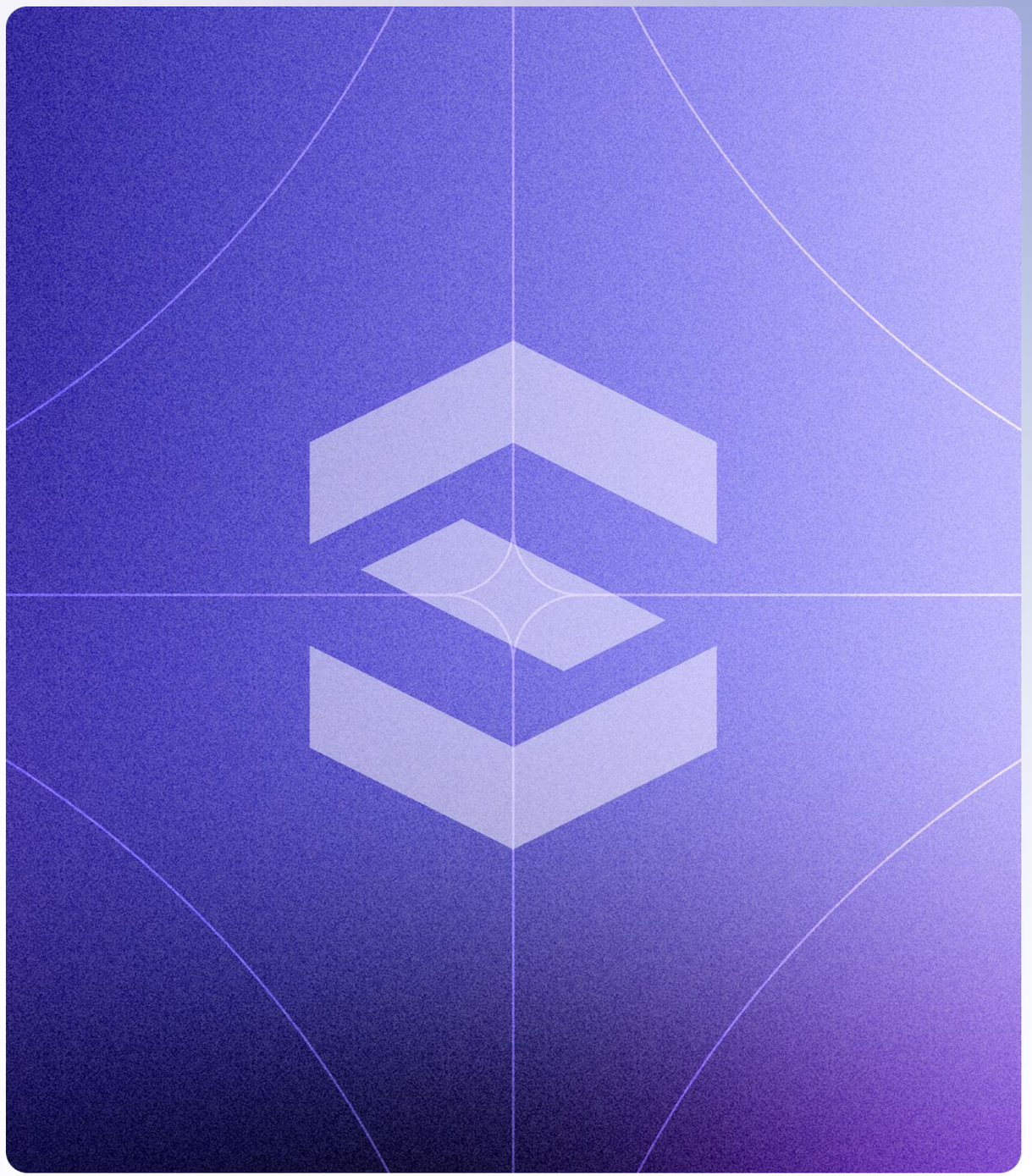
Singularity AI SIEM

Name Goes Here

Title goes here

SentinelOne



Presentation Agenda

- Complex Cyber Security Landscape and Challenges
- Introducing Singularity AI SIEM
- Unmatched Data Accessibility at Scale and Speed
- Adaptable, autonomous real-time operations
- Unlock Your Security Team’s Full Potential

