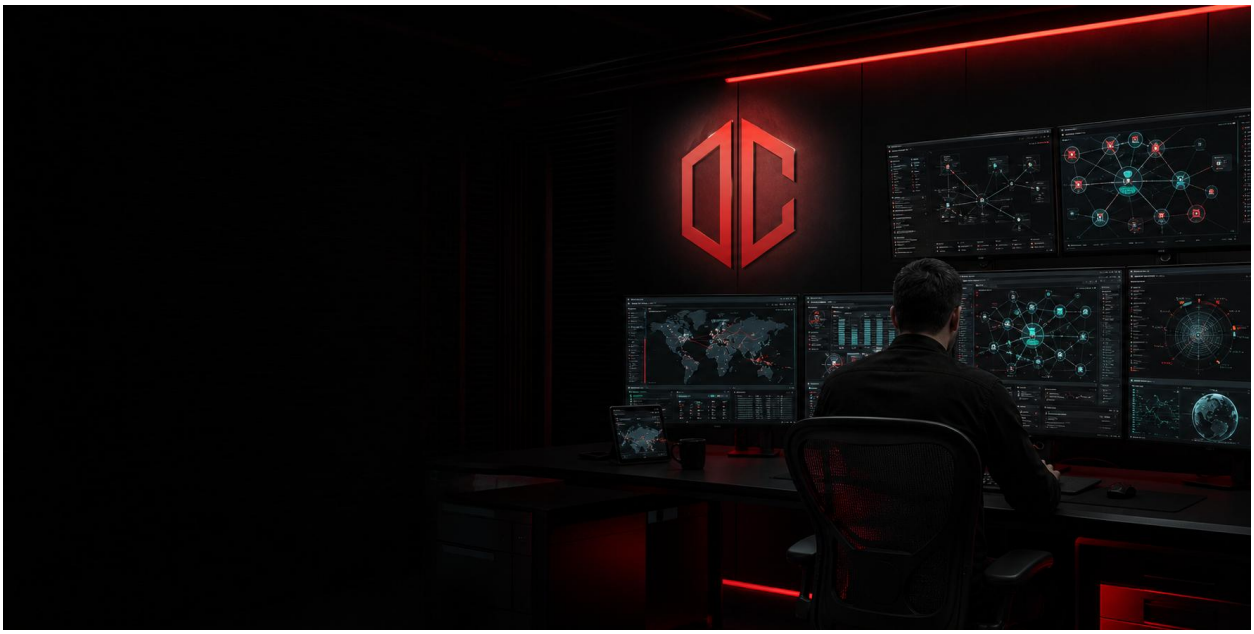
DAEMONCORE // ACADEMY



ENTERPRISE TRAINING & WORKFORCE READINESS

A practical cyber capability platform for teams that need more than passive course completion.

127	120h45	70	7
COMPLETE LESSONS	GUIDED CURRICULUM	SPECIALIST CONDITIONS	SEALED FIELD MISSIONS

ACADEMY 6 // ENTERPRISE CAPABILITY BRIEF // SEPTEMBER 2026

01 // EXECUTIVE BRIEF

Build capability that leaves evidence.

DaemonCore Academy combines structured instruction, scored decisions, disposable live environments, durable operator records, and an authorization-bound professional assessment workspace in one local-first desktop application.

THE ENTERPRISE PROPOSITION

Give employees a repeatable path from understanding a control, to practicing it, to proving an outcome - without turning training progress into an imaginary leaderboard or exposing practice targets to the public internet.

Designed for

- Security teams building common assessment, evidence, and reporting habits across mixed experience levels.
- Engineering organizations strengthening application, identity, cloud, Linux, container, detection, and software supply-chain capability.
- Leaders who need practical learning records and after-action evidence rather than attendance alone.
- Consulting and internal assurance teams that want training and professional authorized diagnostics in the same operating model.

What makes it different

The Academy teaches a method: establish scope, collect a defensible signal, test the boundary, preserve evidence, communicate impact, and verify remediation. FieldOps carries that method into real authorized engagements with signed permits, exact targets, sealed captures, findings, retests, and client-ready exports.

