

Smart Cyber: How does ChatGPT and Bard describe the term...

Steven O'Sullivan

July 2023

Brought to you by Smart Cyber Group
and...ChatGPT and Bard



What Bard and Chat GPT LLM say about “Smart Cyber”



The term “**Smart Cyber**” is not definitively defined, however what can be said is Smart Cyber is a rapidly evolving field, and new solutions are being developed all the time.

As cyber threats become more sophisticated, the need for smart cyber solutions will only grow. With the convergence and tech refresh taking place within OT/ICS and CNI this is particularly relevant.

Using two very common LLM , tools the following explanations were provided:

(1) However, based on the phrase itself, it could potentially refer to the combination of smart technologies and cybersecurity. With the increasing prevalence of connected devices and the Internet of Things (IoT), there is a growing need to secure these devices and the data they generate.

(2) Smart cyber" might involve the use of intelligent systems, machine learning algorithms, or artificial intelligence to enhance cybersecurity measures, such as proactive threat detection, automated response systems, or real-time monitoring of network activity.

(3) Smart cyber is a term used to describe the use of advanced technologies to improve cybersecurity. This includes the use of artificial intelligence (AI), machine learning (ML), and big data analytics to identify and respond to cyber threats.

How can a Smart Cyber approach and mindset help organisations...



- **Prevent cyber attacks** By using AI and ML to analyse data, organisations can identify patterns that may indicate a potential attack. This allows them to take steps to prevent the attack from happening.
- **Detect cyber attacks** Even if a cyber attack is not prevented, smart cyber can help organisations to detect it early. This gives them a better chance of containing the attack and minimising the damage.
- **Respond to cyber attacks** Smart cyber can also help organisations to respond to cyber attacks more effectively. By using AI and ML to analyse data, organisations can identify the best way to respond to an attack.

Here are some examples of smart cyber solutions:

- **AI-powered threat intelligence platforms** that use machine learning to identify and track emerging threats.
- **ML-powered anomaly detection tools** that can identify unusual activity on a network or in an application.
- **Big data analytics tools** that can be used to identify patterns in data that may indicate a cyber attack.

Here are some of the benefits of smart cyber:



Increased efficiency: Smart cyber can help organisations automate many of the tasks involved in cybersecurity, which can free up human resources to focus on more strategic and creative tasks.

Improved effectiveness: Smart cyber can help organisations identify and respond to cyber threats more quickly and effectively.

Reduced costs: Smart cyber can help organisations reduce the cost of cybersecurity by automating tasks and making security more proactive

Here are some of the challenges of smart cyber



Complexity: Smart cyber can be complex to implement and manage.

Data privacy: Smart cyber often relies on the collection and analysis of large amounts of data, which raises privacy concerns.

Security risks: Smart cyber itself can be a target for cyberattacks.

Conclusion



Smart cyber is an rapidly evolving and emerging field, and there is still much research to be done. However, the potential benefits of smart cyber are significant. By using advanced technologies, organisations can improve their cybersecurity and protect themselves from cyber threats. As the technology matures, we can expect to see even more innovative and effective smart cyber solutions being developed.

“Overall, smart cyber is a promising approach to improving cybersecurity. However, there are still some challenges that need to be addressed before it can be widely adopted. Much of this is around the culture, education and integration into the wider organisation. Smart Cyber needs “Smart Cyber trained people” at all levels.

Remember...if your organisation is transforming, (digital and cyber) YOU already have Smart Cyber in place.....Be Ready!