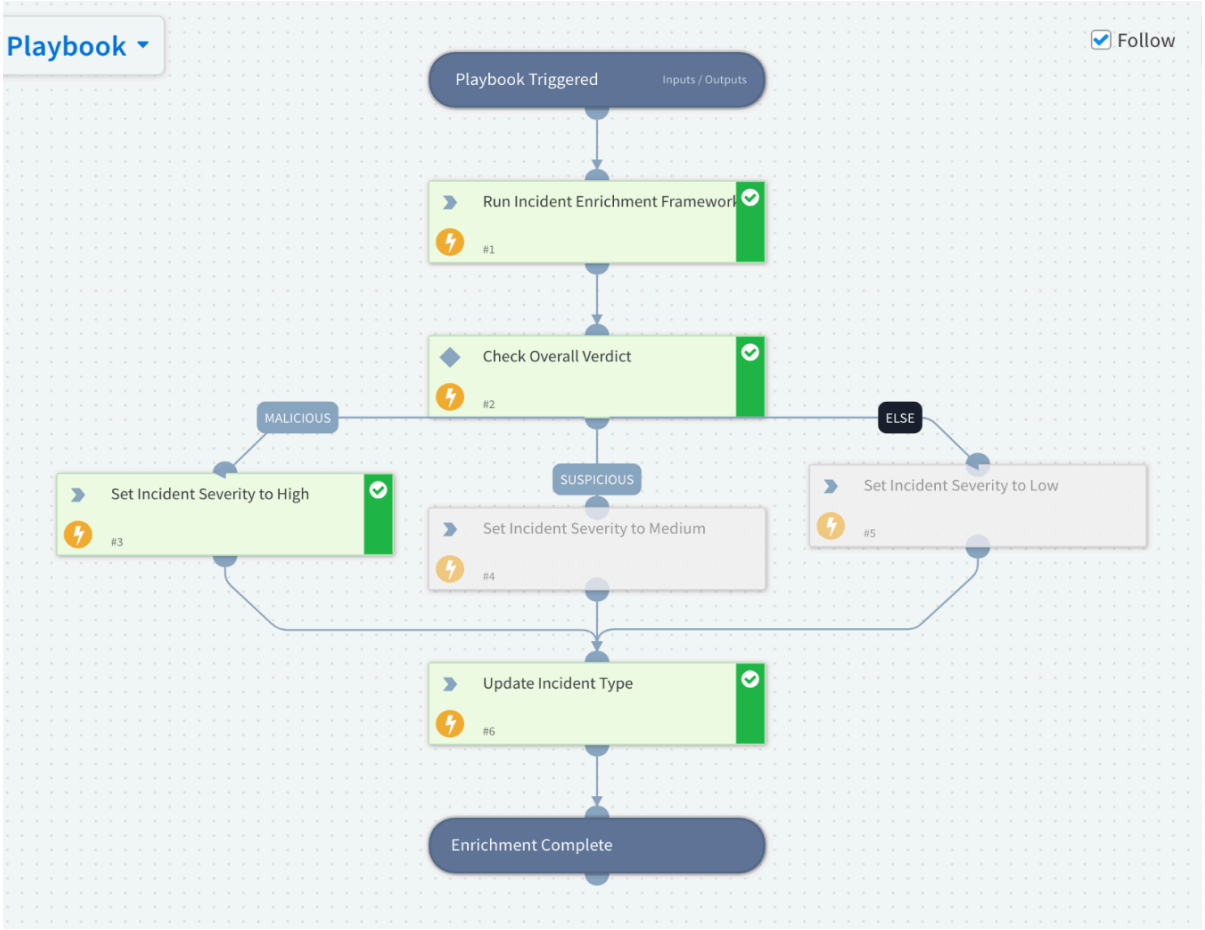
Playbook Flow



Framework report

Unauthorized Credential Extraction Activity – Mimikatz Tool Detected	Malware	High	Active

January 28, 2026 1:59 PM

Task Result #1: Run Incident Enrichment Framework Go to Task

Command: *!IncidentEnrichmentFramework* (Scripts)

```
# Incident Enrichment Report

**Overall Verdict:** MALICIOUS
**Incident Type:** Malware

## Statistics
- Total IOCs: 1
- Malicious: 1
- Suspicious: 0
- Clean: 0

## Enrichment Results

### [!] 61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1 (File)
**Verdict:** MALICIOUS (Score: 90/100)
**Sources:** VirusTotal (API v3), AlienVault OTX v2
```

Parser according to the type of incident source SIEM
Sentinel :

January 28, 2026 1:59 PM

Task Result #1: Run Incident Enrichment Framework Go to Task

Command: *!IncidentEnrichmentFramework* (Scripts)

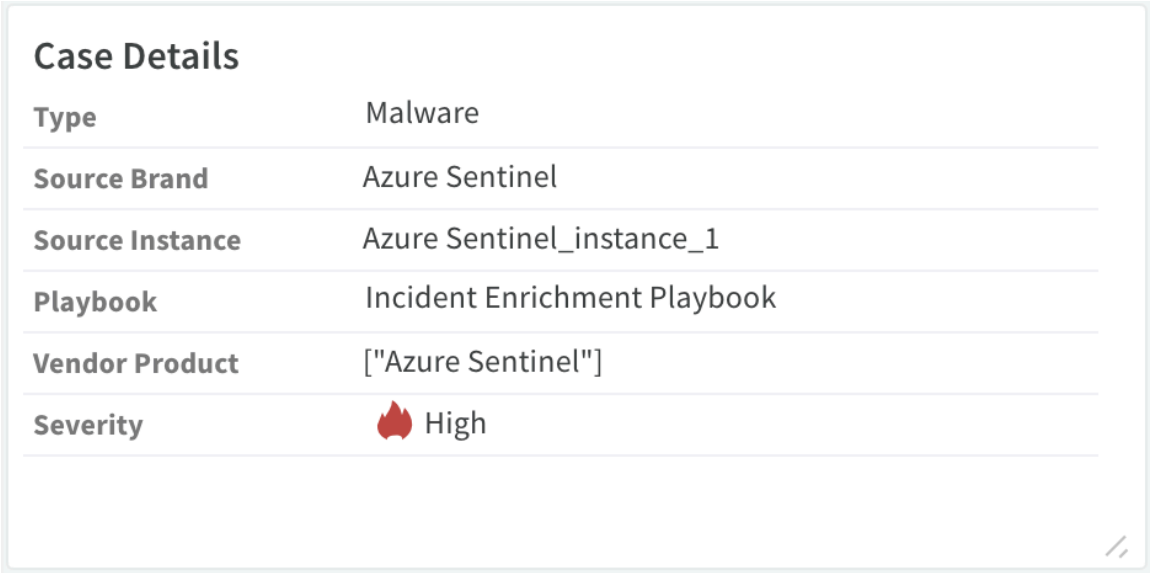
```
### DEBUG: Detected Sentinel incident - using SentinelParser
```

Splunk :

Command: *!IncidentEnrichmentFramework* (Scripts)

```
### DEBUG: Generic incident - using SplunkParser (searchIndicators)
```

Set Incident Type and Severity



Enricher tools :

Abuse IPDB
AlienVault OTX v2
Google Safe Browsing v2
Urlscan.io
VirusTotal (API v3)