DS7-Addressing Advanced Cyber Security Yhreats and Threat Actors

Airbus Defence & Space Cybersecurity

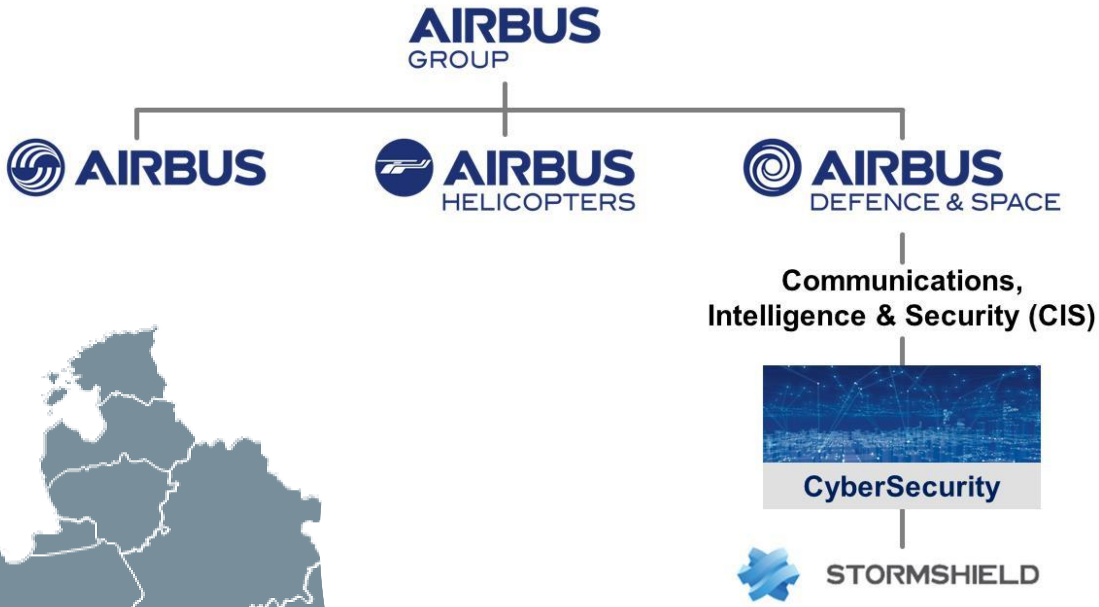
Adrien Bécue

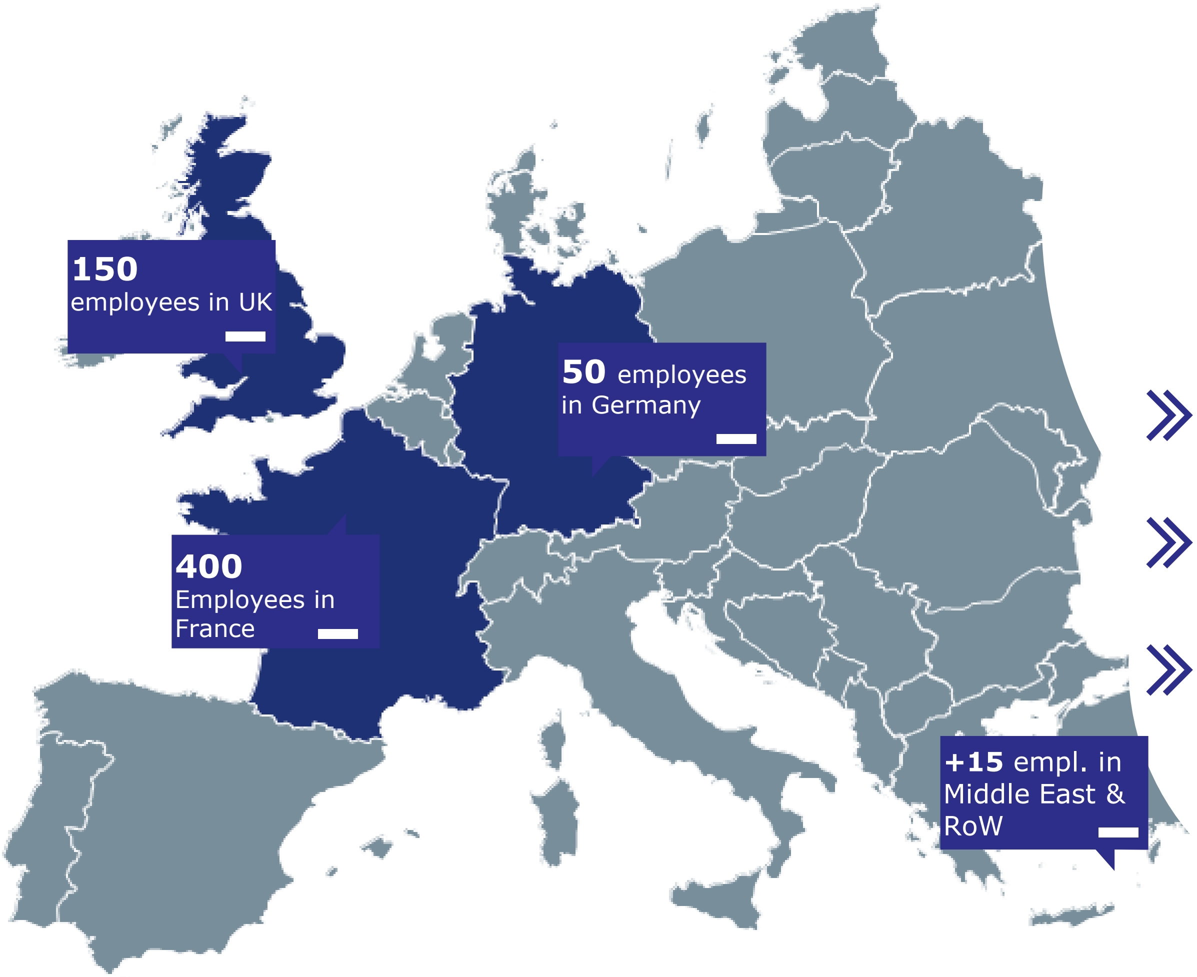
adrien.becue@airbus.com

+33 161386451

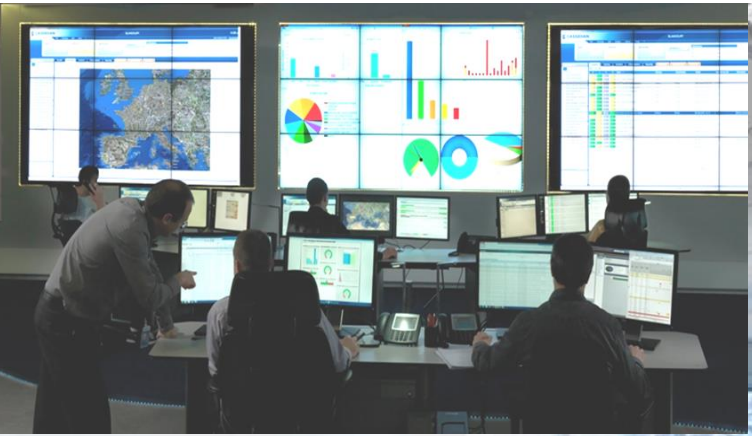
Area of interest	Choose Y or N
DS-07-2017 - RIA: Addressing Advanced Cyber Security Threats and Threat Actors **A) Situational Awareness**	Y
DS-07-2017 - IA: Addressing Advanced Cyber Security Threats and Threat Actors **B) Simulation Environments, Training**	Y
DS-08-2017 – IA - Privacy, Data Protection, Digital Identities – **Privacy-enhancing Technologies (PET)**	N
