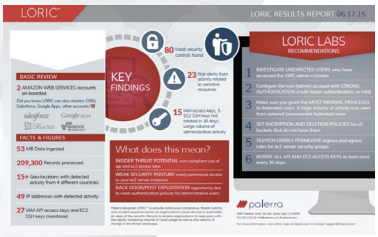
LORIC™ for GitHub



Get a free assessment of usage, threats and compliance violations in your GitHub environment

Cloud Security is a Shared Responsibility

Cloud services are a growing target and in extreme cases, breaches have put companies out of business. Code Spaces is one such example where it had to close doors in June 2014 after hackers gained privileged access to its AWS environment and destroyed critical assets.

Protection of customer data is a priority for GitHub and it takes numerous steps to reduce risk. However, cloud security is a shared responsibility between the organization and the cloud provider. Security of the cloud infrastructure is GitHub's responsibility, while access and usage of the data stored in GitHub is the organization's responsibility.

Terms of Service for GitHub

You expressly understand and agree that GitHub shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data or other intangible losses (even if GitHub has been advised of the possibility of such damages), resulting from: ... (iii) unauthorized access to or alteration of your transmissions or data;

An organization's obligations include being able to answer questions such as:

- Have any privileged accounts been created that may serve as potential backdoors to the repositories?
- Has anyone intentionally or accidentally destroyed any repositories and deleted company IP?
- Has anyone changed GitHub security configurations and made the environment more vulnerable?

There are a number of challenges in meeting these obligations:

- Access to logs and metadata is limited reducing visibility into activities
- Detection of anomalous activity is challenging due to the volume of log data, lack of activity baselines, and lack of context
- Manual monitoring of security configurations and activities is laborious and error-prone
- Remediation requires subject matter expertise in GitHub

Security & Governance for GitHub

PPalerra enables organizations to protect data within GitHub with LORIC™, the cloud security automation platform. It is the only solution to manage the entire security lifecycle of cloud data in a single platform.

VISIBILITY: Insights into GitHub adoption and usage

THREAT DETECTION: Monitoring for anomalous activities

COMPLIANCE MANAGEMENT: Monitoring of configurations and activities leading to policy violations

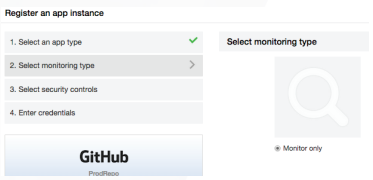
INCIDENT RESPONSE: Logging and remediation

Automation of threat detection, compliance management and incident response with LORIC increases operational efficiency and enables staff to focus on more strategic initiatives. It is delivered as a service and can be deployed in minutes. LORIC enables security and governance for GitHub without altering the native user experience for users.

palerra

3945 Freedom Circle Suite 560 Santa Clara CA 95054 /// 650 300 5222 /// info@palerra.com /// palerra.com

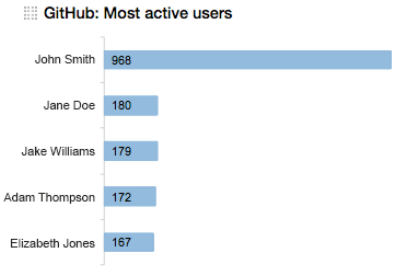
EFFORTLESS DEPLOYMENT



Get started in minutes by creating a GitHub service account for LORIC. No hardware, no software, no agents.

INSIGHTS

Instant insights into adoption and usage of GitHub, such as the most active users.

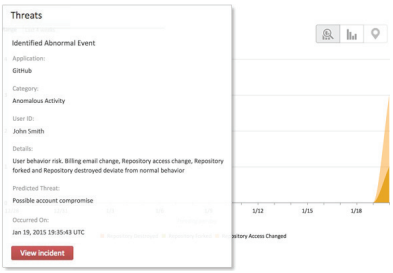


ACTIVITY REPORTS

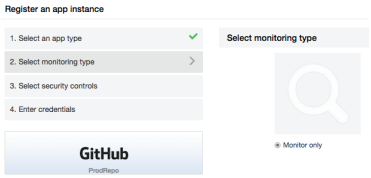
Ability to create custom reports as well as a rich set of predefined reports on potentially risky activities such adding users to repositories.

USER BEHAVIOR ANALYTICS

Studies activities for each GitHub user to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.



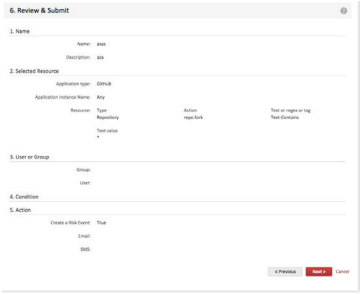
CONFIGURATION MONITORING



Continuously monitors security configurations within GitHub to ensure compliance – say goodbye to laborious manual audits.

MONITORING POLICIES

Ability to build custom policies as well as a library of predefined policies for real-time notifications about activities that may introduce risks, such as granting administrator privileges to a user.



AUTOMATIC INCIDENT RESPONSE

Category	Priority	Details
Anomalous Activity	High	User behavior risk. Billing email change, Repository access change, Repository forked and Repository destroyed deviate from normal behavior
Cross Application Activity	High	User risk threat. Suspicious usage of administrative privilages in two applications within a short period of time.

Automatically logs incidents and executes remedial actions within GitHub ensuring incidents are addressed immediately.

ECOSYSTEM INTEGRATION

Leverages existing IT investments by integrating with LDAP, single sign on, identity and access management, ticketing, and incident management solutions.