3ˆ EDIZIONE

CYBERSEC 2024

ROMA, ITALIA

LA CYBERSECURITY NELL'ERA DELL'AI

6-7 MARZO

www.cybersecitalia.events

CYBERSECURITY ITALIA EVENT

CYBERSECURITYITALIA

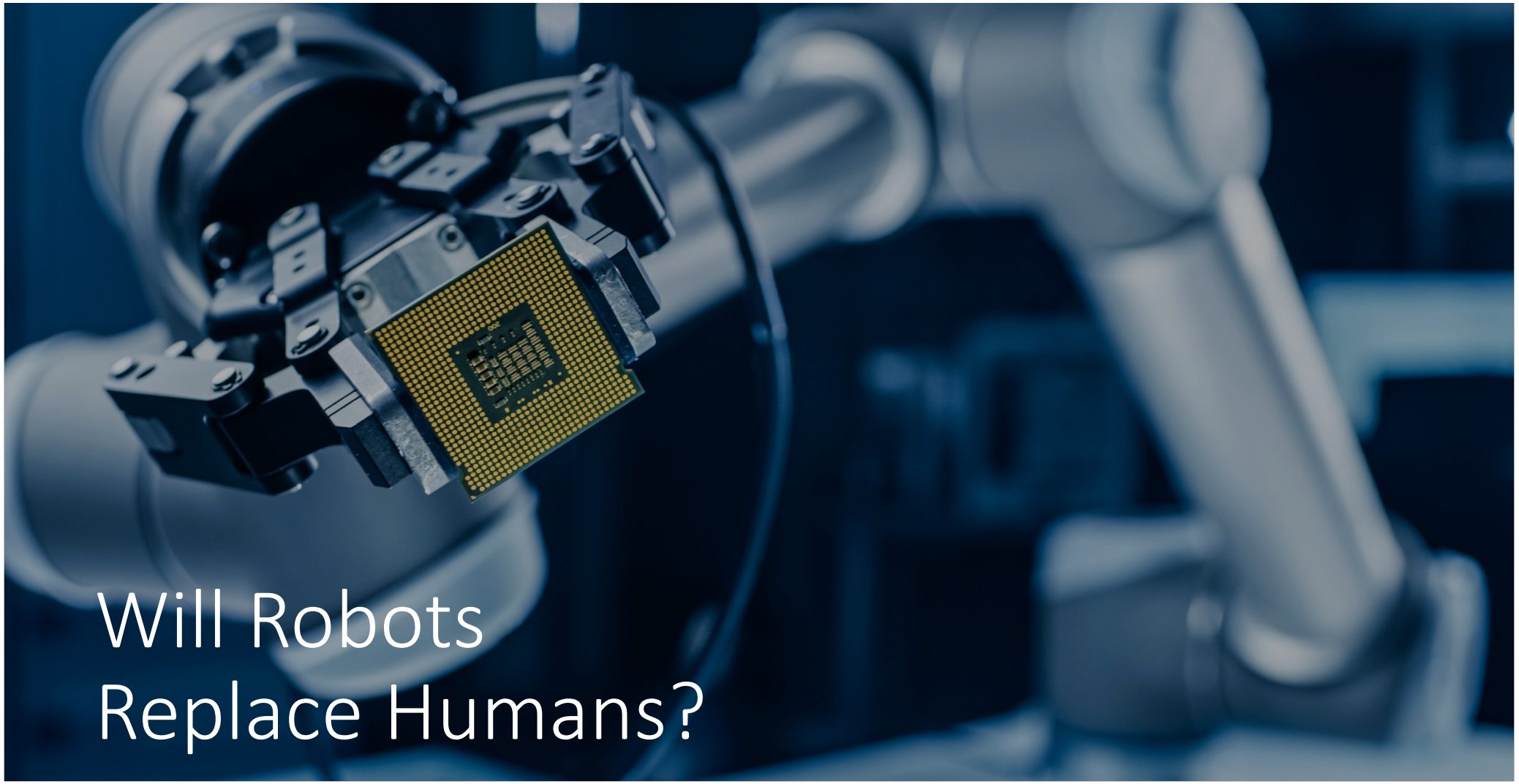
RELATORE

Paolo Cecchi

Sales Director Mediterranean Region,
SentinelOne

SentinelOne®
Secure Tomorrow

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



Will Robots Replace Humans?

