Le soluzioni di Cybersecurity e i requisiti per la Direttiva NIS 2

MARCO ZAMBONI

System Engineer Radware

VEM LIVE 2024

Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

Shifting Threat Landscape

Leveraging new tools & GenAI to attack applications

2

New Regulatory Requirements

New, stricter regulations on cyber-security incidents

3

Hybrid Cloud Deployments Expand

Hybrid-cloud reality creates many entry points

4

Cybersecurity Staff & Skills Shortages

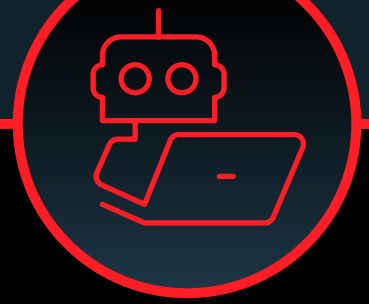
Organizations cannot rely on their internal resources only

Shifting Threat Landscape

1

+94%

Increase in number of DDoS attacks, 2023 vs. 2022



82%

Experience a bot attack on a daily, weekly or monthly basis

+171%

Increase in malicious web and API traffic, 2023 vs. 2022

Attacks increase in frequency, size & complexity across all attack vectors

***Source**: Radware Threat Landscape Report 2024*

Application Security Threats Go Beyond OWASP Top 10

Sharp Rise in API attacks

OWASP TOP 10 **API** SECURITY RISK

Bot Attacks Most Frequent

OWASP TOP 21 **AUTOMATED THREATS**

Supply Chain Raises Concerns

OWASP TOP 10 **CLIENT-SIDE** SECURITY RISKS

All-in-One Modern Attack Tools on Github

- Attackers don't distinguish between WAF, DDoS, Bot attack vectors
- Need an **integrated platform** to **overcome all-in-one attack tools**

Features And Methods

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk_captcha
  - STRESS | Send HTTP Packet With High Byte
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP 'if (isset($_COOKIE))'
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Expliot
  - XMLRPC | WP XMLRPC expliot (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BYPASS | Bypass Normal AntiDDoS
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website

DDoS attack vectors

Bot attack vectors

Web application exploits

Built-in bypass again common defenses

Hybrid Cloud Deployments Expand

3

Most Organizations Today Run **Hybrid Multi Cloud** Environments

55%

Of organizations run three or more environments

73%

Still maintain their on-prem hardware data centers

46%

Use on-prem, private cloud **and** public cloud all at once

Need **consistent protections** across diverse environments

***Source**: Radware Application Security in a Multi-Cloud World 2023*

Organizations Face Cybersecurity Staff, Skill Shortages

4

67%

Face shortages in security staff or skills

3.99M

Estimated open global cybersecurity roles

41%

Can’t find enough qualified talent

Need for **automated protections** and expert **managed services**

***Source**: ISC2 Cybersecurity Workforce Study, 2023*

Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

Shifting Threat Landscape

Leveraging new tools & GenAI to attack applications

2

New Regulatory Requirements

New, stricter regulations on cyber-security incidents

3

Hybrid Cloud Deployments Expand

Hybrid-cloud reality creates many entry points

4

Cybersecurity Staff & Skills Shortages

Organizations cannot rely on their internal resources only

New Regulatory Requirements

2

"Registrants must disclose any cybersecurity incident they experience that is determined to be material [...] within 4 business days"

New & updated requirements:

- *WAF requirements*
- *Positive security*
- *API protection*
- *Client-side security*

EU-wide legal framework for mandating cybersecurity protection measures

Need an **integrated platform** to ensure full compliance

NIS2 – New EU Compliance Requirements

WHEN TO IMPLEMENT

By **October 17, 2024**

WHO IS IT FOR

- Healthcare
- Financial Services
- Digital Infrastructure
- Digital Service Providers
- Transportation
- Digital services
- Communication networks
- Data management services
- Water Supply
- Wastewater and Waste Management
- Food
- Postal and Courier services
- Energy
- Public administration
- Space technology and operations
- manufacturing of critical products (food, pharma, medical devices, vehicles, chemicals, etc.)

