CIKLUM | SPEAKER'S CORNER

SEPTEMBER, 27 | 17:00 (CET) | ZOOM

PROTECTING THE MODERN WEB APPLICATION:
NOT-SO-EASY DECISIONS

VLADYSLAV GRAM
LEAD DEVOPS STRATEGY ADVISOR AT CIKLUM

Meet Ciklum

CIKLUM

We empower companies to meet their digital initiatives by providing end-to-end software, integration and innovation services

Our services:

- Digital Commerce
- Intelligent Automation
- ITO & Managed Service
- Data & Analytics
- Cloud
- Engineering Services

2002 founded

4000+ professionals

20+ offices

300+ clients

Leading companies choose us:

JUST EAT Takeaway.com · METRO MARKETS · eToro · ZURICH · pay · Greensill · KANTAR RETAIL · dacadoo

Speaker:

Vladyslav Gram

Lead DevOps strategy advisor at Ciklum

- 7+ years in DevOps, 18 years in IT
- DevOps and DevSecOps lead, former Head of DevOps
- Cloud architecture and security specialty
- 5 Major projects, 10+ smaller ones, 40+ presales
- DevSecOps on the Ciklum’s biggest project

Web Application security

In this discussion we will talk about the issues and architectural decisions you will have to face when securing a modern modular web application.

The talk is a case study based on the Ciklum’s biggest project highly dependant on the internet purchases and partner integrations.

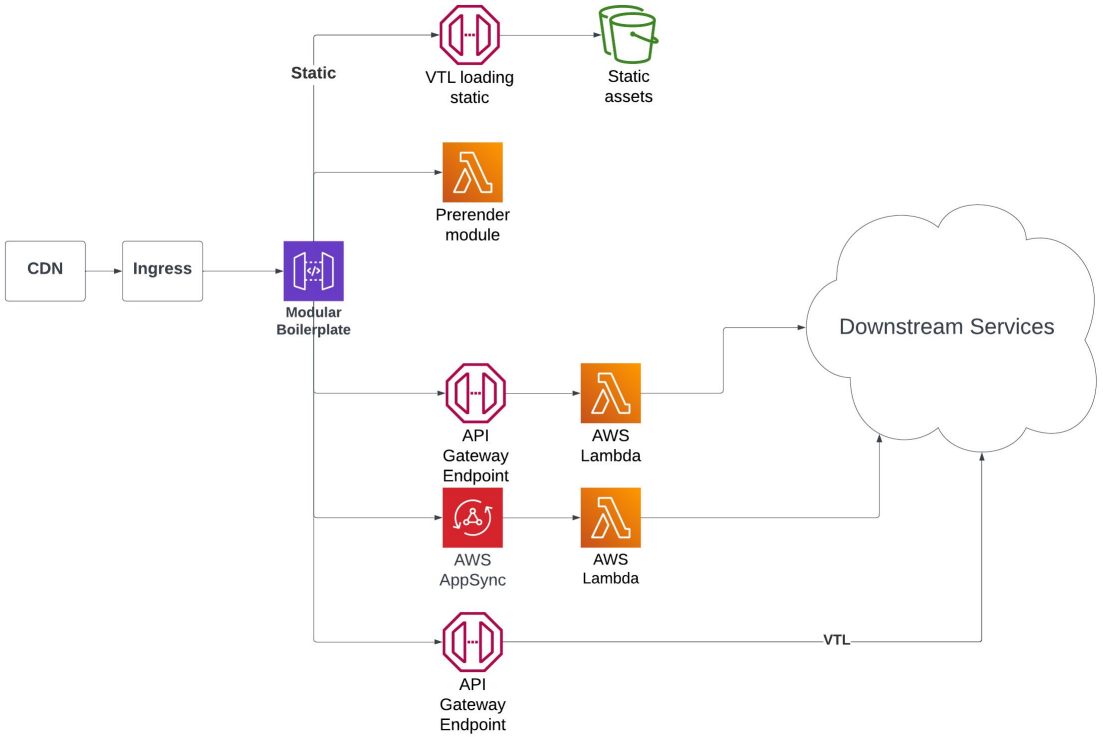
Agenda

- What is the problem
  - Web app components
  - Levels of defence
  - Solutions
- MWA Security
  - Akamai
  - Ingress
  - API-level
- Other considerations
- Conclusions

