NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

File Threat Analysis for Splunk

www.netclean.com

NetClean.

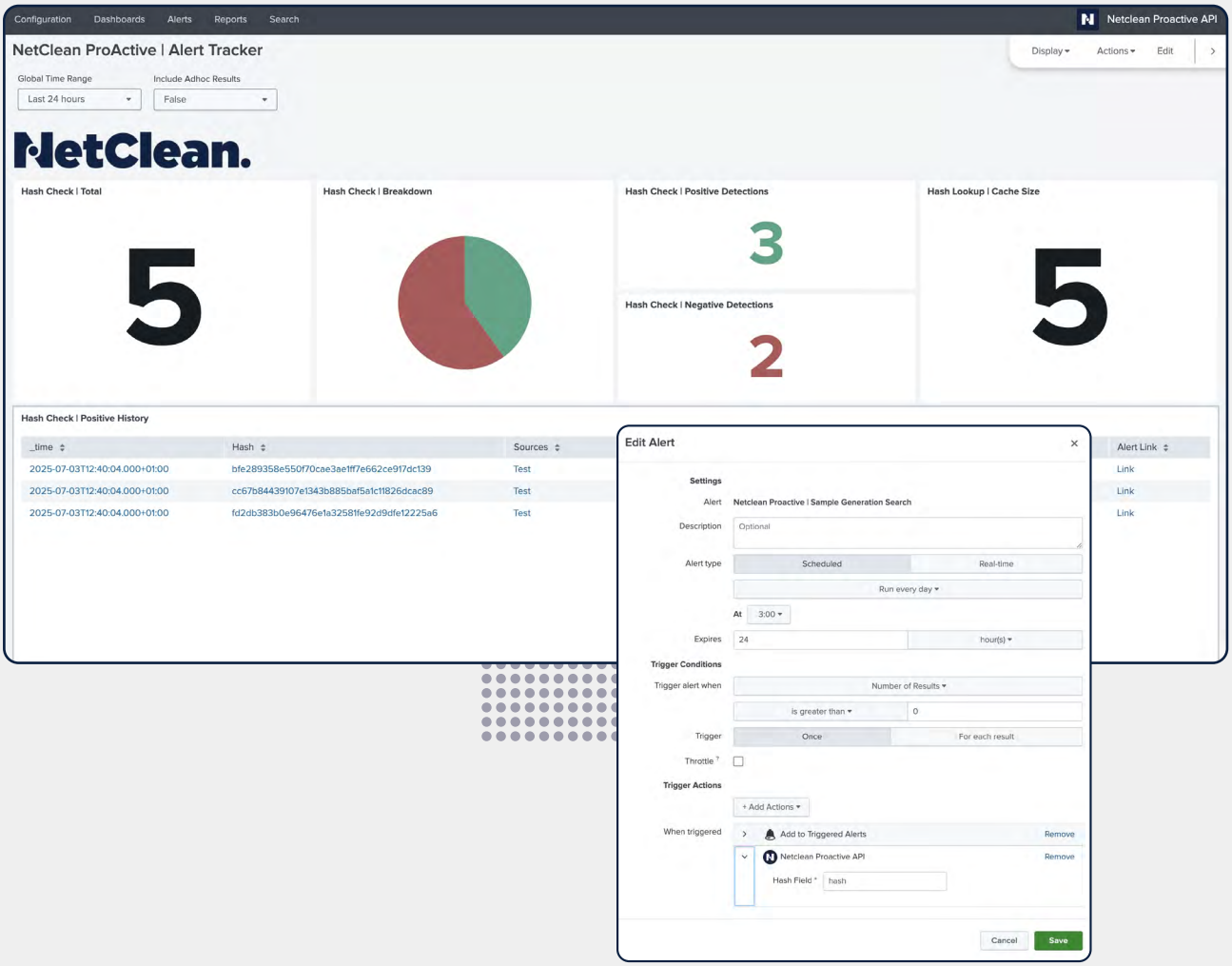
Table of contents

Introduction

ProActive File Threat Analysis for Splunk is a turnkey connector app that brings verified human insider risk detection directly into existing Splunk workflows. It enables security teams to automatically analyze file hashes against NetClean's intelligence database, using the ProActive File Threat Analysis API service. At present, this intelligence is composed of files classified within the Child Sexual Abuse Material (CSAM) threat domain.

NetClean's ProActive File Threat Analysis API is a service available on the NetClean ProActive Cloud Threat Intelligence Platform, providing zero-false-positive identification of high-risk content.

With minimal setup, the Splunk connector app enable organizations to strengthen investigations and enhance visibility to insider-risk without altering established workflows - all within familiar Splunk dashboards, alerts, and searches.



