GitHub Advanced Security Health Check

Project, Workshops, Sessions | Remote or Onsite | Level 300

Description

Solidify offers a comprehensive DevSecOps health check package that enables companies to identify and understand potential shortcomings in their DevSecOps setup. By leveraging this bundle, businesses can accelerate their adoption of DevSecOps by rectifying any deficiencies based on the identified areas. Each area of improvement will come with a detailed list of suggested remediation strategies, enabling organizations to take immediate action to improve their DevSecOps practices.

1. **Scope of Work**

The services provided will cover the following:

- Custom session on GitHub Advanced security features, shift left approach, security overview views, and demo on how Copilot can help out together with GHAS
- Review of DevSecOps processes and workflows to identify gaps and inefficiencies both in processes, tooling, and configuration.
- Analysis of current use of GitHub Advanced Security (GHAS)
- Recommendations for improving the security posture, including a shift-left approach and best practices using GHAS
- Best practices for onboarding and managing Security Champions programs
- Customized remediation plans for addressing identified areas of concern
- Presentation of the findings and remediation plans

2. **Prerequisites**

Before starting the engagement, the following prerequisites will need to be satisfied:

- At least one key stakeholder identified for each of the following roles: Developer, Architect, DevSecOps Specialist, Security Specialist, Security Champion* (in any), and Manager.
- Sufficient access to GitHub or internal help to analyze GitHub Advanced Security setup and usage.

Intended Audience

The recommended audience: - Customers who have purchased GitHub Advanced security and have used the solution for a longer period. - Team Leads - DevOps Teams - Engineering Managers – Security specialists.

Deliverables

Review of DevSecOps Processes and Workflows:

We'll assess your DevSecOps processes, tools, and configurations to identify gaps and inefficiencies

Analysis of Current Use of GitHub Advanced Security (GHAS):

We'll analyze how you're currently using GHAS, looking at scans, alert types, MTTR, overall GHAS usage and configuration and code repository coverage to provide a baseline for improvement.

Recommendations for Improving Security Posture with GHAS:

We'll offer actionable recommendations to enhance security, focusing on a shift-left strategy, GHAS best practices, and necessary tooling adjustments.

Best Practices for Onboarding and Managing Security Champions Programs:

We'll provide guidance for establishing and managing a Security Champions program to promote a security-conscious culture.

Customized Remediation Plans:

Based on our assessments, we'll create remediation plans with clear steps to address identified security concerns and identified enhancements

Presentation of Findings and Remediation Plans:

We will share our assessment results, remediation plans, and provide a written report summarizing our findings.

Training and Support:
In addition to implementation, we will provide training sessions to help teams fully utilize GitHub's capabilities.

Objectives and Outcome

This offering is designed for organizations seeking to assess and enhance their GitHub Advanced Security implementation. Our goal is to help you identify and address any issues, ensuring that your security measures are optimized.
GitHub Advanced Security, when properly configured, delivers alerts and warnings to proactively identify potential security risks. However, misconfigurations, inefficient processes, and other issues can undermine the effectiveness of your investment. Solidify's health check service is designed to assist you in pinpointing potential problem areas, devising remediation plans, and improving your overall security posture.
Our objective is to provide you with actionable insights and recommendations to enhance the security with an efficient GitHub Advanced Security setup.

Methodology

- GitHub usage metrics
- Tool analysis
- DevSecOps Process analysis
- Interviews
- Sessions
- Q&A

Time commitment options

- Delivered over 3-4 weeks. This period may be extended based on the complexity and size of the organization.

Pre-requisites

Before starting the engagement, the following prerequisites will need to be satisfied:

- At least one key stakeholder identified for each of the following roles: Developer, Architect, DevSecOps Specialist, Security Specialist, Security Champion* (in any), and Manager.
- Sufficient access to GitHub or internal help to analyze GitHub Advanced Security setup and usage.

Price for the full project including training sessions

8 000 USD

Primary Contact

For any inquiries regarding our service, please contact Sanjin Medic

sanjin.medic@solidify.dev