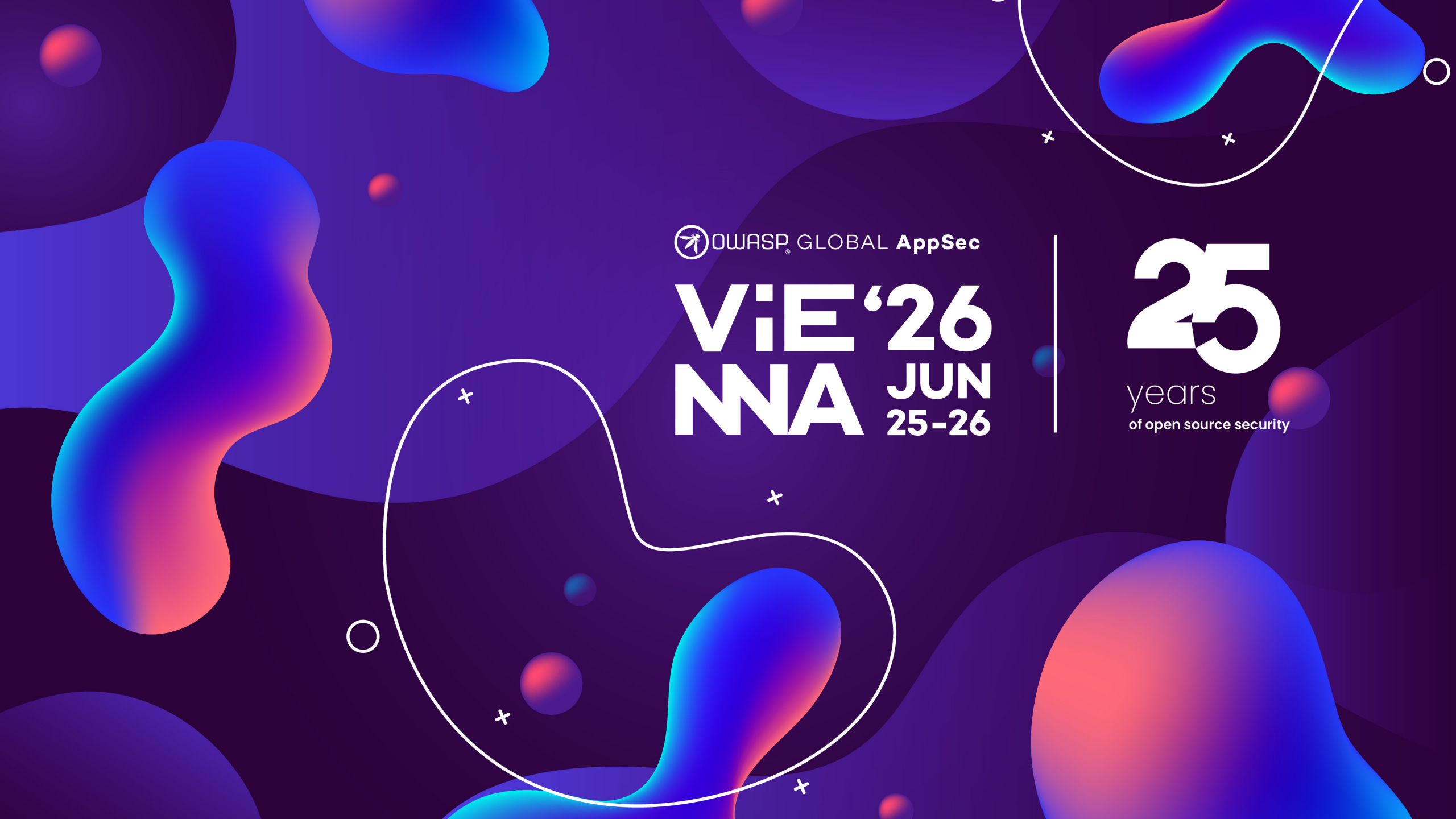

OWASP GLOBAL AppSec
VIE'26
VIENNA
JUN
25-26
25
years
of open source security

OWASP GLOBAL AppSec

VIENNA '26 JUN 25-26

25 years of open source security

Authorization is Where Your App Goes to Lie

Eden Yardeni

BACKGROUND

Quick recap of the OWASP Top 10

2021		2025		
A01	**Broken Access Control**	A01	**Broken Access Control**	=
A02	Cryptographic Failures	A02	Security Misconfiguration	▲3
A03	Injection	A03	Software Supply Chain Failures	▲3
A04	Insecure Design	A04	Cryptographic Failures	▼2
A05	Security Misconfiguration	A05	Injection	▼2
A06	Vulnerable & Outdated Components	A06	Insecure Design	▼2
A07	Identification & Auth Failures	A07	Authentication Failures	=
A08	Software & Data Integrity	A08	Software or Data Integrity	=
A09	Logging & Monitoring Failures	A09	Logging & Alerting Failures	=
A10	SSRF	A10	Mishandling of Exceptions	NEW

