SunTzu CyberSecurity Labs LLC

SECURITY INTELLIGENCE & RISK ANALYSIS

Email Trust & Impersonation Review

External email authentication, impersonation resistance, and identity exposure assessment

Sanitized copy. Selected identifying or technical details have been replaced or removed.

CLIENT Client Organization	CUSTOMER ID Redacted
PRIMARY TARGET target1.example (192.0.2.1)	ASSESSMENT ID SAMPLE
COMPLETED Aug 28, 2026	REPORT GENERATED Sep 01, 2026

Public website sample. Customer-identifying and sensitive technical details have been sanitized.

Executive Summary

Why this matters: Fraudulent email that appears to come from your domain can be used to steal credentials, redirect payments, impersonate executives, and damage customer trust. This assessment tests whether receiving mail systems have enough externally visible evidence and policy direction to distinguish authorized mail from spoofed mail.

What This Means for Your Domain

target1.example was rated weak for externally observable email impersonation resistance. Production header evidence confirmed DKIM pass using target1.example across 2 samples; DMARC is published with p=none and reporting configured. Mail routing appears to use HostedEmail / GoDaddy. SPF is absent or unconfirmed, so authorized senders are not fully defined by a published SPF policy; DMARC is monitoring-only and does not request quarantine or rejection of failing mail; MTA-STS was not observed; SMTP TLS reporting was not observed; BIMI was not observed; it is optional and should follow mature DMARC enforcement. Production header evidence confirmed authenticated alignment and a DMARC pass for the observed mail path; repeat this validation after provider, sender, or DNS changes.

target1.example has a material direct-spoofing gap. SPF is not published, so the domain does not define an SPF sender authorization policy. DMARC is monitoring-only, so it does not ask receivers to quarantine or reject messages that fail authentication. The sampled legitimate mail passed aligned DKIM, which is a useful protection for that sending path, but it does not replace SPF or an enforcing DMARC policy.

What the Scan Found

ASSESSED DOMAIN

target1.example

Mail provider: HostedEmail / GoDaddy

IMPERSONATION RESISTANCE

Weak

Material findings require action.

Next owner action: Material email-authentication weaknesses were confirmed. Address the listed core-control findings before relying on the domain's current impersonation resistance.

Continuous service recommended: For this weak posture, continuous service should support the SPF and DMARC enforcement rollout, validate legitimate senders, and watch for delivery impact or unauthorized traffic during each change.

Scope and Observed Assets

Consolidated identity view

Related hostnames, addresses, services, and URLs are consolidated using evidence-backed relationships so one host is not repeated as several unrelated report assets.

Asset	Observed forms	Scope	Findings
target1.example (192.0.2.1)	ip, subdomain 2 linked records	In scope	3

Email Trust and Impersonation Posture

Passive external assessment

DOMAIN IMPERSONATION RESISTANCE

Weak

The observed email-authentication posture does not currently demonstrate strong domain impersonation resistance. SPF was not observed; DMARC is monitoring-only. Production header evidence already confirms DKIM signing and alignment for the observed path; the remaining deficiencies still prevent a strong posture.

Target Domain

Domain	Mail Provider	Mail Routing	Observed MX Hosts
target1.example	HostedEmail / GoDaddy	Enabled	target4.example

Authentication Controls

Control	Assessment	Evidence Found	Interpretation
SPF	ABSENT	No SPF record observed Header result: NONE	No SPF policy was observed for the assessed email domain.
DKIM	PRESENT	Production header: PASS; selector dkim_key	Production header evidence confirmed DKIM pass and alignment for target1.example.
DMARC	PRESENT	v=DMARC1; p=none; rua=mailto:contact4@example.test	DMARC was externally confirmed.
DMARC Enforcement	ABSENT	v=DMARC1; p=none; rua=mailto:contact4@example.test	DMARC is deployed but configured with p=none. The domain receives monitoring visibility but does not instruct receivers to quarantine or reject failing messages.
DMARC Reporting	PRESENT	v=DMARC1; p=none; rua=mailto:contact4@example.test	DMARC Reporting was externally confirmed.