Complexity of Cyber Security: More than Threats

THREATS

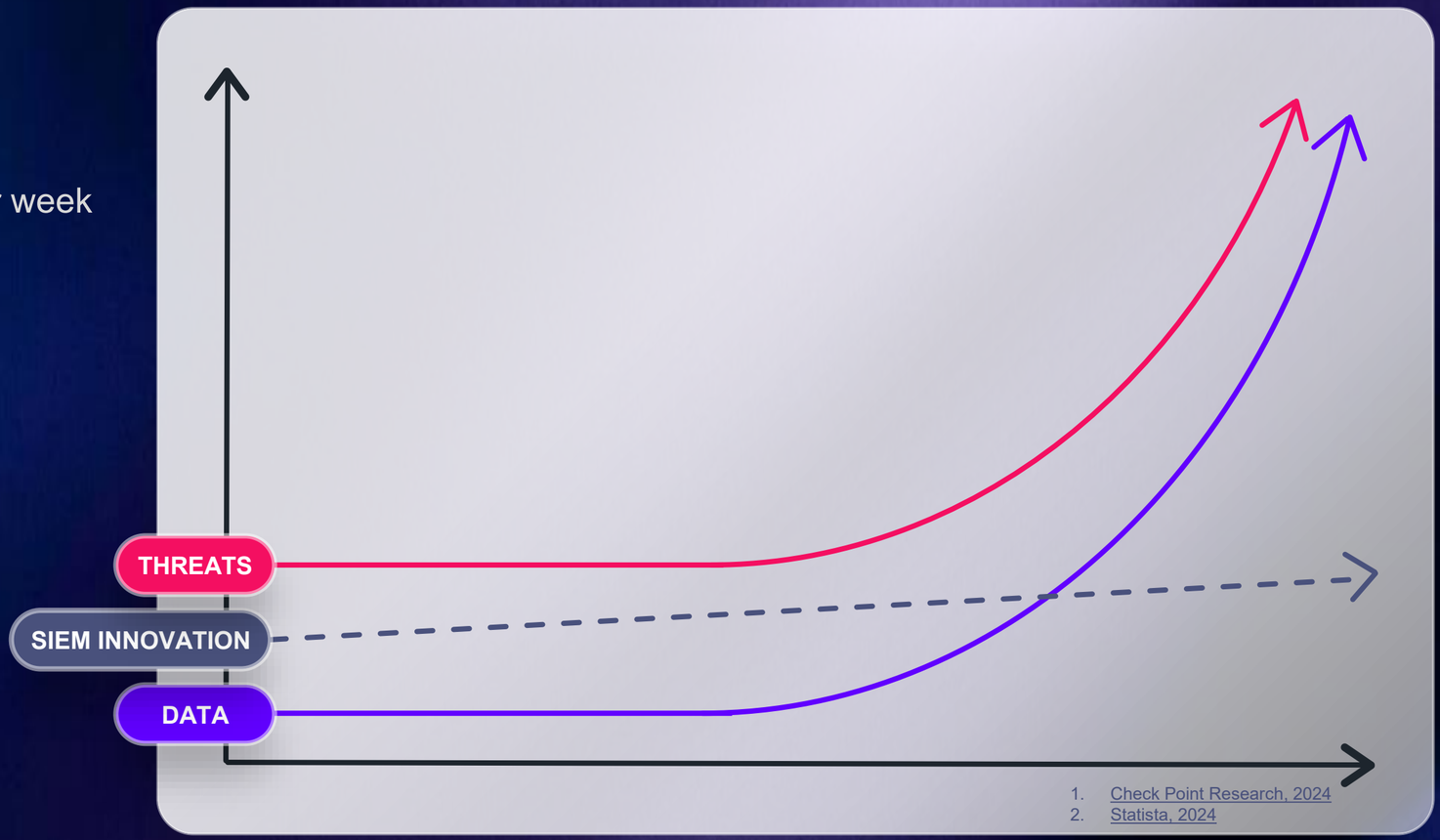
30% YoY increase in attacks[1]
1,636 attacks per organization per week

DATA

Global datasphere projected to grow more than **394 zettabytes** by 2028

SIEM Innovation

Stagnant growth.
Failed adaptations.



1. Check Point Research, 2024
2. Statista, 2024

20 Years: Same Technology. Same Challenges.

Overwhelmed by excessive alerts

Vulnerable to threats

Bogged down by manual investigations

Business disruption

Restrained by budget limitations

Limited visibility

Concerned over data retention

Potential fines or penalties

Uplevel your SOC Regardless of the Landscape

Boost Cyber Resilience

Access all your data without sacrificing performance or risk

Improve Security Posture

Limit blind spots by easily integrating all data sources

Increase SOC Efficiency

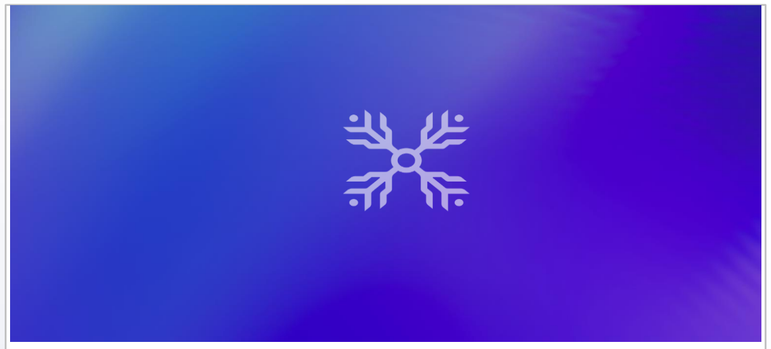
Reduce false positives and remedial work

Maintain Compliance

Break down data silos for complete visibility

SentinelOne Advantage for Singularity AI SIEM

Turning petabytes of telemetry into millisecond outcomes.