CIKLUM

Web application components

CIKLUM



Layered defence

Process and people

- Lack of security competency in every team
- Focus on delivery and features

Code and deployment

- Supply chain attacks
- Code and CI/CD vulnerabilities

Network and Web

- Bots: malicious and legitimate
- Manual whitelisting
- Regex and dynamic path

CIKLUM

Solution - Security Champions

- Every team has a designated **Security Champion**
- It’s not a profession, it’s a team role
- Responsibility - to make sure the team considers security, compliance and best practices during the delivery
- Security champions have a community
- Common toolset, common baselines, common practices
- Team usage of common tools is audited.

CIKLUM

Solution - AppSec Pipeline

To deal with supply chain attacks and common code vulnerabilities we use a centralized quality gate pipeline witch can be included to the CI/CD pipeline of the team as a module.

Quality gates:

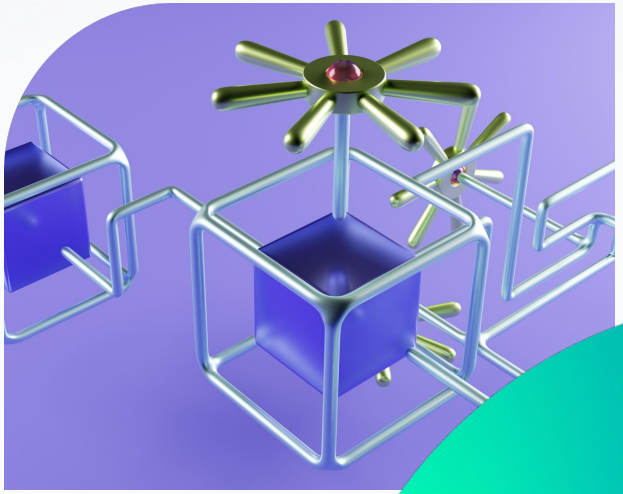
- OWASP-Zap
- Checkov for IaaC
- SonarQube quality gate
- Dockle
- Trivy

CIKLUM

Solution - MWA security

The Modular Web Architecture is protected with defence-in depth approach:

- WAF+CDN endpoint - Akamai
- Ingress solution to hide the internal naming and services
- Private Route53 DNS zone for internal name resolution
- Regex-based solution for internal routing
- REST and GraphQL API endpoints for backend communication.



MWA security - Akamai

CIKLUM

Akamai provides a comprehensive WAF + CDN solution with many interesting features:

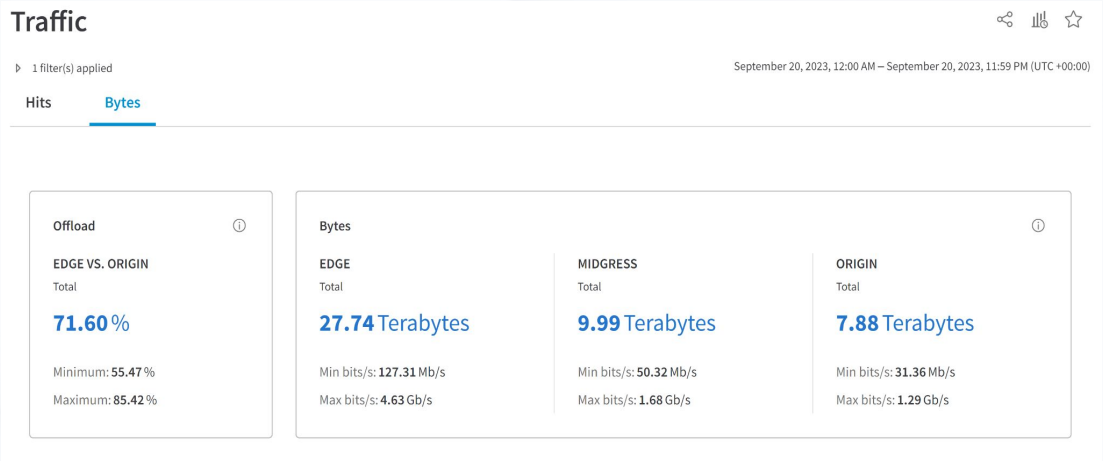
- Bot detection and control
- Error rewrite
- Dynamic traffic control
- Captcha and Crypto Challenge
- IaaC with Terraform and Akamai API