NIS2 – New EU Compliance Requirements

PENALTIES FOR NON-COMPLIANCE

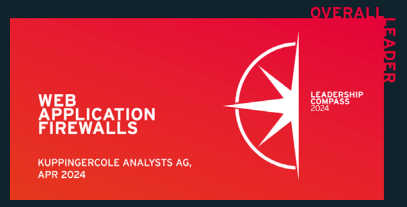
- For Essential entities – Up to **€10,000,000** or **2% of the global annual revenue**, whichever is higher
- For Important entities – Up to **€7,000,000** or **1,4% of the global annual revenue**, whichever is higher

WHAT IS REQUIRED

- Incident handling and crisis management
- Vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- Cyber hygiene practices
- Supply-chain security
- Business Continuity

What is Needed to Stay Ahead?

Radware.



Intelligent Security
powered by AI-based algorithms

Integrated Platform
correlating across wide array of threats

Consistent Protections
across all environments and entry points

Expert Defense
with 24/7 security experts by your side

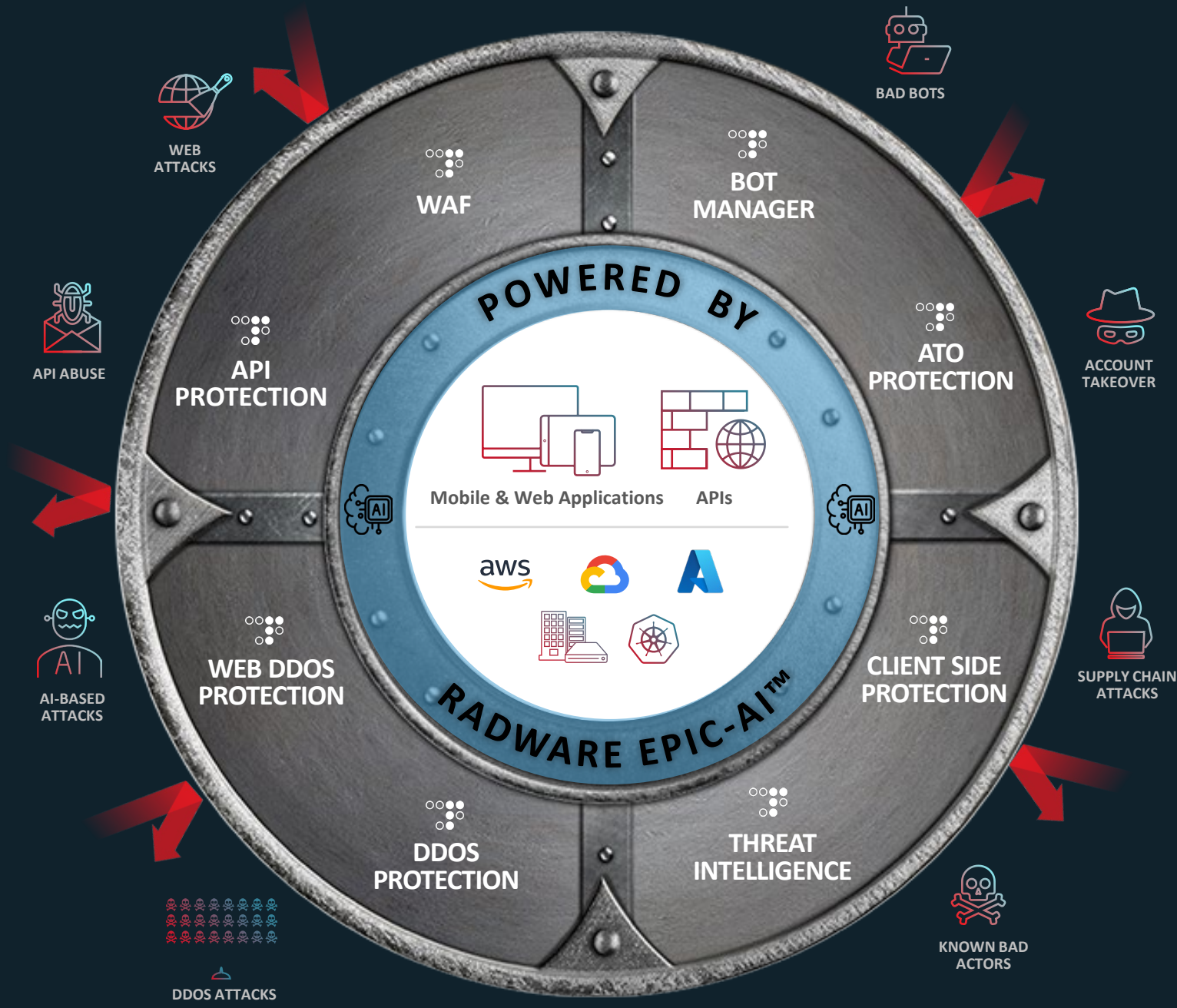
Only way to drive lower MTTR, save costs & protect your brand

