



D2.2 Cybersecurity technology radar 1st Report Autumn 2018

| | |
|-----------|-------------------------------|
| Author(s) | D. Wallom & M. Drescher, UOXF |
| Status | Final |
| Version | V1.0 |
| Date | 4 Dec 2018 |

Dissemination Level

- PU: Public
 PP: Restricted to other programme participants (including the Commission)
 RE: Restricted to a group specified by the consortium (including the Commission)
 CO: Confidential, only for members of the consortium (including the Commission)

Abstract:

We present in this report a visualisation of EC supported activities in the area of Cybersecurity and Privacy that allows possible exploiters of the outputs of these projects to understand their status.



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

| | |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------|
| Document identifier: Cyberwatching.eu – WP2 – D2.2 | |
| Deliverable lead | UOXF |
| Related work package | WP2 |
| Author(s) | D. Wallom & M. Drescher, UOXF |
| Contributor(s) | - |
| Due date | 31 October 2018 |
| Actual submission date | 4 December 2018 |
| Reviewed by | Nicholas Ferguson, Trust-IT Marina Ramírez, Cristina Carmona (CITIC), |
| Start date of Project | 01/05/2017 |
| Duration | 48 months |

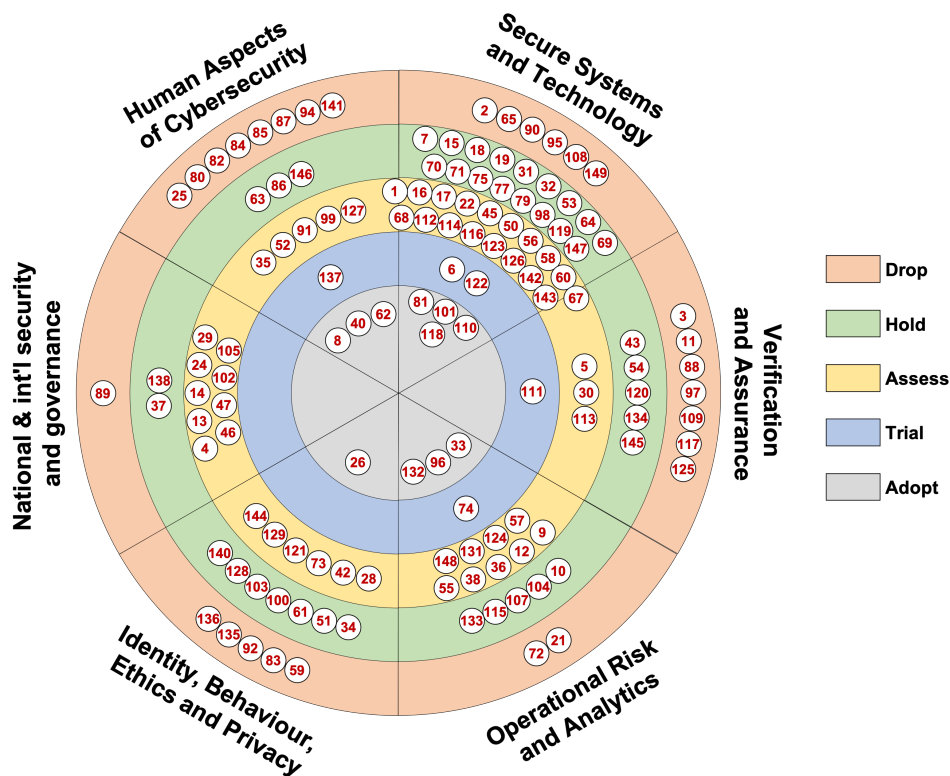
Revision history

| Version | Date | Authors | Notes |
|---------|------------|------------------------------------------------------------------------------|--------------------------------------------------------|
| 0.1 | 1/10/2018 | M Drescher (UOXF) | Core structure of the document agreed |
| 0.2 | 12/10/2018 | M Drescher (UOXF) | First stakes of content provided |
| 0.3 | 7/11/18 | D Wallom & M Drescher (UOXF) | First draft completed |
| 0.4 | 7/11/18 | M Drescher (UOXF) | First full OeRC draft review |
| 0.5 | 7/11/18 | D Wallom (UOXF) | Version submitted for internal Cyberwatching.eu review |
| 0.6 | 8/11/2018 | M. Ramírez, C. Carmona (CITIC), M. Miller (CPT) N. Ferguson (Trust-IT) | Internal review |
| 0.7 | 28/11/18 | D. Wallom, M. Drescher (UOXF) | Response to internal review. |
| 1.0 | 4/12/2018 | D. Wallom, M. Drescher (UOXF), N. Ferguson (Trust-IT) | Final |

Executive Summary

The European Commission has launched 25 calls which were either explicitly supporting projects in the domain of Cybersecurity and privacy or from which projects in this area were supported. As such it is important that we consider what the outputs of these projects have been and where the products they have created have gone in terms of exploitation either by the projects themselves or by others who may reuse their outputs.

Utilising the fairly well known “Technology Radar” methodology the Cyberwatching.eu project used its previously published Cybersecurity taxonomy and a schema that describes guidance on whether a user should invest themselves in the outputs of a project, to produce the radar visualisation as below.



Overall, we can see from this that there is still an imbalance in the domains within which projects have been supported by the EC, with a concentration in the Secure Systems and Technology segment. This is possibly not surprising, as this is still what the majority would consider in need of further development in the area of CS&P.

Unfortunately, another equally important segment, yet not nearly as high profile is one of the most lowly represented: Verification and Assurance. As such, supporting this more explicitly in a future funding round could be necessary.

Analysing the status within the rings, we can see that there are a significant number of projects that are currently at the point of assessment (yellow ring), again led by Secure Systems and Technology though this is the most populated ring for nearly all sectors. A possible concern is that there are no products or outputs in two of the sectors, National and International Security & Governance and Verification & Assurance where all of the activities are either relatively new or have already completed.

Overall, we consider this first version of the Technology Radar as a working document, which will develop with further releases, integrating product trajectories in future versions.

Table of Contents

| | | |
|----------|-------------------------------------------------------|-----------|
| 1 | Introduction | 5 |
| 2 | Methodology | 6 |
| 2.1 | Sectors | 6 |
| 2.2 | Technology Radar rings | 8 |
| 3 | The analysed projects | 11 |
| 4 | The Autumn 2018 Technology Radar | 12 |
| 4.1 | Results by sector | 12 |
| 4.2 | The Autumn 2018 Technology Radar | 20 |
| 5 | Commentary & next steps | 21 |
| 6 | Appendix 1: EC funded projects reference | 22 |

LIST OF FIGURES

| | | |
|------------|-------------------------------------------------------------------------|----|
| Figure 1: | Maturity progression of cybersecurity projects | 8 |
| Figure 2: | Attention level required for project maturity levels | 9 |
| Figure 3: | Mechanics of the technology radar | 9 |
| Figure 4: | “Secure Systems and Technology” radar | 13 |
| Figure 5: | “Verification and Assurance” radar | 15 |
| Figure 6: | “Operational Risk, Management and Analytics” radar | 16 |
| Figure 7: | “Identity, Behaviour, Ethics and Privacy” radar | 17 |
| Figure 8: | “National & international Security, Privacy and Governance” radar | 18 |
| Figure 9: | “Human Aspects of Cybersecurity” radar | 19 |
| Figure 10: | The Autumn 2018 Technology Radar | 21 |

LIST OF TABLES

| | | |
|-----------|----------------------------------------------------------------------------|----|
| Table 1: | “Secure Systems and Technology” overview | 12 |
| Table 2: | “Secure systems and Technology” details | 14 |
| Table 3: | “Verification and Assurance” overview | 14 |
| Table 4: | “Verification and Assurance” details | 15 |
| Table 5: | “Operational Risk, Management and Analytics” overview | 15 |
| Table 6: | “Operational Risk, Management and Analytics” details | 16 |
| Table 7: | “Identity, Behaviour, Ethics and Privacy” overview | 17 |
| Table 8: | “Identity, Behaviour, Ethics and Privacy” details | 18 |
| Table 9: | “National & international Security, Privacy and Governance” overview | 18 |
| Table 10: | “National & international Security, Privacy and Governance” details | 19 |
| Table 11: | “Human Aspects of Cybersecurity” overview | 19 |
| Table 12: | “Human Aspects of Cybersecurity” details | 20 |
| Table 13: | Autumn 2018 Technology Radar overview | 20 |

1 Introduction

A large number of substantial investments have been made by both national governments and the European Commission to support co-ordinated programmes of research and innovation projects within the broad domain of cybersecurity and privacy. Since some of these programmes have now completed and as the European Commission has transitioned from Framework 7 to Horizon 2020, it is important that we are able to evaluate the impact that these programmes have had, and more specifically, how ready the outputs are for utilisation by persons from outside the developing community. As such, in an area such as Cybersecurity it is essential that we are able to consider and present to stakeholders in these enterprises (potential users of the technologies, processes and policies developed) the outputs from the projects alongside a systematic method of the evaluation of the outputs, with commentary on how easy these outputs are to use both generally and more importantly, outside of the team that originally developed them.

