Incident Response Triage Toolkit

User Guide (Customer and Technical)
Clearnet OSINT + Exposure Checks

Version: 0.2.x
Date: 2026-02-26

Use only with explicit permission from the person or organization being assessed.
This guide contains no personal names or customer data.

About this guide

This document explains how to run the Incident Response Triage Toolkit safely and how to interpret the results. It contains two guides:
1) Customer Guide (non-technical)
2) Technical Guide (IT / security staff)

A full Dutch translation is included in the second half of this document.

Key principles:

- Consent first: only run checks for identifiers you are authorized to assess.
- Minimum data: only collect what you need for the case.
- Evidence-minded: keep outputs unchanged and record what actions you took.
- No dark-web crawling: this tool uses clearnet OSINT and approved APIs only.

Quick Start (5 minutes)

Use this if you just want to run a safe first scan.

Recommended launch	Run_Triage.cmd (keeps the window open).
Inputs you need	Case name, customer label, emails, domains, optional usernames.
Best first checks	DNS + WHOIS, Certificate Transparency, and (if available) breach checks via API.
Where results go	C:\ProgramData\...\cases\<CASE>\<timestamp>\ (default).

Step-by-step:

- Start the tool via Run_Triage.cmd (installed: Start Menu -> Run (Recommended); portable: Run_Triage.cmd).
- Enter a case name (example: ACME-2026-02-26) and a customer label (example: ACME Ltd).
- Paste identifiers as comma-separated lists: emails, domains, usernames.
- Type YES to confirm consent.
- Choose checks to run. For a first run, enable DNS + WHOIS and Certificate Transparency.
- When finished, open the case folder and read Incident-Notes.md.

Safety and privacy tips

- Prefer app-based MFA or security keys instead of SMS where possible (reduces SIM-swap risk).
- Treat unexpected calls/SMS/emails as suspicious during an incident. Verify using official numbers.
- Do not share evidence packs through insecure channels. Use encrypted storage or a secure portal.
- Use Redact PII when you plan to share reports outside your team or store multiple customers in one place.
- Keep an incident timeline: who did what, when, and why.

If you are under active attack (15-minute checklist)

- Secure the primary email account first: change password, enable MFA, and review recent sign-ins.
- Check email settings for forwarding rules and unknown app access; remove anything you do not recognize.
- If your phone number is targeted: request SIM-swap/port-out protection and add an account passphrase with the provider.
- Enable bank alerts and watch for new payees or unknown direct debits.
- Pause and verify: do not click links in unexpected messages; use official websites/apps instead.

Part A - Customer Guide (English)

What the tool does

- Checks whether provided emails appear in known breach datasets (if a breach API is configured).
- Checks whether provided emails appear in paste references (metadata only).
- Collects passive information about your domains (DNS, WHOIS, certificates) to spot exposure risks.
- Creates a structured evidence pack for documentation.

What the tool does not do

- It does not hack systems and does not attempt to access private accounts.
- It does not crawl hidden services (.onion) or the dark web.
- It does not download leaked content by default. It records references and metadata.

Before you start (customer checklist)

- Confirm you want this assessment and you understand which identifiers will be checked.
- Prepare the identifiers: emails you use, domains you own/control, and optional online usernames.
- Decide whether you want results saved with redaction (recommended for privacy).
- If you suspect account takeover: change passwords and enable MFA on your primary email first.

Running the tool

When the tool starts, it asks for the following. Use simple values; no special characters needed.

1) Output folder

This is where results are stored. The default location is recommended because it works for all users:
C:\ProgramData\Mismoosh\IncidentResponseTriage

2) Case name

A short label for this investigation. Good examples:

- ACME-2026-02-26
- Client-Email-Exposure-Feb2026
- Domain-Review-Q1-2026

3) Customer label

A readable name for the customer or organization (example: ACME Ltd).

4) Emails

Enter emails separated by commas. Include personal and business emails that matter for the incident.

Example:

security@acme.nl, admin@acme.nl, owner@gmail.com

5) Domains

Enter domains separated by commas. Include all domains the customer owns or operates.

Example:

acme.nl, acme.com

6) Usernames (optional)

Enter online usernames/handles separated by commas. Use only those the customer confirms are theirs.

7) Consent confirmation

Type YES when asked. If consent is not confirmed, the tool exits.

8) Redact PII (recommended)

If enabled, emails/domains/usernames are stored as hashes in the saved JSON outputs. This protects privacy if the evidence pack is forwarded.

Choosing checks to run (simple guidance)

DNS + WHOIS	Good first choice for domain risk review. No API key required.
Certificate Transparency (crt.sh)	Find subdomains that have had public certificates (helps discover forgotten services).
Breach checks (API)	If configured, checks emails against known breach datasets. Useful after a suspected leak.
Paste references (API)	If configured, checks for paste references (metadata).
Monitoring mode	Saves a baseline and highlights new findings on later runs.