360º Application Protection by Radware's Cloud Security Platform

Gartner Peer Insights

*Truly **exceptional protection** for web apps & APIs*

Radware Customer, Telecommunications



Cloud Security Platform Powered by Radware **EPIC-AI™**

LOWER MTTR

AI-Driven SOC

- AI-empowered managed services
- SecOps enablement
- Compliance, analytics & integrations

Cross-Platform AI Reasoning

- Threat intelligence insights & preemptive protection feeds
- Cross-module AI-based correlation
- Continuous AI-powered policy tuning & recommendations

RT Cloud Protection Engines

DDOS PROTECTION | WEB DDOS PROTECTION | WAF | API PROTECTION | BOT MANAGER | ATO PROTECTION | CLIENT SIDE PROTECTION

Enforcement Points

ALTEON | DEFENSEPRO X | CLOUD SERVICES | f5 | NGINX | envoy | HAPROXY | aws

Radware Protects EMEA Bank from Web DDoS Tsunami Attacks

Attack Peaks

Up to

14.6M

RPS

Attack Length

Several days w/ multiple waves lasting

10-20

HOURS

Attack Signature

Signature created in real-time includes

27

PARAMETERS

> *Layer 7 application DDoS protection is **where it shines**. Mean time to **remediation** is within **seconds**.*

Radware Customer, Tech Services

PeerSpot

Fight AI with AI: AI-based algorithms create signatures in real-time

ACHIEVING **NIS2** COMPLIANCE WITH **RADWARE**

Application Protection

- WAF
- Bot Manager
- API Protection
- Web DDoS Protection
- Client-side Protection

DDoS Protection

- On-prem
- Cloud
- Hybrid

Load Balancing

- Alteon ADC

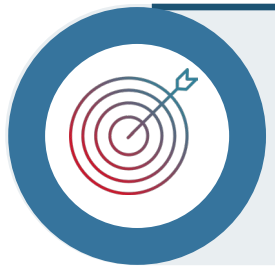
Managed Services

- 24/7 ERT Services
- ERT Active Attackers Feed

New Compliance Requirements

PCI DSS COMPLIANT 4.0

Just a WAF is not enough!



WHO IS IT FOR

All orgs that process online credit card payments (e-commerce, travel, entertainment, FSI, etc.)

WHEN TO IMPLEMENT

Best Effort started March 31, 2024; Mandatory by March 31, 2025

WHAT IS NEEDED

- **WAF** with a comprehensive security approach (WAAP)
- Protection against **Business Logic Attacks on APIs**
- **Client-side Protection** – Monitor payment pages headers & content, and third-party scripts running on the end-user browser-side

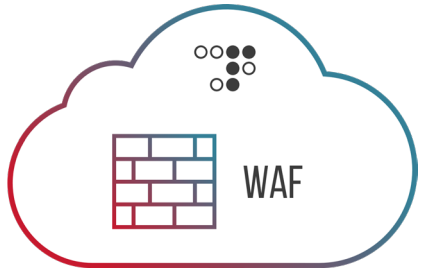
New Compliance Requirements

PCI DSS COMPLIANT 4.0

Just a WAF is not enough!

THE SOLUTION

Radware Application Protection for PCI DSS 4.0 Compliance

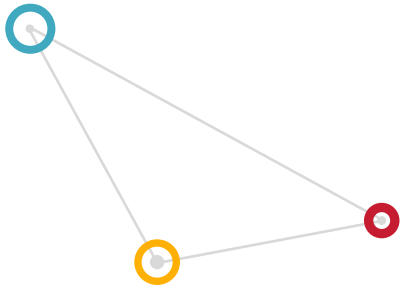


PCI DSS 4.0 Compliance Add-on

Client-side Protection Solution Enhancements

Integrity of Payment Page Scripts: Section 6.4.3 necessitates that organizations uphold the integrity of all payment page scripts executed in the consumer's browser. This requirement extends to scripts sourced from third-party sites, emphasizing the need for robust controls that ensure the security of all elements interacting with the consumer's browser, especially within payment transactions.

