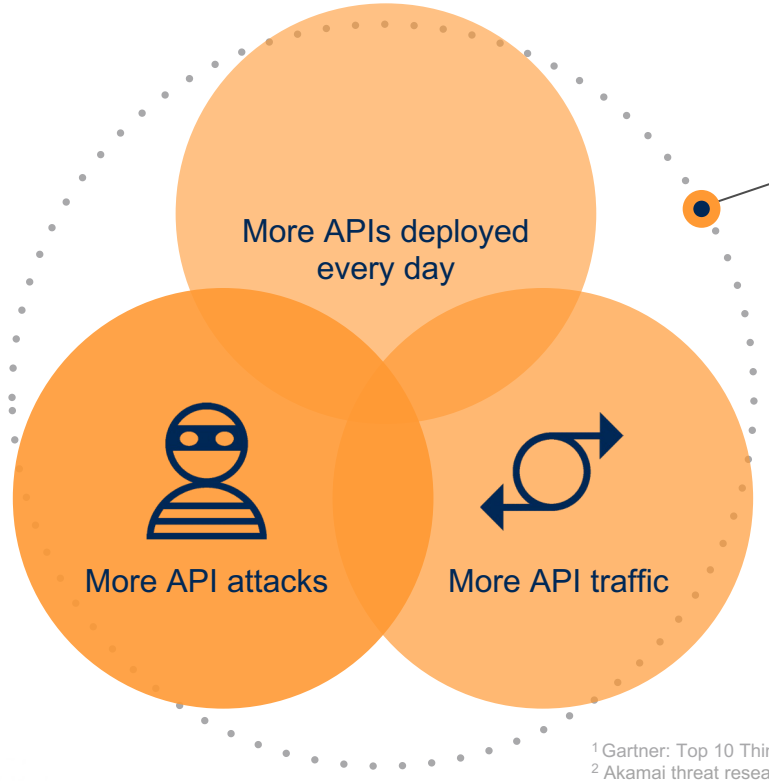
KHNOG : Strengthening API Security from afterthought to forefront

Chao Yin Loong

Akamai

The API Security Environment



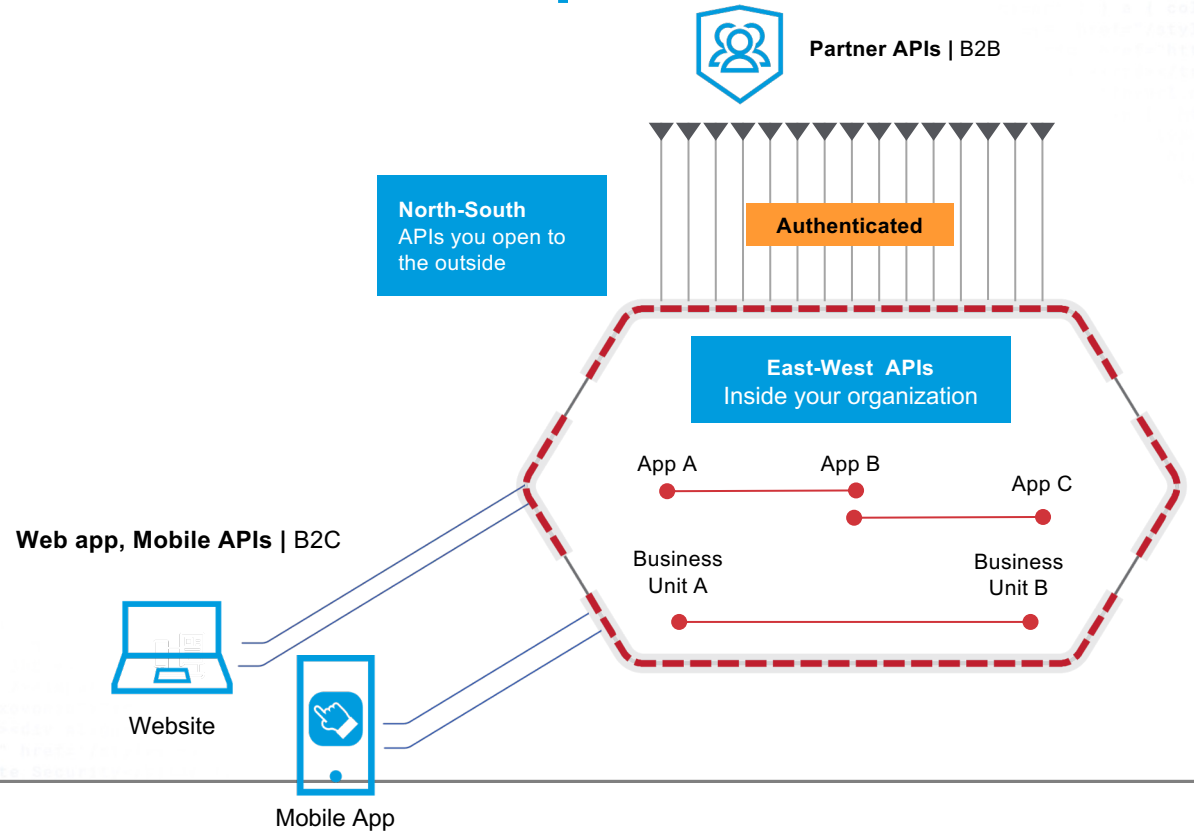
Existing application security solutions not built for APIs

