Monitoring use of Git repositories

Scenario: To facilitate team member collaboration, your organization uses cloud-based code collaboration and version control for sharing computer program source code and associated documentation. This system allows for sharing but also introduces the potential of intellectual property loss via data exfiltration through a systems breach or insider threat. You need some fundamental procedures for detecting insider threat behavior that could be indicative of data exfiltration. Your challenge is being able to separate out normal access to anomalous access. You can use Splunk software to monitor who is accessing specific Git repositories, what actions they take in those repositories, and how their activities compare to those of their peers. You can identify first-time access to repos and compare what is accessed with the role and responsibilities of the identity making the access. You can use Splunk software for statistical analyses like frequency, patterns of access, and time of day information. These approaches use correlations and enrichment.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Software engineer
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data:
  - Code management data
  - Git access logs

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor use of Git repositories. Depending on what information you have available, you might find it useful to identify some or all of the following:

- First time accessing an internal Git repository
- Increase in source code downloads

Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Identity management with roles, responsibilities, teams, and current project assignments to aid in identifying anomalous access from inside.

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that...
can be useful to monitor when implementing this use case:

- Access counts by user to detect anomalous patterns
- Count of downloads to detect anomalous increases

---

**Additional resources**

This use case is also included in the [Splunk Security Essentials](#) app, which provides more information about how to implement the use case successfully in your security maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf Talk: [Making Splunk development a breeze with a deep dive on DevOps containerization, version control, and automation](#)
- Conf Talk: [Extending Splunk MLTK using GitHub Community](#)
- Blog: [Github just got Splunked](#)
- Context: [Detect insider threat](#)