DS-08-2017 – IA - Privacy, Data Protection, Digital Identities – **General Data Protection Regulation in practice**	N
DS-08-2017 – IA - Privacy, Data Protection, Digital Identities – **Secure digital identities**	N

AIRBUS DEFENCE & SPACE



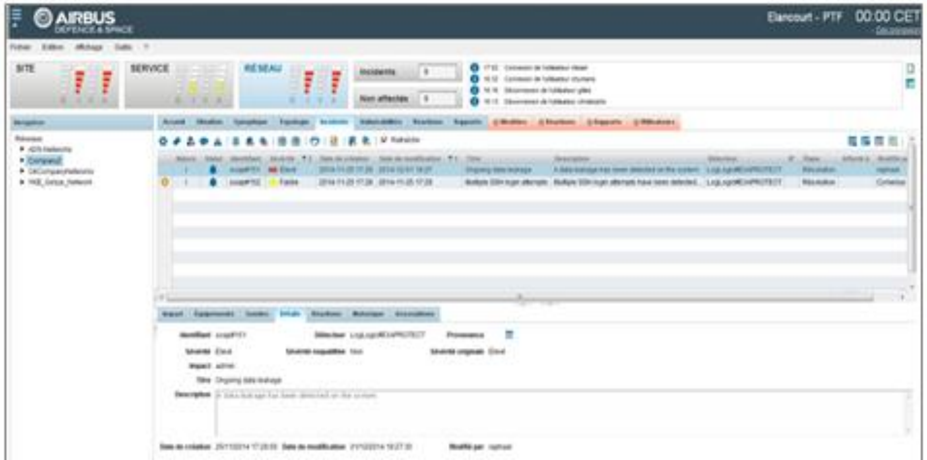


- >100 M € Revenue
- >20% R&D Budget
- 3 Cyber-Defence Centers



Cyber-Defence Center

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



Defence Projects

- ✓ Large Governmental Projects
- ✓ National gateways & Crypto (MIYO, SEG, Ectocryp, etc.)
- ✓ Key Management (UK)

