



# Human Machine Teaming: Why the human element will always be indispensable in Cybersecurity.

**Martin Knopf**

Senior Systems Engineer, SentinelOne

---

Will robots take your job? Humans ignore the coming AI revolution at their peril.

**STEPHEN HAWKING WARNS**

**ARTIFICIAL INTELLIGENCE 'MAY**

**REPLACE HUMANS ALTOGETHER'**

**HUMAN VS AI**

**How will the Artificial intelligence replace workers?**

**Will AI replace Humans?**

This time, the robots really are coming.





A blue-tinted background image showing a robotic arm holding a microchip. The chip is a square component with a grid of gold pins, mounted on a metal fixture. The background is a blurred view of industrial machinery.

# Will Robots Replace Humans?



A photograph of two men in a dark, industrial setting. They are looking at a robotic arm that is positioned over a workbench. The scene is dimly lit, with blue and white tones. The men are wearing glasses and dark clothing. The robotic arm is blue and white. In the background, there are computer monitors and other equipment.

**Or Will Humans and Machines  
Create Greater Value Together?**





01

---

# Cybersecurity Challenges



# Complexity is the Enemy Of Security

- Anytime, Anywhere Computing
- Cloud – PaaS, SaaS, IaaS and FaaS
- Application Proliferation
- Pervasive Digitization
- Corporate Owned vs BYOD
- Endless Data Feeds



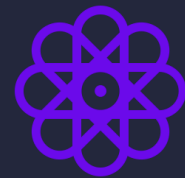
# Challenges We Hear From Customers



## Rapidly Expanding Attack Surfaces

Stealthy, advanced threats that continue to evade even the best defenses

---



## Complex Multi-Vendor Security Stack

Increasing level of complexity as vendor footprint expands without integrated workflows

---



## Manual Triage & Investigation

Disconnected, alert-centric tools with alerts that lack context and correlation

---



## Cybersecurity Skills Shortage

Lack of skilled SecOps practitioners with insufficient domain expertise

---



## Reactive Processes & Flows

Manual orchestration of responses that happen at individual control points and at human speed

