

State of The Art for Cyber Range

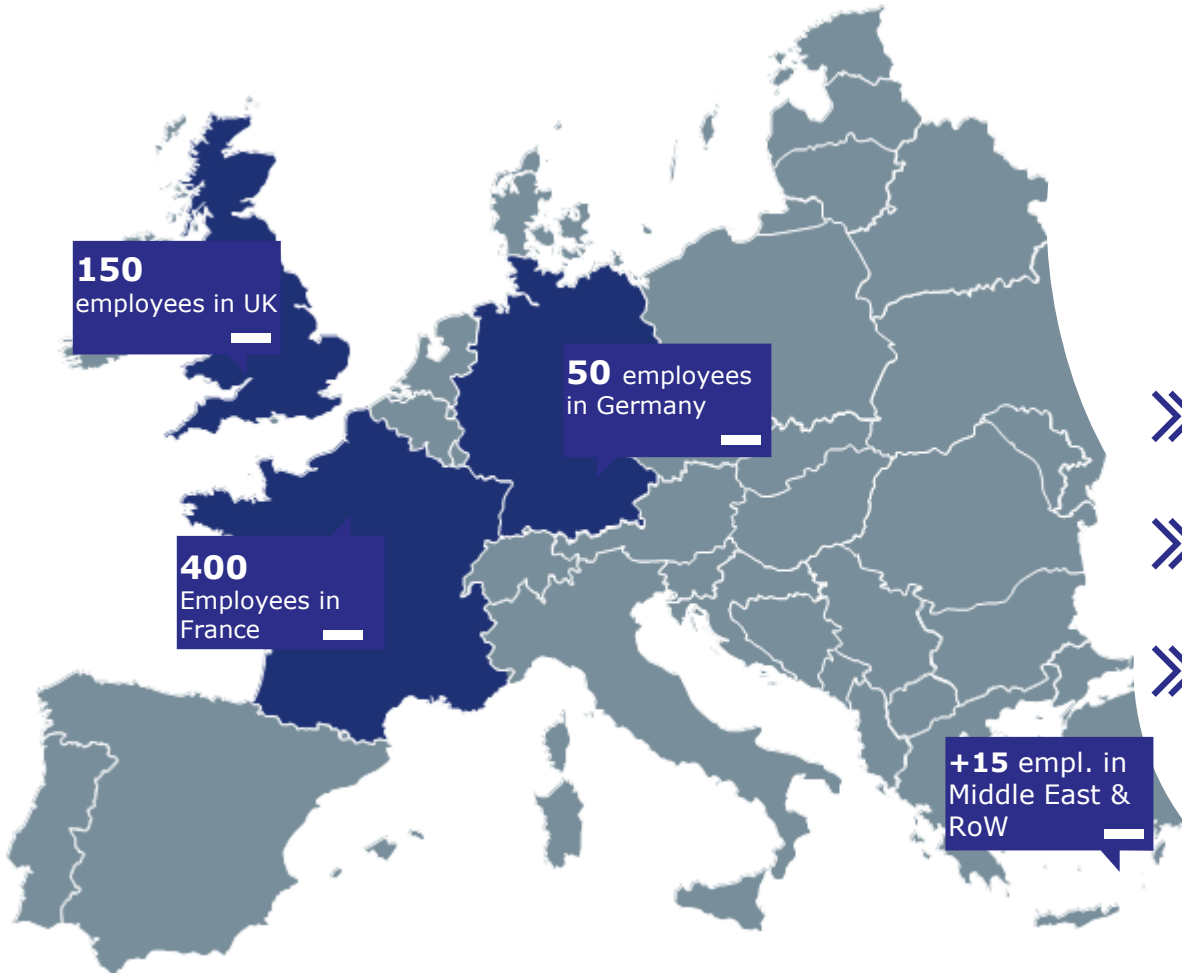
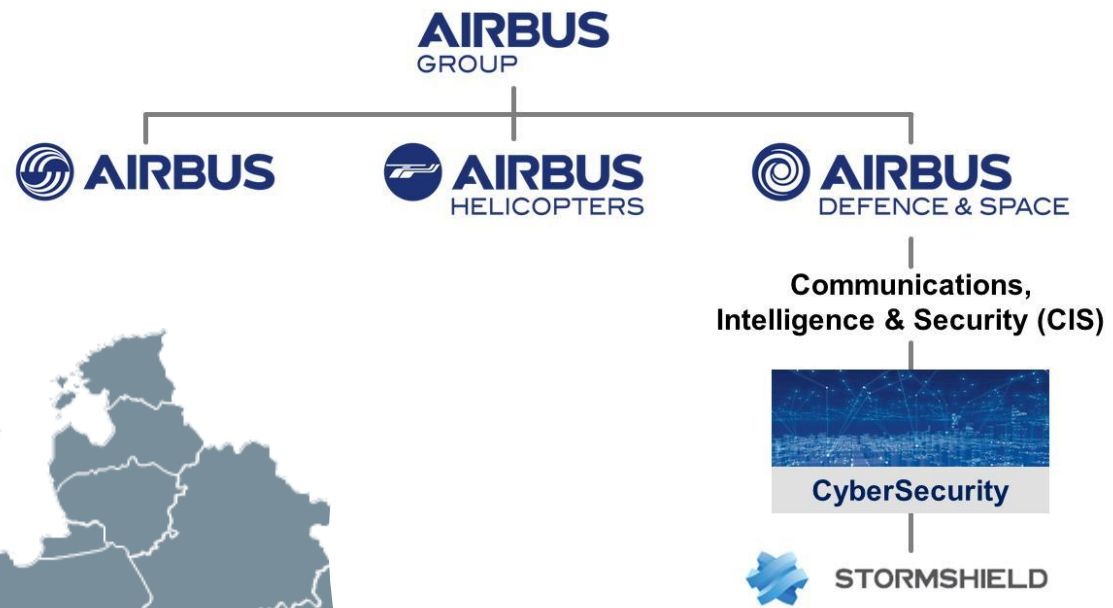
Airbus Defence & Space Cybersecurity