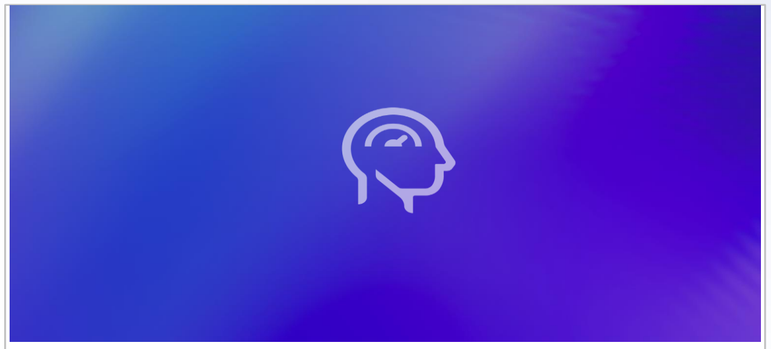


Autonomous Security

AI-Native Protection Across the Enterprise

Human Amplification

AI That Elevates and Empowers Teams

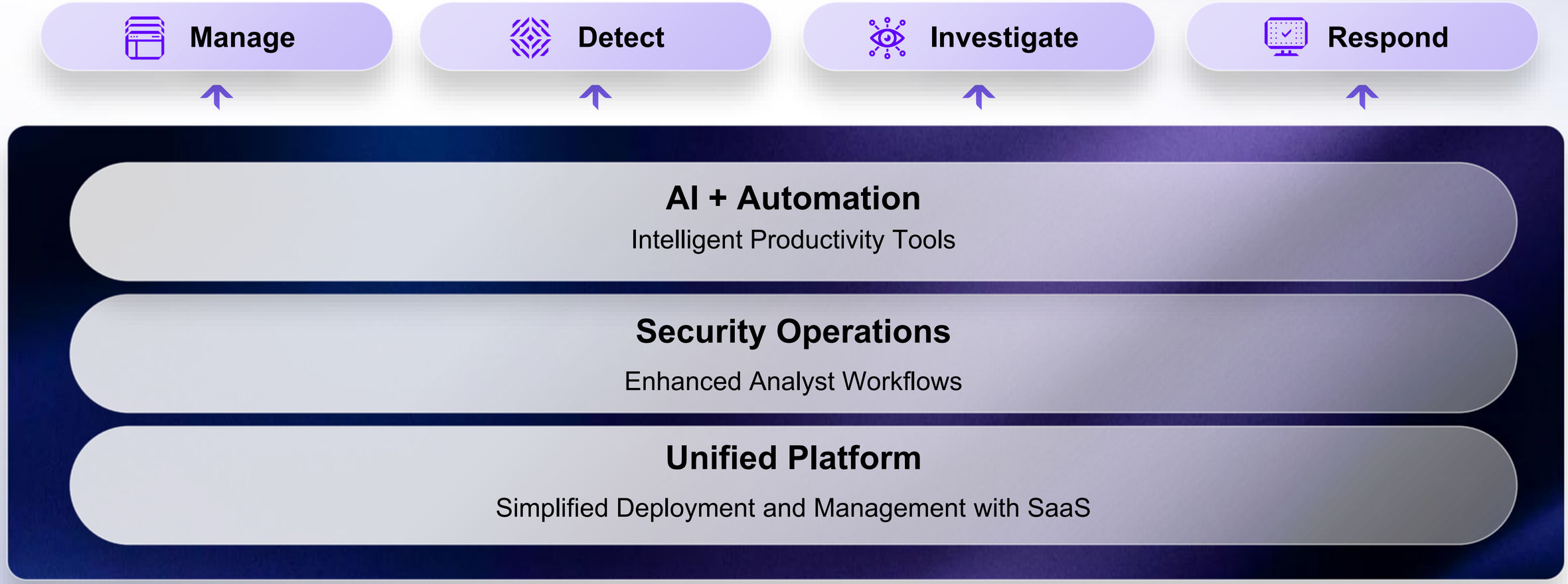


Intuitive By Design

Designed to Elevate Analyst Effectiveness

Introducing Singularity AI SIEM

The Industry's Fastest AI-Powered Open SIEM for All Your Data and Workflows



Why Singularity AI SIEM?

Modern Architecture. Operational Autonomy. Intelligent Tools.