---

**25-49**  
Tools

**10+**  
Vendors

**57%**

Customers claiming to  
be impacted by skills  
shortage

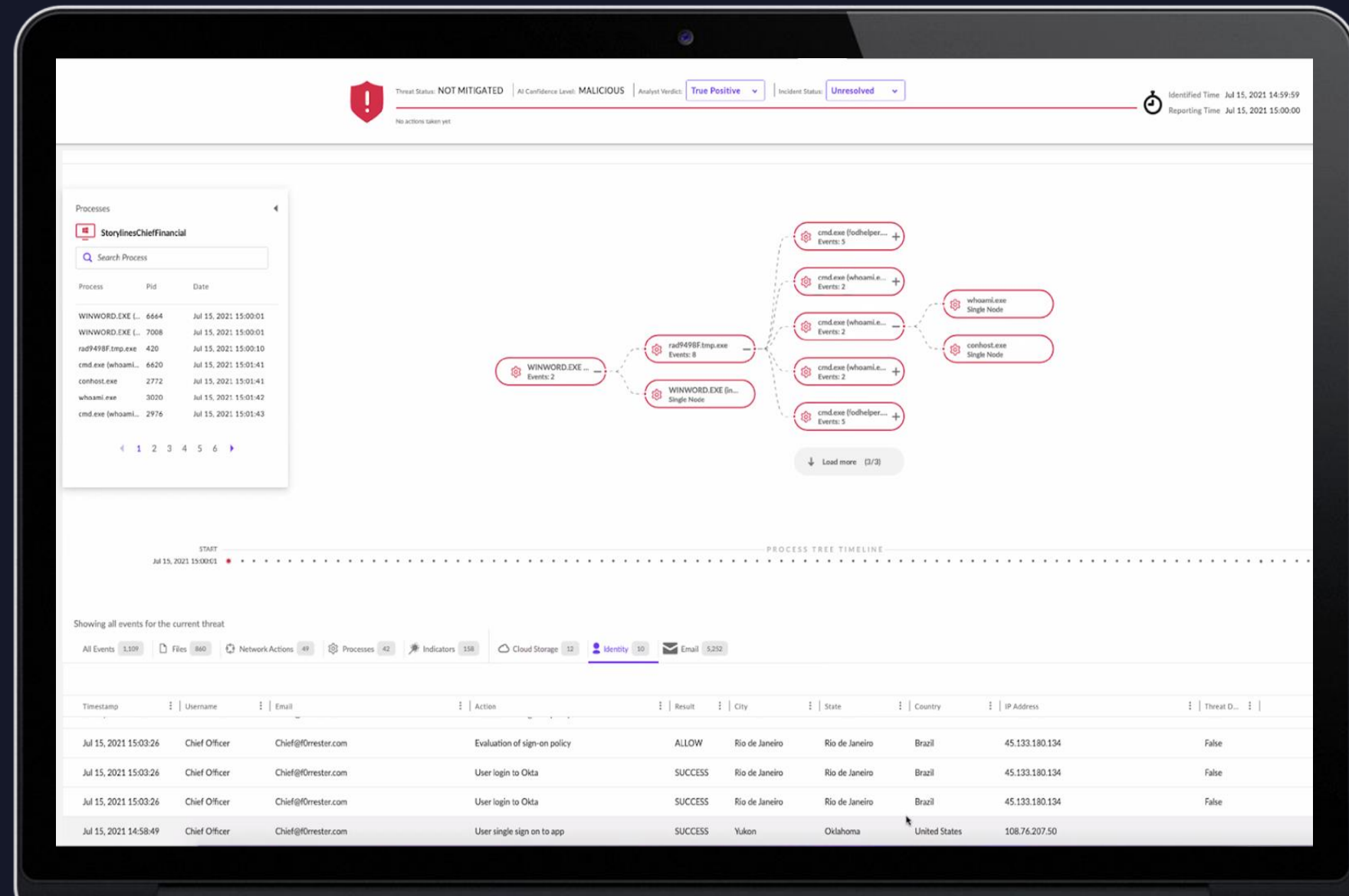
**ESG**



# The Quest for Optimized Security Operations

Single Pane of Glass...