Or Will Humans and Machines Create Greater Value Together?

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

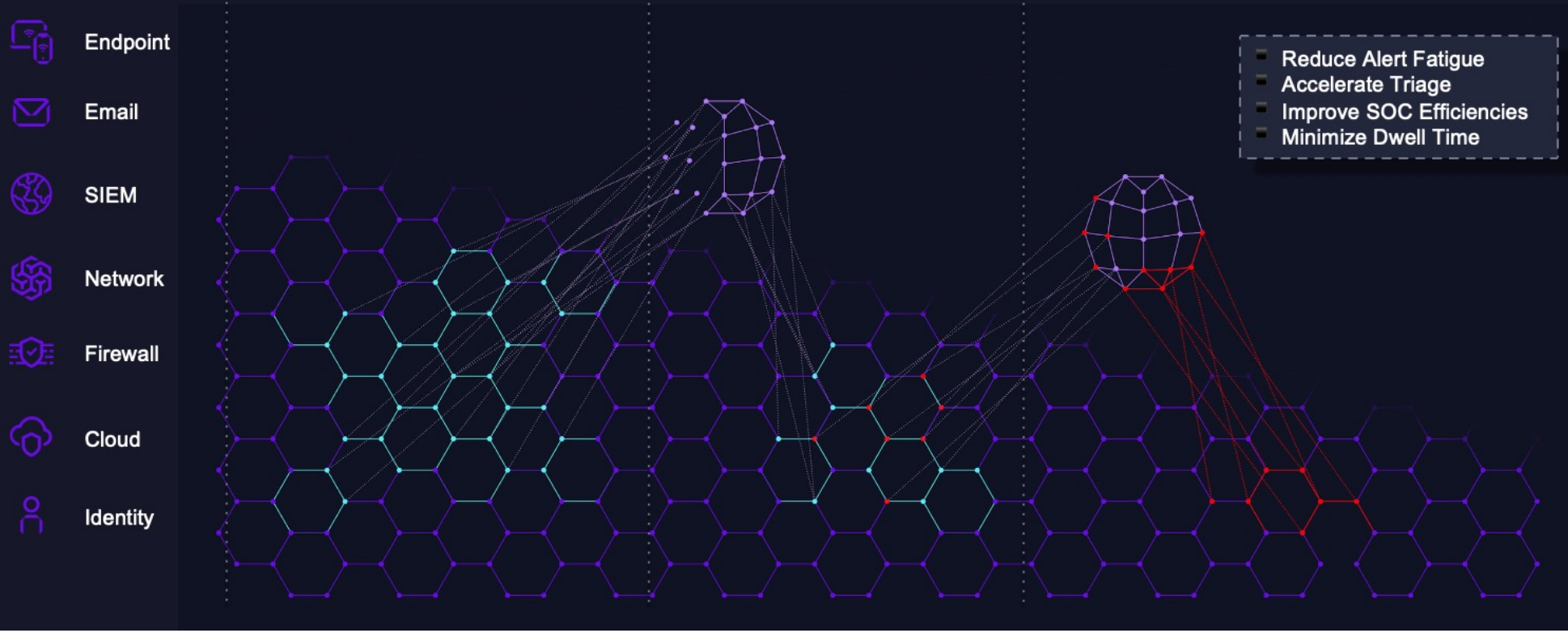
Manual orchestration of responses that happen at individual control points and at human speed