Modules

Access Control
Adaptive Acceleration
Adaptive Image Compression (expired)
Advanced Offload
Akamai API Gateway
Brotli Compression
Brotli Support
Cloud Access Manager (expired)
Content Targeting / EdgeScape
Custom Behaviors
DataStream Logs
Device Characterization
Edge Redirector Cloudlet
Enhanced Akamai Protocol
Enhanced Secure Delivery - Customer Cert
Forward Rewrite Cloudlet
Front End Optimization (expired)
GraphQL Caching
HTTP/2
HTTP/3 (expired)
Image and Video Manager
Image and Video Manager (Videos)
Mobile Detection & Redirect
mPulse
Origin Services (Beta)
Phased Release Cloudlet
Preconnect (Beta) (expired)
Real User Monitoring (expired)
Request Debugging
Resource Optimizer (expired)
Resource Optimizer Extended Compatibility
Script Management
Server Push (Beta) (expired)
Site Failover
SiteShield
Standard Secure Delivery - Customer Cert
Variable Support
Visitor Prioritization Cloudlet
Web Application Firewall

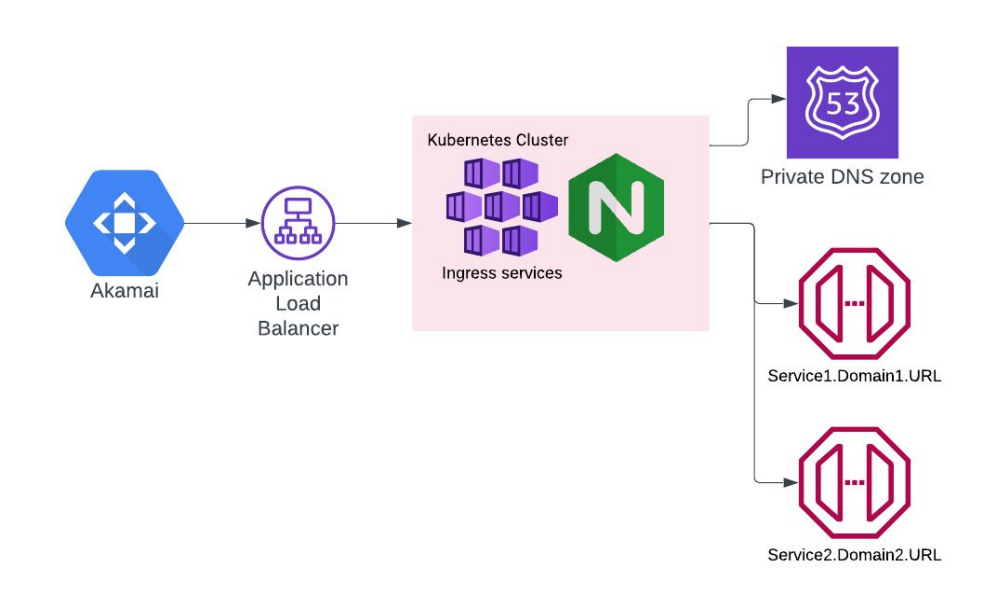
Akamai issues

- Legitimate bots
- End-to-end monitoring
- Property management
  - Permissions
  - PM-Includes
  - IaaC consistency
- Caching headers
- Cache invalidation
- Manual tasks
- Tweaks



