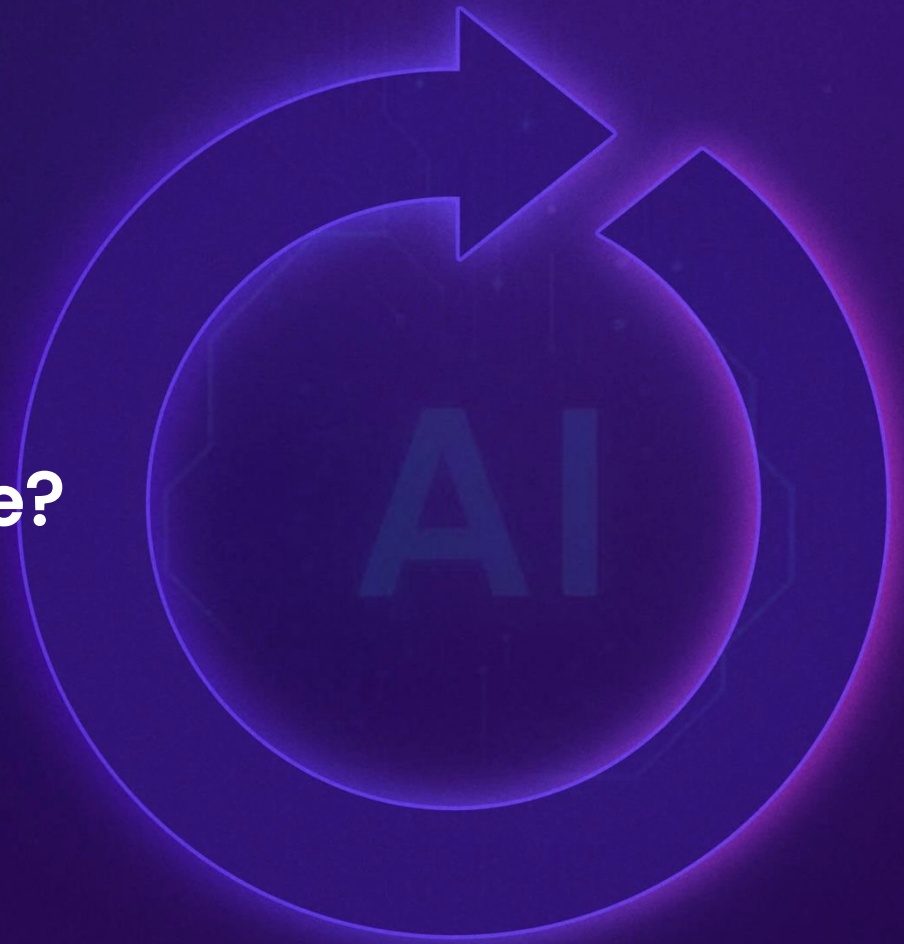
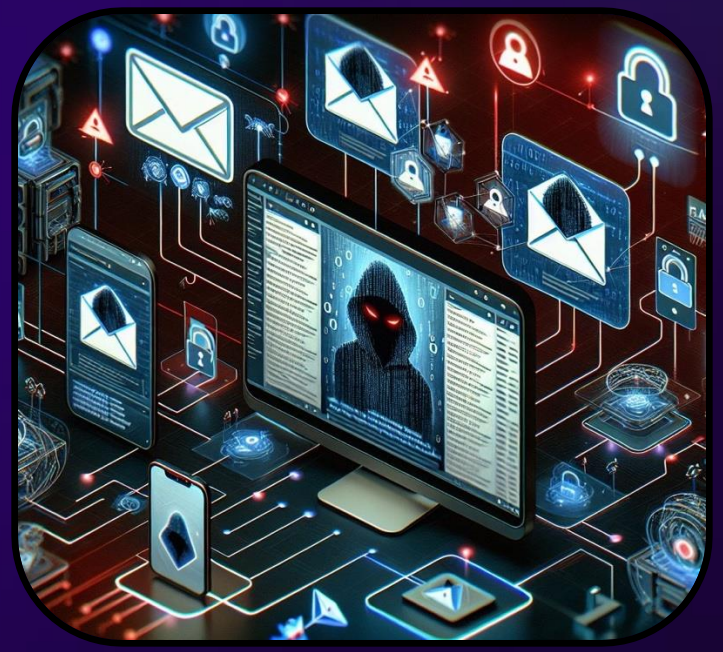
Ontinue

