Security Review

Identify security risks and uncover opportunities to improve security and compliance posture.

Customer Solutions Architects (CSAs) leverage their Heroku security expertise to uncover opportunities to improve your overall security and compliance posture. Our team will prepare a detailed report of your Heroku implementation, which identifies security risks and how to remediate them, and Heroku features and functionality you are not currently leveraging that can improve your security and compliance posture. You'll gain a deeper understanding of potential security risks and how to address them, and a stronger awareness of Heroku features and functionality that can improve your security and compliance posture.

What it can do for you.

- Provide a detailed security profile of your Heroku implementation
- Identify common security risks and identify lack of usage of Heroku security and compliance features and functionality
- Outline discrete steps to remediate security risks and recommendations on how to improve security and compliance posture

How it works.

A CSA will engage your team to identify any security and compliance drivers and concerns. With our customer stakeholders' key areas in mind, the CSA will construct a detailed written report that examines your current Heroku implementation. The document will include relevant data points, configurations and/or metrics, and screenshots of your Heroku implementation. The report will also contain fine-grained analyses based on these findings.

Once completed, the CSA will share the document with customer stakeholders. You'll also be invited to ask questions and discuss the findings with our team. A Security Review Pro Module is often a gateway to a wider dialogue between the CSA team and the customer, thereby guiding your Heroku implementation security and compliance posture towards long-term success.

Discovery: Customer Tasks

- Identify and engage your technical stakeholders
- Complete the pre-Module Questionnaire
- Confirm that your timeline and desired outcomes match the Pro Module deliverables
- Attend the kick-off meeting

Analysis: CSA Tasks

- A CSA reviews the questionnaire and inspects the customer's Heroku configurations
- Findings are collated, analyzed, and explained in a report format, with presented recommendations included therein
- Final report is delivered and customers are then invited to engage in a follow-up dialogue

Outcomes

- Customers receive a document outlining security risks and suggested remediations, and identification of Heroku features or functionality that can improve security and compliance posture
- A dialogue geared towards long-term security and compliance health is begun with CSAs

Additional Information

Lead Time: 2-3 weeks
Customer Time Investment: 1-2 hours

Goal

After a Security Review Pro Module, customers will have a clear understanding of 1) potential security risks related to their usage of Heroku Services and specific actions to remediate these risks, and 2) opportunities to leverage additional Heroku features or functionality to improve their overall security and compliance posture.

Intended User

If you're storing, transmitting or processing sensitive data on Heroku and looking for a security review to identify potential security risks or opportunities to improve your security and compliance posture, and are open to recommendations from the CSA team, this Pro Module is for you.

Prerequisites

To complete this engagement, the customer must have:

- A current Heroku Enterprise license
- A deployed, production-grade Heroku application(s)
- A stakeholder ready and eager to receive feedback on how to improve their application

Scheduling

To schedule this Pro Module, please [open a ticket with the Customer Solutions Architects (CSA) Team](). A CSA will be in touch soon with an invitation to complete the pre-Module Questionnaire and begin the engagement.