Raytheon

# Open Source Intelligence (OSINT) Threat Management Model

**Raytheon's OSINT services aid discovery and assessment to mitigate and remediate current threats.**

## Benefits

- Discovery analytics operations (data mining and discovery of unknowns)
- Collaboration services allowing analysts to share trade craft, methods, sources and analysis
- Threat Intelligence reporting and dissemination
- Monitoring of public and private feed(s)
- Extraction and content inspection; indications, warning and alerting; query and/or request services
- Management of threat data ingest and frequency of collection
- Safe crawl and ingest; ingest management of widely-advertised and openly-public data; commercial subscription feed management
- Management of Internet Service Provider/Period of Performance accounts and source services

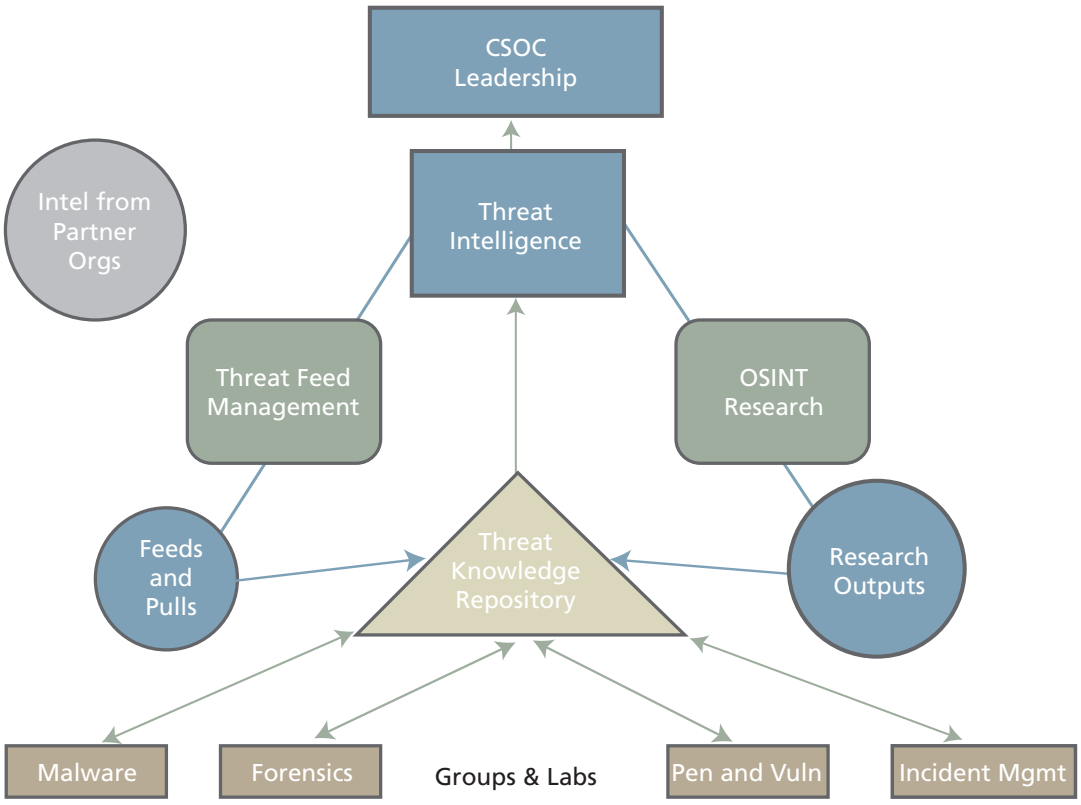
Threat analysts use Raytheon's Open Source Intelligence (OSINT) capabilities and techniques to perform critical research across the Internet for advanced threat indicators. They also aid in the forensics of detected threats or support penetration testing activities. The OSINT solution facilitates access to the Internet through disposable "virtual desktops" that are proxied via VPNs (virtual private networks) to various locations around the world. This ensures that potentially malicious traffic is not brought back into the analysts' core system.

These services aid discovery and assessment to mitigate and remediate current threats. Threat intelligence methods may employ a set of sources or just one source — depending on the case. Some campaigns are conducted in association with a current threat, pre-emptive analysis and/or retrospective cases. This figure highlights specific versions of mission flows consisting of open source, commercial and the potential of combined all-source contributions from national intelligence sources.

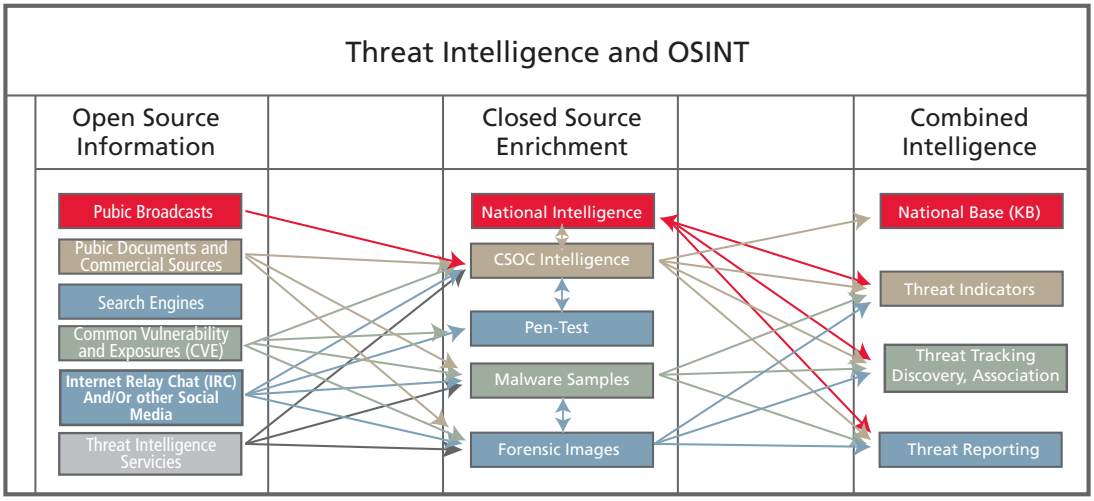
Raytheon offers an integrated OSINT solution, including technology, processes and training, that combines all mission services, managed storage, internal and externally-sourced feeds and analysts' trade craft procedures to enable social media crawl, threat intelligence gathering, access to "open source" subscription feeds, repository access and search/discovery.

Raytheon's solution delivers vital mission capabilities.

# Open Source Intelligence (OSINT) Threat Management Model




**Threat Intelligence Management Model**




**Threat Intelligence and OSINT Sources Processing for Mission Effect**


For further information contact:

**Intelligence, Information and Services**
22260 Pacific Boulevard
Dulles, Virginia
20166 USA
iiscommunications@raytheon.com

**www.raytheon.com**


EVERY SIDE OF CYBER



Raytheon