Finding Malicious Domains Using Shadow Server Reports

Threat Data
- Collect threat data from multiple sources.
  - Open sources
  - Private sources
  - Commercial sources
  - IP addresses
  - DNS names
  - Malware hashes

Indicator Expansion (Optional)
- Merge threat data to discover new associations
  - Attributes that may associate
  - IP addresses
  - Malware
  - Domain names

Retrospective Analysis
- Review sensor data to determine if associated activity was seen
  - Logs
  - Network flow records
  - Passive DNS
  - IDS/IPS

US-CERT Reporting
- Report suspicious or malicious activity