Appel à communications pour C&ESAR

Comité de programme de C&ESAR

2021/02/05

Résumé

La conférence en cybersécurité C&ESAR sollicite des propositions de contribution sur le thème "Automatisation en cybersécurité". La date limite de soumission est le 28 mai 2021.
The cybersecurity conference C&ESAR solicits submissions on the subject "Automation in Cybersecurity". The submission deadline is May 28th, 2021.

À propos de C&ESAR

Chaque année depuis 1997, le Ministère des Armées organise une conférence sur la cybersécurité, appelée C&ESAR. Cette conférence est désormais l'un des principaux événements de la European Cyber Week (ECW) organisée chaque automne à Rennes, France.

L'objectif de C&ESAR est de rassembler et faciliter les échanges entre divers acteurs gouvernementaux, industriels et universitaires ayant un intérêt pour la cybersécurité. Cet événement, à la fois pédagogique et scientifique, rassemble des experts, des chercheurs, des praticiens et des décideurs. Cette approche interdisciplinaire permet aux praticiens opérationnels de connaître et d'anticiper les futures (r)évolutions technologiques, et permet aux académiques et industriels de confronter la recherche et le développement de produits et services aux réalités opérationnelles. Chaque année, C&ESAR explore un sujet différent dans le domaine de la cybersécurité.

Le thème de cette année est : ***Automatisation en Cybersécurité***. L'appel à communications est disponible sur une page web dédiée à l'appel et sous forme de fichier PDF.

Thème de C&ESAR 2021 : *Automatisation en Cybersécurité*

Récemment, de nombreux rapports et enquêtes identifient l'automatisation comme un élément clé en cybersécurité pour améliorer le temps de réponse et gérer la charge de travail croissante malgré des ressources limitées. Ce point de

vue est partagé par beaucoup. Dans une étude récente [7], le Ponemon Institute indique que 77% des personnes interrogées utilisent ou prévoient d'utiliser l'automatisation pour la cybersécurité, tandis que SANS rapporte avoir constaté une augmentation de 11,8% de l'adoption de solutions d'automatisation dédiées au cours de l'année écoulée [8], et que moins de 2% des personnes interrogées n'ont pas identifié de besoin d'automatisation pour l'année à venir. Cet engouement est dû aux avantages offerts par l'automatisation. En effet, IBM déclare [4] que 42% des personnes interrogées (et 55% des organisations les plus cyber-résilientes, "high performers") affirment que l'automatisation améliore la cyber-résilience, et que 70% des "high performers" utilisent l'automatisation de manière significative ou modérée. Dans un autre rapport [3], IBM Security évalue que le coût moyen d'une cyberattaque "réussie" pour les entreprises avec une forte automatisation de leur cybersécurité est plus faible de 3,58 millions de dollars par rapport à celles sans forte automatisation de leur cybersécurité.

L'automatisation ne se limite pas aux SOC (Security Operations Centers), elle peut être appliquée à de nombreux domaines de la cybersécurité. Alors que Osterman Research identifie [6] des opportunités facilement atteignables comme la réinitialisation automatique des mots de passe ou l'automatisation de la gestion des droits d'accès lorsque les employés changent de fonction ou de service, SANS liste [8] de nombreuses autres activités pouvant bénéficier de l'automatisation, telles que: la gestion des vulnérabilités, le support de conformité (que le Ponemon Institute voit également comme l'une des principales incitations à l'automatisation [7]), ou l'évaluation de la posture de sécurité avec des outils de simulation de cyberattaques. Dans le même rapport, SANS répertorie également les outils qui méritent d'être intégrés dans un environnement automatisé, par exemple: les gestionnaires d'identités, les sondes donnant une visibilité sur le chiffrement SSL en bordure de réseau, les systèmes de gestion et d'archivage des évènements de sécurité, les sondes de surveillance de l'intégrité des fichiers (FIM), ou des outils de capture d'écran des navigateurs web. L'automatisation peut également être appliquée à d'autres aspects de la cybersécurité que la seule cyberprotection. Dans leurs publications respectives, le Ponemon Institute [7] et Deloitte [2] évoquent l'automatisation des pratiques de cybersécurité dans le cadre du Dev[Sec]Ops et de l'intégration et déploiement continus (CI/CD). En complément, le Ponemon Institute déclare que 53% des personnes interrogées [7] observent une utilisation croissante de l'automatisation par les attaquants.

