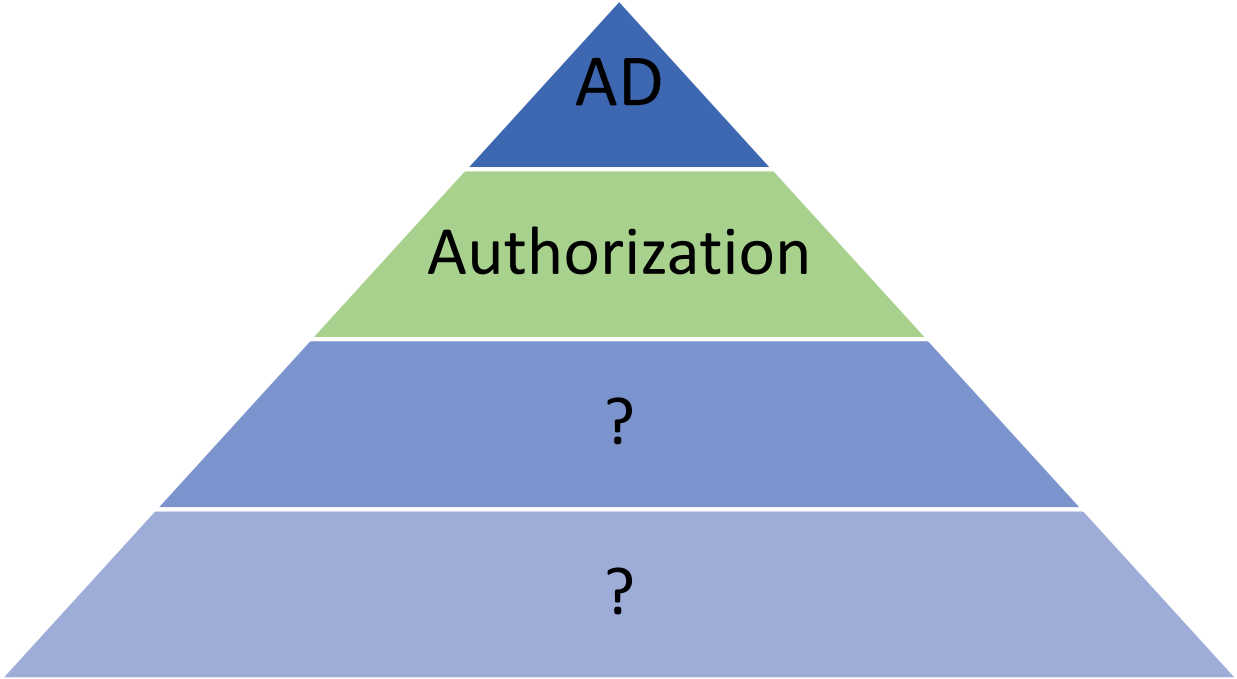
Secure authorization mechanisms

Mikołaj Dobski, Paweł Węgrzak
WP9T2 / PSNC

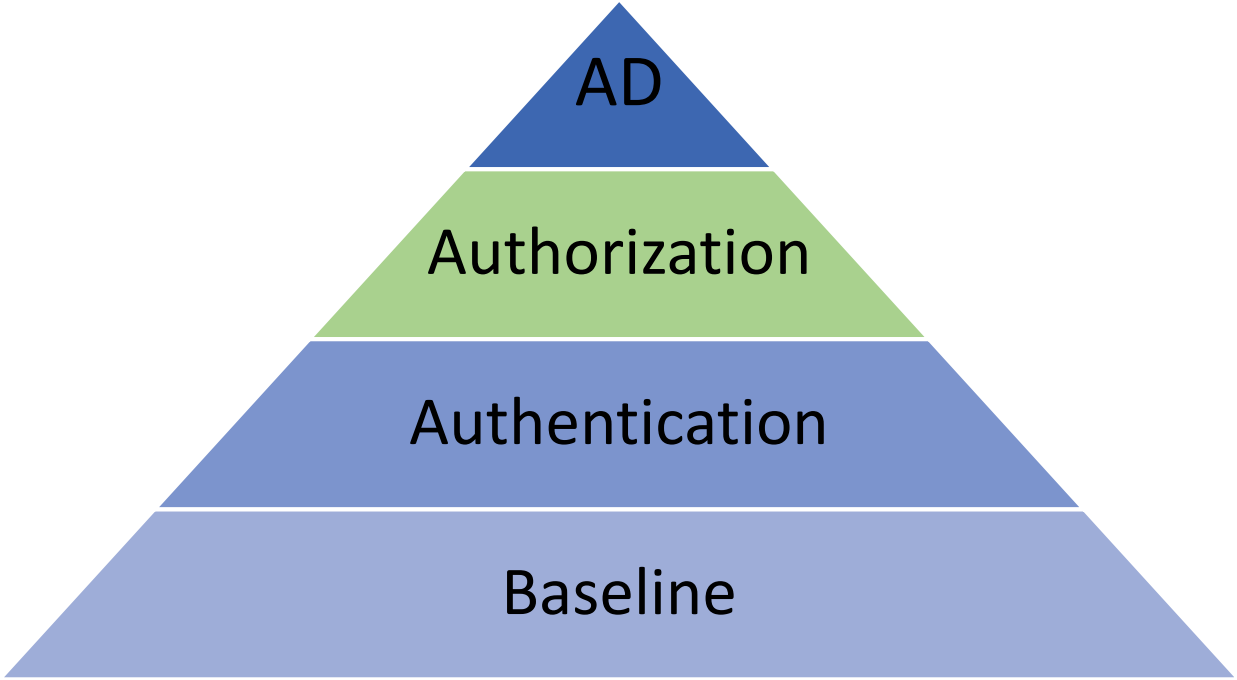
PRACE Days 2019, Poznań, 2019-05-15

www.geant.org

Security solution layers (3)



Security solution layers (3)



Authorization layer

- Resources protected through the **Attribute-Based Access Control (ABAC)** paradigm
- This allows building other AC schemes:
  - …?
  - …?
- **Access Policies** definable for each resource / operation
- Users' attributes processible through a **Mapping Function**

