



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.

Am I being targeted by FIN12?

Filter: (event.type == "Threat Intelligence Indicators")

[columns: event.time, event.id, event.type, site.id, site.name, agent.uuid, src.process.storyline.id, src.process.user, src.process.uuid, src.process.cmdline, src.process.image.path, src.process.parent.storyline.id, src.process.parent.user, src.process.parent.uuid, src.process.parent.cmdline, src.process.parent.image.path, t.indicator.type, t.indicator.mitreTactics, t.indicator.threatActors, t.indicator.categories, t.indicator.addressBy, t.indicator.uuid, t.indicator.externalId, t.indicator.source, t.indicator.metadata]

sort: -event.time  
limit: 1000

28 Items found (Last 24 hours)

Asset Name	TPPs	IOCs
Jadans-Win18	7	18
Proxy-HQ-02	7	7
Srv-LDN-03	5	7
GW-NYC-04	4	5
RI-SYD-05	4	5
DNS-PAR-06	3	4
...	...	...

FIN12 is a Russia-based financially motivated threat group originally known for the creation and deployment of TrickBot since at least 2016. FIN12 possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. Aliases include UNC2458, TEMP/BlackKerber, FIN12 and Grim Spider.

The table outlines the machines in your environment that have either an Indicator of Compromise (IOC) or MITRE technique (TTP) match associated with the threat actor FIN12. The highest occurring IOC was 185.237.96.117, which was communicated to 5 times. The highest occurring TTP was T1041 (Exfiltration over C2 channel), which occurred 3 times. The machine with the highest combination of IOC and TTP matches was FW-DC-01, and 28 total machines were found with matches, indicating a large-scale campaign against your environment by this threat actor.

Ask PurpleAI...

**Purple AI is your AI security analyst.**

**Threat Actor**

Search for presence of a threat actor based on their IOCs and TPPs

[More >](#)

**TTP**

Search for specific Tactics, Techniques, and Procedures (TPPs)

[More >](#)

**IOC**

Search for specific Indicators of Compromise (e.g., hashes, domains)

[More >](#)

**Asset**

Search for assets that may have high-risk activity

[More >](#)

**Malware**

Search for evidence of known malware families

[More >](#)

**Anomaly**

Search for unusual patterns which may need to be investigated

[More >](#)

Purple AI supports associated questions with OS events, indicators, threat intelligence feeds, Okta logs, and the fields within them. The default time range for event search is 24 hours.

## Key Features

<p>✔ 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.</p>	<p>✔ 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.</p>	<p>✔ 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.</p>
<p>✔ Conduct deeper investigations with suggested, contextual follow-on queries.</p>	<p>✔ Surface actionable insights faster with AI-powered threat analyses and summaries.</p>	<p>✔ Refer back to auto-saved private investigations notebooks or boost collaboration on hunts across teams in shared notebooks.</p>

## Innovative. Trusted. Recognized.



A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms



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



96% of Gartner Peer Insights™  
EDR Reviewers Recommend  
SentinelOne Singularity



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