

# Audition MCF

**Maxime Puys**

15 Mai 2023



IUT CLERMONT AUVERGNE

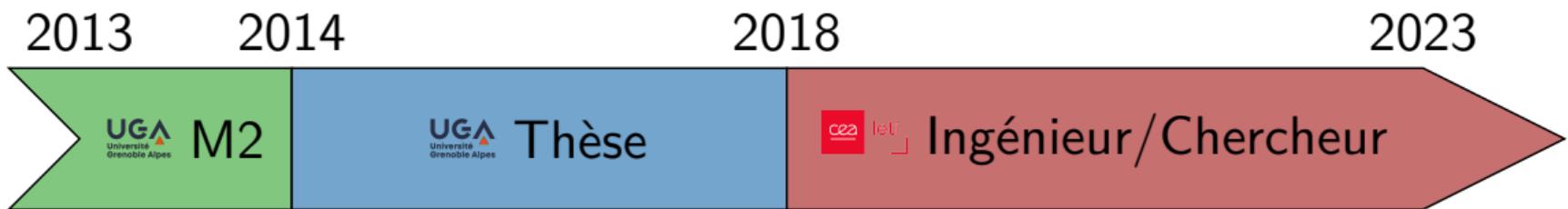
Aurillac - Clermont-Ferrand - Le Puy-en-Velay  
Montluçon - Moulins - Vichy

**UCA**  
UNIVERSITÉ  
**Clermont**  
**Auvergne**

# Plan

- 1 CV et parcours
- 2 Projet d'intégration en recherche
- 3 Projet d'intégration en enseignement

# Parcours professionnel et diplômes



# Parcours professionnel et diplômes

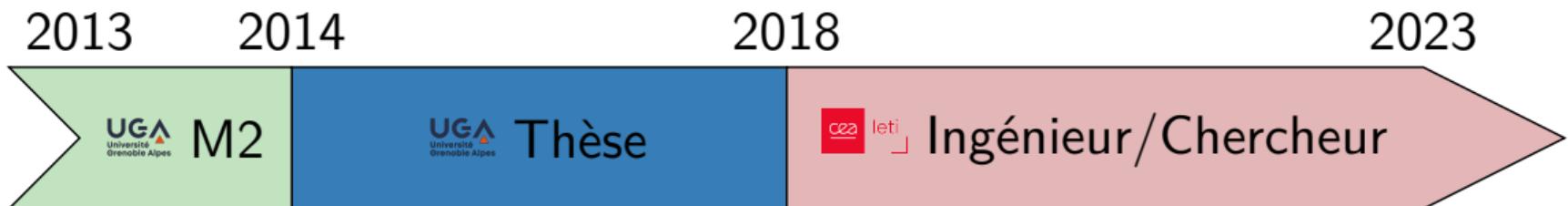


## 2013 - 2014 : Master en sécurité informatique

*Apprentissage entre SAFRAN Morpho, Osny et le Laboratoire Verimag, Grenoble, France*

- **Titre :** Sécurité des cartes à puces: analyses statiques en fautes et macros
- **Encadrants :** Marie-Laure Potet et Thanh-Ha Le

# Parcours professionnel et diplômes

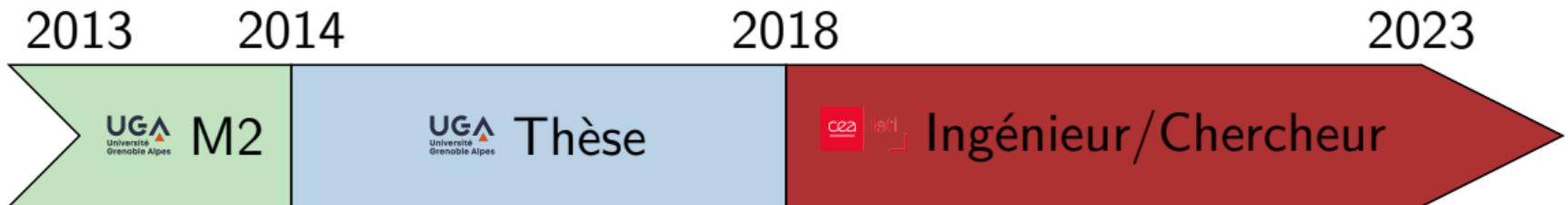


**2014 - 2018 :** Doctorat en sécurité informatique

*Laboratoire Verimag, Grenoble, France*

- **Titre :** Sécurité des systèmes industriels :  
Filtrage applicatif et recherche de scénarios d'attaques
- **Encadrants :** Marie-Laure Potet et Jean-Louis Roch

