



Suhas Bhairav

AI Incident Response Copilot Blueprint

**A practical AI assistant for evidence, timelines,
and escalation in IT and security**

Provide a governed AI assistant to collect evidence,
summarize events, maintain timelines, and
coordinate escalation without autonomous

Suhas Bhairav

suhasbhairav.com

Automation vs Review in IR

Define what the AI copilot should automate, what requires human review, and how to balance speed with accuracy. Identify data sources, tools, and guardrails to support auditable incident response.

Key move **Mandate human sign-off before any containment action.**

PRACTICAL CHECKLIST

- 01** Evidence collection: automatically ingest and tag logs, alerts, and assets with time stamps.
- 02** Event summarization: generate concise incident narratives from disparate data sources.
- 03** Timeline maintenance: auto-sequence events with cross-source correlation and time alignment.
- 04** Playbook step suggestions: propose containment and recovery steps, ordered by impact and resource readiness.
- 05** Escalation coordination: route alerts to on-call owners and ticket systems with status flags.
- 06** Data quality controls: enforce retention, source provenance, and access restrictions for evidence.

Suhas Bhairav AI Resource

Provide a governed AI assistant to collect evidence, summarize events, maintain timelines, and coordinate escalation...

Data, Tools, Access

This page lists the data sources, toolchain, and access controls necessary to support the AI copilot. It also clarifies ownership and permissions.

Key move Document artifact lineage tagging for all evidence entries.

PRACTICAL CHECKLIST

- 01** Data sources: SIEM, EDR, asset inventory, cloud logs, and change management events.
- 02** Evidence store: a structured, time-stamped repository with provenance metadata.
- 03** Toolchain: connect IR platform, AI copilots, SIEM APIs, and ticketing systems.
- 04** Access and governance: least privilege, RBAC/ABAC, and full audit logging.
- 05** Automation interfaces: standardize data formats (JSON/Log schema) and APIs for repeatable automation.
- 06** Runbooks: digital, versioned playbooks consulted by the AI for suggested steps.

Suhas Bhairav AI Resource

Provide a governed AI assistant to collect evidence, summarize events, maintain timelines, and coordinate escalation...

Weekly Pilot Plan

A practical, five-week plan to pilot the AI copilot in IT and Security. Includes approvals, measurement, and ownership.

Key move Stop if data sensitivity risk exceeds threshold.

PRACTICAL CHECKLIST

- 01** Week 1: establish data feeds, access rights, approvals, and a minimal evidence schema; verify privacy controls.
- 02** Week 2: configure AI prompts, timelines, and auto-summarization templates; test with a non-production dataset.
- 03** Week 3: pilot evidence collection and escalation routing for one incident type.
- 04** Week 4: introduce playbook step suggestions to responders; gather feedback on usefulness.
- 05** Week 5: measure against KPIs, adjust guardrails, and confirm ownership.
- 06** Ongoing: require human-in-the-loop for containment decisions, with audit trails.

Suhas Bhairav AI Resource

Provide a governed AI assistant to collect evidence, summarize events, maintain timelines, and coordinate escalation...

ABOUT THE CREATOR

Suhas Bhairav

I build AI systems that combine distributed architecture, retrieval, knowledge graphs, security, and practical workflow design. My focus is AI that can be used repeatedly by real teams: understandable, reliable, and grounded in the work people already do.

EXPERTISE

- Principal systems architecture and applied AI engineering
- Production-grade AI systems, agentic workflows, RAG, and knowledge graphs
- Full-stack workflow applications across AWS, Google Cloud, Azure, on-premise, and hybrid environments
- Practical AI implementation patterns for automotive, manufacturing, finance, logistics, cybersecurity, sales, and customer operations
- Security, governance, observability, approvals, and failure-mode thinking for operational AI systems

WEBSITE

suhasbhairav.com

EMAIL

suhasbhairav@gmail.com