By 2024, API abuses and related data breaches will nearly **double.**[1]

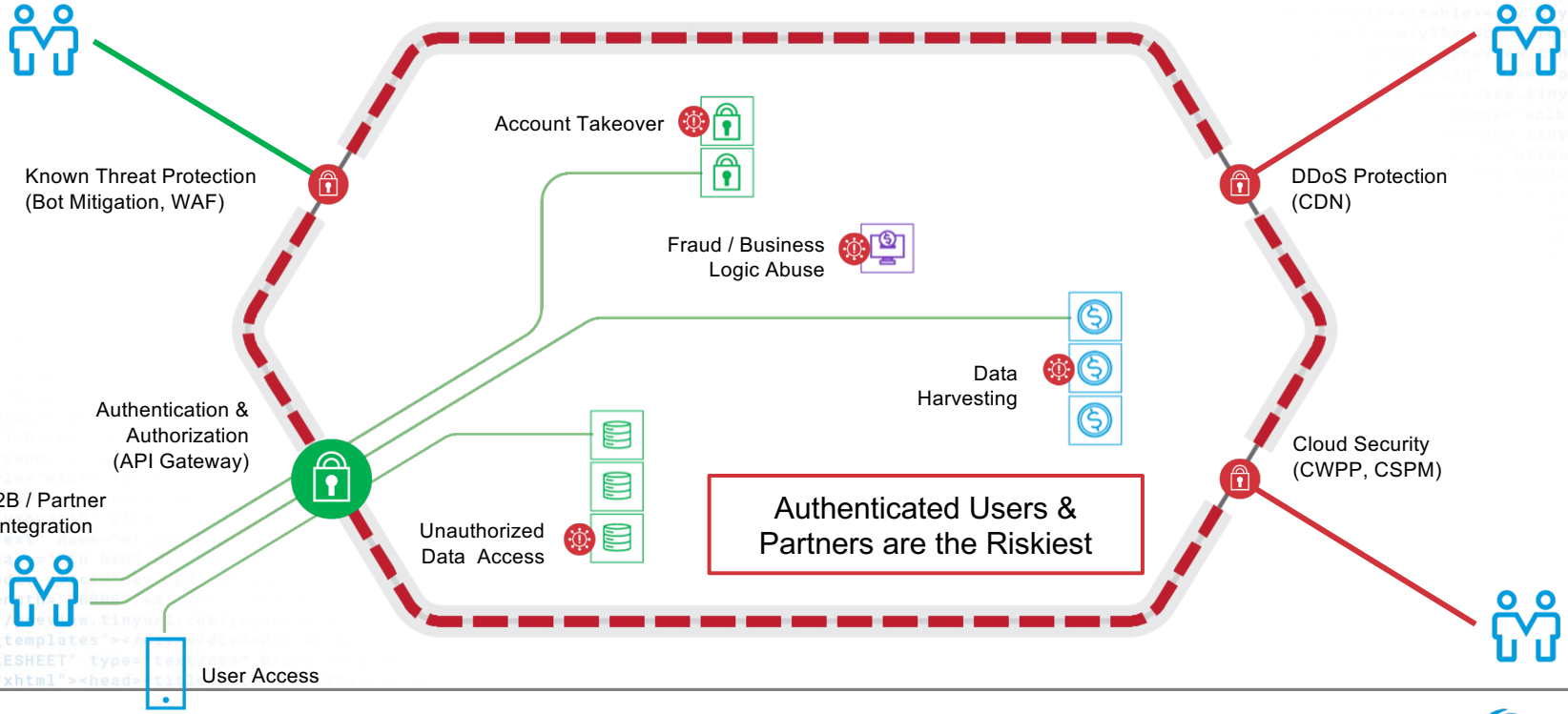
31% of web traffic is APIs [2]

[1] Gartner: Top 10 Things Software Engineering Leaders Need to Know About APIs
[2] Akamai threat researchers have identified that 31% of all traffic protected by Akamai is API traffic

What is your API landscape?



