**Vicysaver Tool- A network anomaly detector for the digital safety of SMBs**

**Melbourne, Herald Sun, December 1, 2021** - The foremost intention of Vicysaver API is to alert the customers of a possible threat to their infrastructure before their business is impacted by detecting unusual behavior and events in their website.

It can be logical to assume that cyber-attacks only occur at Fortune 500 firms or large enterprises. The unfortunate reality is that small businesses are frequently an easy prey for hackers as they either do not have adequate finances or the technical knowledge or both to protect themselves from cyber-attacks. Considering their size, they may assume they only require the bare minimum of protection. The reason smaller firms are especially vulnerable is because many businesses retain sensitive consumer information that might be used for data theft. They may keep billing information from their clients, which is a jackpot for hackers and may handle financial activities, which opens the door to data theft.

The Vicysaver Tool is a Machine Learning powered API that can be integrated with the customer's infrastructure using cloud. This API performs inference on the incoming network traffic data from the client's website and alerts the client back with a response if a suspicious activity is detected. When the end user interacts with our client's website, the API gateway obtains an inference from our Machine learning model and the response is mapped back to the client. That is not all, Vicysaver also sends an auto alert in the form of e-mail to the client with the details of the detected abnormal activity. The tool also supports interactive dashboards and visualizations of the predicted data hosted in a web portal for the client to learn about which online resource and which types of users are trying to attack their infrastructure.

Victoria, who is a participant in our customer survey, used the Vicysaver tool for a while and said "I had no idea that so many unusual events were happening in my website. With the help of auto alerts sent out by Vicysaver, I am now able to know any abnormal activities taking place on my website enabling me to call for help at the right time. The dashboards clearly showed the possible areas of concern and I always keep an eye on it with no difficulty. This is a very useful and easy to use tool and I highly recommend people like me to make the most of it"

# FAQs

**Customer FAQs**

1. **Do I need dedicated IT staff in house to maintain the Vicysaver tool?**
   You do not need any large staff as there is no on-premises equipment to be maintained, managed, or updated. You might need an IT helper to block the IP address from trying to attack your infrastructure again.

2. **Will the Vicysaver API impact my website in any way?**
   Vicysaver is only an intermediary which allows communication between the client website and our machine learning predictor model and therefore it does not impact the website in any way.

3. **Will the API collect my data?**
   We collect and use the website logs to provide as inputs to our machine learning models to train and understand the network better.

4. **How can I get help if I have a problem?**
   Since our API is backed up by Amazon Web services, you will be provided with round the clock service and maintenance.

5. **How often do I have to use your API?**
   Once the API has been integrated into your website, it keeps running in the backend.

6. **How would I minimize the operational cost if the API keeps running in the background?**
   With AWS, you only pay for the services you are opting for as long as you want as we follow a pay as you go approach.

7. **How my data and system get secured with this application?**
   This application does not provide a solution such as a system protector, virus guard or firewall to protect your system from attacks. It is a tool that provides you with alerts on suspicious activities to the client's infrastructure.

8. **Who will have authorized access to my API?**
   You can have authorized access to your API's by setting your own API methods. While setting up a method to have authentication, you can also use other Lambda Authorizers or AWS Signature Version 4 to support your own bearer token auth strategy.

**Stakeholder FAQs**

1. **What is the Vicysaver API about?**
   Vicysaver is a cloud-based anomaly detection tool that detects abnormal activities taking place on user's infrastructure and notifies them via email.

2. **How does Vicysaver protect data?**
   This tool does not directly protect your data. But it provides information on anomalies in the client's network that the businesses can take necessary precautions to ensure the security of their data.

3. **How is this tool different from the other cyber security tools available in the market?**
   Vicysaver is a cloud-based API that the businesses do not have to install in their systems rather integrate it with their infrastructure. Further, Vicysaver is a tool that provides guidance to implement solutions according to the business infrastructure. This tool is powered with Machine learning which is known for detecting anomalies in the real world. So, Vicysaver is mainly a cyber education tool that provides guidance to stay protected from cyber-attacks.

**Technical FAQ's**

1. **Is the app web based or a desktop application? If it's the latter, does it need to be installed, or is it standalone?**
   Vicysaver is a web-based application that does not require the user to install software on their computer. However, in order to use the app, customers must first register on the website.

2. **How will the tool assess cyber risk?**
   The application is designed to identify strange IP addresses and generate an anomaly score based on which the severity of the threat can be detected.

3. **Is the model compatible with all web logs?**
   The model is compatible with any form of web log and works with the data that was used to train it.

4. **What kind of tools are needed to test the API?**
   Any HTTP client for testing web services can be used to test the API.

5. **Which type of API gateway does the solution offer?**
   The solution offers REST API type with features like publishing API's, monetizing API's, usage plans and API keys while also supplying API management and proxy functionalities in a single solution.

6. **Can a customer use other AWS features with API gateway?**
   Yes, the customer will be able to integrate other AWS services with API gateway.

For example, Amazon SNS can be integrated with this API to trigger an alert in case of a high anomaly score.

7. **How can the customer monitor the Amazon API gateway API's?**
   The Amazon CloudWatch present in AWS account holds the logs of API calls, error rates and latencies and the metrics can be found in a dashboard in the gateway Console.

8. **Will the backend systems and apps be impacted by spikes in traffic?**
   Throttling has been provided at many levels including by service calls and global calls and the limits for throttling can be manually given a limit say up to thousand requests per second for some seconds. Any request found to be over the given limit while tracking will be receiving a 429 HTTP-response code.

9. **Can individual developers be throttled from calling my API?**
   Yes, there is a specific usage plan in AWS for setting a specific throttle limit for individual developer's API's.

10. **How does the API scale?**
    The API will inevitably be scaled automatically to cope with the traffic received by the API.

11. **How can I verify and allow access to my API?**
    You can set optional API methods to need authorization by using Lambda authorizers or AWS Signature (Version 4) to aid your authorization strategy.

12. **How will you inform the client about the detected dangers and alerts?**
    Vicysaver's initial phase detects suspicious IP addresses attempting to log in to the website. Vicysaver will be linked with AWS Quicksight in the future to display identified risks, actions to be done, and suggestions, as well as AWS SNS to notify registered users when a danger is detected.

13. **Do I need internet to run this?**
    Yes, because the model is built with AWS tools, Internet access will be necessary to execute it.

14. **How frequently will the customer receive notifications?**
    The threshold value can be modified according to the intensity with which the customer wishes to be notified to avoid frequent notifications.