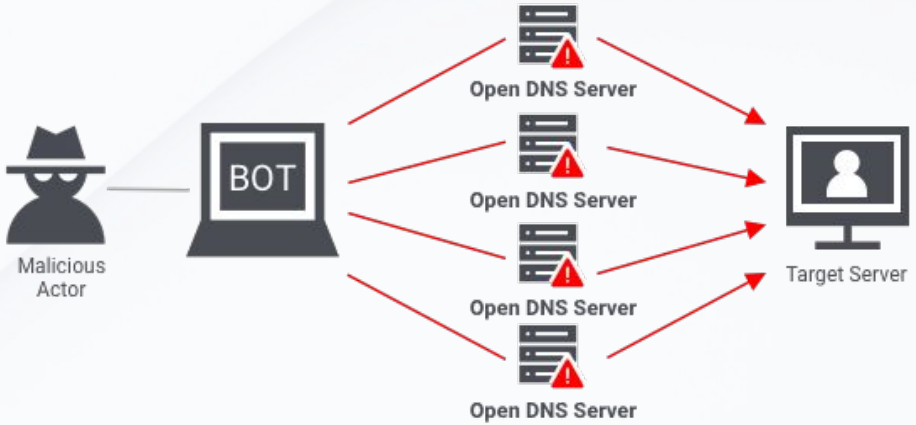
MWA Security: Ingress

- Reverse-proxy solution
- Private domain
- Regex-based name resolution



Ingress issues

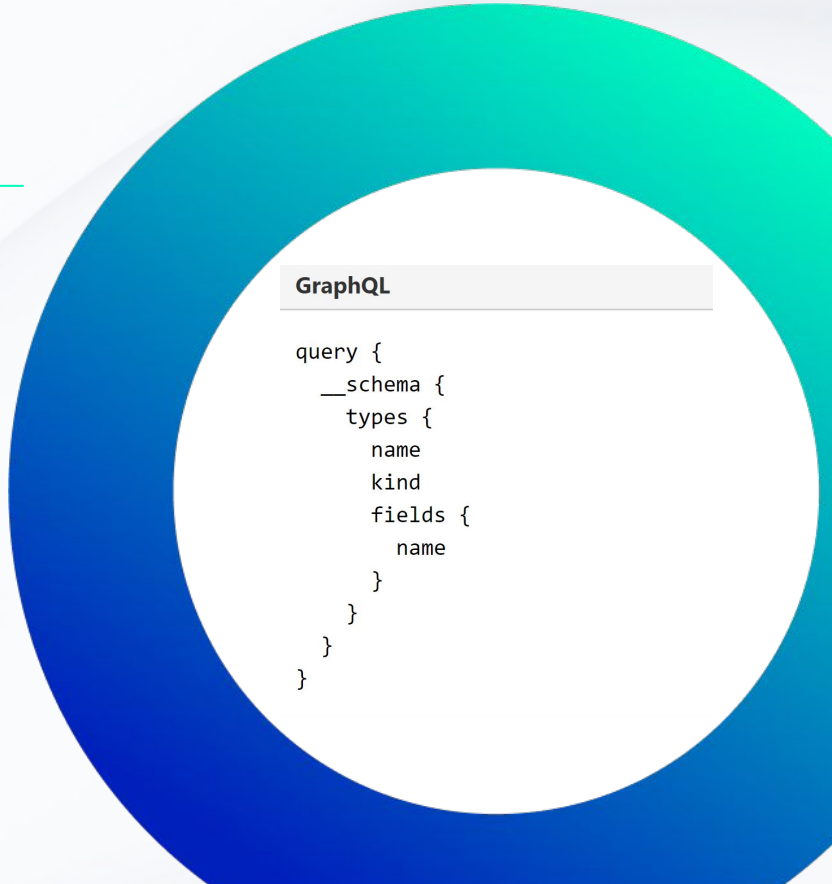
- DNS Flood attack using REGEX
  - Whitelist
  - Alerts
- Performance
  - End-to-end test
  - Scaling and caching
- New service deployment
  - Additional dependency



CIKLUM

MWA Security - API level

- GraphQL still can be queried directly
- Should we publish the schema?
- Should we allow bulk operations?
- What is the throttling level?



Other considerations

Conclusions

CIKLUM

Complex tasks require complex solutions

In our solution we used the following principles:

- Team independence with centralized toolset
- GitOps approach for all services
- Layered security

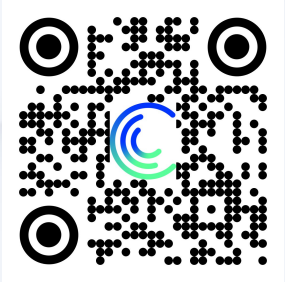
CIKLUM

Any questions?

Share your feedback!

CIKLUM

Thank you!



www.ciklum.com