DOCUMENT 02 / 05 · THE ROADMAP

Crawl, Walk, Run.

A phased adoption path from insurable to proactive.

IR 2.0 is not an all-or-nothing program. This roadmap maps current posture to a three-stage progression — Crawl gets you insurable, Walk gets you resilient, Run gets you proactive. Each stage names its deliverables, transition points, and the metrics that prove it landed.

SERIES
IR 2.0

DOCUMENT
02 of 05

VERSION
1.3 · 2025

THE SPECTRUM

Progress over perfection. Every step forward improves both resilience and insurability.

STAGE 01	STAGE 02	STAGE 03
Crawl	**Walk**	**Run**
"Get insurable."	*"Get resilient."*	*"Get proactive."*
TIMELINE: **30 – 60 days**	TIMELINE: **3 – 6 months**	TIMELINE: **6 – 12 months**
SLA: **≤ 4 h assembly**	SLA: **≤ 1 h response**	SLA: **≤ 15 m auto-contain**
FREQUENCY: **≥ 1 drill / yr**	FREQUENCY: **Quarterly drills**	FREQUENCY: **Monthly chaos**

Start where you are. Use what you have. Do what you can. The roadmap exists so you can stop arguing about where to begin and begin somewhere that earns insurance, then resilience, then leverage.

STAGE 01 / CRAWL

Get insurable.

Establish the minimum viable IR program insurers will quote.

TIMELINE	SLA
30 – 60 days	≤ 4 h assembly

DELIVERABLES

- **IR One-Pager.** Incident definition, severity levels, roles (IC, Comms, Tech), escalation triggers, contacts.
- **The Big 3 controls.** MFA on all critical systems · EDR on all endpoints · Tested immutable backups.
- **First tabletop drill.** 60–90 minutes walking a ransomware scenario with key stakeholders.
- **Evidence collection.** Screenshots, policy docs, restoration tests — your insurance application packet.

QUICK WINS

- Download a cyber insurance application — every "No" answer is your next project.
- Enable MFA on email, VPN, and admin accounts this week.
- Schedule the first tabletop drill within 30 days.
- Test one backup restoration and document the result.

SUCCESS METRICS

METRIC	TARGET
Insurance checklist completion	≥ 70% "Yes" answers
Team assembly time	≤ 4 hours
Tabletop drills completed	≥ 1 per year

STAGE 02 / WALK

Get resilient.

Move from a documented plan to a proven, practiced capability with initial automation.

TIMELINE	SLA
3 – 6 months	≤ 1 h response

DELIVERABLES

- **Documented playbooks.** At minimum: Ransomware, Phishing, Stolen Credentials, Data Exfiltration — each with steps, decision trees, comms templates.
- **SIEM deployment.** Centralized logging, correlation rules for critical alerts, defined alert triage process.
- **First Calm Loop.** One automated workflow: detection → enrichment → notification.
- **Quarterly drills.** Rotated scenarios with documented lessons learned.
- **Reversibility Score policy.** Defines which automated actions require human approval.

KEY TRANSITIONS

From "*we have a plan*" to "*we've tested the plan.*"
From *manual log review* to *automated alert correlation.*
From *improvised response* to *playbook-driven response.*

SUCCESS METRICS

METRIC	TARGET
Mean Time to Detect (MTTD)	≤ 24 hours
Mean Time to Respond (MTTR)	≤ 1 hour
Playbook coverage	≥ 80% of incident types
Tabletop drill frequency	Quarterly

STAGE 03 / RUN

Get proactive.

Predictive operations with full Calm Loop automation and continuous improvement.

TIMELINE
6 – 12 months

SLA
≤ 15 m auto-contain

DELIVERABLES

- **Full Calm Loop automation.** End-to-end response for high-confidence scenarios; human gates for RS-3+.
- **AI-assisted triage.** LLM-powered enrichment, initial analysis, recommended actions — human in the loop.
- **Chaos engineering.** Scheduled live-fire drills. Inject failures to test recovery.
- **Threat intelligence integration.** Proactive hunting, intel-driven playbook updates, preparation for emerging threats.
- **Continuous improvement loop.** Every incident feeds playbooks, automation, and training. Blameless post-mortems standard.

ADVANCED CAPABILITIES

Predictive analytics for high-risk patterns. Cross-team automation across security, IT, and DevOps. Supply-chain incident playbooks. Cloud-native IR for containers, serverless, and multi-cloud.

SUCCESS METRICS

METRIC	TARGET
Mean Time to Contain (MTTC)	≤ 15 minutes (automated)
Automation coverage	≥ 70% of common incidents
False positive rate	< 10%
Chaos drill frequency	Monthly

> *This is a journey, not a destination. Every loop iteration earns the next one.*