Public Identity Exposure

7
Target-domain identities observed

3
Role accounts observed

1
Potential high-value identities

Highest targeting score

Publicly observable email identities can assist legitimate customers and partners, but they can also provide targeting information for phishing, business email compromise, and impersonation attempts. Exposure is therefore reported as context rather than treated automatically as a vulnerability.

Additional Mail Security Controls

Control	Assessment	Owner Action	Security Context
Mail Routing	Present	Maintain and revalidate after DNS or provider changes.	Email Mail Routing was externally confirmed.
MTA-STS	Not observed	Consider implementing MTA-STS with a valid published policy to strengthen inbound SMTP transport security.	No MTA-STS DNS signaling record was observed.
TLS-RPT	Not observed	Publish a TLS-RPT policy and monitor reports for SMTP transport-security failures.	No SMTP TLS reporting policy was observed.
BIMI	Not observed	Consider BIMI only after SPF, DKIM and DMARC enforcement are mature and operationally validated.	No BIMI record was observed. BIMI is an optional identity enhancement rather than a core email-authentication requirement.

Evidence classification: Third-party email domains observed on authorized public content are retained as supporting evidence but are not treated as customer-owned domains and do not determine the target domain's security posture.

Email Identity Intelligence

Observed Email Identities

The following email identities were observed through authorized passive analysis of publicly accessible content. Classification reflects each address's relationship to the assessed domain.

Your Domain

Email Address	Classification	Targeting	Confidence
contact1@example.test	Potential high-value	83	95%
contact2@example.test	Role account	73	95%
contact3@example.test	Role account	73	95%
contact4@example.test	Observed identity	58	95%
contact5@example.test	Observed identity	58	95%
contact6@example.test	Observed identity	58	95%
contact7@example.test	Observed identity	58	99%

Related Domains

Email Address	Domain	Classification	Targeting
contact8@example.test	target2.example	Role account	20

External / Third-Party Identities

Email Address	Domain	Relationship
contact9@example.test	target3.example	Third-party observed
contact10@example.test	does-not-exist.invalid	Third-party observed

External and third-party email identities are retained as supporting evidence because they were observed on authorized public content. They are not treated as customer-owned assets and do not contribute to the assessed domain's email-security posture.

Key Findings

Critical through low severity

Weak Domain Impersonation Resistance

MEDIUM

Asset	target1.example
Location	Domain Impersonation Controls
Category	Email Security

Description: The observed email-authentication posture does not currently demonstrate strong domain impersonation resistance. SPF was not observed; DMARC is monitoring-only. Production header evidence already confirms DKIM signing and alignment for the observed path; the remaining deficiencies still prevent a strong posture.

Evidence: Removed from this sanitized copy

Recommendation: Strengthen SPF, DKIM and DMARC alignment and enforcement and reduce unnecessary exposure of high-value email identities.

SPF Policy

MEDIUM

Asset	target1.example
Location	Email Authentication / DNS
Category	Email Security

Description: No SPF policy was observed for the assessed email domain.

Evidence: Removed from this sanitized copy

Recommendation: Publish a valid SPF policy covering all legitimate sending services and use an appropriately restrictive terminal mechanism after validation.

DMARC Enforcement

LOW

Asset	target1.example
Location	Email Authentication / DMARC
Category	Email Security

Description: DMARC is deployed but configured with p=none. The domain receives monitoring visibility but does not instruct receivers to quarantine or reject failing messages.

Evidence: Removed from this sanitized copy

Recommendation: After validating legitimate mail flows, progress DMARC from monitoring toward quarantine and ultimately reject where operationally appropriate.

Security Improvement Plan

Remediation Plan

This plan translates the assessment findings into specific corrective actions for target1.example. Provider-specific values are identified where they must be obtained from your production email or DNS services.

> **Current posture:** WEAK **Target posture:** STRONG
> **Remaining Strong-posture blockers:** 2

Path to Strong Impersonation Resistance

Control	Current	Required Target	Status
SPF	Absent	Valid and confirmed for all authorized senders	Action required
DKIM	Present	Confirmed production signing and alignment	Satisfied
DMARC	Present	Published and valid	Satisfied
DMARC Reporting	Present	Aggregate reporting operational	Satisfied
DMARC Enforcement	Absent	Quarantine or reject after validation	Action required

A Strong posture is expected after the required authentication controls are implemented and verified. The final posture must be confirmed through post-remediation validation.