# Cyber Threat Trend –
## Warum KI im SOC wichtiger ist denn je?




Andrina Brun
Director, Sales Engineer EMEA
Ontinue AG

# Top KI unterstützte Angriffsmethoden

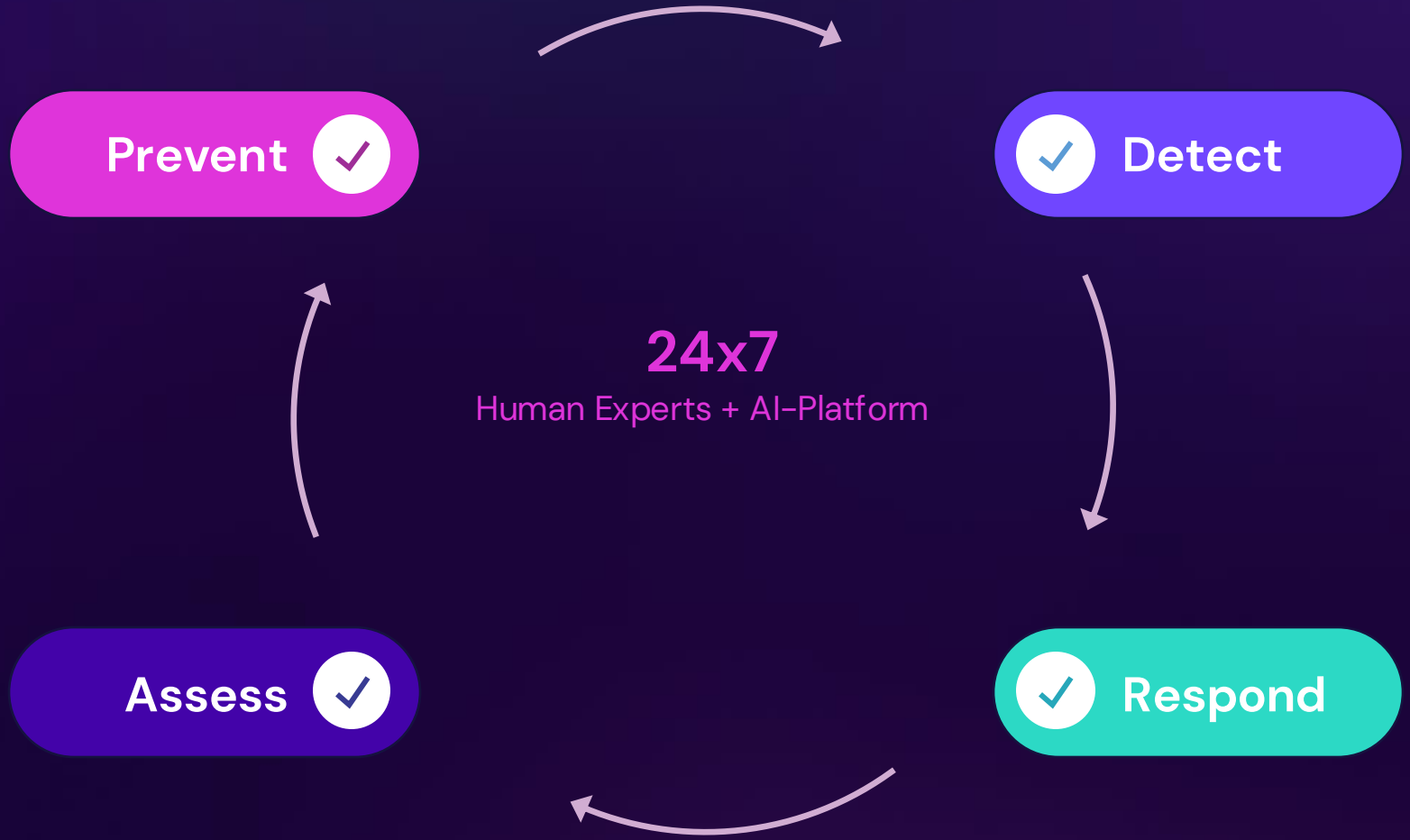


KI powered Phishing

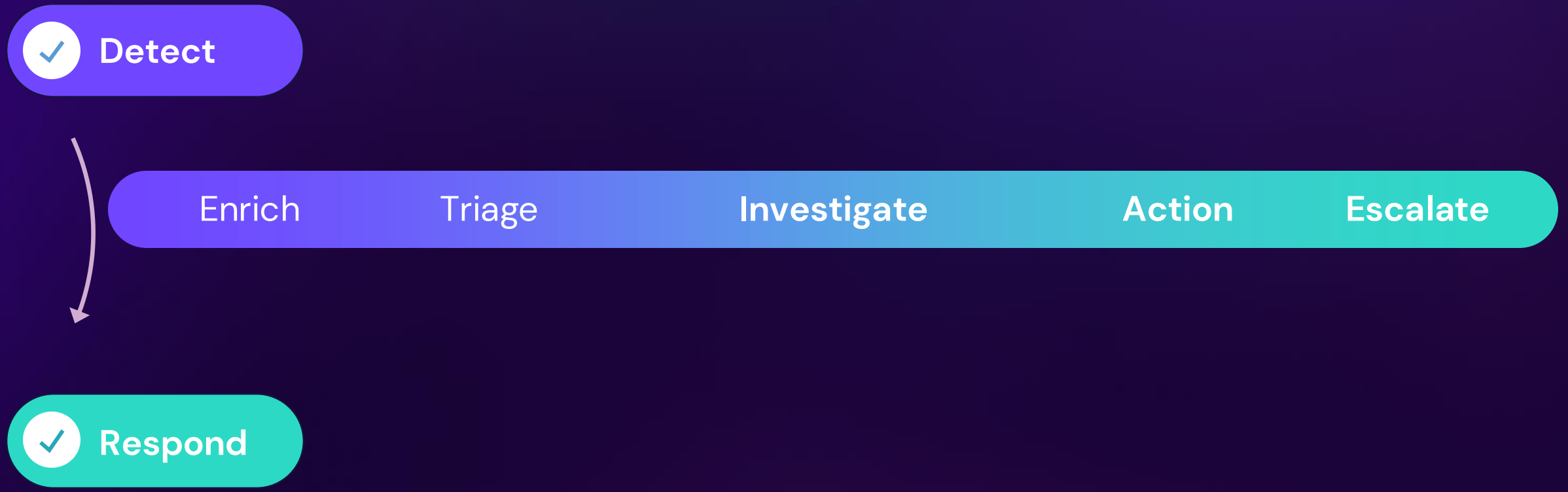

Deep Fake Social Engineering

KI generierte Malware