The method chosen to present the evaluations of the project outputs has been determined to be a type of technology radar, as pioneered by ThoughtWorks¹. This methodology allows not only the subdivision of the items classified to be segmented depending on specific criteria, but also their radial distance from the centre allows a second classification to be presented simultaneously. Through the use of colour for the points rather than the rings within the radar we are able to support a third dimension of assessment for featured project outputs, which future versions of the Cyberwatching.EU Cybersecurity R&I technology Radar will exploit.

As this is the first Cyberwatching.eu Cybersecurity Technology Radar report (with future versions published at M36 and M48 of the project), we will be concentrating at this point on the projects supported by the European Commission. Projects supported through national governments will appear in future releases of the technology radar. Since this is the first edition of the technology radar, this release will not include illustration of trajectory of products and outcomes. These result in a track being established for a particular item within the radar, which can then be used to identify trends and predict the next position of an item in the short to medium term. This track and prediction indicate which tools, productions or services are becoming mature, commercially viable etc. This information will appear for the first time in the next edition.

Following this section, we first describe the assessment methodology used to understand the current status of the projects. This is especially important as it would not be feasible within the confines of this first edition of the radar to ask assessed projects to self-evaluate, or for us to personally walk them through in a more hands-on approach. We then describe the segmentation radially into the different sectors of the cyberwatching.eu taxonomy that was introduced previously in deliverable D2.1. Next, we explain the meaning for the different radial bands which assess project output suitability for external usage. For this first edition, we are utilising the current status of the project itself and then if necessary, the time since or towards project completion as the key assessment within this edition of the Radar. In future editions we will utilise the output from the assessment methodology of the Market and technology Readiness Levels as described within the Cyberwatching.eu deliverable D2.3.

¹ <https://www.thoughtworks.com/radar>

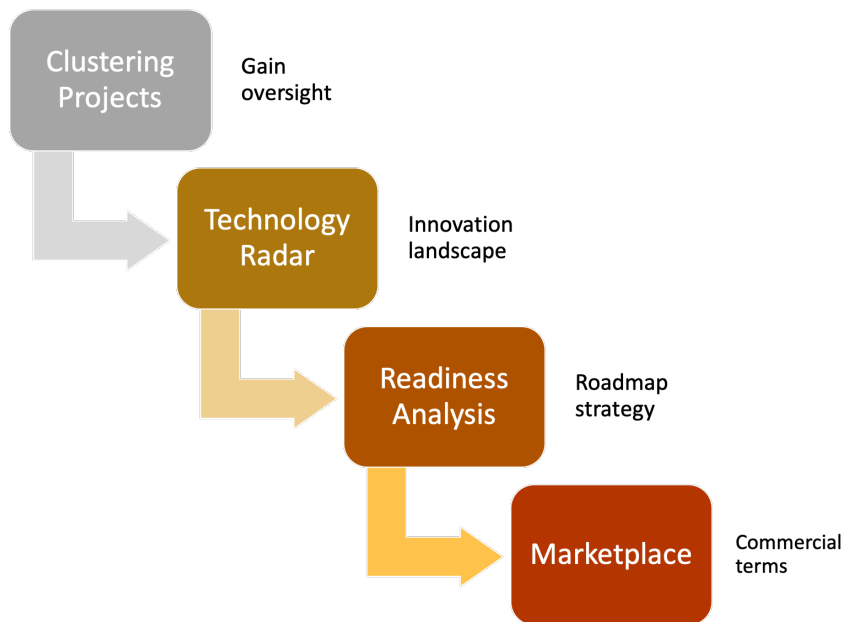


Figure 1: How WP2 tasks feed into each other and, ultimately, into WP4's marketplace

We then present all of the projects that have been assessed within this edition of the radar, which is followed by the radar presentation itself.

The document concludes with a discussion about an overall larger pan-project conclusions that this visualisation is able to give us. It also identifies the impact of the findings in the broader scope of the project and in particular on the promotion of projects through the SME end-user club and Marketplace.

2 Methodology

The Technology Radar as a tool requires a descriptive taxonomy of general areas within a specific domain, and a schema that describes the relationship between the object and its position within the domain sector and the distance from the centre for the visualisation that is used.

In the following sections both of these are described, starting with the taxonomy of domains and then the actual schema and application of the Technology Radar to the cybersecurity domain.

2.1 Sectors

Within the Cyberwatching Technology Radar there are six sectors as described by the six L2 categories of the Cyberwatching taxonomy of R&I in cybersecurity and privacy. These are summarised below for completeness of this deliverable –the full definition and description are found in deliverable D2.1.

2.1.1 Level 1 Taxonomy

The first sub division of the cybersecurity and privacy landscape is done at the highest level possible into three categories;

- **Foundational technical methods & risk management for trustworthy systems in cybersecurity and privacy** – The development of technologies that are directly associated with cybersecurity capabilities or features and methods by which the confidence in the technical capabilities of a system may be validated.

- **Applications and user-oriented services to support cybersecurity and privacy** – Specific capabilities or services which directly interact with system users and are developed with capabilities that are directly about how to improve the inherent capabilities and user experiences of cybersecurity and privacy in consumed services.
- **Policy, governance, ethics, trust, and usability, human aspects of cyber security & privacy** – Aspects of cyber security that are overwhelmingly driven by the human interaction, understanding and dependency on how secure systems are or have been designed to be.

From these three top-level categories we then subdivide into the next level for the taxonomy.

2.1.2 Level 2 Taxonomy

The six sub domains listed below are intended to describe a specific sub area within cybersecurity research and innovation. The individual sectors are listed below along with their parent Level 1 categories.

- **Foundational technical methods & risk management for trustworthy systems in cybersecurity and privacy**
 - **Operational risk, management and analytics:** Understanding the risk and harm resulting from cyberattacks, and how it propagates across and between organisations. Work focuses on creating situational awareness through aiming for a complete understanding of scenario and risk management; metrics and models for security postures; and analytics for predicting risk, prioritising responses and supporting security operations.
 - **Verification and assurance:** Two disciplines that help establish how much confidence you can have in a system, both in terms of security and the privacy of all stakeholder groups who act with or in a system. Assurance focuses on managing risks related to the use, processing, storage, and transmission of information, whereas formal verification seeks to build a mathematical model of a digital system and then try to prove whether it is 'correct', often helping to find subtle flaws.
- **Applications and user-oriented services to support cybersecurity and privacy**
 - **Secure systems and technology:** How security can be built into technology from the design stage including cloud computing security, cryptography, trusted platforms, wireless security, mobile security and secure coding paradigms.
 - **Identity, behaviour, ethics and Privacy:** Bringing diverse perspectives and interpretations to questions such as: Who are you online, how do you communicate, and what can (or should) you do? This also connects to the ongoing activities on Privacy launched through directives and regulations over the past year.
- **Policy, governance, ethics, trust, and usability, human aspects of cyber security & privacy**
 - **National and international security, privacy and governance:** looking at politics, international relations, defence, policy and governance issues: how do countries and communities interact with (and through) technology, and how might this change in different contexts?
 - **Human aspects of cyber security:** Understanding the ways humans interact with (and through) digital systems – whether to understand and design for target users, or to understand how adversaries operate and can exploit the systems. This includes aspects like usability, trust, collaborative practices, social embeddedness, nationhood, cultural diversity, impact on economy, and the relationship between microsocial interactions and global structures.

2.2 Technology Radar rings

Categorising data blips into sectors/segments (see section 2.1 for more detail) provides a *static* grouping of European and national cybersecurity for easy and swift drill-down into the data.

Assessing cybersecurity projects according to maturity allows the reader to make an informed decision as to where and when the project in question should be closer examined, or not examined at all.

This section describes this Technology Radar's *rings* and the state of maturity they capture for every project included in section 4.

2.2.1 Underlying concepts

As any visualisation technique, this Technology Radar relies on applying a number of design principles to the data in order to provide an intuitive reader experience. Combined with an easy to understand way of charging values with expressive yet generic semantics, the results allow for swift conveying on large amounts of information.

Software Development Lifecycle as project maturity metaphor.

The Software Development Life Cycle (SDLC) is a well-known concept capturing the life cycle of any software project, from idea to 'sunsetting', i.e. the discontinuation or retiring a solution, a service, a library, basically any piece of software. The SDLC is comparable to many different concepts; for example, the progression through the SDLC is closely resembling the ascension through the Technology Readiness Levels (TRL) that are ubiquitous in the technology and engineering sectors. (With the exception that TRLs do not capture the concept of sunsetting a piece of software.)

Therefore, mapping the Technology Radar's *rings*, or states to the SDLC, software, or knowledge in this deliverable's context, would undergo the following sequence of assessment:

Assess → Trial → Adopt → Hold → Drop

Figure 2: Maturity progression of cybersecurity projects

The semantics of these terms are described in section 2.2.2.