API Abuse Can Happen Beyond WAAP



Real world examples : Uber: Account Takeover

- How I could Have hacked your Uber Account (Anand Prakash, 2019)
- Anand got from a phone number/email address to full account takeover
- The vulnerabilities were quickly fixed by Uber

(1) POST /addDriver

(1) Error message with UUID

(2) POST /getConsentScreenDetails

(2) PII and access token

Uber

Real world examples : Uber: Account Takeover

```
POST /p3/fleet-manager/_rpc?rpc=addDriverV2 HTTP/1.1
Host: partners.uber.com
{"nationalPhoneNumber":"99999xxxxx","countryCode":"1"}
```

(1)

```
Response:
{"status":"failure","data":{"code":1009,"message":"Driver '
0xx5e-xxxxx-b01a-xxxx' not found"}}
```

```
POST /marketplace/_rpc?rpc=getConsentScreenDetails HTTP/1.1
Host: bonjour.uber.com
Connection: close
Content-Length: 67
Accept: application/json
Origin: https://bonjour.uber.com
x-csrf-token: xxxx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103
Safari/537.36
DNT: 1
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: xxxxx
{"language":"en","userUuid":"xxxx-776-4xxxx1bd-861a-837xxx604ce"}
```

(2)

{"status":"success","data":{"data":
{"language":"en","userUuid":"xxxxxx1e"},"getUser":
{"uuid":"cxxxxxc5f7371e","firstname":"Maxxxx","lastname":"XXXX","role"
:"PARTNER","languageId":1,"countryId":77,"mobile":null,"mobileToken":1
234,"mobileCountryId":77,"mobileCountryCode":"+91","hasAmbiguousMobile
Country":false,"lastConfirmedMobileCountryId":77,"email":"xxxx@gmail.c
om","emailToken":"xxxxxxxx","hasConfirmedMobile":"no","hasOptedInSmsMa
rketing":false,"hasConfirmedEmail":true,"gratuity":"0.3","nickname":"abc
@gmail.com","location":"00000","banned":false,"cardio":false,"token":"
b8038ec4143bb4xxxxxx72d","fraudScore":0,"inviterUuid":null,"pictureUrl
":"xxxxx.jpeg","recentFareSplitterUuids":
["xxx"],"lastSelectedPaymentProfileUuid":"xxxxxx","lastSelectedPayment
ProfileGoogleWalletUuid":null,"inviteCode":
{"promotionCodeId":xxxxx,"promotionCodeUuid":"xxxx","promotionCode":"m
anishas105","createdAt":{"type":"Buffer","data":
[0,0,1,76,2,21,215,101]},"updatedAt":{"type":"Buffer","data":
[0,0,1,76,65,211,61,9]}},"driverInfo":
{"contactInfo":"9999999999xx","contactInfoCountryCode":"+91","driverLic
ense":"None","firstDriverTripUuid":null,"iphone":null,"partnerUserUuid
":"xxxxxxx","receiveSms":true,"twilioNumber":null,"twilioNumberFormatt
ed":null,"cityknowledgeScore":0,"createdAt":{"type":"Buffer","data":
[0,0,1,84,21,124,80,52]},"updatedAt":{"type":"Buffer","data":
[0,0,1,86,152,77,41,77]},"deletedAt":null,"driverStatus":"APPLIED","dr
iverFlowType":"UBERX","statusLocks":null,"contactInfoCountryIso2Code":
"KR","driverEngagement":null,"courierEngagement":null},"partnerInfo":
{"address":"Nxxxxxxx","territoryUuid":"xxxxxx","company":"None","addre
ss2":"None","cityId":130,"cityName":"None","firstPartnerTripUuid":null
,"preferredCollectionPaymentProfileUuid":null,"phone":"","phoneCountry
Code":"+91","state":"None","vatNumber":"None","zipcode":"None","create
dAt":{"type":"Buffer","data":[0,0,1,84,21,124,80,52]},"updatedAt":
{"type":"Buffer","data":
[0,0,1,101,38,177,88,137]},"deletedAt":null,"fleetTypes":
[],"fleetServices":[],"isFleet":true},"analytics":
{"signupLat":133.28741199,"signupLng":111177.1111,"signupTerritoryUuid"
:"xxxxx","signupPromoId":null,"signupForm":"iphone","signupSessionId":
"xxxxxxx","signupAppVersion":"2.64.1","signupAttributionMethod":null,"
createdAt":{"type":"Buffer","data":[0,0,1,76,2,21,219,1]},"updatedAt":
{"type":"Buffer","data":
[0,0,1,76,2,21,219,1]},"signupCityId":130,"signupDeviceId":null,"signu
pReferralId":null,"signupPromoCode":null,"signupPromoCodeUuid":null,"s
ignupPromoUuid":null,"signupMethod":"REGULAR"},"createdAt":
{"type":"Buffer","data":[0,0,1,76,2,21,215,153]},"updatedAt":
{"type":"Buffer","data":
[0,0,1,102,81,35,153,135]},"deletedAt":null,"tenancy":"uber/production
","mobileConfirmationStatus":"MOBILE_NOT_CONFIRMED","nationalId":null,
"nationalIdType":null,"merchantLocation":null,"lastConfirmedMobile":"x
xxxxxxxx","requestedDeletionAt":null,"dateOfBirth":xxxxxx,"userTypes"
:null,"preferredName":"xxxxxxxx","freightInfo":null,"tempPictureUrl":n
ull,"identityVerified":null,"paymentEntityType":null,"riderEngagement"
:null,"identityRejectReasonUuid":null,"genderInferred":null,"genderIde
ntity":null,"genderDocumented":null,"riderIneligibleWhy":null,"default
PaymentProfileByProduct":null,"loginEligibility":null},"getDisclosureV
ersionUuid":"","getLocaleCopy":null}}

