PIVTR-D

A field manual for incident responders.

Habib Tora
Incident response operating guide, version 2.0
September 2026

P Preparation
readiness, authority, playbooks, exercises, hunting

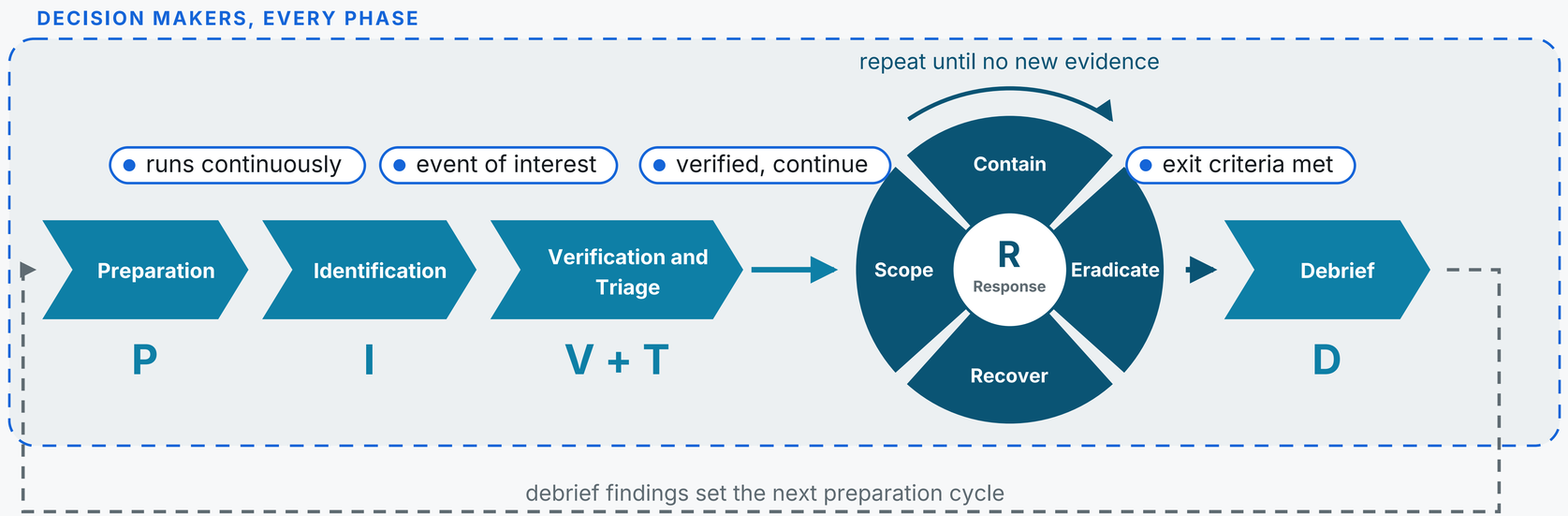
I Identification
alerting, detection and hunting, running continuously

V Verification
event, or incident? and does it require a response

T Triage
prioritizes it against organizational objectives

R Response
scope, contain, eradicate and recover, repeating

D Debrief
lessons learned, post-mortem, RCA close it and turn it into changes



Every phase: what starts it, what finishes it, what it leaves behind

Phase	Starts when	Done when	Record produced
P. Preparation	No incident running	Never closes. Reopened by every debrief.	Authority matrix, playbooks, asset and contact lists
I. Identification	Telemetry and reports flowing	An event of interest is raised	Alert or hunt finding with evidence references
V, T	Event of interest raised	Continue, stop or defer, with a name against it	Incident record, triage brief
R. Scope	Verified incident, one or more indicators	Breadth, systems and impact established	Scope findings, attack timeline
R. Contain	Reach of the compromise clear enough to act	Network, process and log channels all clean	Containment decision record
R. Eradicate	Evidence collected and preserved	The original enumeration reruns clean	Root cause, eradication log
R. Recover	Eradication verified	In production under enhanced monitoring	Pre-restoration sign-off, owner acceptance
D. Debrief	Loop exited and signed	Improvement plan issued with owners and dates	Incident report, metrics, improvement register

Settle before the incident

Containment cannot wait when	Action
Encryption spreading, logs wiped	Isolate now
Bulk transfers, personal data queried	Contain urgently
ICS, medical, payment, safety-critical	Act, lose the intel
HIPAA, PCI, GDPR, NIS2, DORA clock	Contain rapidly

Posture	When
Active	Destruction underway, regulated data, safety-critical, attacker aware of you
Adaptive	Long dwell time with mature monitoring, or scope still unknown
Passive	Commodity malware on a low-value asset, controlled deception environment

Risk	Triggers
Low	Analyst handles it, logged
Medium	Commander informed, daily update
High	Team activated, decision makers briefed
Critical	Executive escalation, containment authority granted, counsel engaged

Records to produce

T1	Incident record
T2	Triage brief
T3	Containment decision record
T4	Loop iteration log
T5	Technical closure
T6	Residual risk acceptance
T7	Pre-restoration sign-off
T8	System owner acceptance
T9	After-action review agenda
T10	Executive debrief

Exit the loop when

- Scoping produces no new indicators
- Monitoring shows no attacker activity
- Eradication verification confirms removal
- Restored systems operate normally
- Residual risk is acceptable and signed
- Regulatory conditions for closure are met

Measure every time

Time to detect, respond, contain, eradicate, recover. Total lifecycle. Systems and accounts affected. Records exposed. Business impact. Effort and cost. Loop iterations.

Drawn by **Habib Tora** | Date **September 2026** | Revision **2.0**
Title **PIVTR-D reference** | Sheet **1 of 1** | Size **36 × 24 in**