# Parcours professionnel et diplômes



**Depuis 2018 : Ingénieur/Chercheur**

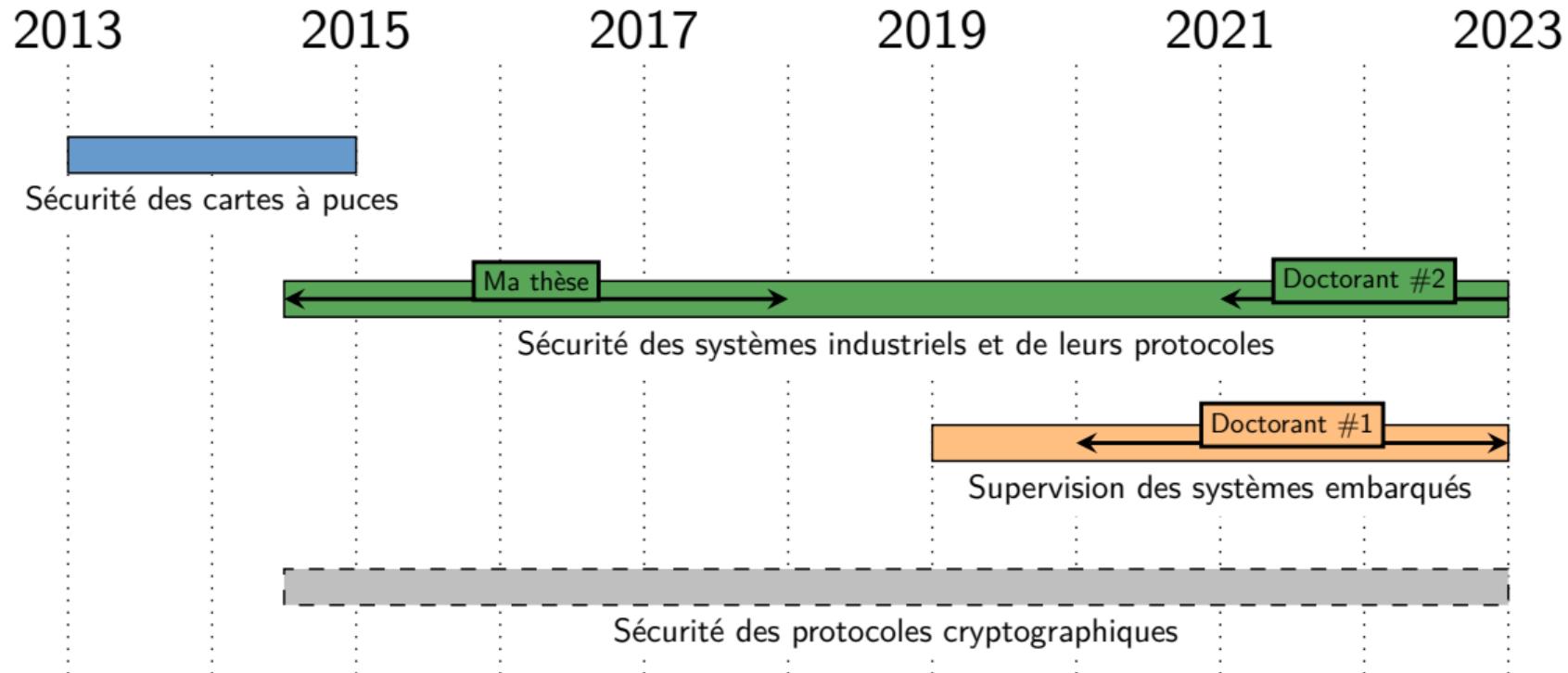
*CEA-LETI, Grenoble, France*

Poste permanent

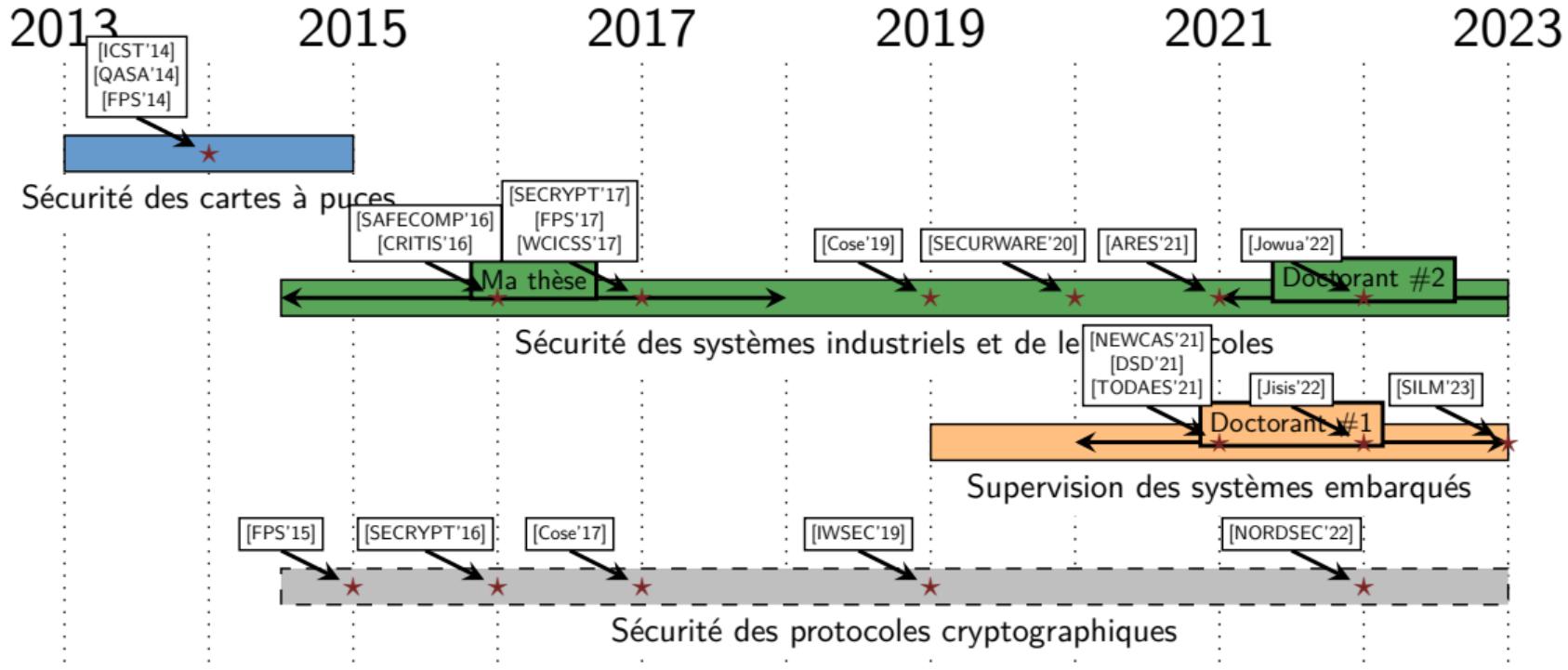
- **Activités :** Recherche et transfert technologique vers l'industrie
- **Sujets :** Sécurité des ICS, IoT, protocoles réseaux, H-IDS