Cyber Consulting

Security consulting:

- ✓Cyber governance
- ✓Architecture
- ✓“Security by design”
- ✓Software code audits
- ✓Security audits
- ✓Threats intelligence
- ✓Vulnerability & risk
- ✓Penetration tests

Incident response:

- ✓Crisis management
- ✓Incident response
- ✓Forensics

Training:

- ✓Cyber Range
- ✓Skills development
- ✓Products & Solutions training

Monitoring & Managed Services

Monitoring solutions:

- ✓ Security Hypervisor (Cymerius)
- ✓ Malware Analyzer (Orion)
- ✓ Sandboxing services
- ✓ Network Sensor (KeelbackNet)
- ✓ Endpoint Sensor

Managed services:

- ✓ Cyber Defence & Security Operations Centers (SOC)
- ✓ Private Cloud Vulnerability Scanning

DS7-IA

DS7-RIA

Stormshield Products

- ✓Network Security
- ✓Endpoint Security
- ✓Data Security
- ✓Manufacturing Security

COMMON CRITERIA CERTIFIED EAL4+

DS7 - Addressing Advanced Cyber Security Threats and Threat Actors

Challenge: increase detection & response capabilities to face fast evolving cyber-threats

Scope:

- **RIA–Situational Awareness:** anomaly detection, visualization tools, big data analysis, threat analysis, deep-packet inspection, protocol analysis, forensics …
- **IA-Simulation Environments, Training:** innovative simulation environments and training tools tailored to train cybersecurity professionals

Impact: shorten response time, improve resilience

RIA–Situational Awareness –Topic Description

Scope:

- providing organizations the appropriate situational awareness towards cyberhreats

- detect and quickly and effectively respond to sophisticated cyber-attacks

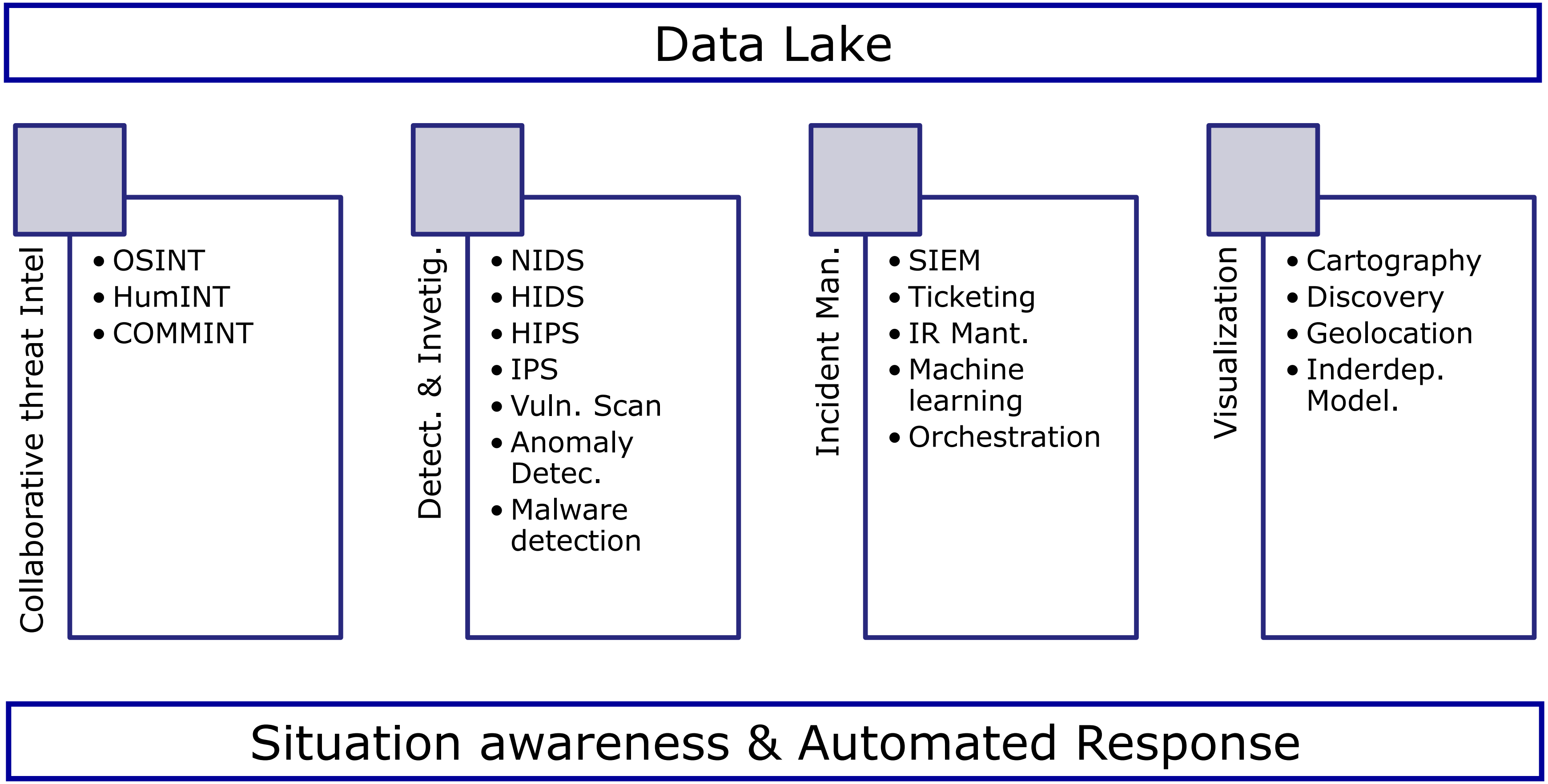
- consider the need to collect necessary forensic information from attackers