Adrien Bécue

adrien.becue@airbus.com

+33 161386451

SU-INFRA01-2018-2019-2020	Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure	IA
SU-DS01-2018	Cybersecurity preparedness	IA
SU-DS04-2018-2020	Electrical Power and Energy System	IA
SU-ICT-01-2018	Dynamic countering of cyber-attacks	IA



» **>100 M € Revenue**

» **>20% R&D Budget**

» **3 Cyber-Defence Centers**



Cyber-Defence Center

- 24/7 operation
- Managed Security Services:
 - Intrusion detection & APT monitoring: KeelBackNet®
 - Risk Monitoring & Situation Awareness: Cymerius®



AIRBUS DEFENCE & SPACE | Elancourt - PTF | 00:00 CET

Incidents: 5 | Non affectés: 5

Accident: 1702 | Criticité de l'incident élevé
 1710 | Criticité de l'incident élevée
 1716 | Niveau de l'incident élevé

Incident: 1702 | Criticité de l'incident élevée
 1710 | Criticité de l'incident élevée
 1716 | Niveau de l'incident élevé

Statut: 1702 | Criticité de l'incident élevée
 1710 | Criticité de l'incident élevée
 1716 | Niveau de l'incident élevé

Date de création: 2014/11/25 17:28 | Date de modification: 2014/11/25 17:28 | Modifié par: system

Cyberdefence portfolio overview



Managed Services

Services

- Security Operation Center (PDIS)
- Vulnerability watch
- Threat intelligence



Consulting

Services

- APT Health Check
- Audit Active Directory
- Penetration testing
- Technical & Organizational Audits (PASSI)
- Consulting in IT Security
- Cybersecurity training & testing services



Incident Response

Services

- Incident Response (PRIS)
- Malware analysis
- Digital investigation & forensics