Real world examples : Uber: Account Takeover

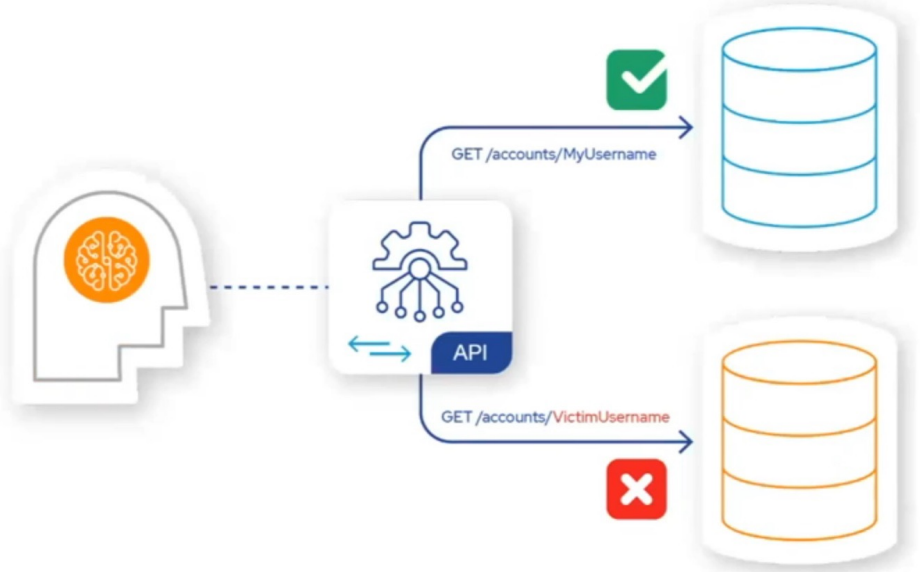
API3:2019 – Excessive data exposure

- The APIs exposed much more data than required to operate

Real world examples : Uber: Account Takeover

API1:2019 – **B**roken **O**bject **L**evel **A**uthorization

- Users can access resources that are not owned by them



Real world examples : Scoolio: Data Exposure

- Scoolio – German student app
- API exposed PII and more for any user in the paltform

(1) GET /api/v3/Explorer

(1) Profile IDs

(2) GET /api/v2/Profile/{ProfileID}

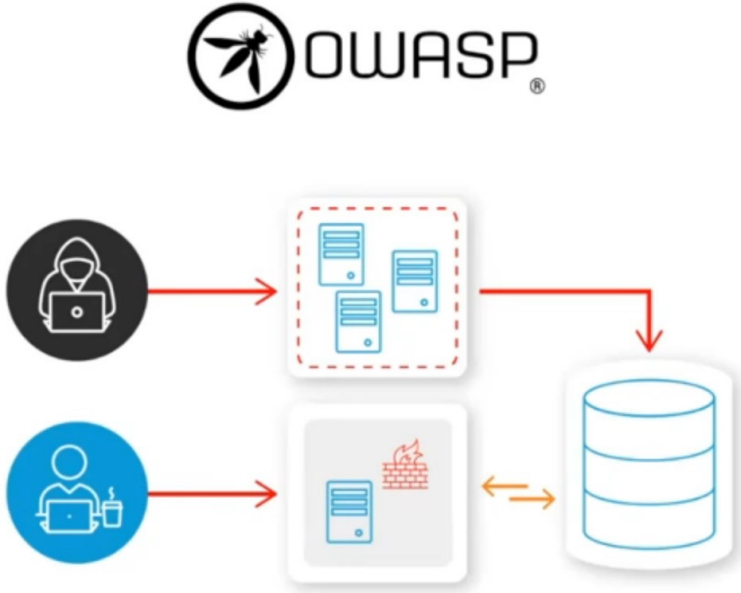
(2) PII (email,DOB, GPS location)

Real world examples : Scoolio Vulnerability

- API1:2019 – Broken object level authorization
  - Once again, PII of users is exposed to any user
- **UUID is a good practice** because it is hard to guess
  - ID is even easier to exploit by a simple iteration
- In this case, the UUID was obtained through another endpoint

Real world examples : Scoolio Vulnerability

- API9:2019 - Improper Assets Management
- Old API version exposing more PII still accessible
  - Also indicates an excessive data exposure of the old API



Real world examples : Scoolio Vulnerability

/api/**v3**/Profile/{ProfileID}


```
{
    "profileId": "26dad47a-8354-45f6-960e-ef05b58a6536",
    "schoolId": "85ce1b51-7da3-4bff-bb29-87d0553ae719",
    "clLvl": 9,
    "clExt": "B",
    "isAmbassador": false,
    "nickName": "MariaMaier2005",
    "slogan": "[redacted]",
    "emojiCount": "2",
    "userTilesIds": [],
    "profileImageId": "154bf0cd-2c53-4a6e-8590-c5879086373c",
    "explorerImageId": "f49b8c4f-76a8-40bd-8716-458fd4cf4080",
    "dayOfBirth": "2005-10-01T00:00:00Z",
    "emailConfirmed": true,
    "blocked": false
}
```


