C&ESAR 2021 Call for Paper

C&ESAR's Program Committee

2021/05/27

Abstract

The cybersecurity conference C&ESAR solicits submissions on the subject "Automation in Cybersecurity". The submission deadline is June 16th, 2021.

About C&ESAR

Every year since 1997, the French Ministry of Defense organizes a cybersecurity conference, called C&ESAR. This conference is now one of the main events of the European Cyber Week (ECW) organized every fall in Rennes, Brittany, France.

The goal of C&ESAR is to bring together governmental, industrial, and academic stakeholders interested in cybersecurity. This event, both educational and scientific, gathers experts, researchers, practitioners and decision-makers. This inter-disciplinary approach allows operational practitioners to learn about and anticipate future technological inflection points, and for industry and academia to confront research and product development to operational realities. Every year, C&ESAR explores a different topic within the field of cybersecurity.

This year's topic is: ***Automation in Cybersecurity***. The call for paper is available on a dedicated web page presenting the call and as a PDF file.

C&ESAR's 2021 Topic: *Automation in Cybersecurity*

Many recent reports and surveys identify automation as a key enabler in cybersecurity to improve response time and handle the increasing work load associated to limited resources. This view is shared by many. In a recent study [7] the Ponemon Institute states that 77% of respondents either use or plan to use automation for cybersecurity, while the SANS reports [8] to have seen an increase of 11.8% in adoption of dedicated automation solutions in the past year, and that less than 2% of respondents do not have a need for an automation project in the coming year. This is due to the perceived benefit of automation. Indeed, IBM states [4] that 42% of the respondents (and 55% of the most cyber resilient

organizations, i.e. high performers) claim that automation improves cyber resilience, and that 70% of the high performers report significant or moderate use of automation. In another report [3], IBM Security evaluates the "savings in average breach costs for companies with fully deployed security automation versus those without deployed security automation" to $3.58 million.

Automation is not restricted to SOC (Security Operations Centers), it can be applied to many cybersecurity areas. While Osterman Research identifies [6] low-hanging opportunities like resetting passwords or managing access rights as employees move across job roles and departments, SANS lists [8] varying activities that can benefit from automation, such as: vulnerability management, compliance support (that the Ponemon Institute also sees as one of the main incentive for automation [7]), or security posture assessment with a breach attack simulation tool. In the same report, SANS also lists tools that deserve integration in an automated environment, for example: identity management, SSL visibility (encryption/decryption) at the network boundary, security case management systems, file integrity monitoring (FIM), or browser and screen-capture tools. Automation can also be brought to other areas than cyberdefense. The Ponemon Institute [7] and Deloitte [2] report on automation of cybersecurity practices in the context of Dev[Sec]Ops and continuous integration and deployment (CI/CD), which is both an opportunity for automation of security and a threat for the security of automation as emphasized by the recent Sunburst fiasco and explicited in a recent column of The Register. Meanwhile, the Ponemon Institute states that 53% of respondents [7] observe an increasing use of automation by attackers themselves.

From a societal point of view, automation in cybersecurity is not so much about replacing IT staff than make them more efficient. Only 5% of respondents to SANS survey [8] expect automation to result in a reduction in staffing. There is a consensus among many reports [7], [4], [1] that automation does, on one side, free up time for staff to focus on higher valued tasks, and in another side, improve staff efficiency on those more important tasks. The question is not if automated tasks will replace humans, but how humans will interact with automated tasks. This last point relates to the notion of *Cyber Centaur* discussed by Aksela in a blog post of 2018.
Still on the societal point of view, this increase of automation raises the concerns of risk evaluation and acceptation by the general society. Among those are the questions of privacy (and security in general) of automatically shared information. Indeed, 59% of respondents to IBM's survey [4] believe in threat intelligence sharing, and 57% of organizations already share information with government and/or industry peers about cyber threats and vulnerabilities. In a federated cybersecurity defense setting, those processes are likely to be automated.

