Code Red — cyber-incident response

Containment, forensics kick-off, and recovery planning for organizations under cyber attack — hospitals, schools, and companies. In an emergency, contact us at lv3.biz/help-hacked-system/.

FOUR STAGES — RUN LIKE AN EMERGENCY ROOM

STEP 1
Stop the bleeding
First containment instructions. Decide what external communication to halt.

STEP 2
Find out what happened
Forensics kick-off: facts, blast radius, root cause.

STEP 3
Stand operations back up
Recovery planning and prioritization.

STEP 4
Close the weakness
Fold prevention into a new architecture.

TIMELINE AFTER ENGAGEMENT START (STANDARD)

First 72 hours	Situation briefing, first containment instructions, external-communication halt decisions
The following week	Forensics kick-off, executive brief, regulator-notification decision
Within one month	Recovery-plan draft delivered, priority list, external-disclosure draft
Year one and beyond	Continued recovery support, or handoff to an SOC vendor

ENGAGEMENT SUMMARY (MODE: RECOVERY)

Team	A senior IT designer with Research (forensics), Data, and Support teams
Duration	Typically around one year
Deliverables	Standing issues & progress reports + damage-assessment report (facts, impact, root cause) · recovery report (post-recovery architecture, prevention, handover)
Not included	Attacker attribution (a matter for law enforcement) / long-term SOC operations
On-site / remote	Remote-first; on-site for large-scale response

The recovery playbook is collected in the book WAH — the book to read in a corporate emergency (planned for early 2027).

How we work (all services)

Our standard engagement modes, flow, and terms. The individual contract takes precedence. Latest version: lv3.biz/en/how-we-work/.

THREE ENGAGEMENT MODES (ALL QUASI-MANDATE AGREEMENTS)

	PROJECT	ADVISORY	RECOVERY (CODE RED)
Scope	Standalone IT-design engagement (roadmap, new-system design, migration planning)	Monthly involvement in a running DX / IT program, at the design layer	Post-incident containment, forensics kick-off, recovery planning
Duration	Typically multi-year	Typically several months to years	Typically around one year
Mode-specific deliverables	Roadmap document · data model	Monthly design-review records · vendor-meeting minutes	Damage-assessment report · recovery report (new architecture)
Not included	Operations outsourcing / 24×7 monitoring	Development staffing (body-shopping)	Attacker attribution / long-term SOC operations

Whatever the mode, we deliver standing issues and progress reports throughout (the standard set — adjustable per engagement).

FROM INQUIRY TO KICKOFF (ABOUT TWO WEEKS AT THE FASTEST)

WEEK 0
Inquiry
Contact form → a short scoping conversation. A 30–60 min online call if useful.

WEEK 1
NDA + scope draft
NDA signed. LV3 drafts the scope document.

WEEK 2
Kickoff
MSA + SOW signed. Team assigned, work begins.

WEEK 3–N
Execution
Weekly reviews plus a monthly executive brief.

CLOSEOUT
Handover
Final documentation delivered. Further support under a separate agreement.

A cyber incident (Code Red) does not wait for this flow — use the emergency path: lv3.biz/help-hacked-system/.

STANDARD CONTRACT TERMS (THE INDIVIDUAL CONTRACT TAKES PRECEDENCE)

Contract type	Quasi-mandate agreement — compensation for professional services (not a fixed-deliverable work contract)
Contract form	Standard MSA + SOW. Client legal review welcome. Purchase-order-based contracting possible
NDA	Standard two-party NDA, available before the first conversation. Client-side templates accepted
Pricing & billing	Pricing on request. First month standalone, then three-month renewals. Foreign currencies available
Data handling	Post-engagement retention and destruction rules stated in the contract
On-site / remote	Remote-first. On-site support for large-scale recovery work