NG-SIEM, NDR, Open XDR - Journey to Autonomous SOC

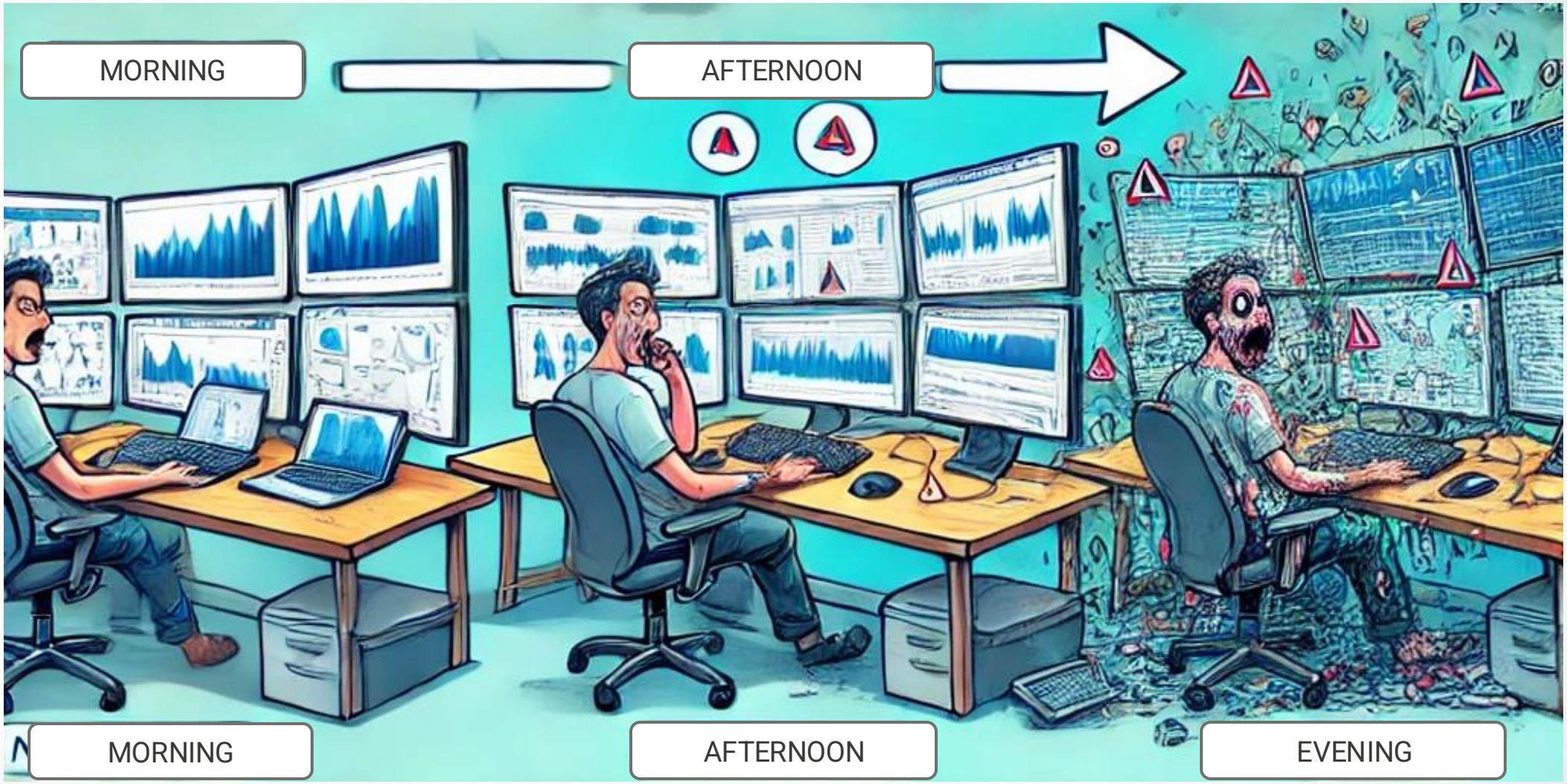
Why Stellar Cyber built it this way and the lessons learned along the way

