C&ESAR'21: Automation in Cybersecurity (Preface)

Gurvan Le Guernic[1,2]

[1] DGA Maîtrise de l'Information, Rennes, France
[2] Univ Rennes, Inria, CNRS, IRISA, Rennes, France

Abstract

C&ESAR is an educational and scientific conference on cybersecurity whose specific topic changes every year. This year C&ESAR is focused on automation in cybersecurity. Automation is identified as a key enabler to tackle today's challenges in cybersecurity. The main objective for using automation in cybersecurity is not to reduce the work force, but to automate as much as possible in many different areas in order to allow experts to focus on tasks requiring more expertise and having more value. C&ESAR 2021 received 32 papers submitted for peer-review. Out of these, 16 papers were accepted for presentation at the conference. After the conference, 14 were short listed for inclusion in this volume.

Keywords

Cybersecurity, Automation, C&ESAR, Conference, Preface

Résumé : *C&ESAR'21: Automatisation en Cybersecurité (Préface)*

C&ESAR est une conférence pédagogique et scientifique sur la cybersécurité dont le sujet spécifique change chaque année. Cette année, C&ESAR se concentre sur l'automatisation de la cybersécurité. L'automatisation est identifiée comme un outil clé pour relever les défis actuels en matière de cybersécurité. Le principal objectif de l'utilisation de l'automatisation en cybersécurité n'est pas de réduire les effectifs, mais d'automatiser autant que possible dans de nombreux domaines différents afin de permettre aux experts de se concentrer sur les tâches nécessitant plus d'expertise et ayant plus de valeur. C&ESAR 2021 a reçu 32 articles soumis pour examen par les pairs. Parmi ceux-ci, 16 articles ont été acceptés pour présentation à la conférence, dont 14 pour inclusion dans les actes.

1. C&ESAR

Every year since 1997, the French Ministry of Defense organizes a cybersecurity conference, called C&ESAR (https://www.cesar-conference.org). This conference is now one of the main events of the European Cyber Week (ECW, https://www.european-cyber-week.eu) 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

C&ESAR'21: Computer & Electronics Security Application Rendezvous, Nov. 16-17, 2021, Rennes, France

EMAIL: gurvan.le_guernic@inria.fr (G. Le Guernic)
ORCID: 0000-0003-0387-9738 (G. Le Guernic)

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.

C&ESAR's 2021 topic is: ***Automation in Cybersecurity***.

2. Automation in Cybersecurity

Many recent reports and surveys [1] 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 [2] the Ponemon Institute (https://www.ponemon.org) states that 77% of respondents either use or plan to use automation for cybersecurity, while the SANS (https://www.sans.org) reports [3] to have seen an increase of 11.8% in adoption of dedicated automation solutions in the year preceding its survey, 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 [5], IBM Security (https://www.ibm.com/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 (https://www.ostermanresearch.com) identifies [6] low-hanging opportunities like resetting passwords or managing access rights as employees move across job roles and departments, SANS lists [3] 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 [2]), 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 [2] and Deloitte (https://www.deloitte.com) [7] 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 [8] and explicited in a recent column of The Register [9]. Meanwhile, the Ponemon Institute states that 53% of respondents [2] 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 [3] expect automation to result in a reduction in staffing. There is a consensus

among many reports [2, 4, 10] 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 [11] 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 [5]. 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 [5]. In particular, only 14% of respondents to the 2021 barometer of CESIN (https://www.cesin.fr) [12] 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 [3]. 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 [2], influence the adoption of automation.

3. C&ESAR 2021 Call

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

The scope of the call covered:

- 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 of the call included (without being limited to them) those mentioned in the previous section as well as, for example:

- 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.

C&ESAR received 32 submissions. Among those 20 proposals have been selected for the final round of reviews (63% pre-selection rate); out of those pre-selected proposals, 16 have been selected for presentation at the conference (a 80% acceptation rate for the final round of reviews, and a 50% overall acceptation rate for the conference). Finally, 14 of the presented papers have been selected for inclusion in the proceedings (an overall acceptation rate of 44% for the proceedings).

4. Program committee

This peer review has been made possible thanks to the dedication of the members of the following program committee:

- Erwan Abgrall
- José Araujo, Orange Cyberdéfense
- Frédéric Besson, Université de Rennes 1
- Christophe Bidan, CentraleSupélec
- Yves Correc, ARCSI
- Frédéric Cuppens, Polytechnique Montréal
- Herve Debar, Télécom SudParis
- Ivan Fontarensky, Thales
- Julien Francq, Naval Group
- Brittia Guiriec, DGA MI
- Gurvan Le Guernic, DGA MI & Université de Rennes 1
- Frédéric Majorczyk, DGA MI & CentraleSupélec
- Guillaume Meier, Airbus R&D
- Laurence Ogor, DGA MI
- Marc-Oliver Pahl, IMT Atlantique & Chaire Cyber CNI
- Yves-Alexis Perez, ANSSI
- Ludovic Pietre-Cambacedes, EDF
- Olivier Poupel, DGA MI
- Denis Real, DGA MI
- Louis RILLING, DGA MI
- Franck Rousset, DGNum
- Florence Schadle, DGA MI
- Eric Wiatrowski

References

[1] Cyentia Institute, Cyentia Cybersecurity Research Library, Search results for ”automation”, 2021. URL: https://library.cyentia.com/search.html?q=automation.

[2] Ponemon Institute, The 2020 Study on Staffing the IT Security Function in the Age of Automation: United States and United Kingdom, Technical Report, Ponemon Institute, 2020. URL: https://www.domaintools.com/resources/survey-reports/2020-ponemon-survey-report-staffing-the-it-security-function, sponsored by DomainTools.

[3] SANS Institute, 2020 SANS Automation and Integration Survey, Technical Report, SANS Institute, 2020. URL: https://www.sans.org/reading-room/whitepapers/analyst/2020-automation-integration-survey-39575, sponsored by Swimlane.

[4] IBM Security, Cyber Resilient Organization Report, Technical Report, IBM Corporation, 2020. URL: https://www.ibm.com/account/reg/us-en/subscribe?formid=urx-45839, 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.

[5] IBM Security, Cost of a Data Breach Report, Technical Report, IBM Corporation, 2020. URL: https://www.ibm.com/security/data-breach, 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.

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

[7] Deloitte, The future of cyber survey 2019, Technical Report, Deloitte, 2019. URL: https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html.

[8] T. Claburn, We’re not saying this is how solarwinds was backdoored, but its FTP password ’leaked on github in plaintext’, in: The Register® - Biting the hand that feeds IT, Situation Publishing, 2020. URL: https://www.theregister.com/2020/12/16/solarwinds_github_password/.

[9] R. Goodwins, Well, on the bright side, the SolarWinds Sunburst attack will spur the cybersecurity field to evolve all over again, in: The Register® - Biting the hand that feeds IT, Situation Publishing, 2020. URL: https://www.theregister.com/2020/12/21/solarwinds_sunburst_evolve/.

[10] Deloitte, Future of cyber, Technical Report, Deloitte, 2020. URL: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/gx-future-of-cyber.html.

[11] M. Aksela, How to Build a Cyber Centaur, in: F-Secure Life, F-Secure Corporation, 2018. URL: https://www.https://blog.f-secure.com/how-to-build-a-cyber-centaur/.

[12] OpinionWay, Baromètre de la cyber-sécurité des entreprises, Rap-

port CESIN, OpinionWay, 2021. URL: https://www.cesin.fr/fonds-documentaire-6eme-edition-du-barometre-annuel-du-cesin.html, sponsored by CESIN.