CryptoPanel

edycja #30

Już za moment zaczynamy...

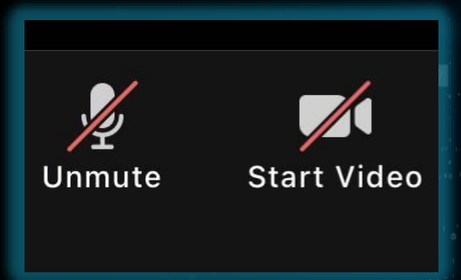
THALES
Building a future we can all trust

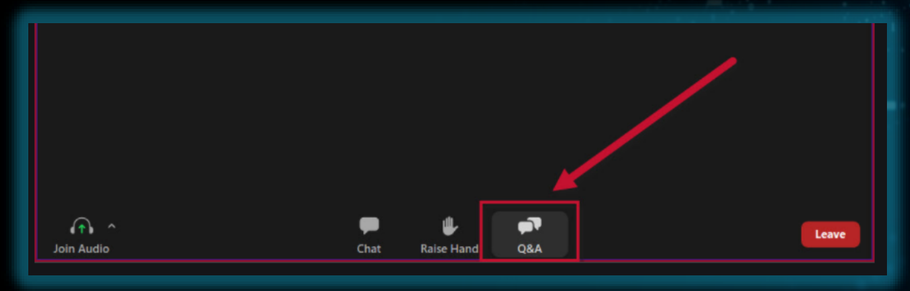
imperva
a Thales company

CLICO

CryptoPanel

edycja #30





CryptoPanel #30

24 Października 11:00

Bezpieczeństwo aplikacji w praktyce na przykładzie aplikacji e-commerce z Imperva Cloud WAF.

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel #30

Dyskusje poprowadzą: Mateusz Paściak i Wojciech Sawicki

Mateusz Paściak

Pre-sales Engineer
mateusz.pasciak@clico.pl
mob. +48 605 445 593

Wojciech Sawicki

Regional Sales Manager, Poland
wojciech.sawicki@thalesgroup.com
mob. +48 731 302 821

CryptoPanel

Le problème...

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Nasze wyzwanie (czyli czelendże *[pisownia challenge]*)

- HyperStep zmaga się z utrzymaniem responsywności sklepu internetowego i aplikacji mobilnej podczas okresów wzmożonego ruchu np. Sprzedaż limitowanych edycji butów premium
- Nieautoryzowani resellerzy wykorzystują automaty do wykupu ich produktów po czym odsprzedają je z większą marżą
- HyperStep korzysta z chmurowego rozwiązania WAF i CDN od innego dostawcy jednak obecny dostawca oferuje ograniczone możliwości ochrony przed botami
- Firma aktywnie wykorzystuje interfejsy API, co tworzy potrzebę skutecznej ochrony API
- Zauważane są okresowe, masowe ataki typu credential stuffing
- Firma odczuwa, że korzysta ze zbyt wielu różnych narzędzi security co spowalnia reakcje zespołu security
- **HyperStep jest sklepem internetowym, który nie może generować sprzedaży, jeśli strona działa wolno lub staje się niereagująca!**

Oczekiwania – czyli co byśmy chcieli po wdrożeniu **CWAF** ☺

- **Chcemy być nieustannie dostępni i wydajni bez względu na obciążenie**
- **Produkty premierowe trafiają do prawdziwych klientów a nie botów i następnie resellerów**
- **Mniej sytuacji awaryjnych w SOC wynikających z ataków na warstwę WEB (OWASP Top 10) i credential stuffing czyli np. poblokowanych kont użytkowników ze względu na liczne nieudane próby logowań czy nadużycia punktów lojalnościowych za historycznie robione zakupy**
- **Konsolidacja narzędzi, uproszczone środowisko zabezpieczeń, w dwóch słowach “lepszy soc”**
- **Pełna widoczność ruchu API**
- **Od strony biznesowej:**
  - Zadowolenie klientów
  - Przewidywalność przychodów
  - Lepsze wykorzystanie zasobów wewnętrznych
  - Brak skarg