Proximity to radar's centre reflects readiness for adoption.

A straight mapping of the project maturity on the rings of the radar would be counter-intuitive to the visual message of the radar where the very centre of the radar requires the most attention, the outermost ring the least attention. By contrast, the level of attention to the software maturity levels peaks with "Adopt", and dropping to lower levels at either side of it – not dissimilar to the bell curve:

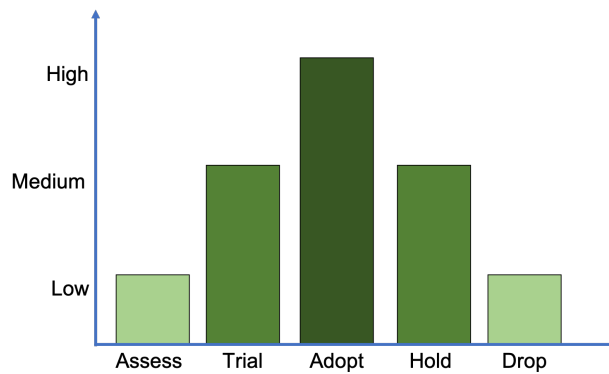


Figure 3: Attention level required for software project maturity levels

Consequently, projects will progress through the radar not in a linear succession from outermost rings towards the centre. Instead, they will “enter” the radar in the middle, gravitate to the centre (the bull’s eye), then jump to the outermost rings for gradually dropping out of scope of the radar altogether:

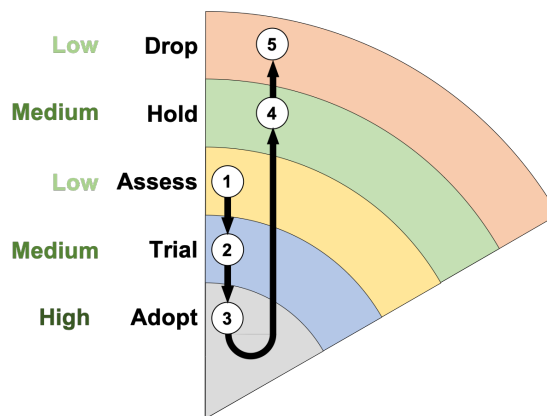


Figure 4: Mechanics of the technology radar

2.2.2 Project maturity: The rings of the radar

The rather generic terms that qualify the rings of the radar need to be further contextualised towards the overall purpose of the radar. In *this* instalment of the Technology Radar report, the focus lies on the introduction of the radar, how it works, and what kind of insights it may deliver.

This first Technology Radar focuses on project maturity based on its contractual timeline, relative to the point in time the report was created. It assumes that projects generally progress satisfactorily towards their goals and outcomes – it relies on this being ensured by the funding programme’s own checks and balances. In the case of EU H2020, these are the regular project reviews, and the selection of expert reviewers for the project by the Commission.

This Technology Radar report addresses the following question, therefore: “Given the current landscape and oversight of projects addressing various aspects of cybersecurity, at which point in time should I start tracking their results and reports?”

1. Assess

Technical criterion: Project is running, and has **more than 6 months to go**.

The project is still running, and has still a considerable amount of time to further mature their results and outputs, yet needs to think about how it will play out the final stretch of project lifetime.

Recommendation: Study the project's high-level description and designated outputs, and compare with your own strategy and needs. If there is a match, put the project on a personal/specific short-list for further check-up later.

2. Trial

Technical criterion: Project is running, but has **less than 6 months to go**.

The project is now seriously busy finalising its planned outputs. That might be a piece of software, an innovative algorithm, or a study whose results may impact your own work. Some of the planned work might have been dropped in order to reach the stated goal for more important outputs.

Recommendation: Check back regularly with the project (either actively or passively) to see how the output you are interested in is progressing. Refine your shortlist based on the results of that exercise; expect your shortlist getting smaller unless there are new projects in the pipeline that stock it up again. For those you consider specifically mature, you should consider first practical trials of integrating the output into your portfolio – not to accomplish it straight away, but to anticipate the level of “integration pain” you may experience later.

3. Adopt

Technical criterion: The project finished **less than 1 year ago**.

The project has finished and published its results and outputs. However, intended follow-on activities may have not yet ramped up, or in case of open source software the intended community around it has not yet formed and you are not prepared to be a first mover in that space. In any case, project outputs are usually considered stable and the focus of uptake into production. There may be further changes to it, especially with active communities supporting it, but expect at least a temporary significant drop in speed of change in this timeframe.

Recommendation: For projects that stayed on your shortlist unto this stage, this is the time to start serious integration trials with stable versions of the output. In case of study results, or non-IT related outputs, the expected integration pain may affect your overall business strategy and cause changes in operations and processes, rather than technical integration challenges that present themselves with IT integrations.

4. Hold

Technical criterion: The project finished **1 – 2 years ago**.

If you haven't already decided to integrate the project's outputs into your own business, or more neutrally, operations at large, projects in this “stage” may still have value to you, but you need to understand the how the then published outputs have fared until now and may fare in the future.

Project results in the IT sector, and especially in the currently very dynamic cybersecurity domain age very quickly, as competition is fierce, and many outputs are superseded by technical innovation, or other projects simply having been faster or more efficient in their execution.

Recommendation: Look out for the support infrastructure and community for the outputs of that project. Is alive and active? Is it expanding or contracting? As far as concepts and new knowledge is concerned, how well are outputs from about 2 years ago still valid? Be very sure about the impact and skills required when deciding to integrate outputs of that age.

5. Drop

Technical criterion: The project finished **more than 2 years ago**.

The project has seen its sunset quite a while ago. At this point in time, you will know whether its outputs have succeeded or not. If it did, then it is usually disassociated from the original project and has formed a life and purpose of its own, and you can focus on the software, hardware, knowledge, or insight itself.

As far as tracking and collecting project related information, it is safe to consign it to the long-term archives.

Recommendation: For all intents and purposes, projects at this stage are safe to discard from your attention.

3 The analysed projects

In order to obtain a first representative sample of projects to be assessed in this Technology Radar, we collected projects funded in 25 calls across the EU's major recent research and innovation programmes, i.e. FP7 and H2020, that address cybersecurity in their DoAs. These calls are, in alphabetical order:

- DRS-17-2014
- DS-02-2016
- ECSEL-2016-2-IA-two-stage
- EE-13-2014
- EINFRA-22-2016
- ERC-CoG-2014
- FCT-09-2015
- FP7-PEOPLE-2011-IOF
- H2020-SMEINST-1-2016-2017
- ICT-06-2016
- ICT-10-2016
- ICT-12-2015
- ICT-2009.1.4
- ICT-2013.6.1
- ICT-32-2014
- ICT-37-2014-1
- INNOSUP-02-2016
- MSCA-ITN-2014-ETN
- PEOPLE-2007-4-3.IRG
- SEC-2011.2.5-1
- SEC-2011.6.1-5
- SEC-2011.6.5-2
- SEC-2012.2.3-1
- SiS-2009-1.1.2.1
- SSH-2009-3.2.1

For the purpose of this technology radar, from the total of 149 projects (see Appendix 1), 15 project were considered out of scope since they incorporate other projects' cybersecurity outcomes rather than offer research and innovation as a project goal in its own right. The remaining 134 EC-funded projects are included in this radar, and are also part of the observatory, which contains a further 85 nationally-funded projects. .

In this deliverable, only EC funded cybersecurity projects have been analysed.

The process of selecting and filtering EC funded projects was a four-step process:

1. Collection of key project data, such as start and end date, budget, call, project type (Research & Innovation Action, Innovation Action, Coordination & Support Action, etc.) coordinator, and high-level project descriptions.

2. Assessment of whether each project in fact does address aspects of cybersecurity directly or merely acts as a consumer of outputs of cybersecurity tools and knowledge. Projects of the latter categorisation were discarded from further analysis, in total 15 projects of the 149 originally collected. 134 projects remained.
3. Grouped projects according to the cyberwatching cybersecurity research taxonomy level 1 domains (see Cyberwatching.eu deliverable D2.1 for details)
4. Clustered projects in our research taxonomy level 2 (and as summarised in section 2.1 earlier in this deliverable)

Once this final list of 134 projects was determined, we applied the methodology described above, arriving at the results provided in section 4 below.

4 The Autumn 2018 Technology Radar

We now present the results of the Radar analysis, initially on a sector by sector basis and then finally bringing them all together to also see the shape of the overall landscape.

4.1 Results by sector

4.1.1 Secure Systems and Technology

| # projects | Assess | Trial | Adopt | Hold | Drop |
|------------|--------|-------|-------|------|------|
| 47 | 18 | 2 | 4 | 17 | 6 |

Table 1: “Secure Systems and Technology” overview

“Secure systems and technology” is understandably the most popular area within the cybersecurity and privacy ecosystem, since it is what most would consider the front line in protecting resources, to develop new technological solutions to what can be a technology driven problem.

