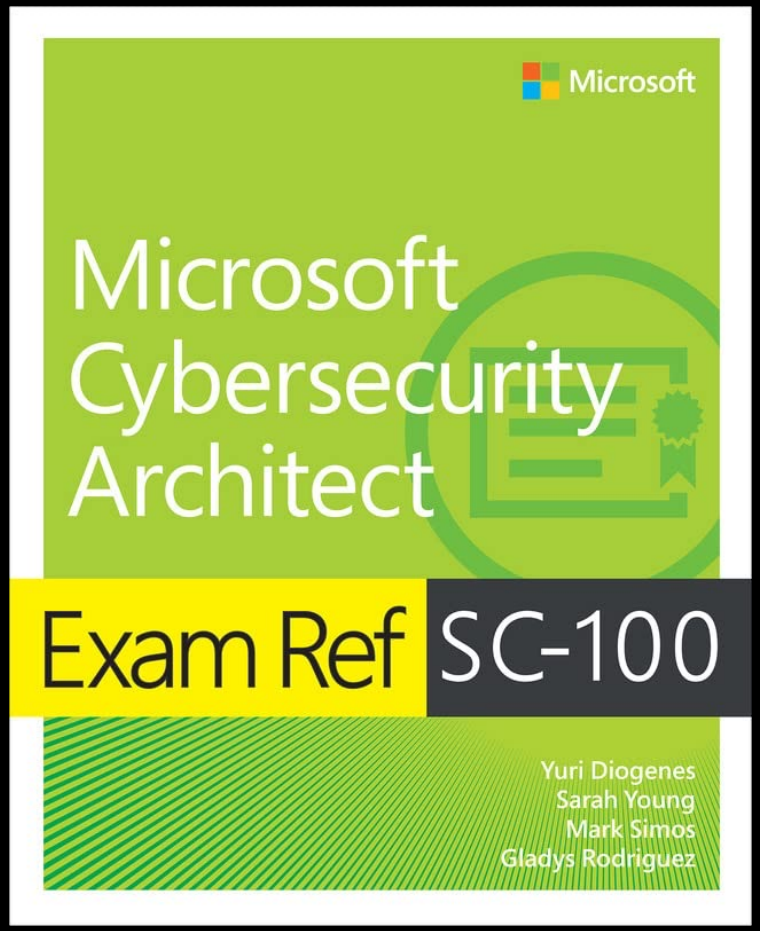
Security advocacy shouldn't be for security professionals: an analysis of how the industry misses the mark and how we can improve

Sarah Young

whoami

- Senior Cloud Security Advocate @ Microsoft.
- Based in Melbourne.
- Prolific meme user.
- Dog mum x 2

@_sarahyo
@sarahyo.com



The Azure Security Podcast

@_sarahyo
@sarahyo.com

Agenda

- In the beginning
- A level set on content and content creators
- Confusing content creation principles
- My research analysis
- How do we fix this?
- The challenges of scale

@_sarahyo
@sarahyo.com

In the beginning...

- Security people started creating things.

@_sarahyo
@sarahyo.com

In the beginning...

- Security people started creating things.
- Interesting, but only for other security professionals.

@_sarahyo
@sarahyo.com

In the beginning...

- Security people started creating things.
- Interesting, but only for other security professionals.
- But, security affects everyone.

@_sarahyo
@sarahyo.com

In the beginning...

- Security people started creating things.
- Interesting, but only for other security professionals.
- But, security affects everyone.
- As an industry we don't write content for everyone.

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

- Online documents

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

- Online documents
- Training material

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

- Online documents
- Training material
- Videos

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

- Online documents
- Training material
- Videos
- Blog posts

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

- Online documents
- Training material
- Videos
- Blog posts
- Podcasts

@_sarahyo
@sarahyo.com

A level set on content

As an industry we don’t write content for everyone. What is “security content”?

- Online documents
- Training material
- Videos
- Blog posts
- Podcasts
- i.e. any consumable media

@_sarahyo
@sarahyo.com

A level set on content creators

- Who do we normally think are content creators?