Prepared for the ISC2 East Bay Chapter on March 14th, 2025

NIST Cyber Security Framework

A Day in the Life of a SOC Analyst

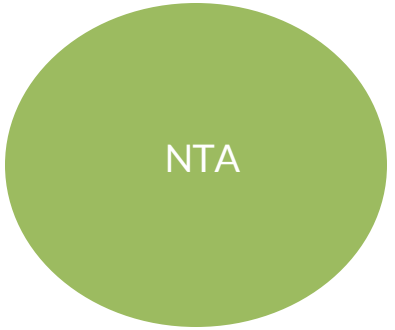
When the journey started in 2015



Key Cyber Security Metrix in 2015

Metrix	Value
Security tools used	~50
Alerts per day	~5000
Time to triage one alert	~30 min
Percentage of alerts not triaged	~60 to 70%
Dwell Time	~146 to 200 days

NG-SIEM, NTA – Adopt ML



AI-Powered Security Operations Center

What we aim to build

MORNING

AFTERNOON

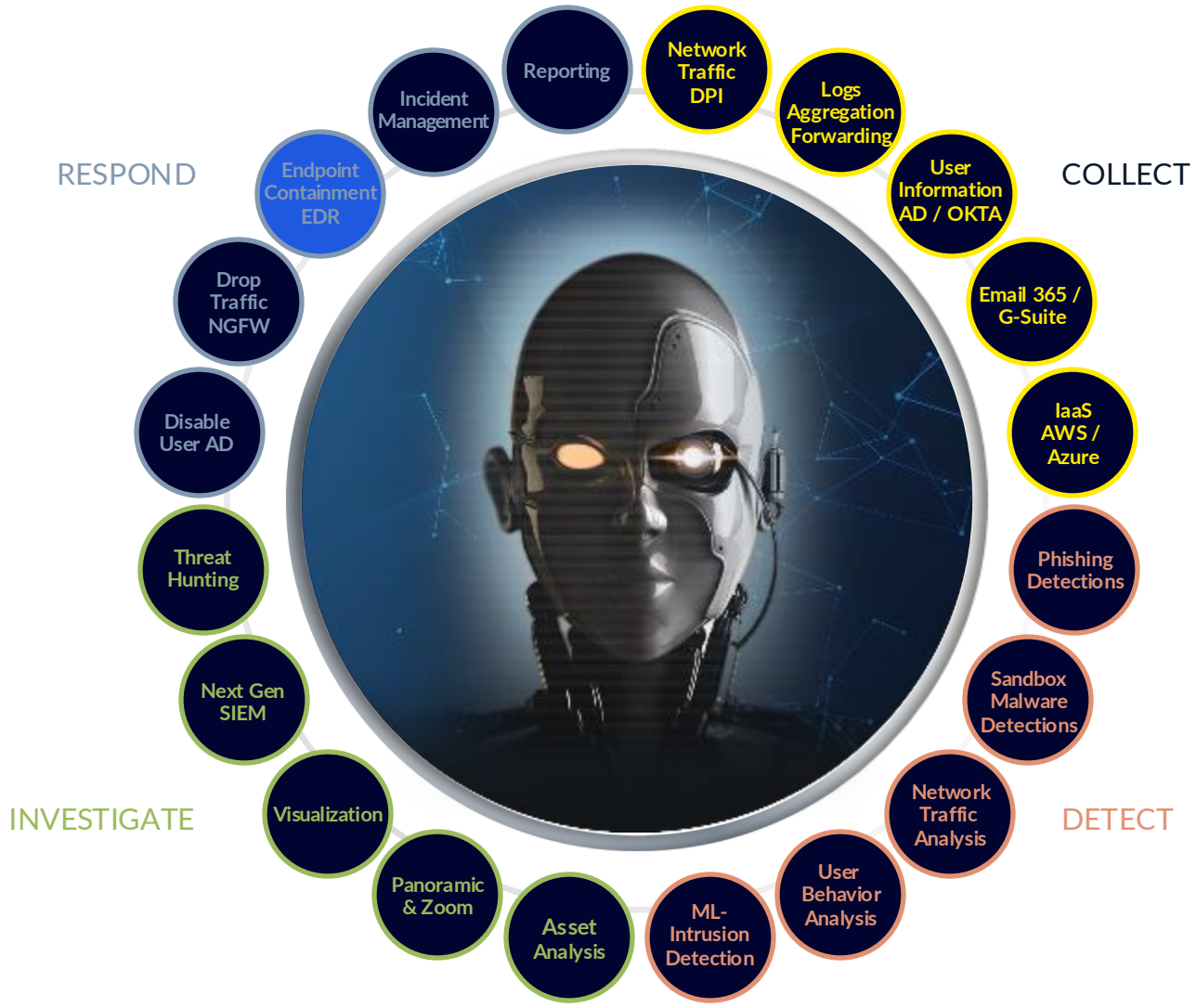
EVENING

A Unified Platform

- See everything, anywhere
- AI + ML-Driven Threat Detection + rules/signatures for known bad
- Connecting the dots
- Response fast
- Seamless Integration with Security tools

.

