Cyber Readiness Now Easier Than Ever For AZ State and Local Organizations

AZ Department of Homeland Security leveraging generative AI tools to answer Cyber Security questions for local organizations.

[PHOENIX - October 12, 2023] The Arizona Department of Homeland Security (AZDOHS) announces the launch of Cyber Homeland Information Portal (CHIP), the generative AI application that allows organizations participating in AZDOHS's Cyber Readiness Program to get real time support on program and cyber security tool implementation. Organizations with little or no IT resources can now leverage tools to secure their information systems with the help of AZDOHS and the CHIP application.

Today, small organizations experience challenges in understanding the cyber security resources available to them and how to implement them in order to appropriately secure their networks and applications. AZDOHS has allocated resources to provide guidance and support to participating organizations, however, the inquiries are backlogged due to limited headcount, leading to delayed responses.

The CHIP application will allow organizations participating in AZDOHS's Cyber Readiness Program to receive real time answers to their questions about the program and tools they need to implement. Trained using program and product onboarding documentation, the CHIP application will leverage machine learning to respond to natural language queries, providing summarized answers, together with document citations for additional validation. If the organization wishes to escalate to a human, the tool will hand off to an AZDOHS agent, along with chat context for a seamless customer experience.

"Many organizations struggle with understanding where to start when trying to secure their systems." said John Roberts, Director of AZ DOHS. "The CHIP application leverages the power of Generative AI to provide additional guidance to Cyber Readiness participants that might be delving into the cyber security field for the first time."

Organizations participating in the Cyber Readiness program will be able to access the 'XXX' application via the AZDOHS website. Once launched, the application will prompt a user to enter their query on topics related to the program or any tool that is a part of the program. The application will search all documents related to the question and present a concise answer for the user.

Jenny Summers, an AZ school district administrator stated, "Getting answers when trying to set up cyber security was really time consuming before the CHIP tool. The real time feedback has allowed me to learn more about the resources available to me, and how I can utilize them effectively."

For more information about the CHIP tool, please navigate to:
https://azdohs.gov/CHIP

Frequently Asked Questions (FAQs)

1. **Who is the Customer?**

   The target customer will be organizations participating in AZ DOHS Cyber Readiness Program that have little or no internal IT resources to setup and maintain the security tools provided by AZ DOHS.

2. **Can anyone use CHIP?**

   No, only the organizations participating in the AZ DOHS Cyber Readiness Program will have access to the tool.

3. **How would the Human in the loop hand off actually work?**

   In use cases that require more detailed Human interaction, the user will be notified and the context of the conversation on CHIP will be emailed to the AZ DOHS Cyber Readiness Team.

4. **Will this system be available 24x7?**

   Yes, CHIP will be accessible 24x7.

5. **Will there be references to documents that form the basis for the answers provided by the chat bot?**

   Yes, whenever a user receives a response from CHIP, the application will also link the documents from where the answer was derived. The user can access and review the documents themselves for additional guidance.

6. **Will we be able to get analytics information from usage of this bot?**

   The production version of the CHIP application will include usage analytics.

7. **How can the customer use this bot? Text message, going to AZ Department of homeland security website?**

   Participants of the AZ DOHS Cyber Readiness Program can access the tool by navigating to https://azdohs.gov/CHIP.

8. **What languages does this bot support?**

   The production version of the CHIP application can support English and Spanish conversations.

9. **Will this bot handle any secure or sensitive information? or is all the info for public consumption?**

Only the organizations participating in the AZ DOHS Cyber Readiness Program will have access to the tool.

10. **How can we add more content or modify/delete any existing content in this application?**

    Yes, admins can update the source documents that train the application for more accurate results.

11. **Is the content processed by CHIP moved outside the AWS Region where I am using Amazon Bedrock?**

    Any customer content processed by Amazon Bedrock is encrypted and stored at rest in the AWS Region where you are using Amazon Bedrock.

12. **Are user inputs and model outputs made available to third-party model providers?**

    No. User inputs and model outputs are not shared with third-party model providers.

13. **How can I securely use my data to customize FMs available through CHIP?**

    CHIP leverages Amazon Bedrock platform, you can privately customize FMs, retaining control over how your data is used and encrypted. Amazon Bedrock makes a separate copy of the base foundational model and trains this private copy of the model. Your data including prompts, information used to supplement a prompt, FM responses, and customized FMs remain in the Region where the API call is processed.

14. **How does CHIP ensure my data used in fine-tuning remains private and confidential?**

    CHIP leverages Amazon Bedrock to customize a model, Amazon Bedrock can fine-tune the model for a particular task without having to annotate large volumes of data. Then, Amazon Bedrock makes a separate copy of the base foundation model that is accessible only by you and trains this private copy of the model. None of your content is used to train the original base models. You can configure your Amazon VPC settings to access Amazon Bedrock APIs and provide model fine-tuning data in a secure manner. Your data is encrypted in transit (TLS1.2) and at rest through service-managed keys.

15. **What security and compliance standards does CHIP?**

    CHIP leverages Amazon Bedrock platform and it offers several capabilities to support security and privacy requirements and is compatible with common compliance standards including GDPR and HIPAA. As with all AWS services, you get the standard AWS Identity and Access Management (IAM) controls for authentication and AWS CloudTrail for auditing API activity. All your data is encrypted at rest using your own AWS Key Management Service (AWS KMS) keys, which provides full control and visibility into how your data and custom models are being stored and accessed. With PrivateLink, you can pass your data on AWS to Amazon Bedrock exclusively through AWS and never through

public internet. Amazon Bedrock can also attach its training instances to your Amazon VPC in order to read from and write data to Amazon S3.