Where results are saved (what to look at)

Open the case folder and focus on these files first:

- reports\Incident-Notes.md - human-readable notes and action checklist.
- evidence\json\findings.json - structured findings (best for technical review).
- logs\events.jsonl - step-by-step log (useful if troubleshooting).
- evidence\raw\ - raw DNS/WHOIS outputs (evidence).

What to do after the scan (common next steps)

- Secure the primary email account: change password, enable MFA, review logins and forwarding rules.
- Secure telecom account if personal data leaked: ask the provider for SIM-swap/port-out protection and a passphrase.
- Review bank security: enable alerts, watch for new direct debits, contact the bank if suspicious transactions occur.
- Beware of follow-up scams: attackers often impersonate telecoms, banks, or compensation services.
- If you see active fraud or account takeover, contact local authorities and your bank promptly.

Troubleshooting

- Black window appears and closes: start with Run_Triage.cmd so you can see prompts and errors.
- No results folder: check the output folder you selected and search for a folder named 'cases'.
- Breach checks fail: the API key may be missing or incorrect; run DNS/WHOIS checks first.
- Corporate firewall blocks lookups: try from a network that allows DNS/WHOIS or ask IT to allow the traffic.

Part B - Technical Guide (English)

System requirements

- Windows 10/11 recommended.
- Windows PowerShell 5.1 for best compatibility with packaging tools.
- Network access for DNS/WHOIS and any enabled APIs.
- Optional: breach API key(s) managed securely (do not hard-code into distributed builds).

Operational model (recommended)

- Run per customer case with a unique case name.
- Store output under ProgramData to avoid permissions issues.
- Use Redact PII by default if outputs will be stored centrally or shared.
- Keep a signed consent statement or ticket reference for each case.

Non-interactive execution (parameters)

You can run the script with parameters for automation. Examples:

```
powershell.exe -ExecutionPolicy Bypass -File .\Mismoosh_IncidentResponse_Triage.ps1 -CaseName "ACME-2026-02-26" -CustomerName "ACME Ltd" -Emails "security@acme.nl","it@acme.nl" -Domains "acme.nl" -EnableDnsWhois -EnableCrtSh -ConfirmConsent -RedactPII
```

```
powershell.exe -ExecutionPolicy Bypass -File .\Mismoosh_IncidentResponse_Triage.ps1 -CaseName "ACME-Monitor" -CustomerName "ACME Ltd" -Emails "security@acme.nl" -Domains "acme.nl" -EnableDnsWhois -EnableCrtSh -MonitoringMode -ConfirmConsent -RedactPII
```

Output structure

Each run creates a timestamped folder under:

```
<OutDir>\cases\<CaseName>\<YYYYMMDD_HHMMSS>\
```

Key files:

- manifest.json - run configuration and environment metadata.
- evidence/json/findings.json - all collected results.
- logs/events.jsonl - JSONL event log suitable for ingestion.
- reports/Incident-Notes.md - analyst notes and actions checklist.
- reports/diff.json - only when MonitoringMode is enabled and a baseline exists.

Evidence integrity (best practices)

- Do not edit raw evidence outputs. If you must annotate, use the notes file.
- Store a SHA256 checksum file for release artifacts (EXE, installer, portable ZIP).
- If you move evidence, keep a chain-of-custody note (who copied it, when, and where).

Monitoring mode (how it works)

Monitoring mode stores a baseline state and produces a diff on later runs. Use a consistent CaseName for the same customer/monitoring stream.

- First run: creates baseline.
- Next runs: generates reports/diff.json with newly observed items.
- Recommended cadence: weekly for SMB; daily only if incident is active.

Scheduling (Windows Task Scheduler)

Example: run weekly as SYSTEM and write to ProgramData. Adjust paths to your install location.

```
schtasks /Create /SC WEEKLY /D MON /TN "IR-Triage-ACME" /TR "powershell.exe -NoProfile -ExecutionPolicy Bypass -File \"C:\Program Files (x86)\Incident Response Triage Toolkit\Mismoosh_IncidentResponse_Triage.ps1\" -CaseName \"ACME-Monitor\" -CustomerName \"ACME Ltd\" -Emails \"security@acme.nl\" -Domains \"acme.nl\" -EnableDnsWhois -EnableCrtSh -MonitoringMode -ConfirmConsent -RedactPII" /RU SYSTEM
```

Packaging and distribution (EXE + installer)

- Compile script to EXE for double-click usability (console visible is recommended for interactive prompts).
- Ship an installer for customers plus a portable ZIP for on-site engineers.
- Provide SHA256SUMS.txt on your download page.
- Consider code signing to reduce SmartScreen warnings.