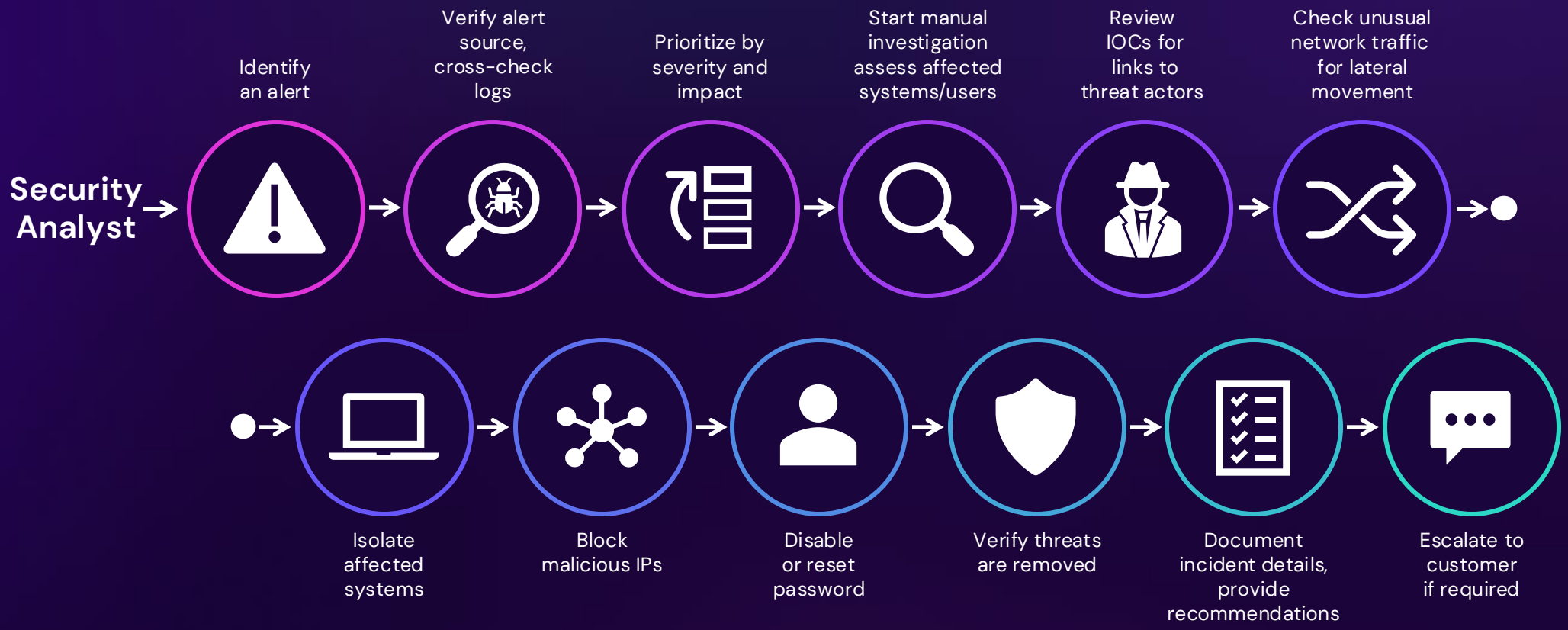
# MXDR


Prevent
Detect
Respond
Assess
24x7
Human Experts + AI-Platform

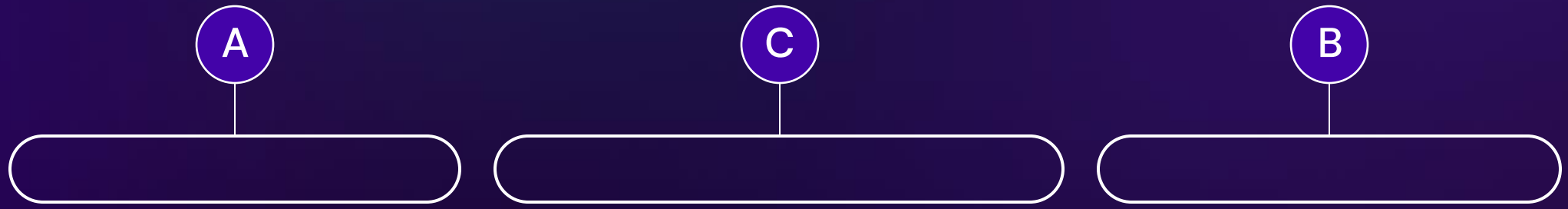
# Detect and Respond



# Classic