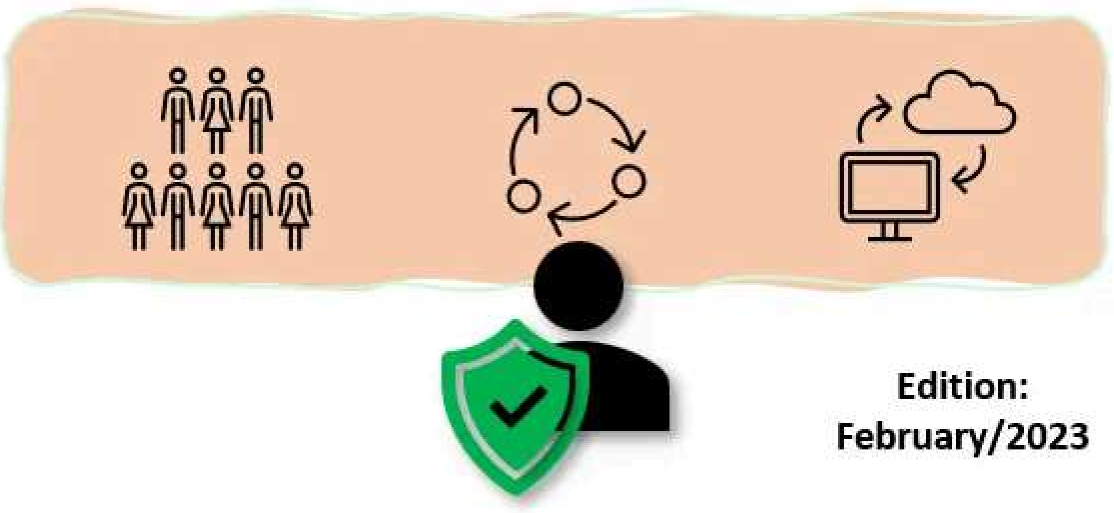
Strategic Cyber Security Report — February 2023 Edition

Andre Camillo, CISSP

Published in Geek Culture · 5 min read · Mar 1, 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

Global Cyber Security Outlook 2023

Or how leader of the segment are dealing with different challenges: Risk-Communication to board, Talent Shortage, Strategic Investment vs Day-to-day operations, and more.

It also puts the spotlight into how Business leaders view compare to Cyber (Security) leaders. An important aspect when thinking about themes such as:

- Geopolitical effects in Cyber Security,
- Law and regulations, (I recently wrote about this from a NZ/AU perspective)
- Cyber Resilience views,
- Supply-chain Risk,
- Cyber Insurance,
- Biggest Threats From the leader’s point of view
- and much more…

Graphical comparisons for each of those are provided for more impact.

A summary of the document according to chatGPT:

> *The 2023 Global Cybersecurity Outlook report shows that while business leaders are becoming more aware of cyber risks and are more willing to address them, they still struggle to fully understand the language used by cybersecurity leaders to articulate the risks. The report also found that cyber attackers are now more likely to focus on business disruption and reputational damage. There is a perception gap between business and cyber leaders' views on the importance of cyber-risk management, and many organizations are focusing more on day-to-day defenses than strategic investment. Structured interactions between cyber and business leaders are becoming more frequent, but more needs to be done to promote understanding between the two teams. Building a security-focused culture requires a common language based on metrics that translate cybersecurity information into measurements that matter to board members and the wider business. Finally, cyber talent recruitment and retention remains a key challenge for managing cyber resilience, and expanding and promoting inclusion and diversity efforts could help increase the supply of cyber professionals.*

Make sure to access the full report here.

Process

Research on AI for Cyber Security defense

The Pacific Northwest National Laboratory released an interesting research on the subject.

> ***Pacific Northwest National Laboratory is a different kind of national lab.*** *PNNL advances the frontiers of knowledge, taking on some of the world's greatest*

> *science and technology challenges. Distinctive strengths in chemistry, Earth sciences, biology, and data science are central to our scientific discovery mission.*

About PNNL.

According to the announcement of their research, the results are promising, though it’s pending further research. The research involved:

> *The starting point was the development of a simulation environment to test multistage attack scenarios involving distinct types of adversaries. Creation of such a dynamic attack-defense simulation environment for experimentation itself is a win. The environment offers researchers a way to compare the effectiveness of different AI-based defensive methods under controlled test settings.*

The full research is available from their article above. And its conclusion is very interesting, it reads:

> *Application of DRL methods for cyber system defense are promising, especially under dynamic adversarial uncertain ties and limited system state information. Evaluating multiple DRL algorithms trained under diverse adversarial settings is an important step toward practical autonomous cyber defense solutions. Our experiments suggest that model free DRL algorithms can be effectively trained under multistage attack profiles with different skill and persistence levels, yielding favorable defense outcomes in contested settings. However, some practical challenges that need to be addressed further in using model-free DRL include (DulacArnold, Mankowitz, and Hester 2019): (i) explainability of the black-box DRL policies, (ii) vulnerability to adversarial noise and data poisoning, and (iii) convergence for large state-action spaces. Future work will include developing DRL-based transfer learning approaches within dynamic environments for distributed multi-agent defense systems.*

This was reported in some major cyber security news outlets.