- address the impact to fundamental rights, data protection and privacy

Range:

-2-3 M€ ; TRL3-5

DS7-RIA-Collaborative tools for enhanced situational awareness



Data Lake

Collaborative threat Intel

- OSINT
- HumINT
- COMMINT

Detect. & Invetig.

- NIDS
- HIDS
- HIPS
- IPS
- Vuln. Scan
- Anomaly Detec.
- Malware detection

Incident Man.

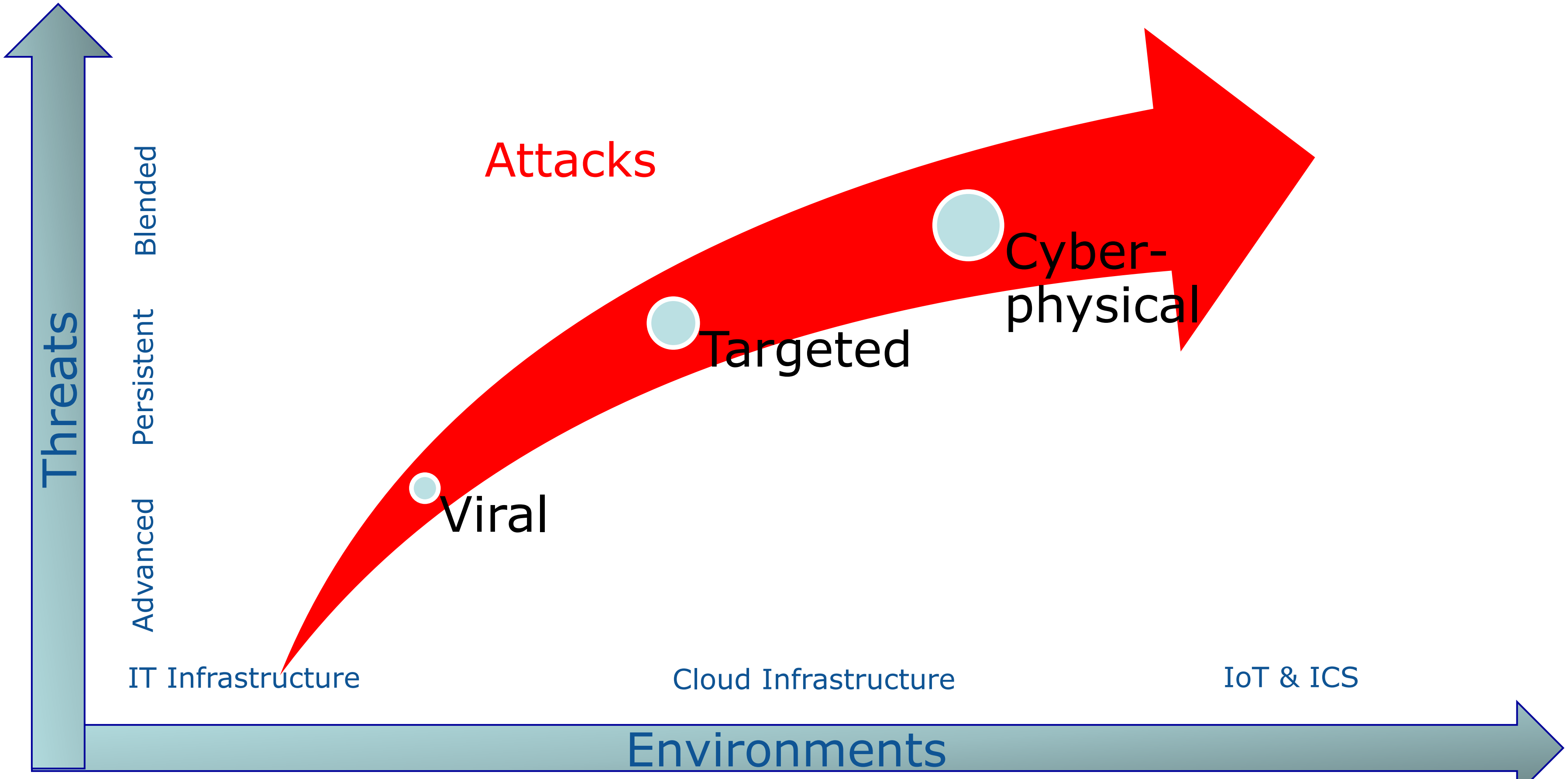
- SIEM
- Ticketing
- IR Mant.
- Machine learning
- Orchestration

