Debunking Common Myths About XDR

Jörg Löhler
Sr. Sales Engineer DACH

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

Agreement on Key Value Propositions for XDR

Reduce Mean Time to
Detect. Investigate. Respond

Reduce Cost

Improve SecOps
Efficiency & Skillset

Improve
Performance & **Scale**

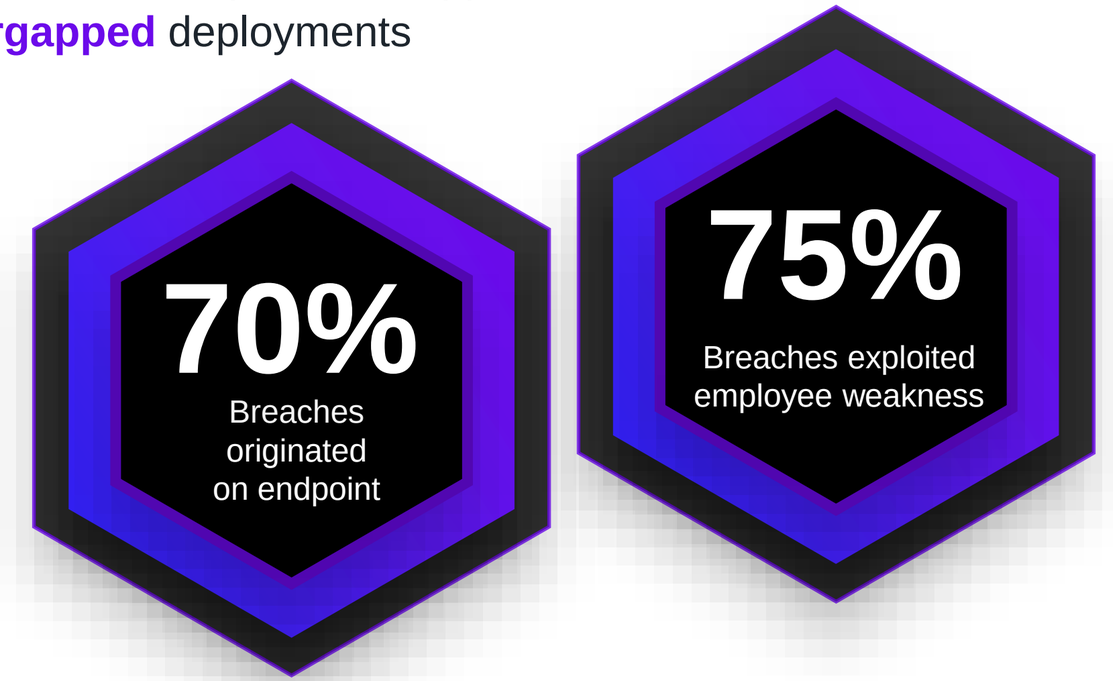
MYTH

01

XDR can exist without a solid EDR foundation

REALITY

- **Endpoint Detection & Response (EDR)**
  - Continues to be the **most effective** threat protection & mitigation tool for enterprise
  - Efficacy proven by recent **MITRE** evaluation
  - Requires **broad platform** support
  - Autonomous operation supports **airgapped** deployments