Projet d'intégration en recherche

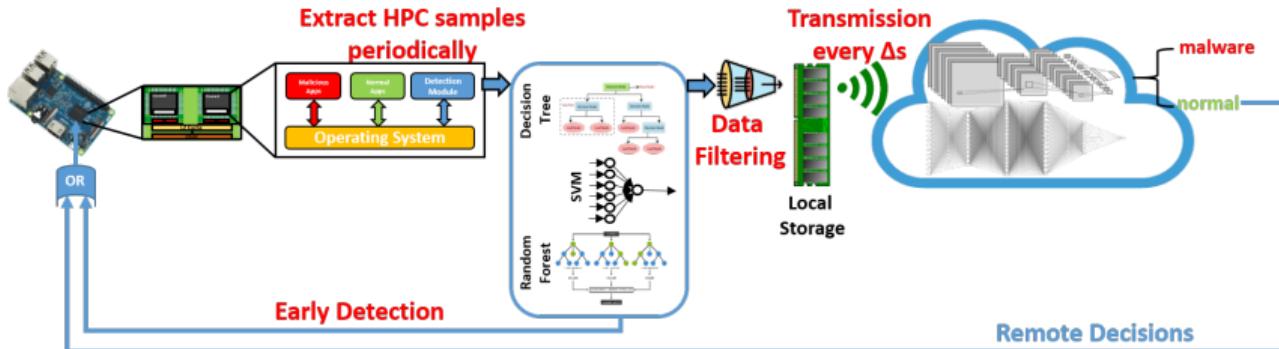
# Historique des thématiques



# Historique des thématiques



# H-IDS avec approche Local-Remote

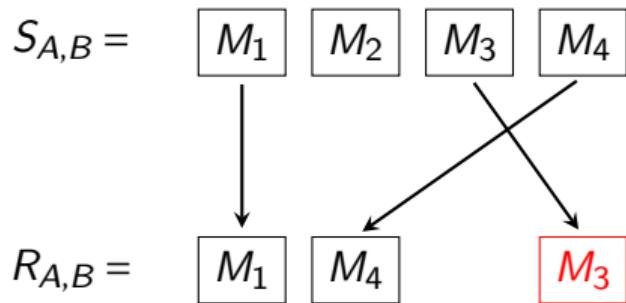


- IA locale ET distante
- **Déetecte localement des échantillons** très probablement malicieux
- Envoie **uniquement les échantillons suspicieux** à une IA distante
  - ▶ Minimize la bande passante requise
  - ▶ Assure la sécurité y compris en cas de panne réseau
- Test malwares automatisé avec Jenkins, buildroot, et docker

[Newcas'21], [DSD'21], [TODAES'21], [JISIS'22]

# Vérification de la couche transport du protocole OPC-UA

**Idée :** Modéliser l'ordre des messages en Tamarin



$$\begin{aligned} (\text{FD} \wedge \text{FA}) &\longleftrightarrow \text{FI} \\ \downarrow &\qquad\qquad\qquad \downarrow &\qquad\qquad\qquad \downarrow \\ (\text{IMD} \wedge \text{IMA}) &\longleftrightarrow \text{IMI} \\ \downarrow &\qquad\qquad\qquad \downarrow &\qquad\qquad\qquad \downarrow \\ (\text{NIMD} \wedge \text{NIMA}) &\longleftrightarrow \text{NIMI} \end{aligned}$$

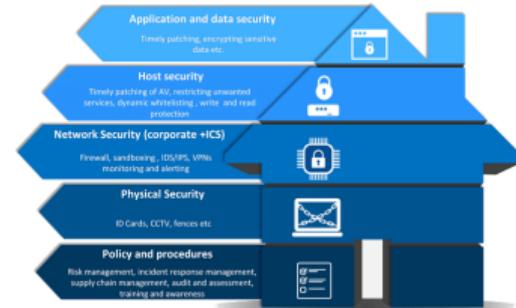
$A \Rightarrow B$  si un protocole vérifiant  $A$  garantit aussi  $B$ .