Visualization

- Cartography
- Discovery
- Geolocation
- Inderdep. Model.

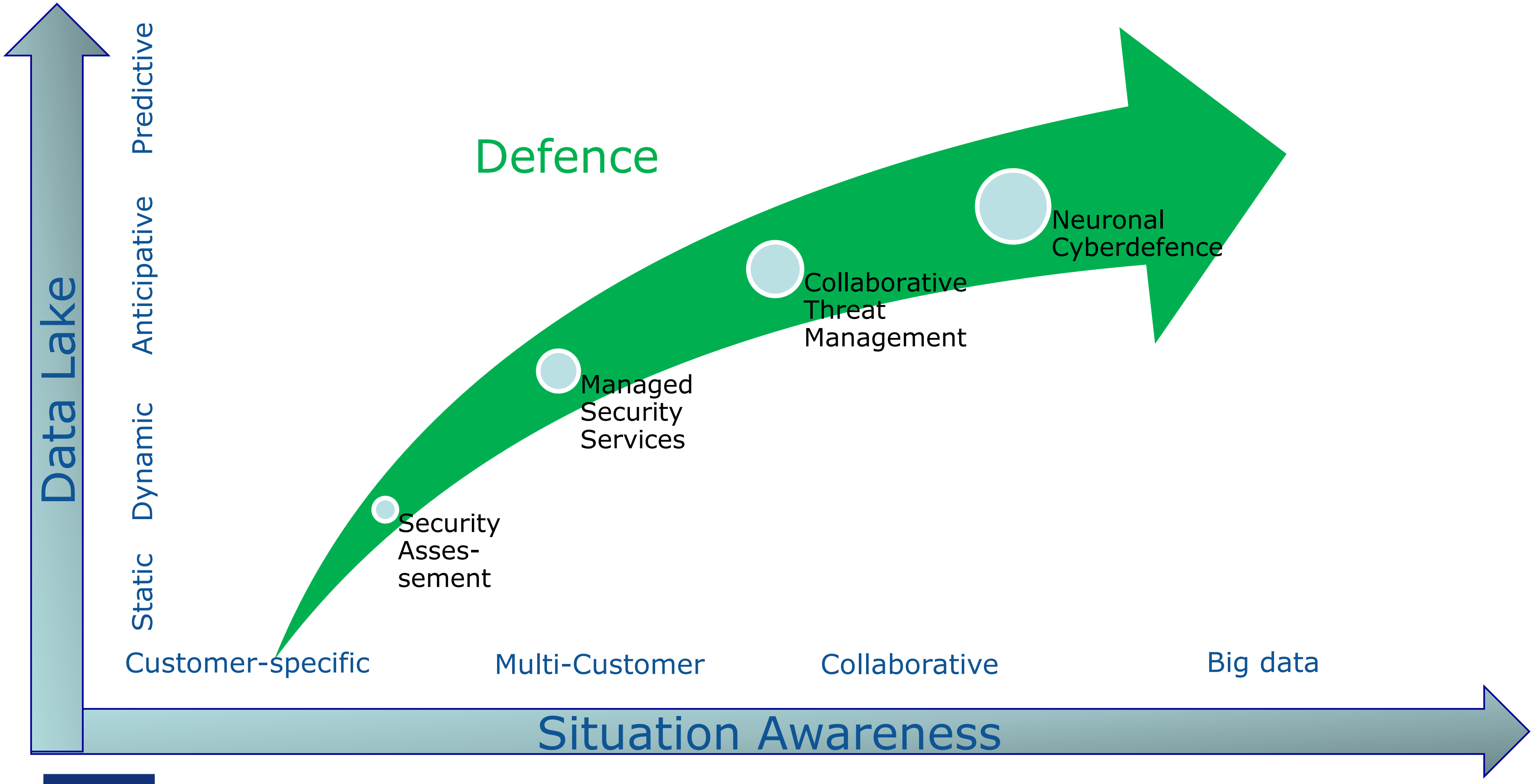
Situation awareness & Automated Response

