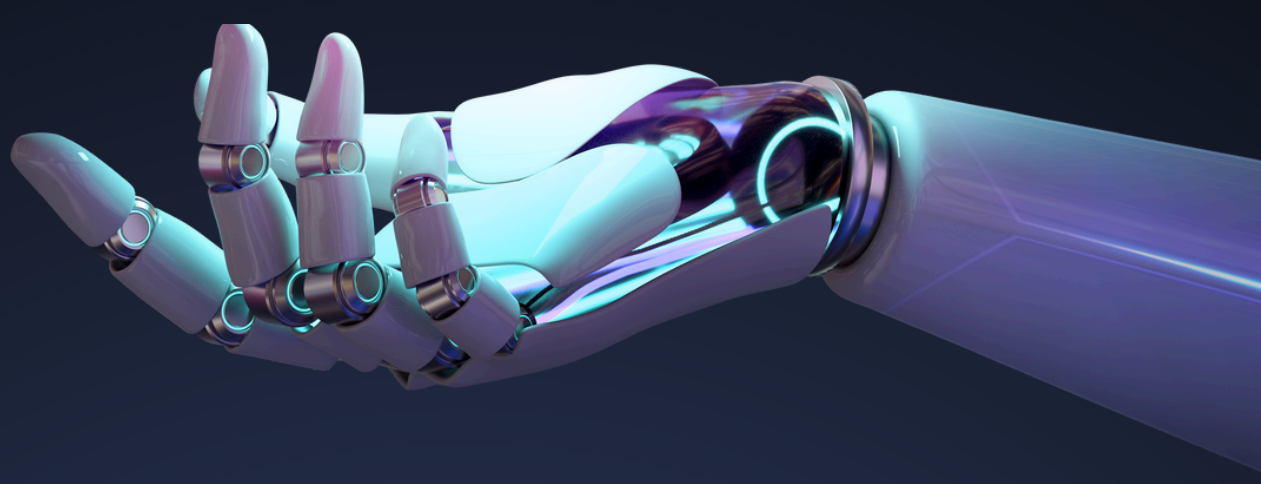
GENRES OF INFORMATION SECURITY



Audience

Generally, presentations will be the go to way to provide information. When presenting or information in the CyberSecurity field, always remember your audience. Are you presenting to the board or are you presenting to your peers? Keeping that in mind wil help you with formulating an appropriate genre.

Purpose

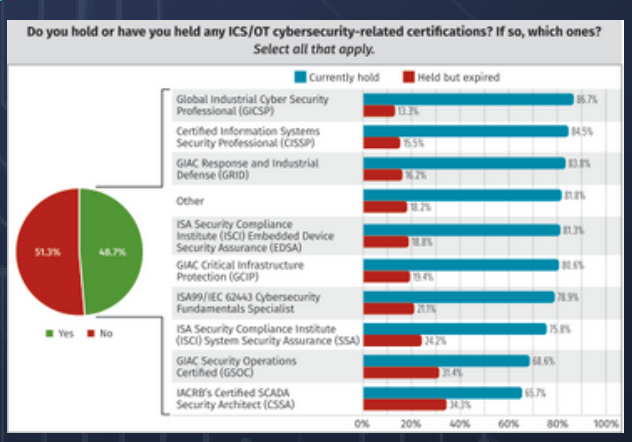
Once you have identified your audience, clarify your purpose. Are you aiming to demonstrate something? Or perhaps you want to educate them on a specific topic? Keep in mind that cybersecurity is a broad term encompassing various aspects. It's important to remember that this subject is flexible and adaptable.

Credibility

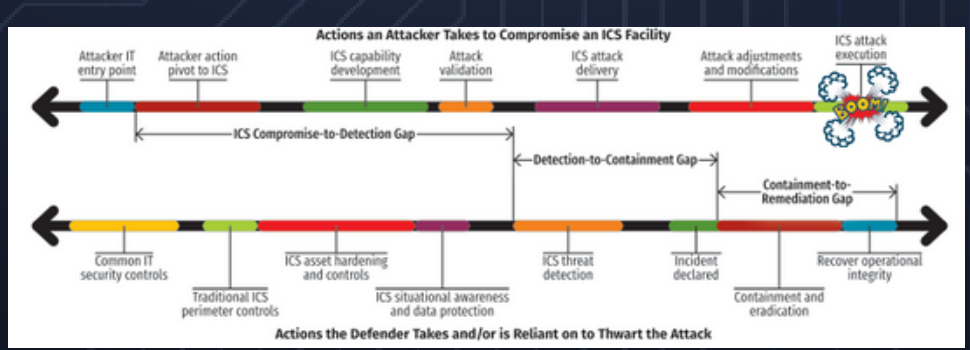
Additionally, pay attention to the clarity and accuracy of the information you present. Double-check your data and ensure that every piece of information is supported by credible sources. This not only enhances your credibility but also encourages your audience to engage more deeply with your content.