/api/**v2**/Profile/{ProfileID}


```
{
  "profileId":"26dad47a-8354-45f6-960e-ef05b58a6536",
  "schoolId":"85ce1b51-7da3-4bff-bb29-87d0553ae719",
  "clLvl":9,
  "clExt":"B",
  "email":"mariamaiercool2005@gmail.com",
  "parentsemail":"dannyroller@gmail.com",
  "parentsAcceptedConditionsDate":"2021-03-12T13:23:33",
  "acceptedConditionsDate":"2021-03-12T11:13:12",
  "slogan": "[redacted]",
  "imgIds":[
    "006642e8-4ec2-4b8d-9077-4d6f7a5a7c2d"
  ],
  "position":{
    "lon":13.7491207,
    "lat":51.0716188,
    "updatedAt":"2021-10-22T05:09:31Z"
  },
  "nickName":"MariaMaier2005",
  "dayOfBirth":"2005-10-01T00:00:00Z",
  "isAmbassador":false,
  "emojiCount":"2",
  "userTilesIds":[

  ],
  "profileImageId":"154bf0cd-2c53-4a6e-8590-c5879086373c",
  "explorerImageId":"f49b8c4f-76a8-40bd-8716-458fd4cf4080",
  "emailConfirmed":true,
  "blocked":false
}
```

Real world examples : Coinbase

coinbase

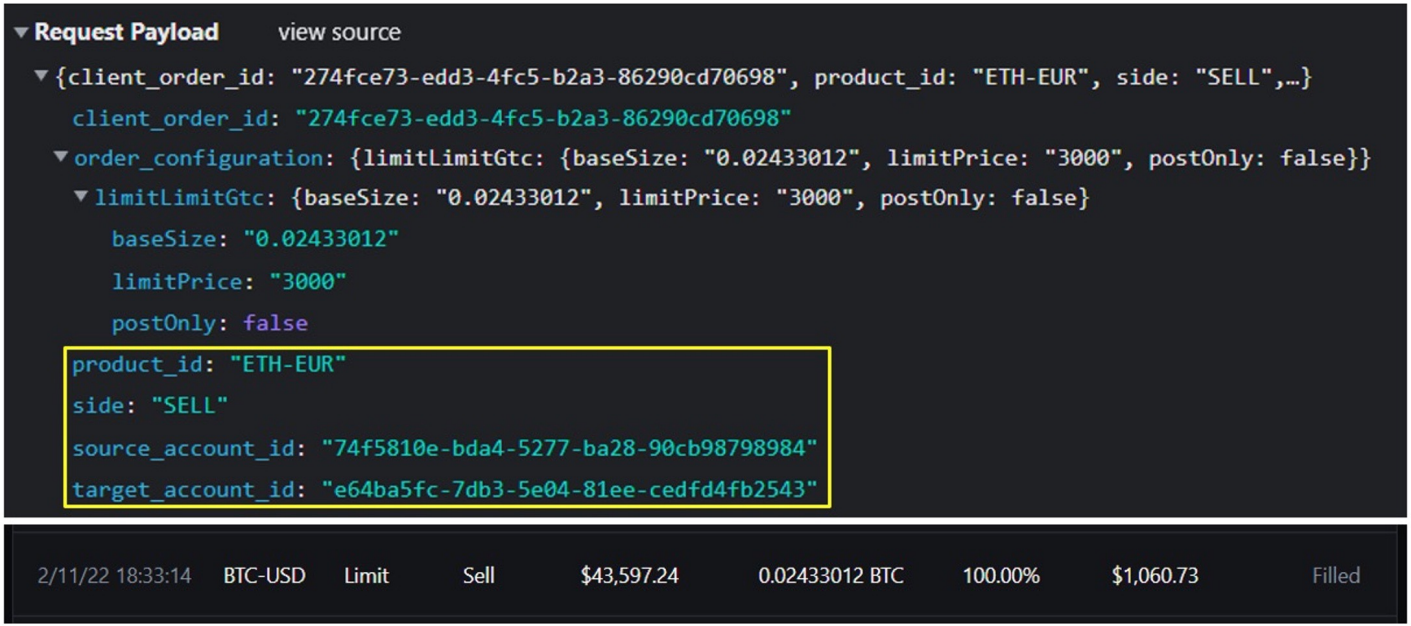
What happened:

- User scraped API calls from web UI
- Identified 4 key parameters for any Coinbase transaction
- Manipulated the parameters via API calls
- Sold crypto they DID NOT own

