## **Cyber threats are real! Learn how to secure your business dreams!**

Team Cyber ushers in a new era of cyber security readiness training today with the launch of their intuitive and carefully curated cyber awareness platform for time sensitive SMBs.

**The Guardian- 14 December 2021, Melbourne, Victoria** - Cyber-attacks on SMBs are rising as global situations, such as Covid-19, have forced small businesses to take their business online. While moving their business online, these SMBs struggle to find the time to provide the necessary training to protect themselves from these threats. Scenar.io aims to alleviate some of the strains these time sensitive SMBs face by providing them with an intuitive and carefully curated cyber awareness platform. Scenar.io gives SMBs analytics-driven relevant and time-efficient cyber security training by placing the person in a virtual 3d scenario that replicates real-world cyber-attack scenarios.

As per the reports of Alert Logic, a cyber threat detection company, 58% of all cyber-attack victims are small businesses. It is also found that 2 out of 5 small businesses have experienced some form of cyber security event. This increase in the number of cyber-attacks can bring businesses to a halt. Attackers may even resort to locking critical resources and seeking ransoms from the SMBs. A more alarming fact is that most SMBs have inadequate knowledge about cyber-attacks in terms of what they are, what they look like, how the attacks impact their business, and how to react in such situations.

“60% of SMEs who fell victims to cyber-attacks could not recover and shut down within 6 months.”, as per the findings of Cybersecurity for Small and Medium-sized Enterprises (SMESEC) Consortium. Small businesses have become a very attractive target for cyber-attacks as the SMBs do not have adequate technical know-how or the human resources to protect their organisations. Most of the SMBs consider investment in cyber security as an additional cost and forgo it. So, an analytics-driven, relevant, time-efficient and yet an affordable cyber security training platform such as Scenar.io fulfils the current need of the SMB industry.

Scenar.io is built by Team Cyber, a newcomer to the field, who is working with the RMIT Cloud Innovation Centre (CIC) powered by Amazon Web Services (AWS). Scenar.io aims to emulate various scenarios of cyber-attacks with an intuitive and intelligent virtual platform. It has a store of different types of cyber-attack simulations that will give the users a real-time experience of an attack and its effect on their business. The training platform will feature an intelligent analytical tool which will analyse the user’s details and work out the attack scenarios customized for the specific user.

“Why can't it always be this easy?” said Gerald, a Head of Operations of an SMB, when asked about Scenar.io. “I mean, I’ve been through cyber security workshops before, but all that tech talk gets difficult as I don’t have prior technical knowledge. After going through the Scenar.io, I was completely surprised as not only was it way more engaging for me since I could walk through it, but it was so quick too. It’s crazy to think that Scenar.io did what that workshop couldn’t do in a fraction of the time. I’ve now got some confidence and peace of mind when it comes to protecting my business from going bankrupt with cyber-attacks as well as extra time thanks to Scenar.io.”

Join them in protecting your business in this new age of online business by signing up for Scenar.io, the immersive cyber security awareness program, visit <www.Scenar.io>.

**FAQs**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Customer FAQ’s:**

1. What is virtual cyber-security awareness training?

Virtual cyber security awareness training is a training in which the users can get more hands-on experiences of cyber security attacks. Cyber-attacks are simulated with many scenarios where the user gains more practical experience with a gentle learning curve.

2. Do I need to be technically sound to use this training platform?

No. The platform is built with an intelligent method to cater to the needs of individuals of various knowledge levels. The platform will use data analytics to understand the user’s role and understanding level and will create a very easy to understand workflow to guide the user through the entire training process.

3. How do I procure these scenarios?

The user need not procure the scenarios specifically. Our intelligent analytics driven system will ensure that users are recommended the most relevant scenarios once the user signs up for the awareness program.

4. How real are your scenarios?

The scenarios are carefully curated by our team of IT security experts who have a deep knowledge and understanding of real-time cyber-attacks. The attacks are based on the latest security attacks which have happened and have affected real businesses.

5. How do I delete my account?

Once the awareness program is completed and the completion certificate is issued, the account details of the users will be deleted from the system. We will not store user’s information beyond the point of completion of all formalities.