Get complete visibility with unmatched data accessibility

Prevent downtime with adaptable, autonomous real-time operations

Supercharge analysts' productivity with intelligent tools

Revolutionizing Threat Detection with Modern Architecture

AI SIEM: Central to the Autonomous SOC

LEVEL 0
Manual

- Simple, single source detection logic
- Manual investigation, response, and remediation

LEVEL 1
Rules-Based

- Multi-source correlation rules for detections
- Expert systems (e.g., SOAR) for investigation, response, and remediation

Legacy SIEM

LEVEL 2
AI-Assisted

- ML algorithms that self-tune for better detections
- AI assistants to simplify and streamline detection engineering, investigation, response, and remediation

Next-Gen SIEM

Today

LEVEL 3
Partial Autonomy

- LLM-based detections that predict new attacks and create detection logic for them
- Agentic approaches for investigation and lower risk response actions
- AI suggests remediation strategies for high-risk situations, leaving final decisions and strategy to humans

AI SIEM

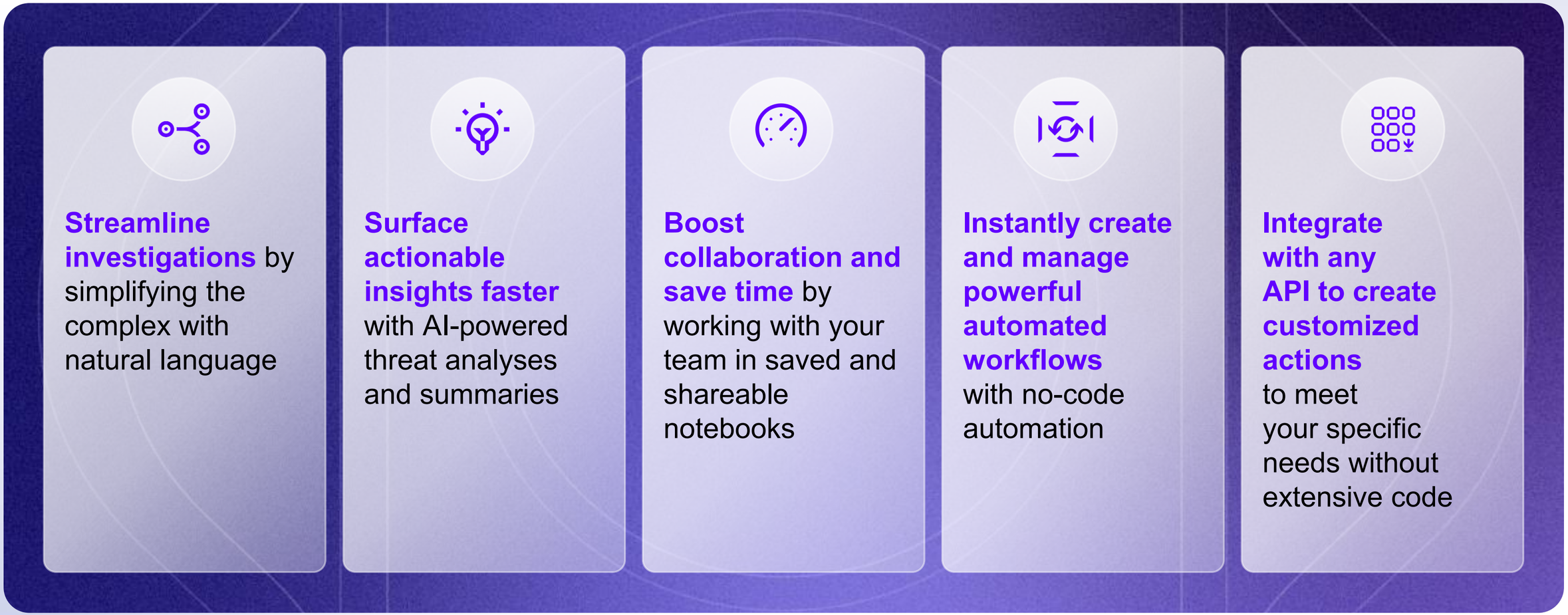
Next

LEVEL 4
High-autonomy

- Agentic approaches for most if not all SOC processes, including remediation actions
- Human role is system guidance and improvement

SentinelOne’s Agentic AI

Even less experienced analysts can now confidently investigate and threat hunt



“I’ve got all of my logs in one central place. I have got the integration creating faster investigation where we can apply analytics and automation where we need it. SentinelOne’s ease required zero training for our team to pick up and use SentinelOne.”

John McLeod
Chief Information Security Officer

AI SIEM

Abacus Technology Corporation
United States
Enterprise

New Relic
United States
High Tech, Commercial

Relay Network
United States
SMB

Q2 Holdings
United States
Computer Software, Commercial

Aalberts N.V.
Netherlands
Manufacturing, Enterprise

Fluidra
Spain
Consumer Product Goods, Enterprise

Access Healthcare
India
Manufacturing, Health Care Providers & Services, Enterprise

BBVA Spain
Spain
Financial Services, Globals

Gartner®

Peer Insights™

5 stars in Security Information and Event Management

"We needed a low code/no code solution to automate some operational tasks and our response to incident. Not everyone in the team is a developer so this solution works perfectly for us."