IDENTIFYING, CORRELATING AND STOPPING A COMPLEX ATTACK



- **Phishing Detection:** CEO received an email with an embedded phishing URL
- **Malware Detection:** CEO downloads a Malware from the site
- **UBA:** Anomalous file server access by CEO @ 2am
- **NTA:** Traffic being sent outside US through DNS tunneling
- **NG-SIEM:** Investigate and validate the above sequence of events
- **Response on NGFW :** Block traffic using manual or automated response
- **Response via EDR:** Send a message

Resolved with a couple of clicks, one analyst and a few minutes vs a team in days

AI-POWER DETECTION & AUTOMATED CORRELATION REQUIRES NEW DATA PIPELINE

LATE DATA PROCESSING – LEGACY SIEM

INGEST

DATA LAKE FOR LONG TERM STORAGE

NORMALIZE & ENRICH

RULE BASED DETECTION & CORRELATION

- Need an Army of People
- Stale data gets analyzed

EARLY DATA PROCESSING – MODERN XDR

Real time association of the event to its context

AI Automation

INGEST

NORMALIZE ENRICH

DATA LAKE FOR LONG TERM STORAGE

AI-POWER DETECTION & AUTOMATED CORRELATION

- Machines do the hard work
- Faster time to detection
- Shorter time to investigate
- Data never stale

