One of the biggest pain points of cyber security teams is alert fatigue — trying to keep up with a tedious, never-ending stream of alerts to triage. In today's reality, security teams can spend a large amount of their valuable time on confirming alerts instead of investigating real incidents. Integrating Intezer with EDRs in your alert triage workflow allows you to automate tasks and make sure your team can identify and focus on the most critical alerts.

To tackle the alert fatigue security teams experience and help improve MTTR (mean time to respond), Intezer's integration with the SentinelOne Singularity XDR combines best of breed solutions to automatically triage incidents and provide advanced, enriched verdicts. SentinelOne provides prevention, detection, response, and threat hunting across all major OSes and cloud workloads.

When an incident is created in SentinelOne, the artifact is automatically sent to Intezer for deep analysis and investigation down to the code level. The results of Intezer's analysis are returned in the SentinelOne console, along with a verdict and link to Intezer for additional context and extracted threat hunting detection opportunities. By replacing manual processes with machine-speed detection and deep malware analysis, security teams can respond to incidents with greater speed and confidence.

Here we'll look at how it works.

Intezer + SentinelOne Joint Solution Highlights

- Reduced response time for critical security investigations.
- Increased accuracy and validation of suspicious incidents around threat analysis.
- Retention of past investigations for future events and campaigns.

How Manual Incident Triage Limits Investigations

As the cybersecurity skills gap continues to widen, organizations face challenges in hiring and retaining skilled security professionals. The deluge of alerts from security tooling and the tedious nature of the Tier 1 analyst position makes burnout one of the leading contributors to the shortage of security talent. Security teams look to automation to help alleviate some of the repetitive tasks of incident triage to focus their limited resources on the highest impact and most critical incidents, increasing throughput and reducing the time to respond.

Get a quick preview of how it works in this 3-minute video:

Integration Benefits

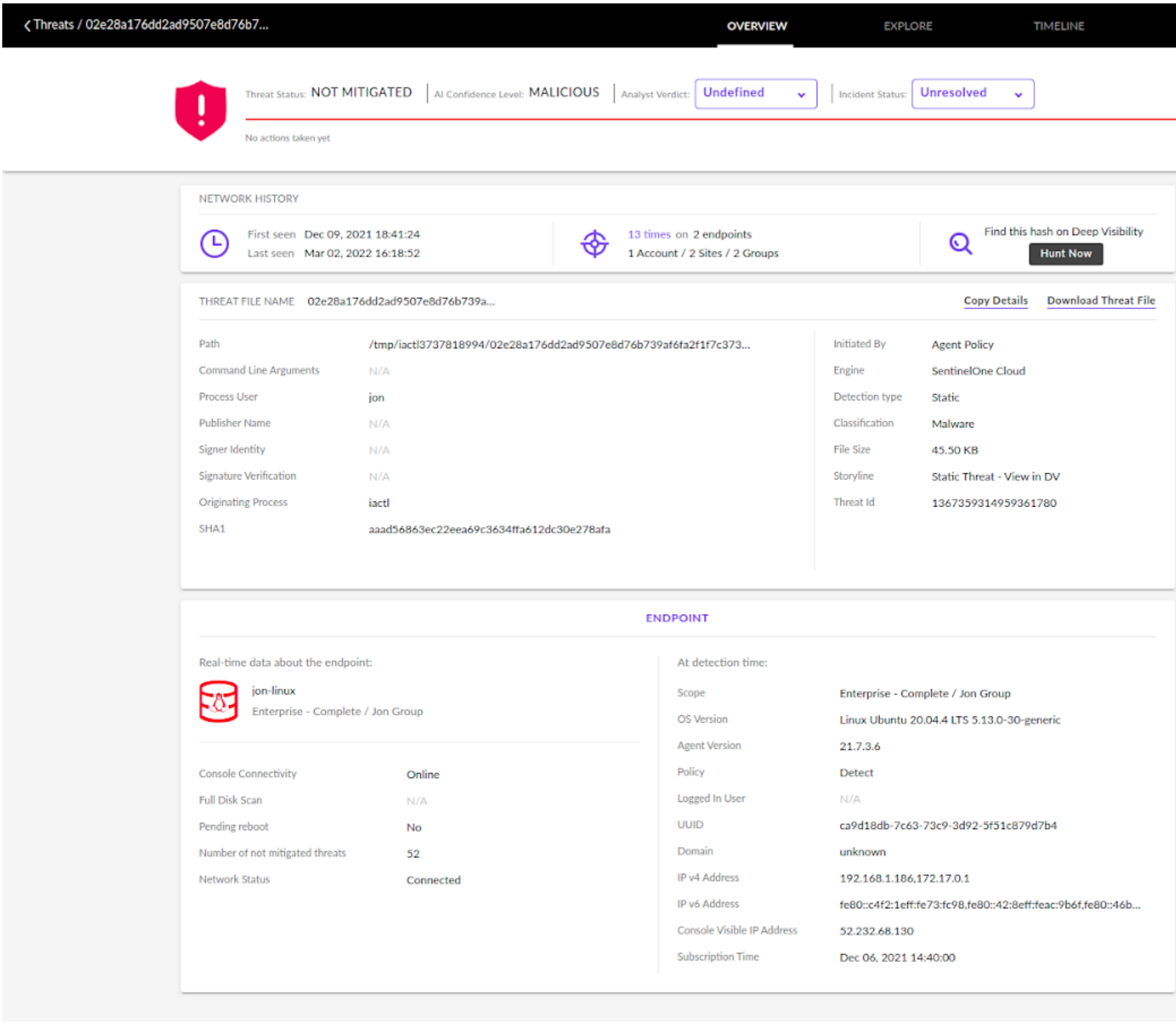
- Alert triage and time savings with a unified workflow.
- Additional context to scanned artifacts including attribution, malware families, indicators of compromise (IOC), and TTPs mapped to MITRE ATT&CK.
- Rapid verdicts of both malicious and benign artifacts classified using Intezer's proprietary genetic analysis solution.
- Out-of-the-box detection content and queries for threat hunting provide immediate time-to-value.