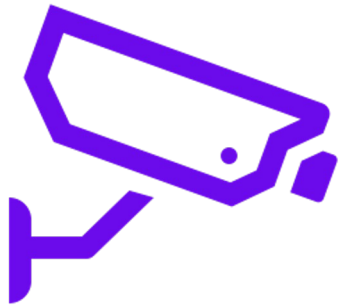
Signal : Noise Reduction is Critical

Trillions
of Rows of Raw Data

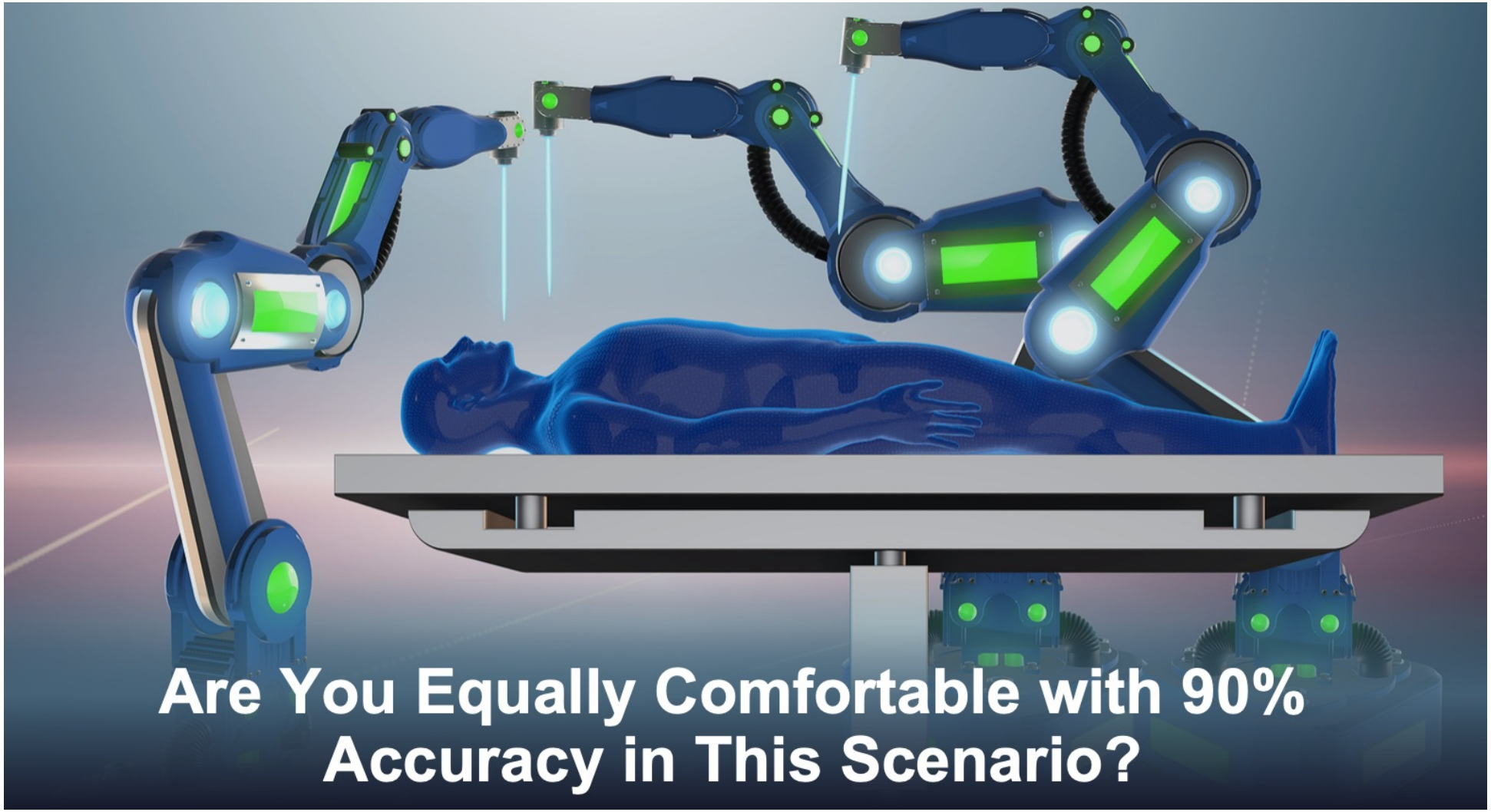