DS7-RIA-Offensive Challenge



AIRBUS DEFENCE & SPACE

DS7-RIA-Defensive Challenge



DS7-RIA-Consortium Building

Existing partners:

-Airbus DS Cybersecurity (FR)

-Institut Mines Telecom (FR)

Looking for:

-End-users and practitioners (public/private)

-Cyberthreat Intelligence actors

-CERTs & SOCs operators

-Security software editors

-Specialized Research labs & academics

IA–Simulation environments, training-Topic description

Scope:

- innovative simulation environments and training materials to prepare defenders to counter advanced cyber-attacks

- creating realistic cyber environments to produce benign and malicious system events

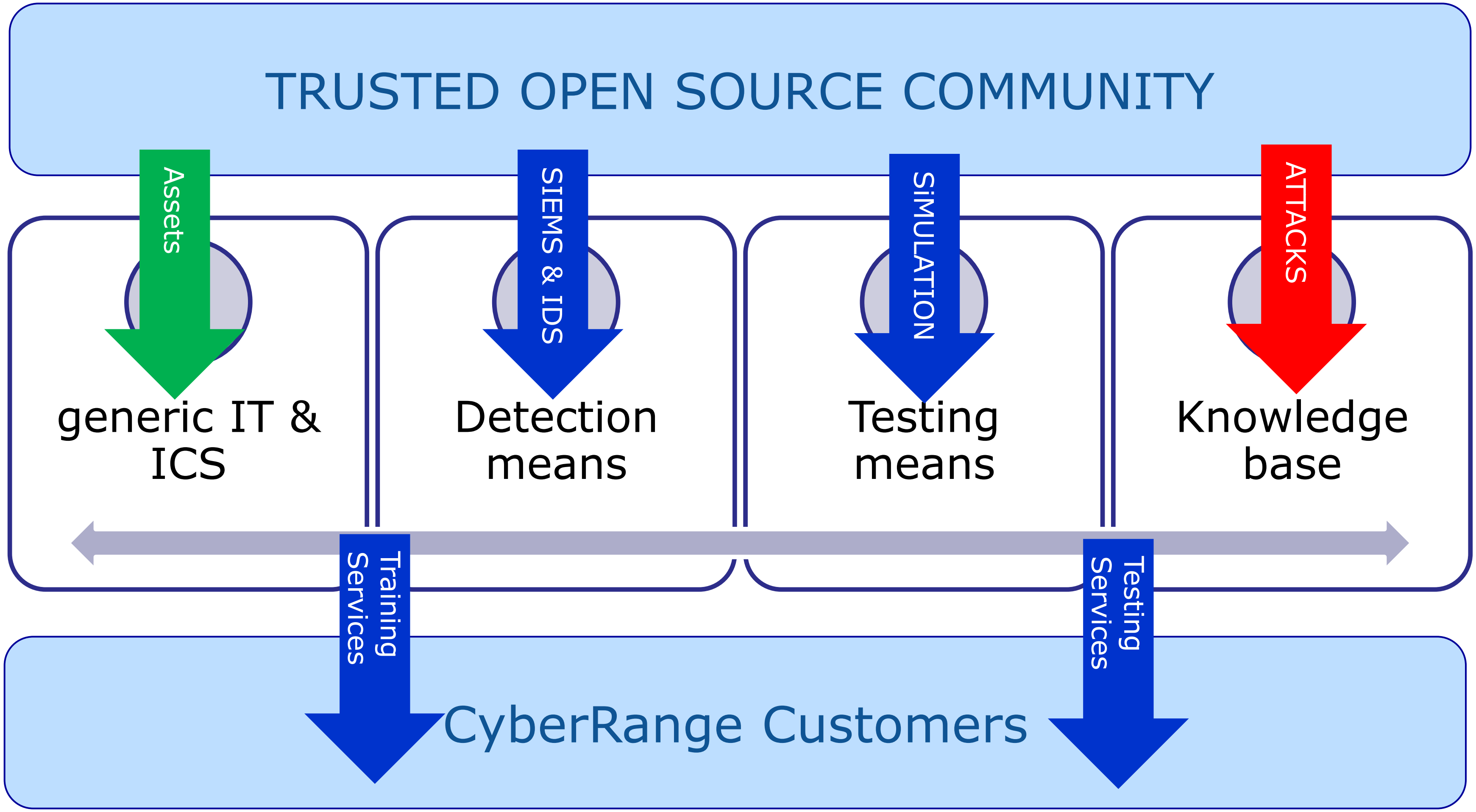
- real-time student performance assessment, dynamic configuration and adaptation of exercise scope and difficulty