@_sarahyo
@sarahyo.com

A level set on content creators

- Who do we normally think are content creators?

- Developer relations / advocates

@_sarahyo
@sarahyo.com

A level set on content creators

- Who do we normally think are content creators?

- Developer relations / advocates
- Content creators

@_sarahyo
@sarahyo.com

A level set on content creators

- Who do we normally think are content creators?

- Developer relations / advocates
- Content creators
- Engineers

@_sarahyo
@sarahyo.com

A level set on content creators

- Who do we normally think are content creators?

- Developer relations / advocates
- Content creators
- Engineers
- Technical writers

@_sarahyo
@sarahyo.com

A level set on content creators

- Who do we normally think are content creators?

- Developer relations / advocates
- Content creators
- Engineers
- Technical writers

- … essentially, it can be anyone.

@_sarahyo
@sarahyo.com

Let’s look at some content creation principles

@_sarahyo
@sarahyo.com

Content creation principles are confusing

- It should position you as an industry thought leader.
- Creating content for everyone is creating content for no one.

@_sarahyo
@sarahyo.com

Content creation principles are confusing

- It should position you as an industry thought leader.
- Creating content for everyone is creating content for no one.

- Good content is concise.
- Good content is meaningful and accessible.

@_sarahyo
@sarahyo.com

The expert problem

- The more you know, the worse you are at explaining something.

@_sarahyo
@sarahyo.com

The expert problem

- The more you know, the worse you are at explaining something.
- Knowledge is assumed.

@_sarahyo
@sarahyo.com

The expert problem

- The more you know, the worse you are at explaining something.
- Knowledge is assumed.
- Experts must always be deferred to.

@_sarahyo
@sarahyo.com

The expert problem

- The more you know, the worse you are at explaining something.
- Knowledge is assumed.
- Experts must always be deferred to.
- Read up on crew resource management (CRM) in aviation for another take on this.*

@_sarahyo
@sarahyo.com

* See appendix A for details on CRM

The expert problem

- The more you know, the worse you are at explaining something.
- Knowledge is assumed.
- Experts must always be deferred to.
- Read up on crew resource management (CRM) in aviation for another take on this.*
- “Easy reading is damn hard writing” - Nathaniel Hawthorne

@_sarahyo
@sarahyo.com

* See appendix A for details on CRM

My scoring system

- Explains concepts with no prior assumption of knowledge.
- Summarises concise go dos / take action steps within the content.
- Can be implemented by one resource.
- Does not link to other resources in order to complete the activity being described.
- Can be consumed in under 1 hour.
- Uses plain language.

@_sarahyo
@sarahyo.com

My research analysis

- I divided my content into a few buckets:

My research analysis

- I divided my content into a few buckets:

.

My method

- I used search engines to find my content.

@_sarahyo
@sarahyo.com

My method

- I used search engines to find my content.
- A manual process. ☹

@_sarahyo
@sarahyo.com

My method

- I used search engines to find my content.
- A manual process. ☹
- I assessed ~200 pieces of content for my analysis.

@_sarahyo
@sarahyo.com

My method

- I used search engines to find my content.
- A manual process. ☹
- I assessed ~200 pieces of content for my analysis.
- To find content, the phrases I searched for were:

[Cyber] Security fundamentals

[Cyber] Security for beginners

[Cyber] Security how tos

[Cyber] Security basics

[Cyber] security essentials

@_sarahyo
@sarahyo.com

SA who writes the most cyber security content online?

There are many different types of sources that contribute to cybersecurity content online, and it is difficult to determine a single group that writes the most. Some of the most common sources of cybersecurity content include:

1. News outlets and journalists - These sources often cover breaking news related to cyber attacks and data breaches, as well as broader cybersecurity trends and issues.
2. Security vendors - As I mentioned earlier, security vendors often produce a significant amount of cybersecurity content, including product documentation, whitepapers, and blog posts.
3. Independent researchers - Many independent security researchers and bloggers share their insights and findings online, often through blog posts and social media.
4. Government agencies - National security agencies, such as the US Department of Homeland Security and the UK's National Cyber Security Centre, provide guidance and resources on cybersecurity issues.
5. Academic institutions - Researchers and academics at universities and other academic institutions often produce scholarly articles and reports on cybersecurity topics.