Remediation Priority 1

SPF — Publish and Validate an SPF Policy

Current State

SPF is currently assessed as absent for target1.example.

Required State

Your domain should publish one valid SPF policy that authorizes every legitimate system permitted to send email using your domain.

Required Changes

- Identify every legitimate service that sends email using @target1.example.
- Publish a single SPF TXT policy containing the mechanisms required by those authorized senders.
- Use a restrictive terminal policy after all legitimate senders have been validated.

Configuration Guidance

target1.example TXT

```
v=spf1 <AUTHORIZED-SENDERS> -all
```

Important: Do not publish this example as written. <AUTHORIZED-SENDERS> must be replaced with the SPF mechanisms required by your legitimate email-sending services.

Information Required Before Implementation

- Primary outbound email provider
- Website or application mail services
- CRM and sales platforms
- Marketing or bulk-email platforms
- Billing and accounting platforms
- Support or ticketing systems
- Any other service that sends email using @target1.example

Implementation Procedure

1. Create an inventory of all authorized outbound email sources.
2. Obtain the required SPF include, IP, or other authorized mechanisms from each sending provider.
3. Consolidate the authorized mechanisms into one SPF record for the domain.

4. Check the resulting policy for SPF syntax and DNS lookup-limit compliance before publication.
5. Publish the validated TXT record through the authoritative DNS provider.

Validation Procedure

1. Confirm exactly one SPF policy is published.
2. Validate SPF syntax.
3. Validate the SPF DNS lookup count.
4. Send representative production messages from each authorized sending service.
5. Confirm SPF authentication succeeds.
6. Confirm authenticated messages align with the intended DMARC domain.

Expected Result

Authorized senders pass SPF while unauthorized systems are not permitted by the domain's SPF policy. Successful validation removes SPF as a blocker to stronger impersonation resistance.

Remediation Priority 3

DMARC — Progress DMARC to Enforcement

Current State

A DMARC policy is present, but enforcement is currently assessed as absent. The observed posture is consistent with monitoring rather than active rejection or quarantine of unauthenticated mail.

Required State

After legitimate sending sources have been validated, your DMARC policy should progress from monitoring toward enforcement, ultimately using p=reject where operationally appropriate.

Required Changes

- Review DMARC aggregate reporting to identify legitimate and unauthorized sending sources.
- Correct SPF and DKIM authentication or alignment for legitimate senders before enforcement.
- Progress the DMARC policy through a controlled enforcement rollout.
- Continue monitoring DMARC reports for legitimate mail affected by the policy.

Configuration Guidance

_dmarc.target1.example TXT

```
v=DMARC1; p=<ENFORCEMENT-POLICY>; <PRESERVE-VALID-REPORTING-AND-POLICY-TAGS>
```

Important: Do not publish this example as written. Preserve valid reporting and policy parameters from your production DMARC record. Select quarantine or reject only after legitimate mail flows have been validated.

Information Required Before Implementation

- Current production DMARC TXT record
- Recent DMARC aggregate-report results
- Validated inventory of legitimate sending sources
- Confirmation that legitimate senders satisfy SPF or DKIM alignment

Implementation Procedure

1. Review current DMARC aggregate reports and inventory all legitimate sending sources.
2. Remediate SPF and DKIM authentication/alignment failures for legitimate mail.
3. Move from monitoring to a controlled quarantine policy when legitimate traffic is ready.
4. Monitor delivery and DMARC aggregate reports during the enforcement period.

5. Progress to reject after legitimate mail streams have been validated and policy impact is understood.

Validation Procedure

1. Confirm the DMARC TXT record parses correctly.
2. Confirm aggregate reporting remains operational.
3. Verify representative authorized mail passes DMARC through aligned SPF or DKIM.
4. Verify unauthorized test conditions do not receive unintended authorization.
5. Review aggregate reports after each enforcement change for legitimate delivery impact.

