



SERVICENOW SECOPS FLIGHTPATH IMPLEMENTATION



OVERVIEW

The ServiceNow SecOps Flightpath for IT/OT security offers a structured, phased approach to unifying cybersecurity, asset visibility, and operational resilience. Spanning 24 months, this roadmap accelerates convergence between IT and OT environments by leveraging ServiceNow Security Operations (SecOps), Operational Technology Management (OTM), Vulnerability Response (VR), Security Incident Response (SIR), Security Posture Control (SPC), and Identity Governance capabilities.

Each phase builds foundational maturity by establishing cross-domain visibility, integrating real-time response, enforcing continuous compliance, and securing identity access. This data sheet summarizes key phases, technical strategy, and benefits for enterprise adoption.

PHASE BREAKDOWN

PHASE 01: ASSET VISIBILITY & UNIFIED CMDB: (MONTHS 0-4)

OBJECTIVE:

Establish a comprehensive inventory of IT and OT assets.

MODULES:

ITOM Discovery, OTAM, OTM.

HIGHLIGHTS:

- Passive discovery via Tenable OT, Claroty, ForeScout, Nozomi, SCADA integrations.
- CMDB schema extended to OT-specific classes.
- Governance for CMDB ownership and lifecycle.

OUTCOMES:

- Unified CMDB with reconciled asset records.
- Baseline inventory and health dashboards.

PHASE 02: INTEGRATED IT/OT OPERATIONS & FSM: (MONTHS 5-8)

OBJECTIVE:

Align incident, change, and dispatch processes for OT support.

MODULES:

ITSM, Field Service Management (FSM), Event Management

HIGHLIGHTS:

- OT incidents routed through ServiceNow with SLA tracking.
- FSM-enabled dispatch for plant-level resolution.
- Integrated alarm feeds from OT systems into IT workflows.

OUTCOMES:

- Centralized ticketing across IT/OT.
- Reduced MTTR and downtime.

PHASE 03:

VULNERABILITY MANAGEMENT
& PATCH GOVERNANCE: (MONTHS 9–14)

OBJECTIVE: Remediate IT/OT vulnerabilities with coordinated patching.	MODULES: ITVR, OTVR, Change Management, FSM.
HIGHLIGHTS: <ul style="list-style-type: none">- Risk-based prioritization of CVEs.- Claroty/ForeScout/Nozomi and Tenable.ot integrations.- FSM work orders for on-site patch deployment.	OUTCOMES: <ul style="list-style-type: none">- Continuous exposure reduction.- Documented risk acceptances for OT constraints.

SECURITY OPERATIONS EXECUTION

PHASE 04:

SECURITY
INCIDENT RESPONSE: (MONTHS 15–18)

OBJECTIVE: Enable coordinated incident triage, containment, and forensics.	MODULES: SIR, IntegrationHub, SOAR, FSM
HIGHLIGHTS: <ul style="list-style-type: none">- Bi-directional integrations with SIEM, EDR, and OT threat tools (e.g., Claroty/ForeScout/Nozomi)- Automated incident creation and correlation- Role-based workflows and playbooks aligned with MITRE ATT&CK.	OUTCOMES: <ul style="list-style-type: none">- Reduced MTTD/MTTR across converged environments.- Complete audit trail for compliance (NIST CSF, IEC 62443).

PHASE 05:

SECURITY POSTURE CONTROL
& CONTINUOUS COMPLIANCE: (MONTHS 19–22)

OBJECTIVE: Operationalize policy enforcement and posture monitoring.	MODULES: SPC, IRM (Policy & Compliance, Risk Management).
HIGHLIGHTS: <ul style="list-style-type: none">- Automated identification of security control gaps.- Real-time SPC dashboards by plant or asset criticality.- Mapped posture findings to regulatory requirements (e.g., NERC CIP).	OUTCOMES: <ul style="list-style-type: none">- Fewer control failures and audit issues.- Preventive remediation before exploitation.

PHASE 06:

IDENTITY &
ACCESS GOVERNANCE: (MONTHS 23–24)

OBJECTIVE: Govern user access across IT/OT systems.	MODULES: Clear Skye IGA (ServiceNow-native), or SailPoint integration.
HIGHLIGHTS: <ul style="list-style-type: none">- Onboarding/offboarding workflows integrated with HR systems.- Role-based access requests, reviews, and SoD enforcement.- Certification campaigns for OT system accounts.	OUTCOMES: <ul style="list-style-type: none">- Eliminated orphan accounts and access misuse.- Full lifecycle visibility for user privileges.

TECHNICAL STRATEGY & PLATFORM BENEFITS


CATEGORY	STRATEGY	PLATFORM BENEFIT
Asset Management Incident Response Vulnerability Management Posture Control IAM Governance	Passive discovery & CMDB consolidation Integrated SIR with FSM & SIEM Claroty/ForeScout/Nozomi/Tenable VR sync & patch workflows SPC with automated alerts & IRM mapping Role-based provisioning & SoD control	Shared visibility across IT/OT devices Unified threat handling with full traceability Risk-prioritized remediation & compliance tracking Continuous enforcement of security baselines Identity oversight across OT and corporate systems

GOVERNANCE & SUCCESS METRICS


STEERING COMMITTEE: Cross-functional IT, OT, SecOps, GRC leadership.	CHANGE MANAGEMENT: Role-specific training and adoption metrics.
PERFORMANCE KPIS: <ul style="list-style-type: none">- Asset coverage (% OT in CMDB).- Vulnerability backlog trend (critical CVEs open).- Incident response speed (MTTD, MTTR).- Access review compliance rate (% on-time completion).- Control coverage via SPC (compliance score by site).	The ServiceNow SecOps Flightpath delivers a resilient, compliant, and intelligent IT/OT security capability. By combining asset, vulnerability, and incident management with posture control and identity governance, the program enables continuous cyber resilience and audit readiness.


To learn more or request a tailored roadmap consultation, contact your Templar Shield representative.

Contact Information

 +1-619-344-2573

 www.templarshield.com

 info@templarshield.com

 350 10th Ave, Suite 1000, San Diego, CA 92101