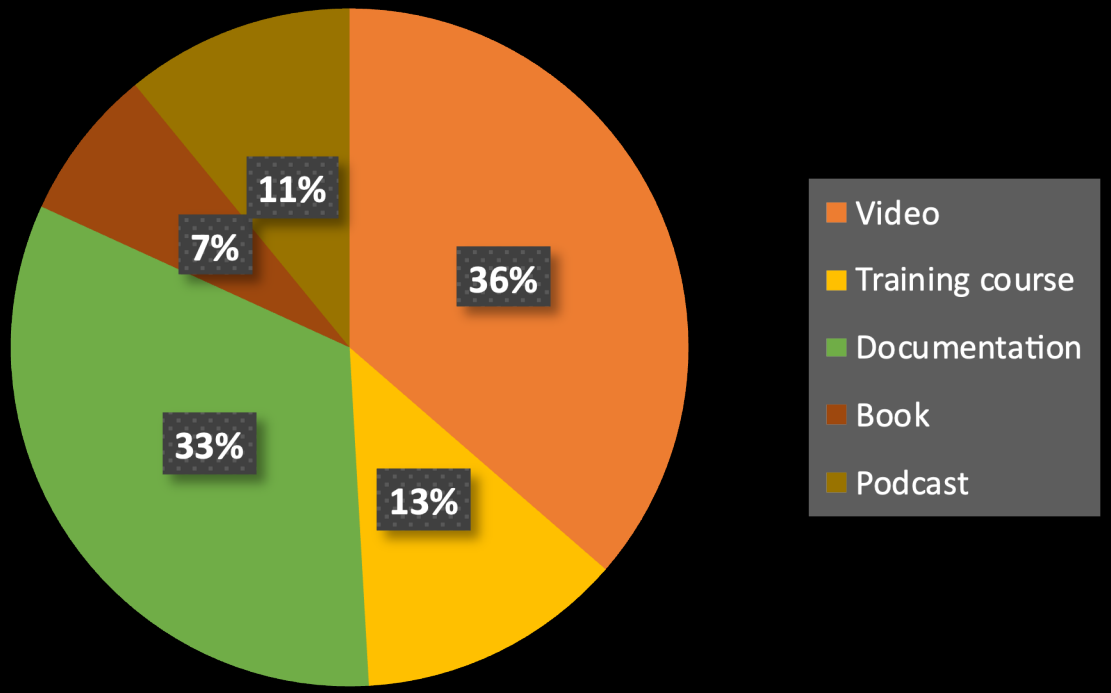
Overall, the landscape of cybersecurity content online is diverse and constantly evolving, with new voices and sources emerging all the time. It is important to approach online content with a critical eye, and to evaluate sources carefully in order to ensure the accuracy and relevance of the information presented.

