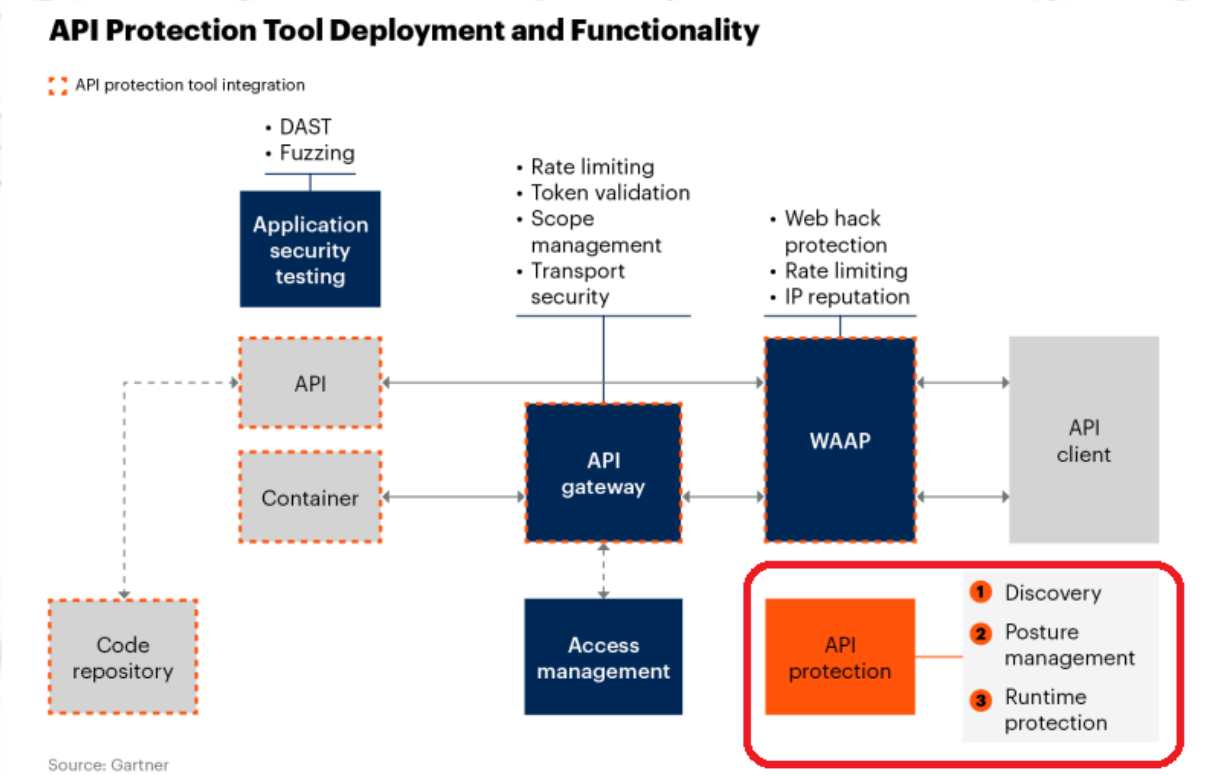
- Нужно начинать с обнаружения и категоризации API
- Затем выполнять непрерывную оценку состояния безопасности для инвентаризированных API
- Заложите дополнительные ресурсы на runtime защиту API
- Оцените возможность использовать опции по защите от WAAP и API Gateway

SQUAD

Основные функции защиты API

Защита API должна фокусироваться на:

