SCHOOL OF ENGINEERING • CSE (CYBER SECURITY) • DAYANANDA SAGAR UNIVERSITY•

CYBER RANGE CENTRE OF EXCELLENCE

A 6,300 sq. ft. integrated cybersecurity ecosystem designed for experiential and project-based learning, applied research, professional training, Life Fire Exercises (LFEs) and industry collaboration.

CYBER DEFENSE • CYBER RESILIENCE • APPLIED AI • DIGITAL FORENSICS • WARFARE SIMULATION • SOC / NOC • FORENSICS • THREAT INTELLIGENCE • CYBER AI

EXPLORE THE CYBER RANGE

Cyber Security Courses | SOC | NOC | Digital & Cyber Forensics | Cyber AI | Threat Intelligence | Professional Training | Research | Life Fire Exercises | Corporate Training | Executive Training | Internship | Certification| CTF & HACKATHON|

What We Offer

Four engagement lines built on one shared cyber-range infrastructure — enabling students, researchers, government and industry teams to work with the same simulated environments, security platforms and faculty expertise.

P1 — CYBER OPERATIONS Cyber Warfare Simulation — Red / Blue / Purple Team exercises, attack simulation, threat hunting, incident response, ransomware containment and CTFs.	**P2 — ACADEMIC TRAINING** Experiential Cyber Learning — Hands-on modules in cyber security, cloud security, cryptography, VAPT, AI security, malware analysis, forensics and security operations.
P3 — RESEARCH & INNOVATION Applied Cyber Research — AI-driven threat detection, malware classification, behavioural analytics, predictive threat intelligence, LLM security and digital-forensic research.	**P4 — INDUSTRY & GOVERNMENT** Professional Capacity Building — Industry programmes, government / law-enforcement training, cyber exercises, consultancy, sponsored projects and cyber preparedness.

Cyber Range Infrastructure

A unified environment spanning cyber warfare simulation, SOC/NOC operations, digital & cyber forensics, AI security research, training, incident response and professional cyber exercises.

6,300	12	600+
SQ. FT. FACILITY	FUNCTIONAL ZONES	OPEN-SOURCE TOOLS

Infrastructure — Functional Zones

01 CYBER WAR ROOM Red/Blue/Purple Team exercises, SOC monitoring, threat hunting & incident response.	**02 AV RACK ROOM** Video-wall control, AV switching, conferencing, recording & streaming.
03 CRISIS ROOM Executive incident management, risk, continuity, recovery & tabletop exercises.	**04 CYBER AI INNOVATION LAB** Threat detection, malware classification, behavioural analytics & LLM security research.
05 DIGITAL & CYBER FORENSIC LAB Disk, memory, mobile and network forensics; malware analysis.	**06 EVIDENCE STORAGE & FARADAY** Evidence preservation, chain-of-custody, secure storage & RF shielding.

07 DISCUSSION ROOM Research meetings, incident reviews, mentoring & industry consultation.	**08 FORENSIC TRAINING ROOM** Evidence acquisition, tool demonstrations, workshops & certification.
09 VIDEO CONFERENCING FACILITY Hybrid learning environment with AI-enabled cameras and beamforming audio.	**10 VISITOR ROOM** Controlled demonstrations for partners, accreditation teams & stakeholders.
11 CYBER RANGE MASTER CABIN Exercise planning, supervision, compliance & quality assurance.	**12 CHIEF ARCHITECT CABIN — SOC/NOC** SOC/NOC architecture, policy, optimisation & strategic leadership.

INDUSTRY-READY TECHNOLOGY ECOSYSTEM

SIEM / SOAR: ArcSight • QRadar • Splunk • Elastic • Microsoft Sentinel • Cortex XSOAR
EDR / XDR: CrowdStrike • Carbon Black EDR • Microsoft Defender • McAfee
NETWORK SECURITY: Palo Alto • Fortinet • Check Point • Cisco ASAv • pfSense • F5 WAF
CLOUD / MALWARE / OT: AWS CloudTrail • S3 • SQS • Cuckoo • Cisco Secure Malware Analytics • Claroty
PLATFORMS: Kali Linux • Parrot OS • Ubuntu LTS • Windows 10 • Windows Server 2019 • Kubernetes • KIWI Syslog • Zenoss Core.

USP & Engagement Model

Built as an active academic, research and professional ecosystem — not a static laboratory — so the facility can continuously support learning, innovation, cyber preparedness and industry collaboration.

Full-spectrum cyber environment
Cyber warfare simulation, SOC/NOC, forensics, AI security, threat intelligence and training are connected under one ecosystem.

Faculty-led, research-connected
Programmes combine hands-on learning with applied research, professional development and industry-facing projects.

End-to-end cyber exercise pipeline
Plan → simulate → detect → investigate → respond → report — with controlled environments for repeatable exercises.

Direct talent pipeline
UG/PG learners work with professional security platforms and real-world scenarios, supporting internships, projects and employability.

ENGAGEMENT & COLLABORATION MODELS

ACADEMIC PROGRAMMES	Curriculum-linked labs, electives, capstone projects, CTFs and experiential learning.
PROFESSIONAL TRAINING	Certification-oriented programmes, faculty development and capacity building.
INDUSTRY / GOVERNMENT	Sponsored projects, cyber exercises, consultancy, threat research and preparedness.
RESEARCH & INNOVATION	AI security, malware analysis, digital forensics, threat

	intelligence and applied cybersecurity research.
TESTING & VALIDATION	Controlled security testing, network experimentation and cyber range-based validation.

Build Cyber Capability. Train for Real-World Resilience.

Innovate Today. Secure Tomorrow.

PARTNER WITH THE DSU CYBER RANGE CENTRE OF EXCELLENCE