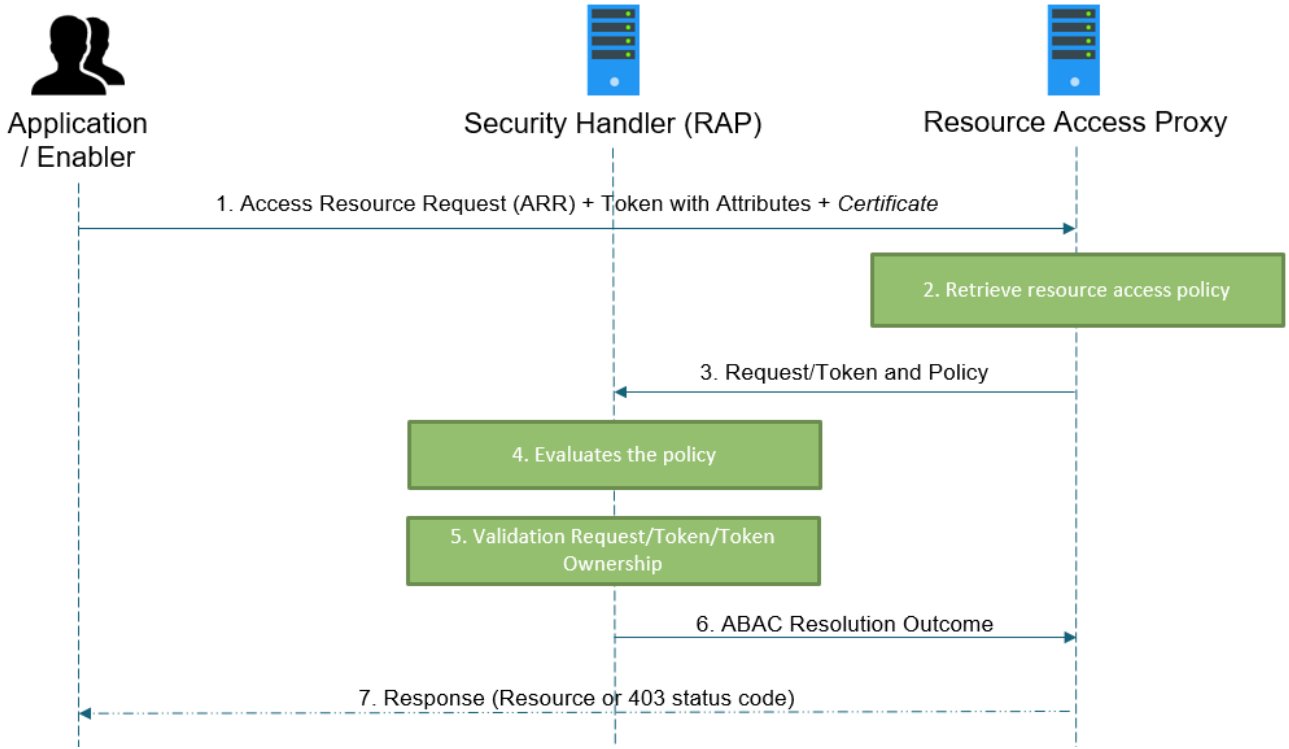
Authorization layer

- Resources protected through the **Attribute-Based Access Control (ABAC)** paradigm
- This allows building other AC schemes:
  - RBAC – Role based AC
  - IBAC – Identity based AC
- **Access Policies** definable for each resource / operation
- Users' attributes processible through a **Mapping Function**

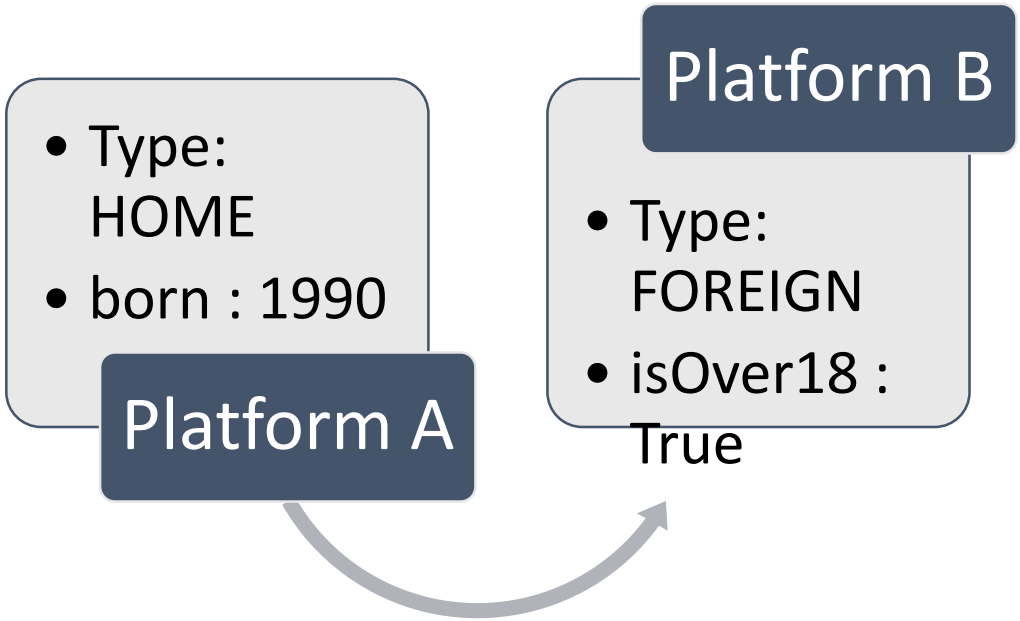
Task – designing policies (15’)