Millions of
Enriched Storylines

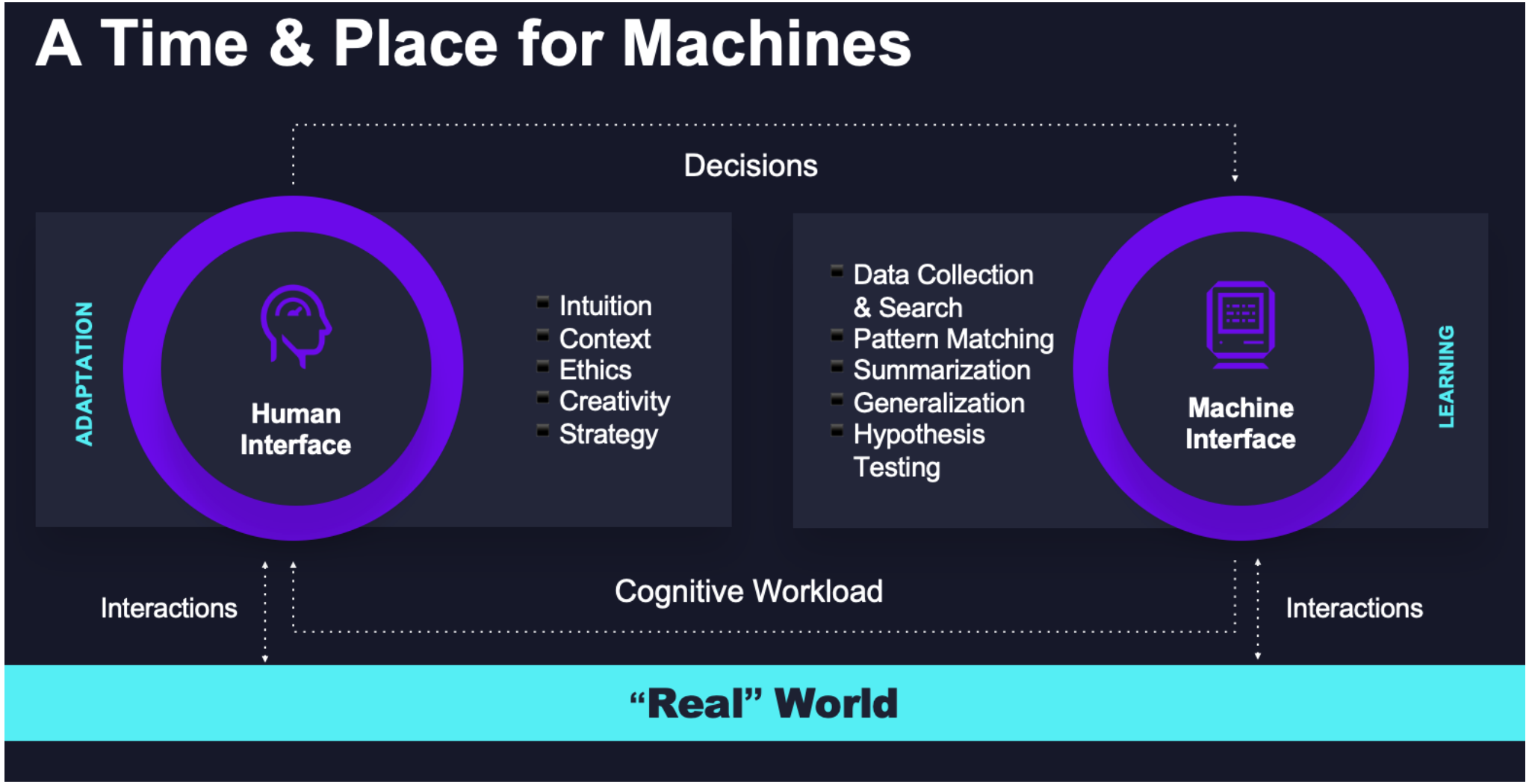
Handful of Actionable
Campaign Level Incidents

