

# Generating a Cyber Security Report

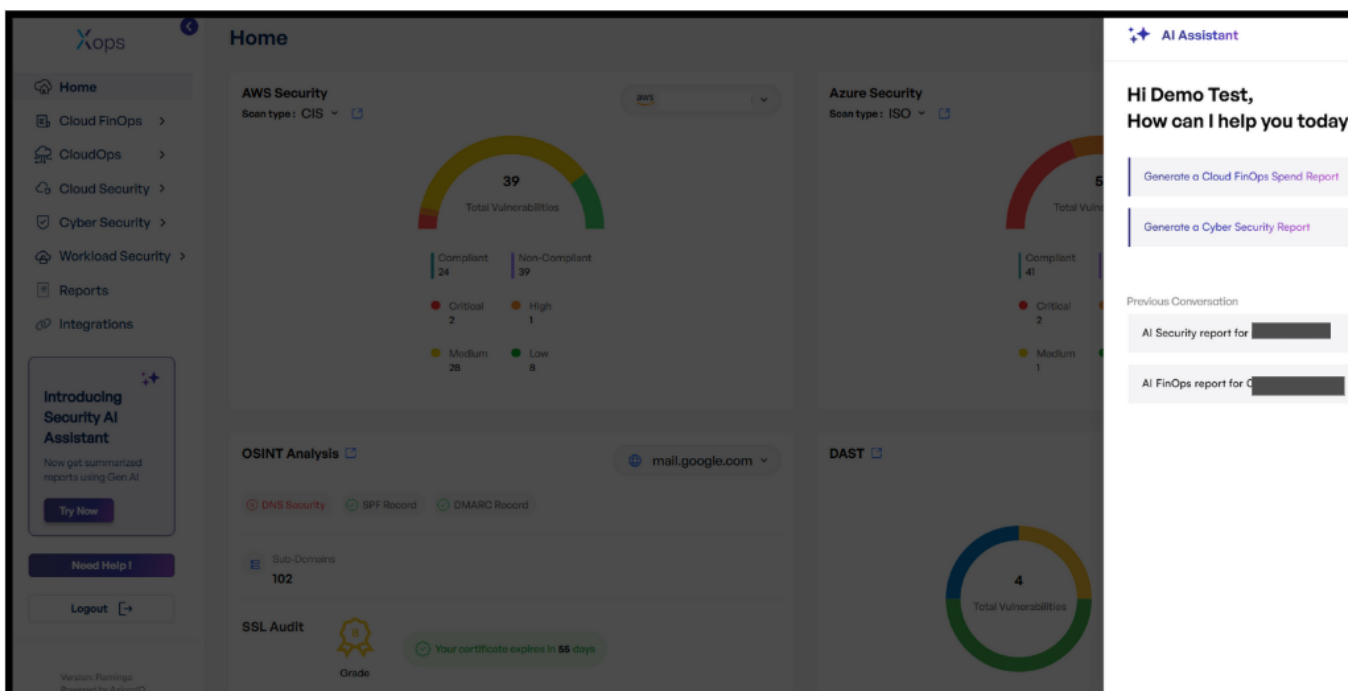
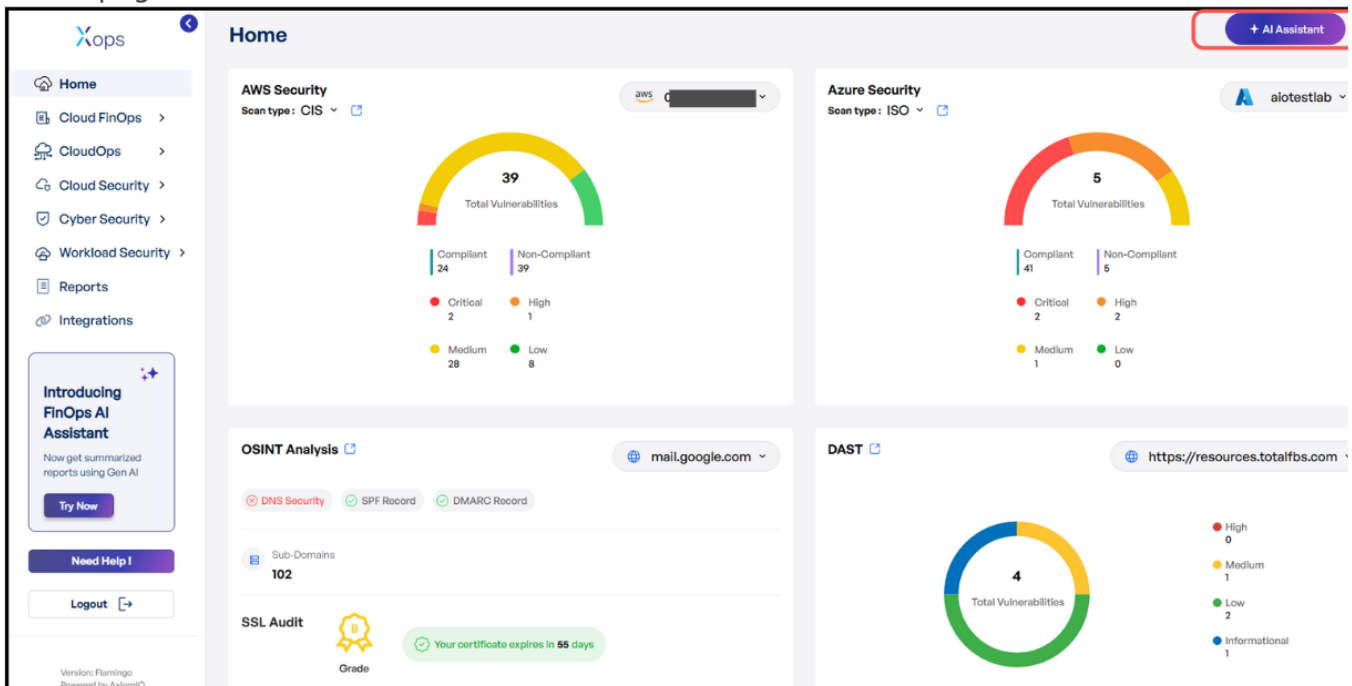
## Generating a Cyber Security Report

