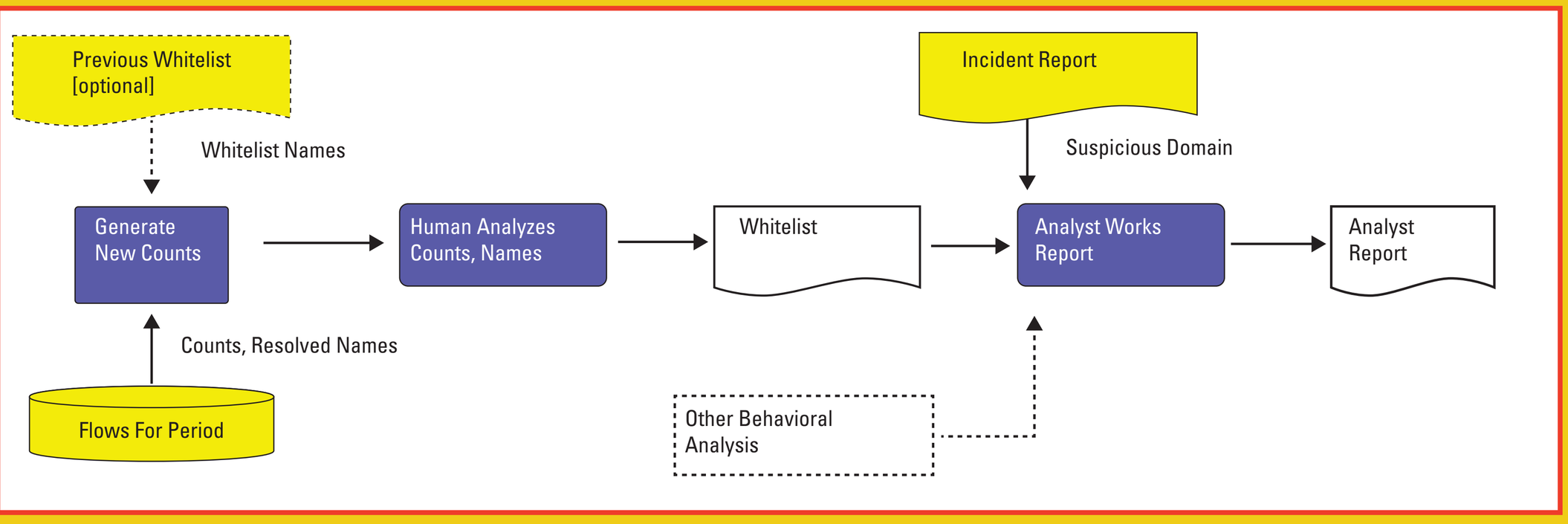
FloCon®2013

Behavioral Whitelists of High Volume Web Traffic to Specific Domains

CERT: George Jones, Tim Shimeall



What

Create whitelists of external domains receiving large volumes of web traffic for use in incident analysis.

Why

Situational Awareness

- "Is that bad traffic coming from an obscure isolated IP or from GigantoProxyFarmInc?"

Sanity Checks for Security Analysts

- "Am I about to tell my constituents to block all traffic to or from MegaCloudCo?"

How

Pull outbound web traffic some period.

Count flows and bytes per destination address.

For the "large" destination

- Deduplicate and resolve domain names
- Drop unresolved addresses
- Drop large, popular sites that may actually be used for malicious purposes (e.g., don't whitelist something large that may be suspect)
- Save the results as sets (ip, name,flows|bytes)

Have a human decide which results to include in whitelists

- Rerun and maintain

So What?

- Avoid issuing embarrassing false reports
- Maintain credibility
- This is one example of behavioral sets; Others might include:
  - Blacklists, beacon destinations, destinations, never seen before, proxies, clients, etc.
- Enables analysts to ask questions like:
  - Tell me everything I know about this destination in terms of behavior over time.
- Volumes, times, services and behaviors-of-interests will vary.

http://www.cert.org/flocon

CERT | Software Engineering Institute | Carnegie Mellon