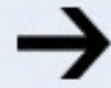


# CYBERSECURITY SKILLS JOURNAL

**Idea**



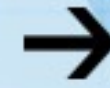
**Attend  
Workshop**



**Submit an  
Abstract**



**Get Assigned  
a Team**



**Get  
Published**



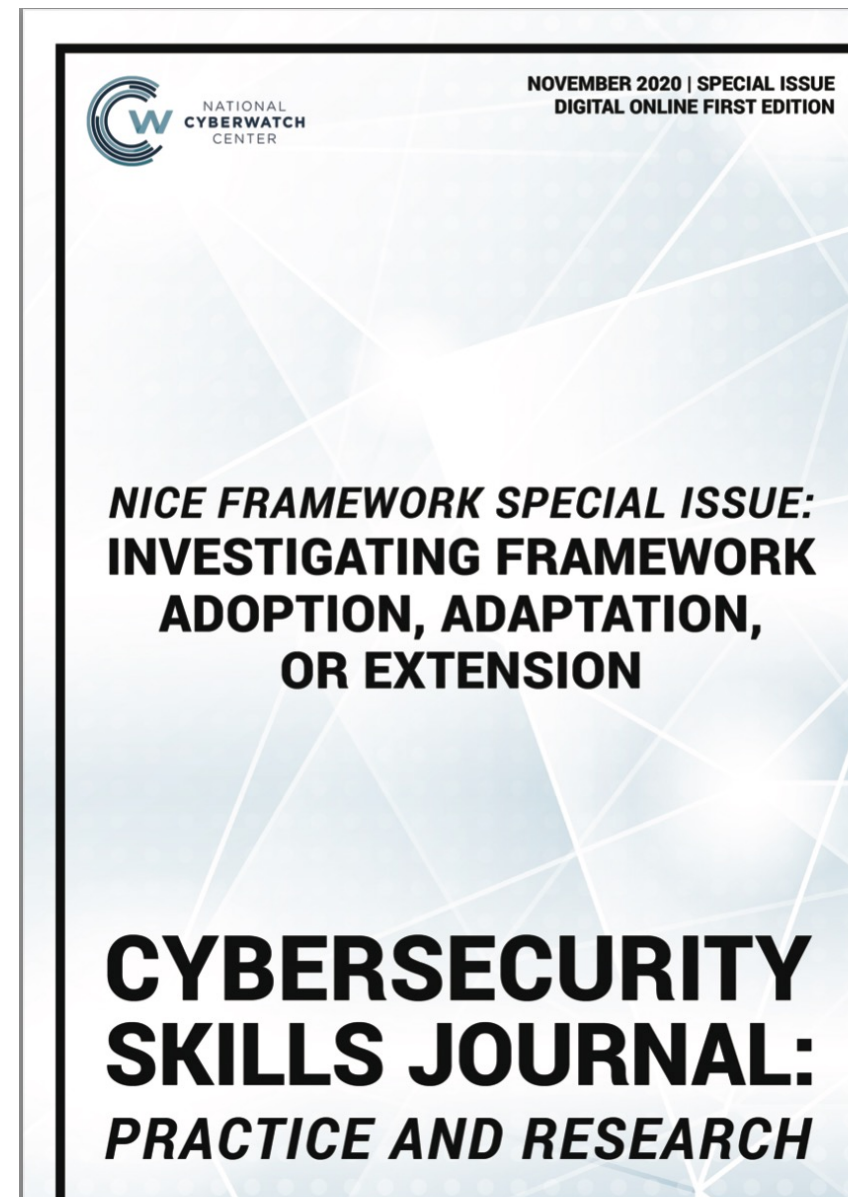
**Developing Dialogues for the NICE Special Issue**

1. About CSJ, NICE Special Issue & Focus Groups – *3 min*
2. How to propose a Focus Group Session – *5 min*
3. Using Google Scholar to find “research relatives” for your proposed research questions – *7 min*
4. Hands On Proposal Development Example - *30 min*
  - i. Do a Google Scholar search on your draft research questions – *5 min*
  - ii. Introduce yourself, share title/concept of your presentation; discuss Google Scholar search results – *5 min / person*
5. Submitting proposals to *CSJ* – *2 min*

# CSJ and the NICE Framework Special Issue series

Studies that examine the usefulness, benefits, and challenges associated with the adoption, adaptation, or extension of the NICE Framework to improve learning and advance the state of cybersecurity capability maturity.