SentinelOne

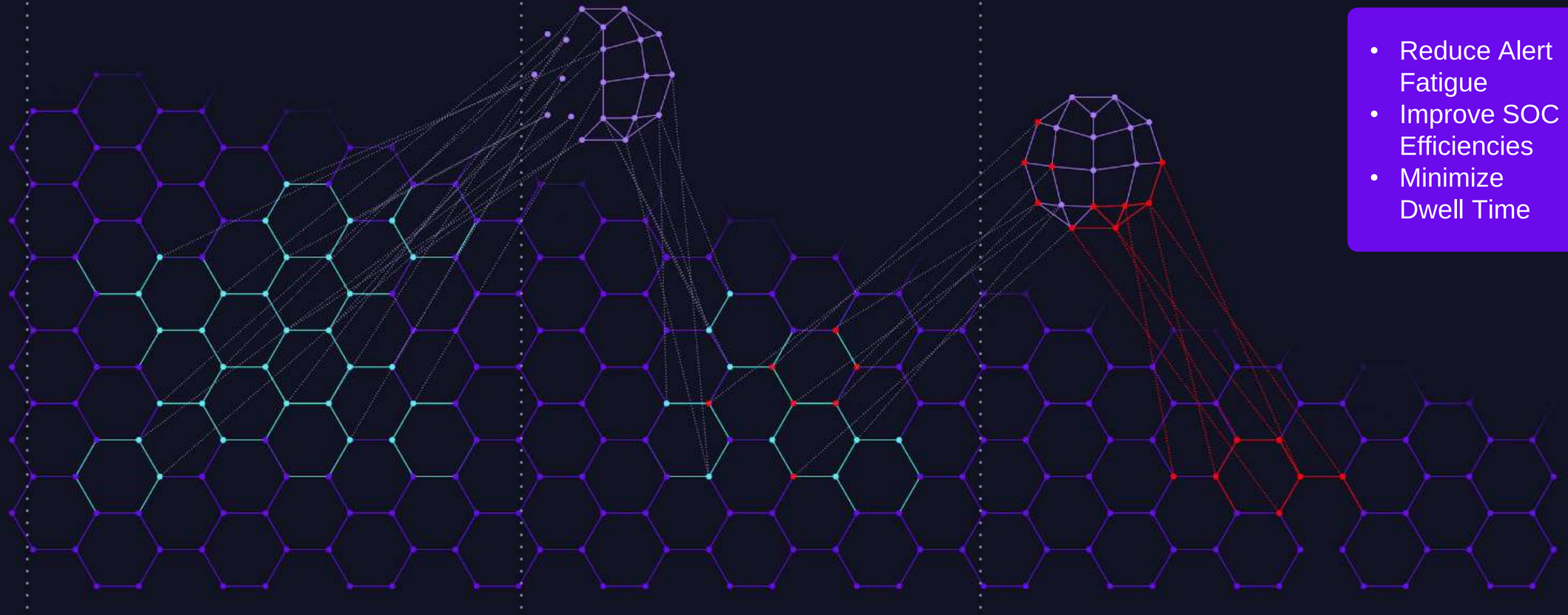
XDR Adds Vital *Non-Endpoint* Telemetry

Trillions
of Points of Telemetry

Hundreds
of Suspicions

Handful
of Incidents

- Endpoint
- Email
- Web Gateway
- Network
- Firewall
- Cloud
- Identity



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

SentinelOne

MYTH

02

XDR is just Next-Gen SIEM

REALITY

- **SIEM Strengths**
  - Broad **data ingestion** support
  - Satisfies governance & **compliance** security use cases

- **SIEM Complaints**
  - Too **expensive**
  - Detects **known** threats
  - Operational **complexity**
  - Requires constant rule **creation** and **tuning**
  - Difficult to **scale** to meet growth of security event data

- **SIEM and XDR are Complimentary**

SentinelOne

SIEM and XDR on a Collision Course

	SIEM	XDR
Business Focus	Risk-Centric	**Threat-Centric**
Deployment Models	On-Premises, Cloud, Hybrid	**Cloud-Native**
Use Cases	• Compliance (Log Management) • Reporting • Threat Detection (Rule-based Correlation) • Triage & Hunting (Artifacts/IOCs)	• **Threat Detection (ML/AI)** • **Triage & Hunting (Behaviors/TTPs)** • **Intelligent Response**
Data Models	Rigid, normalized, structured data schema	**Open, flexible data architecture**
Analytics	Rule-based correlation + ML *(bolted on)*	**AI-based detections + Rules *(BYO Logic)***
Operational Models	• Consume Everything *(that you can afford)* • Build Static Detection Logic • Determine Actionability *(if supported)*	• **Consume Relevant / Actionable Data** • **Enrich Investigations / Net New Detections** • **Prescribe One-Click Responses**

+ SOAR? +UEBA? +TIP?

