Sepio Platform Training Agenda

Customer training program

This training program is designed to support the effective adoption and operation of the Sepio platform across your environment. It provides a guided framework for understanding the platform's architecture, deployment model, and operational capabilities, while establishing the foundation for ongoing use by technical and security teams.
By combining theory, platform walkthroughs, and practical exercises, the program helps translate product capability into operational readiness. Its purpose is to ensure that participating teams can confidently manage the platform, derive meaningful security value, and support broader organizational resilience goals.

Brand: Sepio
Client: **TBC**
Date: April 2026
Ver: 1.01

Program Overview

Course Details

Course name	Sepio Platform Operator + Administrator Training (On-Prem + Network + Endpoint)
Format	Instructor-led, hands-on labs + guided walkthroughs
Recommended duration	2 days (can be compressed into 1 day; see option at the end)
Primary outcome	Participants can install, connect network infrastructure and endpoints, interpret risk, and automate mitigation using Control Center, notifications, and reporting.

Target Audience

- SecOps / SOC analysts (risk triage, investigations, reporting)
- IT Ops / Network admins (switch onboarding, scan engines, enforcement actions)
- Endpoint / EUC admins (agent rollout, device control posture)
- Platform admins (roles, integrations, logs, operations)

Prerequisites

- Basic networking (VLANs, switches, SNMP/SSH, ports)
- Basic endpoint management (MSI deployment / software distribution tools)
- Familiarity with SIEM/SOAR concepts is helpful (for integrations)

Recommended Training Environment

- On-prem Sepio management server deployed and accessible via TCP/443
- At least 1–2 lab switches reachable from Sepio / Scan Engine over SSH + SNMP
- 1–2 Windows endpoints for agent exercises + optional VDI endpoint
- Optional: a “test peripherals kit” (USB storage, HID, composite device, etc.) for agent policy exercises

Learning Objectives

- Install / operate the containerized on-prem management platform
- Deploy and manage Scan Engines (internal/external), onboard switches/WLCs, and tune scanning
- Deploy Sepio agents and select operating modes (visibility vs enforcement postures)
- Investigate and action Risk Indicators, including workflows for Accepting Risk and mitigation
- Use filters/queries/tags to operationalize Sepio data in day-to-day SOC workflows
- Configure Control Center rules/policies for automatic actions (allow/block/auto-tag)
- Enable integrations + outbound feeds (Syslog formats, SIEM/SOAR/CMDB)
- Use event/audit logs, notifications, and scheduled reports for operational readiness

- Day 1 agenda — Installation + Architecture + Network onboarding

Day 1 Agenda - Installation, Architecture, and Network Onboarding

Time	Session
09:00 – 09:30	**Kickoff + course orientation** • Goals, success criteria, lab rules of engagement • "What good looks like" at the end of Day 2 (working deployment + enforced controls)
09:30 – 10:15	**Module 1: Sepio Architecture Overview** • What Sepio solves and the "visibility → risk → mitigation" chain • Solution components: Management Platform + Scan Engine + Endpoint Agents • Why Sepio doesn't rely on traffic monitoring; Layer-1 detection properties • Deployment patterns: centralized + per-branch scan engine, multi-branch scan engine
10:15 – 10:30	**Break**
10:30 – 12:00	**Module 2: Sepio On-Prem Installation (Admin focus)** • Installation prerequisites • Access model, TLS/443 entry point • DNS/FQDN considerations and "who needs to reach what" • Installation process • Containerized deployment & operational model (docker compose) • Initial hardening checklist (accounts, RBAC, baseline settings) • Post-install validation • First login + supported auth methods (local users / LDAP / SAML) • Health checks and "is it working?" indicators • Hands-on Lab 1 (guided): On-prem bring-up + first login • Validate UI access, confirm system health, create admin + operator roles
12:00 – 13:00	**Lunch**
13:00 – 14:15	**Module 3: Platform UI & Navigation (Operator foundations)** • Visibility Overview and key widgets • Visibility screens: discovered assets / hosts / network infrastructure • Queries (saved searches) • Logs, Reports, and Settings map • Hands-on Lab 2: "UI scavenger hunt" • Find: top risks, newest discovered assets, network inventory, agent inventory • Build and save 2 queries: "Unsupervised infra" and "High risk peripherals"
14:15 – 14:30	**Break**
14:30 – 16:30	**Module 4: Network Infrastructure onboarding (Core operational skills)** • Scan Engines

Time	Session
	• Internal vs External Scan Engine; where to use each • Adding switches / WLCs • SSH preferred vs SNMP; why SSH matters for Asset DNA; SNMP for enforcement • Bulk onboarding (CSV) • Scan intervals • Per-switch and bulk tuning; manual scan • Switch-related data • Port layout, CDP/LLDP, PoE, fingerprint/DNA, risk score • Actions • Accept/Unaccept risk, rescan, priority, assign domain, tag, debug logs • Block port workflow • Hands-on Lab 3 (capability lab): Add 2 switches + validate Asset DNA collection • Onboard 1 switch via SSH+SNMP and 1 via SSH only (as applicable) • Verify assets appear, verify per-port fingerprints, run a rescan, set scan interval • Execute: “Accept Risk” vs “Block Port” on a test port (safe sandbox)
16:30 – 17:00	**Day 1 wrap** • Q&A, “what to prep for tomorrow” (agents + risk workflows)