Technology

Gartner’s Emerging technologies Impact radar 2023

This is a chart from Gartner that can create a blueprint of potential conversations in the year to come.

I’ve heard queries from customers about ChatGPT and generative AI in cyber security and it’s a matter of time before some of the topics below come up… Responsible AI, Decentralized Identity and others are directly related to Cyber Security.

Whilst everything else — has Cloud or Cyber Security as an implied dependency.

According to Gartner 4 emerging technologies require attention in the next 3 to 8 years (where to start specializing yourself on 😉):

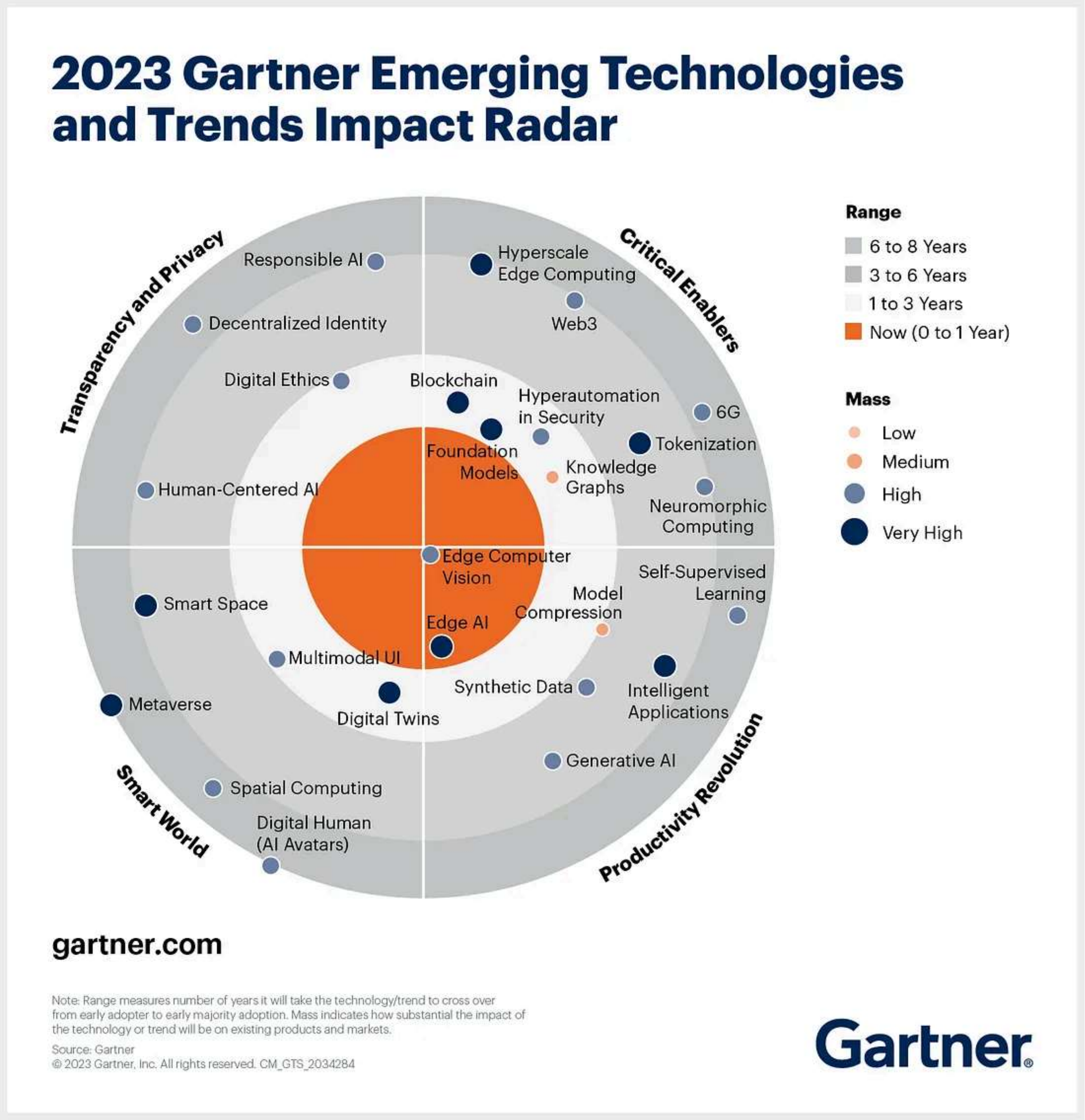
№1: Neuromorphic computing

№2: Self-supervised learning

№3: Metaverse — Apple’s schedule to launch their AR/VR product in June 2023…

№4: Human-centered AI

Read more about those and more on the official article, link below:



Note: Range measures number of years it will take the technology/trend to cross over from early adopter to early majority adoption. Mass indicates how substantial the impact of the technology or trend will be on existing products and markets.

Source: Gartner

Source: Emerging Technologies on the 2023 Gartner Impact Radar

It’s important to note the document is vague towards its own time estimates of each technology. Perhaps a deeper document will have details on how they arrived at the expected time of market adoption per segment…

IBM 2023 X-Threat report Released

IBM released their annual “X-Threat” Report recently, available here.

Some worthwhile highlights in my opnion from the reported findings include:

> **Attack types:**
>
> *→ 21% Of incidents saw backdoors deployed*
>
> *→ 17% Of attacks in 2022 were ransomware*
>
> *→ 6% Of attacks were business email compromise*

Ransomware remains at the top of attacks, remote backdoors being leveraged as entry way, investigating against MITRE ATT&CK’s TTPs always important.

> **Infection vectors:**
>
> *→ 41% Of attacks used phishing*
>
> *→ 26% Of attacks exploited public-facing apps*
>
> *→ 16% Of attacks abused valid accounts*

Phishing remains main infection vector. User inbox protection is crucial.

Lastly, they provide insight into how Ransomware attacks have evolved from a timeline perspective:

> → ***2019*** *ransomware deployment time: 60+ days*
>
> → ***2020*** *ransomware deployment time: 9.5 days*
>
> → ***2021*** *ransomware deployment time: 3.85 days*

Metrics such as MTTD and MTTR are always useful.

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 Cybersecurity Strategy Threat Intelligence

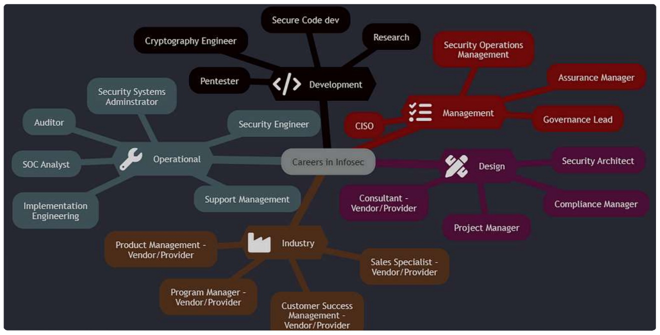
Written by Andre Camillo, CISSP

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



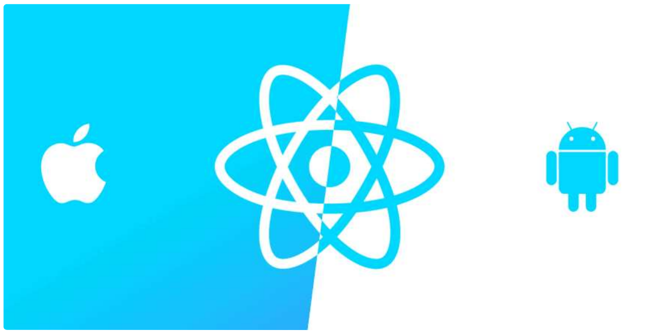
Secure Code dev
Cryptography Engineer
Research
Security Operations Management
Pentester
Development
Assurance Manager
Security Systems Adminstrator
Management
Governance Lead
Auditor
Security Engineer
CISO
SOC Analyst
Operational
Careers in Infosec
Design
Security Architect
Implementation Engineering
Support Management
Consultant - Vendor/Provider
Compliance Manager
Project Manager
Product Management - Vendor/Provider
Industry
Sales Specialist - Vendor/Provider
Program Manager - Vendor/Provider
Customer Success Management - Vendor/Provider

Andre Camillo, CISSP in CloudnSec

Cybersecurity Careers and Jobs for 2024

I've recently had the chance to talk about Diversity & Inclusion & the cyber security fiel...

Feb 21 · 52 · 2



Anshul Borawake in Geek Culture

React Native Generate APK — Debug and Release APK

Generate Debug and Release APK in React Native; Windows, iOS and Linux

Apr 4, 2021 · 1.8K · 11