SentinelOne

Purple^ai

Your AI security analyst to detect earlier, respond faster, and stay ahead of attacks

Today's security teams are dealing with a sophisticated threat landscape and endless alert queues that grow far faster than what teams can even hope to resolve. It's labor-intensive, precludes any proactive threat hunting, and leads to burnout and missed alerts.

Purple AI is the industry's most advanced AI security analyst that translates natural language into structured queries, summarizes event logs and indicators, guides analysts of all levels through complex investigations with recommended next questions and auto-generated summary emails, and scales collaboration with shared investigation notebooks—ensuring rapid detection, investigation, and response.

Unlike other solutions that act as a console chat bot, Purple AI is a force multiplier that helps analysts conduct faster, better investigations with:

+ **One-click threat hunting quickstarts** based on the latest threat intelligence
+ **Intelligent suggested next queries** to continue your hunt
+ **Lightning fast queries and visibility** of native and third party data in a single view
+ **Shared investigation notebooks** to collaborate across teams
+ **Direct answers to SentinelOne support questions** so you don't have to search online documentation

Unlock Your Security Team's Full Potential

Simplify the Complex

Streamline investigations by intelligently combining common tools, synthesizing threat intelligence and contextual insights into a single conversational user experience.

Uplevel Every Analyst

Find hidden risk, conduct deeper investigations, and respond faster—all in natural language. Train analysts with power query translations from natural language prompts.

Take Hunts from Hours to Minutes

Accelerate SecOps with our patent-pending hunting quick starts, AI-powered analyses, auto-summaries, and suggested queries. Save time by seamlessly collaborating on investigations in saved and shareable notebooks.

Safeguard Your Data

Leverage a solution designed for data protection and privacy by design. Purple AI is never trained with customer data and is architected with the highest level of safeguards.

The Purple AI Difference

+80%

Faster threat hunting & investigations as reported by early adopters

Speed & Visibility with One Console, Platform, & Data Lake

Accelerate operations and see the full picture more clearly with one console, one platform, and the industry's most performant data lake. Purple AI is the only AI analyst that understands OCSF logs—so you can instantly query native and partner data in a single normalized view.

Threat Hunting Quickstarts & Guided Investigations

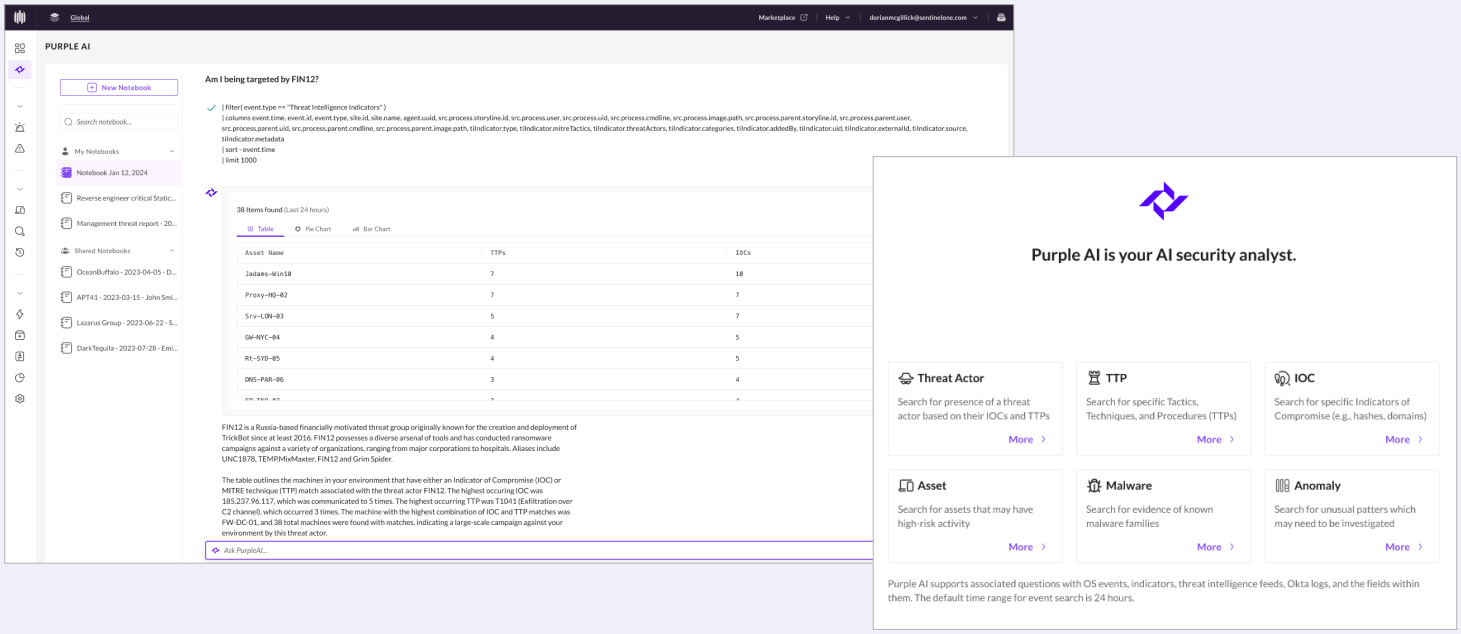
Help every analyst reduce MTTD and proactively find risk with our patent-pending hunting quick starts library. Leverage intelligent, contextually-suggested next queries to continue investigations in natural language.

Accelerate Collaboration Across the Board

Auto-generate threat summaries, reports, and communications that can be shared across teams and cut down on unnecessary back and forth by collaborating in saved, shared, and editable notebooks.

Open & Reliable AI

AI shouldn't be a black box. With Purple AI, you can easily view query translations for verification and analyst training. Purple AI is also carefully architected with guardrails that protect against misuse and hallucinations.



Key Features

- Translate natural language into structured PowerQueries to search for hidden risk. Get outcomes you can trust with full views of queries and summarized results in natural language.
- Lightning fast queries and greater visibility. Built on top of the Singularity Data Lake, Purple AI is the only GenAI analyst that supports the Open CyberSecurity Schema Framework (OCSF) to provide native and third party data in a single normalized view.
- Patent-Pending Threat Hunting Quickstarts enable analysts to proactively hunt for threats with a single click, using pre-populated queries based on our leading threat intelligence.
- Conduct deeper investigations with suggested, contextual follow-on queries.
- Surface actionable insights faster with AI-powered threat analyses and summaries.
- Refer back to auto-saved private investigations notebooks or boost collaboration on hunts across teams in shared notebooks.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATTACK Evaluation

+ 100% Protection. 100% Detection
+ Top Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733

© SentinelOne 2024