

---

THREAT-INFORMED DEFENSE // MITRE CTID

# What Attack Flow Is (And Why It's Worth Using)

A free MITRE project that maps how attackers chain techniques together — not just which techniques exist.

---

## 01 // THE PROJECT, PLAINLY

# Free. Open. Built by MITRE CTID.

Attack Flow is a free (Apache-2.0) MITRE CTID project: a STIX 2.1 extension language and schema, a web Builder GUI, and a corpus of roughly 47 real flows — Conti, REvil, Black Basta, and others.

It describes how adversaries chain ATT&CK techniques into multi-stage flows, with dependencies and branching — not techniques viewed in isolation. Currently v3.2.0, ATT&CK v17-aligned.

*"Helps executives, SOC managers, and defenders easily understand how attackers compose ATT&CK techniques into attacks."*

---

02 // ZERO BUILD. FREE WEB TOOL.

## What each role gets immediately

### 1 CTI Analyst

Turns a prose report or incident into a structured, shareable, machine-readable flow.

### 2 SOC Manager / Exec

Gets a visual attack narrative — here's how it unfolds, and where we'd break it.

### 3 Detection Engineer

Reasons about technique sequences to build correlation detections, and finds where a whole path runs undetected.

---

02 // ZERO BUILD. FREE WEB TOOL. (CONT.)

## Two more roles, same free tool

### 4 IR Analyst

Reconstructs an incident as a flow for the report, plus earliest-detection lessons for next time.

### 5 VTM Analyst / Manager

Gets path-aware prioritization — spots a chokepoint many paths depend on, and funds the one control that breaks multiple paths instead of covering every atomic technique.

---

### 03 // WORKED EXAMPLE: RANSOMWARE, HEALTHCARE

# The representative attack chain

- T1566 Phishing
- T1204 User Execution
- T1003 Cred Dumping
- T1078 Valid Accounts
- **T1021 Remote Services**
- T1041 Exfil-over-C2
- T1486 Encrypt-for-Impact

---

## 04 // THE PAYOFF

# One control instead of six

A detection engineer and VTM analyst adapt a corpus flow in the free Builder, then manually mark which steps their detections cover.

### By inspecting the graph:

T1021 (Remote Services) is the chokepoint most paths to encryption route through — and it's uncovered.

### The move:

One control at the chokepoint breaks the whole path — instead of six isolated detections. Doable in an afternoon, when coverage data is already on hand.

---

## 05 // WHAT THIS DOESN'T DO

# The honest boundaries

- Attack Flow does not compute or score chokepoints. It gives the dependency graph — the chokepoint is human interpretation.
- No Attack Flow ↔ INTERRO/VTM integration exists today. Coverage overlays and any re-weighting are manual, complementary analyst steps.
- The technique IDs used in examples are representative — not the only correct choices for a given incident.

---

## 06 // A COMPLEMENTARY TOOL, NOT AN INTEGRATION

# Where INTERRO AI fits alongside Attack Flow

INTERRO AI doesn't build or ingest Attack Flow diagrams today — that work is Attack Flow's Builder, done manually, as described above.

### What it can do alongside it:

Serve as an ATT&CK + D3FEND research companion while you build the flow — live technique lookups, countermeasure mapping, and posture context for each node you're placing on the graph.

*Two separate tools, used side by side — not one product doing both jobs.*

---

INTERRO AI // AN AI SECURITY ANALYST, ON DEMAND

## Building your own Attack Flow? Research it faster.

Get live ATT&CK and D3FEND lookups for every node you place — a research companion, not a replacement for the Builder.

**Get Your Free Demo Key → [InterroAI.com/demo](https://InterroAI.com/demo)**

---

**Try Attack Flow itself, free:**

[center-for-threat-informed-defense.github.io/attack-flow](https://center-for-threat-informed-defense.github.io/attack-flow)