- Tester l'inclusion entre  $S_{A,B}$  et  $R_{A,B}$
- Propriété classique en réseau (ex : compteur de séquence TCP)
  - ▶ Jamais implémenté dans les outils de vérif crypto
- Test réel des attaques sur une stack Python

[Secrypt'17], [Cose'19]

# Projet de recherche

- **Problématique :** Comment optimiser le choix des fonctions de sécurité dans les réseaux et assurer leur résilience en cas d'attaques ?
- **Motivation :** Sécurité essentielle mais pas partout et pas au même niveau :
  - ⚠ Trop de défense : overhead, finance, frugalité
    - ▶ Besoin d'analyses de risque cyber ET métier [FPS'17]
    - ▶ **Objectif :** faire de la défense là où c'est important et analyser les relations entre les lignes de défense
- Décliné sur deux axes :
  - ① Optimisation du choix des fonctions de sécurité dans les réseaux
  - ② Résilience des réseaux



# Axe 1 : Optimisation du choix des fonctions de sécurité dans les réseaux

- Des analyses de risque, déduire une **heatmap** du réseau :
  - ▶ Points à protéger, chemins de vulnérabilités
  - ▶ **Orchestration de contre-mesures**
  - ▶ État de l'art existant mais manque les aspects métiers
- **Caractérisations** des contre-mesures :
  - ▶ **Apports** au regard de l'analyse de risque
  - ▶ **Coût en terme de performances** (garantie de *fail-safe*)
- Utilisation d'**apprentissage automatique** pour :
  - ▶ Tuning des paramètres des contre-mesure
  - ▶ GAN / IA génératives pour la découverte des besoins et la proposition de contre-mesures

## Axe 2 : Résilience des réseaux

- Beaucoup de travaux sur la détection et la protection ;
- Peu sur la réponse et la récupération.
- Concepts pourtant très étudiés hors de la sécurité :
  - Chemins alternatifs, topologies en anneau ou mesh, checkpointing
  - Solutions parfois étudiées en présence d'agents malveillants
- **Idée :**
  - Valider le delta entre les solutions existantes et leur utilisation en sécurité
  - Ex: protocoles HSR/PRP, découpage du réseau en zone et conduits, redéploiement de fonctionnalités métier/cyber



# Collaborations à court et moyen terme

- Avec Gérard CHALHOUB :

*Utilisation de l'IA pour l'optimisation des réseaux :*

- ▶ Lien avec mes travaux sur la détection de malwares par IA [Newcas'21], [DSD'21], [JISIS'22]

*Vérification de chemin empruntés dans le routage :*

- ▶ Semble proche de mon Axe 1 (optimisation du choix des CM dans les réseaux)

- Avec Pascal LAFOURCADE :

*Collaboration existante sur la vérification de protocoles*

- ▶ Développement de BIFROST [NORDSEC'22] (validation des attaques des outils de vérif) :
  - ★ Pourrait s'intégrer dans les projets ANR PRIVA-SIQ, MOBIS5, SEVERITAS
- ▶ Axe 2 (Résilience des réseaux)
  - ★ Pourrait débuter par une contribution à la proposition de projet ANR SEC-NGMN

# Responsabilités actuelles

- **Supervision d'étudiants :**

- ▶ Thèses : 1 soutenue, 1 en cours
- ▶ M2 : 3 soutenus
- ▶ Apprentis : 1 en cours

- **Montage de projets :**

- ▶ **Expérience de montage** sur : ANR, EU, DGA, PEPS CNRS, Carnot, Indus
- ▶ Taux de réussite sur académique : **36%** (4/11)
- ▶ **5 projets indus** montés en 5 ans au CEA

- **Objectif** : Passage HDR à horizon 3 ans.

## Projet d'intégration en enseignement

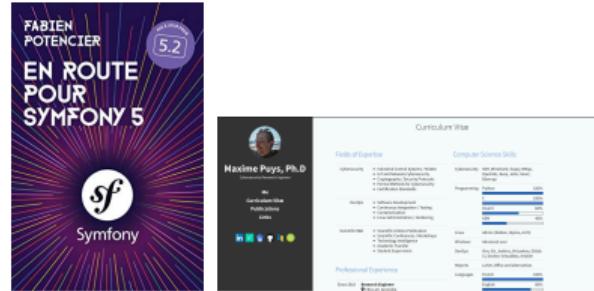
# Récapitulatif des activités d'enseignement

Période	Titre	Public	Type	Volume
2017 – 2018	Sécurité des protocoles cryptographiques	BAC+5	TD/TP	3h
	Introduction à la sécurité	BAC+3	CM/TD	6h
2018 – 2019	Sécurité, audit, et sécurité des systèmes et réseaux	BAC+5	TP	33h
	Théorie des langages	BAC+2	TD/Projets	15h
	Programmation fonctionnelle	BAC+1	TP	15h
2018 – 2022	Introduction à la sécurité	Ingénieurs du privé	CM/TP	60h