To generate a Cyber Security report using the X-Ops AI Assistant, follow these steps:

- **Log in to the Platform**
  - Access the platform and sign in using your credentials.

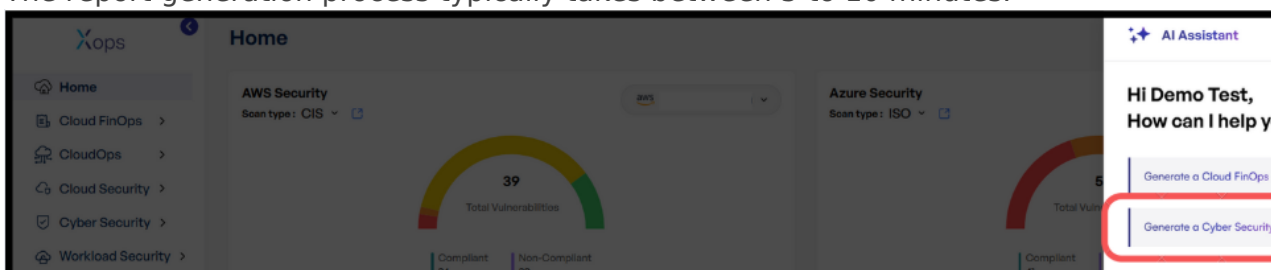
## • Access AI Assistant

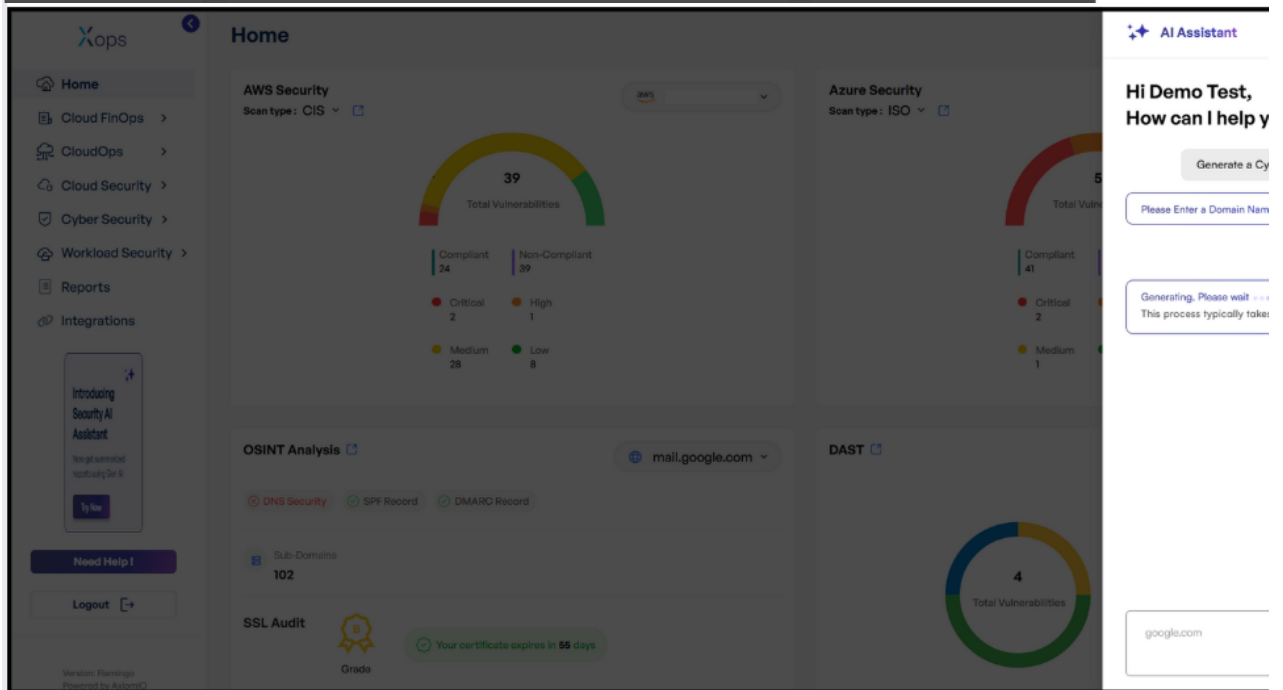