- Public
- Group
- Identity
- Identity + Role
- Composite

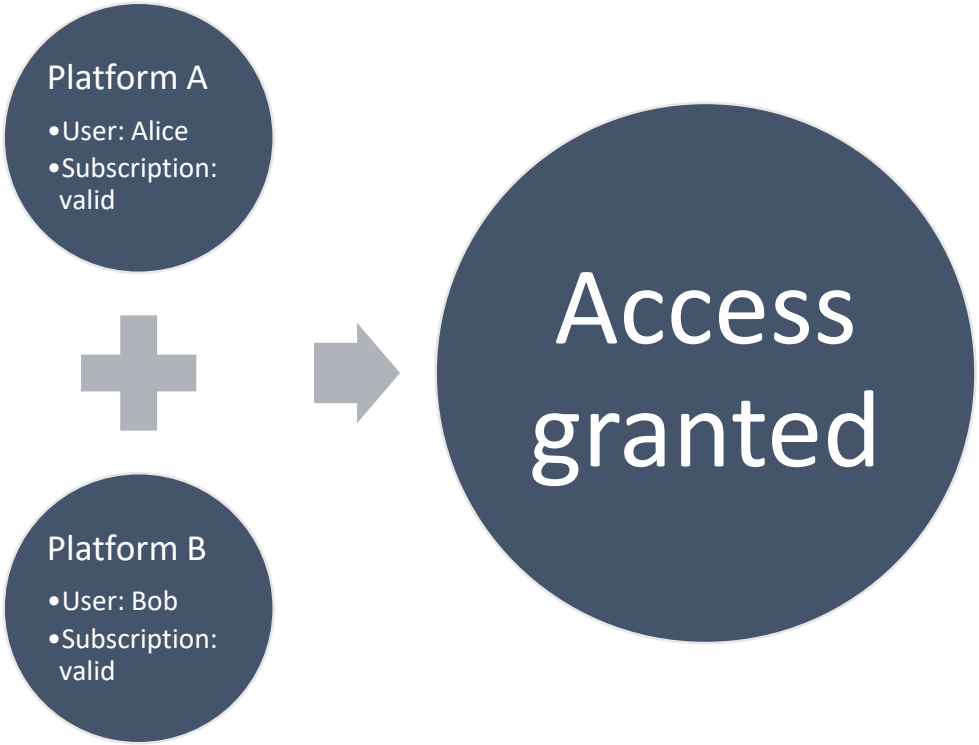
Auth(Z) with ABAC policies and JWS



Mapping function – extra flexibility / semantics



Multi-Domain Access Rights Composition

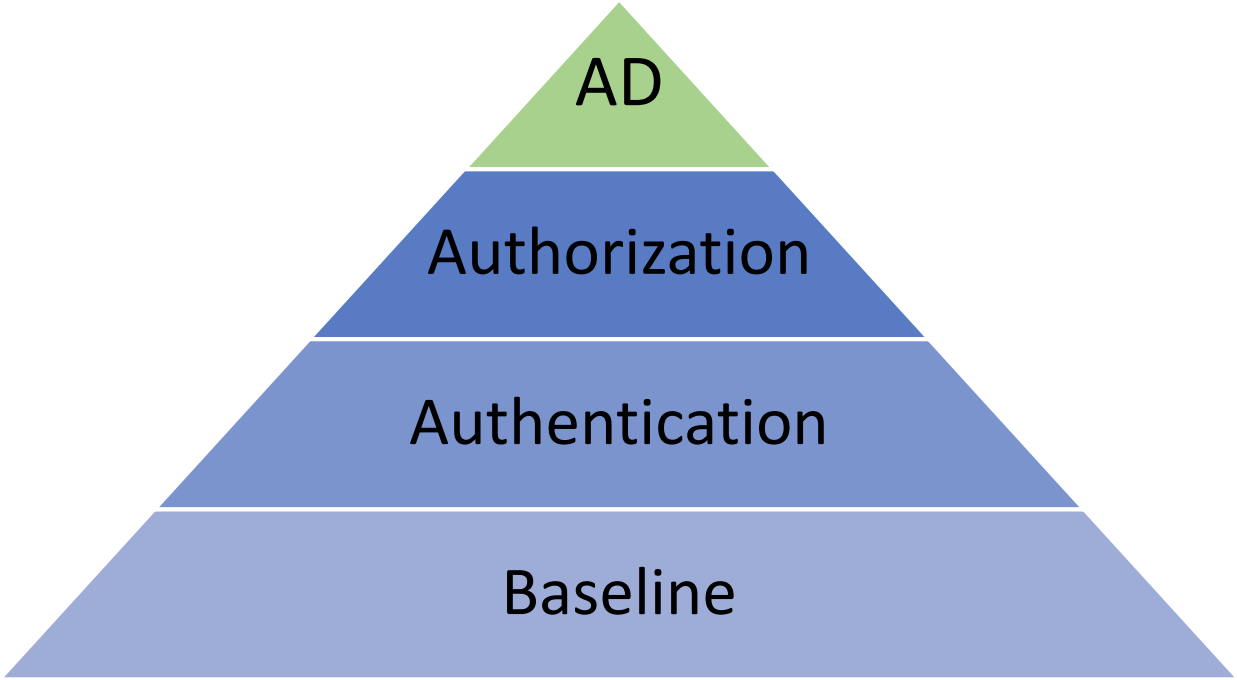


Define and delegate responsibilities
Focus on your responsibility
Trust the previous step