BACKGROUND

We've had ways to formalize AuthZ for decades

access matrix	→	RBAC	→	XACML	→	ABAC	→	ReBAC	→	policy engines
1971		1992		2003		2014		2019		today

+ ALFA · 2014

BACKGROUND

This check would pass a code review

```
public async Task<TransactionReceipt> ExecuteTransactionAsync(
...
        bool allowed =
            source.OwnerId == caller.Id
            || source.JointHolders.Contains(caller.Id)
            || caller.HasPowerOfAttorneyFor(source.OwnerId)
            || caller.Role == Role.BankManager;
```

BACKGROUND

Reviewers and triagers have nothing to check against

Review

correct against what?

(going in)

Triage

allowed by what?

(coming out)

BACKGROUND

We solve harder problems than this

memory safety

crypto discipline

post-quantum

RESOLUTION

Specified where?

V4 Access Control

Control Objective

Authorization is the concept of allowing access to resources only to those permitted to use them. Ensure that a verified application satisfies the following high level requirements:

- Persons accessing resources hold valid credentials to do so.
- Users are associated with a well-defined set of roles and privileges.
- Role and permission metadata is protected from replay or tampering.

RESOLUTION

ASVS 5.0 added Documented Security Decisions

ASVS 5.0 · Documented Security Decisions

Documentation requirements were included which mandate that the application developer's approach and configuration to these sorts of controls must be documented.

ASVS 5.0 · V8.1

Document authorization rules, including decision-making factors and environmental contexts. Consumers should have access only to resources permitted by their defined entitlements.

RESOLUTION

Leading engines all using more or less the same vocab

who acts

XACML / ALFA · Subject
Cedar · principal
OPA / Rego · *your keys*

doing what

XACML / ALFA · Action
Cedar · action
OPA / Rego · *your keys*

to what

XACML / ALFA · Resource
Cedar · resource
OPA / Rego · *your keys*

under what conditions

XACML / ALFA · Environment
Cedar · context
OPA / Rego · *your keys*

METHOD

Your product owner's answer compiles into policy

a product owner answers

"A bank manager acts only within their own branch."

compiles to

```
base_grant if {
  input.subject.role == "BankManager"
  input.subject.branch ==
      input.resource.branch

}
```

THREAT MODEL

Risk register for transaction.execute

		STRIDE / LINDDUN	
T01	Caller acts on an account they don't own	*EoP*	→ **policy**
T01a	Branch manager acts outside their own branch	*EoP*	→ **policy**
T02	Teller sets a branch outside their own	*EoP*	→ **policy**
T03	Caller redirects the confirmation email	*Tampering*	→ **policy**
T04	Auditor holds execute from a stale grant	*EoP*	→ **policy**
T05	Execute against a transaction in review	*Tampering*	→ **policy**
T06	High-value transfer at base assurance	*Spoofing/EoP*	→ partial
T07	Stolen or fixated session reused	*Spoofing*	
T08	Principal denies having executed	*Repudiation*	
T09	Error reveals an account exists	*Info Disc.*	
T10	Transaction flooding degrades service	*DoS*	
T11	Requests tampered in transit	*Tampering*	
P01	Email routes financial data to an attacker	*Disclosure*	→ **policy**
P02	Patterns link a customer across branches	*Linkability*	
P03	Execution breaches residency / sanctions	*Non-compliance*	→ **policy**

RESOLUTION

GlobalShop adopts ASVSv5's AuthZ Requirements!

