Security Architecture Narrative

ACME Evil Anvil Corporation

January 2019

Contents

1 Security Architecture Narrative **3**

2 ACME Evil Anvil Corporation Product Architecture **3**

3 ACME Evil Anvil Corporation Infrastructure **3**
3.1 Product Infrastructure 3
3.1.1 Authorized Personnel 3
3.2 IT Infrastructure 3

4 ACME Evil Anvil Corporation Workstations **3**
4.1 Remote Access 4

5 Access Review **4**

6 Penetration Testing **4**

7 ACME Evil Anvil Corporation Physical Security **4**

8 Risk Assessment **5**
8.1 Adversarial Threats 5
8.2 Non-Adversarial Threats 5

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
Jun 1 2018	Initial document

1 Security Architecture Narrative

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

2 ACME Evil Anvil Corporation Product Architecture

Describe product architecture here, emphasizing security implications

3 ACME Evil Anvil Corporation 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**
- **ACME Evil Anvil Corporation SSH** access is granted to a limited group of **Operators**
- **ACME Evil Anvil Corporation DB** access is granted to a limited group of **Data Operators**

3.2 IT Infrastructure

ACME Evil Anvil Corporation 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 ACME Evil Anvil Corporation employee and is reviewed quarterly as well as via regular onboarding/offboarding tasks for new and departing employees.

4 ACME Evil Anvil Corporation Workstations

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

5 Access Review

Access to ACME Evil Anvil Corporation 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

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

7 ACME Evil Anvil Corporation Physical Security

ACME Evil Anvil Corporation has one physical location, in San Francisco, CA. Key issuance is tracked by the Office Physical Security Policy Ledger. Office keys are additionally held by the lessor, property management, and custodial staff. These keys are not tracked by the Office Physical Security Policy Ledger. ACME Evil Anvil Corporation managers regularly review physical access privileges.

ACME Evil Anvil Corporation infrastructure is located within AWS. ACME Evil Anvil Corporation does not have physical access to AWS infrastructure.

8 Risk Assessment

ACME Evil Anvil Corporation 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 ACME Evil Anvil Corporation.

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