

\$4.3M - \$12.3M

Total Unmitigated Financial Exposure

Across 5 critical & high severity findings in your AWS environment

3 Critical

2 High

4 Medium

Findings

CRITICAL

Unencrypted S3 Buckets Containing PII

Resource

s3://acmefs-customer-data-prod, s3://acmefs-audit-logs (+ 12 more)

Description

14 S3 buckets with server-side encryption disabled contain customer PII fields. Data is stored in plaintext, violating GDPR Article 32 and SOC 2 CC6.1.

Frameworks

GDPR

SOC 2

HIPAA

Auto-Remediation: AWS CLI -- enforce SSE-S3 on all buckets

```
# Enable default encryption on every unencrypted bucket
aws s3api list-buckets --query 'Buckets[].Name' --output text | \
  tr '\t' '\n' | while read BUCKET; do
  aws s3api put-bucket-encryption \
    --bucket "$BUCKET" \
    --server-side-encryption-configuration '{
      "Rules":[{"ApplyServerSideEncryptionByDefault":
        {"SSEAlgorithm":"AES256"}}]}'
done

# Verify (repeat for each bucket):
aws s3api get-bucket-encryption --bucket acmefs-customer-data-prod
```

Financial Exposure

Category	Low	High
GDPR regulatory fines	\$1.2M	\$3.1M
Litigation & settlements	\$0.6M	\$1.8M
Operational remediation	\$0.3M	\$0.9M
Total Exposure	\$2.1M	\$5.8M

HIGH

No Incident Response Plan

Resource

Organization-wide -- no IR runbook found in any repo or wiki

Description

No documented or tested incident response procedure exists. SOC 2 CC7.3 and ISO 27001 A.16.1 require a defined IR process. Absence was flagged in last external audit.

Frameworks

SOC 2

ISO 27001

Auto-Remediation: Terraform -- provision IR runbook S3 bucket and SNS alerting topic

```
resource "aws_s3_bucket" "ir_runbooks" {
  bucket = "acmeefs-ir-runbooks-${var.env}"
  tags   = { Compliance = "SOC2-CC7.3" }
}

resource "aws_sns_topic" "ir_alerts" {
  name = "acmeefs-incident-response"
}

resource "aws_sns_topic_subscription" "ir_email" {
  topic_arn = aws_sns_topic.ir_alerts.arn
  protocol  = "email"
  endpoint  = var.security_team_email
}
```

Financial Exposure

Category	Low	High
SOC 2 audit failure cost	\$200K	\$600K
Litigation exposure	\$300K	\$900K
Operational downtime	\$300K	\$800K
Total Exposure	\$800K	\$2.3M

CRITICAL

Unaudited Third-Party API Access

Resource

IAM users: stripe-webhook-prod, datadog-agent, sendgrid-relay (+ 6 more)

Description

9 external vendor integrations hold active IAM credentials with broad permissions. Access has not been reviewed in 18+ months. Violates PCI-DSS Requirement 8.6 and GDPR data processor obligations.

Frameworks

PCI-DSS

GDPR

SOC 2

Auto-Remediation: AWS CLI -- rotate and scope third-party IAM credentials

```
# List all IAM users with access keys older than 90 days
aws iam generate-credential-report
aws iam get-credential-report --query 'Content' --output text | \
  base64 -d | awk -F, '$10 != "N/A" && $10 < "$(date -d '-90 days' +%Y-%m-%d)"' | \
  cut -d, -f1

# For each stale user -- create new key, update secret, delete old key:
aws iam create-access-key --user-name stripe-webhook-prod
# (update key in vendor dashboard, then:)
aws iam delete-access-key --user-name stripe-webhook-prod \
  --access-key-id AKIA_OLD_KEY_ID

# Attach a least-privilege inline policy (example for Stripe webhook user):
aws iam put-user-policy \
  --user-name stripe-webhook-prod \
  --policy-name LeastPrivilege \
  --policy-document file://policies/stripe-webhook-policy.json
```

Financial Exposure

Category	Low	High
PCI-DSS fines & re-audit	\$500K	\$1.5M
Reputational / customer churn	\$600K	\$1.8M
Operational containment	\$300K	\$900K
Total Exposure	\$1.4M	\$4.2M