CURRENT COMMERCIAL MODEL

The Academy is free to use. FieldOps is the paid professional gate. The current retail FieldOps license is $199 one time; organization-wide deployment, support, procurement, and commercial terms should be scoped separately.

02 // PLATFORM MODEL

One desktop. Four connected capability layers.

Employees move through guided learning, live practice, scored proof, and professional operations without stitching together unrelated websites and disposable progress records.

A local-first operating model designed for dedicated workstations and controlled team environments.

LAYER	PURPOSE	PROOF PRODUCED
Mission OS	Diagnose strengths and select role-based routes	Persisted baseline and next actions
Academy + Forge	Teach concepts through workshops and live specialist conditions	Attempts, decisions, accepted conditions
Sealed Range	Practice unrestricted investigation inside disposable containment	Evidence ledger and completion receipt
FieldOps War Room	Run authorized diagnostics and assessment campaigns	Signed permits, captures, findings, reports

03 // CURRICULUM ARCHITECTURE

Breadth for the workforce. Depth for specialists.

The catalog is large enough to support foundational onboarding, role development, cross-training, and advanced evidence-led practice without forcing every employee through one identical route.

CURRICULUM	LESSONS	TIME	FOCUS
Full-Spectrum Security Assessment	28	24h	Scope, networks, Windows, Linux, web, identity, cloud, containers, supply chain, evidence
Web + API Specialist	27	24h45	Browser contexts, authorization, OAuth, JWT, GraphQL, business logic, races, framing, caching
Enterprise Forge pathways	72	72h	AD, cloud engineering, detection, Linux, Kubernetes, software supply-chain defense
Total	127	120h45	Eight complete Academy pathways

Six Mission OS routes

- Penetration Tester - validate attack paths and write evidence-led findings.
- Web & API Specialist - identify and explain application trust failures.
- Identity Security - map authentication and delegated-control paths.
- Cloud Security - audit effective access and software provenance.
- Detection & Response - turn telemetry into bounded incident conclusions.
- Security Engineer - build controls across application, identity, and cloud systems.

ADVANCED SEQUENCE

Eight hour-long deep dives inside the full-spectrum path cover Linux privilege graphs, Windows service control, Active Directory paths, Kerberos trust, segmentation and pivot analysis, SSRF, OAuth/OIDC, and CI/CD provenance.

04 // LEARNING WORKFLOW

Learn. Practice. Launch. Prove.

Every activity identifies whether the operator is reading an example, making a scored decision, or working against a live disposable target. This removes the ambiguity common to terminal-styled courses.

1. Diagnose - a twelve-scenario baseline measures six capability domains and persists to the local operator record.
2. Select - Mission OS recommends a role route and calculates progress from completed work on the device.
3. Learn - lessons combine mental models, commands, artifacts, workshops, validation checks, and primary references.
4. Practice - Web Forge and Enterprise Forge require accepted live conditions rather than canned browser output.
5. Launch - sealed Docker ranges open only after containment verification and provide an unrestricted in-range shell.
6. Prove - after-action reviews score evidence coverage, independence, method discipline, and time discipline.

Recorded learner signals

Attempts	Evidence	Scores	Time
METHOD REPETITION	ACCEPTED OUTCOMES	DECISION QUALITY	GUIDED EFFORT

The local operator record retains completion, attempts, practical scores, capstone decisions, weekly minutes, achievements, and activity. Progress is calculated from completed work; DaemonCore does not seed fake readiness scores or public leaderboards.

MANAGEMENT IMPLICATION

Today, records are workstation-local and exportable. A centralized enterprise administration console, SSO/SCIM lifecycle, LMS synchronization, and organization-wide analytics are not represented as shipping capabilities.

05 // PRACTICAL ENVIRONMENTS

Practice against systems that can fail safely.

DaemonCore separates high-intensity learning from public-network operations. The most permissive exercises stay inside disposable ranges with verified containment.

