



Purple AI™

Detect earlier, respond faster, and stay ahead of attacks with the world's most advanced AI security analyst

Modern security operations push defenders beyond human limits. The velocity and scale of today's attacks force teams to operate in environments they simply cannot manage with legacy technology, leading to critical coverage gaps and widespread burnout. Purple AI drives a fundamental shift in the SOC operating model, giving defenders the advantage of speed, skill and scale. Stop fighting the broken workflows and endless tool pivoting. Start fighting the adversary.

Purple AI is the industry's leading agentic AI security analyst. A powerful force multiplier drawing on frontline MDR intelligence, it uses reasoning AI to autonomously hunt, triage, and investigate alerts, delivering clear, explainable verdicts. It offloads manual data collection and reasoning, dramatically increasing analyst bandwidth so your team can clear backlogs and outmaneuver modern adversaries.



Simplify the Complex

Purple AI turns fragmented, high-volume security data into instant insight and action. Secure the broadest visibility across native and third-party data while AI agents analyze threats, prioritize alerts, and surface critical issues. Eliminate advanced query barriers so analysts can focus entirely on defeating the adversary.



Amplify Every Analyst

Maximize your team's impact by offloading manual, repetitive tasks to agentic workflows. Drawing on frontline MDR expertise, Purple AI scales elite human knowledge across your entire team. Elevate your SecOps team to operate beyond human limits.



Accelerate Security Operations

Move beyond rigid playbooks to dynamic, context-aware analysis. Purple AI translates investigations into actionable response recommendations, seamlessly triggering automated workflows to help teams resolve threats 55% faster.



Embrace Autonomy Responsibly

Your security and privacy are protected by design. Purple AI is advanced AI with responsible, secure foundations—architected with the highest level of safeguards. Maintain absolute control over automated responses using strict analyst-in-the-loop governance.

The Purple AI Advantage¹

63%

Faster to identify security threats

55%

Faster to remediate security threats

338% Return on Investment

Gartner.
Peer Insights.



This product is truly bleeding edge technology that pairs with our security stack to provide the best SOC efficacy and productivity.



IT Security & Risk Management
ENERGY AND UTILITIES

¹IDC, Business Value of SentinelOne Purple AI (April 2025)

Global / Account / Site
Cloud Native Security | Marketplace | Help |

- Dashboards
- Purple AI
- Triage
 - Alerts**
 - Incidents
 - Attack Paths
 - Misconfigurations
 - Vulnerabilities
 - Compliance
- Discover
 - Event Search
 - Inventory
 - Graph Explorer
 - Activities
- Automate
 - Hyperautomation
 - RemoteOps
- Configure
 - Detections
 - Agent Management
 - Reports
 - Policy & Settings

Alerts

All Endpoint Custom alerts Identity Cloud Partner alerts

Load filter Property name contains Search Last 30 days Alert status Severity Mitigate

Mitigate Actions Group by Select 134 items

Alert name	Severity	Auto-investigation	Mitigation status
apollo.exe detected as Ransomware	High	Complete View	Unmitigated
Ramnit Command and Control Traffic Detection	Critical	Investigate	Unmitigated
Backdoor/MSIL.bladabind.luze	Medium	Complete View	Mitigated
WRBrDa.exe detected as Malware	High	Complete View	Unmitigated
::1 (STARFLEET\jeanluc) - Lateral movement: Ra...	Low	Investigate	Mitigated
PolicyUpdate.exe detected as Malware	High	Complete View	Unmitigated
openssl - Ransomware Marker detected	Critical	Complete View	Unmitigated
Unauthorized Credential Access Detected	Critical	Investigate	Unmitigated
AD Privilege Group Enumeration Detected	Critical	Investigate	Unmitigated
9672B0.exe detected as Ransomware	Critical	Complete View	Unmitigated
bdata.bin detected as Malware	Critical	Complete View	Unmitigated
sbsimulation_sb_55501_bs_38888_gold.exe - Ma...	Critical	Investigate	Unmitigated
bdata.bin detected as Malware	Critical	Investigate	Unmitigated
Domain Controller Discovery Detected	Critical	Investigate	Unmitigated
sbsimulation_sb_55744_bs_38989_gold.exe - Ma...	Critical	Investigate	Unmitigated
Backdoor/MSIL.bladabind.luze	Critical	Investigate	Unmitigated
7z.exe detected as Malware	Critical	Investigate	Unmitigated

mimikatz.exe detected as Infostealer

Purple AI Verdict: True Positive Oct 1, 2026 06:38 AM [Open alert](#) [Copy report](#)

Was this report helpful?

Executive Summary

SentinelOne CWS generated a HIGH-severity alert for mimikatz.exe detected as an Infostealer on host srv-app-01(10.10.45.23,AWS EC2 us-east-2) at 2026-02-17T17:31:57Z.

Investigation confirms execution of a signed Mimikatz binary (SHA1: ab12cd34ef56ab78cd9bef12ab34cd56ef78ab98, SHA256: 9f8e7d6c5b4a3210fedcba9876543210abcdef1234567890fedcba9876543210) via PowerShell by Domain Admin STARFLEET\jeanluc, with commands explicitly dumping Kerberos tickets.

This activity is assessed as a TRUE POSITIVE credential theft attempt with high impact potential, despite limited confirmation of successful data exfiltration.

Table of Contents

- Key Findings
- Threat Summary
- Verdict
- Timeline
- Recommended Next Steps
- Final Assessment

Key Findings

Alert & Host Context

- Alert ID: abc1234-5678-90ef-gh12-ijklmnopqrst
- Name: "credtool.exe detected as Infostealer"
- Severity: HIGH
- Classification: INFO_STEALER
- Confidence: MALICIOUS
- Result: UNMITIGATED

Key Differentiators

✔ Embedded Expertise

Harnesthecollectiveexpertise of SentinelOne's global analyst community to remove triage silos and accelerate MTTR.

- Human-Level Reasoning

Advanced agentic reasoning capabilities that mimic the thought process of a skilled SOC analyst.

- ✔ Unrivalled Architecture and Speed

Seamless search across native and 3rd party data,
powered by the industry's fastest data lake—
5-10x faster than legacy SIEMs.

✔ Security and Privacy by Design

Purple AI's advanced AI with responsible, secure foundations—architected with the highest level of safeguards.

- ✔ Seamless SecOps Workspace

A dedicated AI workbench with shared or private notebooks that auto-save and maintain full investigation context.

✔ Self-Documenting Notebooks

Create auditable, self-documenting investigation reports with multi-lingual support.

👉 Open Framework for Agentic Security

Purple AIMCP Serverempowers youto buildand
deploy custom AI agents with any LLM, powered
by the Singularity Platform.

- ✔ Human-in-the-Loop Governance

Responses execute only within your pre-approved policies or explicit authorization. Every action is predictable and auditable.