This includes a large number of projects that have recently started and a smaller number that are more mature within the software development lifecycle. Indeed, these are all at the Trial or Adopt stage. There are also a large number of projects that have already come to the end of their development lifecycle having ended already. In some cases, the technologies implemented are likely to have been superseded by outputs from more latterly funded activities.

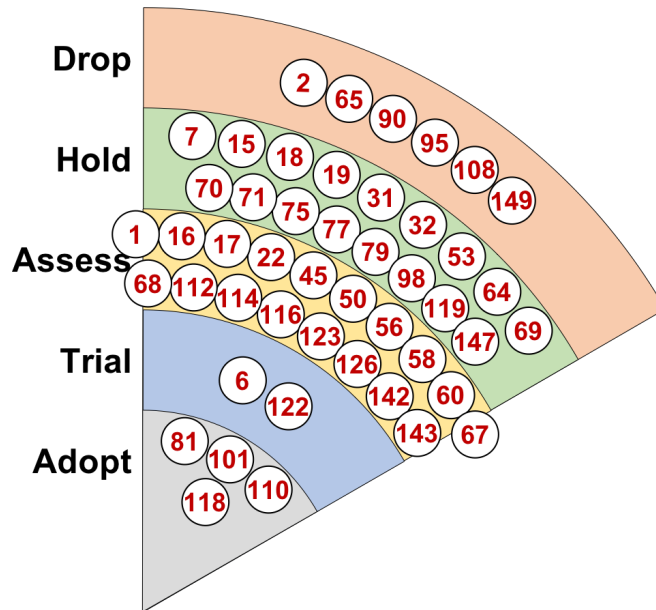


Figure 5: “Secure Systems and Technology” radar

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|----|-------------------|------------|----------|--------|-------|-------|------|------|
| 1 | AARC2 | May 2017 | Apr 2019 | X | | | | |
| 2 | ABC4Trust (F) | Nov 2010 | Feb 2015 | | | | | X |
| 6 | ARIES | Sep 2016 | Feb 2019 | | X | | | |
| 7 | ARMOUR (F) | Feb 2016 | Jan 2018 | | | | X | |
| 15 | CHOReVOLUTION (F) | Jan 2015 | Dec 2017 | | | | X | |
| 16 | CIPSEC | May 2016 | Apr 2019 | X | | | | |
| 17 | CITADEL | Jun 2016 | May 2019 | X | | | | |
| 18 | CLARUS (F) | Jan 2015 | Dec 2017 | | | | X | |
| 19 | CloudSocket (F) | Jan 2015 | Dec 2017 | | | | X | |
| 22 | COEMS | Nov 2016 | Oct 2019 | X | | | | |
| 31 | CyberWiz (F) | Sep 2015 | Aug 2017 | | | | X | |
| 32 | CYCLONE (F) | Jan 2015 | Dec 2017 | | | | X | |
| 45 | ENCASE | Jan 2016 | Dec 2019 | X | | | | |
| 50 | FutureTrust | Jun 2016 | May 2019 | X | | | | |
| 53 | HEAT (F) | Jan 2015 | Dec 2017 | | | | X | |
| 56 | HIPS | Oct 2014 | Sep 2019 | X | | | | |
| 58 | KONFIDO | Nov 2016 | Oct 2019 | X | | | | |
| 60 | LIGHTest | Sep 2016 | Aug 2019 | X | | | | |
| 64 | MAS2TERING (F) | Sep 2014 | Aug 2017 | | | | X | |
| 65 | MATTHEW (F) | Nov 2013 | Oct 2016 | | | | | X |
| 67 | mF2C | Jan 2017 | Dec 2019 | X | | | | |
| 68 | MH-MD | Nov 2016 | Oct 2019 | X | | | | |
| 69 | MIKELANGELO (F) | Jan 2015 | Dec 2017 | | | | X | |
| 70 | MITIGATE (F) | Sep 2015 | Feb 2018 | | | | X | |
| 71 | MUSA (F) | Jan 2015 | Dec 2017 | | | | X | |
| 75 | OCTAVE (F) | Jun 2015 | Jul 2017 | | | | X | |
| 77 | OPERANDO (F) | May 2015 | Apr 2018 | | | | X | |
| 79 | PaaSword (F) | Jan 2015 | Dec 2017 | | | | X | |

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|-----------------|------------|----------|--------|-------|-------|------|------|
| 81 | PANORAMIX (F) | Sep 2015 | Aug 2018 | | | X | | |
| 90 | PreserviX | May 2015 | Oct 2015 | | | | | X |
| 95 | PRISM CODE | Nov 2012 | Oct 2016 | | | | | X |
| 98 | PRIVACY FLAG | May 2015 | Apr 2018 | | | | X | |
| 101 | ProBOS | Oct 2016 | Sep 2018 | | | X | | |
| 108 | RESPECT | Feb 2012 | May 2015 | | | | | X |
| 110 | SafeCloud | Sep 2015 | Aug 2018 | | | X | | |
| 112 | SAFERtec | Jan 2017 | Dec 2019 | X | | | | |
| 114 | SAURON | May 2017 | Apr 2019 | X | | | | |
| 116 | SCOTT | May 2017 | Jun 2020 | X | | | | |
| 118 | SecIoT | Sep 2017 | Aug 2018 | | | X | | |
| 119 | SERECA | Mar 2015 | Feb 2018 | | | | X | |
| 122 | SHIELD | Sep 2016 | Feb 2019 | | X | | | |
| 123 | SISSDEN | May 2016 | Apr 2019 | X | | | | |
| 126 | SODA | Jan 2017 | Dec 2019 | X | | | | |
| 142 | UNICORN | Jan 2017 | Dec 2019 | X | | | | |
| 143 | VESSEDIA | Jan 2017 | Dec 2019 | X | | | | |
| 147 | WITDOM | Jan 2015 | Dec 2017 | | | | X | |
| 149 | SAWSOC | Jan 2014 | Dec 2016 | | | | | X |

Table 2: “Secure systems and Technology” details.
(F) indicates projects having ended at the time of writing.

4.1.2 Verification and Assurance

| # projects | Assess | Trial | Adopt | Hold | Drop |
|------------|--------|-------|-------|------|------|
| 16 | 2 | 2 | 0 | 5 | 7 |

Table 3: “Verification and Assurance” overview

This area is significantly smaller in terms of population than nearly every other sector. It is also one where the majority of the projects assessed have already ended. A small number of projects have started but are still very early in their development lifecycles. As such and understanding the importance of this area, it would appear that this is an area ripe for further support, and also where there may be gaps in the future that will need filling.

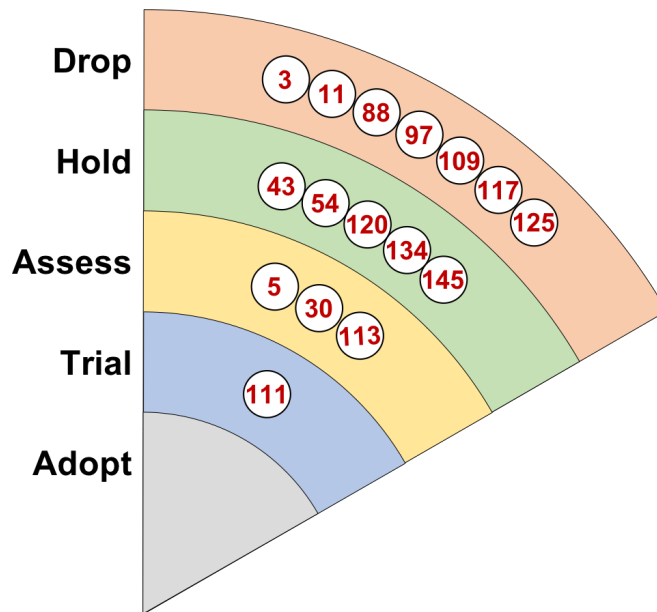


Figure 6: “Verification and Assurance” radar

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|-----------------|------------|----------|--------|-------|-------|------|------|
| 3 | ADDPRIV (F) | Feb 2011 | Mar 2014 | | | | | X |
| 5 | ANASTACIA | Jan 2017 | Dec 2019 | X | | | | |
| 11 | BIOSEC (F) | Mar 2009 | Feb 2012 | | | | | X |
| 30 | CYBECO | May 2017 | Apr 2019 | X | | | | |
| 43 | ECRYPT-CSA (F) | Mar 2015 | Feb 2018 | | | | X | |
| 54 | HECTOR (F) | Mar 2015 | Feb 2018 | | | | X | |
| 88 | PRECIOSA | Mar 2008 | Aug 2010 | | | | | X |
| 97 | PRISMS | Feb 2012 | Jul 2015 | | | | | X |
| 109 | REVEN-X1 | Jul 2015 | Dec 2015 | | | | | X |
| 111 | SAFEcrypto | Jan 2015 | Dec 2018 | | X | | | |
| 113 | SAINT | Mar 2017 | Feb 2021 | X | | | | |
| 117 | SCR | Jul 2016 | Dec 2016 | | | | | X |
| 120 | SHARCS | Jan 2015 | Dec 2017 | | | | X | |
| 125 | SocialPrivacy | Sep 2012 | Aug 2015 | | | | | X |
| 134 | SUPERCLOUD | Feb 2015 | Jan 2018 | | | | X | |
| 145 | VisiOn | Jul 2015 | Jun 2017 | | | | X | |

Table 4: “Verification and Assurance” details.
(F) indicates projects having ended at the time of writing.