Works With All Tools And Investments With 500+ Integrations

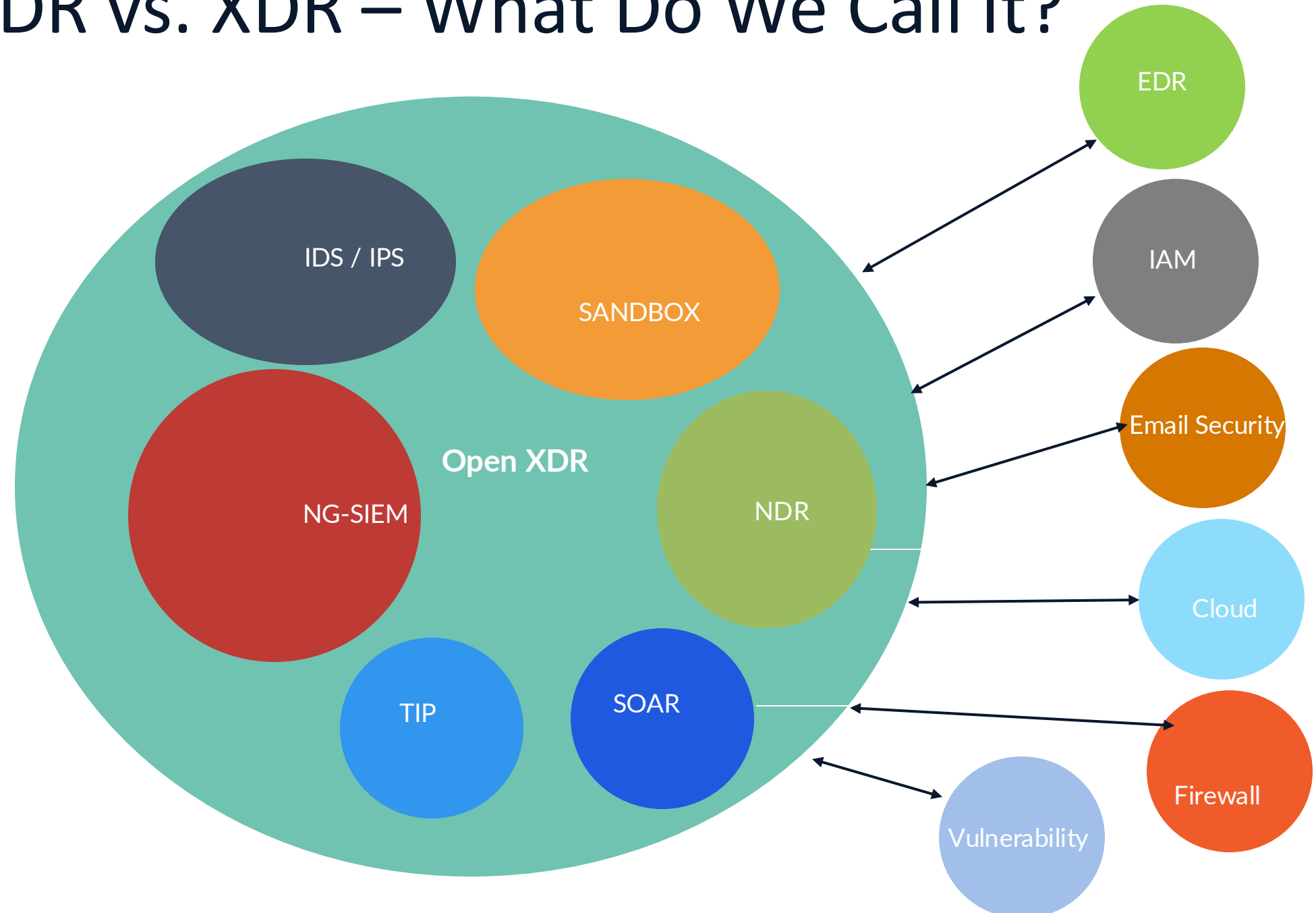
Unified

Simplified

Automated

Open

Open XDR vs. XDR – What Do We Call It?



Gartner

Table 1: Representative Vendors Offering XDR

Vendor ↓	*Product Name* ↓
CrowdStrike	Falcon Insight XDR
Cisco	XDR
Fortinet	FortiXDR
Trellix	XDR
Microsoft	365 Defender
Palo Alto Networks	Cortex XDR
SentinelOne	Singularity
STELLAR CYBER	**OPEN XDR**
Sophos	XDR
Trend Micro	Trend Vision One
Vendors offering various XDR capabilities that could also meet an organization's requirements include Cybereason, Elastic, F-Secure, VMware and Secureworks.	

Source: Gartner (August 2023)

Stellar Cyber is listed as one of the 10 vendors 2 years in a row

Are We Catching Up?
Key Cyber Security Metrix (2015 to present)

Metrix	2015	2020	2023 -2024
Security tools used	~50	~45	~76
Alerts per day	~5000	~10000+	~50000
Time to triage one alert	~30 min	~20 to 30 min	~10 min
Percentage of alerts not triaged	~60 to 70%	~50%	~30 to 40%
Dwell Time	~146 to 200 days	~56	~10 to 16 days

The appearance of GenAI by late 2023

Good or bad?

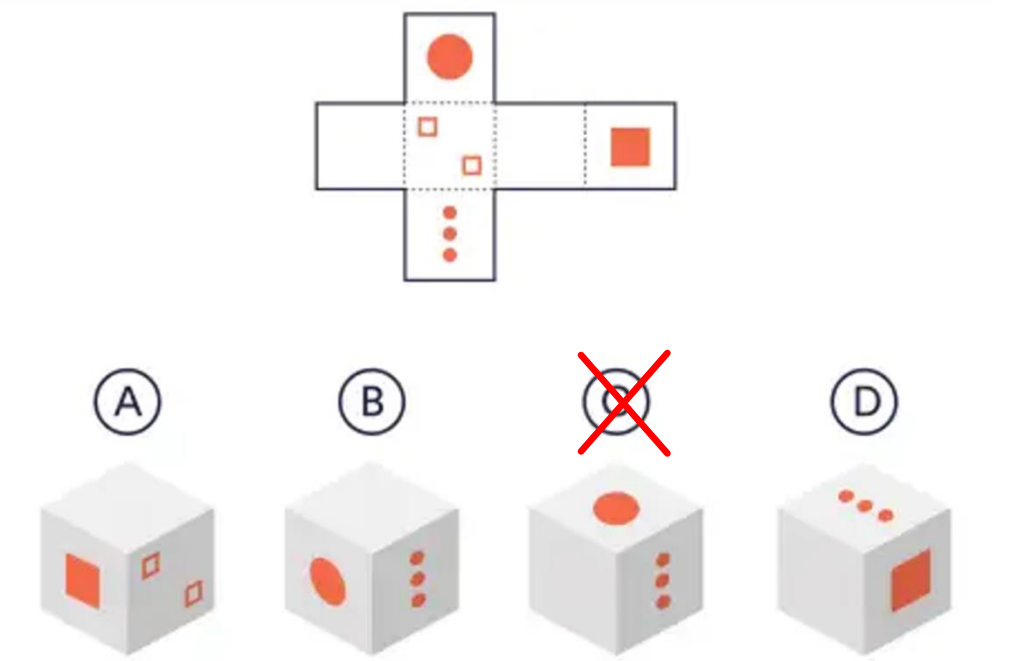
- Will AI solve all the cyber security issues magically?
- Are human still needed?
- Can we fully trust AI?
- Will AI bring more security challenges?

