Technology Stack Research

Study Cryptographic Libraries (OpenSSL, LibreSSL)

A. OpenSSL (Industry Standard Crypto & TLS Library)

Most widely used crypto library for TLS **[Transport Layer Security]**, hashing, signatures.

Why OpenSSL matters for your EDR

- mTLS certificate creation & verification
- SHA256 hashing functions
- RSA/ECDSA signature generation & verification
- Secure update pipeline

Pros

- Industry standard
- Feature-rich (TLS, PKI, crypto)
- Large community

Cons

- API can be confusing because old and verbose

How OpenSSL Works

OpenSSL provides:

- TLS 1.2/1.3 implementation
- X.509 certificate parsing & validation
- Random number generation

Agents typically link against libssl + libcrypto.

Does OpenSSL Work for Your EDR? → YES (Strongly Recommended)

Why It Works

✓ Required for mTLS (agent certificate + server certificate)
✓ Required for signed updates
✓ Required for SHA256 hashing
✓ Cross-platform and secure
✓ Well-documented

Limitations

✕ Common source of bugs if memory not handled correctly

Suitability Score: 10/10

→ Recommended for both agent and CMS security.

B. LibreSSL

How LibreSSL Works

LibreSSL is a fork of OpenSSL created by the OpenBSD team to improve:

- Cleaner codebase
- More secure defaults
- Simpler API design

It provides the same functionality (mostly) as OpenSSL.

Why LibreSSL may be considered

Pros

- Enhanced security
- Drop-in replacement for many OpenSSL uses.

Cons

- Fewer features
- Smaller community
- Less documentation

Does LibreSSL Work for Your EDR? → POSSIBLY (But Not Recommended)

Why IT works

✓ More secure defaults
✓ Cleaner codebase
✓ Easier-to-maintain API

Limitations:

✕ Many features of OpenSSL are missing (Like mention in cons)
✕ Not fully compatible with all OpenSSL API's.

Suitability Score: 6/10

→ Suitable only if you prioritize minimal, secure crypto without full OpenSSL features.

Final Recommended Stack for BESS EDR:

1. **C++ Frameworks**
    - Poco + selected Boost libraries

    Reason: Best mix of simplicity + performance

2. **Agent Database**
    - SQLite for agent
      Reason: Lightweight, embedded, reliable

3. **CMS Database**
    - PostgreSQL for CMS (optional scaling).
      Reason: Handles multiple devices efficiently.

4. **Real-time Protocol**
    - WebSocket for dashboards
    - gRPC for high-scale version
      Reason: Both serve different needs.

5. **Cryptography Library**
    - OpenSSL (mTLS, signatures, hashing)
      Reason: Best for mTLS + signatures