# Projet d'intégration en enseignement

- **R5.A.05 – Développement Symfony :**

- ▶ Jamais enseigné pour le moment
- ▶ Expérience sur des frameworks web :
  - ★ PHP/SQL (PDO, Codeigniter), Flask, Pelican, Hugo
- ▶ Quantité importante d'outils pédagogiques existants



- **R4.A.08 – Virtualisation et Dev(Sec)Ops :**

- ▶ Forte expérience : Docker et compose, Vagrant, Jenkins, Git et pipelines

- **R6.A.05 – Sécurité :**

- ▶ Forte expérience : Fondements de la sécurité, devsec, pentest

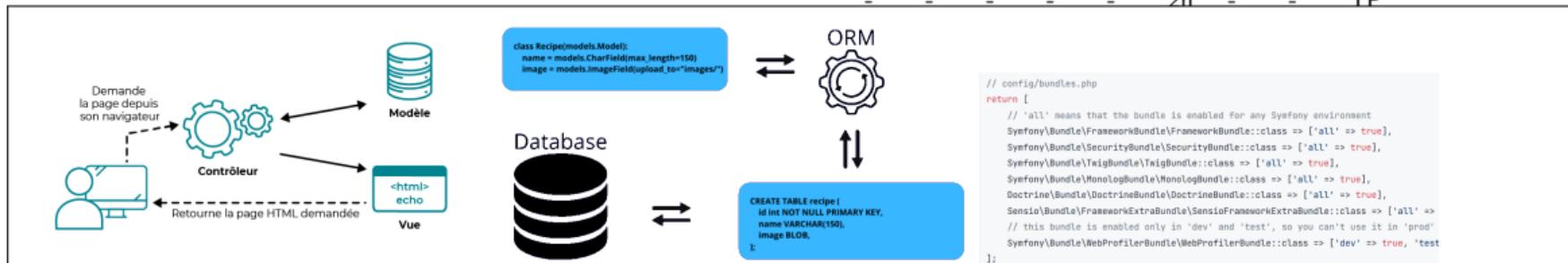
- **Autres compétences :** Linux, réseau, HTML/CSS, C, Python, IA

# Syllabus de cours sur le module R5.A.05 (34h)

Concepts	Répartition des cours								CM	TP
	S1	S2	S3	S4	S5	S6	S7	S8		
Architecture du projet et rappel (?) de concepts clés (architecture MVC, frameworks ORM, bundles, etc)	2h	-	-	-	-	-	-	-	CM	TP
Développement d'un site Web en Symfony (routage de pages, services, injections de dépendances, etc.)	2h	-	-	-	-	-	-	-	CM	TP
Mappage d'objets de base de données à l'aide de Doctrine	-	2h	-	-	-	-	-	-	CM	TP
Développement d'un site web en Symfony basé sur des événements	-	-	-	2h	-	-	-	-	CM	TP
Templating avec Twig	-	-	-	-	-	-	-	-	-	TP
Pratiques de développement sécurisé en PHP/Symfony (prévenir les attaques web simples)	-	-	-	-	-	-	-	-	-	TP
Evaluation	-	-	-	-	-	-	-	2h	DS	TP

# Syllabus de cours sur le module R5.A.05 (34h)

Concepts	Répartition des cours								
	S1	S2	S3	S4	S5	S6	S7	S8	
Architecture du projet et rappel (?) de concepts clés (architecture MVC, frameworks ORM, bundles, etc)	2h	-	-	-	-	-	-	-	CM
	2h	-	-	-	-	-	-	-	TP
Développement d'un site Web en Symfony (routage de pages, services, injections de dépendances, etc.)	-	2h	-	-	-	-	-	-	CM
	-	4h	-	-	-	-	-	-	TP
Mappage d'objets de base de données à l'aide de Doctrine	-	-	2h	-	-	-	-	-	CM
	-	-	4h	-	-	-	-	-	TP
Développement d'un site web en Symfony basé sur des événements	-	-	-	2h	-	-	-	-	CM
	-	-	-	2h	4h	-	-	-	TP
Templating avec Twig	-	-	-	-	-	-	-	-	-
	-	-	-	-	-	2h	-	-	TP



# Syllabus de cours sur le module R5.A.05 (34h)

Concepts	Répartition des cours								
	S1	S2	S3	S4	S5	S6	S7	S8	
Architecture du projet et rappel (?) de concepts clés (architecture MVC, frameworks ORM, bundles, etc)	2h	-	-	-	-	-	-	-	CM
	2h	-	-	-	-	-	-	-	TP
<b>Développement d'un site Web en Symfony (routage de pages, services, injections de dépendances, etc.)</b>	-	2h	-	-	-	-	-	-	CM
	-	4h	-	-	-	-	-	-	TP
Mappage d'objets de base de données à l'aide de Doctrine	-	-	2h	-	-	-	-	-	CM
	-	-	4h	-	-	-	-	-	TP
Développement d'un site web en Symfony basé sur des événements	-	-	-	2h	-	-	-	-	CM
	-	-	-	2h	4h	-	-	-	TP