...or Single **Glass of Pain?**



# Signal : Noise Reduction is Critical

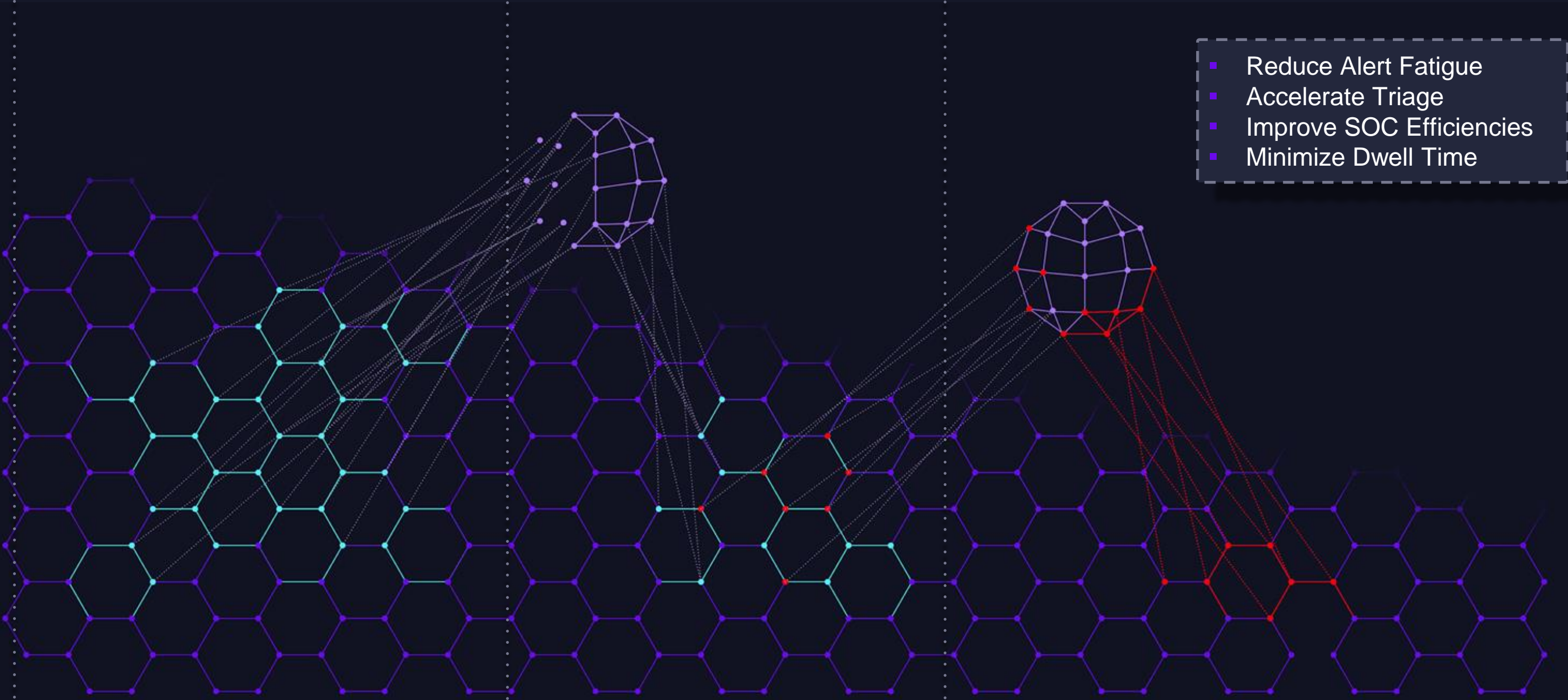
Trillions  
of Rows of Raw Data

Millions of  
Enriched Storylines

Handful of Actionable  
Campaign Level Incidents

- Endpoint
- Email
- SIEM
- Network
- Firewall
- Cloud
- Identity

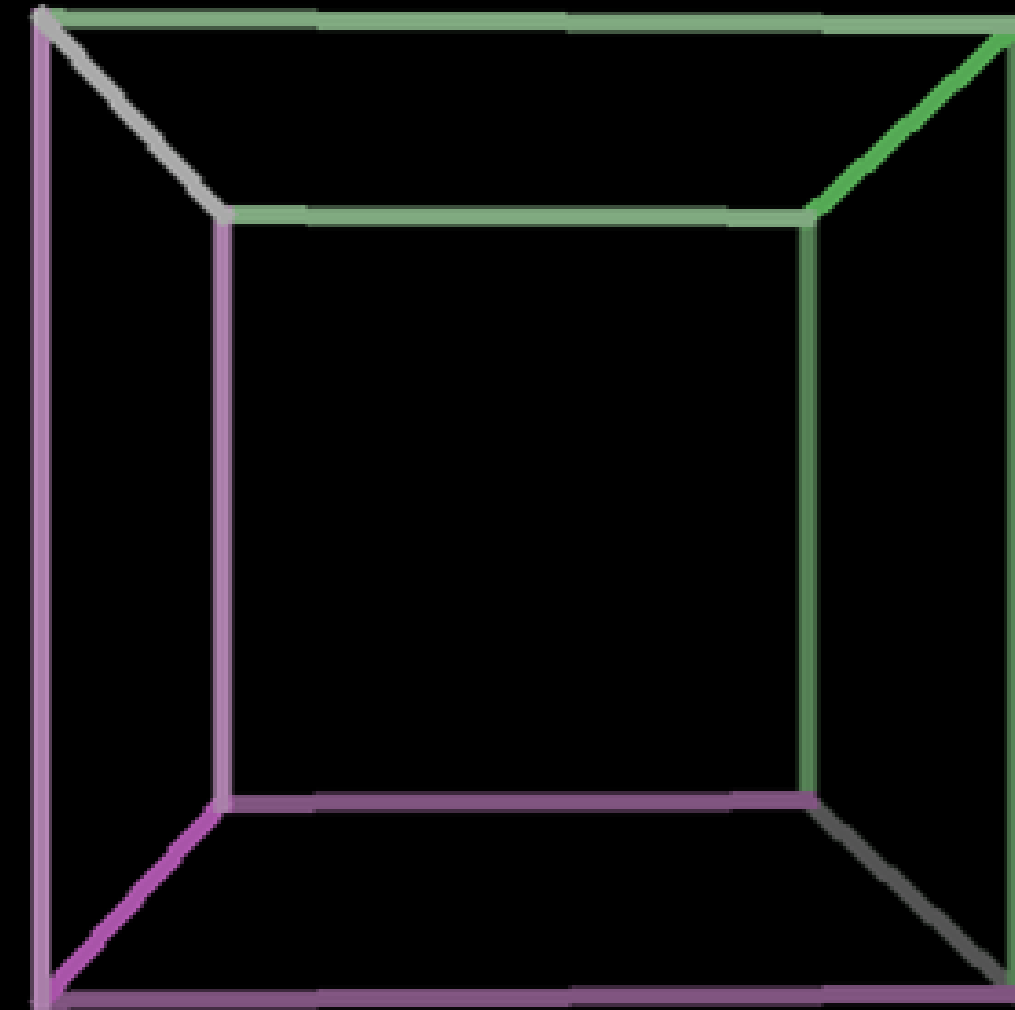
- Reduce Alert Fatigue
- Accelerate Triage
- Improve SOC Efficiencies
- Minimize Dwell Time





# The “Duality” of Black-Box AI

- Non-Deterministic(results may vary)
- Detect Previously Unseen Attacks
- Often Unable to Explain “Rationale” for Conclusion
- False Positives and False Negatives are Inherent



Accuracy & Explainability?

