Suhas Bhairav

AI Vulnerability Prioritization Framework

Rank threats by exploitability, asset exposure, and business impact.

A practical, runnable framework to prioritize and remediate vulnerabilities with AI.

Suhas Bhairav

suhasbhairav.com

Intro & Goals

AI-driven prioritization translates threats into actionable risk rankings. It aligns IT security with business impact using AI-assisted scoring.

Key move **Pilot early, measure risk reduction weekly**

PRACTICAL CHECKLIST

01	Define scoring dimensions: exploitability, asset exposure, business criticality, compensating controls, active exploitation, remediation effort.
02	Use simple risk bands (Low/Med/High) to guide triage and sequencing.
03	Automate data ingestion: asset inventories, patch status, CVEs, telemetry, and exploit data.
04	Remain human-in-the-loop for ambiguous items or policy decisions requiring risk appetite.
05	Define ownership: asset owner, security lead, and business sponsor.
06	Run a 4-week pilot in a single domain before organization-wide rollout.

Suhas Bhairav AI Resource

A practical, runnable framework to prioritize and remediate vulnerabilities with AI.

Inputs, Tools, and Automation

This page lists data sources and automation rules to implement the framework. Distinguish automated collection from human-reviewed decisions.

Key move **Lock data sources, document ownership, and secure AI prompts**

PRACTICAL CHECKLIST

01	Data inputs: asset inventory, patch status, CVE feed, misconfig telemetry, and active exploitation indicators.
02	Automation targets: scoring, triage prioritization, and remediation sequencing suggestions.
03	Human review triggers: threshold breaches, policy exceptions, or business-critical changes.
04	Tools to consider: SIEM, asset management, ticketing, AI agents (Claude/ChatGPT) for summaries.
05	Remediation playbooks: patch, reconfigure, or compensate with controls; track via an AR plan.
06	Data governance: owners, retention, and privacy considerations for automation outputs.

Suhas Bhairav AI Resource

A practical, runnable framework to prioritize and remediate vulnerabilities with AI.

Pilot, Measure, Scale

Adoption runs in weekly sprints with clear ownership. Establish governance, approvals, and metrics to monitor progress and risk.

Key move **Ensure policy alignment; no production changes without review**

PRACTICAL CHECKLIST

01	Week 1: map assets, owners, and current vulnerabilities; configure data feeds.
02	Week 2: implement automated scoring, risk bands, and triage rules in the ticketing system.
03	Week 3: establish remediation playbooks and assign owners for High-risk items.
04	Week 4: run a tabletop exercise on one critical vulnerability to validate process.
05	Ongoing: weekly reviews with security lead, asset owners, and executive sponsor.
06	KPIs: mean time to remediate, risk reduction, and automation coverage.
07	Governance guardrails: no auto-remediate without human sign-off for critical systems.

Suhas Bhairav AI Resource

A practical, runnable framework to prioritize and remediate vulnerabilities with AI.

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