CryptoPanel

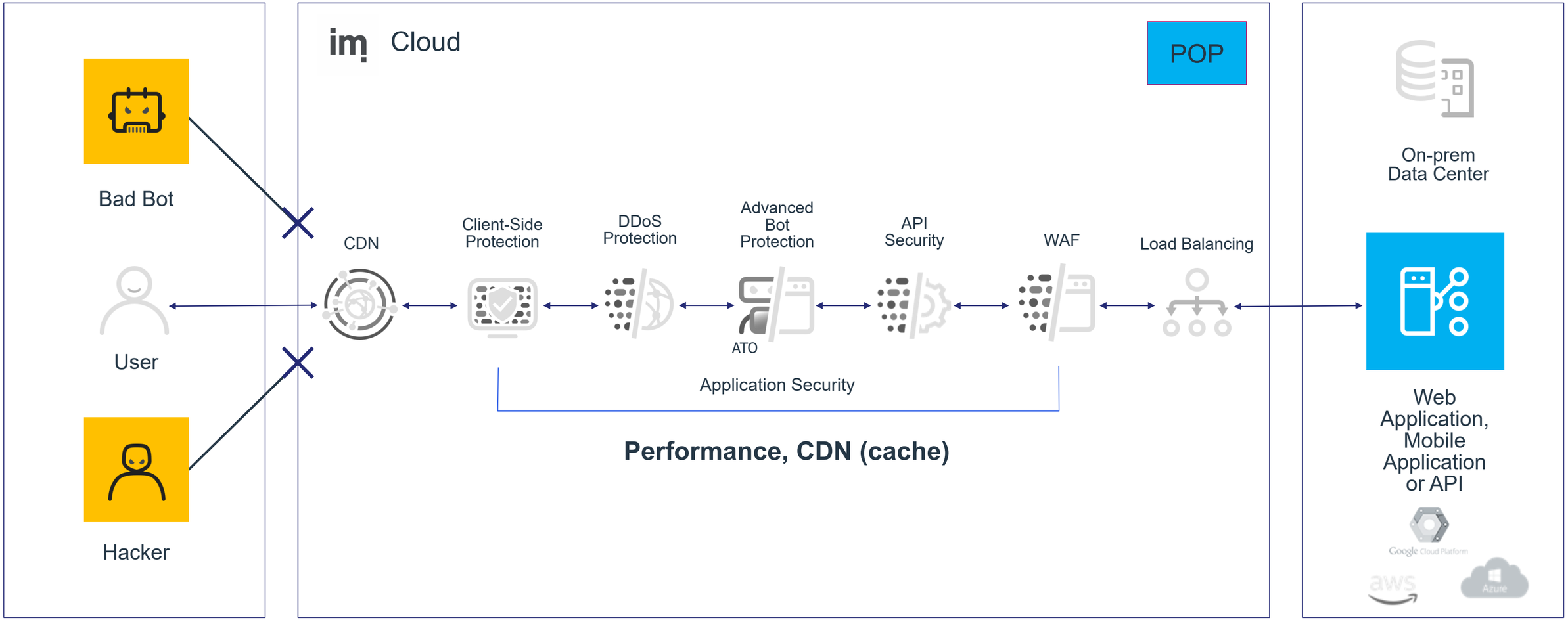
rozwiązanie

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CWAF architektura i podejście platformowe



Globalna sieć Imperva

- Global Mesh
- CDN
- Anycast Network
- Fully Automated Load Balancing and Policy Adjustment
- 63+ PoPs
- 13+ TBps capacity
- Tier 1 ISPs, IXs and T1 Data Centers
- Single Stack

Jedna platforma, wiele ataków, unifikacja bezpieczeństwa

DDoS Attacks

Layer 3/4

UDP floods
NTP amplification
DNS amplification
Tsunami
SYN flood
CharGEN amplification
Memcache amplification
SSDP amplification
SNMP amplification
GRE-IP UDP floods
CLDAP attacks
ARMS (ARD)
Jenkins
DNS Water Torture
SYN floods
TCP RST floods SSL
Negotiation floods
TCP connect floods
Fragmented attacks
TCP ACK floods
CoAP
WS-DD
NetBIOS