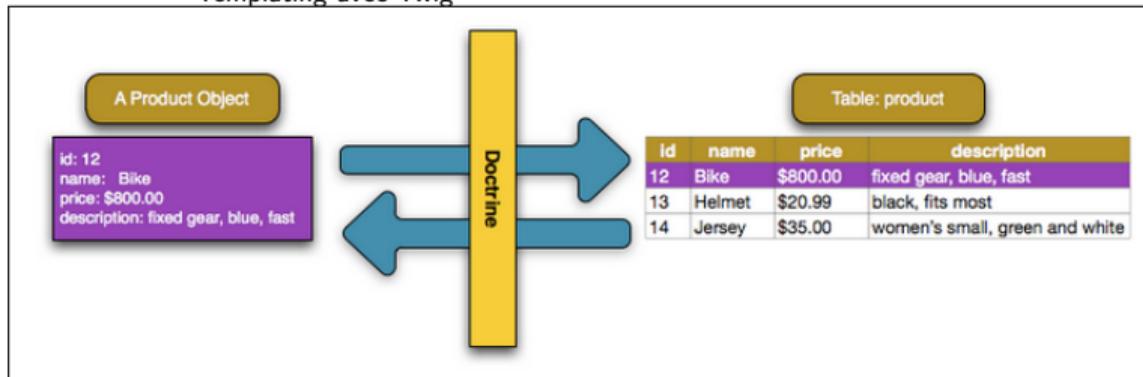
## Templating avec Twig

```
# config/routes.yaml
api_post_show:
    path:      /api/posts/{id}
    controller: App\Controller\BlogApiController::show
    methods:   GET|HEAD

api_post_edit:
    path:      /api/posts/{id}
    controller: App\Controller\BlogApiController::edit
    methods:   PUT
```

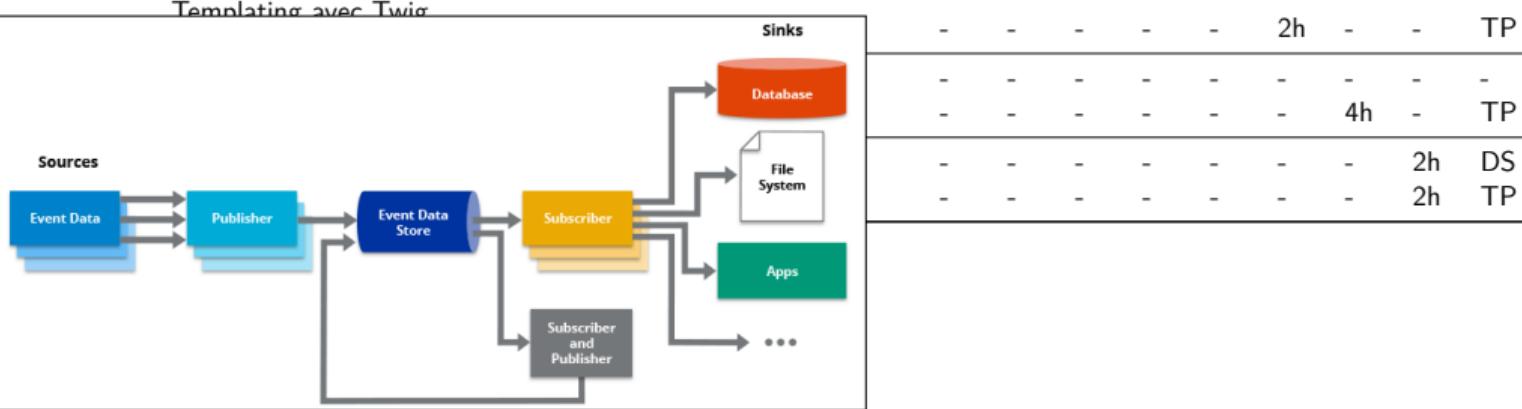
```
# config/services.yaml
services:
    App\Service\MessageGenerator:
        arguments:
            # this is not a string, but a reference to a service called 'logger'
            - '@logger'
```

## Syllabus de cours sur le module R5.A.05 (34h)



# Syllabus de cours sur le module R5.A.05 (34h)

Concepts	Répartition des cours							
	S1	S2	S3	S4	S5	S6	S7	S8
Architecture du projet et rappel (?) de concepts clés (architecture MVC, frameworks ORM, bundles, etc)	2h	-	-	-	-	-	-	- CM
	2h	-	-	-	-	-	-	- TP
Développement d'un site Web en Symfony (routage de pages, services, injections de dépendances, etc.)	-	2h	-	-	-	-	-	- CM
	-	4h	-	-	-	-	-	- TP
Mappage d'objets de base de données à l'aide de Doctrine	-	-	2h	-	-	-	-	- CM
	-	-	4h	-	-	-	-	- TP
<b>Développement d'un site web en Symfony basé sur des événements</b>	-	-	-	2h	-	-	-	- CM
	-	-	-	2h	4h	-	-	- TP
<u>Templating avec Twig</u>								
<b>Sources</b>								
Event Data								
Publisher								
Event Data Store								
Subscriber								
Subscriber and Publisher								
Sinks								
Database								
File System								
Apps								
...								



