INQUEST®

Sandboxes

InQuest provides the ability to integrate with a variety of sandboxes and automated malware analysis solutions. These tools perform in-depth, dynamic analysis of malware in a controlled environment, extracting characteristics at runtime that may be hidden from static analysis of the files. The integrations can be configured to be enabled, disabled, or only to run for certain file types as well as threat score ranges assigned by our platform prior to detonation. Dynamic analysis results are then automatically fed into the InQuest platform for score calculation and assignment.

Third-party integrations provide the perfect balance of detection between executable malware and the prolific document-based attacks. There are currently integrations available for a variety of antivirus and sandbox technologies that serve in a complementary capacity to the static analysis that InQuest is performing.

FEATURES & BENEFITS

- Automatically extract, analyze, and score all session artifacts including URLs, IPs, domains, files, and even e-mail addresses
- Can be used as on-premise software or a cloud-based solution, offering more flexibility for CERTS, CIRTS, SOCs, malware analysts and incident responders
- Retrograding threat assignment on historical artifacts based on the latest available threat information enables you to discover attacks that may have previously gone under the radar

DIFFERENTIATORS

- Industry's deepest malware analysis; from high-level system behavioral analytics down to a single assembly instruction
- Threat scoring algorithm factors information from all available sources to produce a single, digestible, well balanced threat score
- Achieve automated file analytics at scale by leveraging our static analysis and reduce your sandbox footprint by only submitting a subset of the artifacts in your environment for dynamic analysis

CROWDSTRIKE

cuckoo

Hatching™ A Recorded Future® Company

JoeSecurity

paloalto® NETWORKS

VMRAY