How it works

Collect: Gathering signals

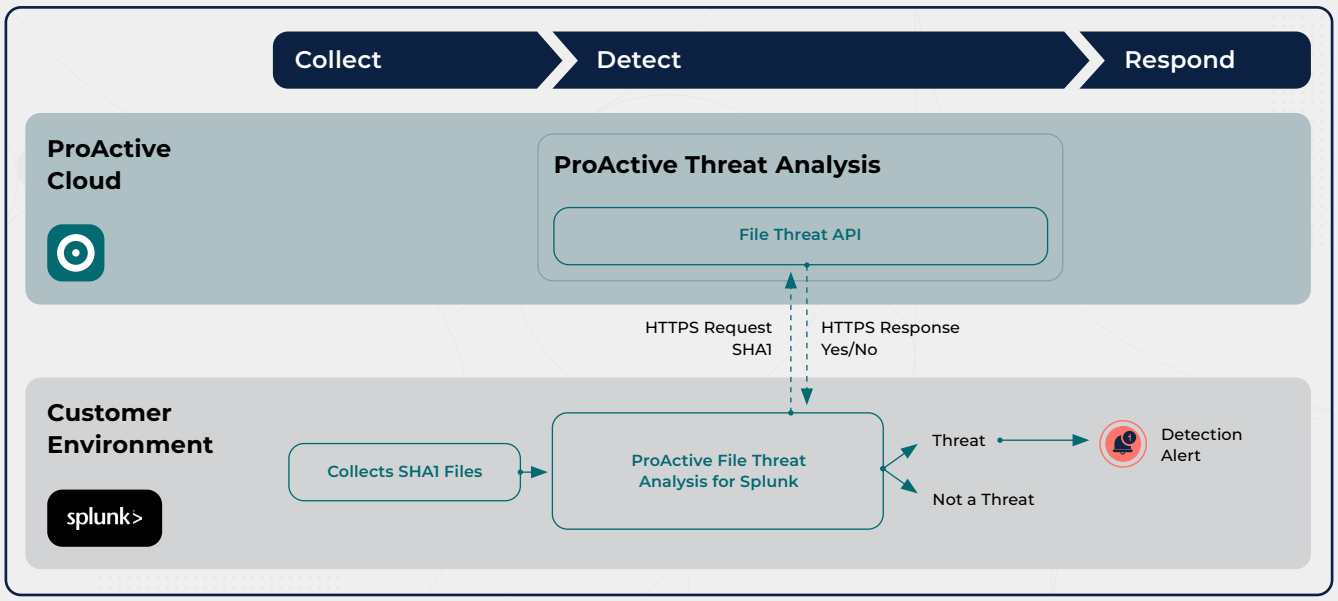
Splunk searches (scheduled or real-time) or other existing security tools identifies SHA-1 hashes from endpoint logs, file scans, or DLP systems.

Detect: Identifying threats from signals

The Splunk connector app automatically queries the ProActive File Threat Analysis API with scheduled or real-time hash batches. The API returns a simple true/false result for known CSAM, which is then appended to the corresponding Splunk events. There are no false positives – a “true” response is a verified, high-priority security event.

Respond: Acting on threats

Splunk dashboards and alerts that trigger automated playbooks can enable security teams to investigate, escalate, and remediate CSAM incidents if such content is identified. Any such identification should be treated as a high-risk security incident.



How to set up the service

Prerequisites:

- Splunk Enterprise (on-prem), Splunk Cloud or Splunk versions 9.x.
- Collected SHA-1 file hashes.
- Ability to install and configure Splunk add-ons.

The following setup steps are typically completed in under 30 minutes. See all installation and configuration details in Splunkbase.

- Install the app ProActive Threat Analysis from Splunkbase.
- Configure API credentials. Authentication setup details and API documentation are available in the ProActive Cloud portal, in section ProActive File Threat Analysis API.
- Create a Splunk index to store results.
- Enable the built-in alert in Splunk to receive email notifications when a hash is identified as a CSAM classified file.
- Customize alert actions to fit your organization's workflow — such as triggering investigations, creating tickets, or integrating with SOAR tools.

Value scenarios

The ProActive File Threat Analysis for Splunk add-on enriches existing Splunk searches, dashboards, and alerts with verified insights on file hashes collected from the IT environment. Integrated directly into Splunk ingestion and correlation workflows, the add-on enables organizations to automatically detect known high-risk content and operationalize insider-risk signals through established SIEM processes.

Detection & Alerting in Splunk Correlation Searches

The add-on enhances Splunk's correlation searches by appending high-confidence intelligence to events containing file hashes. This enables detection rules to classify events involving illicit or high-risk content as priority security incidents. As a result, Splunk Enterprise Security can escalate these events through risk-based alerting and adaptive response actions without additional configuration complexity.

Event Enrichment for Investigations & Incident Review

By enriching relevant events with the API response, the add-on supports Splunk's Incident Review and search workflows with authoritative, zero-false-positive indicators. This gives analysts immediate clarity when reviewing file-related activity, helping differentiate between routine technical events and those requiring legal, HR, or governance escalation.

Monitoring File Activity Across Endpoints, Servers, and Storage

When Splunk ingests file activity from endpoints, network shares, cloud storage, or collaboration tools, the add-on provides an automated mechanism to surface events involving high-risk files. This allows organizations to use Splunk as a central monitoring layer for prohibited content stored or accessed within the environment.