@_sarahyo
@sarahyo.com

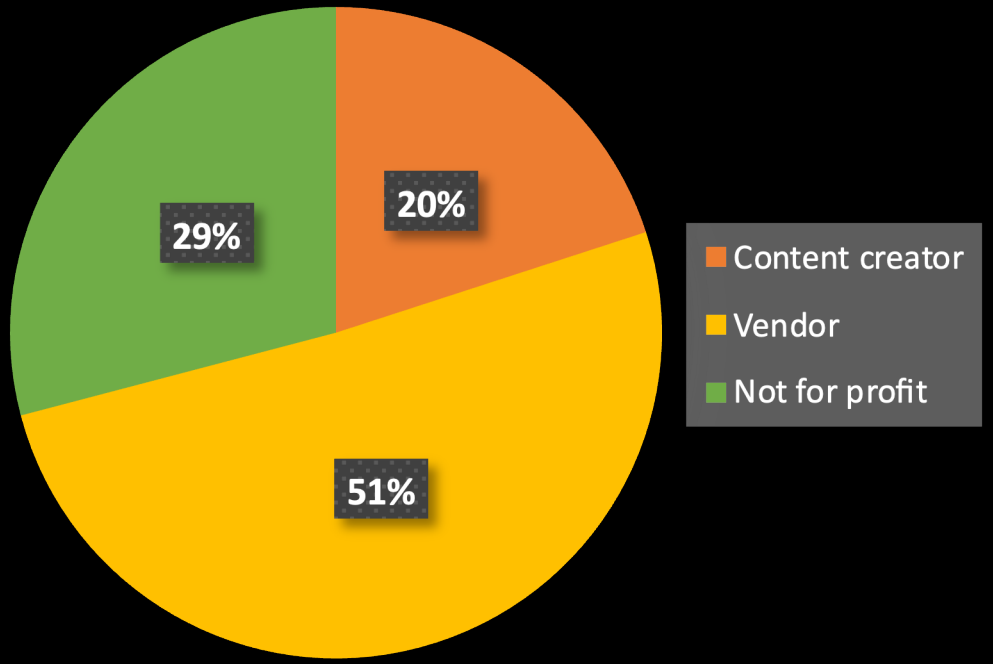
* See appendix B for full chat GPT response

