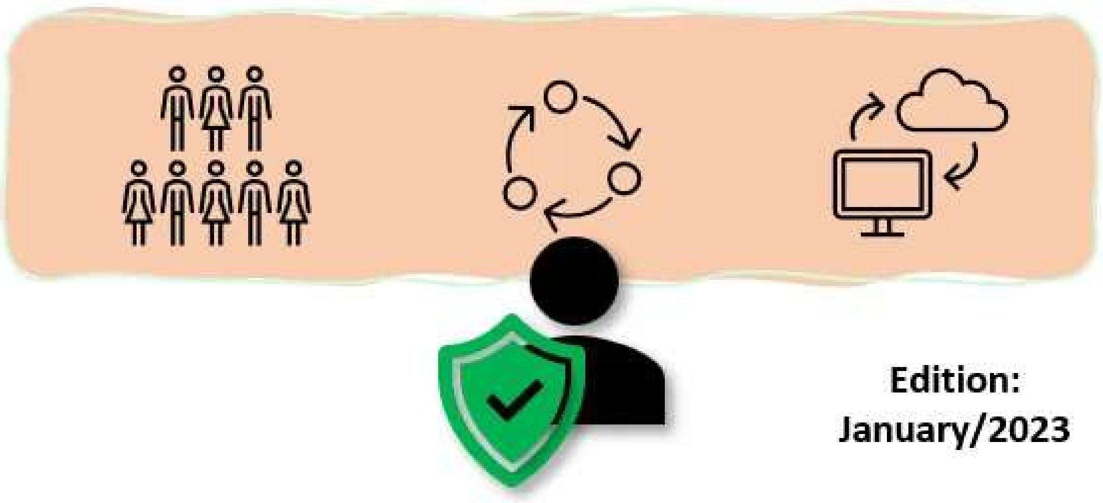
Strategic Cyber Security Report — January 2023 Edition

Andre Camillo, CISSP

Published in Geek Culture · 4 min read · Feb 6, 2023

A Monthly summary of Strategic Information for Cyber Security Leaders



This is a series spun from a need I identified when talking to CISOs — as explained on the kick-off article, this series follows the format of:

What's Top of mind in 3 domains: People, Processes, Technology for CISOs.

People

Microsoft Research 2022 year in Review

Microsoft published a blog post looking back at the advances its Research team has made in 2022 in the field of AI.

From our perspective (Cloud or Security), given how the subject gained worldwide headlines late last year, it's fair to be across the matter and how its development is being done in a responsible and safe manner.

And in this aspect, it's good to see "Responsible use of AI" as one of the highlighted Researches — something I alluded to in my previous article.

Here's the blog post on Microsoft's Research highlights of 2022.

World Economic Forum's Global Cyber Security Outlook Report 2023

A great document by the World Economic Forum.

The 2023 version of the yearly result is compared against 2022 and the findings are a good picture of what challenges Cyber leaders are facing — across talent shortage, addressing risks and strategic decision making and more. An excerpt from it reads:

> *the study indicates that business leaders are more aware of their organizations' cyber issues than they were a year ago. They are also more willing to address those risks. Nonetheless, cyber leaders still struggle to clearly articulate the risk that cyber issues pose to their organizations in a language that their business counterparts fully understand and can act upon. As a result, agreeing on how best to address cyber risk remains a challenge for organizational leaders.*

The public document can be found here.

Process

Forrester Wave Security Analytics Platform Report

Forrester released its Wave report on "Security Analytics Platform". These are solutions for the SOC (SIEM/SOAR).

Amongst the main findings, Forrester highlighted that it's seen that "Vendors Are Finally Putting The 'Security' Into Security Analytics Platforms" — Claiming some vendors are focusing on analyzing data than warehousing it.

They recommend looking for vendors that:

- **Prioritize depth over breadth**
- **Improve the analyst experience**
- **Have a unique product vision with a strong execution path**

Read more in Forrester's report, found here.

Some vendors have talked about it. Microsoft highlighted in a blog post its position. They highlighted the following:

> *Microsoft achieved the highest possible score in 17 different criteria, including partner ecosystem, innovation roadmap, product security, case management, and architecture.*

Find the Microsoft post here.

Microsoft Identity Security Trends for 2023

I'm a big fan of looking to the future, understanding what's next in a particular field, and reflect on how and what we want to follow next. It's a life choice, but also applies to tech!

January being the beginning of our calendar year — literally (see note below 😁) has techies talking about trends and what's next.

This time around I'm talking about trends in Microsoft Security Identity trends for 2023, this great blog post by the identity VP contains some bits of gold on the subject.

By looking back at popular identity attacks, it was possible to derive and define some trends to harden the area.

Quoting the document:

> *If I may be so bold as to propose some New Year's resolutions for your identity security efforts:*

> *1. Protect all your users with multifactor authentication, always, using Authenticator, Fast Identity Online (FIDO), Windows Hello, or CBA.*
>
> *2. Apply Conditional Access rules to your applications to defend against application attacks.*
>
> *3. Use mobile device management and endpoint protection policies — especially prohibiting running as admin on devices — to inhibit token theft attacks.*
>
> *4. Limit on-premises exposure and integrate your SOC and identity efforts to ensure you are defending your identity infrastructure.*
>
> *5. Bet hard on agility with a cloud-first approach, adaptable authentication, and deep commitments to automated responses to common problems to save your critical resources for true crises.*

Have a look at the document for more information.

Ps.: The word “January” actually originates from “the Latin noun use of Jānuārius, equivalent to Jānus.

In ancient Roman culture, Jānus was a god of doorways, beginnings, and the rising and setting of the sun. His name comes from the Latin jānus, meaning “doorway, archway, arcade.””

Technology

Identifying AI content

During my break, I spent some time playing around with new tech, different AIs such as Midjourney and OpenAI's ChatGPT.

And as always, I'm thinking of Information Security. With so much power available to us via this kind of technology, how do we know for sure whether we're reading/seeing/hearing something created by AI?

I reckon Content Validation is going to be massive in the coming years — both for Information Security and general population Safety.

Anything created by AI has the potential to be misused, and that's when I stumbled on this very interesting article written by Melissa Heikkilä about AI detection tools (specifically for text), a good read to understand what some start-ups like Hugging Face are tackling.

According to the article:

> *"AI is already fooling us. Researchers at Cornell University found that people found fake news articles generated by GPT-2 credible about 66% of the time."*

The article can be found here.

Learn more about my Cloud and Security Projects: https://linktr.ee/acamillo

Consider subscribing to Medium (here) to access more content that will empower you!

Thank you for reading and leave your thoughts/comments!

./references

Scattered throughout the document

Report Cloud Cybersecurity Strategy Leadership

Written by Andre Camillo, CISSP

Edit profile

1K Followers · Writer for Geek Culture

Cloud and Security technologies, Career, Growth Mindset. Follow: https://linktr.ee/acamillo .
Technical Specialist @Microsoft. Opinions are my own.

More from Andre Camillo, CISSP and Geek Culture