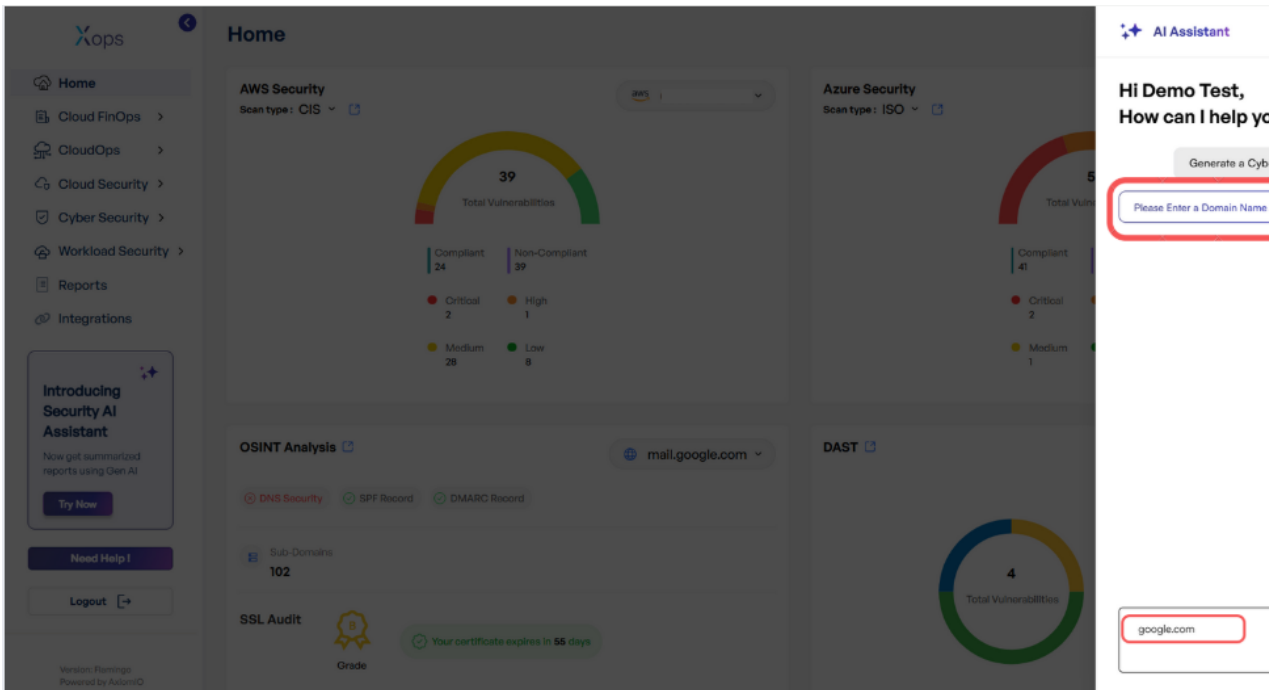
- Locate the AI Assistant icon in the top right corner of the screen and click on it.
- This action will open the AI Assistant, it will open as a side panel on the right side of the page.