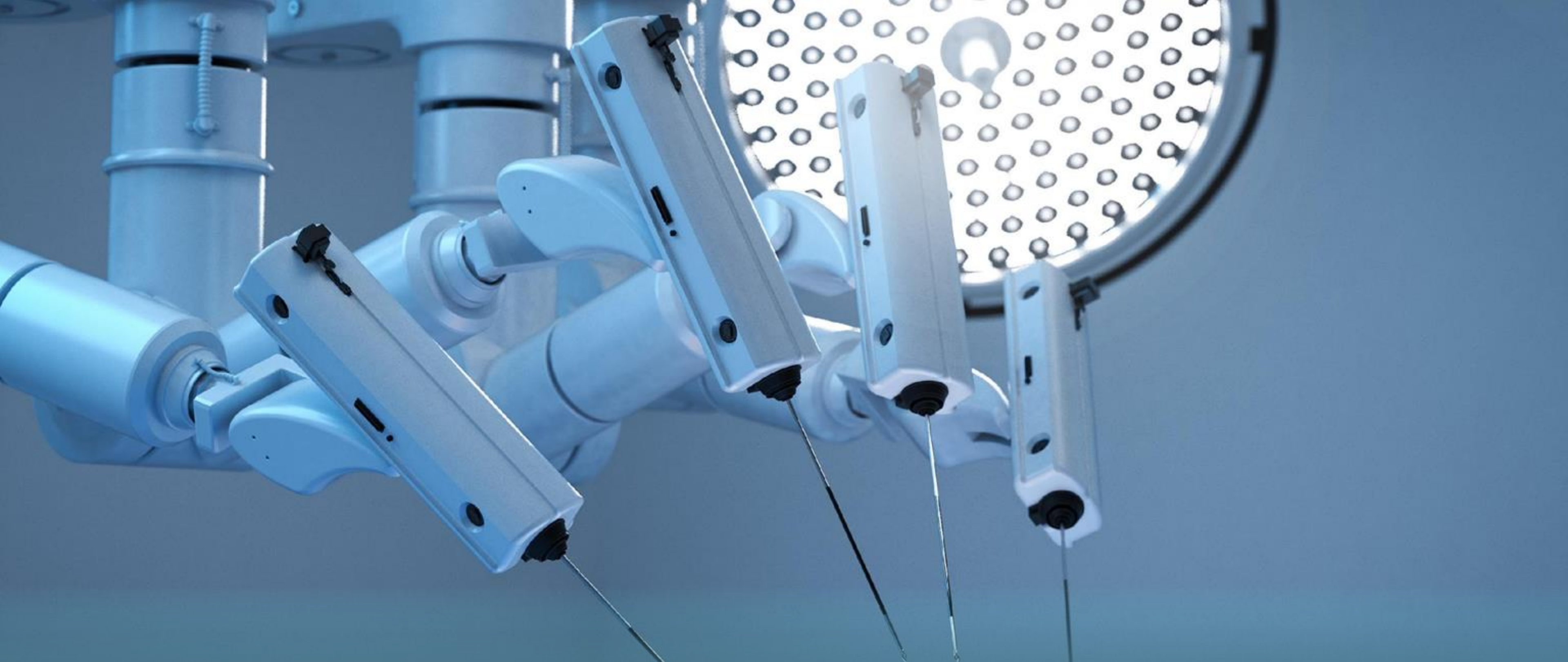




# Can AI Tell the Difference?







**Are You Equally Comfortable with 90% Accuracy in This Scenario?**

# A Time & Place for Machines







02

---

# SOC as a Proofpoint

# Challenges Facing Today's SOC

Disparate Data Silos


Endpoint (EDR)



3rd-Party (SIEM)

