Quick Heal Seqrite EPS/EDR – Local Corporate Rollout (Single Office)

"Project Tag"

"Local corporate rollout of Quick Heal Seqrite EPS/EDR with AD-mapped policies, IDS/IPS, web threat controls, and email-based alerting & runbooks."

==

Report Owner / Author

- Name: Niranjan Bhardwaj
- Current Role: System Administrator (3+ years of experience in IT Infrastructure & Security)
- Core Competencies: Endpoint Security, Infrastructure Management, SIEM Deployment, Vulnerability Assessment, Security Analyst
- Certifications:
    - **Certified Ethical Hacker (CEH v13)** – EC-Council
    - **Cisco Certified Network Associate (CCNA)** – Cisco
- GitHub Portfolio: https://github.com/BhardwajNiranjan
- Linkedin: https://www.linkedin.com/in/niranjan-bhardwaj-64577a185
- Contact **cyber01help@gmail.com**

==

Role: System Admin (IT Secruity)
Scope: Internal Security Monitoring for one site (LAN), Windows/MAC/Linux Endpoints & Servers
Tooling: Seqrite EPS / EDR (by Quick Heal)
Functions in Scope: On-access Scanning, Scheduled Scans, Threat **Detection & Prevention**, **Alerting & Response**, **Malicious Site Blocking (as per policy)**, **Host IDS/IPS**, **Email Notifications**
Deployment Modes: Manual Installer, Remote IP push, AD Synchronization.

---

1) Objectives & Success Criteria

- Standardize endpoint protection and EDR telemetry across all in-scope systems.
- Enforce policy-based controls (AV/EDR, Host Firewall, IDS/IPS, Web/malicious site blocking, device control).
- Establish reliable alerting via **SMTP email** to security mailbox.
- Provide step-by-step deployment, validation, and runbooks for incident handling.

Done = All targeted endpoints enrolled, baseline policies applied, alerts delivered to mailbox, runbooks tested, and reporting operational.

---

2) Environment & Assumptions

- **Directory:** Active Directory (single forest/domain, OU structure by department/role).

- **Endpoints:** Windows 10/11 (user devices), Windows Server (infra apps).
- **Network:** Single site (LAN/WLAN)
- **Email (SMTP):** only for Alert Notifications
- **Firewall:** Internal allow rules for EPS server ↔ endpoints (agent comms, definitions).
- **Access:** Domain admin for GPO deployment; local admin or secure cred for remote IP push.

---

3) Roles & RACI (concise)

- **Implementation Lead (You):** Own install/config, policies, alerts, rollout, docs (Responsible/Accountable).
- **Infra Admin:** AD/GPO support, firewall/ports, file shares (Responsible).
- **Helpdesk:** Staging devices, user comms, basic triage (Responsible).
- **IT Manager:** Approvals, exceptions, acceptance (Consulted/Informed).

---

4) High-Level Architecture (Local)

- **Seqrite EPS Server** (Mgmt + MYSQL DB) on hardened Windows Server (member server).
- **Endpoint Agents** installed on workstations/servers/Endpoint Devices.
- **Active Directory Integration** for OU import & policy mapping.
- **SMTP** configured on EPS for notifications (alerts, detections, agent health).
- **Dashboards/Reports** Status of all connected users, patch update, Deployed client agent, Assets Information, Scanning Reports, Threats Level, Attack Types or Netwrok Health.

---

5) Pre-Requisites & Preparation

1. **Sizing & Platform**
   - Windows Server VM (meets EPS specs), system & data disks separated; AV exclusions for EPS folders/DB.
   - Time sync (NTP), hostname/DNS set, service account (if used).
2. **Network & Ports**
   - Allow EPS server management & agent channels (per vendor docs).
   - Allow internet for definition/signature updates (or configure internal proxy).
3. **Directory & Shares**
   - AD access for **read** (OU import); GPO creation rights for deployment.
   - SMB share for MSI/EXE packages (read for Domain Computers).
4. **Email**

   - Security mailbox (e.g., security@company), SMTP relay host/port, TLS/credentials if required.

5. **Inventory & Policy Matrix**
   - Endpoint list (hostname/OU/owner/role).
   - Policy personas: **User-Workstation**, **Laptop**, **Server (Non-Critical)**, **Server (Critical)**, **IT/Exceptions**.

---

6) EPS Server Installation & Core Setup

1. Install **Seqrite EPS/EDR Server** (latest stable(used V7.6)).
2. Create **admin roles**:
   - Security Admin (full), Helpdesk (view/acknowledge only), Reporting (read).
3. **AD Integration**
   - Connect domain, import OU structure, schedule periodic sync.
   - Map **EPS Groups ↔ AD OUs** (so endpoints inherit correct policies).
4. **SMTP Notifications**
   - Configure SMTP host/port/TLS/auth.
   - Test email to *security@company*.
5. **Update/Signature Settings**
   - Stagger definition updates to avoid bandwidth spikes; set retry windows.

---

6) Baseline Security Policies (by Persona)

Create separate policies for each persona. Below are recommended controls.

A) Real-Time & Scheduled Scanning

- Real-time/on-access scanning: **Enabled** for files, scripts, archives.
- **Quick Scan**: Daily during low activity (e.g., lunch window).
- **Full Scan**: Weekly for users; **bi-weekly/monthly** for servers during maintenance.
- **Heuristics/Behavior**: Enabled with balanced sensitivity.

B) Web & Malicious Site Control

- Enable **malicious/phishing** categories block.
- Block **known malware distribution** domains.
- Optional: limit risky categories for general users per HR/Policy.
- Configure user notification when access is blocked.