SOC Workflow



# Ease of Automation



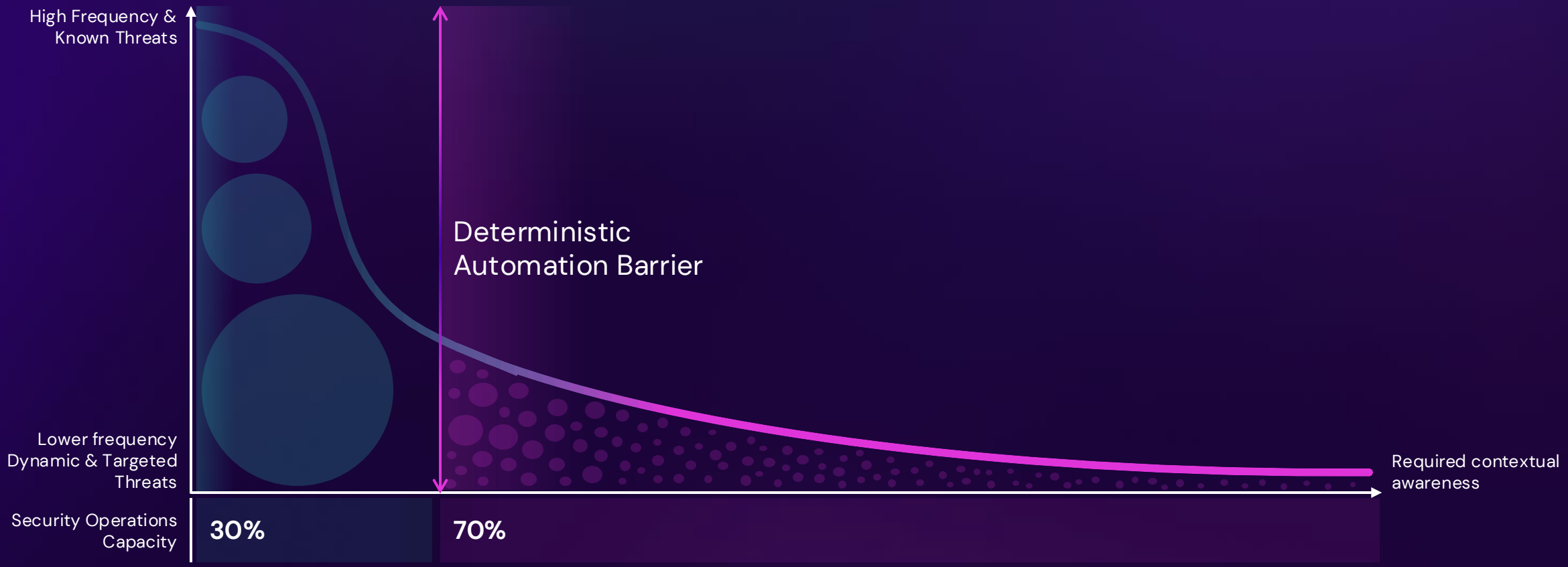

Enrich | Triage | **Investigate** | **Action** | **Escalate**

A Automation “easy”