# Syllabus de cours sur le module R5.A.05 (34h)

## Concepts

Architecture du projet et rappel (?) de concepts clés (architecture MVC, frameworks ORM, bundles, etc)

Développement d'un site Web en Symfony (routage de services, injections de dépendances, etc.)

Mappage d'objets de base de données à l'aide de Doctrine

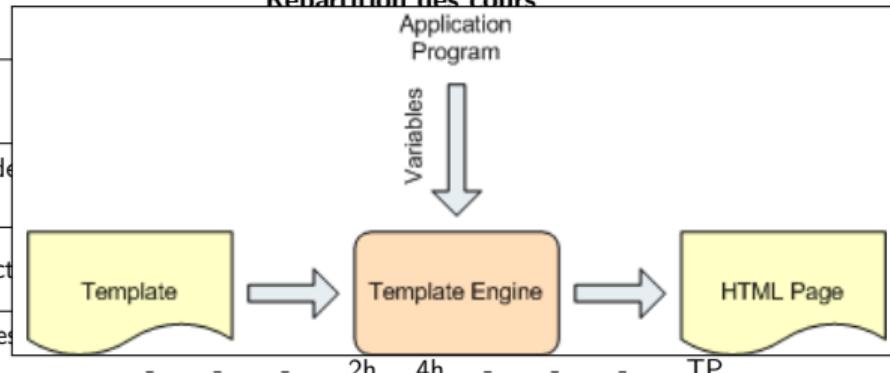
Développement d'un site web en Symfony basé sur des événements

## Templating avec Twig

Pratiques de développement sécurisé en PHP/Symfony (prévenir les attaques web simples)

Evaluation

## Répartition des cours



# Syllabus de cours sur le module R5.A.05 (34h)

## How Cross Site Request Forgeries (CSRFs) Work

① A hacker creates a request (in the form of a URL) for their own benefit from a website

② Hacker embeds that request into a hyperlink and sends it to a visitor who they hope is logged in to the site

③ The website visitor clicks the link, unwittingly sending the request to the site

④ Assuming the request is legitimate, the website fulfills the request, sending data, funds, or access to the hacker

## SQL Injection

Attacker: Http://teachers.com?teacherId=117 or 1=1--

Web API Server: SELECT \* FROM teachers WHERE teacherId=117 or 1=1;

Data for all teachers is returned to the attacker

Return data for all teachers

okta

## Templating avec Twig

-	-	-	-	-	-	2h	-	-	TP
---	---	---	---	---	---	----	---	---	----

## Pratiques de développement sécurisé en PHP/Symfony (prévenir les attaques web simples)

-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	4h	-	TP

## Evaluation

-	-	-	-	-	-	-	-	2h	DS
-	-	-	-	-	-	-	-	2h	TP

# Syllabus de cours sur le module R5.A.05 (34h)

Concepts	Répartition des cours								
	S1	S2	S3	S4	S5	S6	S7	S8	
Architecture du projet et rappel (?) de concepts clés (architecture MVC, frameworks ORM, bundles, etc)	2h 2h	- -	- -	- -	- -	- -	- -	- -	CM TP
Développement d'un site Web en Symfony (routage de pages, services, injections de dépendances, etc.)	- -	2h 4h	- -	- -	- -	- -	- -	- -	CM TP
Mappage d'objets de base de données à l'aide de Doctrine	- -	- -	2h 4h	- -	- -	- -	- -	- -	CM TP
Développement d'un site web en Symfony basé sur des événements	- -	- -	- -	2h 2h	- 4h	- -	- -	- -	CM TP
Templating avec Twig	- -	- -	- -	- -	- -	- 2h	- -	- -	- TP
Pratiques de développement sécurisé en PHP/Symfony (prévenir les attaques web simples)	- -	- -	- -	- -	- -	- -	- 4h	- -	- TP
<b>Evaluation</b>	- -	- -	- -	- -	- -	- -	- -	2h 2h	DS TP

# Responsabilités possibles à moyen terme

- **Lien important avec l'industrie tout au long de mon parcours :**
- Bonne **connaissance de l'entreprise et carnet d'adresse :**
  - ▶ En adéquation avec le côté professionnalisaing du BUT
  
- **Responsabilités envisageables à court terme :**
  - ▶ Suivi des alternants du BUT
  - ▶ Suivi des stages des étudiants
- **Responsabilités envisageables à moyen/long terme :**
  - ▶ Gestion du programme d'alternance du BUT
  - ▶ Gestion des stages des étudiants



## Conclusion

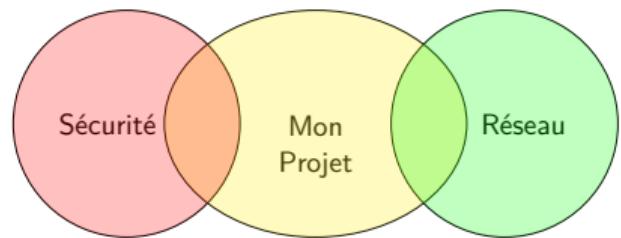
# Conclusion

- **Enseignement :**

- ⊖ Expérience limitée
- ⊕ Lien avec l'industrie en phase avec l'esprit du BUT
- ⊕ Syllabus réaliste et capacité à enseigner les concepts de Symfony
- ⊕ Compétences pour enseigner d'autres modules