EXAMPLES

A structured graphic defining terrms from Gartner



An infographic depicting the percentage of information security workers owning certifications

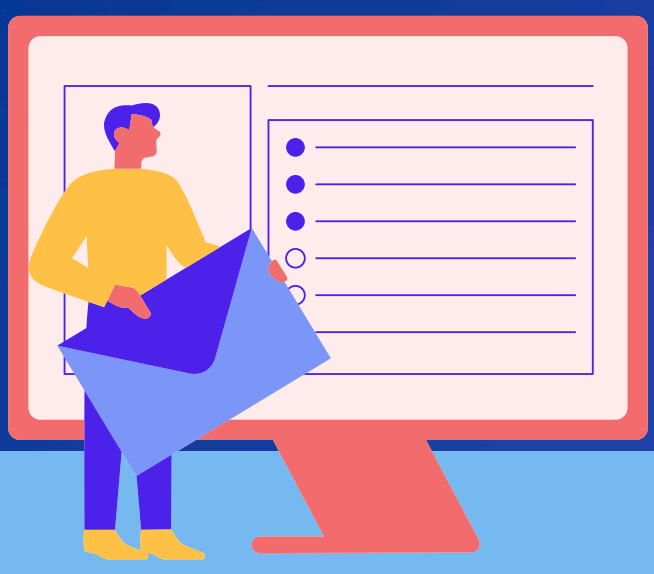


Another graphic that shows which attacks are fatal to security systems

IN SUMMARY:

- Visual tools provide distinct insights and perspectives.
- charts and graphs can break down intricate data
- Infographics convey a narrative at a glance
- comprehensive reports offer thorough analysis for those interested in exploring further.
- Interactive dashboards facilitate real-time data exploration, enabling users to swiftly make informed decisions. Integrate these tactics into your presentation/speech and you will succeed!

WHICH ONE IS BETTER?



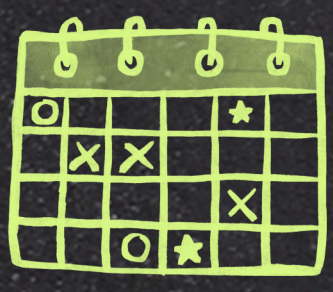
Community vs Professional

	Community	Professional
Purpose	Cybersecurity is focused on safeguarding individuals, small businesses, schools, and local non-profits from threats such as phishing, malware, and identity theft. The emphasis is on fostering cyber hygiene and raising awareness among non-technical audiences.	about protecting corporate data, financial systems, intellectual property, and ensuring compliance with regulations (e.g., GDPR, HIPAA). Professionals work to defend against more sophisticated threats like ransomware
Tools	often rely on training workshops, flyers, and social media campaigns to inform people about cybersecurity best practices, such as using strong passwords or avoiding phishing scams. Public libraries, schools, and community centers may offer resources and guides for digital safety.	employs complex tools like SIEM (Security Information and Event Management) systems, intrusion detection systems (IDS), and penetration testing to detect and mitigate risks.
Policies	The primary audience here includes families, students, and small businesses, with a focus on accessibility. Community-based initiatives may use simple language and practical examples to help people protect their digital lives.	must follow strict cybersecurity protocols and regulations, such as NIST frameworks, to ensure security across all layers of the organization.
Values	values usability and accessibility, ensuring that cybersecurity advice and resources are easy to understand and implement for those with limited technical knowledge.	places a high value on credibility, reliability, and efficiency. Cybersecurity practices must not only defend against breaches but also ensure minimal downtime and quick recovery from incidents.

Process for students & interns

Research

Use platforms like Google Scholar, IEEE Xplore, and academic databases to find peer-reviewed articles and up-to-date resources. They also reference cybersecurity standards like NIST guidelines and frameworks



Brainstorming

Brainstorming involves sketching out network architectures, defense mechanisms, and potential attack vectors. Students may also use simulation tools like Kali Linux, Wireshark, or Metasploit to understand how cyberattacks unfold and how to defend against them.

Inspiration

Stay updated by exploring cybersecurity blogs, attending webinars, or participating in guest lectures led by industry experts. Connecting with cybersecurity communities, such as DEFCON or Black Hat conferences, serves as a vital source of inspiration.

Execution

In academic environments, students participate in labs, virtual settings, and cloud platforms to simulate cybersecurity scenarios. They work together on team projects to test and secure systems, utilizing virtual machines or online sandboxes to practice safely without endangering actual systems.

Feedback

Feedback in cybersecurity education includes code reviews, lab evaluations, and graded reports. In CTF (Capture the Flag) challenges, students get immediate feedback on their strategies. Professors provide postmortems on simulated attacks or projects, highlighting successes and areas for improvement.