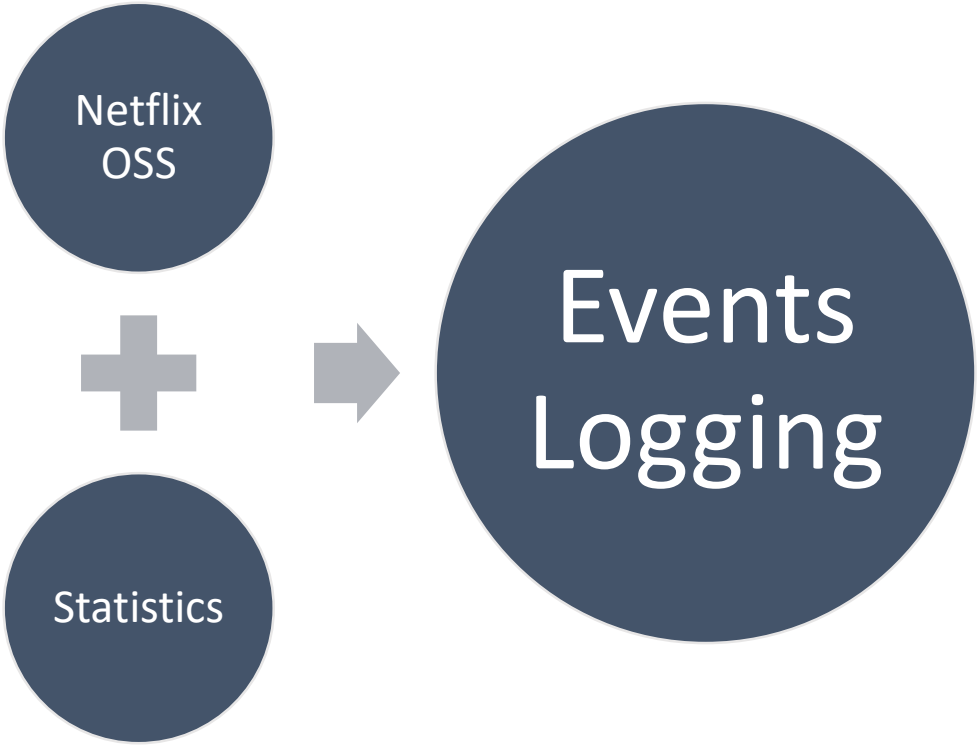
Relief time!

- Some extra info and summaries.

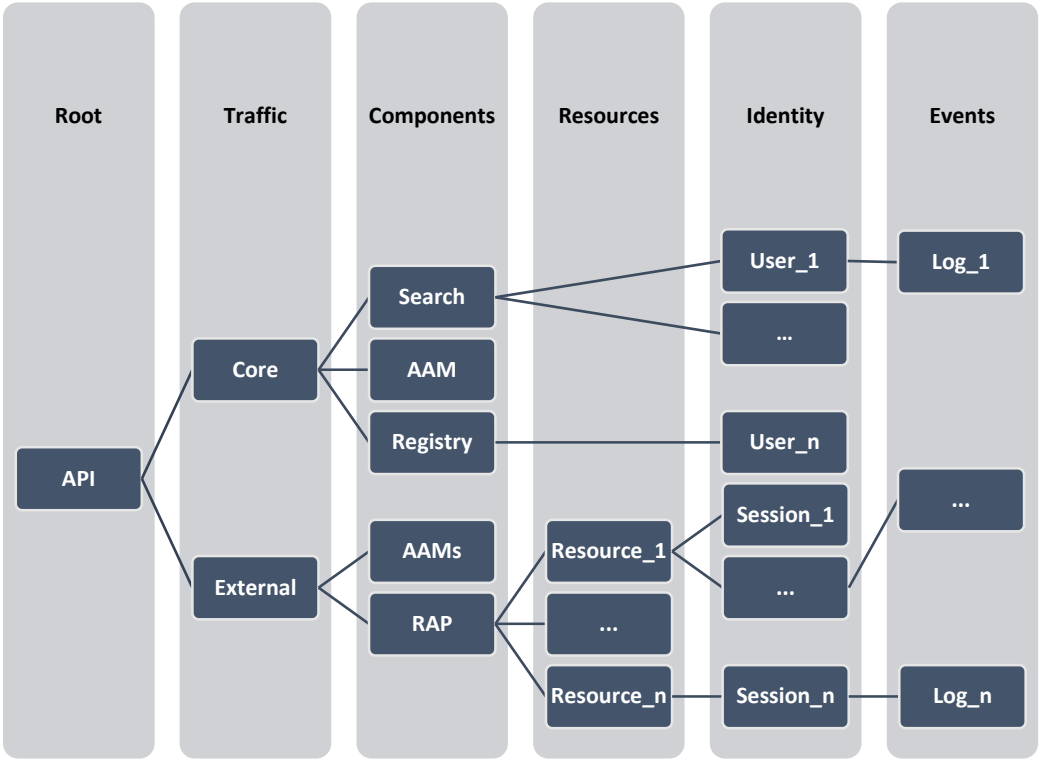
Security solution layers (4)