- [Call for Proposals - Special Issue: NICE Framework, vol. 2](#)
- [Special Issue: NICE Framework, vol. 1](#) published in 2020
- Digital release of NICE SI vol. 2 planned for September 2023





# Types of Manuscripts Published by CSJ

## Dialogue

- Planning a study
- Discussion of specific questions related to problem
- Gather data for systematic study
- Opinions & experiences of stakeholders
- Not peer reviewed



## Note

- Proposed or early stage of study
- Documents design of systematic study
- Structured Abstract format required
- Peer reviewed



## Study (Article)

- Study is complete
- Reports early findings or outcomes from systematic study
- Supports replication of study
- Structured Abstract format required
- Peer reviewed

More details in the CSJ Overview: <https://bit.ly/csj-overview>

## How do Focus Groups fit in?

Focus Groups seek to discover common themes and ideas for future systematic study

- Not a panel presentation with speakers presenting data or slides – but a roundtable discussion, with both key invited guests and attendees responding to all questions
- Transcripts of Facilitated Virtual Focus Group sessions may be submitted to *CSJ* for publication as Dialogues (see slide at end)
  - Learn more about CSJ Focus Group proposals and Dialogues:  
<https://bit.ly/CSJ-dialogues>

Exchange of ideas between subject matter experts and stakeholders  
–***highlighting different points of view, experiences and expertise*** – on a problem or area within the human factors of cybersecurity.

- There may or may not be any prior substantive and rigorous evidence-based research about this problem within the arena of cybersecurity.
- Discussion of ideas, methods, or approaches, with supporting statements and observations from all participants rather than facts of an investigation.
- Ideal opportunity for data collection or crowdsourcing plans: brainstorming, collecting ideas and suggestions, experiences, anecdotal “what worked here” stories



# Facilitated Virtual Focus Groups

Call for Proposals:

*Facilitated Virtual Focus Group Event for NICE Special Issue*

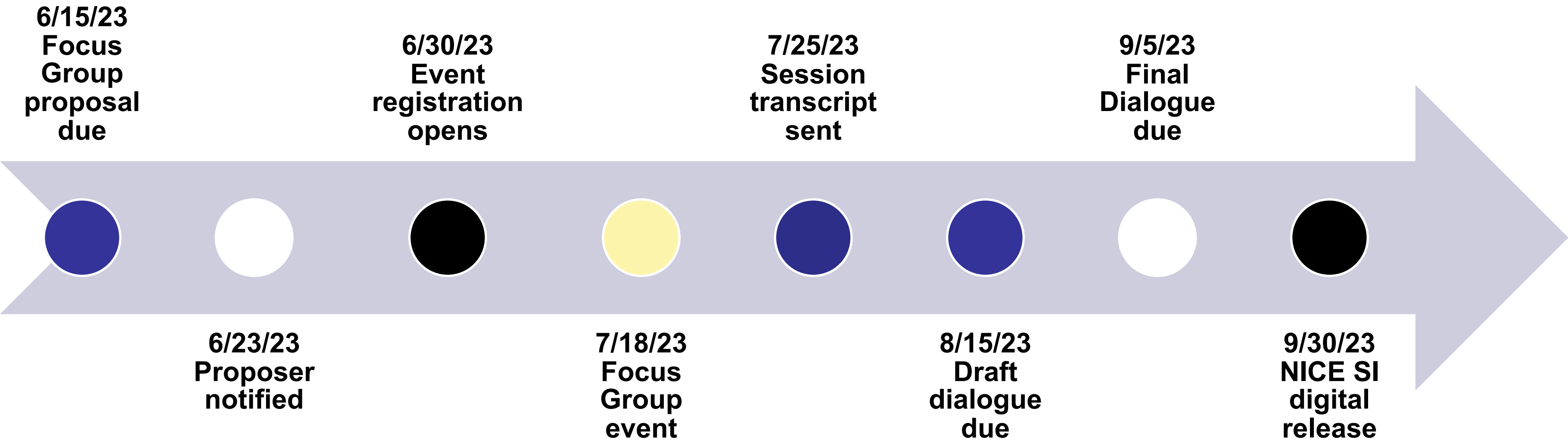
*< be sure to read the downloadable PDF! >*

*Focus Group Event will be on July 17, 2023*

Seeking ideas for discussion on research questions related to any ***challenges, opportunities, or effective practices*** related to the NICE Workforce Framework

Particular focus on the human factors of cybersecurity; CSJ does not accept submissions about technical solutions that lack a substantive contribution for improving or teaching skilled performance

# Focus Group Timeline





## Proposing ideas to *CSJ*

*CSJ* does not ask for a completed paper, or draft, or even an outline.