Expected Result

DMARC moves from monitoring toward active enforcement, materially reducing the ability of unauthorized senders to impersonate the domain.

Implementation Services

Remediation Assistance Available

SunTzu CyberSecurity Labs can implement the recommended email-authentication and DNS changes, coordinate provider-specific configuration requirements, validate authorized sending systems, and perform post-remediation testing to verify the resulting security posture.

Remediation Objective

Move the assessed domain from its current Weak impersonation-resistance posture toward Strong while minimizing the risk of disrupting legitimate email delivery.

Remediation should be followed by post-change validation to confirm authentication behavior, alignment, enforcement, and the resulting impersonation-resistance posture.

Methodology and Limitations

Assessment Activities

- Authorized domain normalization and passive DNS review
- Mail exchanger and provider identification
- SPF, DMARC, and commonly published DKIM selector assessment
- MTA-STS, TLS reporting, and BIMI record review
- Passive email exposure correlation when data is available

Scope Boundary

Testing was limited to the authorized email domain and externally observable email-security information. Related or third-party domains and addresses observed on authorized public content were retained as evidence but were not automatically treated as customer-owned infrastructure or authorization to assess those domains.

Limitations

Results represent a point-in-time passive external assessment. DNS records, mail-routing information, public email identities, and commonly used DKIM selectors were reviewed without sending mail, authenticating to customer systems, accessing mailboxes, or attempting to deliver spoofed messages.

DKIM selectors are not globally predictable. Failure to discover a selector through passive testing does not prove DKIM is absent. Production message headers can provide stronger evidence of DKIM signing and DMARC alignment when such evidence is available.

Public email-address exposure is reported as targeting context. The presence of a publicly listed email address is not, by itself, treated as a vulnerability.

Recommended Use

Use this report to prioritize remediation and follow-up validation. Findings should be evaluated alongside asset ownership, business criticality, compensating controls, and operational context.

Tech Findings, Remediations and Recommendations

Owner action register

This final register consolidates the scan evidence into technical findings, the corrective action indicated by the evidence, and a practical owner recommendation. Confirmed protections are included so the report documents what should be preserved as well as what should change.

Technical Evidence Summary

Evidence	Observed Value	Meaning
Mail routing	`target4.example`	Identifies the externally published inbound mail path and apparent provider.
SPF record	`Not observed`	Defines which systems are authorized to send mail for the domain.
DKIM selectors	`Not observed`	Shows discoverable public keys; production message validation is still required.
DMARC record	`v=DMARC1; p=none; rua=mailto:contact4@example.test`	Defines authentication policy, enforcement, and reporting destinations.
MTA-STS / TLS-RPT	MTA-STS not observed; TLS-RPT not observed	These controls improve and monitor transport security for inbound SMTP.
Production header authentication	2 samples; DKIM pass; SPF none; DMARC pass; TLS1_3	Message-level evidence verifies actual authentication and transport behavior beyond DNS configuration alone.

Technical Action Register

Domain impersonation resistance — Not confirmed

RECOMMENDED HARDENING

Finding: The observed email-authentication posture does not currently demonstrate strong domain impersonation resistance. SPF was not observed; DMARC is monitoring-only. Production header evidence already confirms DKIM signing and alignment for the observed path; the remaining deficiencies still prevent a strong posture.

Remediation: Strengthen SPF, DKIM and DMARC alignment and enforcement and reduce unnecessary exposure of high-value email identities.

Recommendation: Validate a representative production message for SPF/DKIM alignment and DMARC pass behavior.

SPF — Absent

RECOMMENDED HARDENING

Finding: No SPF policy was observed for the assessed email domain.

Remediation: Publish a valid SPF policy covering all legitimate sending services and use an appropriately restrictive terminal mechanism after validation.

Recommendation: Maintain one valid SPF record, inventory every authorized sender, and revalidate after sender or DNS changes.

DKIM — Present

CONFIRMED PROTECTION

Finding: Production header evidence confirmed DKIM pass and alignment for target1.example.