MYTH

03

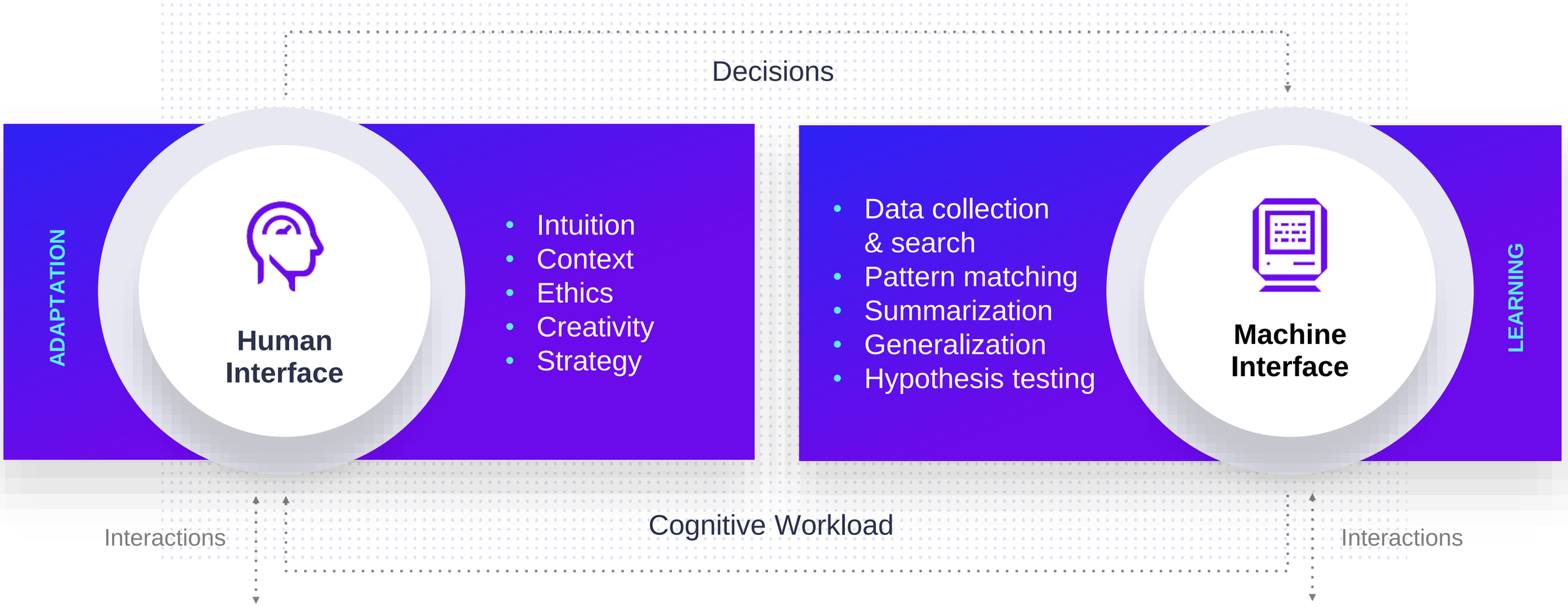
Automated response means loss of control

REALITY

- **Automated Response vs. Recommendation**
  - Keep the human in the loop to gain confidence
  - Learn from prior manual actions to guide prescription
- **Some Tasks can be Safely Automated**
  - Threat Intelligence (ingestion & enrichment)
  - User Authentication (Challenge: Response)
- **One-Click Actions**
  - Block IoC
  - De-provision User Credentials
  - Isolate Device
  - Rollback Malicious Activities
  - Revert Container Image

SentinelOne

A Time & Place for Machines



MYTH

04

More data yields better detections

REALITY

- **Data lakes -> Data swamps**
  - Structured Data?
  - Unstructured Data?

- **Data Ingestion is Hard**
  - Structured DB schemas force **normalization**
  - Too many **parser** formats and enrichment sources
  - On-Prem vs Cloud vs Hybrid?

- **Data Storage & Transport is Expensive**
  - Consumption-based pricing forces **poor decisions**
- **XDR should help Democratize your Data**

SentinelOne

Why Singularity XDR?

Unparalleled Speed & Scale

Data analytics platform at machine speed and scale

Complete Visibility

Ingest, correlate, search, and action data from many sources

Cross-Stack Correlation

Detect advanced threats across the entire enterprise security estate

Built-in Integrations

Frictionless, no code integration across your security stack

Automated Resolution

Automate and orchestrate unified response & remediation

Reduced Complexity

One console for prioritized alerts and response

Thank you

To learn more or connect with us s1.ai

SentinelOne®

sentinelone.com