All initial submissions require 3 parts designed to help you explain your idea:



# Focus Groups and Dialogues: The Problem

**Problem:** What is the primary problem being explored in the Dialogue? Please address the following questions when framing your problem statement:

- **Why:** Why is this an urgent and/or severe problem? Why does it need study?
- **When:** When did this become a problem? (brief historical references add to understanding.)
- **How:** How is this problem related to workforce capability? How might solving this problem improve the capabilities or education of cybersecurity practitioners?
- **Who:** Which practitioners, researchers, or educators are being impacted by this problem?

# Focus Groups and Dialogues: The Questions

**Questions.** Identify 2-5 "how" or "why" type questions related to the core problem that this dialogue will explore with key stakeholders.

Considering these points may help identify the primary and secondary questions for a dialogue:

- What questions have not been answered by prior investigations of the problem?
- Why are practitioners or prior systematic investigations lacking an understanding of the problem or issue?
- Is information needed to address the problem missing or unknown?
- How might different factors contribute to different perspectives on the problem?



# Focus Groups and Dialogues: the Contribution

**Contribution.** What is the potential contribution of this discussion to the broader conversation, e.g., recent research and published articles, blog posts, conference presentations, etc.?

- Identify who else is “talking” about the problem,
- Identify your identified participants who will be responding to the questions and who represent key stakeholders for this problem. Provide a brief bio (250 words) for each of these stakeholders.
- Describe the summary goals of this Dialogue, including any insights regarding how the outcomes might adapt, extend or modify the contributions of others.





# Focus Groups and Dialogues: Proposal

**Implications for Practice.** What advances in cybersecurity workforce capabilities are implied? Why or how is the study advancing cybersecurity workforce capabilities? What specific workforce roles or practitioner communities will benefit?

**Implications for Future Research.** What advances in research are implied or new questions might be raised which future research should investigate? What new investigations are suggested by the findings?

**Expected Outcomes.** What positive outcomes do you believe will be a result of the discussion?

Note: you may not have these details at the time of proposal, but they must be included in any Dialogue submitted for publication.

# Hands On: Drafting research questions

Develop one or more “researchable” questions answerable by presenting evidence

Begin your question with “how,” “when,” “where,” or “why”