Customer safety tips (what to recommend)

- Enable MFA on primary email and critical accounts.
- Ask telecom provider for SIM-swap and port-out protections if personal data may have leaked.
- Warn about targeted phishing/scams after a public breach.
- Use a password manager and unique passwords; avoid password reuse.
- Escalate to professional DFIR if you see re-compromise, unknown admin accounts, or financial fraud.

Deel C - Klantgids (Nederlands)

Wat deze tool doet

- Controleert of opgegeven e-mailadressen voorkomen in bekende datalekken (als een lek-API is ingesteld).
- Controleert of e-mailadressen voorkomen in paste-verwijzingen (alleen metadata).
- Verzamelt passieve informatie over domeinen (DNS, WHOIS, certificaten) om blootstellingsrisico's te vinden.
- Maakt een gestructureerd bewijspakket voor incidentdocumentatie.

Wat deze tool niet doet

- De tool hackt niets en probeert geen toegang te krijgen tot priveaccounts.
- De tool crawlt geen hidden services (.onion) of het dark web.
- De tool downloadt standaard geen gelekte inhoud. Alleen verwijzingen en metadata worden opgeslagen.

Voor je begint (checklist)

- Bevestig dat je deze controle wilt en welke identifiers worden gecontroleerd.
- Verzamel de juiste identifiers: e-mails, domeinen die je bezit/beheert en optioneel usernames.
- Kies of je resultaten met redactie (privacy) wilt opslaan (aanbevolen).
- Bij vermoeden van account overname: beveilig eerst je primaire e-mailaccount (wachtwoord + MFA).

De tool uitvoeren

De tool vraagt om de volgende velden. Houd het eenvoudig; geen speciale tekens nodig.

1) Output map

Hier worden de resultaten opgeslagen. De standaardlocatie is aanbevolen:
C:\ProgramData\Mismoosh\IncidentResponseTriage

2) Case naam

Korte naam voor dit onderzoek. Voorbeelden:

- ACME-2026-02-26
- Klant-Email-Exposure-Feb2026
- Domein-Review-Q1-2026

3) Klantlabel

Leesbare naam voor de klant of organisatie (bijvoorbeeld: ACME Ltd).

4) E-mails

Voer e-mails in, gescheiden door komma's.

Voorbeeld:

security@acme.nl, admin@acme.nl, owner@gmail.com

5) Domeinen

Voer domeinen in, gescheiden door komma's.

Voorbeeld:

acme.nl, acme.com

6) Usernames (optioneel)

Voer online usernames/handles in, alleen als de klant bevestigt dat ze van hem/haar zijn.

7) Toestemming

Typ YES om toestemming te bevestigen. Zonder toestemming stopt de tool.

8) PII redactie (aanbevolen)

Als dit aan staat, worden e-mails/domeinen/usernames als hashes opgeslagen in JSON outputs. Dit beschermt privacy bij delen of centrale opslag.

Welke checks kies je? (snelle uitleg)

DNS + WHOIS	Goede eerste keuze voor domeincontrole. Geen API key nodig.
Certificate Transparency (crt.sh)	Vindt subdomeinen die in publieke certificaten zijn gezien.
Lekcontrole (API)	Als ingesteld: controleert e-mails tegen bekende datalekken.
Paste verwijzingen (API)	Als ingesteld: controleert paste-verwijzingen (metadata).
Monitoring mode	Slaat een baseline op en markeert nieuwe bevindingen bij volgende runs.

Waar staan de resultaten?

Open de case map. Deze bestanden zijn het belangrijkst:

- reports\Incident-Notes.md - leesbare notities en checklist.
- evidence\json\findings.json - alle bevindingen (gestructureerd).
- logs\events.jsonl - log voor troubleshooting.
- evidence\raw\ - ruwe DNS/WHOIS output (bewijs).

Na de scan (aanbevolen acties)

- Beveilig primaire e-mail: nieuw wachtwoord, MFA, controleer logins en forwarding rules.
- Beveilig telecom account bij mogelijk datalek: vraag om SIM-swap/port-out bescherming en een passphrase.
- Controleer bankbeveiliging: alerts aanzetten, let op onbekende incasso's, neem contact op bij verdachte transacties.
- Let op scams: aanvallers doen zich vaak voor als telecom, bank of 'compensatie' dienst.

- Bij actieve fraude: neem direct contact op met bank en lokale autoriteiten.

Problemen oplossen

- Zwart venster en meteen weg: start via Run_Triage.cmd zodat je prompts en fouten ziet.
- Geen output map: controleer de output folder en zoek naar een map 'cases'.
- Lekchecks falen: API key kan ontbreken of fout zijn; draai eerst DNS/WHOIS checks.
- Firewall blokkeert lookups: probeer een netwerk dat DNS/WHOIS toelaat of vraag IT om toegang.