4.1.3 Operational Risk, Management and Analytics

| # projects | Assess | Trial | Adopt | Hold | Drop |
|------------|--------|-------|-------|------|------|
| 20 | 9 | 1 | 3 | 5 | 2 |

Table 5: “Operational Risk, Management and Analytics” overview

From the current distribution of projects within this sector we can see that there have been recent funding decisions made to support projects in this area at a much larger

scale than those projects that went before in this sector. There are a small number of mature project outputs that we consider sit well within the adopt domain. There has also been previous support in this area which has come to an end, the outputs of which in the Hold domain would need careful investigation due to a no longer being actively developed due to project closure.

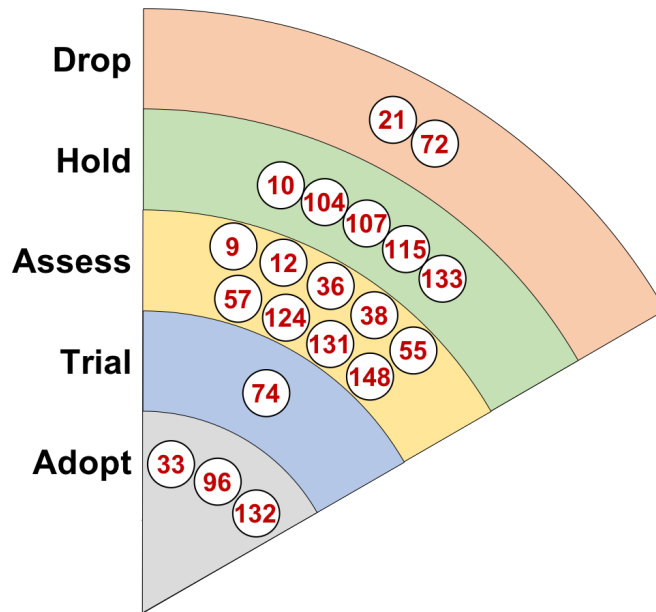


Figure 7: “Operational Risk, Management and Analytics” radar

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|-----------------|------------|----------|--------|-------|-------|------|------|
| 9 | ATENA | May 2016 | Apr 2019 | X | | | | |
| 10 | BEACON (F) | Feb 2015 | Jul 2017 | | | | X | |
| 12 | C3ISP | Oct 2016 | Sep 2019 | X | | | | |
| 21 | COCKPITCI (F) | Jan 2012 | Dec 2014 | | | | | X |
| 33 | CYRail (F) | Oct 2016 | Sep 2018 | | | X | | |
| 36 | DEFENDER | May 2017 | Apr 2020 | X | | | | |
| 38 | DiSIEM | Sep 2016 | Aug 2019 | X | | | | |
| 55 | HERMENEUT | May 2017 | Apr 2019 | X | | | | |
| 57 | IMPACT | Feb 2015 | Jan 2021 | X | | | | |
| 72 | NECOMA (F) | Jun 2013 | Mar 2016 | | | | | X |
| 74 | OCGN | May 2017 | Nov 2018 | | X | | | |
| 96 | PRISMACLOUD | Feb 2015 | Jul 2018 | | | X | | |
| 104 | RAPID | Jan 2015 | Dec 2017 | | | | X | |
| 107 | REDSENTRY | Jul 2017 | Dec 2017 | | | | X | |
| 115 | SCISSOR | Jan 2015 | Dec 2017 | | | | X | |
| 124 | SMESEC | Jun 2017 | May 2020 | X | | | | |
| 131 | STOP-IT | Jun 2017 | May 2021 | X | | | | |
| 132 | STORM | Mar 2015 | Aug 2018 | | | X | | |
| 133 | SUNFISH | Jan 2015 | Dec 2017 | | | | X | |
| 148 | FENTEC | Jan 2018 | Dec 2020 | X | | | | |

Table 6: “Operational Risk, Management and Analytics” details.
(F) indicates projects having ended at the time of writing.

4.1.4 Identity, Behaviour, Ethics and Privacy

| # projects | Assess | Trial | Adopt | Hold | Drop |
|------------|--------|-------|-------|------|------|
| 19 | 6 | | 1 | 7 | 5 |

Table 7: “Identity, Behaviour, Ethics and Privacy” overview

This sector is another that is significantly under populated when compared to others. It also has a large proportion of its projects either recently underway and therefore with immature outputs or that have already completed and therefore will not be developed further or have even been superseded already. From the distribution within the sector it is clear though that in the past this has been strongly supported but then left for a while and has become important again, most likely in response to the general increase in importance in personal privacy.

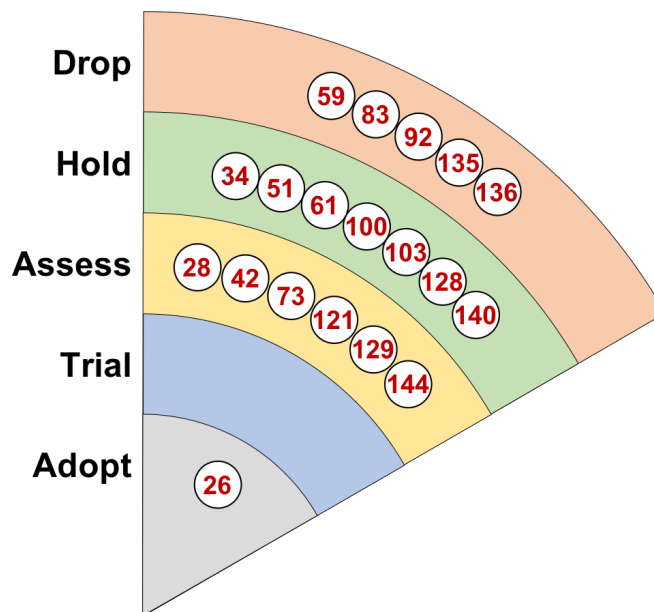


Figure 8: “Identity, Behaviour, Ethics and Privacy” radar

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|-------------------|------------|----------|--------|-------|-------|------|------|
| 26 | CREDENTIAL (F) | Oct 2015 | Sep 2018 | | | X | | |
| 28 | CryptoCloud | Jun 2014 | May 2019 | X | | | | |
| 34 | DAPPER (F) | Apr 2014 | Mar 2018 | | | | X | |
| 42 | e-Sides | Jan 2017 | Dec 2019 | X | | | | |
| 51 | GenoPri (F) | May 2016 | Apr 2018 | | | | X | |
| 59 | LAST (F) | Oct 2009 | Sep 2014 | | | | | X |
| 61 | LV-Pri20 (F) | Jun 2015 | Jun 2017 | | | | X | |
| 73 | NeCS | Sep 2015 | Aug 2019 | X | | | | |
| 83 | PASS (F) | Dec 2008 | Nov 2012 | | | | | X |
| 92 | PrimeLife | Mar 2008 | Jun 2011 | | | | | X |
| 100 | PRIVACY4FORENSICS | Feb 2015 | Mar 2018 | | | | X | |
| 103 | Ps2Share | Jan 2017 | Dec 2017 | | | | X | |
| 121 | SHIELD | Jan 2017 | Dec 2019 | X | | | | |
| 128 | SpeechXRays | May 2015 | Apr 2018 | | | | X | |
| 129 | SPOOC | Sep 2015 | Aug 2020 | X | | | | |

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|-----------------|------------|----------|--------|-------|-------|------|------|
| 135 | SurPRISE | Feb 2012 | Jan 2015 | | | | | X |
| 136 | SysSec | Sep 2010 | Nov 2014 | | | | | X |
| 140 | TYPES | May 2015 | Oct 2017 | | | | X | |
| 144 | VIRT-EU | Jan 2017 | Dec 2019 | X | | | | |

Table 8: “Identity, Behaviour, Ethics and Privacy” details. (F) indicates projects having ended at the time of writing.

4.1.5 National & international Security, Privacy and Governance

| # projects | Assess | Trial | Adopt | Hold | Drop |
|------------|--------|-------|-------|------|------|
| 12 | 9 | | | 2 | 1 |

Table 9: “National & international Security, Privacy and Governance” overview

The smallest sector by far this is a domain where there is basically little or no previous work in this area with only three projects previously supported. A new set of projects have now been supported which are all very new. They are all so early in their project lifecycle that they are all only classified as being projects to assess their outputs.