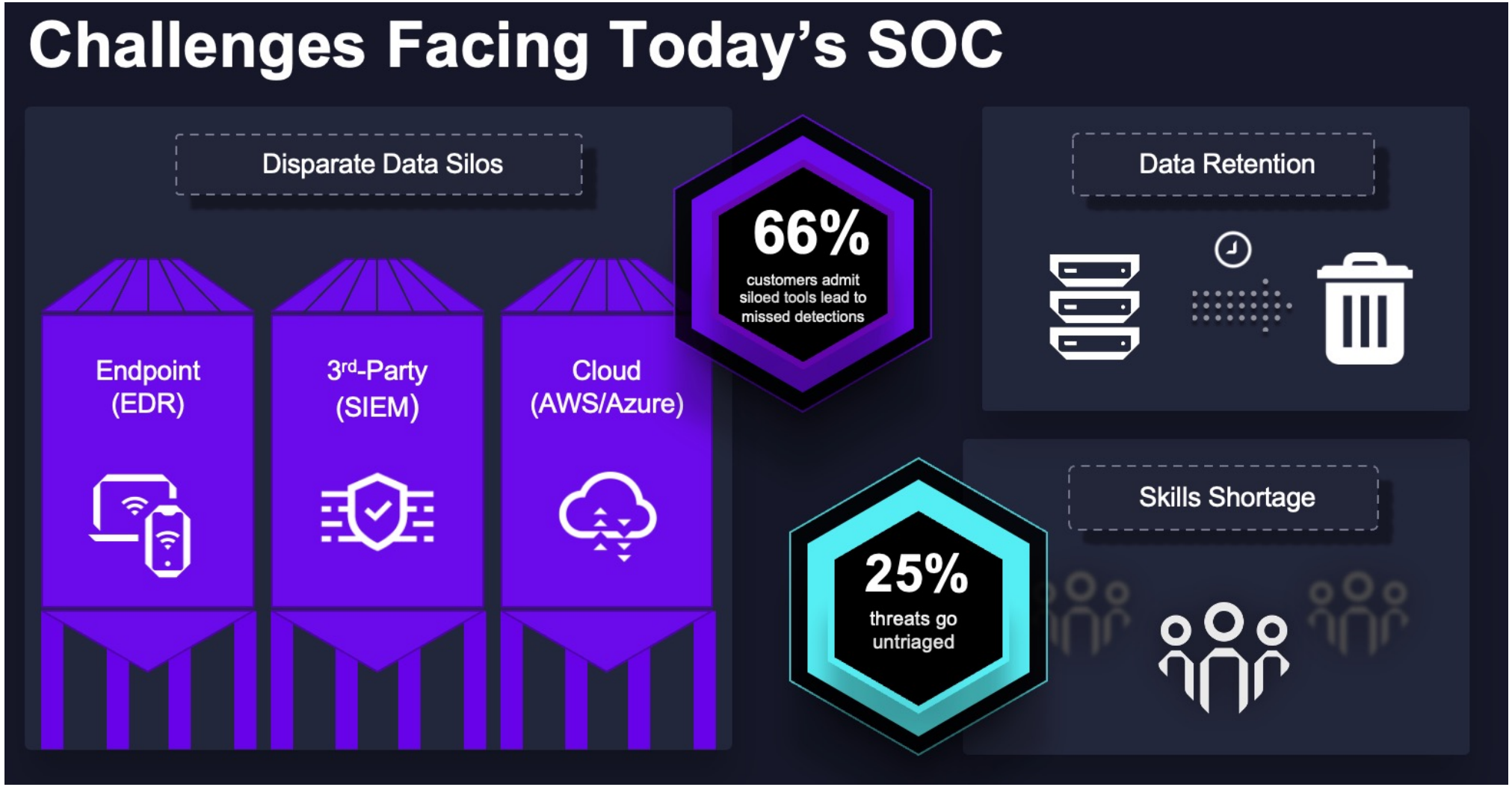


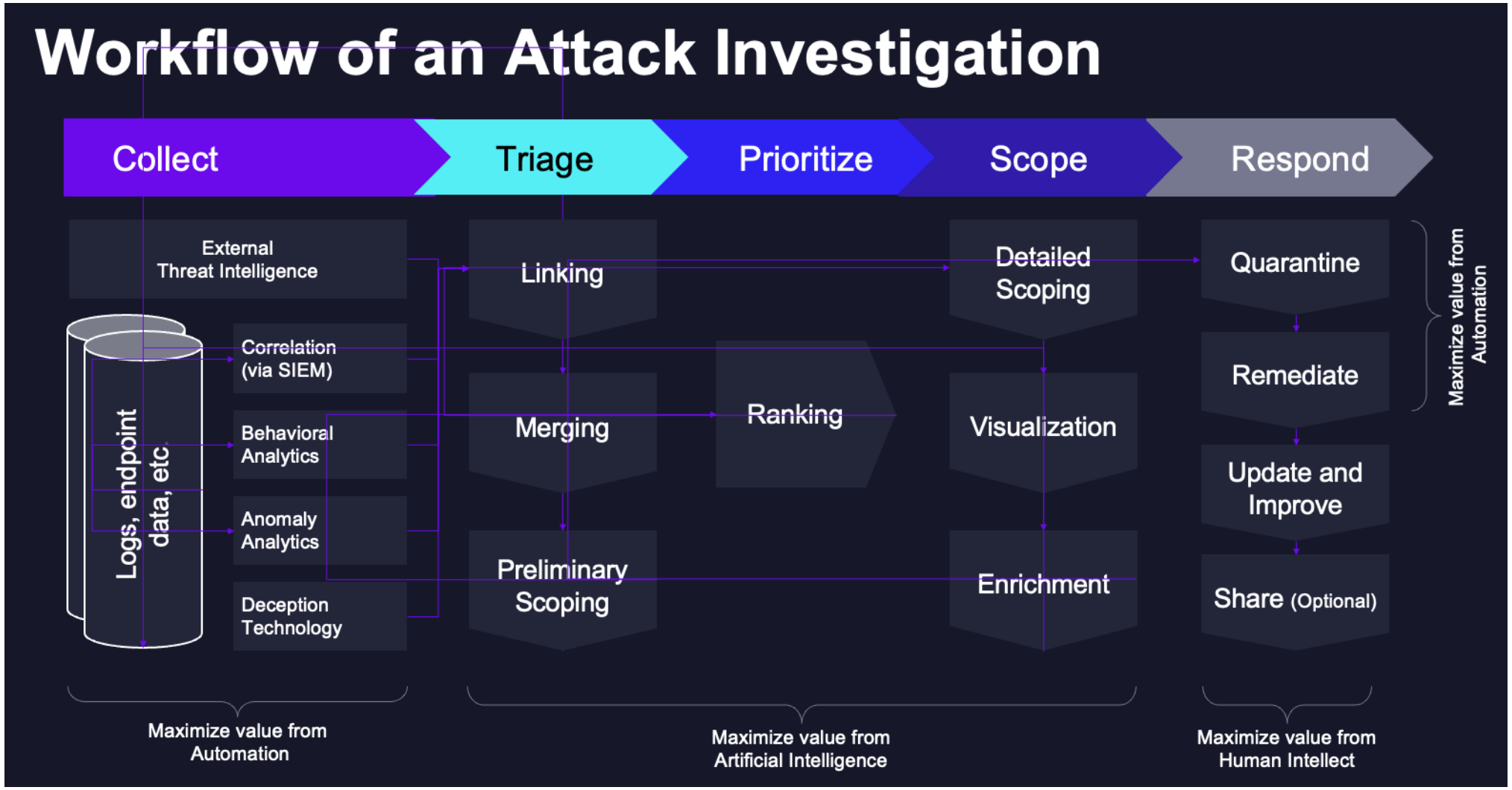


Can AI Tell the Difference?


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


A Time & Place for Machines
Decisions
ADAPTATION
Human Interface
Intuition
Context
Ethics
Creativity
Strategy
Data Collection & Search
Pattern Matching
Summarization
Generalization
Hypothesis Testing
Machine Interface
LEARNING
Interactions
Cognitive Workload
Interactions
"Real" World


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
Collect
Triage
Prioritize
Scope
Respond