- definition and creation of new scenarios and cyber threats in a cost and time-effective manner

Range:

-4-5 M€ ; TRL6-7

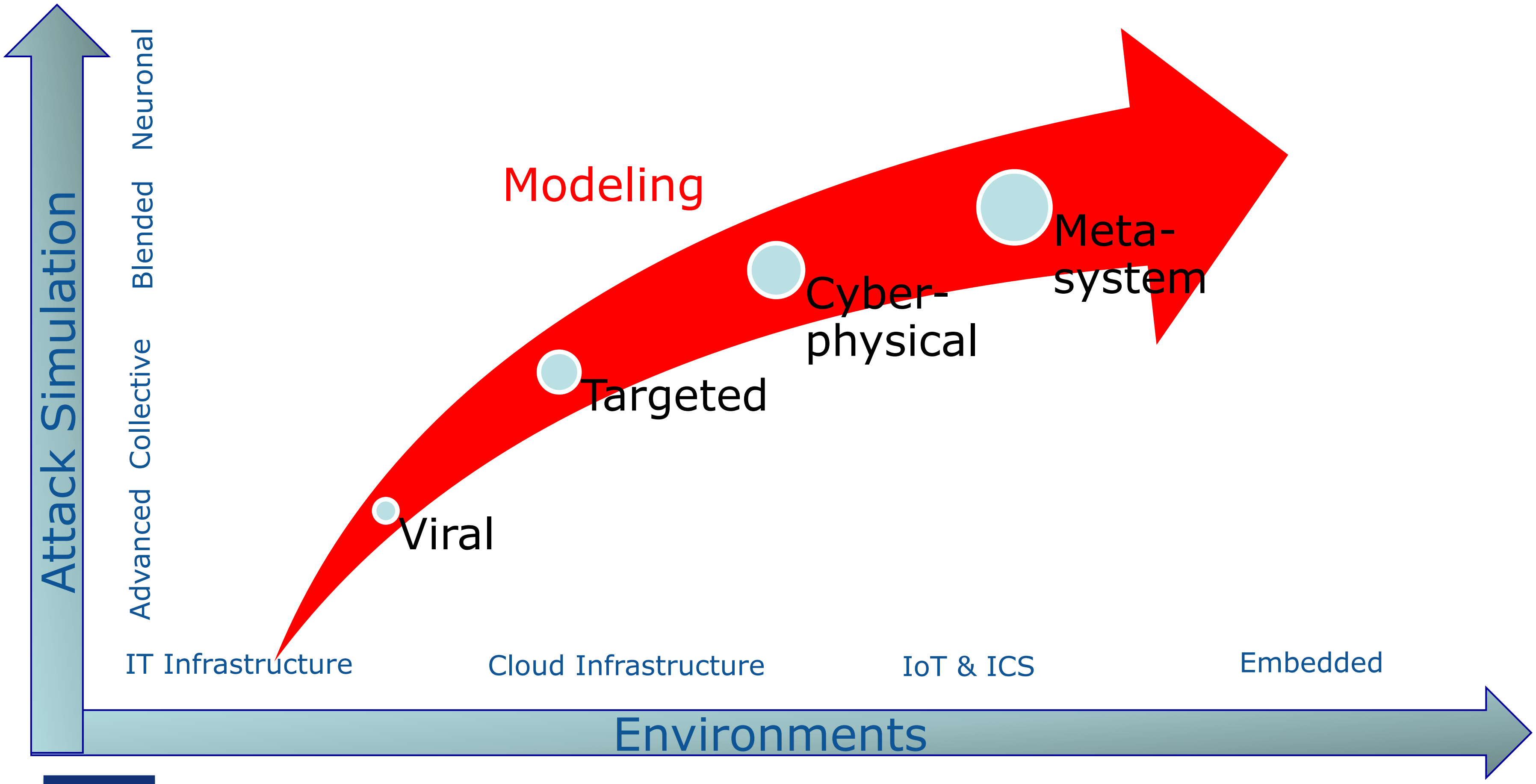
DS7-IA: Open Source Cyber-security Training Platform – Project Idea