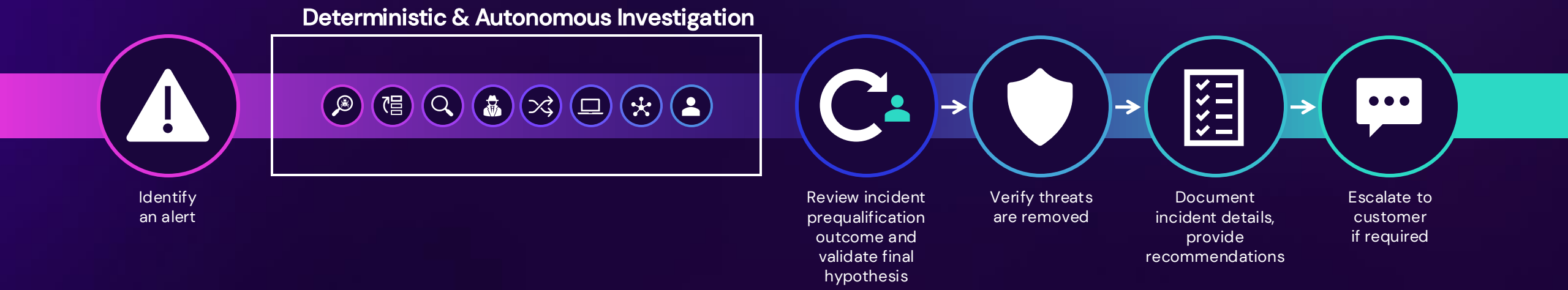
B Automation harder

C **Automation hardest**

# Automation Barrier



# SOC Workflow with Agentic AI




Enrich & Triage
**0.5–5min**

Investigate, Action & Escalate
**3–10min Autonomous Investigator**

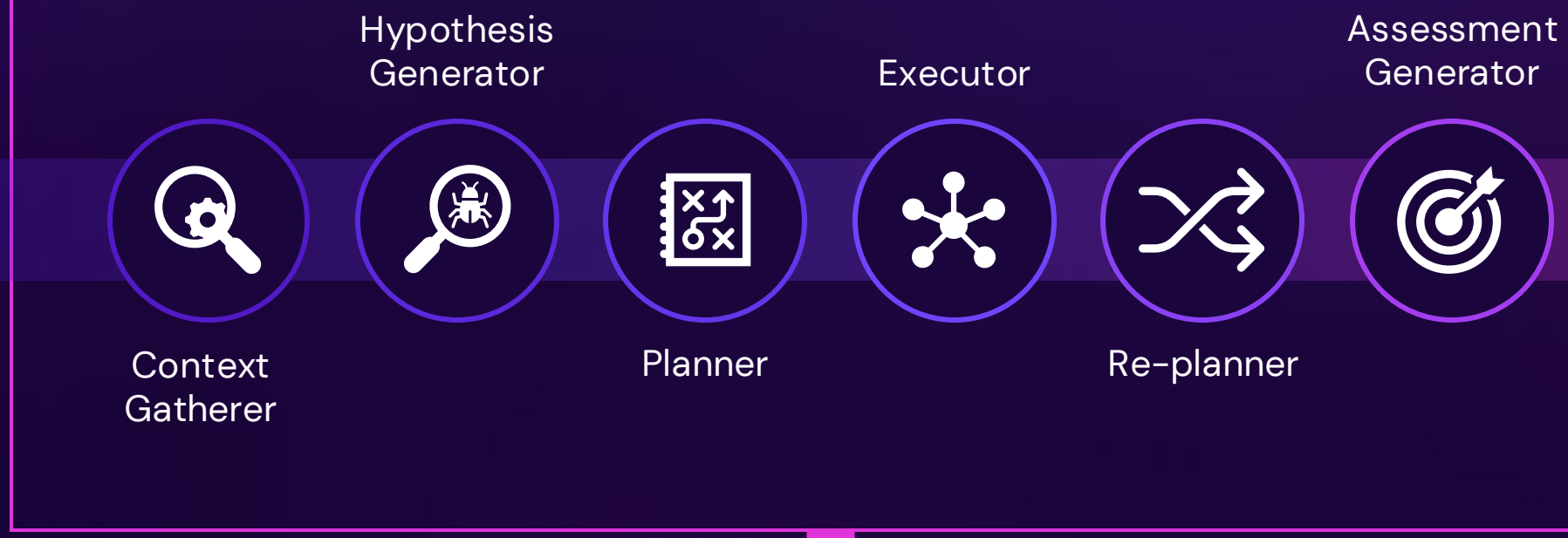
Investigate, Action & Escalate
**10–15min Cyber Defender**