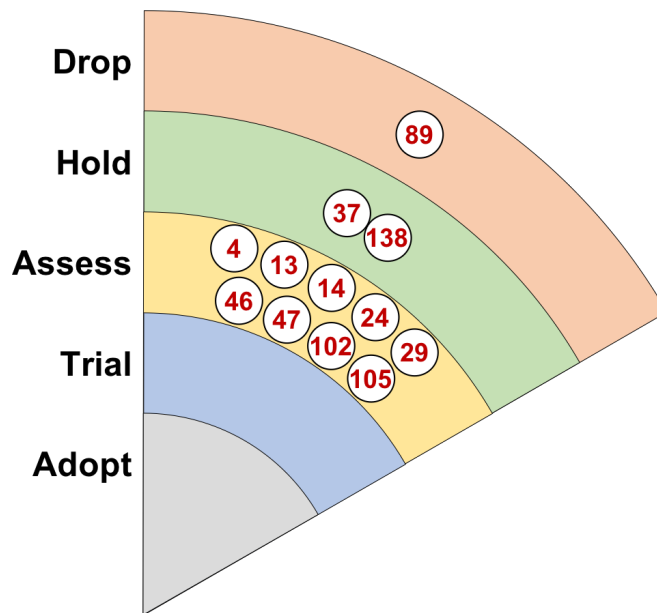


Figure 9: “National & international Security, Privacy and Governance” radar

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|----|-----------------|------------|----------|--------|-------|-------|------|------|
| 4 | AEGIS | May 2017 | Apr 2019 | X | | | | |
| 13 | CANVAS | Sep 2016 | Aug 2019 | X | | | | |
| 14 | certMILS | Jan 2017 | Dec 2020 | X | | | | |
| 24 | COMPACT | May 2017 | Oct 2019 | X | | | | |
| 29 | CS-AWARE | Sep 2017 | Aug 2020 | X | | | | |
| 37 | DISCOVERY (F) | Jan 2016 | Dec 2017 | | | | X | |
| 46 | EU-SEC | Jan 2017 | Dec 2019 | X | | | | |

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|-----------------|------------|----------|--------|-------|-------|------|------|
| 47 | EUNITY | Jun 2017 | May 2019 | X | | | | |
| 89 | PRESCIENT | Jan 2010 | Mar 2013 | | | | | X |
| 102 | PROTECTIVE | Sep 2016 | Aug 2019 | X | | | | |
| 105 | REASSURE | Jan 2017 | Dec 2019 | X | | | | |
| 138 | TREDISEC | Apr 2015 | Mar 2018 | | | | X | |

Table 10: “National & international Security, Privacy and Governance” details.
(F) indicates projects having ended at the time of writing.

4.1.6 Human Aspects of Cybersecurity

| # projects | Assess | Trial | Adopt | Hold | Drop |
|------------|--------|-------|-------|------|------|
| 20 | 5 | 1 | 3 | 3 | 8 |

Table 11: “Human Aspects of Cybersecurity” overview

This sector has a significant percentage of projects which have ended, mostly such a long time ago that their outputs have been most likely superseded. There are a small number of projects whose outputs are mature and still supported and therefore should be adopted. As per most other sectors, there are also a reasonable number of projects that have been recently supported and therefore should be assessed to understand their current level of development as well as overall the level of support any project is able to give to those externally who may use it.

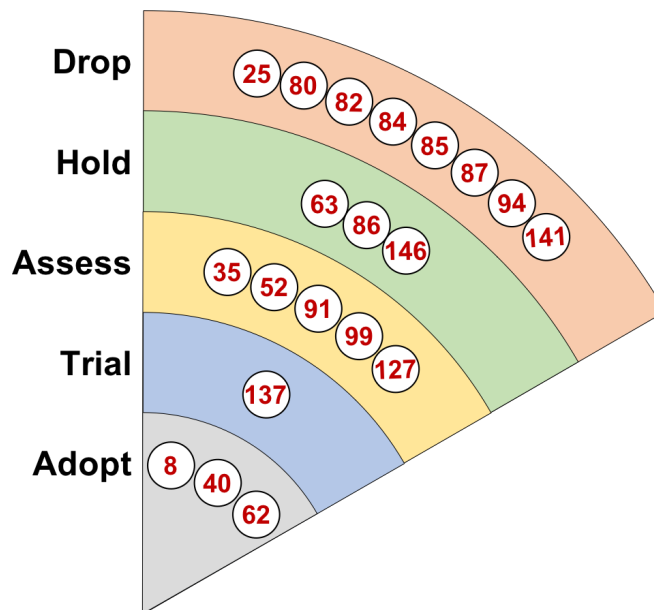


Figure 10: “Human Aspects of Cybersecurity” radar

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|----|-----------------|------------|----------|--------|-------|-------|------|------|
| 8 | ASAP (F) | Oct 2012 | Sep 2018 | | | X | | |
| 25 | CONSENT (F) | May 2010 | Apr 2013 | | | | | X |
| 35 | DECODE | Dec 2016 | Nov 2019 | X | | | | |
| 40 | DOGANA (F) | Sep 2015 | Aug 2018 | | | X | | |
| 52 | GHOST | May 2017 | Apr 2020 | X | | | | |

| # | EC Project name | Start date | End date | Assess | Trial | Adopt | Hold | Drop |
|-----|----------------------------|------------|----------|--------|-------|-------|------|------|
| 62 | MAMI (F) | Jan 2016 | Jun 2018 | | | X | | |
| 63 | MAPPING (F) | Mar 2014 | Feb 2018 | | | | X | |
| 80 | PACT (F) | Feb 2012 | Jan 2015 | | | | | X |
| 82 | PARIS (F) | Jan 2013 | Feb 2016 | | | | | X |
| 84 | PATS (F) | Aug 2009 | Mar 2012 | | | | | X |
| 85 | PICOS (F) | Feb 2008 | Jun 2011 | | | | | X |
| 86 | PQCRYPTO (F) | Mar 2015 | Feb 2018 | | | | X | |
| 87 | PRACTIS (F) | Jan 2010 | Mar 2013 | | | | | X |
| 91 | PrEstoCloud | Jan 2017 | Dec 2019 | X | | | | |
| 94 | PRISM | Mar 2008 | May 2010 | | | | | X |
| 99 | Privacy.Us | Dec 2015 | Nov 2019 | X | | | | |
| 127 | SPECIAL | Jan 2017 | Dec 2019 | X | | | | |
| 137 | TOREADOR | Jan 2016 | Dec 2018 | | X | | | |
| 141 | U2PIA | Nov 2016 | Mar 2017 | | | | | X |
| 146 | WISER | Jun 2015 | Nov 2017 | | | | X | |

Table 12: “Human Aspects of Cybersecurity” details.
(F) indicates projects having ended at the time of writing.

4.2 The Autumn 2018 Technology Radar

| Segment | Assess | Trial | Adopt | Hold | Drop | Total |
|-----------------------------------------------------------|--------|-------|-------|------|------|-------|
| Secure Systems and Technology | 18 | 2 | 4 | 17 | 6 | 47 |
| Verification and Assurance | 2 | 2 | 0 | 5 | 7 | 16 |
| Operational Risk, Management and Analytics | 9 | 1 | 3 | 5 | 2 | 20 |
| Identity, Behaviour, Ethics and Privacy | 6 | 0 | 1 | 7 | 5 | 19 |
| National & international Security, Privacy and Governance | 9 | 0 | 0 | 2 | 1 | 12 |
| Human Aspects of Cybersecurity | 5 | 1 | 3 | 3 | 8 | 20 |
| | 49 | 6 | 11 | 39 | 29 | 134 |