April 15, 2025
Transportation, $3B-10B USD
IT Security & Risk

"SentinelOne Singularity Platform is a cutting-edge cybersecurity solution … It is a best choice for businesses who want to enhance their cybersecurity posture."

March 4, 2025
Services, $50M USD
IT Security & Risk

"Unified Endpoint and SIEM security, Great automation, Lightweight."

February 12, 2025
Banking, $50M-250M USD
Information Security Analyst

"User friendly interface with effective threat detection. Provide comprehensive visibility across their entire security environment."

February 11, 2025
IT Services, $50M USD
IT Associate

Singularity AI SIEM: The AI SIEM for the Autonomous SOC

Register

AI SIEM Office Hours | **Click here**

Explore

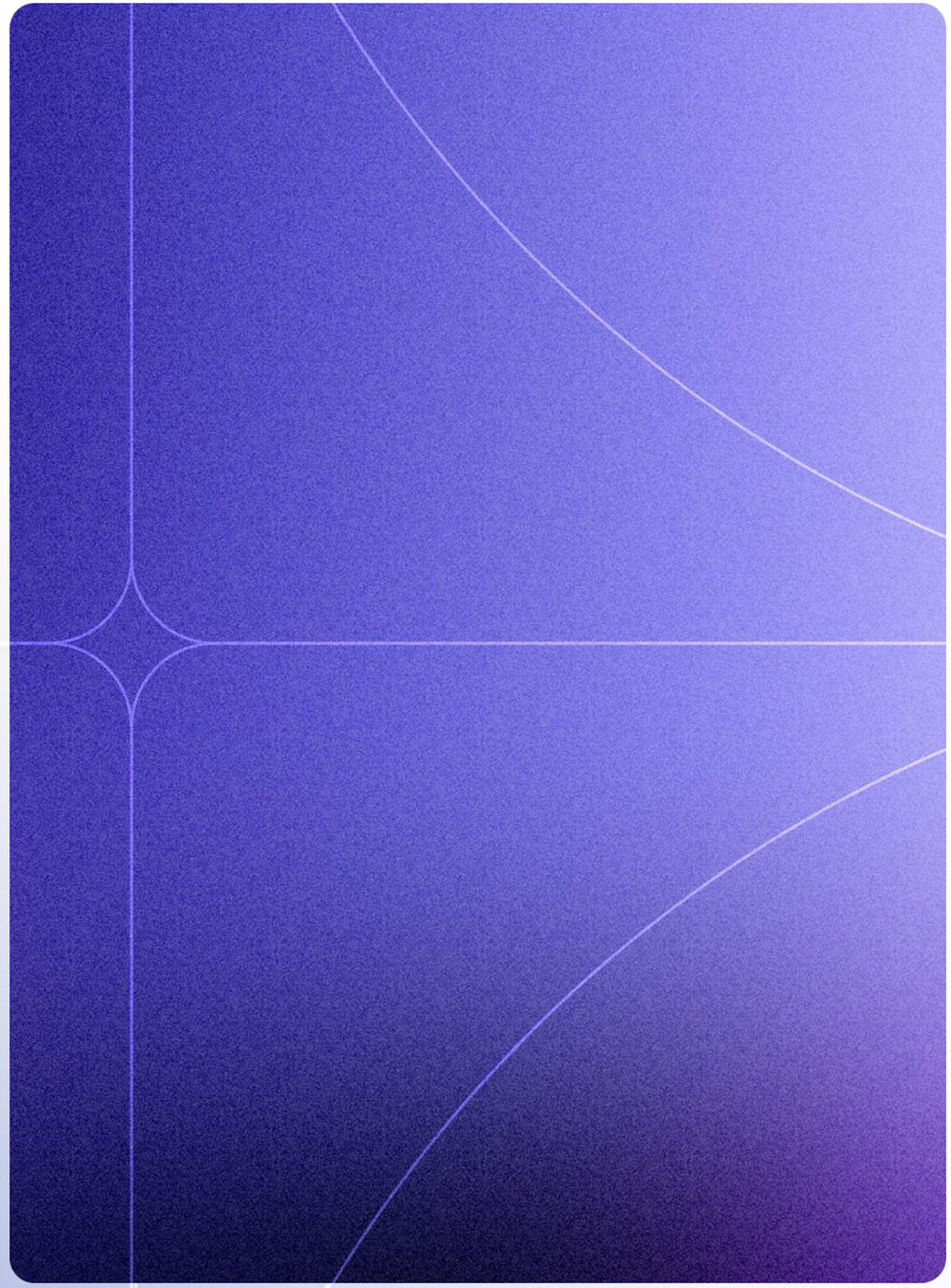
AI SIEM product page | **Click here**

Contact

Your SentinelOne Rep to schedule a deep dive

Discover

Read the datasheet | Click here



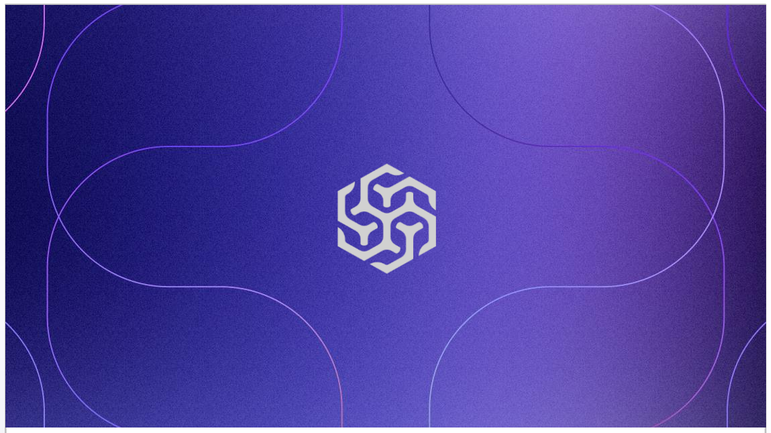
SentinelOne

Thank You

Sentinelone.com

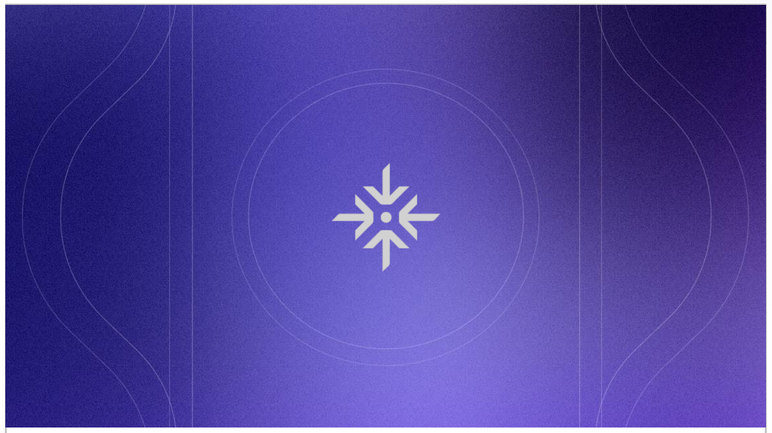

SentinelOne®

Powering Your Entire Security Ecosystem: SentinelOne's Broad Integration Network



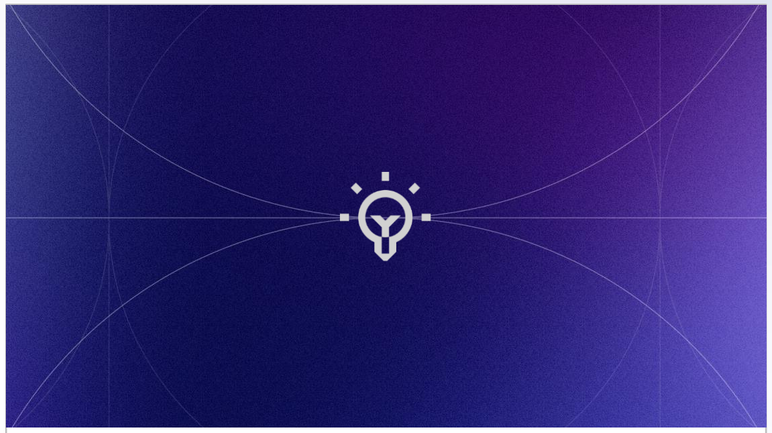
Unified Visibility & Context

Ingesting crucial data from across your diverse environment for a complete security picture.



Accelerated Detection & Response

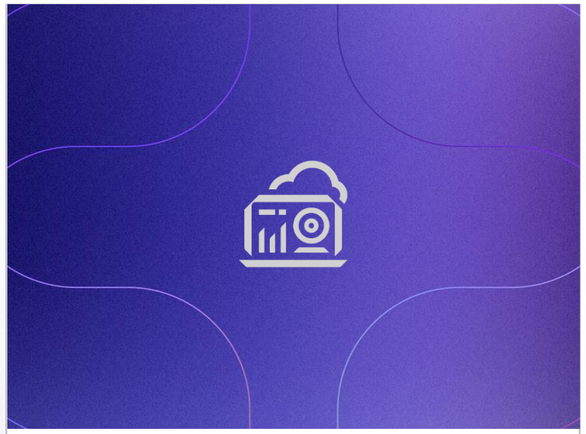
Enhancing threat insights and automating actions across your security stack.