D'un point de vue sociétal, l'automatisation de la cybersécurité n'a pas tant pour but de remplacer le personnel que de le rendre plus efficace. Seuls 5% des personnes interrogées par l'enquête SANS [8] s'attendent à ce que l'automatisation se traduise par une réduction du personnel. Il existe un consensus parmi de nombreux rapports [7], [4], [1] selon lesquels l'automatisation, d'un côté, libère du temps pour que le personnel se concentre sur les tâches à plus forte valeur ajoutée, et d'un autre côté, améliore l'efficacité du personnel sur ces tâches plus importantes. La question n'est pas de savoir si les tâches automatisées remplaceront les humains, mais comment les humains interagiront avec les tâches automatisées. Ce dernier point est en lien avec la notion de *Cyber Centaur*

évoquée par Aksela dans un article de blog de 2018.
Cette montée en puissance de l'automatisation soulève également des préoccupations d'évaluation et d'acceptation des risques par la société en général. Parmi celles-ci figurent les questions de confidentialité (et de sécurité en général) des informations partagées automatiquement. En effet, 59% des personnes interrogées par l'enquête d'IBM [4] sont favorables au partage de renseignements sur les menaces, et 57% des organisations partagent déjà des informations avec des organisations gouvernementales ou industrielles sur les cyber-menaces et les vulnérabilités. Dans un contexte de défense fédérée, ces processus sont susceptibles d'être automatisés.

Même si l'intérêt de l'automatisation dans la cybersécurité est reconnu, son déploiement varie fortement selon les industries et les pays [3]. Par exemple, le déploiement de l'automatisation en France est nettement plus faible que dans des pays au développement similaire, avec près de la moitié des personnes interrogées travaillant dans des organisations sans automatisation déployée [3]. En particulier, seuls 14% des personnes interrogées pour le baromètre 2021 du CESIN [5] déclarent avoir une solution d'orchestration et automatisation de la réponse à incidents (SOAR) en place dans leur entreprise. À minima, on peut donc constater un potentiel pour une augmentation de l'automatisation de la cybersécurité dans certaines industries et certains pays, ce qui semble être confirmé par le fait qu'1 personne interrogée sur 4 [4] identifie le "manque de technologies avancées telles que l'automatisation" comme un défi pour améliorer la cyber-résilience. Cependant, ce n'est pas seulement une question d'adoption, mais aussi une question de développement de solutions nouvelles et plus efficaces. Ce dernier point est confirmé par l'écart existant entre le niveau de satisfaction inférieur des projets d'automatisation antérieurs par rapport au niveau de satisfaction anticipé des projets en cours [8]. Il est également motivé par le développement de nouvelles réglementations (telles que le RGPD, la loi chinoise sur la sécurité d'Internet et le cadre de confidentialité de l'APEC) qui, selon près de 3 personnes interrogées sur 4 [7], influencent l'adoption de l'automatisation.

Dans ce contexte, C&ESAR sollicite des soumissions présentant des états de l'art ou de la pratique clairs, des solutions innovantes ou des retours d'expérience pertinents sur le thème de "l'automatisation de la cybersécurité".

L'appel à contributions couvre:

— toutes les étapes de la cybersécurité, du DevSecOps à la cyberdéfense opérationnelle ou au pentesting;
— tous les types de produits ou contextes, y compris par exemple: réseaux, systèmes embarqués, systèmes industriels, IoT, Edge computing, ...;
— tous les niveaux d'automatisation, de l'automatisation partielle à l'automatisation complète (à condition qu'une plus-value évidente soit fournie par la partie automatisée).

Les sujets incluent (sans s'y limiter) ceux mentionnés ci-dessus et ci-dessous:

— impact sociétal de l'automatisation;

— vie privée et propriété intellectuelle dans un contexte automatisé;
— automatisation des processus fédérés (publication et intégration de la cyber-intelligence, défense et réponse fédérées, ...);
— interaction humain/machine dans un contexte d'automatisation partielle: pré-traitement automatique des processus manuels, sélection manuelle des processus automatiques, itération des processus mêlant humain et machine, entrées manuelles pour processus automatiques, validation manuelle des processus automatiques, retour (feedback) vers l'humain, ...;
— vérification et validation de l'automatisation;
— ...

Références

[1] Deloitte, « Future of cyber », Deloitte, 2020. [En ligne]. Disponible sur: 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. [En ligne]. Disponible sur: 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, juill. 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. [En ligne]. Disponible sur: https://www.ibm.com/security/data-breach.

[4] IBM Security, « Cyber Resilient Organization Report », IBM Corporation, juill. 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. [En ligne]. Disponible sur: https://www.ibm.com/account/reg/us-en/subscribe?formid=urx-45839.

[5] OpinionWay, « Baromètre de la cyber-sécurité des entreprises », OpinionWay, Rapport CESIN, janv. 2021. Sponsored by CESIN. [En ligne]. Disponible sur: 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. [En ligne]. Disponible sur: 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, févr. 2020. Sponsored by DomainTools. [En ligne]. Disponible sur: 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, mai 2020. Sponsored by Swimlane. [En ligne]. Disponible sur: https://www.sans.org/reading-room/whitepapers/analyst/2020-automation-integration-survey-39575.

