Security Architecture Narrative

Githaxs

August 2021

Contents

1 Security Architecture Narrative **3**

2 Githaxs Product Architecture **3**

3 Githaxs Infrastructure **3**
3.1 Product Infrastructure 3
3.1.1 Authorized Personnel 3
3.2 IT Infrastructure 3

4 Githaxs Workstations **3**
4.1 Remote Access 3

5 Access Review **4**

6 Penetration Testing **4**

7 Githaxs Physical Security **4**

8 Risk Assessment **4**
8.1 Adversarial Threats 4
8.2 Non-Adversarial Threats 4

9 References **5**
9.1 Narratives 5
9.2 Policies 5
9.3 Procedures 5

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.6, CC6.7, CC7.1, CC7.2

Table 2: Document history

Date	Comment
Aug 25 2021	Initial document

1 Security Architecture Narrative

Here we narrate why our org satisfies the control keys listed in the YML block

2 Githaxs Product Architecture

Describe product architecture here, emphasizing security implications

3 Githaxs Infrastructure

3.1 Product Infrastructure

Describe product infrastructure, emphasizing security measures

3.1.1 Authorized Personnel

- **AWS root account** access is granted only to the CTO and CEO
- **AWS IAM** access is granted to to a limited group of **Operators**
- **Githaxs SSH** access is granted to a limited group of **Operators**
- **Githaxs DB** access is granted to a limited group of **Data Operators**

3.2 IT Infrastructure

Githaxs uses the following cloud services for its internal infrastructure:

- AWS

Access to these cloud services is limited according to the role of the Githaxs employee and is reviewed quarterly as well as via regular onboarding/offboarding tasks for new and departing employees.

4 Githaxs Workstations

Githaxs workstations are hardened against logical and physical attack by the following measures:

- operating system must be within one generation of current
- full-disk encryption
- onboard antivirus/antimalware software
- OS and AV automatically updated

Workstation compliance with these measures is evaluated on a quarterly basis.

4.1 Remote Access

Many Githaxs employees work remotely on a regular basis and connect to production and internal IT systems via the same methods as those employees

connecting from the Githaxs physical office, i.e., direct encrypted access to cloud services. It is the employee's responsibility to ensure that only authorized personnel use Githaxs resources and access Githaxs systems.

5 Access Review

Access to Githaxs infrastructure, both internal and product, is reviewed quarterly and inactive users are removed. Any anomalies are reported to the security team for further investigation. When employees start or depart, an onboarding/offboarding procedure is followed to provision or deprovision appropriate account access.

6 Penetration Testing

Githaxs commissions an external penetration test on an annual basis. All findings are immediately reviewed and addressed to the satisfaction of the CTO/CEO.

7 Githaxs Physical Security

Githaxs has no physical locations.

Githaxs infrastructure is located within AWS. Githaxs does not have physical access to AWS infrastructure.

8 Risk Assessment

Githaxs updates its Cyber Risk Assessment on an annual basis in order to keep pace with the evolving threat landscape. The following is an inventory of adversarial and non-adversarial threats assessed to be of importance to Githaxs.

8.1 Adversarial Threats

The following represents the inventory of adversarial threats:

Threat	Source	Vector	Target	Likelihood	Severity

8.2 Non-Adversarial Threats

The following represents the inventory of non-adversarial threats:

Threat	Vector	Target	Likelihood	Severity

9 References

9.1 Narratives

Products and Services Narrative System Architecture Narrative

9.2 Policies

Encryption Policy Log Management Policy Office Security Policy Remote Access Policy Security Incident Response Policy Workstation Policy

9.3 Procedures

Apply OS Patches Review & Clear Low-Priority Alerts Review Access Review Devices & Workstations