**<30 min**

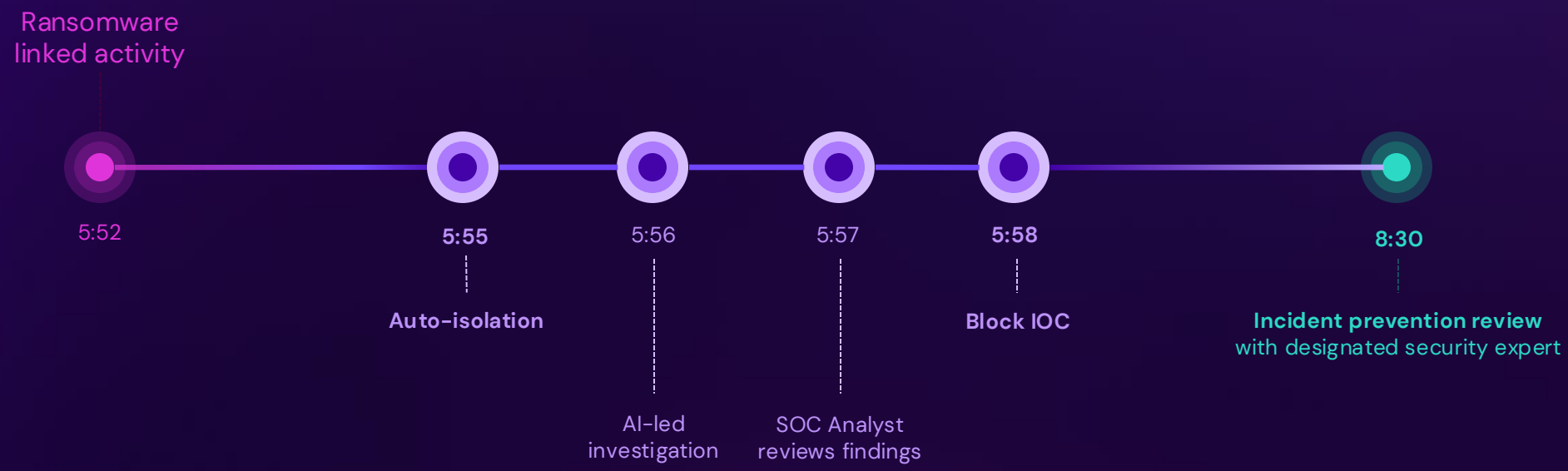
# Agentic AI

Human Analyst Feedback

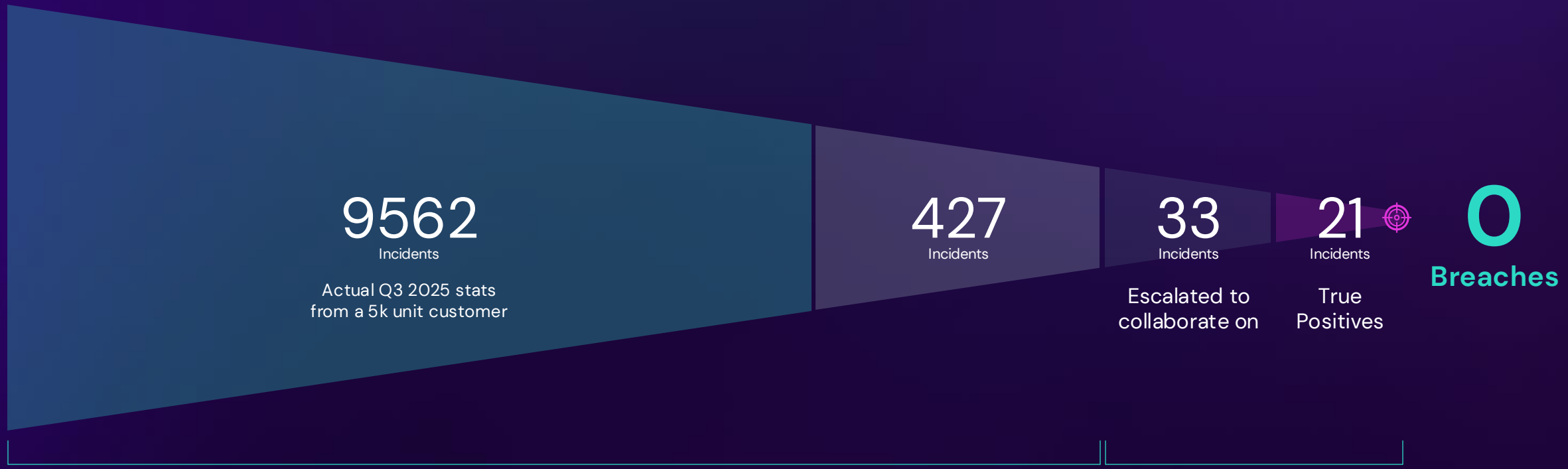
120+ Skills




Hypothesis-driven investigation


Ransomware linked activity
5:52
5:55
Auto-isolation
5:56
AI-led investigation
5:57
SOC Analyst reviews findings
5:58
Block IOC
8:30
Incident prevention review
with designated security expert