## • Report Generation

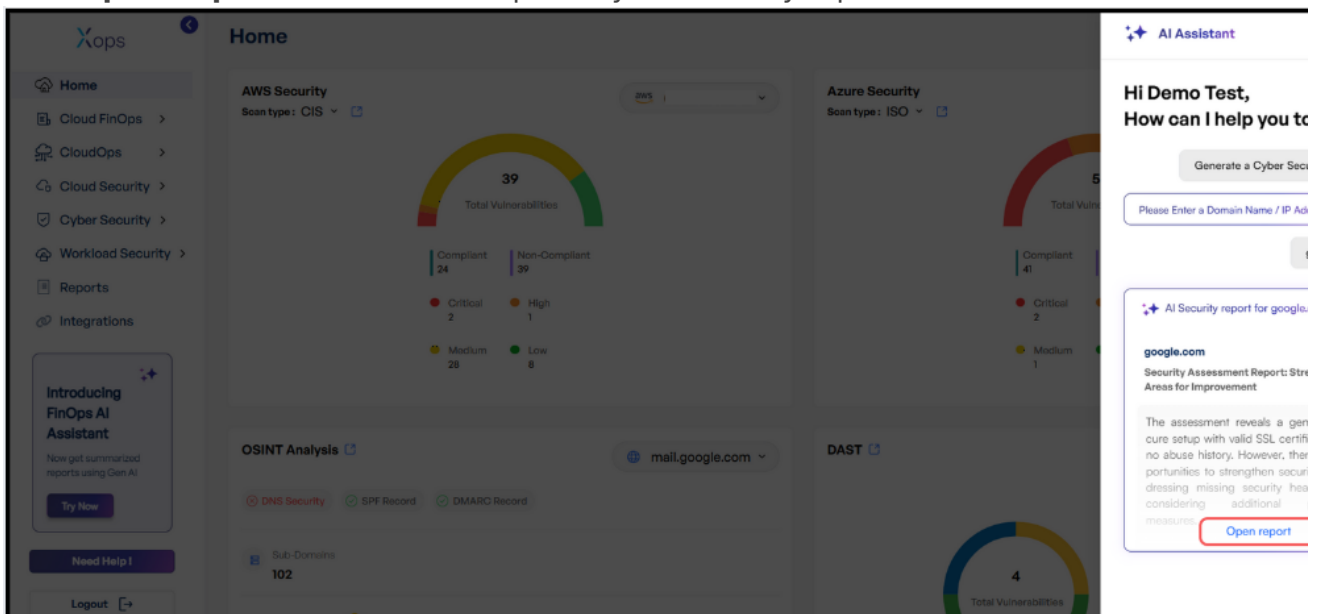
- Select **Generate a Cyber Security Report** from the options displayed.
- When prompted, enter the domain or IP address for which you want to generate the report.
- The AI Assistant will begin generating the Cyber Security report based on the provided details.
- The report generation process typically takes between 5 to 10 minutes.