- **Recherche :**

- ▶ Thématique historique en sécurité mais projet qui recoupe réseau et sécurité (thème RS de l'axe SIC)



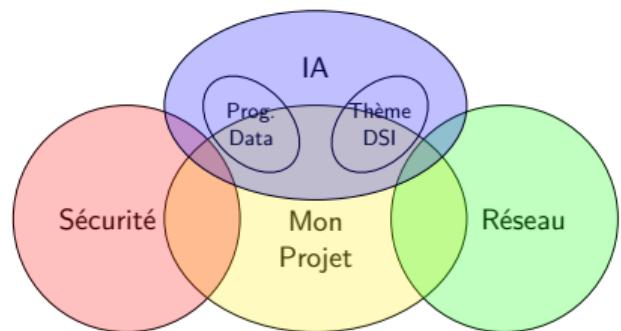
# Conclusion

- **Enseignement :**

- ⊖ Expérience limitée
- ⊕ Lien avec l'industrie en phase avec l'esprit du BUT
- ⊕ Syllabus réaliste et capacité à enseigner les concepts de Symfony
- ⊕ Compétences pour enseigner d'autres modules

- **Recherche :**

- ▶ Thématique historique en sécurité mais projet qui recoupe réseau et sécurité (thème RS de l'axe SIC)
- ▶ Expérience en IA :
  - ★ Collaboration possibles avec thème DSI et "Programme DATA" I-Site CAP 20-25



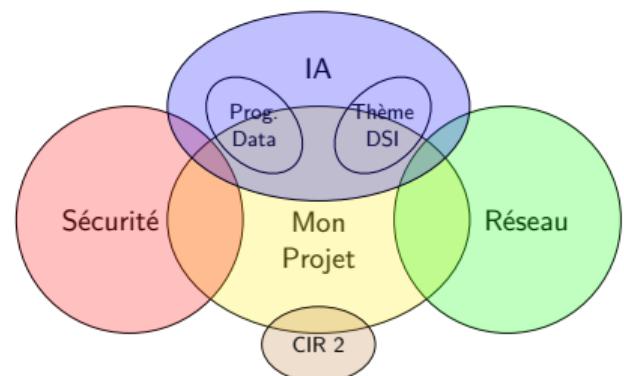
# Conclusion

- **Enseignement :**

- ⊖ Expérience limitée
- ⊕ Lien avec l'industrie en phase avec l'esprit du BUT
- ⊕ Syllabus réaliste et capacité à enseigner les concepts de Symfony
- ⊕ Compétences pour enseigner d'autres modules

- **Recherche :**

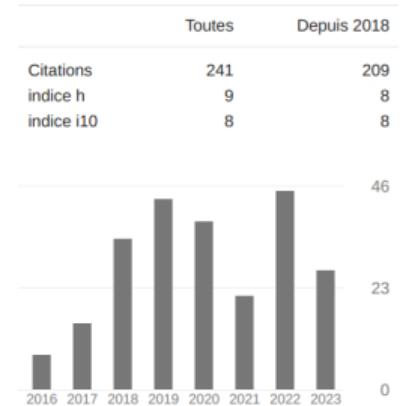
- ▶ Thématique historique en sécurité mais projet qui recoupe réseau et sécurité (thème RS de l'axe SIC)
- ▶ Expérience en IA :
  - ★ Collaboration possibles avec thème DSI et "Programme DATA" I-Site CAP 20-25
- ▶ Expérience en sécurité des systèmes industriels :
  - ★ Collaboration possibles avec le CIR 2 I-Site CAP 20-25 ("Usine du futur")



# Conclusion

Merci de votre attention !

Type de Publication	Nombre	Rangs des publications
Journaux internationaux	5	Q1 (2) / Q2 (2) / Q3 (1)
Conférences internationales	16 (+ 1)	A (1) / B (8) / C (2)
Conférence nationales	8	



# Environnement de recherche CEA

- **Statut et missions :**
  - ▶ Établissement public à caractère industriel et commercial (EPIC)
  - ▶ Recherche appliquée et transfert vers l'industrie
- **Financement :**
  - ▶ 25% de subvention de l'état
  - ▶ 75% restant à trouver via des projets (IRT, EU, indus, DGA)
  - ▶ Recherche permanente de co-financements (beaucoup de réutilisation des travaux)
  - ▶ Projets "alimentaires"
- **Valorisation :**
  - ▶ Sujets de recherche choisis et cadrés en fonction du potentiel de valorisation (TRL 3-5)
  - ▶ Forte pression pour breveter
  - ▶ Pression pour publier rapidement (conférences B/C)
- **Mais présence de financements internes (thèses, stages, etc)**

# Curriculum vitæ



- **Maxime Puys**
- **Âge :** 32 ans
- **Doctorat :** Sécurité info en 2018, Verimag, Univ. Grenoble Alpes
- **Depuis 2018 :** Ingénieur/Chef de projet au CEA-LETI, Grenoble
- **Thématiques de recherche :**
  - ▶ Sécurité des dispositifs et réseaux (I)IoT
  - ▶ Protocoles réseaux