# Incident Funnel



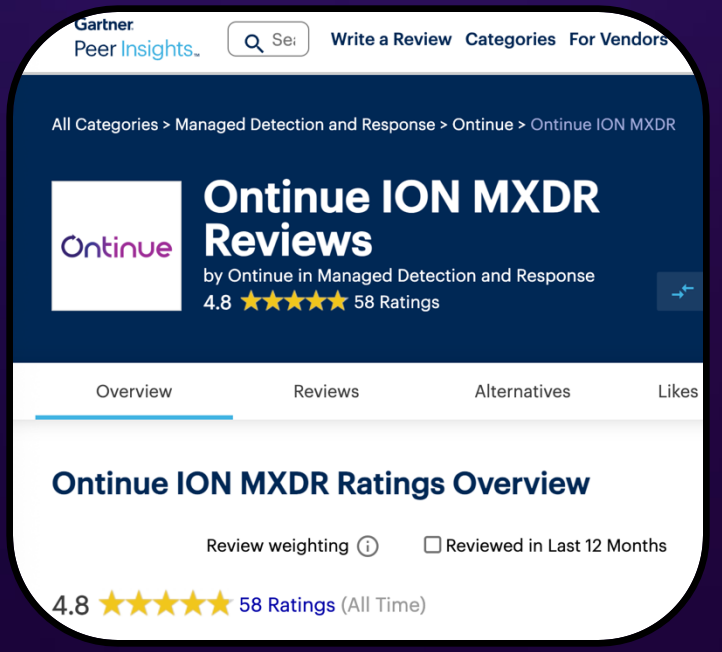

**Investigated and resolved for you**
by the Ontinue platform and SOC

**Jointly resolved**
by Ontinue and your
security team

# KI and SOC Metrics


100% SLA Achieved – 12+ Months

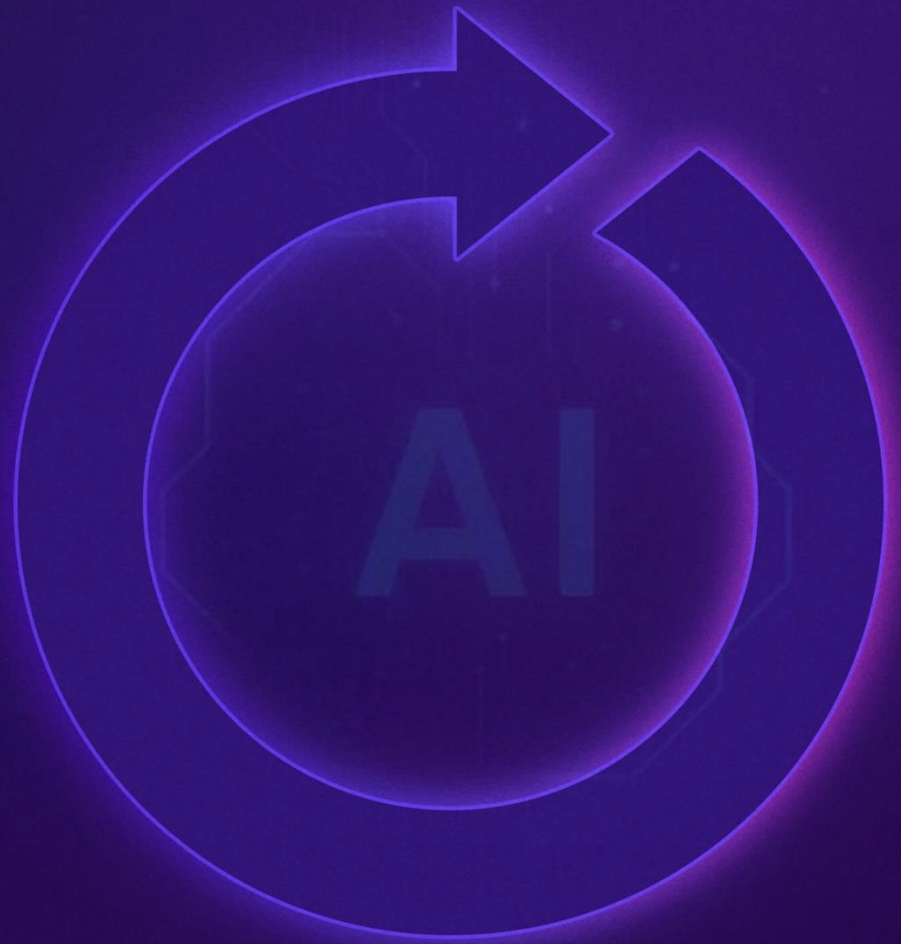

MTTR of HIGH Incident lower than ‹ 13min (10min this month so far)




4.8 ★ Peer Review for Ontinue ION MXDR

Ontinue

# Join us at 15:55




Andrina Brun
Director, Sales Engineer EMEA
Ontinue AG