Analysis results

Content I reviewed



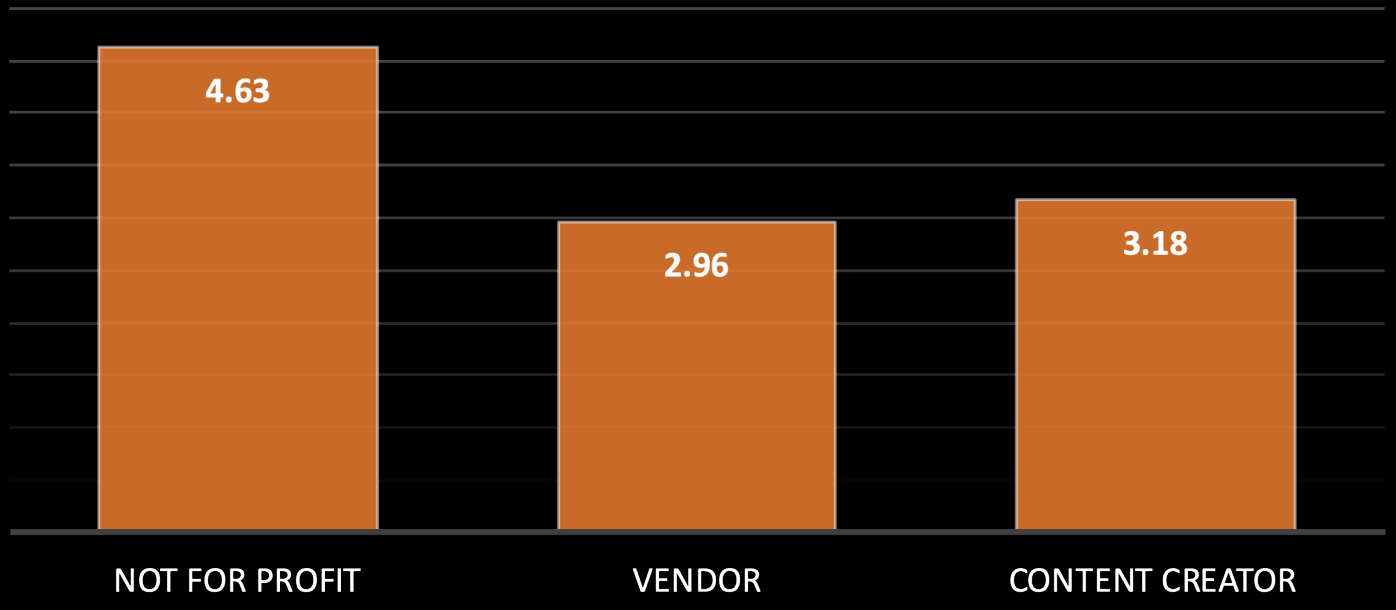
Types of creators



@_sarahyo
@sarahyo.com

Analysis results

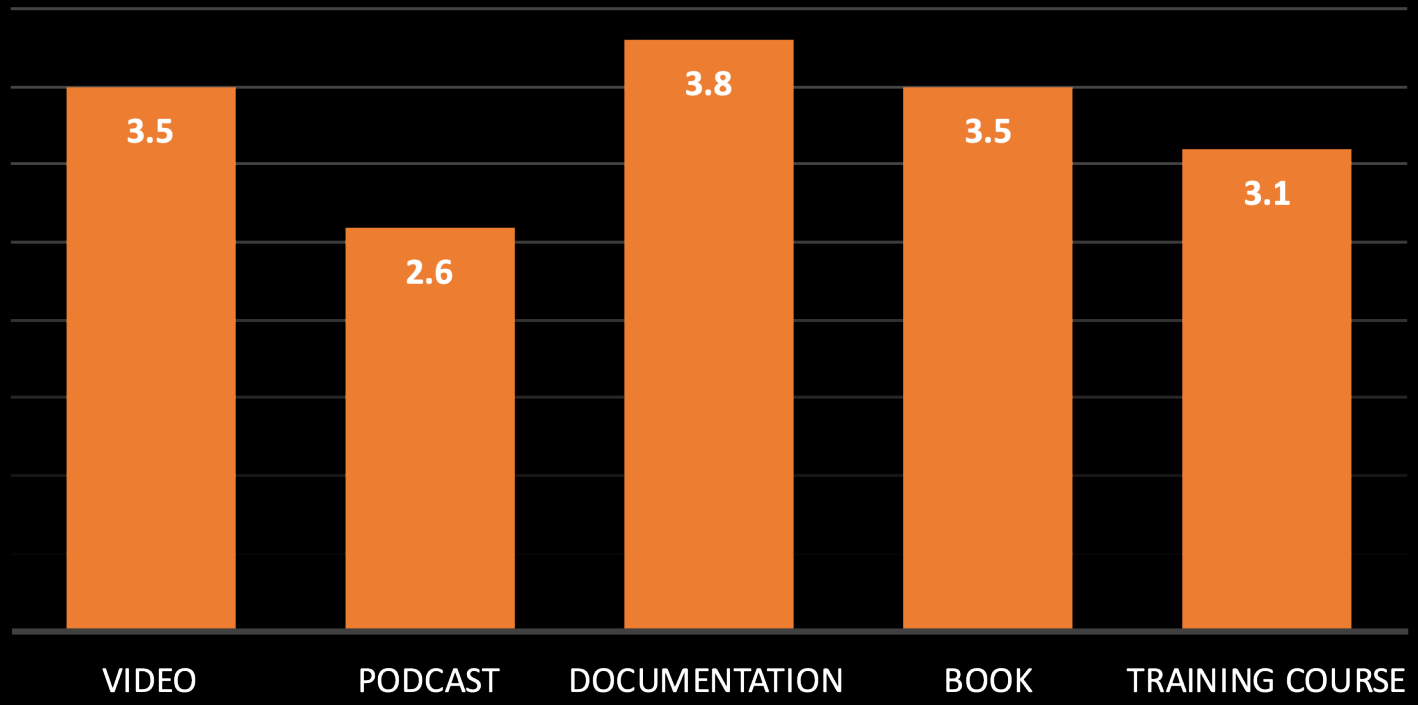
Average accessibility rating by creator type