OWASP API #1
Broken Object Level Authorization

Real world examples : Coinbase

coinbase



Real world examples : Coinbase

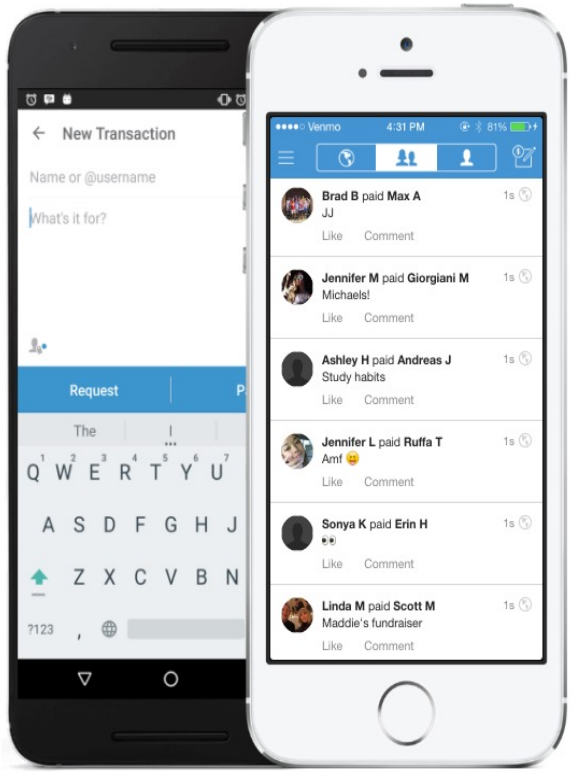
coinbase

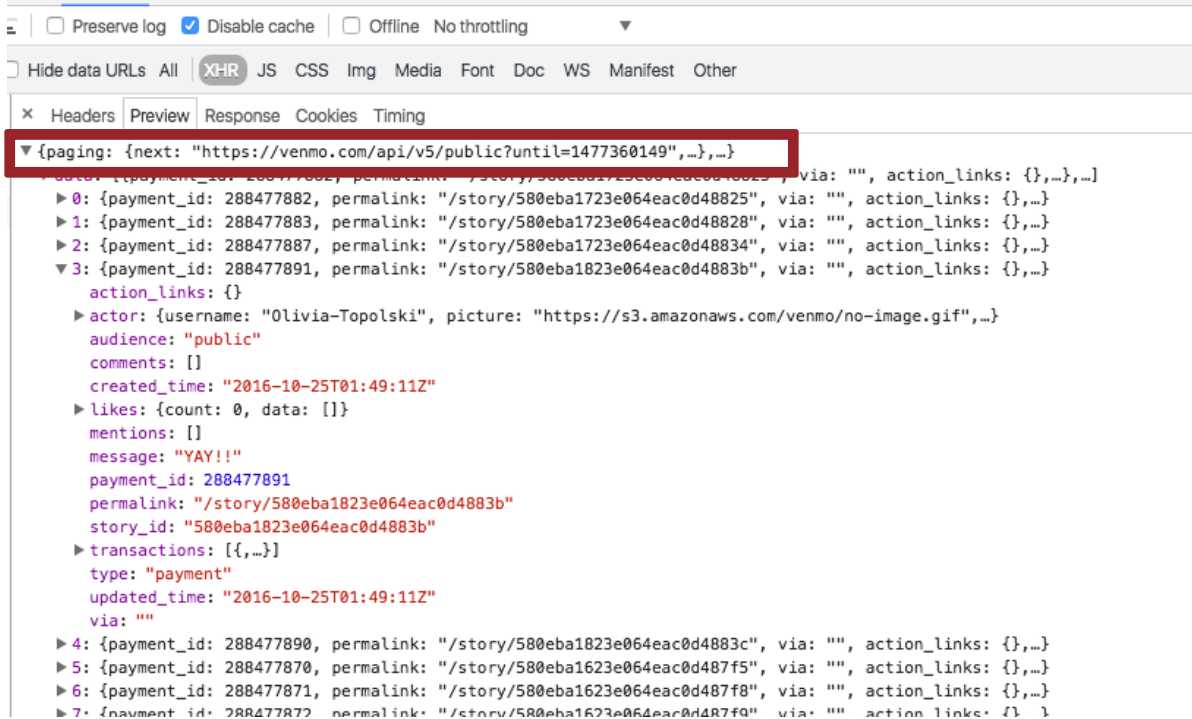
Root Cause

The underlying cause of the bug was a missing logic validation check in a Retail Brokerage API endpoint, which allowed a user to submit trades to a specific order book using a mismatched source account. This API is only utilized by our Retail Advanced Trading platform, which is currently in limited beta release.

```
{
  success: false,
  failure_reason: 'UNKNOWN_FAILURE_REASON',
  order_id: '',
  error_response: {
    error: 'UNSUPPORTED_ORDER_CONFIGURATION',
    message: 'validate order in post order failed',
    error_details: 'Source account does not match product id'
    new_order_failure_reason: 'UNSUPPORTED_ORDER_CONFIGURATION'
  }
}
```