Examples

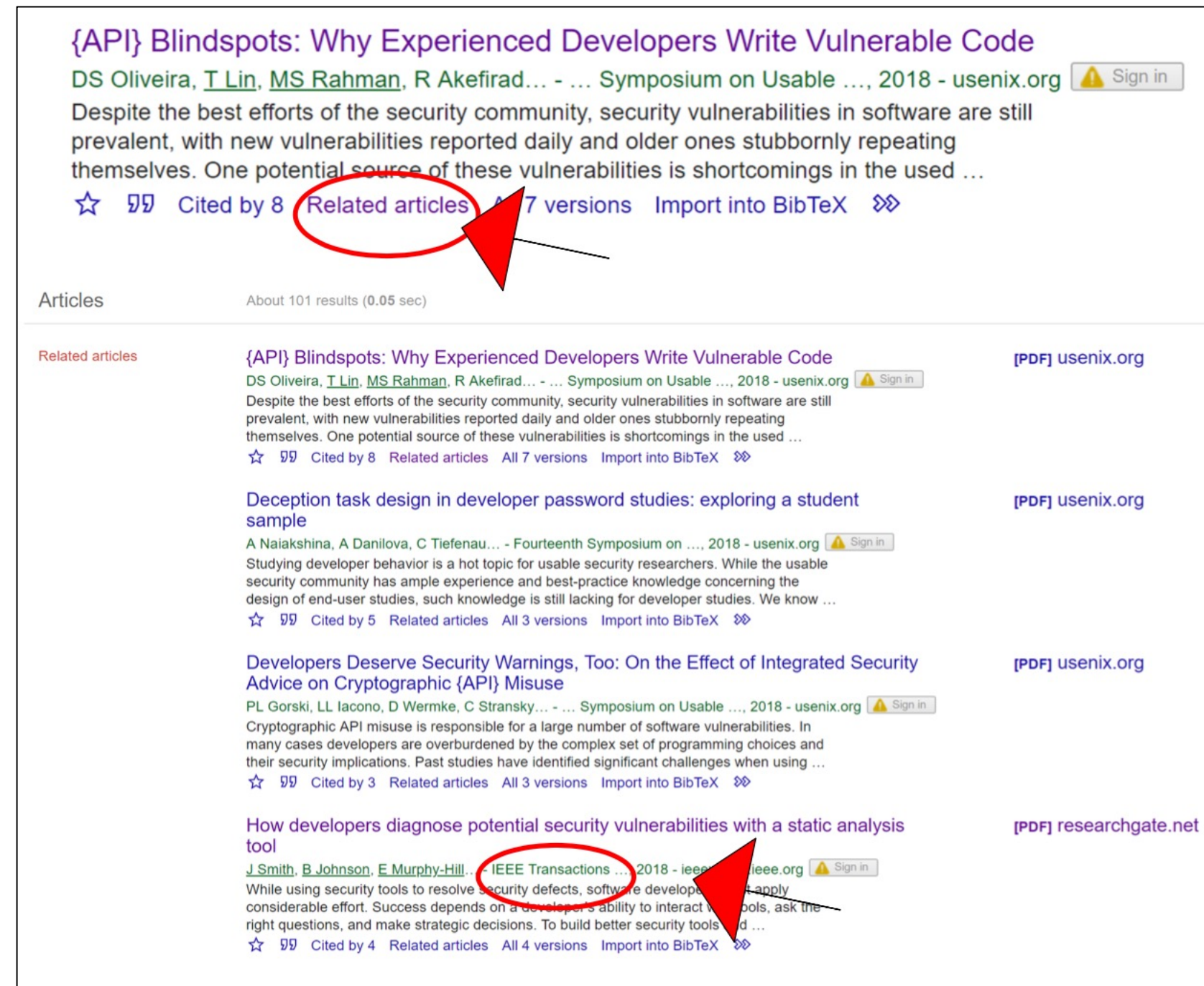
- Why do developers still write code with buffer overflows?
- How do we teach secure coding to experienced developers?

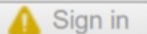
Tip: use the Research Proposal Form template from Google Drive:

[http://bit.ly/Paper\\_Proposal\\_Template](http://bit.ly/Paper_Proposal_Template)




# Hands-On: Identify the conversation

1. Locate a “salon” by pasting your initial research questions into Google Scholar  
<https://www.google.com/scholar>
2. Look for relevant articles published in last 5 years; select a Custom Date Range
3. Prefer conference or journal publications to books
4. Click “Cited by” and “Related Articles” links  
Note terms used, authors that repeatedly appear
5. Check out 2nd page of results!
6. Locate at least three potential “conversants”
7. Iterate searching and revising Problem, RQ and Contribution until they fit together




{API} Blindspots: Why Experienced Developers Write Vulnerable Code  
DS Oliveira, T Lin, MS Rahman, R Akefirad... - ... Symposium on Usable ..., 2018 - usenix.org 

Despite the best efforts of the security community, security vulnerabilities in software are still prevalent, with new vulnerabilities reported daily and older ones stubbornly repeating themselves. One potential source of these vulnerabilities is shortcomings in the used ...



☆  Cited by 8 **Related articles**  All 7 versions Import into BibTeX 


Articles About 101 results (0.05 sec)

Related articles


{API} Blindspots: Why Experienced Developers Write Vulnerable Code [PDF] usenix.org  
DS Oliveira, T Lin, MS Rahman, R Akefirad... - ... Symposium on Usable ..., 2018 - usenix.org 

Despite the best efforts of the security community, security vulnerabilities in software are still prevalent, with new vulnerabilities reported daily and older ones stubbornly repeating themselves. One potential source of these vulnerabilities is shortcomings in the used ...