Simplified Operations

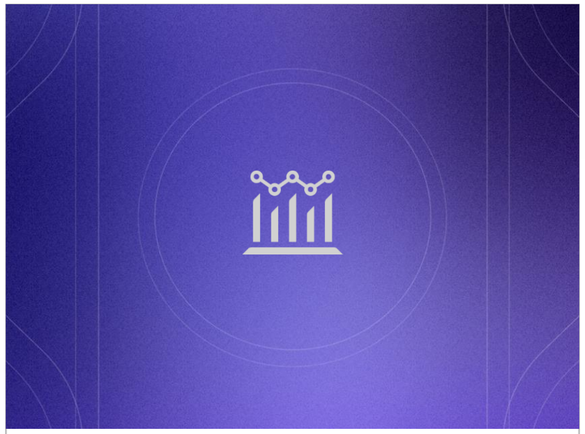
Leveraging existing investments and streamlining data flow for increased efficiency.

Key Integration Categories and Examples



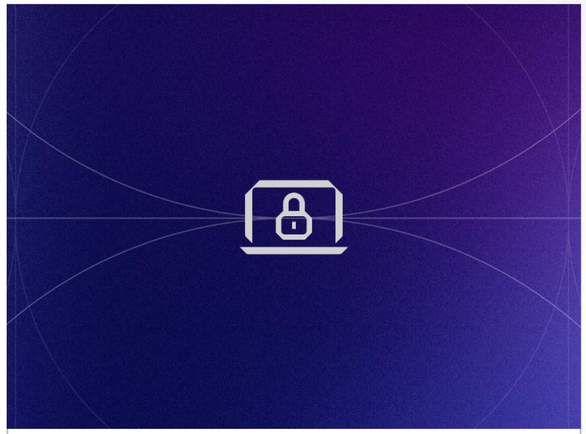
Cloud & Infrastructure

- **AWS:** CloudTrail, GuardDuty, VPC Flow, WAF, EKS
- **Microsoft Azure/365:** Azure Active Directory, Defender, Microsoft 365
- **Google Cloud:** GCP Audit, Workspace, Security Command Center
- **Container Security:** Kubernetes (EKS, Pods), Docker



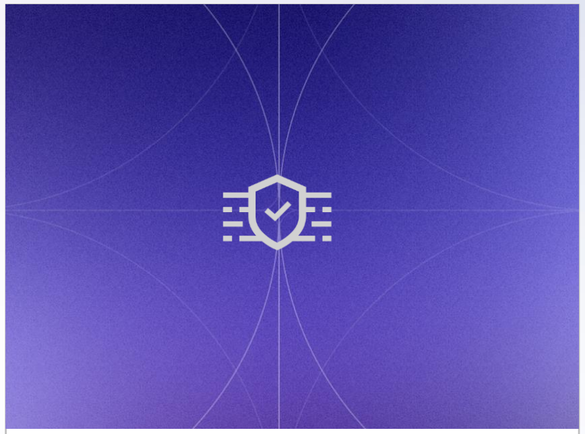
Network & Perimeter

- **Firewalls:** Palo Alto Networks, Check Point
- **DNS/Load Balancing:** AWS Route 53, Elastic Load Balancing
- **Secure Web Gateways:** Zscaler, Mimecast



Identity and Access Management

- **Microsoft Active Directory:** Azure AD
- **SSO/IAM:** Okta, Ping Identity, CyberArk
- **ZTNA:** Appgate SDP



Security and Threat Intelligence Tools

- **SIEM/XDR:** Splunk, QRadar, Palo Alto Networks Cortex XDR, Securonix
- **Vulnerability Management:** Tenable, Rapid7
- **Threat Intelligence:** Mandiant, Recorded Future, MISP, Intezer
- **Orchestration/SOAR:** Torq, Swimlane, Siemplify

AI SIEM Use Cases

Management & Ingestion
Ensure high-quality, reliable data access

Expand Visibility
Unlimited data ingestion. Rapid deployment and time-to-value.

Streamline Onboarding
Ingest first-party data, third-party data, structured and unstructured data with OCSF. Guided workflows and prebuilt connectors simplify integration

Acceptable Use Monitoring
Consistently enforced policies help maintain organizational standards

Automated Compliance Reporting
Support compliance workflows by generating reports on endpoint status, patch levels, and incident handling

Advanced Threat Detection
Catch what traditional SIEMs miss

Sophisticated Cyber Threats
Expanded visibility, context, and intelligence to identify threats (malware, data exfiltration, account takeover)

False Positive Reduction
Filter out noise by using STAR Cool Off Period

Proactive Investigation
Stay ahead of risks, prevent disruption

Complex Queries
Multi-tenancy architecture with massively parallel query engine breaks down complex queries (detect credential abuse, identify ransomware activity, monitor supply chain attacks)

Alert Enrichment
Purple AI provides alert summaries. HA enriches alerts with context from TI feeds, vulnerability data, and historical event logs.