- **Receiving and Viewing the Report**

- Once the report is ready, you will receive a report with an **Open Report** option.
- Click **Open Report** to view the complete Cyber Security report.



The screenshot displays a web interface for an AI Security report. At the top, it shows the domain 'google.com', the date 'Wed, June 18, 2025', and the time '09:51:04 UTC'. A 'Download' button is visible in the top right corner. The report is divided into several sections:

- Security Scan Summary:** A sub-section titled 'Security Assessment Report: Strengths & Areas for Improvement' stating that the setup is generally secure but has room for improvement in security headers and protective measures.
- Overall Threat Risk:** A prominent green box indicating a 'LOW-MEDIUM' risk level, based on vulnerabilities, security controls, and potential impact.
- What's Good:** A section with a green checkmark highlighting 'Valid SSL Certificate' as a strength.
- What can be improved:** A section with a red 'X' icon listing 'Missing Security Headers' and 'No WAF Identified' as areas for improvement.
- AI Recommendations:** A section titled 'AI-Powered Security Recommendations: Enhancing Protection & Mitigating Risks' with three numbered items: 'Enhance SSL Certificate Management', 'Implement Missing Security Headers', and 'Consider Web Application Firewall (WAF)'.

- **Downloading the Report**

- Inside the report view, locate the **Download** button at the top right corner.

- o Click **Download** to save the report to your device.

The screenshot displays a web application security report interface. At the top, the page title is "AI Security report for google.com". Below the title, there are three tabs: "google.com", "Wed, June 18, 2025", and "09:51:04 UTC". In the top right corner, there is a red-bordered button with a download icon. The main content area is divided into several sections:

- Security Scan Summary:** A section with a sub-header "Security Assessment Report: Strengths & Areas for Improvement". It contains a paragraph stating: "The assessment reveals a generally secure setup with valid SSL certificates and no abuse history. However, there are opportunities to strengthen security by addressing missing security headers and considering additional protective measures."
- What's Good:** A section with a green checkmark icon and the sub-header "What's Good". It highlights existing security strengths and effective measures in place. It lists "1. Valid SSL Certificate" with the description: "The SSL certificate is valid, uses strong encryption, and covers a wide range of domains." Below this is a "Read More" link.
- What can be Improved:** A section with a red 'X' icon and the sub-header "What can be Improved". It identifies areas needing enhancement to strengthen security and reduce risks. It lists two items:
  - 1. Missing Security Headers:** "Absence of several security headers leaves the web application vulnerable to certain types of attacks."
  - 2. No WAF Identified:** "Lack of a WAF may expose the application to web-based attacks that could otherwise be mitigated."Below this section is a "Read Less" link.
- Overall Threat Risk:** A section with a green checkmark icon and the sub-header "Overall Threat Risk". It states: "The overall cybersecurity threat risk is assessed based on identified vulnerabilities, security controls in place, and potential exploitation impact." Below this is a green box containing the text "LOW-MEDIUM".
- AI Recommendations:** A section with a plus icon and the sub-header "AI Recommendations". It is titled "AI-Powered Security Recommendations: Enhancing Protection & Mitigating Risks". It lists three recommendations:
  - 1. Enhance SSL Certificate Management:** "Monitor and renew the SSL certificate well before the expiration date to avoid service disruption."
  - 2. Implement Missing Security Headers:** "Add missing security headers like X-Content-Type-Options, Strict-Transport-Security, and Content-Security-Policy to enhance protection against common web vulnerabilities."
  - 3. Consider Web Application Firewall (WAF):** "Evaluate the need for a WAF to provide an additional layer of security against web-based attacks."Below this section is a "Read Less" link.

Revision #7

Created 18 June 2025 05:56:21 by Axiom IO

Updated 23 September 2025 10:03:47 by Axiom IO