Real world examples : Venmo





Real world examples : Venmo

https://venmo.com/api/v5/public?since=1476921600&until=1476921660&limit=1000000

Researches found there was 2 other undocumented query params since and limit that can be added to scrape much more data


```
{
    payment_id: 2038598177,
    permalink: "/story/5cf5379e7addfb4bc7a43016",
    via: "",
    action_links: { },
    transactions: [
        {
            target: {
                username: "Lindsay-Pelley",
                picture: "https://s3.amazonaws.com/venmo/no-image.gif",
                is_business: false,
                name: "Lindsay Pelley",
                firstname: "Lindsay",
                lastname: "Pelley",
                cancelled: false,
                date_created: "2016-10-05T15:29:07",
                external_id: "2054482061950976570",
                id: "14515489"
            }
        }
    ],
    story_id: "5cf5379e7addfb4bc7a43016",
    comments: [ ],
    updated_time: "2019-06-03T15:07:10Z",
    audience: "public",
    actor: {
        username: "r_pelley",
        picture: "https://venmopics.appspot.com/u/v1/m/82e7cc5a-fab2-4764-bd4f-f26e637da0bc",
        is_business: false,
        name: "robert pelley",
        firstname: "robert",
        lastname: "pelley",
        cancelled: false,
        date_created: "2017-01-18T14:16:36",
        external_id: "2130547014893568807",
        id: "17515985"
    },
    created_time: "2019-06-03T15:07:10Z",
    mentions: [ ],
    message: "🔑🚽",
    type: "payment",
    likes: {
        count: 0,
        data: [ ]
    }
```

API Security Problems

Steps to Maturing Your Security Posture

Shadow APIs

Discover your complete API footprint - including rogue, legacy, admin, zombie, etc.

Vulnerable APIs

Prevent OWASP Top 10 vulnerabilities and misconfigurations from hitting production.

API Abuse

Stop business logic abuse such as data scraping or data exfiltration using behavioral analytics.