C) Host Firewall & IDS/IPS

- Host firewall: default-deny inbound; allow required outbound.
- IDS/IPS: enable rules for exploit attempts, suspicious SMB/WinRM, port scans (with tuned thresholds).

D) Device Control

- USB storage **read-only** for users; **blocked** on critical servers.
- Allow smartcard/keyboard/mouse; log all new device class events.

E) Tamper Protection & Passwords

- Lock console changes; admin password for uninstall/disable.
- Protect agent services from stop/kill.

F) Email Notifications & Logging

- Trigger emails for **High/Critical detections**, **quarantine events**, **scan failures**, **agent offline beyond threshold**.
- Include **IOC fields**: file hash, path, process, user, timestamp, hostname.

G) Update & Bandwidth

- Hourly signature polls with jitter; local caching if supported.

---

7) Agent Deployment – Three Methods

(1) Manual Installer (Pilot / Exceptions)

- Build installer from EPS console (includes server address/token).
- Local install command (silent example – **replace properties with vendor-provided ones**):
- Verify device appears in the correct **Group/OU** and policy is applied.
- Run .exe installer file for windows, Extract Installer Zippped file for Linux/MAC.

(2) Remote IP Push (Small Batches)

Prereqs: Endpoint reachable, admin creds, remote registry/WMI/SMB allowed.

- From EPS console: **Add by IP/IP-range**, supply credentials, push agent, Remote installation, by Active Directory Sync.
- Post-install: confirm heartbeat, definitions, and policy sync.

(3) AD Sync + GPO (Primary @ Scale)

1. Ensure EPS imports OUs; **map** OU → EPS Group/Policy.
2. Place **MSI** on a UNC share (Domain Computers: Read).
3. Create **GPO**:
    - Computer Config → Software Installation → New Package → Select UNC MSI.

    - Set **Assigned** (install at startup).
    - Link GPO to target OU(s).
4. Coordinate reboots/off-hours install.
5. Validate enrollment & policy through EPS console.

Note: Exact MSI properties vary by release—use the EPS console/package builder and vendor docs for the correct property names.

---

8) Validation & UAT (Local Office)

- **Coverage Check:** All targeted hosts show in console with green health.
- **Policy Check:** Endpoint shows correct persona policy; test a benign **EICAR** string in a safe lab to validate detection & quarantine.
- **Web Block Test:** Attempt a known test category (e.g., "malware sites" category test pages) to confirm block/notify.
- **Email Alert Test:** Trigger a controlled alert; verify **security@company** receives details within expected time.
- **Server Windows:** Confirm scans run in maintenance windows with no business impact.

---

9) Operations – Daily/Weekly/Monthly

Daily

- Console health: offline agents, outdated definitions, new detections.
- High/Critical alert mailbox triage; ticket creation.

Weekly

- Report: detections by type, top hosts, blocked URLs, scan compliance.
- Review new exceptions; confirm they're time-bounded and documented.
- Check device control violations (USB insert events).

Monthly

- Policy tuning review (false positives, new app rollouts).
- Agent & server updates; DR test of EPS database backup/restore.
- Stakeholder summary to IT Manager/InfoSec.

---

10) Incident Runbooks (Local SOC Style)

A) Malware Detected (High/Critical)

1. **Contain:** Auto-quarantine; isolate host if suspicious lateral movement observed.

2. **Verify:** Hash check, process tree, user session, first-seen time.
3. **Eradicate:** Remove file, kill process, clear persistence (startup tasks/Run keys).
4. **Recover:** If false positive, restore & add scoped exclusion after approval.
5. **Document:** Ticket with IOC, root cause, and controls adjusted.

B) Malicious Site Blocked

1. Confirm user/process, URL/domain, and frequency.
2. Educate user; if campaign suspected, send advisory.
3. Add domain/IP to upstream deny lists (firewall/proxy) if required.
4. Monitor for repeats across endpoints.

C) IDS/IPS Host Alert

1. Inspect signature, source/destination, ports.
2. Correlate with Windows event logs (e.g., 4624/4625/4672) and admin activity.
3. If suspicious, tighten host firewall temporarily, scan endpoint, and review neighboring systems.
4. Escalate if persistence/lateral indicators found.

---

11) Change, Exceptions & DR

- **Change Control:** All policy edits via ticket with approver & rollback plan.
- **Exceptions:** Time-boxed, least-privilege scope, documented reason & owner.
- **Backups:** EPS config/MYSQL-DB backups scheduled; restore steps documented and tested.
- **Versioning:** Maintain version log of EPS server/agent and policy change history.

---

12) Handover Artifacts

- **Admin Guide:** EPS console tour, policies, deployment, alert routing.
- **Runbooks:** Malware, URL block, IDS/IPS, agent health.
- **GPO Doc:** Linked OUs, MSI path, install options, troubleshooting.
- **Contact Sheet:** Roles, escalation path, vendor support info.

---

13) Troubleshooting Quick Notes

- **Agent not enrolling:** DNS/name resolution, firewall ports, token mismatch, time skew.
- **GPO install fails:** Use UNC (not local path), computer-scope permissions, reboot needed.
- **Excessive alerts:** Tune sensitivity, add scoped exclusions, confirm no conflict with other agents.
- **Email not sending:** SMTP auth/TLS/port, mailbox quota, spam filtering.

“Project Tag”

“Local corporate rollout of Quick Heal Seqrite EPS/EDR with AD-mapped policies, IDS/IPS, web threat controls, and email-based alerting & runbooks.”