Tamper-Detection Mechanism: Section 11.6.1 seeks to counter the potential impact of Magecart attacks by mandating a tamper-detection mechanism. This mechanism would promptly alert organizations about unauthorized alterations to HTTP headers and payment page content as perceived by the consumer's browser.

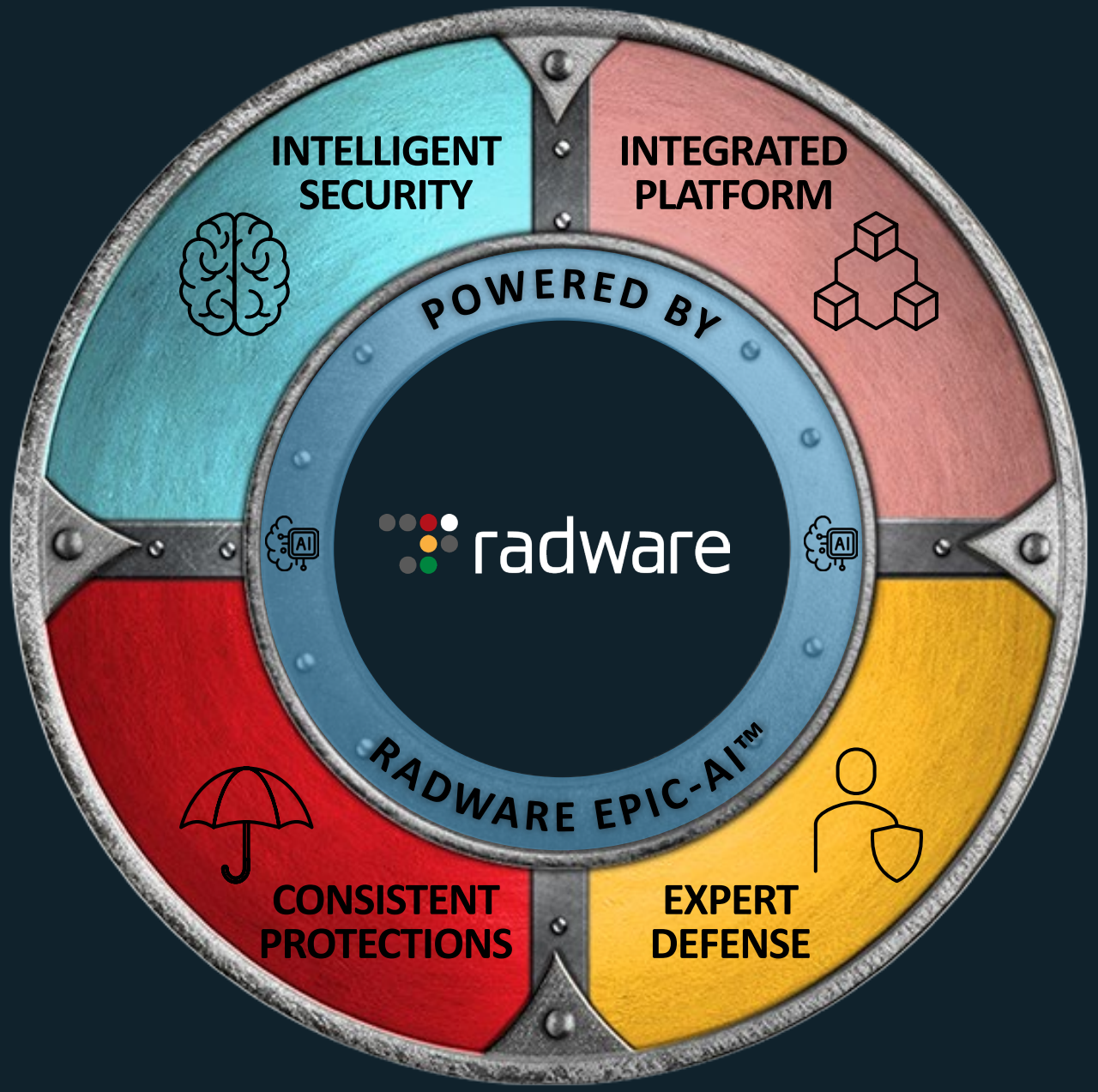


COMING SOON – DORA