Day 2 Agenda - Agents, Risk Workflows, Automation, and Reporting

Time	Session
09:00 – 09:30	**Day 2 kickoff + recap** • What we deployed yesterday; quick health check
09:30 – 11:00	**Module 5: Installing Agents + Endpoint operations** • Agent purpose (visibility + enforcement) • Deployment approaches (manual, software distribution tools) • Agent modes (operating postures) • Free/Visibility mode • Armed (allow-list enforcement) • BKT modes (block known threats; mass storage variations) • Composite devices and approval logic • Agent UUID behavior (hardware-based persistency) • CLI install options (CENTRALIZEDIP and recovery override behavior) • Hands-on Lab 4: Agent rollout + posture change • Install agent on 1–2 endpoints • Validate host appears in Visibility → Hosts • Run: Visibility-only → Armed → test approval flows with a composite USB device

Time	Session
11:00 – 11:15	**Break**
11:15 – 12:45	**Module 6: Understanding Risk (SOC workflows)** • Risk Indicator model and risk score logic • Risk Indicator groups (network vs peripheral) and investigation flow • Notifications by Risk Indicator group (App / Syslog / Email) • "Accepting Risk" workflow: when to accept, when to mitigate, and how to document • Hands-on Lab 5: Triage to action • Pick 3 risks (2 network, 1 peripheral) • For each: confirm root cause, decide accept vs mitigate, document rationale • Configure a notification rule for a high-signal Risk Indicator group
12:45 – 13:45	**Lunch**
13:45 – 14:45	**Module 7: Understanding Sepio Data (Filters, Query Hub, Tags)** • Filters strategy for SOC: slicing by location, domain, risk, asset type • Saved Queries (building reusable detections) • Tagging and user attributes: • Operational tagging model (site, business unit, criticality) • Tag-driven workflows (triage routing, reporting, policy targeting) • Hands-on Lab 6: Build an "operations pack" • Create 5 saved queries (examples): • New unmanaged assets (last 24h) • High-risk peripherals on endpoints with Armed mode • Rare devices in critical VLAN • Unsupervised infrastructure • Assets with repeated anomalies • Apply tagging strategy and generate a tag-based report
14:45 – 15:00	**Break**
15:00 – 16:00	**Module 8: Control Center (Automated mitigation / policy)** • Rules, rulesets, policies and how they map to actions • Automatic actions: • Network devices: allow/block/auto-tag (granular match criteria) • Hosts: current scope (auto-tag) • Policy design patterns: • "Containment first" vs "Zero Trust enforcement" • Safe rollout (monitor → tag → enforce) • Hands-on Lab 7 (capstone automation): From detection to enforcement • Create a policy that targets a tag/domain and auto-tags suspicious assets • Create a second policy that blocks a specific test scenario (lab port / lab device) • Validate actions and audit trail

Time	Session
16:00 – 16:40	**Module 9: Integrations + logs + scheduled reporting** • Integration landscape (CMDB, SIEM/SOAR, NAC, microseg, UEM, etc.) • Syslog outbound formats + transport options • Event/Audit logs and how to use them operationally • Scheduled and on-demand reporting • Hands-on Lab 8: Operational readiness • Enable syslog feed (pick format), validate receipt in lab collector/SIEM • Export logs and produce a “weekly posture report” template • Configure 2 scheduled reports: Exec summary + SOC queue view
16:40 – 17:00	**Final assessment + close** • Short practical check: • Onboard a switch / rescan • Identify 1 risk and choose mitigation path • Show 1 saved query + 1 policy + 1 report • Wrap-up + next steps (runbooks, escalation, support channels)

Certification: SCSA Final Test + Issuance

Timing	Day 2, last 60–90 minutes (or immediately after the last module in a 1-day version)
Objective	Verify the attendee can independently operate Sepio in production-like conditions (install/onboard/triage/mitigate/report).

Part A — Practical exam (recommended, 45–60 min)

Attendees must complete a guided-but-graded scenario:

Platform readiness	Confirm UI access and basic health checks
Network onboarding	Add a switch (or validate an existing one), trigger a scan/rescan, confirm key artifacts appear
Agent operations	Validate at least one endpoint agent is reporting and apply an operating posture change (visibility → enforcement)
Risk triage & mitigation	Investigate 2 risks (1 network + 1 peripheral), decide Accept Risk vs Mitigate, and execute one mitigation action (policy / port action / containment workflow)

Operationalization	Create 1 saved query + 1 tag strategy item Configure 1 notification rule OR generate 1 scheduled report

Passing criteria (example):

- Practical: 80%+ completion of required tasks, with no critical mistakes (e.g., unsafe enforcement on non-lab assets)

Part B — Knowledge quiz (optional, 15–20 min)

- 20–30 questions (multiple choice + short answers)
- Covers architecture, scanning concepts, indicators, filters/queries/tags, integrations/logs/reports

Passing criteria (example):

- Quiz: 75%+

Certification award

Upon successful completion of the final test, attendees will receive a formal Sepio Certified Specialist – Security Administrator (SCSA) certificate, including certification date and validity period, issued in the same format as the attached certificate.