Table 13: Autumn 2018 Technology Radar overview

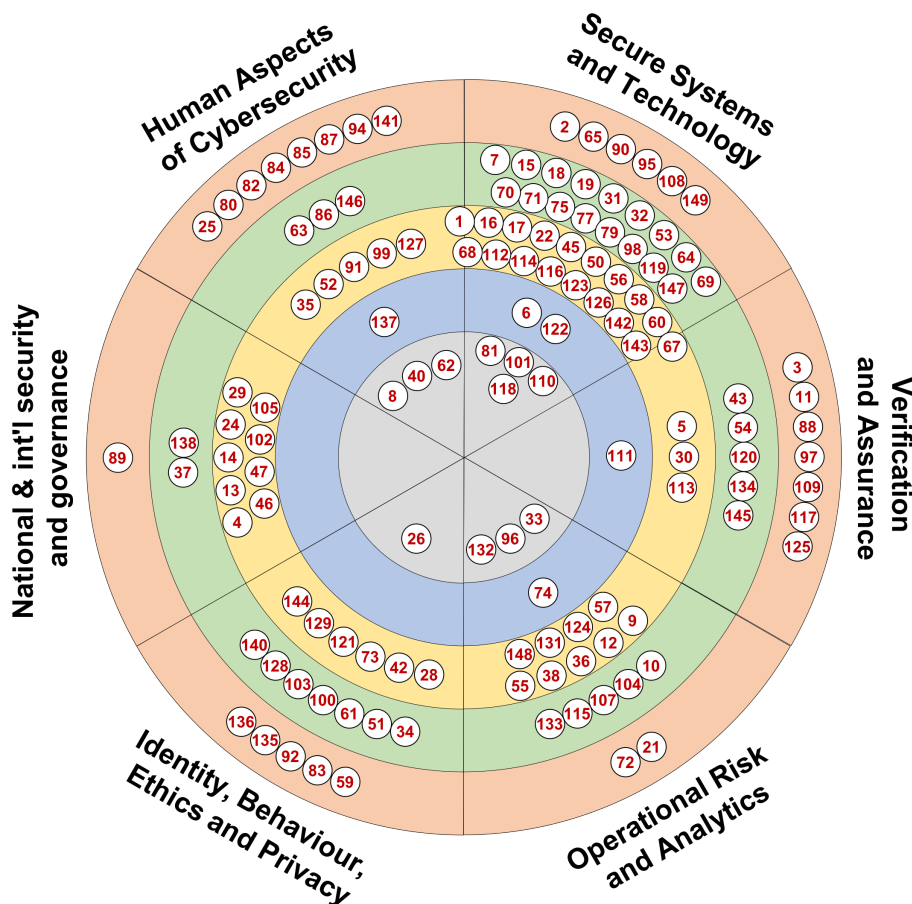


Figure 11: The Autumn 2018 Technology Radar, showing L2 taxonomy sectors, with analysed projects distributed radially into bands depending on their maturity level.

5 Commentary & next steps

Looking at the full radar it is clear that we are at a point where we have a significant growth in the number of activities that are occurring, as shown by the large number of projects that sit within Assess. It is also clear that there have been different parts of the cybersecurity research ecosystem that have been supported previously at different times, and at different levels. We would expect over the next months that we will both grow the number of products that are within the Trial and Adopt rings.

The next version of the Technology Radar report will include the utilisation of the MTRL assessment methodology described in deliverable D2.3 on these projects which will allow us to introduce a third dimension in this which is readiness for market. We will have to consider whether we represent this using the allocation to rings and colours to describe project age. Overall having a multi-dimensional visualisation where all of this is bought together will allow the community to better understand where they are and where other sit within the ecosystem.

The analysis of the 134 projects is also very important in the broader scope of the cyberwatching.eu project and in particular already introducing project results and services into the SME end-user club and marketplace. Projects categorised under Trial will be considered and contacted to provide results to the SME end-user club for potential validating and testing of results. Projects categorised under Adopt will be contacted and invited to publish their results on the actual marketplace where cyberwatching.eu can facilitate them in reaching potential adopters.

6 Appendix 1: EC funded projects reference

The following projects were included and analysed in this deliverable, in alphabetical order:

| Project | Call | Type | Start | End |
|-------------------|---------------------|--------|----------|----------|
| AARC2 | EINFRA-22-2016 | RIA | May 2017 | Apr 2019 |
| ABC4Trust | ICT-2009.1.4 | CP | Nov 2010 | Feb 2015 |
| ADDPRIV (F) | SEC-2010.6.5-2 | CP | Feb 2011 | Mar 2014 |
| AEGIS | DS-05-2016 | CSA | May 2017 | Apr 2019 |
| ANASTACIA | DS-01-2016 | RIA | Jan 2017 | Dec 2019 |
| ARIES | FCT-09-2015 | RIA | Sep 2016 | Feb 2019 |
| ARMOUR (F) | ICT-12-2015 | RIA | Feb 2016 | Jan 2018 |
| ASAP (F) | ERC-AG-PE6 | ERC-AG | Oct 2012 | Sep 2018 |
| ATENA | DS-03-2015 | IA | May 2016 | Apr 2019 |
| BEACON (F) | ICT-07-2014 | RIA | Feb 2015 | Jul 2017 |
| BIOSEC (F) | FP7-PEOPLE-IOF-2008 | MC-IOF | Mar 2009 | Feb 2012 |
| C3ISP | DS-04-2015 | IA | Oct 2016 | Sep 2019 |
| CANVAS | DS-07-2015 | CSA | Sep 2016 | Aug 2019 |
| certMILS | DS-01-2016 | IA | Jan 2017 | Dec 2020 |
| CHOReVOLUTION (F) | ICT-09-2014 | RIA | Jan 2015 | Dec 2017 |
| CIPSEC | DS-03-2015 | IA | May 2016 | Apr 2019 |
| CITADEL | DS-03-2015 | IA | Jun 2016 | May 2019 |
| CLARUS (F) | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| CloudSocket (F) | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| CloudTeams (F) | ICT-07-2014 | IA | Mar 2015 | Feb 2017 |
| COCKPITCI (F) | SEC-2011.2.5-1 | CP-FP | Jan 2012 | Dec 2014 |
| COEMS | ICT-10-2016 | RIA | Nov 2016 | Oct 2019 |
| COLA | ICT-06-2016 | IA | Jan 2017 | Jun 2019 |
| COMPACT | DS-02-2016 | IA | May 2017 | Oct 2019 |
| CONSENT (F) | SSH-2009-3.2.1. | CP-FP | May 2010 | Apr 2013 |
| CREDENTIAL (F) | DS-02-2014 | IA | Oct 2015 | Sep 2018 |
| CROSSMINER | ICT-10-2016 | RIA | Jan 2017 | Dec 2019 |
| CryptoCloud | ERC-AG-PE6 | ERC-AG | Jun 2014 | May 2019 |
| CS-AWARE | DS-02-2016 | IA | Sep 2017 | Aug 2020 |
| CYBECO | DS-04-2016 | RIA | May 2017 | Apr 2019 |

| Project | Call | Type | Start | End |
|----------------|---------------------|-----------------------------|----------|----------|
| CyberWiz (F) | DRS-17-2014 | SME-2 | Sep 2015 | Aug 2017 |
| CYCLONE (F) | ICT-07-2014 | IA | Jan 2015 | Dec 2017 |
| CYRail (F) | S2R-OC-IP2-01-2015 | Shift2Rail-RIA | Oct 2016 | Sep 2018 |
| DAPPER (F) | FP7-PEOPLE-2013-CIG | MC-CIG | Apr 2014 | Mar 2018 |
| DECODE | ICT-12-2016 | RIA | Dec 2016 | Nov 2019 |
| DEFENDER | CIP-01-2016-2017 | IA | May 2017 | Apr 2020 |
| DISCOVERY (F) | ICT-38-2015 | CSA | Jan 2016 | Dec 2017 |
| DISIEM | DS-04-2015 | IA | Sep 2016 | Aug 2019 |
| DITAS | ICT-06-2016 | RIA | Jan 2017 | Dec 2019 |
| DOGANA (F) | DS-06-2014 | IA | Sep 2015 | Aug 2018 |
| DSSC | MSCA-COFUND-2016 | MSCA-COFUND-DP | May 2017 | Apr 2022 |
| e-Sides | ICT-18-2016 | CSA | Jan 2017 | Dec 2019 |
| ECRYPT-CSA (F) | ICT-32-2014 | CSA | Mar 2015 | Feb 2018 |
| ECRYPT-NET | MSCA-ITN-2014-ETN | MSCA-ITN-ETN | Mar 2015 | Feb 2019 |
| ENCASE | MSCA-RISE-2015 | MSCA-RISE | Jan 2016 | Dec 2019 |
| EU-SEC | DS-01-2016 | IA | Jan 2017 | Dec 2019 |
| EUNITY | DS-05-2016 | CSA | Jun 2017 | May 2019 |
| FIDELITY (F) | SEC-2011.3.4-1 | CP-IP | Feb 2012 | Jan 2016 |
| FORTIKA | DS-02-2016 | IA | Jun 2017 | May 2020 |
| FutureTrust | DS-05-2015 | IA | Jun 2016 | May 2019 |
| GenoPri (F) | MSCA-IF-2015-EF | MSCA-IF-EF-ST - Standard EF | May 2016 | Apr 2018 |
| GHOST | <u>DS-02-2016</u> | IA | May 2017 | Apr 2020 |
| HEAT (F) | ICT-32-2014 | RIA | Jan 2015 | Dec 2017 |
| HECTOR (F) | ICT-32-2014 | RIA | Mar 2015 | Feb 2018 |
| HERMENEUT | DS-04-2016 | RIA | May 2017 | Apr 2019 |
| HIPS | ERC-CG-2013-PE6 | ERC-CG | Oct 2014 | Sep 2019 |
| IMPACT | ERC-2013-SyG | ERC-SyG | Feb 2015 | Jan 2021 |
| KONFIDO | DS-03-2016 | RIA | Nov 2016 | Oct 2019 |
| LAST (F) | ERC-SG-PE6 | ERC-SG - ERC Starting Grant | Oct 2009 | Sep 2014 |
| LIGHTest | DS-05-2015 | IA | Sep 2016 | Aug 2019 |
| LV-Pri20 (F) | MSCA-IF-2014-EF | MSCA-IF-EF-CAR | Jun 2015 | Jun 2017 |
| MAMI (F) | ICT-12-2015 | RIA | Jan 2016 | Jun 2018 |
| MAPPING (F) | SiS.2013.1.2-1 | CSA-SA | Mar 2014 | Feb 2018 |

