C1 SmartStart for Vulnerability Response (VR)

Rapid deployment of ServiceNow VR—ingesting scanner data, enriching findings, prioritizing risks using CMDB context, and automating remediation workflows. Organizations move from spreadsheets to continuous, auditable, risk-based vulnerability management with unified ingestion, normalization, and real-time dashboards for Security, IT Ops, and Compliance.

Unified Ingestion

Consolidate scanner findings from Qualys, Tenable, Rapid7 with CVE/CVSS/KEV enrichment and exploit intelligence.

Risk-Based Prioritization

CMDB-driven criticality scoring using business impact and service-impact analysis for true risk assessment.

Automated Workflows

SLA-driven routing, change management integration, and exception workflows with expiry controls and governance.

Primary Use Cases

- Consolidate and enrich scanner data into one system
- Prioritize vulnerabilities using true risk and impact
- Automate routing, remediation, and change processes
- Manage exceptions with defensible governance
- Provide unified reporting for operations and leadership

Core Capabilities

- Real-time dashboards for MTTR, SLA health, exposure trends
- IRM linkage for risks, POAMs, and failed controls
- Complete audit-ready remediation traceability
- Centralized exception and risk acceptance workflows

50-70%

Triage Reduction

Reduction in triage and routing effort

40-60%

MTTR Improvement

Improvement in mean time to remediate

70%+

Manual Tracking

Reduction in manual spreadsheet tracking

> SmartStart delivers a fast, standardized, ServiceNow-aligned VR program—centralizing ingestion, prioritization, remediation, and compliance to create a continuous, defensible vulnerability lifecycle with fewer audit findings through full traceability and stronger compliance alignment.