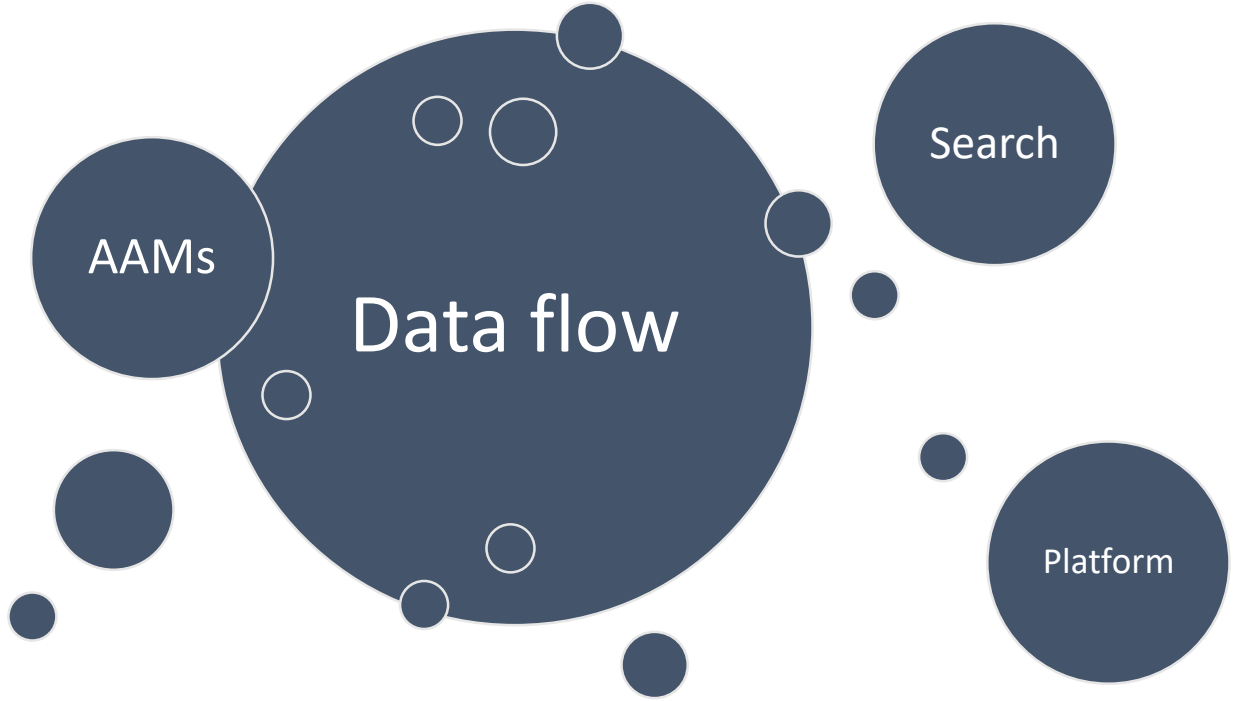
SymbIoTe Anomaly Detection layer tech



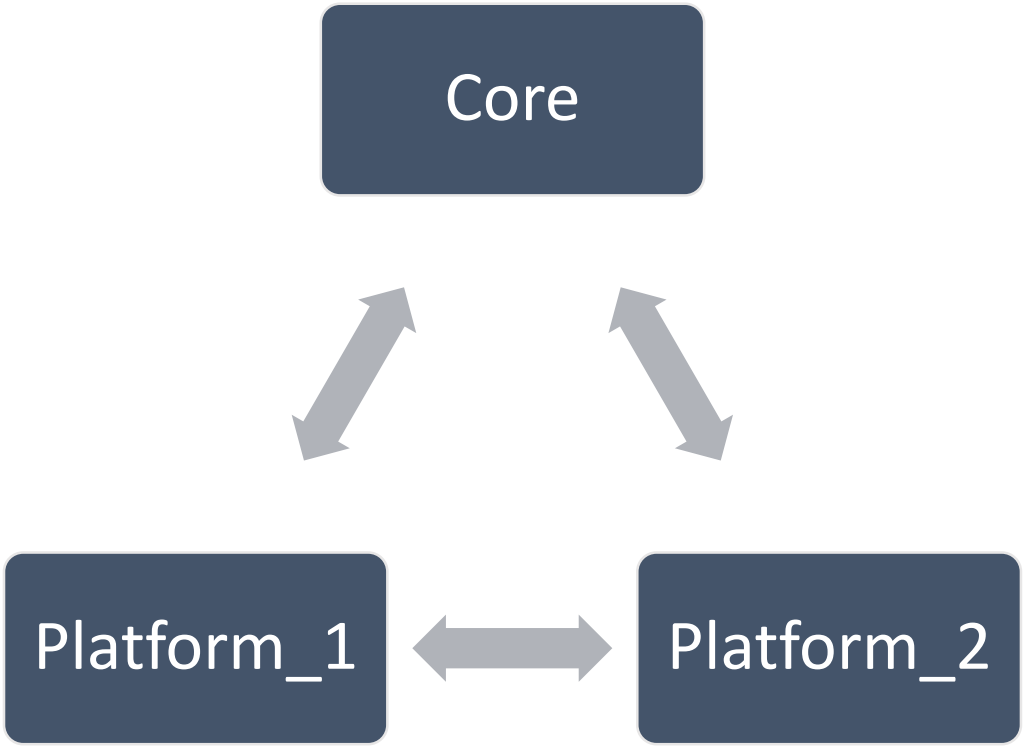
Behavioral patterns Decision Tree



Temporal patterns

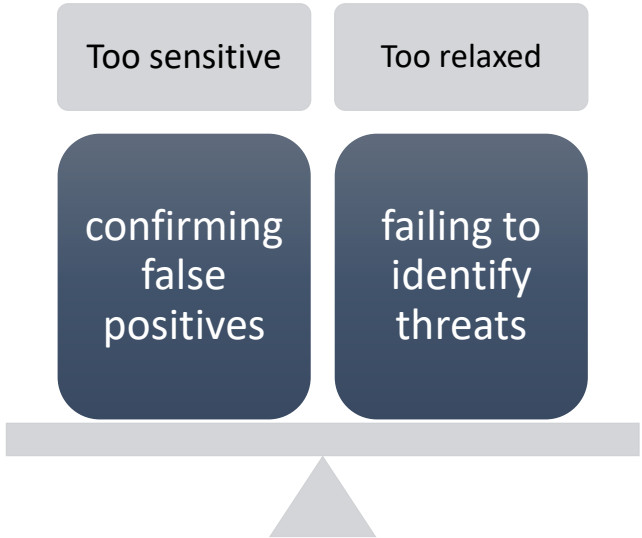


Identified AD threats



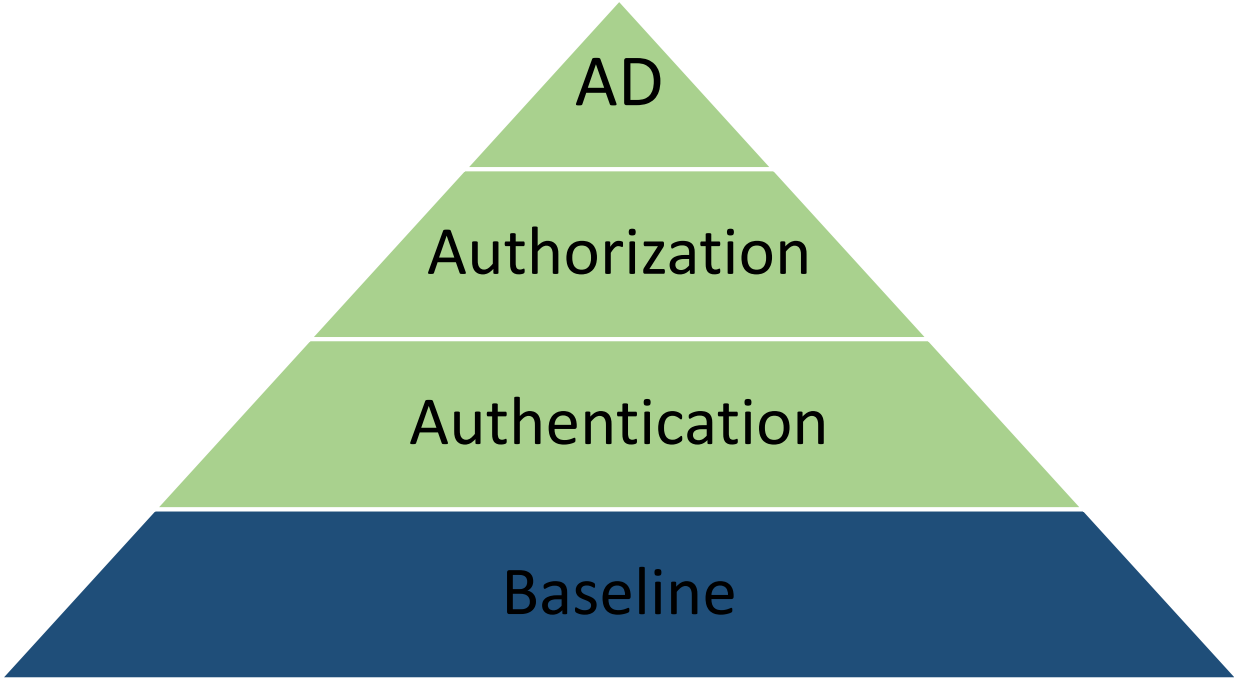
Common AD questions

- System usage statistics (GDPR)
- What is an anomaly in your scenario?
- Quality of AD service as a cost measure of:



You cannot predict everything
Don’t hinder business performance

Provided software



SymbIoTe security layer components

- Authentication & Authorization Managers (PKI CAs)
  - Issuing credentials (X.509 certs and JWTs)
  - Authenticating platforms and users (by credentials validation)
  - Managing credentials translation (Attributes mapping function)
- Security Handlers
  - Reference Cryptography operations implementation
  - Managing a key store with clients' certificates
  - Generating client's Auth(N) payloads