48	22	7	3
ENTERPRISE CASES	WEB CONDITIONS	FIELD MISSIONS	PRINCIPAL CAPSTONES

Sealed range contract

- Internal-only Docker networking with no target ports published to the host.
- Zero host mounts, no privileged containers, dropped capabilities, no-new-privileges, and resource ceilings.
- Verified internet-egress denial before the operator shell is released.
- Run-specific seeds, full-tree pack fingerprints, launch receipts, and SHA-256 evidence ledgers.
- Guided, Assisted, Blind, and Professional modes with different hint availability and scoring behavior.

High-intensity resilience laboratory

Inside the sealed Academy range, bounded breakpoint experiments can run at up to 500 requests per second, 100 concurrent workers, and a 30,000-request budget against a disposable target that cannot reach the host or internet. The purpose is saturation, breakpoint, guardrail, and recovery engineering - not anonymous public-network disruption.

SAFETY BOUNDARY

DaemonCore does not provide an arbitrary public-network shell, DDoS engine, or online password-guessing system. Unrestricted command execution and high-intensity exercises remain inside the sealed range.

06 // FIELDOPS WAR ROOM

Turn authorized assessments into reviewable operations.

FieldOps is the professional layer for scoped diagnostics, multi-target campaigns, asset intelligence, sealed evidence, finding lifecycle, retesting, reporting, and bounded resilience work.

Campaign imagery. The shipping War Room presents real operator, permit, target, evidence, finding, campaign, and ledger state.

CAPABILITY	ENTERPRISE VALUE
Live command deck	Selected permit window, signed operator, integrity state, surface coverage, campaigns, findings, and latest ledger activity
Campaign Engine	Repeatable multi-target Complete Assessment, Service Inventory, and Change Verification profiles
Evidence vault	Digest-sealed raw captures with target, timing, resolved addresses, and immutable source context
Findings and retests	Severity, impact, remediation, disposition, and closure backed by later evidence
Exports	Machine-readable case file plus printable professional assessment report

07 // AUTHORIZATION AND GOVERNANCE

Capability begins at a signed boundary.

A FieldOps license unlocks the tool. It does not authorize a target. Execution requires an active engagement permit tied to a protected operator identity and exact scope.

Every new permit binds

- Named operator, organization, role, device-key fingerprint, and Ed25519 public key.
- Client or system owner, approving authority, approver email, and rules-of-engagement reference.
- Observe, Validate, or Stress policy level; internal or external network boundary.
- Exact targets, declared TCP ports, valid-from time, valid-until time, and operator attestation.

Execution safeguards

CONTROL	BEHAVIOR
Destination pinning	Resolve and pin an exact address before an operation begins
Boundary rejection	Block loopback, link-local, multicast, reserved, and mixed-boundary results
Tool bridge	Pass only normalized pinned addresses and declared ports through direct process invocation
Evidence integrity	Hash captures and chain audit events; preserve completed and blocked actions
Attribution	Sign new permits and operation receipts with the protected device key

EVIDENCE CLAIM

Device-key signatures provide attribution and tamper evidence. They do not independently prove that a typed identity or authorization statement is truthful; organizations remain responsible for validating identity and authority.

08 // DEPLOYMENT AND PROCUREMENT FACTS

A clear current-state view for enterprise evaluation.

DaemonCore is a local-first desktop platform. The following status is stated directly so technical, security, and procurement teams can evaluate the product without implied certifications or hidden cloud dependencies.

AREA	CURRENT STATE	ENTERPRISE CONSIDERATION
Windows	Stable 6.0 installer for Windows 10/11 x64	Installer is not yet Authenticode-signed; verify release SHA-256 checksums
Linux	x64 AppImage and Debian package beta	Ubuntu 22.04+ and Debian 12+ target; Linux remains separately labeled beta
Runtime	Docker Desktop on Windows; Docker Engine on Linux	Dedicated workstation or managed VM recommended for live ranges
Secrets	OS-protected credentials; GNOME Keyring/KWallet on Linux	FieldOps blocks unencrypted Electron basic_text storage
Records	Local operator and engagement data with exports	Define endpoint backup, retention, and case-handling policy
Administration	No shipping central tenant administration console	Plan workstation-based pilot; scope SSO, LMS, analytics, and fleet needs separately
Assurance	No SOC 2, ISO 27001, or FedRAMP claim is made	Run normal vendor security and legal review before broad deployment

RECOMMENDED ENTERPRISE POSTURE

Begin with a managed pilot on dedicated endpoints or virtual machines, validate the release checksum, constrain Docker access to trained operators, and treat exported learner and engagement records according to company retention policy.