8.1.1	function & data-level rules	→	**Owner, joint holders, POA delegate, branch manager** *T01*
8.1.2	field-level read/write, object state	→	**No execute while the transaction is in review** *T05*
8.1.3	contextual attributes	→	**Manager's branch must match the account's branch** *T01a · T02*
8.1.4	thresholds, actions	→	**High-value transfers step up; auditor is deny-always** *T06 · T04*

ASVSv5.0.0 · V8.1.1–8.1.4

Demo

How GlobalShop does it

TAKEAWAYS

Open-source engines that run your AuthZ policy as code

OPA

Rego

```
allow if {
  input.subject.role
      == "BankManager"
  input.subject.branch
      == input.resource.branch
}
```

Cedar

Cedar policy

```
permit(
  principal, action, resource
)
when {
  principal.role
      == "BankManager"
  && principal.branch
      == resource.branch
};
```

OpenFGA

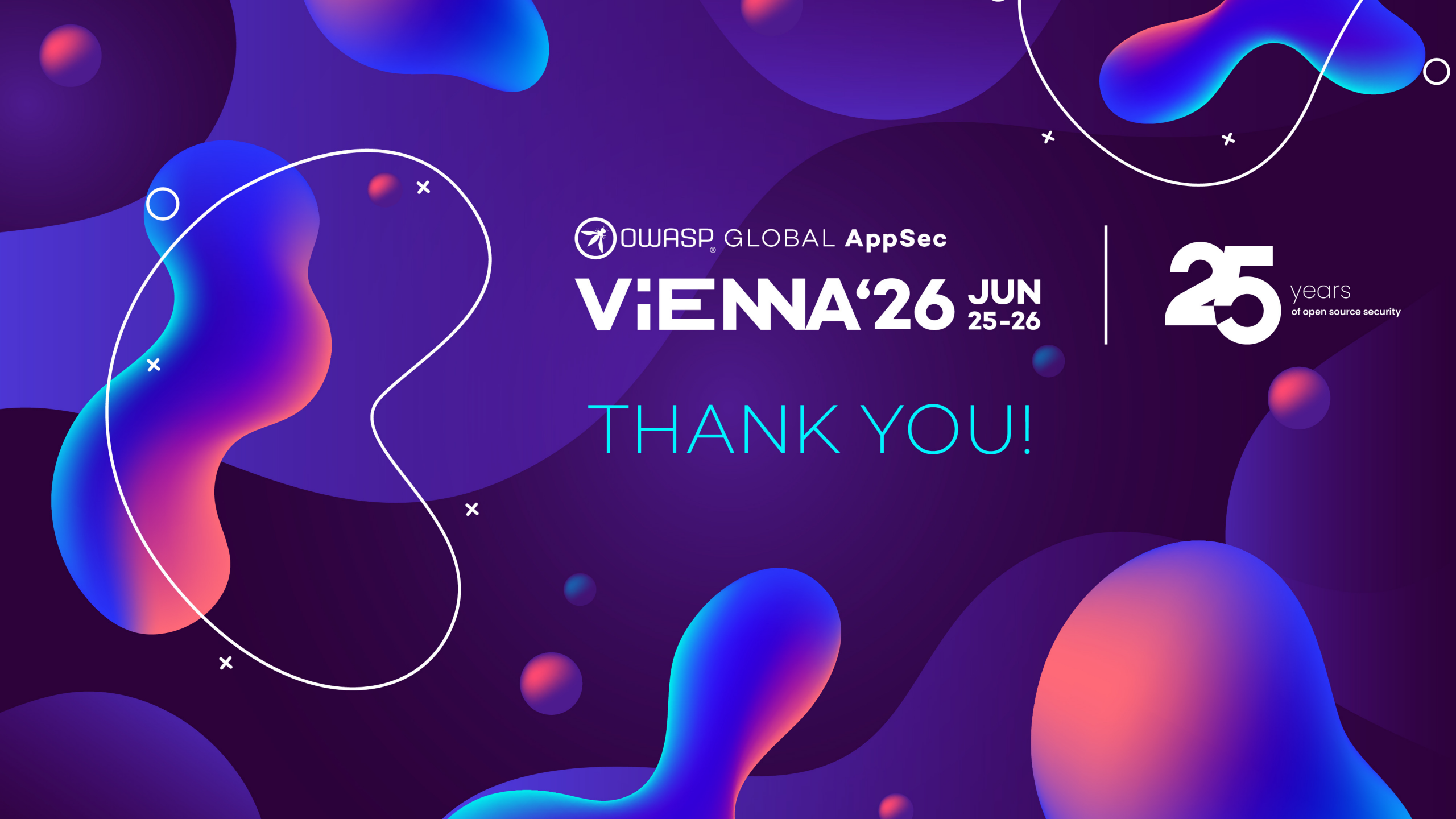
model + tuples

```
type branch
  relations
    define manager: [user]
type account
  relations
    define branch: [branch]
    define can_act:
      manager from branch
```

TAKEAWAYS

"A network hop per request?!"

embedded	sidecar	centralized service
≈ µs	≈ sub-ms	≈ ms


OWASP GLOBAL AppSec
VIENNA'26 JUN 25-26
25 years
of open source security
THANK YOU!