

ENABLE EDR FILE ACQUISITIONS FOR MANDIANT THREAT DEFENSE

Mandiant Threat Defense needs permission to acquire files from your Endpoint Detection and Response (EDR) environment. This permission is required to triage suspicious files discovered with threat hunting leads. If access is not given, leads may not be correctly classified and the Mandiant Threat Defense service may result in more false positive investigations.

The configuration steps necessary for acquiring files for the following security technologies listed are:

- **CrowdStrike API Access Requirements** (<https://docs.mandiant.com/home/mtd-crowdstrike-api-access-requirements>)
- **Microsoft Defender for Endpoint API Access Requirements** (<https://docs.mandiant.com/home/mtd-microsoft-defender-for-endpoint-api-access-requirements>)
- **SentinelOne Singularity API Access Requirements** (<https://docs.mandiant.com/home/mtd-sentinelone-singularity-api-access-requirements>)