Root Cause Analysis
Purple AI helps provide the origin and propagation of a threat across a network

Threat Hunting
Natural language queries, multi-language support, Quick Starts, and Self-documenting notebooks

Automated Response
Reduce manual repetitive tasks

Incident Response Automation
Automate workflows to execute incident response (isolate endpoints, disable accounts, kill processes, change permissions)

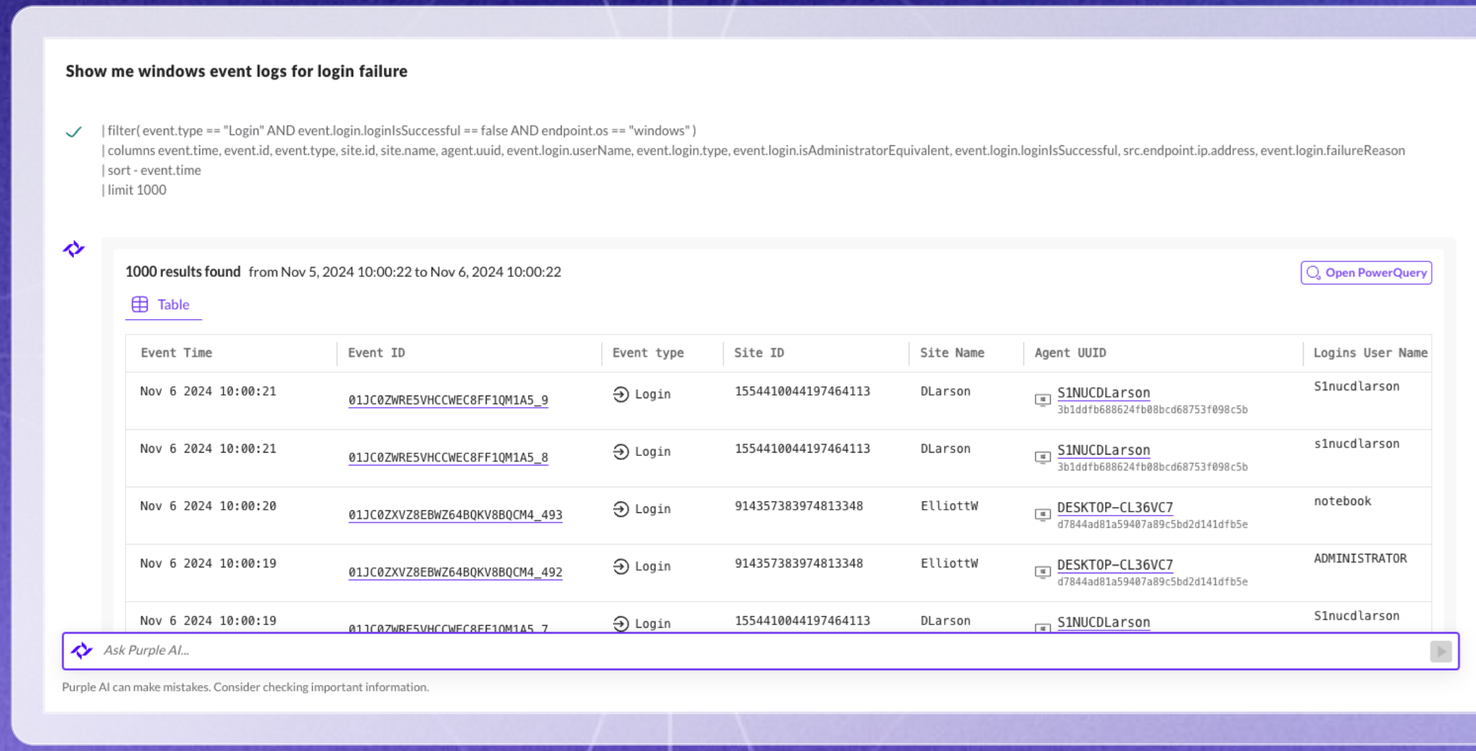
Remediation Orchestration
Suggested follow-ups and investigation notebooks

Upskilling Analysts
Step-by-step guidance and AI-suggested actions

Singularity™ AI SIEM

for Windows Event Logs & EDR Data

- Improve MTTR
- Minimize costs associated with deployment, management, and maintenance
- Minimize costs associated with storage and query



Singularity AI SIEM

Redefining SIEM with AI and Automation

Enterprise Visibility View everything and get deeper insights with limitless scalability and data retention

Real-time Detection Stay ahead of emerging risks with AI-driven detection and automated responses

Enhanced Productivity Empower analysts to investigate faster and optimize workflows with built-in AI and automation