Remediation: No corrective action indicated by this external scan.

Recommendation: Confirm each production sending platform signs with an aligned domain; rotate keys according to provider guidance.

DMARC — Present

CONFIRMED PROTECTION

Finding: DMARC was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Continue reviewing DMARC reports and progress toward p=reject when all legitimate mail streams are validated.

DMARC reporting — Present

CONFIRMED PROTECTION

Finding: DMARC Reporting was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Confirm the reporting mailbox is monitored and that aggregate reports are retained for trend review.

DMARC enforcement — Absent

RECOMMENDED HARDENING

Finding: DMARC is deployed but configured with p=none. The domain receives monitoring visibility but does not instruct receivers to quarantine or reject failing messages.

Remediation: After validating legitimate mail flows, progress DMARC from monitoring toward quarantine and ultimately reject where operationally appropriate.

Recommendation: Treat quarantine as active enforcement and evaluate a controlled move to reject after validating legitimate senders.

Mail routing — Present

CONFIRMED PROTECTION

Finding: Email Mail Routing was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Confirm the observed MX provider and records remain authorized and remove stale routing entries.

MTA-STS — Not confirmed

RECOMMENDED HARDENING

Finding: No MTA-STS DNS signaling record was observed.

Remediation: Consider implementing MTA-STS with a valid published policy to strengthen inbound SMTP transport security.

Recommendation: Implement MTA-STS after confirming the production MX endpoints support the required TLS behavior.

TLS-RPT — Not confirmed

RECOMMENDED HARDENING

Finding: No SMTP TLS reporting policy was observed.

Remediation: Publish a TLS-RPT policy and monitor reports for SMTP transport-security failures.

Recommendation: Publish TLS-RPT and monitor reports for inbound SMTP transport security failures.

BIMI — Not confirmed

OPTIONAL ENHANCEMENT

Finding: No BIMI record was observed. BIMI is an optional identity enhancement rather than a core email-authentication requirement.

Remediation: No core security remediation is required.

Recommendation: Consider BIMI only as a later brand-trust enhancement after DMARC enforcement and operational monitoring are mature.

Public email identity exposure — Present

CONFIRMED PROTECTION

Finding: Public Email Address Exposure was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Perform a manual public-footprint review and retain only the organizational addresses that serve a business need.

High-value identity exposure — Present

CONFIRMED PROTECTION

Finding: High-Value Email Identity Exposure was externally confirmed.

Remediation: No corrective action indicated by this external scan.

Recommendation: Manually review exposure of executive, finance, privileged, and other high-value identities and apply phishing-resistant MFA.

Recommended Continuous Protection

Continuous Email Trust Monitoring

This assessment is a point-in-time baseline. Email providers, DNS records, authorized sending platforms, DKIM keys, and publicly exposed identities change over time. Continuous monitoring detects control drift and suspicious sending activity before the next scheduled assessment.

For this weak posture, continuous service should support the SPF and DMARC enforcement rollout, validate legitimate senders, and watch for delivery impact or unauthorized traffic during each change.

- Alert on SPF, DKIM, DMARC, MX, MTA-STS, and TLS-RPT record changes
- Collect and review DMARC aggregate reports for authorized and suspicious senders
- Maintain the inventory of services permitted to send as the domain
- Validate representative production headers after provider or DNS changes
- Track public and high-value email identity exposure
- Provide a recurring owner summary of posture, changes, incidents, and next actions

SunTzu CyberSecurity Labs can operate this service as the ongoing control layer after remediation, with alerts and recurring reporting tied to the assessed domain.

Confused or Unsure What to Do Next?

Email security can feel like evil wizardry: DNS records, authentication alignment, provider settings, reporting feeds, and delivery risk all have to work together. You do not need to translate or implement this report alone.

SunTzu CyberSecurity Labs can identify your legitimate sending services, prepare provider-safe DNS changes, implement SPF, DKIM, DMARC, MTA-STS, and TLS-RPT, validate production mail, and operate the continuous monitoring program.

Contact SunTzu CyberSecurity Labs to schedule an Email Security Remediation and Continuous Monitoring consultation.