External Threat Intelligence
Logs, endpoint data, etc
Correlation (via SIEM)
Behavioral Analytics
Anomaly Analytics
Deception Technology
Linking
Merging
Preliminary Scoping
Ranking
Detailed Scoping
Visualization
Enrichment
Quarantine
Remediate
Update and Improve
Share (Optional)
Maximize value from Automation
Maximize value from Automation
Maximize value from Artificial Intelligence
Maximize value from Human Intellect

Benefits of Human-Machine Teaming

Simplified Triage

- Improve Artifact Extraction
- Automate Data Gathering
- False-Positive Reduction
- Signal from Noise
- Reduced Complexity

Integrated Response

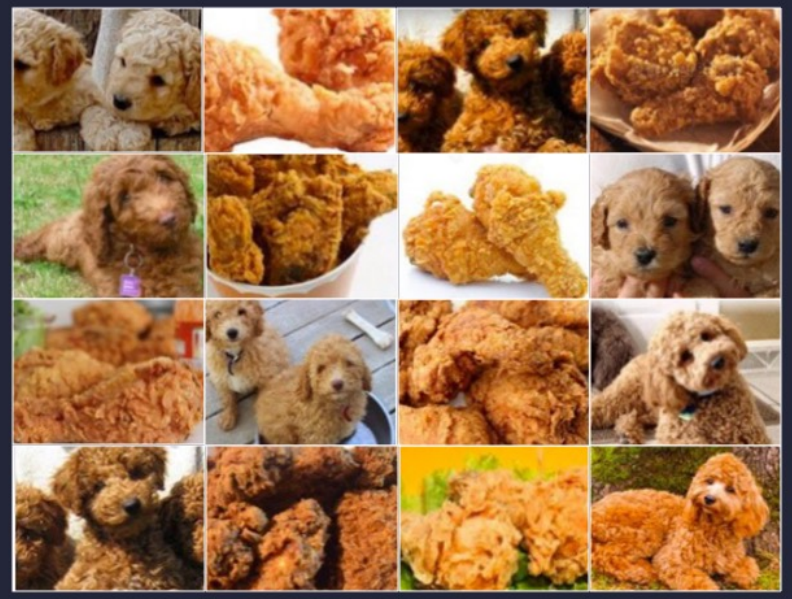
- Conformity of Actions
- Designed for Repeatability
- Improve Confidence
- Reduce MTTD & MTTR

Staff Efficiencies

- Reduce FTE Requirements
- Automate / Replace Tier 1
- Analyst Coaching
- Reduce Alert Fatigue

The Whole Is Greater Than The Sum Of Its Parts

AI: 90% Accurate



Fried Chicken or Labradoodle?

Humans: 100% Accurate

Chocolate Chip Ice Cream or Dalmatian?

Humans and Machines are **Better Together!**

SentinelOne®
Secure Tomorrow

Thank You!

Sentinelone.com