- Keelback NET®
- Cymerius®
- Orion Malware

Airbus Technologies

- BTA (Audit AD)
- Keelback HOST®
- **CyberRange**

- Keelback HOST®
- Orion Malware
- SOC Mobile

Cyber Range: definitions

***Cyber Range:** a virtual environment used for cyberwarfare training and cyber-technology development.*



Facts & figures

60 % of Cyber security applicants Lack of qualification

Source: ISACA

1.8

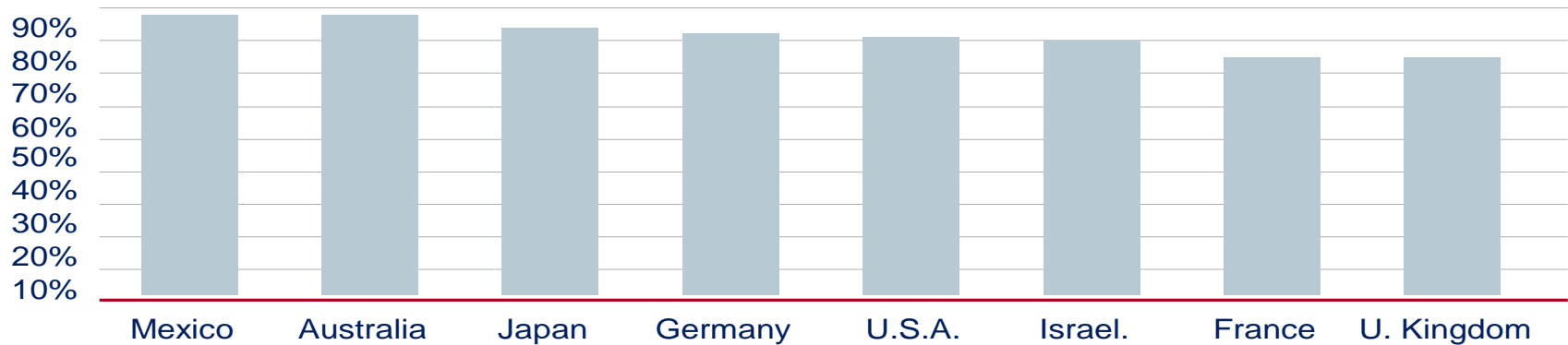
MILLION

unfilled security jobs worldwide by 2022

Source : the Center's 2015 Global Information Security Workforce Study (GISWS).

Source : the Center's 2015 Global Information Security Workforce Study (GISWS).

Percentage of respondents who say there is a shortage of cybersecurity professionals in their country



Source : Hacking the skills shortage CSIS and Intel Security, July 2017

Market potential

49% of the organization plan to spend more on Training (EY information security survey 2016).

Cyber security Training and education market size by Region, 2014-2019 (\$Billion)

Region	2014	2015	2016	2017	2018	2019	CAGR (2014-2016)
NorthAm	1.13	1.19	1.27	1.35	1.44	1.55	6.4%
EU	0.69	0.71	0.75	0.78	0.83	0.89	5.2%
APAC	0.47	0.52	0.57	0.64	0.72	0.82	12%
EMEA	0.19	0.21	0.24	0.26	0.30	0.34	11.6%
LatAm	0.15	0.17	0.19	0.22	0.25	0.30	15.4%
Total	2.63	2.80	3.01	3.25	3.55	3.90	8.2%

