CWIL ACADEMY · COURSE CATALOGUE 2026–27

CW-BF

CWIL BlueForge™

Threat-Informed Defense Operations Programme

FLAGSHIP FORGE™ · DEFENSIVE

Repeatable defensive monitoring, triage and hardening built from evidence.

Aligned with NIST CSF 2.0 · MITRE ATT&CK & D3FEND · ISO/IEC 27001

ABOUT THIS COURSE

Defensive Operations connects security telemetry, asset knowledge, and response decisions into a practical operating rhythm. Learners work from evidence and documented assumptions rather than from product-specific recipes.

WHO IT IS FOR

Early-career defenders, systems administrators moving into security, and teams formalising a monitoring function.

PREREQUISITES

Comfort with basic operating-system concepts, networked services, and reading structured logs is useful. No vendor certification or paid tool is required.

SYLLABUS, MODULE BY MODULE

01	Defensive mission & asset criticality
02	Telemetry planning & retention
03	Baselines, alert context & triage
04	Control validation & secure configuration
05	Incident communication & escalation
06	Metrics & continuous improvement

LEARNING OUTCOMES

- Create a defensible map of assets, data sources, and monitoring responsibilities
- Turn ambiguous alerts into documented, prioritised investigation questions
- Evaluate defensive controls using evidence and stated risk assumptions

- Produce clear handover notes, escalation records, and improvement actions

LABS

Labs use isolated synthetic hosts and pre-generated telemetry. Activities stop at observation, configuration review, and safe validation; no public targets, persistence, credential collection, or uncontrolled traffic are used.

ASSESSMENT

A learner submits a monitoring plan, a short triage journal, and a control-review briefing. Feedback considers evidence quality, prioritisation, clarity, and ethical handling of lab data.

Register for CW-BF

Fees and batch dates are confirmed on enquiry. Remote, instructor-led, open across India.

cwil.in/register?course=cw-bf · info@cwil.in

IMPORTANT NOTICE

CWIL programmes are aligned with the frameworks listed and are not issued, endorsed or accredited by NIST, ISO, ENISA or any other standards body. CWIL credential and Forge™ programme names are trademarks of Cyber Warfare Intelligence Lab (OPC) Private Limited.