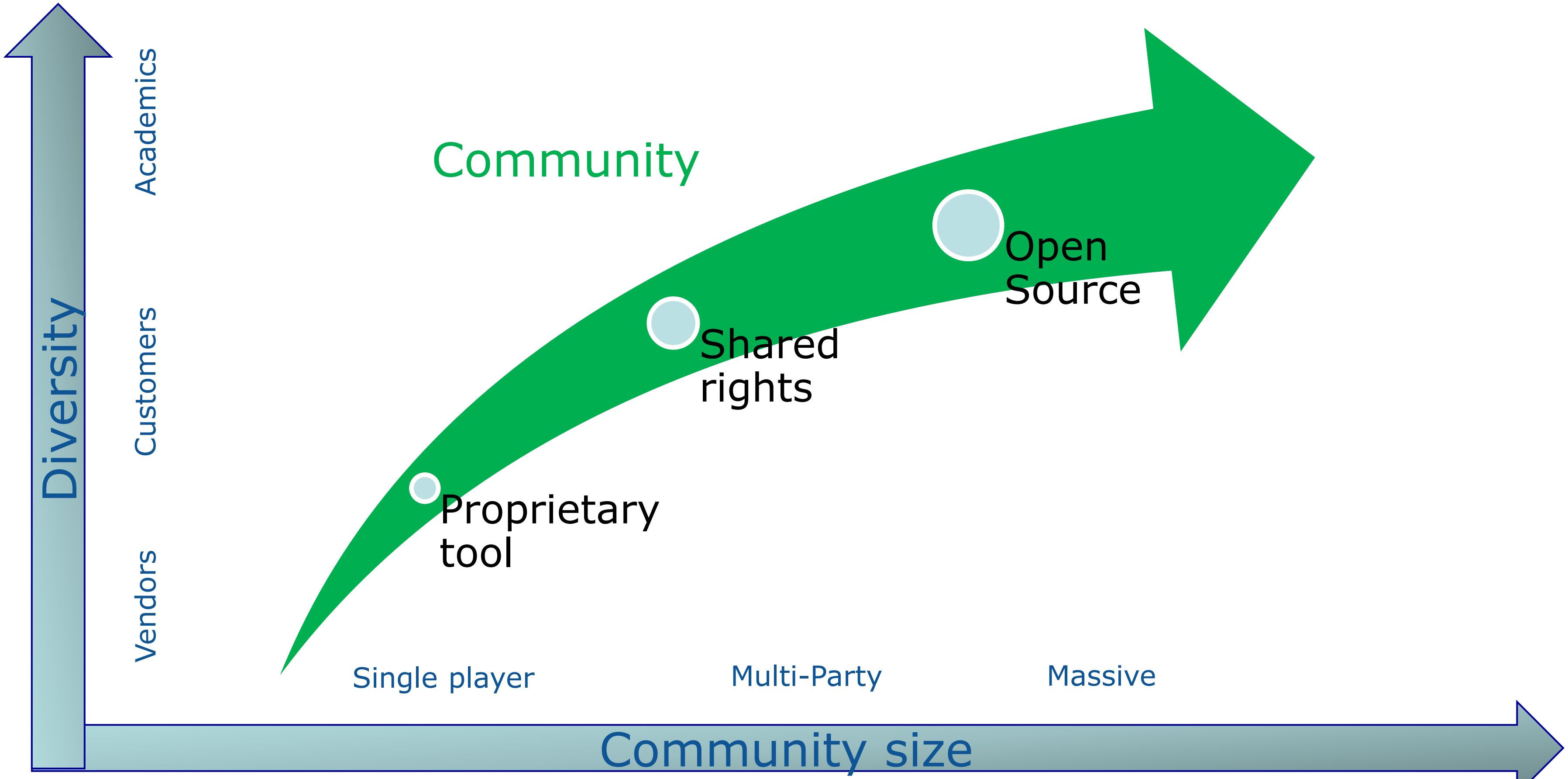
TRUSTED OPEN SOURCE COMMUNITY

CyberRange Customers

DS7-IA- Modeling challenge



DS7-RIA-Community Challenge



DS7-IA-Consortium Building

Existing partners:

-Airbus DS Cybersecurity (FR)

-Institut Mines Telecom (FR)

Looking for:

-End-users and practitioners (public/private)

-Traffic injection equipment vendors

-Cybersecurity academic actors

-Cybersecurity training centers

-Virtualization software editors

-Security software editors