Even if the interest in cybersecurity automation is recognized, its deployment varies greatly among industries and countries [3]. For example, the deployment of automation in France is notably lower than in similarly developed countries, with nearly half of respondents working in organizations without deployed automation

[3]. In particular, only 14% of respondents to the 2021 CESIN's barometer [5] declared having a Security Orchestration, Automation and Response (SOAR) system deployed in their company. It can therefore be expected to see an increase of automation in cybersecurity, with 1 out of 4 respondents [4] identifying the "lack of advanced technologies such as automation" as a challenge to improve cyber resilience. However, it is not only a question of adoption, but also a question of development of new and improved solutions. This is emphasized by the gap between the lower satisfaction level of prior automation projects compared to the anticipated satisfaction level of current projects [8]. It is also driven by the development of new regulations (such as GDPR, China Internet Security Law and APEC Privacy Framework) which, according to nearly 3 out of 4 respondents [7], influence the adoption of automation.

In this context, C&ESAR solicits submissions presenting clear surveys, innovative solutions, or insightful experience reports on the subject of "automation in cybersecurity".

The scope covers:

- all steps of cybersecurity, from DevSecOps to operational cyberdefense or pentesting;
- all types of products or context, including for example: networks, embedded systems, industrial systems, IoT, edge computing, ...;
- all levels of automation, from partial to full automation (as long as a clear benefit is provided by the automated part).

The topics include (without being limited to them) those mentioned above and below:

- societal impact of automation;
- privacy and intellectual property in an automated context;
- automation in federated processes (cyber intelligence publication and integration, federated defense and response, ...);
- human/machine interaction in a context of partial automation: automatic preprocessing for manual processes, manual selection of automatic processes, iteration in human/machine processes, manual inputs to automatic processes, manual validation of automatic processes, feedback to humans, ...;
- verification and validation of automation;
- ...

References

[1] Deloitte, "Future of cyber," Deloitte, 2020. [Online]. Available: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/gx-future-of-cyber.html.

[2] Deloitte, "The future of cyber survey 2019," Deloitte, 2019. [Online]. Available: https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-

survey.html.

[3] IBM Security, "Cost of a Data Breach Report," IBM Corporation, Jul. 2020. Produced jointly between Ponemon Institute and IBM Security: the research is conducted independently by Ponemon Institute, and the results are sponsored, analyzed, reported and published by IBM Security. [Online]. Available: https://www.ibm.com/security/data-breach.

[4] IBM Security, "Cyber Resilient Organization Report," IBM Corporation, Jul. 2020. Produced jointly between Ponemon Institute and IBM Security: the research is conducted independently by Ponemon Institute and results are sponsored, analyzed, reported and published by IBM Security. [Online]. Available: https://www.ibm.com/account/reg/us-en/subscribe?formid=urx-45839.

[5] OpinionWay, "Baromètre de la cyber-sécurité des entreprises," OpinionWay, Rapport CESIN, Jan. 2021. Sponsored by CESIN. [Online]. Available: https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html.

[6] Osterman Research, "How to Minimize the Impact of the Cybersecurity Skills Shortage," Osterman Research, White Paper, Oct. 2020. Sponsored by Trustwave. [Online]. Available: https://www.trustwave.com/en-us/resources/library/documents/how-to-minimize-the-impact-of-the-cybersecurity-skills-shortage/.

[7] Ponemon Institute, "The 2020 Study on Staffing the IT Security Function in the Age of Automation: United States and United Kingdom," Ponemon Institute, Feb. 2020. Sponsored by DomainTools. [Online]. Available: https://www.domaintools.com/resources/survey-reports/2020-ponemon-survey-report-staffing-the-it-security-function.

[8] SANS Institute, "2020 SANS Automation and Integration Survey," SANS Institute, May 2020. Sponsored by Swimlane. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/2020-automation-integration-survey-39575.

Submission process

C&ESAR solicits two types of papers:

- ***Regular paper***: ***8 to 16 pages*** paper describing work not yet published;
- ***Extended abstract***: ***3 to 6 pages*** abstract of a large audience didactic paper recently published in a peer-reviewed journal or conference proceedings (papers of interest include in particular: states of the art or practice; surveys; experience reports; and directly applicable solutions to common problems).