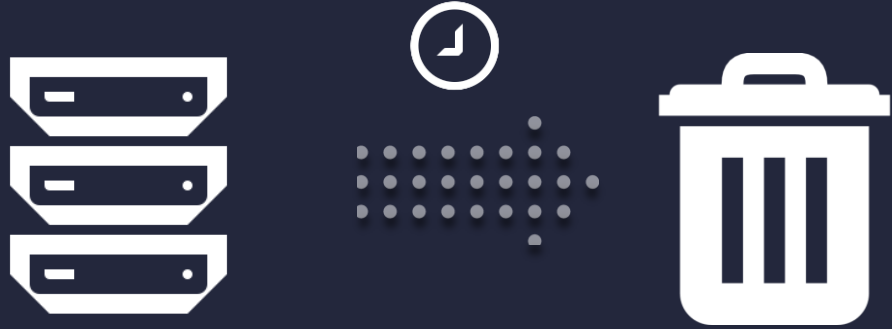


Cloud (AWS/Azure)



**66%**  
customers admit  
siloed tools lead to  
missed detections

Data Retention



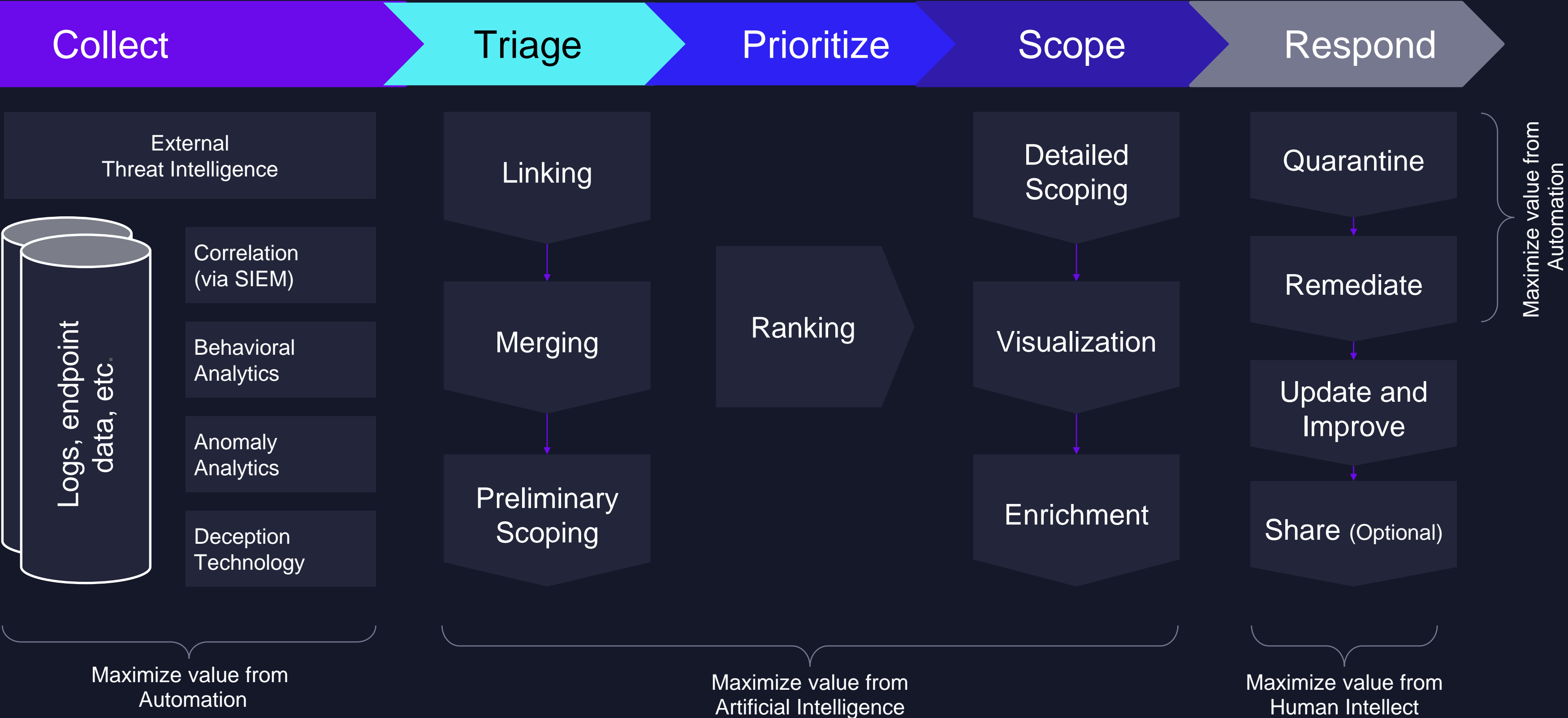
**25%**  
threats go  
untriaged

Skills Shortage





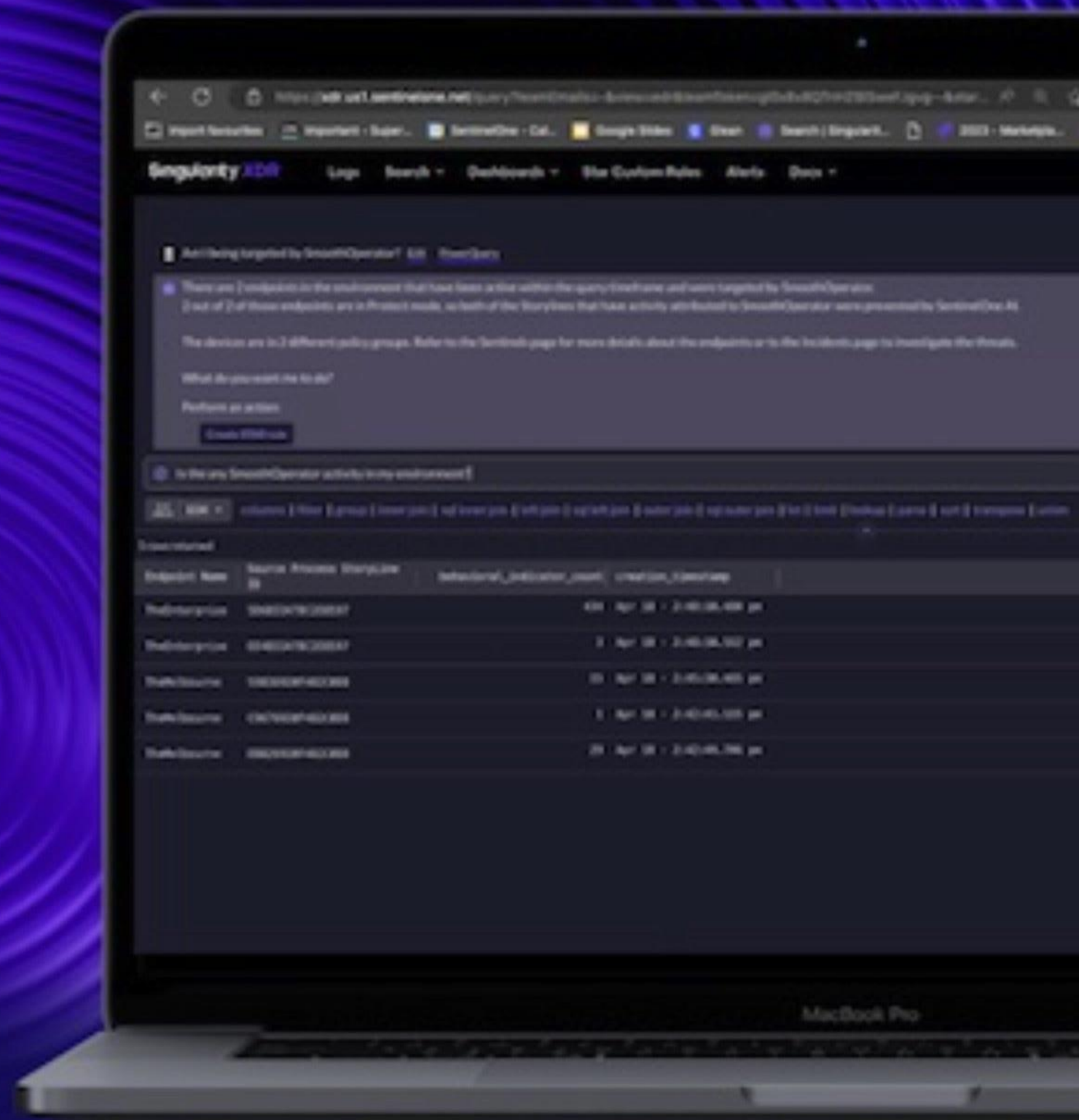
# Workflow of an Attack Investigation





Introducing

# Purple AI













# The Whole Is Greater Than The Sum Of Its Parts

Complex Data Analysis



Human Intellectual Capital





# Thank You

---



[sentinelone.com](https://sentinelone.com)





SentinelOne®