@_sarahyo
@sarahyo.com

Analysis results

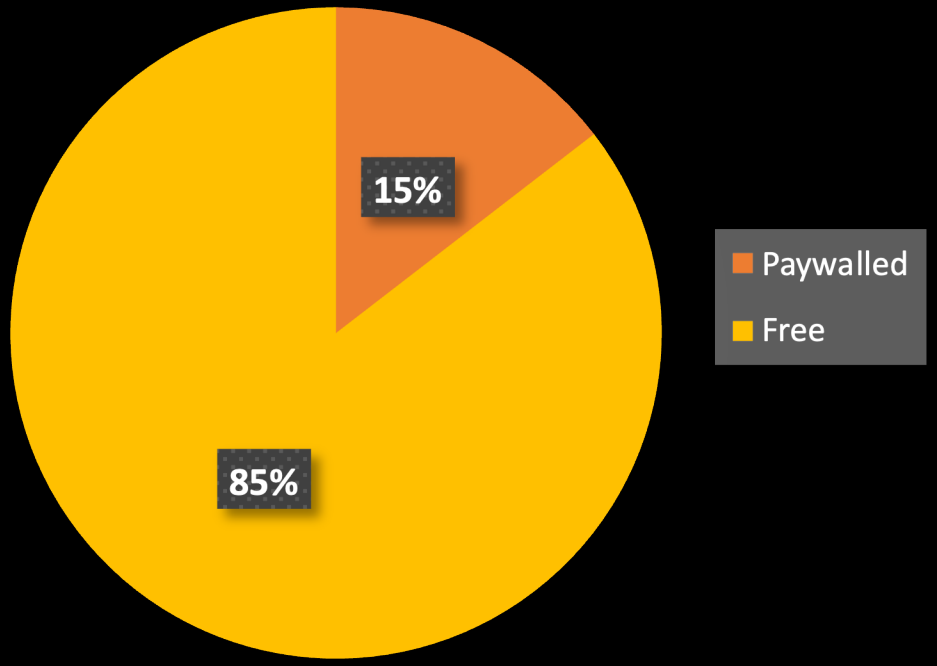
Average score by content type



@_sarahyo
@sarahyo.com

Analysis results

Proportion of paywalled content



@_sarahyo
@sarahyo.com

Let’s look at an example

@_sarahyo
@sarahyo.com

So, what do we do to fix this?

@_sarahyo
@sarahyo.com

Ask yourself these questions

- Can anyone consume this content and go and do the thing?

@_sarahyo
@sarahyo.com

Ask yourself these questions

- Can anyone consume this content and go and do the thing?

- Who is going to use this and for what purpose?

@_sarahyo
@sarahyo.com

Ask yourself these questions

- Can anyone consume this content and go and do the thing?
- Who is going to use this and for what purpose?
- Does an individual need to take a significant proportion out of their working day to consume this material?

@_sarahyo
@sarahyo.com

Ask yourself these questions

- Can anyone consume this content and go and do the thing?
- Who is going to use this and for what purpose?
- Does an individual need to take a significant proportion out of their working day to consume this material?
- Does this material have a clear start-middle-end or does it sprawl?

@_sarahyo
@sarahyo.com

Could my mum understand this?

Could a frontline worker understand this?

@_sarahyo
@sarahyo.com

Use TL;DR

TLDR is a common online abbreviation that stands for "Too Long Didn't Read." If that sounds a little rude or passive aggressive, you're aptly sensing one of its uses; that is often the way TLDR is used in response to densely worded articles online. While TLDR is the most common usage, you may also see the semicolon inserted in the acronym, as in: "TL;DR."

*https://www.businessinsider.com/guides/tech/tldr-meaning

@_sarahyo
@sarahyo.com

Use TL;DR

@_sarahyo
@sarahyo.com

Where would I start?

- Refactoring content is not easy.
- Target your most used/visited/downloaded content.
- It’s a journey!

@_sarahyo
@sarahyo.com

Where would I start?

- Refactoring content is not easy.
- Target your most used/visited/downloaded content.
- It's a journey!

@_sarahyo
@sarahyo.com

Where would I start?

