ARTIFACT SECURITY

Email Phishing & BEC Evaluation Methodology

ARTIFACT SECURITY

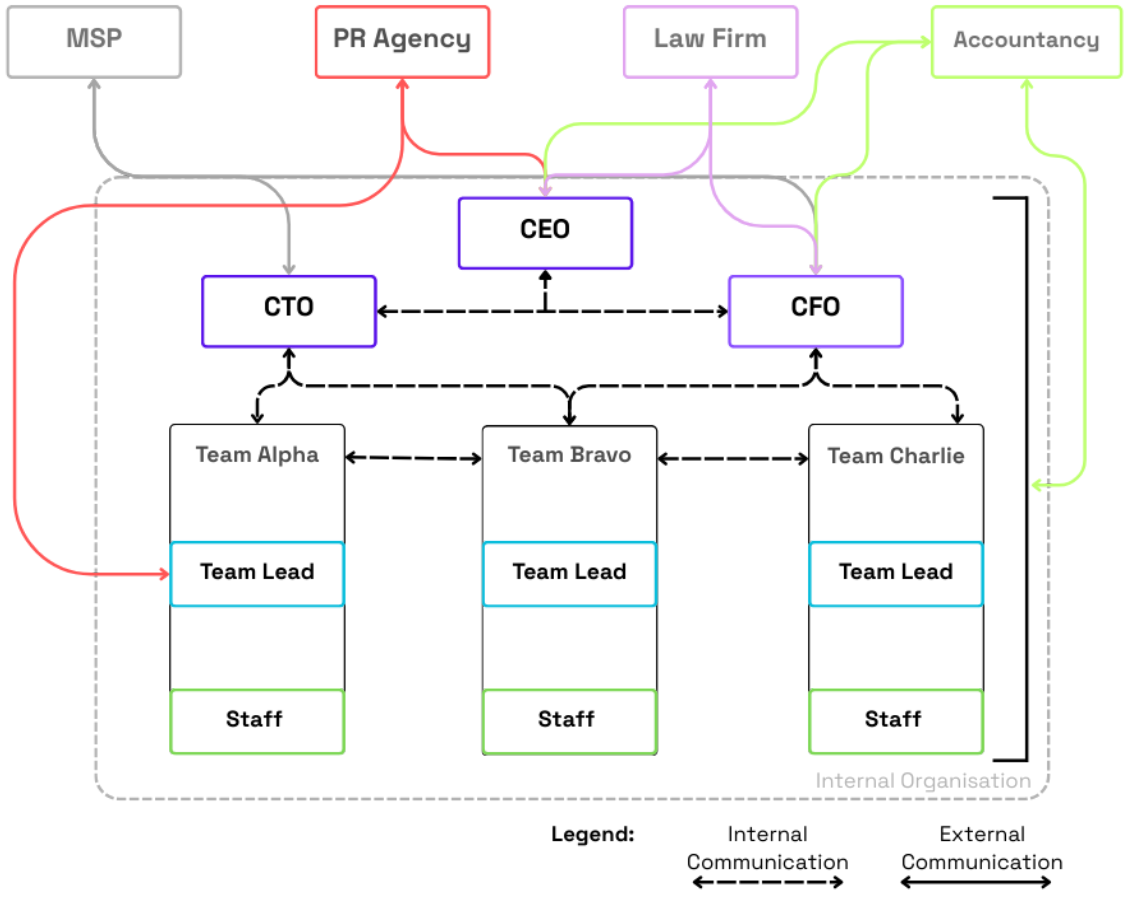
1. Goals

This evaluation aims to measure the effectiveness of email security solutions when defending against Phishing & Business Email Compromise (BEC).

The secondary goal is to evaluate Remediation Capabilities, measuring how effectively a solution can contain a threat after delivery, identify account takeovers and roll back malicious configuration changes.

2. Environment

A Target Organisation simulation is maintained with persistent digital identities and communication patterns reflecting a typical SME. This environment creates a baseline of ”normal” behavior that offers the opportunity of realistic behaviour to be analysed by the security solution.



Internal Personas and Communication Patterns

The staffing model utilizes three primary tiers to simulate organizational hierarchy and cross-departmental trust.

Source	Destination	Direction	Frequency	Type
Executive Tier (CEO, CFO)	Team Leads	Bi-directional	Medium	Financial authorization, high-value strategic directives.
Operational Management (Project Leads)	Staff Members	Bi-directional	High	Task coordination, standard document exchange (Office files).
Support Infrastructure (IT Support)	All Staff	One-way	Low	Technical broadcasts, system updates, helpdesk links.
Finance/HR Team	All Staff	Bi-directional	Medium	Payroll updates, PII collection, tax requests.