Layer 7

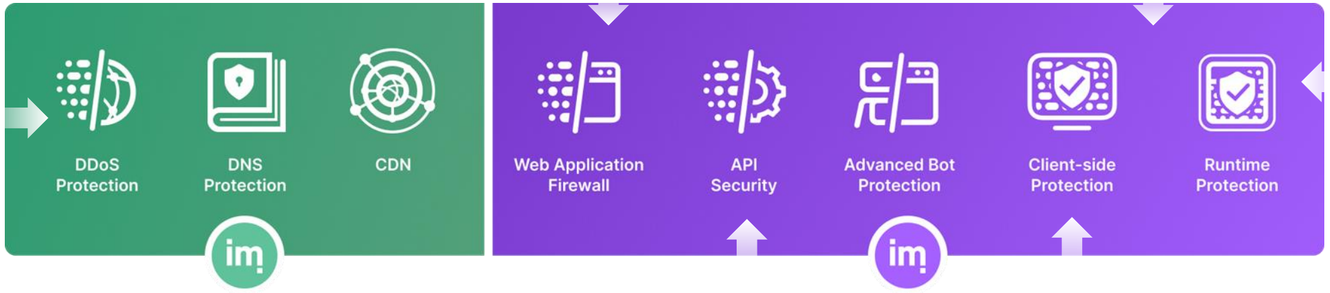
NS Query floods
SlowLoris attack
HTTP(S) GET request floods
HTTP(S) POST request floods
SMTP request flood

OWASP Top 10 Attacks

Injection
Broken authentication
Sensitive data exposure
XML external entities (XXE)
Broken access control
Security misconfiguration
Cross-site scripting (XSS)
Insecure deserialization
Using components with known vulnerabilities
Insufficient logging & monitoring

OWASP Automated Threats

Account Aggregation
Account Creation
Ad Fraud
CAPTCHA Defeat
Card Cracking
Carding
Cashing Out
Credential Cracking
Credential Stuffing
Denial of Inventory
Denial of Service
Expediting
Fingerprinting
Footprinting
Scalping
Scraping
Skewing
Sniping
Spamming
Token Cracking
Vulnerability Scanning



OWASP API Top 10 Attacks

Broken object level authorization
Broken user authentication
Excessive data exposure
Lack of resources & rate limiting
Broken function level authorization
Mass assignment

Client-Side Attacks

Formjacking
Credit card skimming
Card skimming
Digital Skimmers
Magecart
JavaScript supply chain attacks

Supply Chain & Zero-Day Attacks

Insider threats
Unknown new attacks
Internal facing app attacks

Techniques

Clickjacking
HTTP Response Splitting
HTTP Method Tampering
Large Requests
Malformed Content Types
Path Traversal
Unvalidated Redirects
Software Supply Chain Attacks

Injection Attacks

Command Injection
Cross-Site Scripting
Cross-Site Request Forgery
CSS & HTML Injection
Database Access Violation
JSON & XML Injection
OGNL Injection
SQL Injection

Weaknesses

Insecure Cookies & Transport
Logging Sensitive Information
Unauthorized Network Activity
Uncaught Exceptions
Vulnerable Dependencies
Weak Authentication
Weak Browser Caching
Weak Cryptography

CryptoPanel

Live Demo

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel

podsumowanie

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Coś na wynos…

https://www.imperva.com/products/imperva-plans/#application-products-table

CryptoPanel

pytania i odpowiedzi

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel

Dziękujemy za udział!!

Mateusz Paściak

Pre-sales Engineer
mateusz.pasciak@clico.pl
mob. +48 605 445 593

Wojciech Sawicki

Regional Sales Manager, Poland
wojciech.sawicki@thalesgroup.com
mob. +48 731 302 821

THALES
Building a future we can all trust

imperva
a Thales company

CLICO