SUCCESS STORY

E-Commerce Giant Radically Simplifies GitHub Leak Monitoring

The Customer

- E-Commerce industry
- Multinational distributed teams
- Fortune 100 company

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.

> **“It was impossible before to keep track of all developer actions happening in GitHub for distributed multinational developer teams, but with Flare we know for sure that we’re monitoring everything accurately, automatically, and consistently.”**
>
> CTI Analyst, Fortune 100 E-Commerce Company

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.

As teams collaborate across distributed teams and remote workers, the potential for sensitive information leaking on clear web platforms such as GitHub can increase dramatically. Our customer, a Fortune 100 company, sought out Flare to monitor sensitive information on their GitHub repositories.

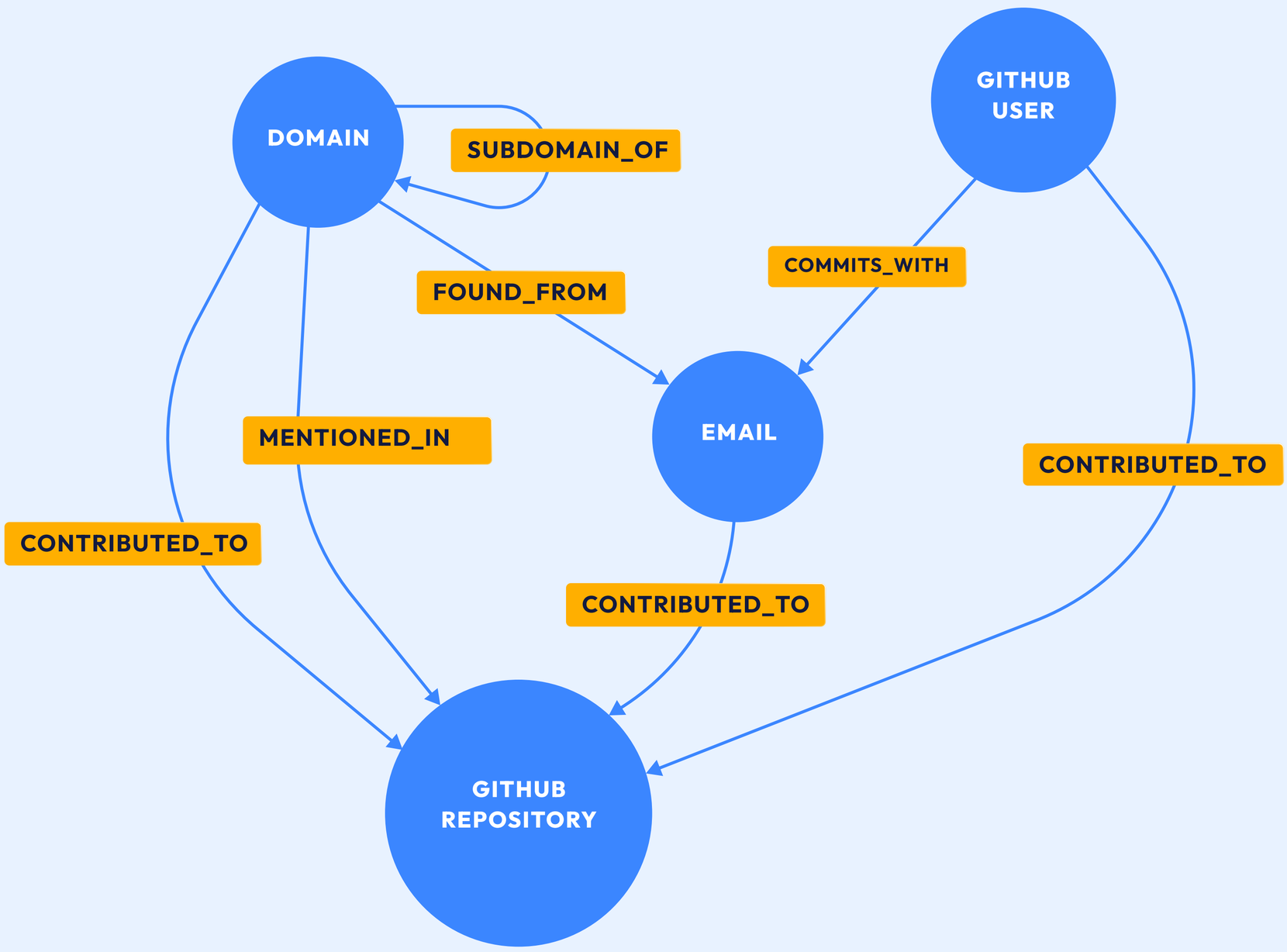
Challenge: Too Difficult to Manually Monitor Developers' GitHub Work Across Distributed Teams

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

The security team wanted to gather data on commits, leaked secrets, and email addresses.

Benefit: Automate Asset Tracking Relations in GitHub

By tracking asset relations between GitHub repositories, users, domains, and emails (in diagram below), Flare enables this security 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 security 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**

After implementing Flare, the security 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 security team has caught numerous API key and code leaks. With the comprehensiveness of Flare's GitHub monitoring, this security team is confident in securing these clear web leaks.