Security Architecture Narrative

Sour Lemon Digital, LLC

May 2023

Contents

Table 1: Control satisfaction

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

Table 2: Document history

Date	Comment
Nov 1 2022	Initial document

1 Security Architecture Narrative

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

2 Monicur Journey Product Architecture

Describe product architecture here, emphasizing security implications

3 Sour Lemon Digital, LLC 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**
- **Monicur Journey SSH** access is granted to a limited group of **Operators**
- **Monicur Journey DB** access is granted to a limited group of **Data Operators**

3.2 IT Infrastructure

Monicur Journey uses the following cloud services for its internal infrastructure:

- List cloud services

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

4 Sour Lemon Digital, LLC Workstations

Sour Lemon Digital, LLC 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

Sour Lemon Digital, LLC employees working remotely on a regular basis and connect to production and internal IT systems via the same methods as those employees connecting from eventual physical offices, i.e., direct encrypted access to cloud services. It is the employee's responsibility to ensure that only authorized personnel use Sour Lemon Digital, LLC resources and access related systems.

5 Access Review

Access to Sour Lemon Digital, LLC 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

Sour Lemon Digital, LLC commissions an external penetration test on an annual basis. All findings are immediately reviewed and addressed to the satisfaction of the CTO/CEO.

7 Sour Lemon Digital, LLC Physical Security

Sour Lemon Digital, LLC has one physical location, Iowa City, IA. Key issuance is tracked by the Human Resources Division. Office keys are held by office personnel and custodial staff. These keys are also tracked by Human Resources Division. Sour Lemon Digital, LLC managers regularly review physical access privileges.

Sour Lemon Digital, LLC infrastructure is located within AWS. Sour Lemon Digital, LLC does not have physical access to AWS infrastructure.

8 Risk Assessment

Sour Lemon Digital, LLC 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 Sour Lemon Ditial.

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