  - Matching ABAC policies against received Auth(Z) payloads
- Anomaly Detection Layer
  - Continuously building APIs' temporal and behavioral usage models to detect anomaly spikes

SymbIoTe Security Layer can be reused in your project!
Review the design as a whole!

Summary

Baseline	Divide (your design) and conquer!
	Ask SecOps for assistance in baseline security
	Code quality ahead of features
Authentication	Don’t reinvent the wheel
	Open acknowledged standards FTW
	Let someone review your processes
Authorization	
Anomalies	
Summary	

Summary

Baseline	Divide (your design) and conquer!
	Ask SecOps for assistance in baseline security
	Code quality ahead of features
Authentication	Don’t reinvent the wheel
	Open acknowledged standards FTW
	Let someone review your processes
Authorization	Define and delegate responsibilities
	Focus on your responsibility
	Trust the previous step
Anomalies	
Summary	

Summary

Baseline	Divide (your design) and conquer!
	Ask SecOps for assistance in baseline security
	Code quality ahead of features
Authentication	Don’t reinvent the wheel
	Open acknowledged standards FTW
	Let someone review your processes
Authorization	Define and delegate responsibilities
	Focus on your responsibility
	Trust the previous step
Anomalies	You cannot predict everything
	Don’t hinder business performance
Summary	

Summary

Baseline	Divide (your design) and conquer!
	Ask SecOps for assistance in baseline security
	Code quality ahead of features
Authentication	Don’t reinvent the wheel
	Open acknowledged standards FTW
	Let someone review your processes
Authorization	Define and delegate responsibilities
	Focus on your responsibility
	Trust the previous step
Anomalies	You cannot predict everything
	Don’t hinder business performance
Summary	SymbIoTe Security Layer can be reused in your project!
	Review the design as a whole!

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).