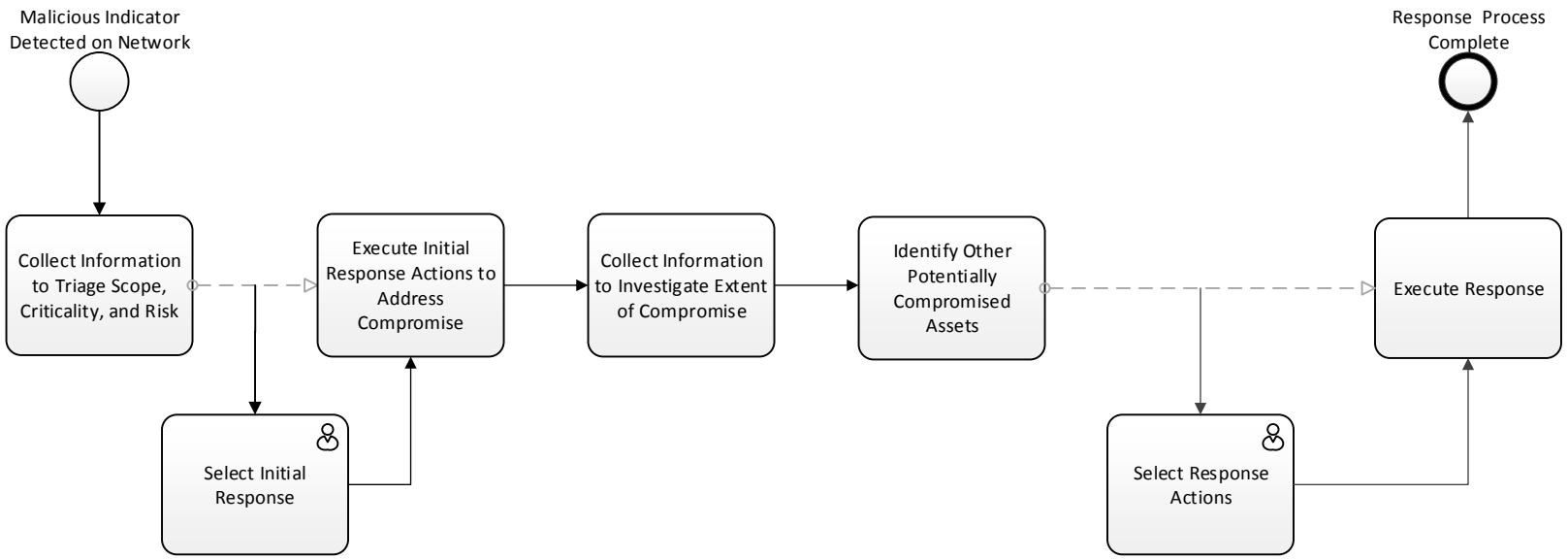
Malicious Indicator Detected on Network



Triage Information

- Criticality of Associated Assets
- Potential Scope of Compromise
- Connectivity of Compromised Assets

Initial Response Options

- Quarantine System(s) or Device(s)
- Blocking Specific IP/URL/Domain
- Update Email Filtering
- Initiate Enhanced Monitoring of Assets
- Log Users Off Associated Device(s)
- Restrict Account Privileges
- HoneyNet Assets
- Collect Forensic Information
- Blackholing Website

Extent of Compromise Information

- Network, Proxy, and Email Logs
- Network Traffic
- Logs of Account Usage/Accesses
- Forensic Analysis
- User and Device Information and Privileges
- Vulnerability Analysis
- Incident Response Logs/ History
- Malware Scan

Response Options

- Compromised Account Playbook
- Produce Incident Report
- Suspicious Account Playbook
- Flag for Further Investigation
- Clean or Reimage Device(s)
- Clean Backup(s) and Image(s)
- Clean Profile(s)

This playbook maintains the effectiveness of a subset of controls associated with:
NIST Cybersecurity Framework: PR.PT-1, DE.AE-2, DE.AE-3, RS.RP-1, RS.AN-1, RS.AN-3, RS.MI-1, RS.MI-2