Deel D - Technische gids (Nederlands)

Systeemeisen

- Windows 10/11 aanbevolen.
- Windows PowerShell 5.1 (beste compatibiliteit met packaging tools).
- Netwerktoegang voor DNS/WHOIS en eventuele APIs.
- Optioneel: API keys veilig beheren (niet hardcoden in builds die je verspreidt).

Aanpak (aanbevolen werkwijze)

- Werk per klant met een unieke case naam.
- Gebruik ProgramData als output om permissieproblemen te voorkomen.
- Gebruik PII redactie standaard bij centrale opslag of delen.
- Leg toestemming vast (formulier, ticketnummer of e-mail) per case.

Niet-interactief draaien (parameters)

Voor automatisering kun je parameters gebruiken. Voorbeelden:

```
powershell.exe -ExecutionPolicy Bypass -File .\Mismoosh_IncidentResponse_Triage.ps1 -CaseName "ACME-2026-02-26" -CustomerName "ACME Ltd" -Emails "security@acme.nl","it@acme.nl" -Domains "acme.nl" -EnableDnsWhois -EnableCrtSh -ConfirmConsent -RedactPII
```

```
powershell.exe -ExecutionPolicy Bypass -File .\Mismoosh_IncidentResponse_Triage.ps1 -CaseName "ACME-Monitor" -CustomerName "ACME Ltd" -Emails "security@acme.nl" -Domains "acme.nl" -EnableDnsWhois -EnableCrtSh -MonitoringMode -ConfirmConsent -RedactPII
```

Output structuur

Elke run maakt een timestamp folder onder:

```
<OutDir>\cases\<CaseName>\<YYYYMMDD_HHMMSS>\
```

Belangrijkste bestanden:

- manifest.json - configuratie en environment metadata.
- evidence/json/findings.json - alle resultaten.
- logs/events.jsonl - JSONL log (handig voor ingest).
- reports/Incident-Notes.md - notities en acties.
- reports/diff.json - alleen bij MonitoringMode + bestaande baseline.

Bewijs en integriteit (best practices)

- Wijzig raw evidence outputs niet. Gebruik notities voor annotaties.
- Publiceer SHA256 checksums voor release bestanden (EXE, installer, portable ZIP).
- Als je bewijs verplaatst: noteer chain-of-custody (wie, wanneer, waarheen).

Monitoring mode

Monitoring mode slaat een baseline op en maakt later een diff met nieuwe items. Gebruik dezelfde CaseName voor dezelfde monitoring stream.

- Eerste run: maakt baseline.
- Volgende runs: reports/diff.json met nieuwe bevindingen.
- Aanbevolen frequentie: wekelijks voor MKB; dagelijks bij actieve incidenten.

Plannen (Taakplanner)

Voorbeeld: wekelijks draaien als SYSTEM. Pas paden aan naar jouw installatie.

```
schtasks /Create /SC WEEKLY /D MON /TN "IR-Triage-ACME" /TR "powershell.exe -NoProfile -ExecutionPolicy Bypass -File \"C:\Program Files (x86)\Incident Response Triage Toolkit\Mismoosh_IncidentResponse_Triage.ps1\" -CaseName \"ACME-Monitor\" -CustomerName \"ACME Ltd\" -Emails \"security@acme.nl\" -Domains \"acme.nl\" -EnableDnsWhois -EnableCrtSh -MonitoringMode -ConfirmConsent -RedactPII" /RU SYSTEM
```

Distributie (EXE + installer)

- Compileer naar EXE voor gebruiksgemak (console zichtbaar voor prompts).
- Lever een installer voor klanten en een portable ZIP voor engineers on-site.
- Plaats SHA256SUMS.txt op je downloadpagina.
- Overweeg code signing om SmartScreen waarschuwingen te verminderen.

Veiligheidsadvies voor klanten

- MFA aanzetten op primaire e-mail en kritieke accounts.
- Telecom bescherming vragen (SIM-swap/port-out) bij mogelijk datalek.
- Waarschuw voor gerichte phishing/scams na een datalek.
- Gebruik password manager en unieke wachtwoorden; geen hergebruik.
- Schakel professionele DFIR in bij re-compromise, onbekende admin accounts of financiele fraude.

Appendix - Suggested consent text (English)

Use this or your own legal text. Keep it short and explicit:

"I authorize the operator to run OSINT and exposure checks for the identifiers I provide (emails/domains/usernames) for the purpose of security assessment and incident response. I confirm I have the authority to provide these identifiers."

Bijlage - Voorbeeld toestemmingstekst (Nederlands)

Gebruik dit of je eigen juridische tekst. Houd het kort en duidelijk:

"Ik geef toestemming om OSINT- en blootstellingschecks uit te voeren voor de identifiers die ik aanlever (e-mailadressen/domeinen/usernames) met als doel beveiligingsanalyse en incident response. Ik bevestig dat ik bevoegd ben om deze identifiers aan te leveren."