



# DevOps

Security Controls in Shared Source Code Repositories by  
James Brown

# Topics

- **What is a security incident?**
- **Common Security threats in version control software:**
- **Common Security threats in version control software:**
- **Why do we need security in repos?**
- **Github Security Controls**
- **Pros**
- **Best Practices**

# What is a security incident?

Security incidents relate to when an “event leads to a violation of an organization’s security policies” (CyberShark). This can include:

- -passwords stored in an unsecured manner
- -data breach
- -Unauthorized access to internal systems
- -Unauthorized changes are made to a repo

# Common Security threats in version control software

- Unauthorized access to restricted source code
- Source code may provide clues to how an attacker can attack software running in an application
- Login credentials getting stored
- Insider threats



A thick yellow vertical bar on the left side of the slide, with a horizontal extension at the top.

# Why do we need security in repos?

- If we do not maintain security controls in repositories, it can lead to:
- Repos getting deleted with authorization
- Malicious cyber attacks on a repo
- Sensitive data getting accessed
- Unauthorized code changes



## Github Security Controls

Github offers a wide variety of security controls to ensure your repositories are safe. Some features include:

- Two factor authentication
- Security audit logs
- Git over SSH and HTTPS
- Read only deploy keys
- Required reviews
- And much more

# Pros

Security controls in GitHub prevent the following:

- Loss of customer trust
- Imposed fines by the government if a breach were to occur
- Brand reputation being damaged
- Customer abandonment

# Best Practices

---



There's no one best practice solve that makes repository security management full proof. It takes a collective of things.



Don't store login credentials in Github.



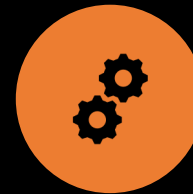
Triple check repository security settings



Collect GitHub logs



Perform routine scans of developer accounts



Automate monitoring



## Sources:

- Murphy, R. (2019, September 05). What Is the Difference Between a Security Incident and a Security Breach? Retrieved August 26, 2020, from <https://www.blackstratus.com/what-is-the-difference-between-a-security-incident-and-a-security-breach/>
- Saurabh, K. (2018, April 18). It's Time to Take GitHub Threats Seriously. Retrieved August 26, 2020, from <https://www.darkreading.com/application-security/its-time-to-take-github-threats-seriously/a/d-id/1331577>