SUCCESS STORY

flare

North American E-Commerce Giant Radically Simplifies GitHub Monitoring

The Customer

- E-Commerce
- Multinational
- Billions of dollars in assets

The Challenges

GitHub Leaks

Code hosting platforms like GitHub are invaluable as developers collaborate from distributed locations. About 84% of Fortune 100 companies use GitHub.

GitHub hosts public repositories (repos) that are accessible to anyone online. Organizations can use public repositories for open-source projects and individual developers can share their own projects and skills. On the other hand, private repositories host code for internal projects.

Threat actors can steal information by sneaking into private repositories or by finding private repositories that were accidentally made public. A report found that there are roughly two million corporate secrets that are publicly accessible on GitHub. This private information includes login credentials, certificates, and API keys.

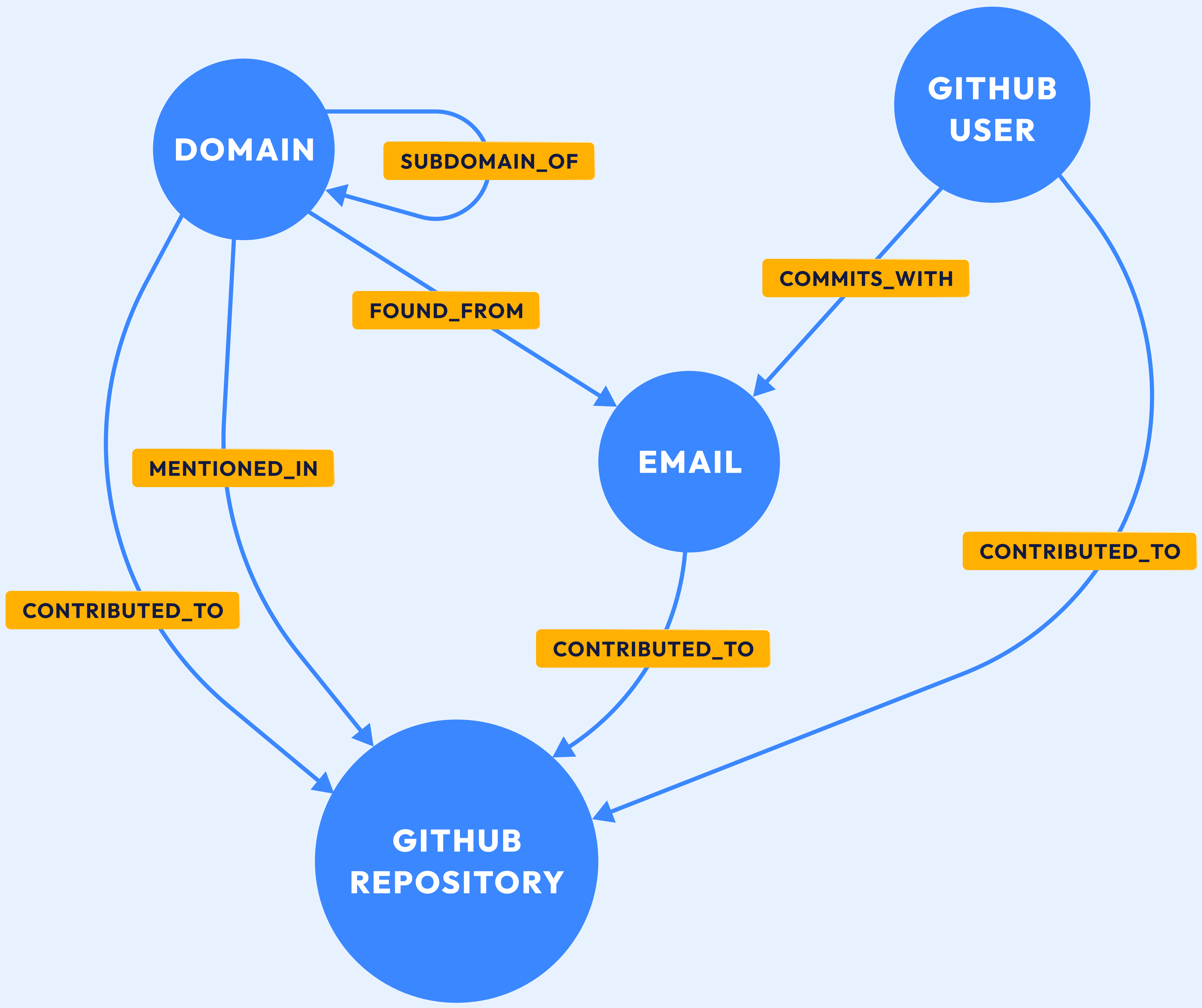
E-Commerce Company's CTI Team's Challenges

It was impossible for the multinational e-commerce giant's Cyber Threat Intelligence (CTI) team to manually keep track of all the different domains (across multiple countries), and linking each developer to each public asset.

The Implementation

The CTI team searched for a platform that could monitor sensitive information on their GitHub repositories. They wanted to gather data on commits, leaked secrets, and email addresses.

By tracking asset relations between GitHub repositories, users, domains, and emails (in diagram below), Flare enables this CTI team to understand any issues related with GitHub leaked secrets without cumbersome manual searches.



Flare enables this team to automatically track asset relations between GitHub repositories, users, domains, and emails.

Through Flare, the CTI team can now easily view:

- All the GitHub repositories in which a sensitive domain asset is mentioned and identify the GitHub users and emails committing into it
- All the GitHub repositories in which the emails from the organization are committing publicly and order them by number of commits and leaked secrets
- All the GitHub repositories in which specific monitored actors are committing publicly and identify those containing leaked secrets

Impact and Benefits

After implementing Flare, the CTI team monitors the public GitHub event feed, creates documents for every monitored commit, and maps the relationships between different assets and collaborators.

This allows for the creation of API endpoints that enable exploration of the gathered data, such as listing GitHub repositories with mentions of sensitive domains, listing repositories with commits from a specific domain, or listing email addresses associated with commits in a monitored repository. By implementing this solution, the client stays on top of potential security breaches and keeps sensitive information secure.

Since starting Flare, the CTI team has caught numerous API key and code leaks. With the comprehensiveness of GitHub monitoring, this CTI team is confident in securing GitHub.

Learn more about our solution →

Request a Demo

flare

flare.io

hello@flare.io