REPORT ANALYSIS · VISUALIZATION · ENRICHMENT

One threat report in. Every major framework out.

RAVEN reads a single intelligence report and projects it across six frameworks at once, fully grounded, fully cited, and decision ready in seconds.

WHAT IT IS

Analysts spend hours pulling techniques, actors, and indicators out of a report and mapping them across one framework after another. RAVEN automates that entire cross walk. Drop in a PDF, a live URL, a web page, or a STIX bundle, and RAVEN extracts the intelligence, validates every element against the real framework catalogs, and renders one interactive dashboard you can explore, share, and defend.

HOW IT WORKS

01 INGEST
PDF, URL, HTML, or JSON and STIX. The source type is detected automatically.

02 MAP
Techniques, countermeasures, actors, and indicators are extracted and mapped.

03 GROUND
Every element is validated against the real catalogs, with evidence and a score.

04 VISUALIZE
A single interactive dashboard ties every framework together.

05 EXPORT
Navigator layer, CAD graph, STIX bundle, and PDF, ready to share.

SIX FRAMEWORKS · ONE PASS

ATT&CK — MITRE ATT&CK
Adversary tactics and techniques across the Enterprise matrix, each confidence scored and exported as a ready to load ATT&CK Navigator layer.

D3FEND — MITRE D3FEND
The matching defensive countermeasure for every technique, rendered as a native Cyberattack Defense (CAD) graph.

KILL CHAIN — Cyber Kill Chain
The full intrusion reconstructed phase by phase, from reconnaissance through actions on objectives.

DIAMOND — Diamond Model
Adversary, capability, infrastructure, and victim, assembled directly from what the report describes.

DISARM — DISARM
A cross framework view into influence operation and disinformation tradecraft for the information domain.

STIX 2.1 — STIX 2.1 Bundle
A standards compliant bundle of the full analysis, ready to push straight into your existing tooling.

AT A GLANCE

- **Confidence scoring** — Per technique and overall mean
- **Threat actor ID** — Known groups matched from the text
- **Pyramid of Pain** — IOCs tiered by analytic value
- **Malware and tools** — Named families detected and mapped
- **Evidence on tap** — Source text behind every result
- **Navigator ready** — One click ATT&CK layer export
- **Self hosted** — Runs on your own infrastructure
- **Live progress** — Watch each stage as it runs

INPUTS

PDF reports
Vendor and government advisories, threat reports

Live URLs
Point RAVEN straight at a published report online

HTML pages
Raw web pages and saved articles

JSON and STIX
Structured bundles from other tools

OUTPUTS

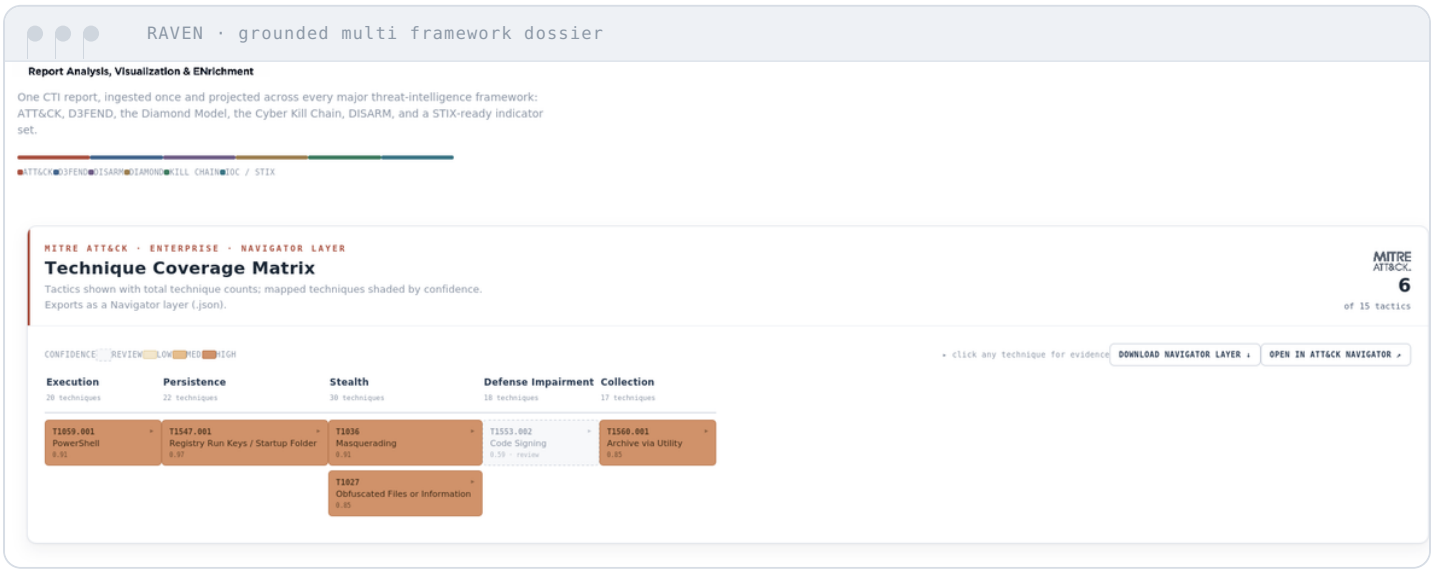
Interactive dashboard
Every framework, tied together in one view

ATT&CK Navigator layer
Load straight into the MITRE Navigator

D3FEND CAD graph
Attack to artifact to countermeasure

STIX 2.1 bundle and PDF
Plus IOCs tiered by the Pyramid of Pain

THE DASHBOARD



One report projected across every framework. The ATT&CK matrix alone exports straight to the MITRE Navigator, and every panel is generated by RAVEN from the source document.

THE DIFFERENCE

Grounded by design. Nothing fabricated.

Every technique, countermeasure, threat actor, and indicator RAVEN produces is checked against the real framework catalogs. Nothing is invented, and every result can be traced back to the report it came from.

VALIDATED
Every ID is real, verified against the live framework catalog before it is shown.

EVIDENCED
Each mapping cites the exact passage in the source it was drawn from.

SCORED
Every match carries a confidence score, so analysts can trust and verify it.

BUILT FOR

CTI Analysts · SOC Teams · Threat Hunters · Incident Responders · Intelligence Shops

The Cyber Security Forum Initiative (CSFI) is a non-profit advancing cyber security capacity across the public and private sectors. RAVEN is a project of its Cyber Threat Intelligence Division.

Engineered to Eliminate Operational Friction

yourorg.org · contact@yourorg.org