NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

File Threat Analysis API

www.netclean.com

NetClean.

Table of contents

Introduction

The **ProActive File Threat Analysis API** is a service available on the NetClean ProActive Cloud Threat Intelligence Platform. It enables security teams to automatically analyse file hashes against NetClean's intelligence database, providing zero-false-positive identification. At present, this intelligence is composed of files classified within the Child Sexual Abuse Material (CSAM) threat domain.

By embedding ProActive intelligence directly into monitoring, detection, and governance workflows, organizations can more effectively identify high-risk content. It adds a unique layer of threat analysis that enhances the current threat intelligence and complements traditional security tools. Designed for automated processing, the API supports decision-making wherever file hash intelligence contributes to early classification and risk assessment.

How it works

Collect: Gathering signals

Existing security tools capable of extracting file hashes, collect SHA-1 hashes from the IT environment (endpoints, DLP systems, forensic tools, cloud storage, etc.)

Detect: Identifying threats from signals

The ProActive File Threat Analysis API analyzes collected hashes against NetClean's intelligence database.

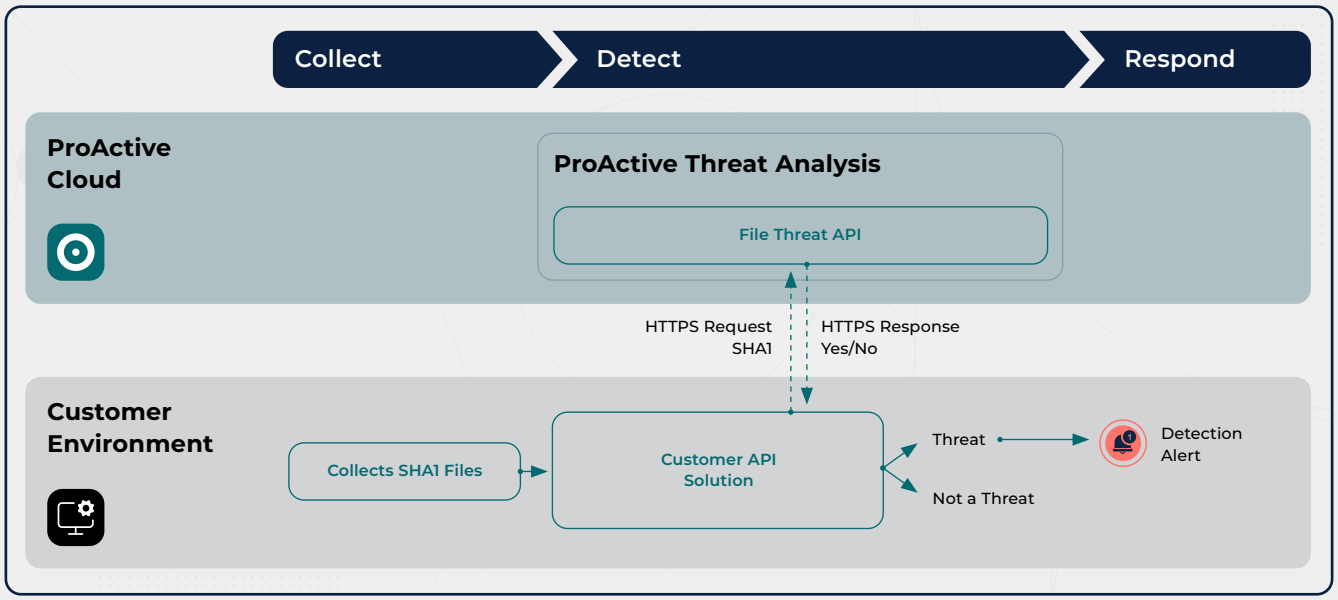
1. API Query: hashes are submitted to the API via secure HTTPS requests.

2.Response: the API returns a clear true/false response for each hash.

- True → Confirmed match with a hash in NetClean's database.
- False → No match in the database.

Respond: Acting on threats

Security teams can use the API's confirmed matches to trigger alerts, initiate investigations, log incidents, or automate response workflows.



How to access the service

Authentication setup details and API documentation for the ProActive File Threat Analysis API are available in the ProActive Cloud portal.

Integration with security ecosystem

The ProActive File Threat Analysis API is designed to fit naturally into your existing security processes:

- **SIEM/SOAR:** CSAM matches found by the API can be integrated as high-confidence detection events, not just generic log signals.
- **MDR/IR:** API alerts can be used to trigger structured investigations, containment, and escalation.
- **Compliance:** Policy enforcement and regulatory reporting can be supported with auditable evidence.

Value scenarios

The ProActive File Threat Analysis API is not intended to replace existing security platforms or function as a standalone solution. Instead, it serves as an integration-ready intelligence component that strengthens existing security, compliance, and operational workflows.

Monitoring & Detection Workflows (MDR, SOC, SIEM, SOAR)

The API enhances monitoring and detection workflows by providing automated intelligence on file hashes collected through continuous security telemetry. By confirming whether specific artifacts correspond to illicit or high-risk content, the API supports accurate early-stage event classification and improves the prioritization of alerts. This strengthens the ability of MDR, SOC, SIEM, and SOAR platforms to differentiate between routine technical events and signals with significant legal or reputational implications. The result is a more precise, efficient detection pipeline that improves downstream decision-making and accelerates incident handling when escalation is required.

Digital Storage & Content Moderation

The API provides storage platforms, collaboration tools, and content moderation systems with an automated mechanism for identifying high-risk content at scale. By screening file hashes during upload, synchronization, or periodic scanning, the API helps organizations prevent the storage or distribution of material that could expose them to legal, reputational, or operational consequences.

MSSPs & Multi-Tenant Security Services

The API allows Managed Security Service Providers to enhance their service offerings by integrating high-confidence file intelligence into multi-tenant monitoring and response workflows. This enables MSSPs to differentiate their services with advanced insider risk detection capabilities and deliver standardized, scalable playbooks for customers across diverse verticals. By embedding the API into their platforms, MSSPs can provide consistent, value-adding intelligence.