Robust Inbox Forwarding Rule Exfil in Splunk — Risk-Based Enrichment (SPL Included)

Triage & detection for mailbox auto-forward/redirect rules—enriched with freemail/disposable domain flags, WHOIS age, and threat feeds—so exfil attempts pop out from the noise.

SPL Included

PREREQUISITES

- **Lookups** (optional but recommended): `freemail_domains.csv` (domain → `is_freemail`), `disposable_domains.csv` (domain → `is_disposable`), `whois_domains.csv` (domain → `created_epoch` or `age_days`), `otx_domains.csv` (domain → `otx_pulse_count`), `openphish_domains.csv` (domain → `openphish_flag`)
- **Custom command**: `ipqs` (e.g., `domain=<domain>` emits `ipqs.domain_risk_score`)
- Field names differ by source; use `coalesce()` and adjust `index`/`sourcetype` to your environment.

SPL A — Triage Defender “Suspicious Inbox Forwarding Rule” (domain reputation + risk)

```
/* Purpose: Triage Defender alert about inbox forwarding/redirect rules and enrich the desti
   Works with M365 Defender / Defender for Office 365 alerts ingested to Splunk.
   Pre-reqs (all optional but recommended):
     - freemail_domains.csv (domain -> is_freemail=Yes/No)
     - disposable_domains.csv (domain -> is_disposable=Yes/No)
     - whois_domains.csv (domain -> created_epoch)  // or age_days
     - otx_domains.csv (domain -> otx_pulse_count)
     - openphish_domains.csv (domain -> openphish_flag=1)
     - Custom command: ipqs domain=<domain>  // emits ipqs.domain_risk_score
*/

index=azure (sourcetype=m365:defender:alert OR sourcetype=azure:defender:cloudalert)
| search alert_display_name IN ("Suspicious inbox forwarding rule","Suspicious inbox rule","
| eval user=coalesce(user_principal_name, tostring(properties.userPrincipalName,""), user)
| eval rule_name=coalesce(tostring(properties.ruleName,""), tostring(properties."ruleDetails
```

```
| eval fwd_to_raw=coalesce(tostring(properties."ruleDetails.forwardTo",""), tostring(additio
| mvexpand fwd_to_raw
| eval fwd_to=trim(fwd_to_raw)
| where len(fwd_to)>0
/* Extract destination domain */
| rex field=fwd_to "(?i)@(?<fwd_domain>[^ >;,'\"\"]+)$"
| where isnotnull(fwd_domain)
/* Enrichment lookups (best-effort) */
| lookup freemail_domains domain AS fwd_domain OUTPUT is_freemail
| lookup disposable_domains domain AS fwd_domain OUTPUT is_disposable
| lookup whois_domains domain AS fwd_domain OUTPUT created_epoch
| eval domain_age_days = if(isnull(created_epoch), null(), round((now() - created_epoch)/864
| lookup otx_domains domain AS fwd_domain OUTPUT otx_pulse_count
| lookup openphish_domains domain AS fwd_domain OUTPUT openphish_flag
| ipqs domain=fwd_domain
| rename ipqs.domain_risk_score AS domain_risk
/* Risk fusion */
| eval risk = 25 /* base for forwarding rule */
  + case(is_freemail="Yes",10, true(),0)
  + case(is_disposable="Yes",25, true(),0)
  + case(isnotnull(domain_age_days) AND domain_age_days<=30,20, true(),0)
  + case(coalesce(otx_pulse_count,0)>=1,20, true(),0)
  + case(coalesce(openphish_flag,0)>=1,25, true(),0)
  + round(coalesce(domain_risk,0)/5,0)
/* Keep material risk */
| where risk>=50
| table _time alert_id alert_severity user rule_name fwd_to fwd_domain is_freemail is_dispos
| sort - _time
```

SPL B — Direct detector from Exchange Unified Audit Log (source-of-truth)

```
/* Purpose: Catch mailbox-forwarding exfil setups directly from Exchange audit logs and enri
   Telemetry: O365 Management Activity (Unified Audit Log) -> Exchange / Mailbox rules & mai
   We look for:
     - New-InboxRule with ForwardTo/RedirectTo to an external domain
     - Set-Mailbox with ForwardingSmtpAddress (server-side forwarding)
   Same enrichments as in (A).
*/

index=o365 sourcetype=o365:management:activity (Workload=Exchange OR Workload=ExchangeAdmin)
| search Operation IN ("New-InboxRule","Set-InboxRule","Set-Mailbox")
```

```
/* Extract parameters (Splunk stores JSON arrays under Parameters{}) */
| spath input=Parameters
| mvexpand Parameters{}
| eval pName=mvindex(Parameters{}.Name,0), pValue=mvindex(Parameters{}.Value,0)
| eval user=coalesce(UserId, UserKey, ActorUPN, user)
/* Collect rule and forwarding fields */
| eventstats values(pValue) AS allValues by _time, user, Operation, Id
| eval candidate=lower(mvjoin(allValues,";"))
| where like(candidate,"%forward%") OR like(candidate,"%redirect%") OR like(candidate,"%forw
/* Try to pull the actual target(s) (email address strings) */
| rex field=candidate max_match=10 "(?i)(?<fwd_to>[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,})"
| mvexpand fwd_to
| where isnotnull(fwd_to)
/* Normalize + domain extraction */
| eval fwd_to=lower(fwd_to)
| rex field=fwd_to "(?i)@(?<fwd_domain>[^ >;,'\"\"]+)$"
/* Skip internal/tenant domains (optional: replace 'yourcorp.com' with your org domains or u
| where isnotnull(fwd_domain) AND NOT like(fwd_domain,"%yourcorp.com%")
/* Enrichments */
| lookup freemail_domains domain AS fwd_domain OUTPUT is_freemail
| lookup disposable_domains domain AS fwd_domain OUTPUT is_disposable
| lookup whois_domains domain AS fwd_domain OUTPUT created_epoch
| eval domain_age_days = if(isnull(created_epoch), null(), round((now() - created_epoch)/864
| lookup otx_domains domain AS fwd_domain OUTPUT otx_pulse_count
| lookup openphish_domains domain AS fwd_domain OUTPUT openphish_flag
| ipqs domain=fwd_domain
| rename ipqs.domain_risk_score AS domain_risk
/* Risk model */
| eval risk = 30 /* base for mailbox forwarding */
  + case(is_freemail="Yes",10, true(),0)
  + case(is_disposable="Yes",25, true(),0)
  + case(isnotnull(domain_age_days) AND domain_age_days<=30,20, true(),0)
  + case(coalesce(otx_pulse_count,0)>=1,20, true(),0)
  + case(coalesce(openphish_flag,0)>=1,25, true(),0)
  + round(coalesce(domain_risk,0)/5,0)
/* Threshold + tidy output */
| where risk>=50
| table _time user Operation fwd_to fwd_domain is_freemail is_disposable domain_age_days otx
| sort - _time
```

NOTES

- Swap `yourcorp.com` for your organization's internal domains (or use an allowlist lookup) to avoid false positives.

- Domain-age <= 30 days + disposable/freemail + phish flags is a strong exfil signal; tune weights as needed.
- In Splunk ES (RBA), append: `| eval risk_object=user, risk_score=risk` and save as a correlation search.

EXPORT TIP: `CTRL/CMD` + `P` → SAVE AS PDF → UPLOAD TO LINKEDIN AS A **DOCUMENT**.