6. How do I buy it? Is there a one-time fee or a subscription system?

Team Cyber is providing this service for free. The company believes in ensuring that businesses feel free in conducting their business online. Scenar.io is one initiative of the company in building that trust.

7. What if the scenar.io platform gets hacked?

Our platform is secured by industry standard IT security measures. We also maintain strict compliance to national and international security and privacy regulations and standards such as Privacy Act 1988, Payment Card Industry Data Security Standard (PCI DSS) etc.

8. Can you provide a guarantee that a scenario provided in your platform will cover every problem related to that scenario?

We strive to update our scenarios constantly with the changing nature of cyber threats. We ensure that our scenario is as real as wide as it gets to cover all facets of problems related to that scenario.

9. Why is your platform better than other cheaper training alternatives?

Our platform is a breakthrough solution with a more realistic and easier training program which is suitable for the business personnel who cannot afford time or effort to go through monotonous training documents. Our scenario-based training provides more practical and realistic experience, which is easier to learn, engage in. Information is easier to retain with the action-oriented training approach.

10. What is the average length of each training session?

Our training session can run anywhere, depending on the intricacy of the course. We have created this platform more for the advancement of the user.

11. What is the maximum number of participants who can attend a single training session?

Our training is tailored to a specific user or company and there is no pre-requisite for number of participants.

12. Why are SMBs expected to implement senaro.io?

The importance of cybersecurity to a company's bottom line cannot be overstated. Every year, cybercrime costs firms billions of dollars in lost profits and efficiency, which can have long-term consequences for a small business.

13. How do I access the senaro.io training remotely?

You may access our app via signup process, and we will be guiding throughout the process.

14. Can we update the scenario?

No, the user cannot add the scenario directly, but we could take up your feedback. You can send the scenario that you wanted to be seen in the respective category.

15. How will customers be guided through simulated attacks? Will there be instructions? Will they be written or video?

 The user will be given a hint/some instruction in the simulation to assist them in completing the session.

16. How will customers take away learnings? Will you be providing them with an understanding of how to avoid those potential attacks that have been simulated? What form will that understanding be in?

On completion users will be emailed the key summary of the training and detailed plan of action to prevent, respond to and mitigate the attack covered in the training.

**Technical FAQs:**

1. What hosting service is used by the scenar.io?

The scenar.io services are hosted using AWS services. The AWS tools are used to make the sessions reliable, and resistant to any disruption and unavailability.

2. What type of technology is used in Scenar.io?

Scenar.io provides cloud-based interactive 3d training spaces, and it is accessed through a website. The simulations are built using Amazon Sumerian and the front end and web interfaces are built using react native and Amazon Amplify, and Amazon Lambda is used for authentication of the users.

3. How do you ensure security of the data?

We use a strong encryption system to keep the data secure. Access control to the data is also protected based on the principle of least privilege, which means, access to information is given to only those people who are necessary to access the information.

4. What makes the Scenar.io technically strong from other cyber ranges?

We have a strong cloud-based infrastructure that would hold a lot of users at a time and ensure to have uninterrupted training sessions, more over the user information and other things are handled securely in the way that we will audit our system on a regular basis

5. Will scenar.io expose the flaws in my network?

No, Scenar.io will not expose your network flaws to the attackers, because all the attacks are performed in a simulated environment, and not on your infrastructure.

6. How many users can scenar.io can support?

Unlimited number of users can be supported due to the AWS auto scaling support, which automatically adjusts the scalability respectively.

7. What sort of platform would be used to host the simulations?

The scenar.io will be hosted as the app which will be hosted in IOS, Android, and web app.

8. What technology stack would be used?

To develop the web app we will be developing the app using React native for the front-end and Node.js for the back-end.

9. Would users need to deploy anything in their environment, or would the sceanr.io will host this all?

The user will not need to deploy anything in their local environment. The app will be hosted entirely as a Software as a Service (SaaS) platform wherein users can use it by signup.

10. What type of attacks will you be focusing on?

We will be focussing on the cyber-attacks which are currently affecting the small and medium sized businesses. Further, among the current attack types, the recommendation of the attacks will be based on the analysis of the variables relevant to the users, such as their job nature and technical competence related to cyber-attacks.