Digital Operational Resilience Act

Where?	EU
For Whom?	Financial Services
When?	**January 17, 2025**

Give Your Apps the Most **Precise**, **Hands-Free**, **Real-Time** Protection



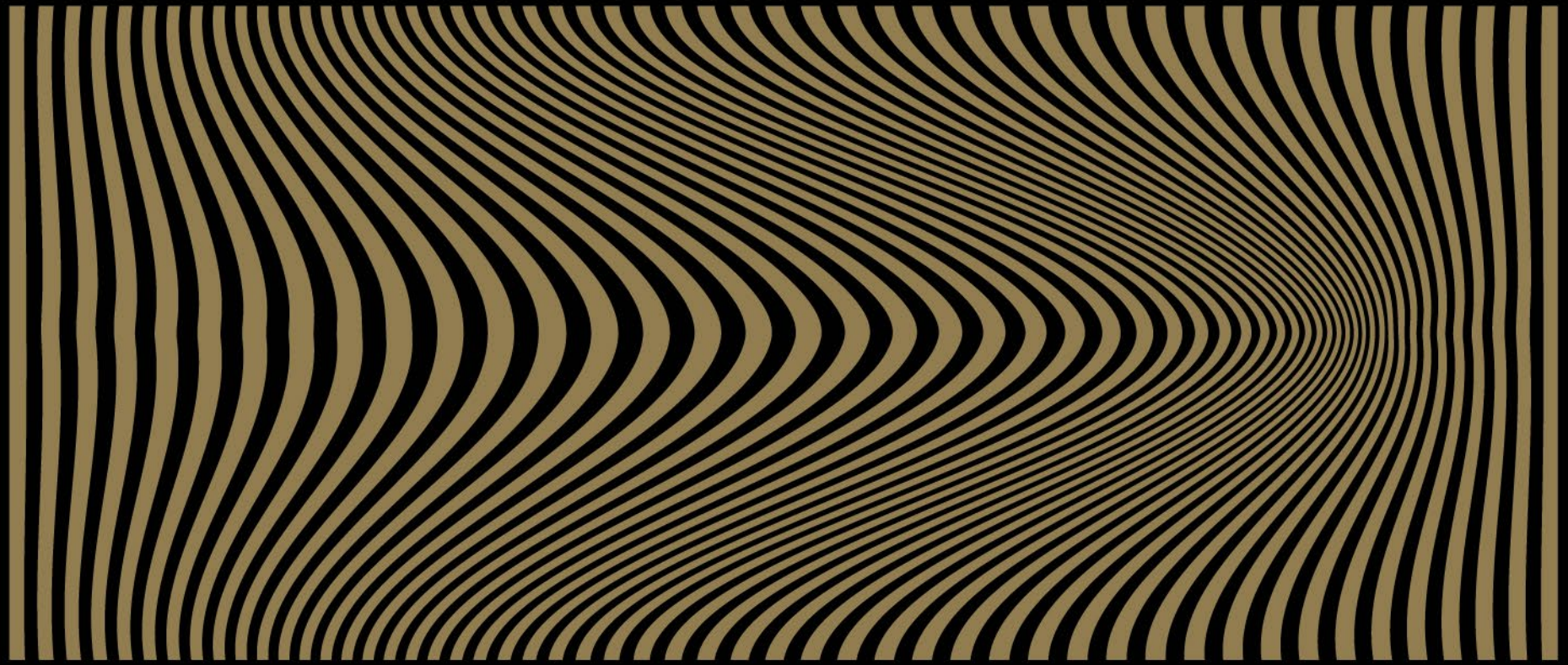
Thank you!

VEM LIVE 2024

gruppo VEM

Passione, Tecnologie, Competenze Metronomiche

nello sviluppo di Intelligenze Digitali.



PULSE

RUOTE DA SOGNO // RE 11/10/24