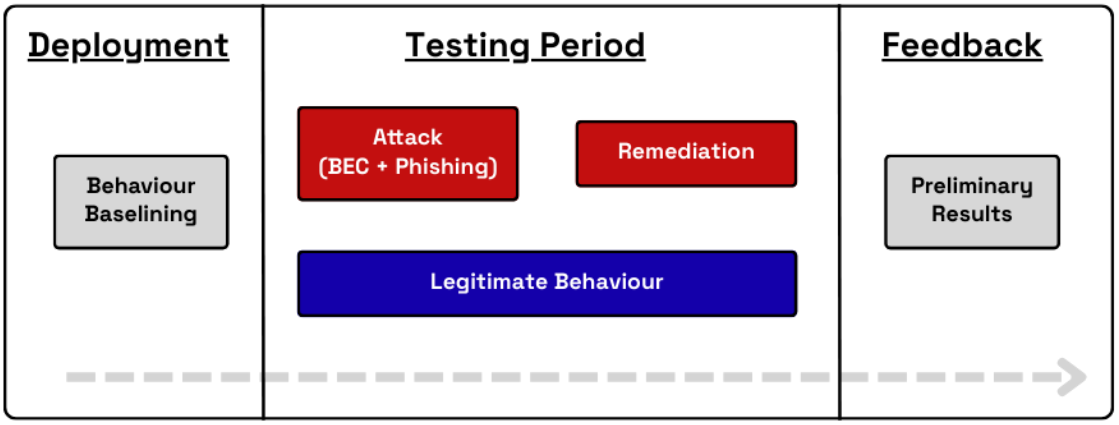
External Ecosystem Patterns

BEC often involves the impersonation of trusted external partners. As such 4 partners are set up.

Source	Destination	Direction	Frequency	Type
Accountancy Firm	CFO / Finance	Bi-directional	Medium	Invoices, wire transfer details, bank updates.
Law Firm	CEO / CFO	Bi-directional	Low	Confidential legal documents, sensitive data.
PR Agency	CEO/General Staff	Bi-directional	Medium	Media Strategy, press releases, standard Office Files
MSP	IT Support	One-way	Low	Procurement quotes, technical attachments.

3. Execution

The evaluation follows a 3-phase testing structure to ensure both preventive and reactive capabilities are tested under realistic conditions.



1. Behaviour Baselining (up to 2 Weeks): The solution observes the Target Organisation to populate identity graphs and learn relationship cadences (e.g., the CFO typically communicates with the Accountancy firm on Tuesdays).
2. Attack Period: Delivery of the BEC and Phishing corpus.
3. Remediation Phase: Triggered for attacks that bypass initial filters. Evaluates the solution's ability to "claw back" mail and clean up mail rules.
4. Legitimate Behaviour: Measured throughout to identify "alert fatigue" caused by false positives.

4. Attack Scenarios & Evasion

The attack corpus is mapped to known adversary behaviors and modern evasion techniques.

Across the testing period a minimum of 500 emails are received by the target users. The number of emails exchanged during the Testing Period does not deviate from the Baseline period's volume by more than 30%.

Evasion Methods

Evasion methods considered in scope (not an exhaustive list).

- Quishing (QR Phishing): Malicious links embedded in QR code images or ASCII art.
- HTML Smuggling: Malicious Javascript embedded in attachments to bypass gateway scans.

- Thread Hijacking: Using compromised accounts to reply within existing trusted conversations.
- Lookalike/Homoglyph Domains: Using characters from different alphabets to visually mimic legitimate corporate domains.

5. Rating

BEC attack rating:

Stage	Description	Points
Priming Emails	The email or malicious content/intent is blocked or removed from the user's reach. Clawback emails are given full credit but represented in a report for full transparency.	+2
CTA/Payload/ Malicious intent Email	The email or malicious content/intent can reach the user without admin request but is flagged as malicious. Post-delivery notifications or modifications are given full credit but represented in a report for full transparency.	+8
NOTE: Priming emails points can be retroactively applied upon successful identification of the malicious thread. All malicious emails in the chain must be appropriately flagged for full marks.		

Phishing protection rating:

Severity Level	Description	Rating
Red/High (Block/Clawback/ Quarantine)	The email or malicious content/intent is blocked or removed from the user's reach. Clawback emails are given full credit but represented in a report for full transparency.	+10
Amber - User Accessible	The email or malicious content/intent can reach the user without admin request but is flagged as malicious. Post-delivery notifications or modifications are given full credit but represented in a report for full transparency.	+8
None	The email is delivered without any intervention from the security product.	0

Remediation Rating

Remediation is defined as the product's ability to mitigate threats already inside the tenant. Points are awarded based on response efficiency and scope. Automated responses are recorded and showcased in reports as **Automation Rating**. Defined as the percentage of remediation done without human operators.

Remediation Capability	Description	Rating
Account/Session Containment	Password resets or revocation of OAuth session tokens for compromised accounts.	+10
Mail Rule Cleanup	Deletion of unauthorized "auto-forwarding" or "move to folder" rules.	+10
MTTR (Mean Time to Remediate)	Time from detection to full containment.	Given as HH:MM:SS

7. Legitimate Rating

Alert efficiency is critical for operational success. Solutions are penalized for interrupting legitimate communication.

Severity Level	Description	Unknown Behaviour	Learned Behaviour
None	Email delivered successfully.	+10	+10
Amber - User Accessible	Email flagged or placed in a user accessible folder/quarantine.	0	-5
Red/High (Block/Clawback)	Email blocked from reaching the recipient or removed post-delivery.	-10	-10

8. Awards

Awards are based on **Total Accuracy** calculated as

Attack Rating + Remediation Rating + Legitimate Rating

Award	Thresholds
Platinum	90% ≤ 100%
Gold	80% ≤ 89%
Silver	70% ≤ 79%
Bronze	60% ≤ 69%

9. Configuration Disclosure

Full configuration and licensing details must be disclosed in the event of a public report. This is hosted on Artifact Security publicly available resources. Links to vendor resources are also accepted.

10. Change Log

10/03/2026 - v1.0 Document Created - Identifier: Email Evaluation 2026 V1