Steps

- *First phase*: ***proposals (3 to 6 pages for both types of papers)*** shall be submitted as a PDF file no later than ***June 16th, 2021*** via https://easychair.org/conferences/?conf=cesar2021. Each submission shall include a title, authors' names and affiliation, corresponding author's email address, an abstract (10 lines max.), and a list of keywords. Authors will be notified of their proposal acceptance by *September 3rd, 2021*.
  - ***Extended abstract*** proposals must: be clearly identified as such by the mention "extended abstract" in their title; clearly identify and cite the abstracted original publication; and contain an appendix (in addition to the 3 to 6 pages) containing the (anonymized) comments made by the reviewers of the original publication.
- *Second phase*: authors of accepted papers shall send the camera-ready version of their paper by ***October 1st, 2021*** to contact@cesar-conference.org, cc to cesar2021@easychair.org. Authors whose papers are accepted commit to address reviewers comments in the final version.

Language and selection criteria

Papers are written in French or in English (English translations of title and abstract of papers written in French must be provided).

For both types of papers, selection criteria include in particular: clarity; pedagogical (didactical) value; and respect of this call for papers topic and guidelines.

For ***regular papers***, specialized technical papers will be appreciated if they contribute to explain and analyze the state of the art or practice and their deficiencies.

For ***extended abstracts***, the original publication must be clearly identified and cited. Moreover, the selection process is more selective, and places a particular focus on the didactical quality and large audience of the papers.

Instructions for the format of proposals and papers

Proposals and papers must be submitted as PDF files, without page numbering, following the single column format of "CEUR Workshop Proceedings" (http://ceur-ws.org/).

Templates are available for LaTeX, docx (Word) and ODT (Word or LibreOffice) at the following URL: http://ceur-ws.org/Vol-XXX/CEURART.zip.

An Overleaf (LaTeX) project is also available at https://www.overleaf.com/project/5e76702c4acae70001d3bc87. It must be duplicated before edition.

Proceedings

As far as possible, the conference proceedings will be formally published as "CEUR Workshop Proceedings" (http://ceur-ws.org/). This publication is conditioned by the respect of this publisher's constraints (http://ceur-ws.org/HOWTOSUBMIT.html), in particular respect of its paper format and having a majority of articles written in English.

In the event that only a subset of the papers can be formally published as "CEUR Workshop Proceedings", a selection of papers will **potentially** be made to form the official conference proceedings which will be published as a volume of "CEUR Workshop Proceedings". The official proceedings inclusion decision is at the discretion of the editors of the proceedings and is based, in part, on the following recommendations:

- articles in English strictly following the "CEUR Workshop Proceedings" format are included;
- articles in French strictly following the "CEUR Workshop Proceedings" format are **potentially** included;
- articles that do not respect the "CEUR Workshop Proceedings" format are not included.

Articles accepted for presentation at the conference, but not included in the official conference proceedings (all articles if there are no proceedings published as a volume of "CEUR Workshop Proceedings"), are published on C&ESAR conference's website.

As far as possible, indexing of articles in DBLP and Google Scholar is facilitated.

Deadlines

- Submission of the *proposals* (3 to 6 pages): June 16th, 2021
- Notification to authors: September 3rd, 2021
- Final version: October 1st, 2021
  - 8 to 16 pages for *regular papers*
  - 3 to 6 pages for *extended abstracts*
- European Cyber Week (ECW): Tuesday November 16th, 2021 to Thursday November 18th, 2021

Program committee

- Erwan ABGRALL (CALID)
- José ARAUJO (Orange Cyberdéfense)
- Christophe BIDAN (CentraleSupélec)
- Yves CORREC (ARCSI)
- Frédéric CUPPENS (Polytechnique Montréal)
- Herve DEBAR (Télécom SudParis)

- Guillaume DUVEAU (MinArm)
- Ivan FONTARENSKY (Thales)
- Patrick HEBRARD (Naval Group)
- Gurvan LE GUERNIC (DGA MI, Université de Rennes 1)
- Guillaume MEIER (Airbus R&D)
- Marc-Oliver PAHL (IMT Atlantique, Chaire Cyber CNI)
- Yves-Alexis PEREZ (ANSSI)
- Ludovic PIETRE-CAMBACEDES (EDF)
- Louis RILLING (DGA MI)
- Franck ROUSSET (MinArm)
- Assia TRIA (CEA)
- Eric WIATROWSKI (Orange Cyberdéfense)

Sponsors

Figure 1: Sponsors list