NetClean Threat Analysis – Cloud Software (SaaS)

Service Overview

NetClean Threat Analysis is a cloud-based software service delivered via API that enables organisations to analyse file hashes against NetClean's threat intelligence database. Delivered as licensed cloud software, the service allows automated identification of known high-risk files within security, monitoring, and governance workflows without requiring on-premise infrastructure.

The service is provided as part of the NetClean ProActive Cloud platform and supports automated, high-confidence classification of file hashes. At present, the intelligence dataset is focused on files associated with the Child Sexual Abuse Material (CSAM) threat domain, enabling zero-false-positive identification of known illicit content.

Platform Capabilities

- Cloud-hosted file threat intelligence accessed via secure API
- Automated analysis of file hashes against NetClean's intelligence database
- Deterministic true/false results indicating confirmed matches
- High-confidence identification of known high-risk content
- Designed for automated, large-scale processing
- Integration-ready for security, compliance, and governance use cases

File Threat Analysis & Intelligence

- Support for analysis of SHA-1 file hashes
- Hashes submitted to the service via secure HTTPS requests
- Each query returns a clear response indicating whether a match exists in the intelligence database
- Intelligence designed to complement existing threat detection and monitoring tools
- Supports early-stage classification and risk assessment within security workflows

User Access & Administration

- Access provided via API endpoints hosted within the NetClean ProActive Cloud
- Authentication and API configuration managed through the ProActive Cloud portal
- Administrative controls for managing API access and usage
- Designed for integration into existing tools rather than direct end-user interaction

Security & Compliance

- Secure API access using encrypted HTTPS communication
- Logical tenant separation within the cloud platform
- Controlled access to intelligence through authenticated API usage
- Supports UK GDPR-aligned data handling requirements
- No file content is transferred; analysis is performed using file hashes only

Support for Integrations & Extensions

- Designed to integrate with existing security tooling and workflows
- Suitable for use with SIEM, SOAR, MDR, incident response, and forensic platforms
- Supports enrichment of security events with high-confidence file intelligence

Development of bespoke integrations, automation, or response workflows is not included as part of the software licence and is delivered separately where required.

What the Software Enables

- Automated identification of known high-risk files within IT environments
- Improved prioritisation of security alerts and investigations
- Reduced false positives in content-related security monitoring
- Enhanced compliance and governance through auditable intelligence
- More efficient handling of sensitive or legally significant content risks

How the Software is used

NetClean Threat Analysis is used by organisations that require cloud-based access to file threat intelligence to support security monitoring, investigation, and compliance activities. File hashes extracted by existing tools are submitted to the API for analysis, and the resulting intelligence is used to inform alerting, investigation, and automated response workflows using licensed functionality appropriate to organisational needs.