☆  Cited by 8 Related articles All 7 versions Import into BibTeX 



Deception task design in developer password studies: exploring a student sample [PDF] usenix.org  
A Naiakshina, A Danilova, C Tiefenau... - Fourteenth Symposium on ..., 2018 - usenix.org 


Studying developer behavior is a hot topic for usable security researchers. While the usable security community has ample experience and best-practice knowledge concerning the design of end-user studies, such knowledge is still lacking for developer studies. We know ...

☆  Cited by 5 Related articles All 3 versions Import into BibTeX 



Developers Deserve Security Warnings, Too: On the Effect of Integrated Security Advice on Cryptographic {API} Misuse [PDF] usenix.org  
PL Gorski, LL Iacono, D Wermke, C Stransky... - ... Symposium on Usable ..., 2018 - usenix.org 

Cryptographic API misuse is responsible for a large number of software vulnerabilities. In many cases developers are overburdened by the complex set of programming choices and their security implications. Past studies have identified significant challenges when using ...

☆  Cited by 3 Related articles All 3 versions Import into BibTeX 

How developers diagnose potential security vulnerabilities with a static analysis tool [PDF] researchgate.net  
J Smith, B Johnson, E Murphy-Hill... - IEEE Transactions ..., 2018 - ieee.org 

While using security tools to resolve security defects, software developers must apply considerable effort. Success depends on a developer's ability to interact with tools, ask the right questions, and make strategic decisions. To build better security tools and ...

☆  Cited by 4 Related articles All 4 versions Import into BibTeX 

## Hands on Activity

**Google Scholar search of a question (see prior slide) – 5 min**

**Discussing results and suggested next steps – 5 min per person**

We suggest using Zoom chat to share  
your name, organization, and initial research question –  
you may find a proposal partner or invited experts for your proposal!



**Submit your idea for a NICE SI Focus Group by June 15, 2023**

**<https://easychair.org/conferences/?conf=csjoc2023>**

## **Track 1 Dialogues**

Questions?

Contact us at:

**[csjeditors@nationalcyberwatch.org](mailto:csjeditors@nationalcyberwatch.org)**

# Publishing your Focus Group as a Dialogue

1. Transcript of discussion – the Dialogue questions and bio statements of key invited guests of a Focus Group, or Dialogue participants
2. Write an introduction based on your proposal
  - State the Problem and motivation for the Dialogue
  - Identify Questions to be explored
  - Anticipated goals of the session
3. Write a conclusion summarizing the discussion
  - Any common themes, reactions, responses or conclusions
  - New questions, “next step” ideas or solutions that may have come up
  - Was the problem / challenge even more complicated?  
Did a lengthy discussion / different perspectives on a particular question / issue take more time than anticipated?



## Additional potential Focus Group ideas

What are challenges for adopting a skills framework like the NICE Framework? How might future research be designed help to address those challenges?

How might existing research into the impact of <<specific critical societal or global issues >> on U.S. workforce be applied to identify the impact on the cybersecurity workforce? How might we develop and collect relevant metrics on the impact of those issues on the cybersecurity workforce?

How might methods used in other domains to obtain insights into employer needs be applied to cybersecurity and the NICE Workforce Framework?

How might you, or your organization, obtain insights into employer needs and apply them in adapting or adopting the NICE Workforce Framework? How might you measure what was effective and what was not effective?

How might recommendations or best practices from other domains be applied to help facilitate broader participation in responding to cybersecurity workforce challenges such gathering workforce data, identifying standard curriculum, curating best practices, communication channels, hiring, etc.

How might the cybersecurity community understand and apply evidence-based practices to improve workforce (and cybersecurity) outcomes based on models from other domains, e.g., clinical medicine, the FAA Incident Reporting System, etc.



## Additional potential Focus Group ideas

How do YOU (your industry or workrole) find out about leading practices? What challenges do you experience? How might the disseminate of information be improved (efficiency, ease, speed)?

How do YOU (your industry, your workplace or workrole) define effective practices defined? What challenges do you experience in defining, or measuring effective practices

How does the NICE Framework relate to or is in use with other related skills frameworks? How might this be improved?

What are emerging areas – how might the NICE Framework plan for and incorporate those?

Are there ways that research can support the integration of successful learning practices across education, training, and workforce development?