| Project | Call | Type | Start | End |
|-----------------|---------------------|---------------|----------|----------|
| MAS2TERING (F) | ICT-2013.6.1 | CP | Sep 2014 | Aug 2017 |
| MATTHEW (F) | ICT-2013.1.5 | CP | Nov 2013 | Oct 2016 |
| MELODIC | ICT-06-2016 | RIA | Dec 2016 | Nov 2019 |
| mF2C | ICT-06-2016 | RIA | Jan 2017 | Dec 2019 |
| MH-MD | ICT-18-2016 | RIA | Nov 2016 | Oct 2019 |
| MIKELANGELO (F) | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| MITIGATE (F) | DS-06-2014 | IA | Sep 2015 | Feb 2018 |
| MUSA (F) | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| NECOMA (F) | ICT-2013.10.1 | CP | Jun 2013 | Mar 2016 |
| NeCS | MSCA-ITN-2015-ETN | MSCA-ITN-ETN | Sep 2015 | Aug 2019 |
| OCGN | MSCA-IF-2015-EF | MSCA-IF-EF-ST | May 2017 | Nov 2018 |
| OCTAVE (F) | DS-02-2014 | IA | Jun 2015 | Jul 2017 |
| OPENREQ | ICT-10-2016 | RIA | Jan 2017 | Dec 2019 |
| OPERANDO (F) | DS-01-2014 | IA | May 2015 | Apr 2018 |
| P5 (F) | SEC-2012.2.3-1 | CP-FP | Aug 2013 | Oct 2016 |
| PaaSword (F) | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| PACT (F) | SEC-2011.6.5-2 | CP-FP | Feb 2012 | Jan 2015 |
| PANORAMIX (F) | DS-01-2014 | IA | Sep 2015 | Aug 2018 |
| PARIS (F) | SEC-2012.6.1-2 | CP-FP | Jan 2013 | Feb 2016 |
| PASS (F) | PEOPLE-2007-4-3.IRG | MC-IRG | Dec 2008 | Nov 2012 |
| PATS (F) | SiS-2008-1.2.2.1 | CSA-SA | Aug 2009 | Mar 2012 |
| PICOS (F) | ICT-2007.1.4 | CP | Feb 2008 | Jun 2011 |
| PQCRYPTO (F) | ICT-32-2014 | RIA | Mar 2015 | Feb 2018 |
| PRACTIS (F) | SiS-2009-1.1.2.1 | CP-FP | Jan 2010 | Mar 2013 |
| PRECIOSA | ICT-2007.6.2 | CP | Mar 2008 | Aug 2010 |
| PRESCIENT | SiS-2009-1.1.2.1 | CP-FP | Jan 2010 | Mar 2013 |
| PreserviX | ICT-37-2014-1 | SME-1 | May 2015 | Oct 2015 |
| PrEstoCloud | ICT-06-2016 | RIA | Jan 2017 | Dec 2019 |
| PrimeLife | ICT-2007.1.4 | CP | Mar 2008 | Jun 2011 |
| PRIPARE | ICT-2013.1.5 | CSA | Oct 2013 | Sep 2015 |
| PRISM | ICT-2007.1.4 | CP | Mar 2008 | May 2010 |
| PRISM CODE | FP7-PEOPLE-2012-CIG | MC-CIG | Nov 2012 | Oct 2016 |
| PRISMACLOUD | ICT-32-2014 | RIA | Feb 2015 | Jul 2018 |

| Project | Call | Type | Start | End |
|-------------------|---------------------------|--------------|----------|----------|
| PRISMS | SEC-2011.6.5-2 | CP-FP | Feb 2012 | Jul 2015 |
| PRIVACY FLAG | DS-01-2014 | IA | May 2015 | Apr 2018 |
| <u>Privacy.Us</u> | MSCA-ITN-2015-ETN | MSCA-ITN-ETN | Dec 2015 | Nov 2019 |
| PRIVACY4FORENSICS | FP7-PEOPLE-2013-IIF | MC-IIF | Feb 2015 | Mar 2018 |
| ProBOS | SMEInst-13-2016-2017 | SME-2 | Oct 2016 | Sep 2018 |
| PROTECTIVE | DS-04-2015 | IA | Sep 2016 | Aug 2019 |
| Ps2Share | ICT-35-2016 | RIA | Jan 2017 | Dec 2017 |
| RAPID | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| REASSURE | DS-01-2016 | RIA | Jan 2017 | Dec 2019 |
| ReCRED | DS-02-2014 | IA | May 2015 | Apr 2018 |
| RESENTRY | H2020-SMEINST-1-2016-2017 | SME-1 | Jul 2017 | Dec 2017 |
| RESPECT | SEC-2011.6.1-5 | CP-FP | Feb 2012 | May 2015 |
| REVEN-X1 | ICT-37-2015-1 | SME-1 | Jul 2015 | Dec 2015 |
| SafeCloud | DS-01-2014 | IA | Sep 2015 | Aug 2018 |
| SAFEcrypto | ICT-32-2014 | RIA | Jan 2015 | Dec 2018 |
| SAFERtec | DS-01-2016 | RIA | Jan 2017 | Dec 2019 |
| SAINT | DS-04-2016 | RIA | Mar 2017 | Feb 2021 |
| SAURON | CIP-01-2016-2017 | IA | May 2017 | Apr 2019 |
| SCISSOR | ICT-32-2014 | RIA | Jan 2015 | Dec 2017 |
| SCOTT | ECSEL-2016-2-IA-two-stage | IA | May 2017 | Jun 2020 |
| SCR | SMEInst-13-2016-2017 | SME-1 | Jul 2016 | Dec 2016 |
| SecIoT | INNOSUP-02-2016 | CSA | Sep 2017 | Aug 2018 |
| SERECA | ICT-07-2014 | RIA | Mar 2015 | Feb 2018 |
| SHARCS | ICT-32-2014 | RIA | Jan 2015 | Dec 2017 |
| SHIELD | DS-03-2016 | RIA | Jan 2017 | Dec 2019 |
| SHIELD | DS-04-2015 | IA | Sep 2016 | Feb 2019 |
| SISSDEN | DS-04-2015 | IA | May 2016 | Apr 2019 |
| SMESEC | DS-02-2016 | IA | Jun 2017 | May 2020 |
| SocialPrivacy | FP7-PEOPLE-2011-IOF | MC-IOF | Sep 2012 | Aug 2015 |
| SODA | ICT-18-2016 | RIA | Jan 2017 | Dec 2019 |
| SPECIAL | ICT-18-2016 | RIA | Jan 2017 | Dec 2019 |
| SpeechXRays | DS-02-2014 | IA | May 2015 | Apr 2018 |

| Project | Call | Type | Start | End |
|--------------------|----------------------|---------|----------|----------|
| SPOOC | ERC-CoG-2014 | ERC-COG | Sep 2015 | Aug 2020 |
| STAMP | ICT-10-2016 | RIA | Dec 2016 | Nov 2019 |
| STOP-IT | CIP-01-2016-2017 | IA | Jun 2017 | May 2021 |
| STORM | EE-13-2014 | RIA | Mar 2015 | Aug 2018 |
| SUNFISH | ICT-07-2014 | RIA | Jan 2015 | Dec 2017 |
| SUPERCLOUD | ICT-07-2014 | RIA | Feb 2015 | Jan 2018 |
| SurPRISE | SEC-2011.6.5-2 | CP-FP | Feb 2012 | Jan 2015 |
| SysSec | ICT-2009.1.4 | NoE | Sep 2010 | Nov 2014 |
| TREADOR | ICT-16-2015 | RIA | Jan 2016 | Dec 2018 |
| TREDISEC | ICT-32-2014 | RIA | Apr 2015 | Mar 2018 |
| <u>TRUESSEC.EU</u> | DS-01-2016 | CSA | Jan 2017 | Dec 2018 |
| TYPES | DS-01-2014 | IA | May 2015 | Oct 2017 |
| U2PIA | SMEInst-13-2016-2017 | SME-1 | Nov 2016 | Mar 2017 |
| UNICORN | ICT-06-2016 | IA | Jan 2017 | Dec 2019 |
| VESSEDIA | DS-01-2016 | RIA | Jan 2017 | Dec 2019 |
| VIRT-EU | ICT-35-2016 | RIA | Jan 2017 | Dec 2019 |
| VisiOn | DS-01-2014 | | Jul 2015 | Jun 2017 |
| WISER | DS-06-2014 | IA | Jun 2015 | Nov 2017 |
| WITDOM | ICT-32-2014 | RIA | Jan 2015 | Dec 2017 |
| FENTEC | H2020-DS-LEIT-2017 | RIA | Jan 2018 | Dec 2020 |
| SAWSOC | | | | |