How It Works

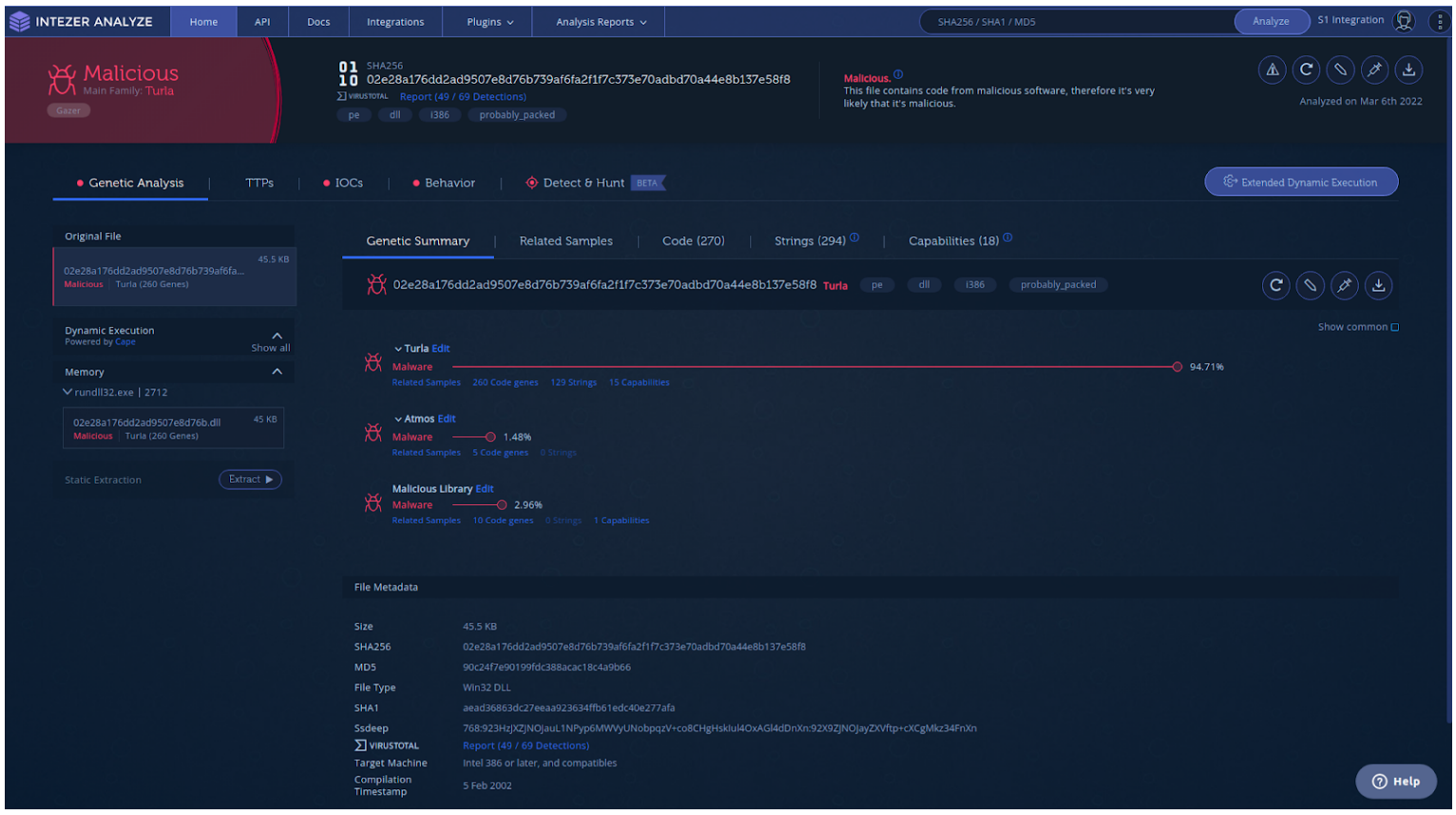
- SentinelOne detects malicious activity on an endpoint and creates an incident.
- Intezer is alerted to the incident and SentinelOne retrieves the artifact from the endpoint for analysis. The artifact is sent to Intezer for analysis.
- Intezer enriches the incident in SentinelOne with an analysis link, context, verdict, and malware family information.
- Users can dive into the linked Intezer analysis report to identify additional IOCs and threat hunting queries.
- Threat hunting queries can be used with SentinelOne Deep Visibility to hunt for additional indicators across the environment.
- Additional indicators can be added to the SentinelOne blacklist or used in a Storyline Active Response (STAR) rule to alert and perform an automated response next time those indicators are seen.
- Autonomously respond in SentinelOne by killing, quarantining, remediating, or rolling back the effects of the malicious file.

Solution Use Cases

- Alert Triage — With automated analysis of suspicious binaries, analysts are able to determine and confirm whether an alert is a true positive which warrants escalation to incident responders.



- Curated Threat Hunting — Intezer provides out-of-the-box detection content and threat hunting queries that can be used within SentinelOne Deep Visibility.



“Too many teams face challenges hiring and retaining skilled security professionals, but they can feel empowered by introducing more automation into their workflows for alert triage, response, and threat hunting with Intezer’s integration that combine seamlessly with SentinelOne’s platform.”

—— Itai Tevet, CEO and Founder, Intezer

Reducing EDR Alert Fatigue for SOC/IR Teams to Improve MTTR

When security teams are overwhelmed with alerts and experiencing alert fatigue, integrating automation into an alert triage process is key reducing the mean time to respond (MTTR) to an incident.

If you are an Intezer customer, use your SentinelOne API key to activate the integration now. If you are not yet an Intezer customer? Request access for a free trial now.

Intezer

Track the latest malware variants and threat actors analyze.intezer.com

Alert Triage Automation EDRs Incident Response integrations SentinelOne Threat Hunting