Triggers

- STIX Threat Hunting
- Ad Hoc Collection
- Periodic Collection
- Change Triggered Collection

Endpoint Identification & Assessment Planning

Endpoint Discovery: determine the type of endpoint to be posture assessed
← Endpoint Information

Endpoint Target Identification: Identify what potential endpoint targets the checklist should apply to
← Endpoint Information

Endpoint Component Inventory: Collect & consume the hardware / software / account inventory for target endpoints (if needed)
← Endpoint Information

Could be same or different stores

Posture Attribute Identification: Determine the set of posture attribute values needed

Endpoint Posture Attribute Value Collection

Collection Guidance Acquisition: query appropriate security automation data stores to find the "applicable" collection guidance
← Collection Guidance

Posture Attribute Value Collection: values for the required posture attributes are collected
→ Posture Attribute Values

Posture Attribute Evaluation

Posture Attribute Value Query: Posture attribute values are queried from the appropriate data stores

Evaluation Guidance Acquisition: query appropriate security automation data stores to find the "applicable" evaluation guidance
← Evaluation Guidance

Posture Attribute Evaluation: posture attribute values from previous collection processes are evaluated using the evaluation guidance
→ Posture Evaluation Results

RFC 7632: Automated Checklist Verification (2.2.2)