- Refactoring content is not easy.
- Target your most used/visited/downloaded content.
- It’s a journey!

@_sarahyo
@sarahyo.com

My TL;DR of this presentation

- Security content is not written for the majority.

@_sarahyo
@sarahyo.com

My TL;DR of this presentation

- Security content is not written for the majority.
- Not for profits are stronger at creating more “accessible” content than other parts of industry.

@_sarahyo
@sarahyo.com

My TL;DR of this presentation

- Security content is not written for the majority.
- Not for profits are stronger at creating more “accessible” content than other parts of industry.
- We must change the way we create security content.

@_sarahyo
@sarahyo.com

My TL;DR of this presentation

- Security content is not written for the majority.
- Not for profits are stronger at creating more “accessible” content than other parts of industry.
- We must change the way we create security content.
- Use the TL;DR principle and ask “could my mum understand this?”

@_sarahyo
@sarahyo.com

My TL;DR of this presentation

- Security content is not written for the majority.
- Not for profits are stronger at creating more “accessible” content than other parts of industry.
- We must change the way we create security content.
- Use the TL;DR principle and ask “could my mum understand this?”
- Don’t be afraid to give definitive guidance.

@_sarahyo
@sarahyo.com

Your go dos

1. Review your organization’s security content: does it give concise and direct guidance that can be followed by non-security folks?

@_sarahyo
@sarahyo.com

Your go dos

1. Review your organization's security content: does it give concise and direct guidance that can be followed by non-security folks?

2. Create TL;DRs and / or clear steps for how to accomplish a task.

@_sarahyo
@sarahyo.com

Your go dos

1. Review your organization's security content: does it give concise and direct guidance that can be followed by non-security folks?

2. Create TL;DRs and / or clear steps for how to accomplish a task.

3. Talk about this challenge with your content creators: the first challenge is to become conscious of the issue.

@_sarahyo
@sarahyo.com

black hat ASIA 2023

Thank you, Black Hat Asia!

If you have any questions, feel free to reach out to me:

sarah.young@microsoft.com

@_sarahyo
@sarahyo.com

Appendix A

- Notable aviation accidents that have happened due to a failure of crew resource management (CRM)
- Air France 447
- Airblue 202
- The Tenerife airport disaster
- Asiana 214

Appendix B

Chat GPT response to “who writes cyber security content online and what proportion of the content do they create?”

The individuals and organizations who write cyber security content online vary widely, and the proportion of content that they create can depend on the specific source and the type of content being produced. However, here are some common groups and their contributions to cyber security content online:

1. Cybersecurity companies and vendors: These organizations often produce a significant amount of cyber security content online, including white papers, product documentation, blog posts, and other types of resources. While it is difficult to estimate the exact proportion of cyber security content they create, they are likely to be a significant source of content online.

2. Independent researchers and consultants: These individuals often contribute to cyber security content online, particularly in the form of blog posts and articles that share their research findings and expertise. While they may not produce as much content as larger organizations, they can provide valuable insights and perspectives on cyber security issues.

3. News outlets and journalists: News outlets and journalists often cover breaking news related to cyber attacks and data breaches, as well as broader cyber security trends and issues. While they may not produce as much content as other groups, their reporting can be an important source of information for the public.

4. Government agencies: National security agencies, such as the US Department of Homeland Security and the UK's National Cyber Security Centre, provide guidance and resources on cyber security issues. While their content may be more focused on policy and regulation than on technical details, it can be an important source of information for individuals and organizations seeking to improve their cyber security posture.

5. Academics and researchers: Researchers and academics at universities and other academic institutions often produce scholarly articles and reports on cyber security topics. While their content may be more technical and specialized than other types of cyber security content, it can be a valuable resource for individuals and organizations seeking to improve their understanding of cyber security issues.

Overall, the landscape of cyber security content online is diverse and constantly evolving, with many different groups contributing to the conversation in different ways. The proportion of content created by each group may vary depending on the specific topic and type of content being produced.