NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

Web Threat List

www.netclean.com

NetClean.

Table of contents

Introduction

The **ProActive Web Threat List** is a service within the NetClean ProActive Cloud Threat Intelligence Platform that provides a continuously updated set of verified web indicators. The service consists of domains and URLs associated with elevated human risk linked to the consumption of compromising online content that may increase coercion or exploitation risk.

The indicator set is designed to be integrated into existing security enforcement and monitoring architectures, where web access activity is already inspected and logged. By introducing externally validated indicators derived from verified sources, the service enables identification of high-risk web access patterns that are not typically covered by traditional malware, phishing, or network-centric threat intelligence.

The service supports detection and investigation of serious human-centric web threats without requiring additional data collection, user tracking, or changes to existing security architecture.

How it works

Collect: Gathering signals

Web access activity is already inspected as part of standard security enforcement and logging. Requests to domains and URLs are evaluated at policy enforcement points where outbound web traffic is controlled, and the resulting events are recorded with associated metadata.

Detect: Identifying threats from signals

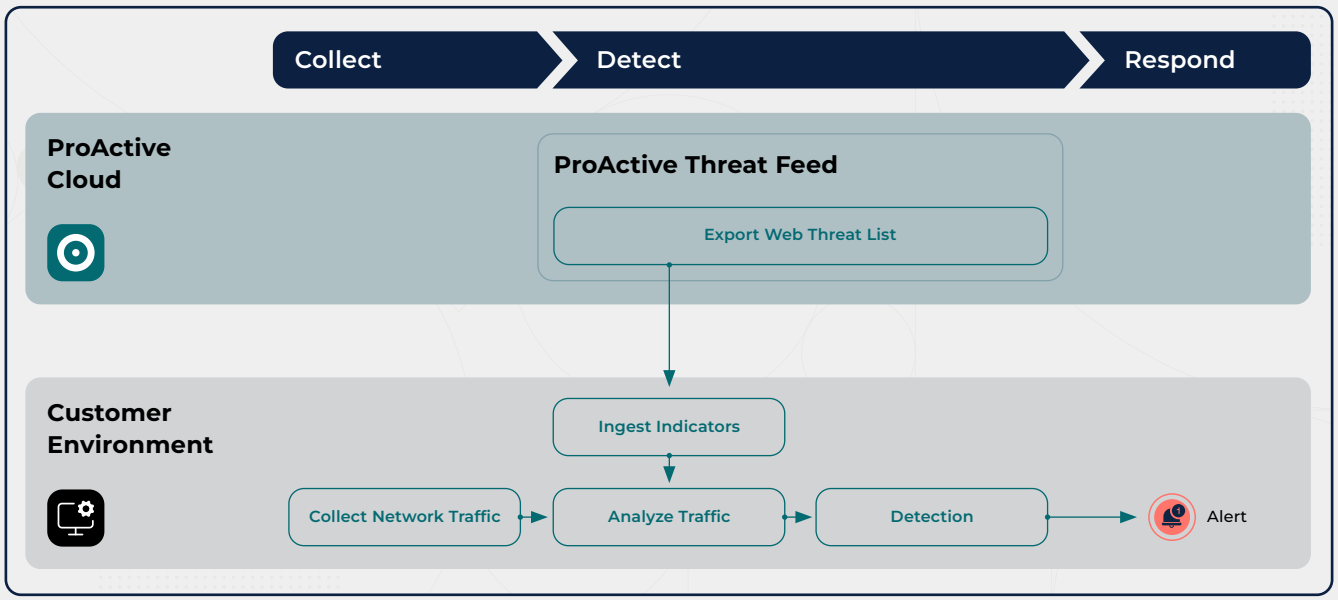
The ProActive Web Threat List provides a curated set of verified indicators consisting of domains and URLs associated with elevated human risk. Detection occurs by matching observed web access destinations against the indicators provided by the service.

The indicator set is distributed in a structured format suitable for integration with existing enforcement and monitoring functions, enabling access attempts to listed destinations to be identified during normal inspection and logging processes.

Respond: Acting on threats

When a match is identified, response actions are determined by existing security policies. Depending on configuration, responses may include logging, alerting, access restriction, or escalation to downstream investigation and response workflows accross the security stack..

Detected events can be forwarded to monitoring, analytics, or orchestration systems for correlation with other signals and further handling in accordance with organizational procedures.



NetClean.

How to access the service

The ProActive Web Threat List is made available through the NetClean ProActive Cloud portal. The service provides a downloadable CSV file containing the current set of verified web indicators.

The CSV file is updated on a continuous basis to reflect changes in the indicator set. Customers are responsible for retrieving the file and integrating it into their existing security enforcement, monitoring, or analysis workflows in accordance with their operational requirements.

Integration with security ecosystem

The ProActive Web Threat List is designed for integration across modern security architectures, including SASE-based environments and hybrid deployments. This includes both cloud-based SASE platforms and traditional security controls that perform equivalent enforcement, inspection, or logging functions.

The indicator set can be applied at multiple functional layers where web access activity is inspected, logged, or controlled:

- **Policy enforcement and web access control**
  Access attempts to domains or URLs included in the indicator set can be identified during web inspection and evaluated against existing security policies. Resulting actions are determined by policy and configuration and may include logging, alerting, or access restriction.
- **Name resolution and DNS inspection**
  DNS queries can be evaluated against the indicator set to identify resolution attempts to listed domains as part of standard DNS inspection and logging processes.
- **Monitoring and analytics**
  Events associated with matches can be forwarded to monitoring and analytics platforms for correlation with identity, device, session context, and other security signals.
- **Endpoint and network telemetry**
  Web access events observed at the endpoint or network level can be compared against the indicator set to support broader detection, investigation, and attribution workflows.
- **Orchestration and response**
  Matches can be used as inputs to orchestration and response workflows, enabling consistent handling in accordance with organizational policies and procedures.