09 // SUGGESTED ENTERPRISE PILOT

Prove the operating model before scaling it.

A six-week pilot gives security, learning, endpoint, and procurement stakeholders enough evidence to judge instructional value, deployment fit, and governance requirements.

WEEK	ACTIVITY	EXIT EVIDENCE
0	Security, legal, endpoint, and training readiness review	Approved pilot boundary and endpoint standard
1	Install, checksum validation, Docker preflight, operator onboarding	Working managed environment and named cohort
2	Mission OS diagnostic and route assignment	Baseline across six capability domains
3	Role lessons, workshops, and specialist conditions	Completion, attempt, and accepted-condition sample
4	Sealed range missions in Guided and Professional modes	Evidence ledgers and after-action reviews
5	Principal capstone and remediation cycle	Decision record, mastery gaps, reassigned work
6	Optional FieldOps tabletop on organization-owned test assets	Signed permit, sealed captures, findings, and report

Pilot success measures

- Operators can distinguish worked examples from live actions without instructor intervention.
- At least one accepted evidence chain is produced in each assigned practical domain.
- Participants improve decision quality or reduce guidance use across repeat attempts.
- Endpoint, Docker, keyring, export, and upgrade procedures meet internal operational expectations.
- Security leadership can identify which centralized features are required before a larger rollout.

10 // STAKEHOLDER VALUE

One platform, different reasons to care.

The enterprise decision is not only a training purchase. It touches capability development, endpoint operations, evidence handling, authorized testing, and procurement readiness.

STAKEHOLDER	PRIMARY VALUE	DECISION EVIDENCE
CISO / security leadership	Role-aligned capability development and defensible practice boundaries	Pilot outcomes, gaps, and governance requirements
Security managers	Structured routes, repeat attempts, capstones, and after-action remediation	Exported operator records and practical receipts
Learning & development	120h45m catalog with clear learning-to-practice workflow	Cohort plan, completion signals, learner feedback
Internal assurance / red team	Signed scope, campaigns, evidence, findings, retests, reports	FieldOps tabletop and sample case file
Endpoint engineering	Local deployment with controlled Docker and keyring dependencies	Install, upgrade, rollback, and data-retention runbook
Procurement / legal	Transparent retail model and explicit current-state disclosures	Commercial agreement, EULA, security review

Where DaemonCore fits

DaemonCore is best positioned as a practical workforce-development and authorized assessment platform for teams willing to manage local endpoints and evaluate current enterprise gaps directly. It should complement - not falsely claim to replace - a company's identity provider, LMS, SIEM, vulnerability-management system, or centralized cyber range infrastructure.

BUYER TAKEAWAY

The near-term value is real practical depth, sealed local environments, evidence-led progression, and accountable FieldOps operations. The enterprise expansion opportunity is centralized administration, integrations, fleet deployment, and formal assurance.

DAEMONCORE // ENTERPRISE EVALUATION

Build operators who can show their work.

Use the platform to diagnose capability, build deliberate learning routes, practice inside disposable systems, preserve evidence, and graduate authorized operators into the FieldOps War Room.

RECOMMENDED NEXT STEP

Run a managed six-week cohort with representative junior, mid-level, and senior practitioners. Include one endpoint engineer, one security leader, and one training owner in the evaluation team.

Evaluation checklist

- Select pilot roles, endpoints, and a named internal owner.
- Review EULA, release signing notice, Docker privileges, and local data handling.
- Choose Academy routes and define practical evidence expectations.
- Decide whether FieldOps is included and identify organization-owned test assets.
- Document required enterprise integrations and support terms before scale-up.

academy.daemoncore.app	github.com/DaemoncoreApps
PRODUCT AND DOWNLOADS	RELEASE TRANSPARENCY

Product facts validated against the DaemonCore Academy 6.0.0 repository and release contract on 1 September 2026. This brief is product information, not a certification, penetration-test authorization, or substitute for organizational security review.