Today's Focus

Tomorrow's Focus

Reinventing API Security

AI-Driven | 100% SaaS Platform | Data rich | API Detection and Response

Shadow APIs

Continuous API Discovery

Vulnerable APIs

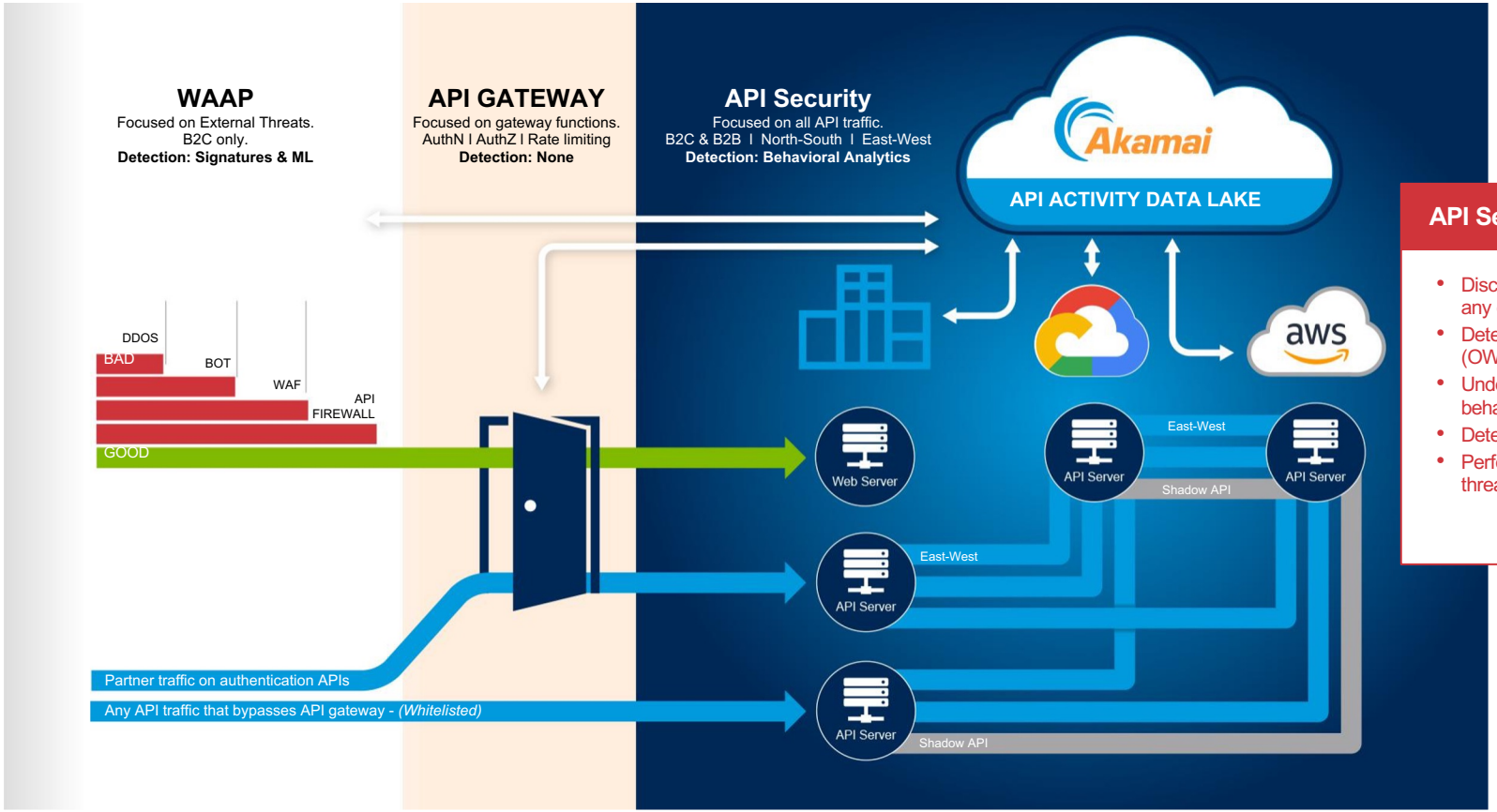
Risk Audit & Posture Alerts

API Abuse

Behavioral Alerts Detection & Response

Visibility & Investigations & Threat Hunting

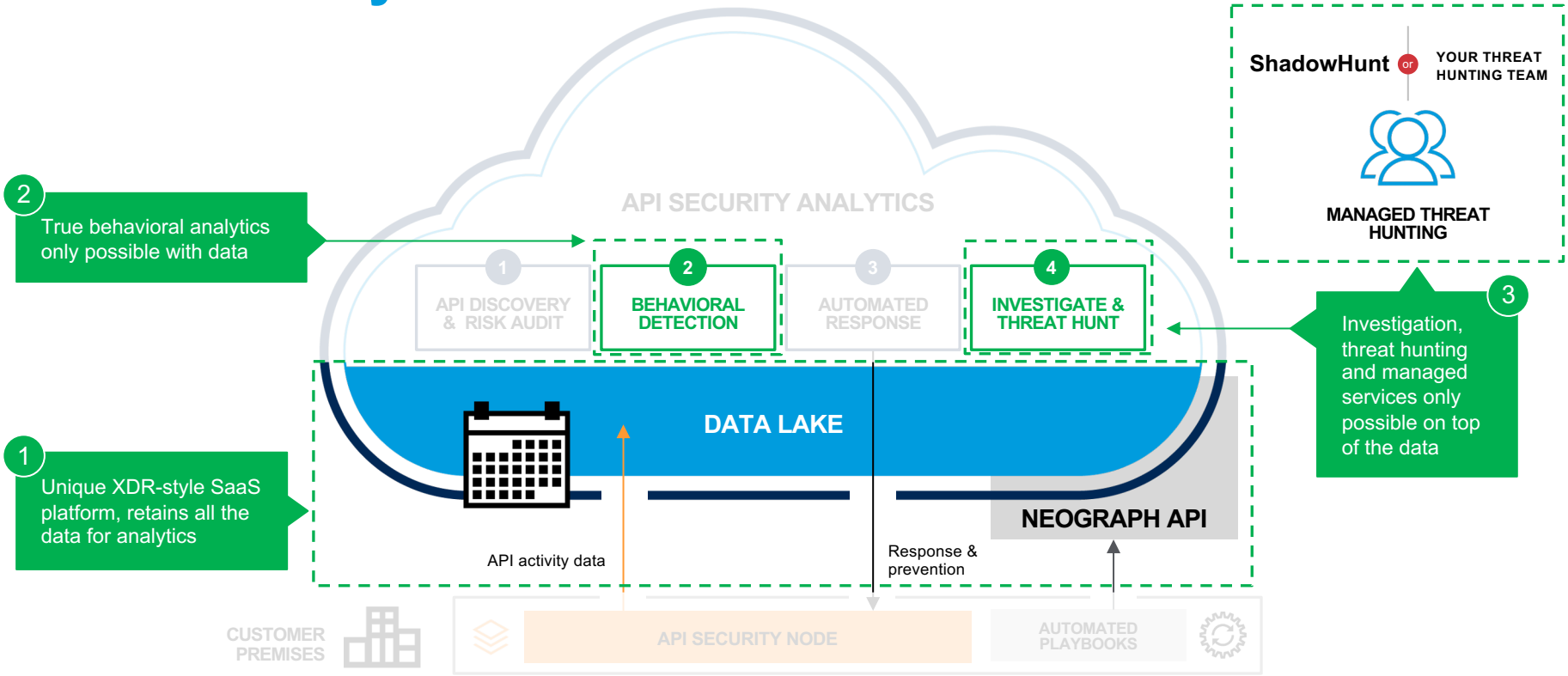
Why you need API Security?



API Security Problems

- Discovery of APIs in any environment
- Determine risk posture (OWASP API Top 10)
- Understanding API user behavior
- Detect API abuse
- Perform Investigations and threat hunting

API Security Differentiators




Akamai