Processus de soumission

C&ESAR sollicite deux types de communications :

- ***Article régulier*** (regular paper) : communication de ***8 à 16 pages*** décrivant des travaux non encore publiés ;
- ***Résumé étendu*** (extended abstract) : résumé de ***3 à 6 pages*** d'une communication pédagogique à large audience publiée récemment dans une revue ou les actes d'un congrès avec comité de lecture (les publications concernées inclues en particulier : les états de l'art ; les états de la pratique ; les enquêtes et sondages ; les retours d'expériences ; et les solutions directement applicables à des problématiques courantes).

Déroulé

- *Première phase*: les ***propositions (3 à 6 pages pour les deux types de communication)*** doivent être soumises sous forme de fichier PDF au plus tard le ***28 Mai 2021*** via https://easychair.org/conferences/?conf=cesar2021. Chaque soumission doit inclure un titre, les noms et affiliation des auteurs, l'adresse e-mail de l'auteur correspondant, un résumé (10 lignes max.), et une liste de mots-clés. Les auteurs seront informés de l'acceptation de leur proposition le *3 Septembre 2021*.
  - Les propositions de communication de type ***résumé étendu*** doivent : être clairement identifiées par la mention "résumé étendu" ou "extended abstract" dans leur titre ; clairement identifier et citer la publication originale résumée ; et contenir une annexe (en plus des 3 à 6 pages) contenant les retours (anonymisés) effectués par les relecteurs de la publication originale résumée.
- *Deuxième phase*: les auteurs des articles acceptés doivent envoyer la version finale de leur article avant le ***1er Octobre 2021*** à contact@cesar-conference.org, cc à cesar2021@easychair.org. Les auteurs s'engagent à répondre aux commentaires des relecteurs dans la version finale.

Langue et critères de sélection

Les articles sont rédigés en français ou en anglais (si l'article est en français, il doit être accompagné d'une traduction en anglais de son titre et résumé).

Pour les deux types de communication, les critères de sélection incluent en particulier : la clarté ; la dimension pédagogique ; et le respect du thème et des instructions de cet appel à contributions.

Pour les ***articles réguliers***, les communications très techniques ou très spécialisées sont les bienvenus si elles contribuent à expliquer et analyser l'état de l'art ou de la pratique et leurs lacunes.

Pour les ***résumés étendus***, la publication originale doit être clairement identifiée et citée. En outre, le processus de sélection est plus relevé, et met un focus particulier sur l'aspect pédagogique et l'audience large des communications.

Instructions pour le format des propositions et articles

Les propositions et articles en version finales doivent être soumis sous forme de fichiers PDF sans numérotation des pages, en respectant le format des "CEUR Workshop Proceedings" (http://ceur-ws.org/).

Des patrons sont disponibles pour les formats LaTeX, docx (Word) et ODT (Word et LibreOffice) à l'adresse suivante : http://ceur-ws.org/Vol-XXX/CEUR ART.zip.

Un patron est disponible pour Overleaf (LaTeX) à l'adresse suivante : https://www.overleaf.com/project/5e76702c4acae70001d3bc87. Il doit être dupliqué dans un nouveau projet pour être édité.

Publication des actes

Dans la mesure du possible, les actes de la conférence seront formellement publiés en tant que "CEUR Workshop Proceedings" (http://ceur-ws.org/). Cette publication est conditionnée par le respect des contraintes de cet éditeur (http://ceur-ws.org/HOWTOSUBMIT.html), en particulier le respect du format et une majorité d'articles en anglais.

Dans le cas où seul un sous-ensemble des articles peut être formellement publié en tant que "CEUR Workshop Proceedings", une sélection d'articles sera **potentiellement** effectuée pour former les actes officiels de la conférence qui seront publiés sous ce format. La décision d'inclusion dans cette sélection pour former les actes officiels est à la discrétion des éditeurs des actes et s'appuie entre autre sur les recommandations suivantes :

- les articles en anglais respectant scrupuleusement le format "CEUR Workshop Proceedings" sont inclus ;
- les articles en français respectant scrupuleusement le format "CEUR Workshop Proceedings" sont **potentiellement** inclus ;
- les articles ne respectant pas le format "CEUR Workshop Proceedings" ne sont pas inclus.

Les articles acceptés pour présentation à la conférence, mais ne faisant pas partie des actes officiels de la conférence (tous les articles si il n'y a pas d'actes publiés au format "CEUR Workshop Proceedings"), sont publiés sur le site Web de la conférence C&ESAR.

Dans la mesure du possible, l'indexation des articles dans DBLP et Google Scholar est facilitées.

Principales dates

- Soumission des *propositions* (3 à 6 pages): 28 Mai 2021
- Notification aux auteurs: 3 Septembre 2021
- Version finale : 1er Octobre 2021
  - 8 à 16 pages pour les *articles réguliers*
  - 3 à 6 pages pour les *résumés étendus*
- European Cyber Week (ECW): Mardi 16 Novembre 2021 au Jeudi 18 Novembre 2021

Comité de programme

- Erwan ABGRALL (CALID)
- José ARAUJO (ANSSI)
- Christophe BIDAN (Central-Supélec)
- 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)
- 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)

Partenaires

FIGURE 1 – Liste des partenaires