Source: MarketsandMarkets Analysis

Main characteristics



Fixed



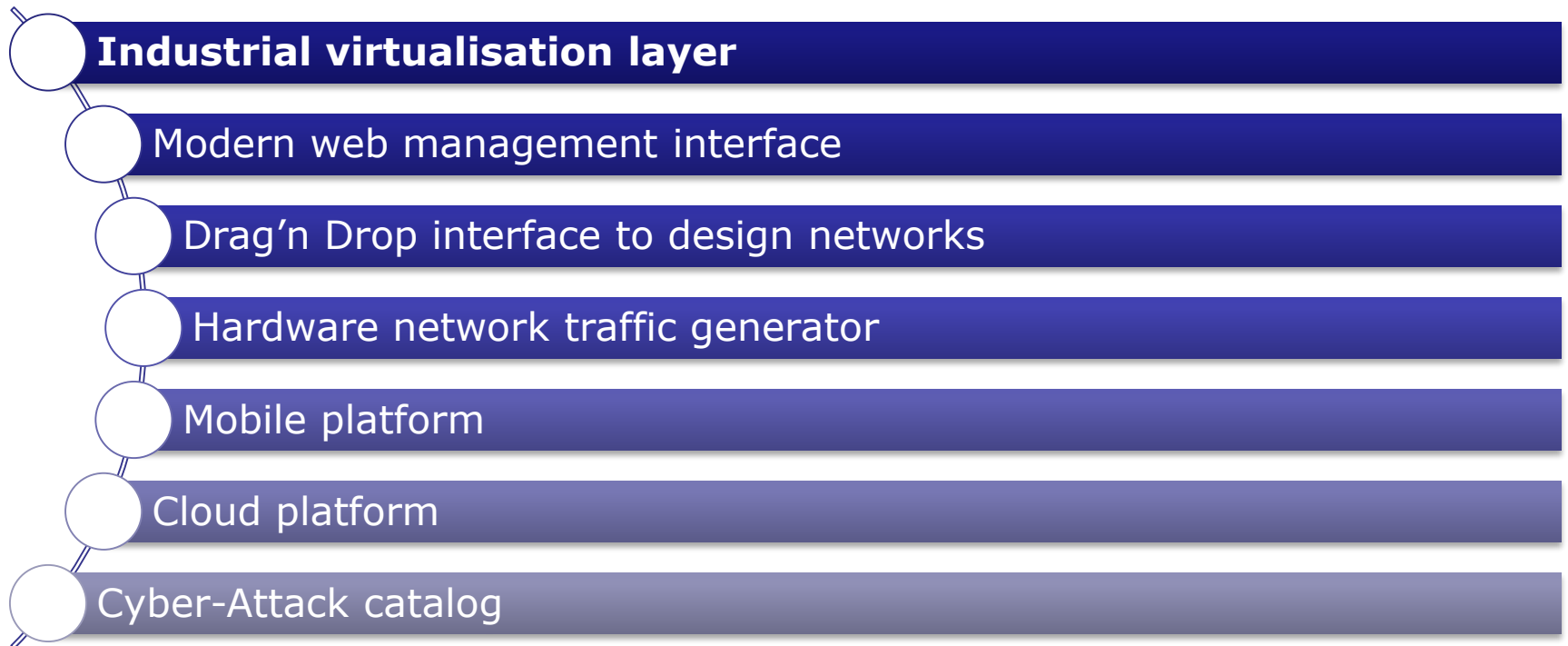
Mobile



Cloud



Differentiation criteria



Functionalities	CyberRange (Airbus)	Hynesim (Diateam)	Malice (Sysdream)	CyberBit	Pao Alto (CTS)	Raytheon	Simspac e (travell o)	Cisco	cDex (vector synergy)
Industrial virtualisation layer	Y		Y	Y		Y	Y	Y	Y
Modern web management interface	Y		Y	Y	Y	?	Y	?	?
Drag'n Drop interface to design networks	Y	Y		Y			Y	?	?
Hardware network traffic generator	Y	Y		Y			Y		?
Mobile platform	Y	Y	Y	Y	Y	Y	Y		
Cloud platform	Planned 2018	Y	Y	Planned 2018	Y		Y	Y	
Cyber-Attack catalog	Y			Y		Y	Y	Y	Y
Scenario Engine for complex attacks and automated test plans	Y			Y	Y	Y	Y	Y	Y
LMS (Learning Management System) portal	Planned 2018	Y	Y	Planned 2018		Y	Y		
Customizable without professional services	Y			Y			Y		?
BUSINESS MODEL	platform, training	platform	platform, training	Platform training	Platform + Service Providers	Platform		Platform training	Cyber training



Scénario : Intelligence services report that a transnational organization to prepare a wave of cyber-attacks targeting multiple energy production sites en Europe in an attempt to trigger series of environmental catastrophes in their surroundings.



400
 participants

48 finalists
 split into 16
 teams

6 hours
 exercise

300 Virtual
 Machines

EUROPEAN
 CYBER WEEK

FINALE DU CHALLENGE DE CYBERSÉCURITÉ



THALES


 PÔLE D'EXCELLENCE
 CYBER


LE CHALLENGE EST TERMINÉ !

SITE : PARC NATUREL DE LA FORÊT BAVAROISE, ALLEMAGNE

POLLUTION : FAIBLE

EQUIPE : ENSIBS 1

RESSOURCES : 60.8 %

PROTECTION : 50 %

CLASSEMENT DES ÉQUIPES

1	ENSIBS 1	60.8 %
2	INTER-ÉCOLES	60.4 %
3	TÉLÉCOM-BRETAGNE 3	59.7 %
4	ENSIBS 2	49.8 %
5	TÉLÉCOM-BRETAGNE 1	46.4 %
6	CFA-AFTI	44.6 %
7	ESISAR 1	40.2 %
8	CENTRALESUPELEC	39.2 %
9	ENSIBS 3	38.7 %
10	INSA-CVL	29.2 %
11	ENSEIRB	27.8 %
12	ENSI BOURGES	26.5 %
13	EPITA	26.1 %
14	TÉLÉCOM-BRETAGNE 2	26 %
15	UNILIM	15.5 %
16	ESISAR 2	13 %