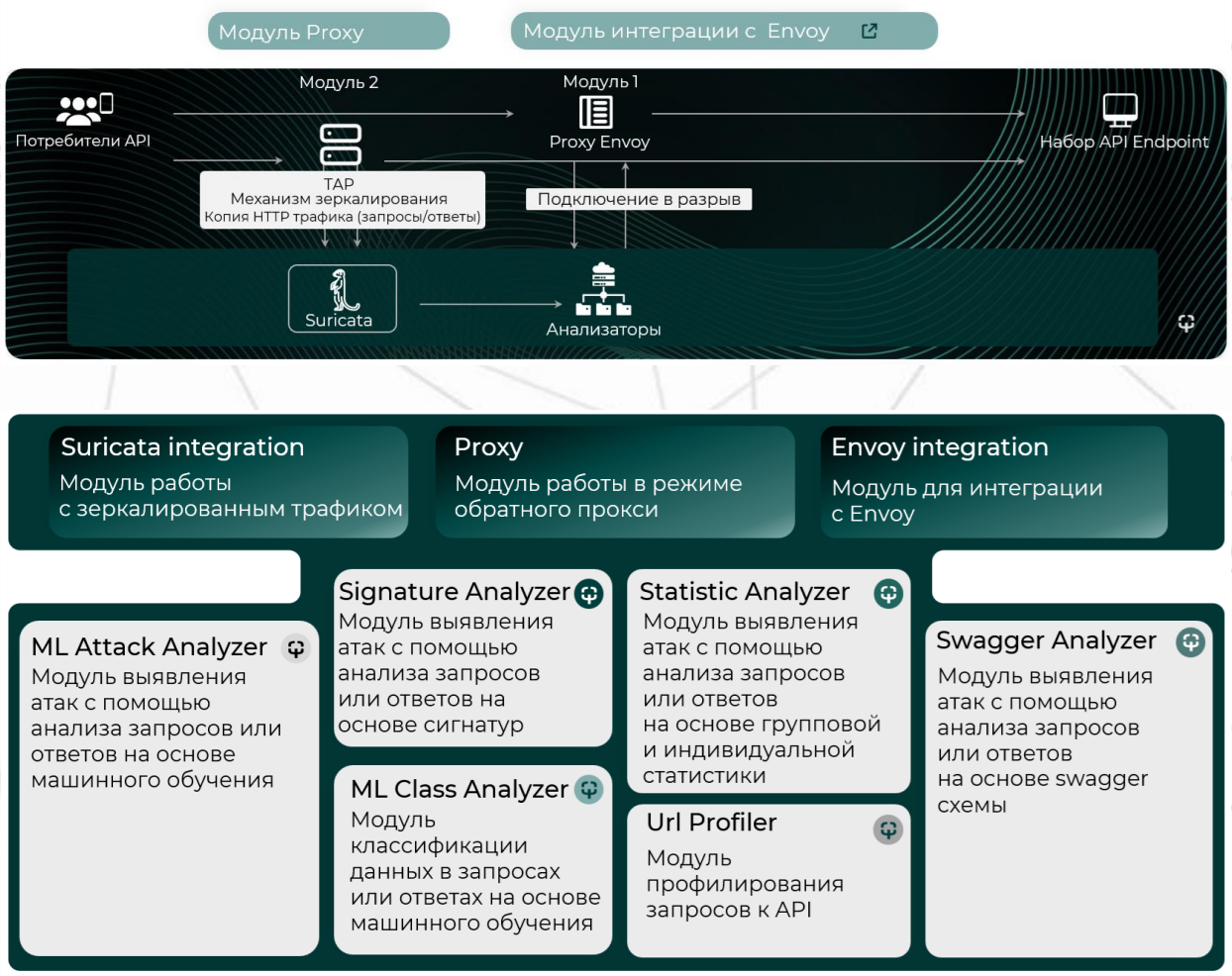
1. API discovery
2. API security posture management
3. API runtime protection (API detection and response)



SQUAD

Дополнительные возможности

- Защита от атак (вкл. OWASP API TOP 10)
- Детектирование и предотвращение передачи КИ
- Работа в режиме детектирования и блокировки
- Поддержка установки агентов (nginx, istio, …)
- Обнаружение эндпойнтов API
- Поддержка схем OpenAPI (Swagger)
- Активные и пассивные проверки на уязвимости
- Отслеживание сессий и пользователей
- Защита от ботов
- On-prem/cloud/hybrid
- Security Data Lake
- …



SQUAD

AI?

- Анализ пользовательской активности и вывление аномалий
- Повышение точности при инвентаризации, обогащение данными по endpoint-ам
- Приоритизация атак и уязвимостей (risk scoring)
- Детектирование ботов
- Анализ security data lake (общие паттерны атак, связи между пользователями и endpoint-амич, …)
- Рекомендации по правилам блокировки и мерам митигации (LLM)

SQUAD

Альтернативные способы защиты API

WAF

WAF эффективен для защиты от типов угроз OWASP TOP10, но имеет технические ограничения для защиты от угроз OWASP API TOP10. Современные WAF обычно не выполняют инвентаризацию API и передаваемых в них данных.

API Manager

Решение обычно умеет собирать аналитику и выполнять инвентаризацию, функции безопасности как правило реализуются с помощью аутентификации, авторизации и шифрования при передаче данных.

DevSecOps

Подход позволяет значительно повышать безопасность разрабатываемых приложений/сервисов, однако не является средством мониторинга или защиты, позволяющим активным способом предотвращать атаки и утечки данных.

SQUAD

Почему WAF недостаточно

- Не защищает от угроз от угроз OWASP **API** TOP10, связанных с контролем доступов и инвентаризацией:
  API1:2023 - Broken Object Level Authorization
  API3:2023 - Broken Object Property Level Authorization
  API4:2023 - Unrestricted Resource Consumption
  API5:2023 - Broken Function Level Authorization
  API9:2023 - Improper Inventory Management
- Анализирует запросы вне контекста соединения и бизнес-логики приложения, даже если такие функции есть, они требуют значительного времени на настройку и поддержку
- В первую очередь ориентирован на контроль и управление доступом, а не на проверку надлежащего использования
- Не строит и не проверяет сооответствие схеме OpenAPI (Swagger)
- Анализирует атаки, а не уязвимости (забытые API, валидация токенов, лимиты по запросам, ...)

SQUAD

Выводы

- Каждый делает сам :)
- Использование API, как и средств по их защите, будет расти
- Вендоры WAF и API Gateway будут инвестировать в защиту API, в том числе через покупку отдельных игроков на рынке
- Средства защиты API будут предлагать различные наборы функций, акцентируя фокус на том, что у них более развито
- AI будет выполнять вспомогательные задачи, не оказывая решающей роли при блокировке атак на API в реальном времени