Cyber Skills

	Experienced Security Analyst	Artificial Intelligence
General cyber security knowledge	■■■□□	■■■■□
Recognize patterns	■■□□□	■■■■■
Spot anomalies in large dataset	■□□□□	■■■■□
Make decisions based on their experience	■■■■□	■■■□□
Understand nuance and adversarial objectives	■■■■□	■■■□□
Write scripts and code	■■□□□	■■■■■

Limitation of LLMs

GPT 4.5
(as of March 2025)



What's the correct answer to this test?

The correct answer is **option C**.

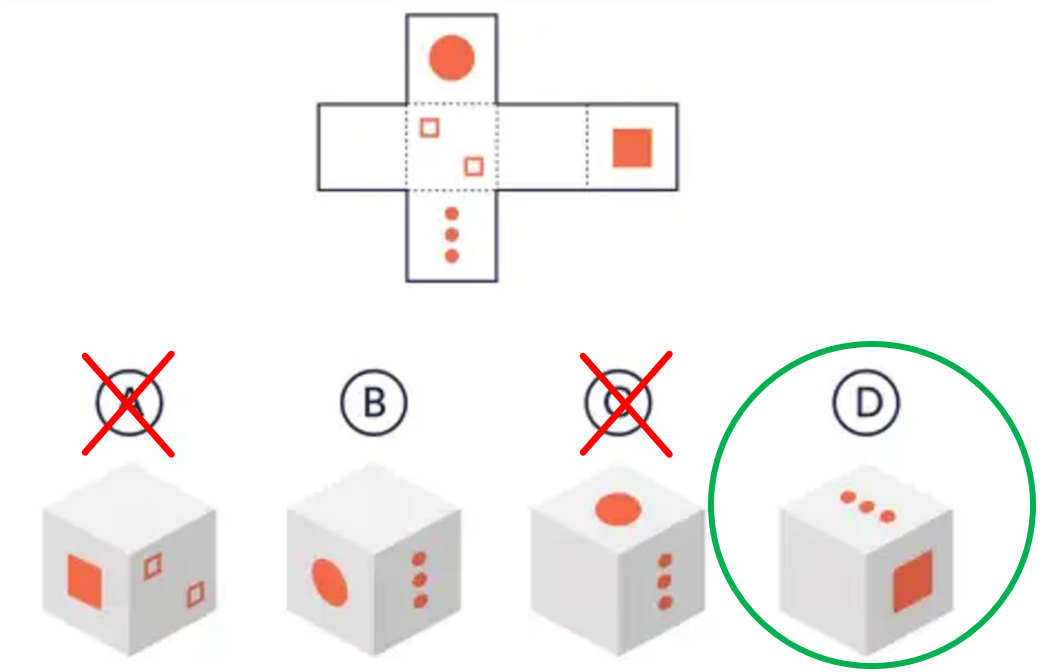
Here's why:

- The unfolded cube indicates clearly which sides are adjacent:
  - The side with a large circle is opposite the side with three dots.
  - The side with three small squares is opposite to the one large square.
  - The blank face (no dots visible on the net) is opposite the face with three dots.

Option C correctly represents the cube, accurately showing the relationship between the faces.

Limitation of LLMs

GPT 4.5
(as of March 2025)



Are you sure?

Let's double-check step by step to be absolutely sure:

...Long detailed explanation...

Final Answer:

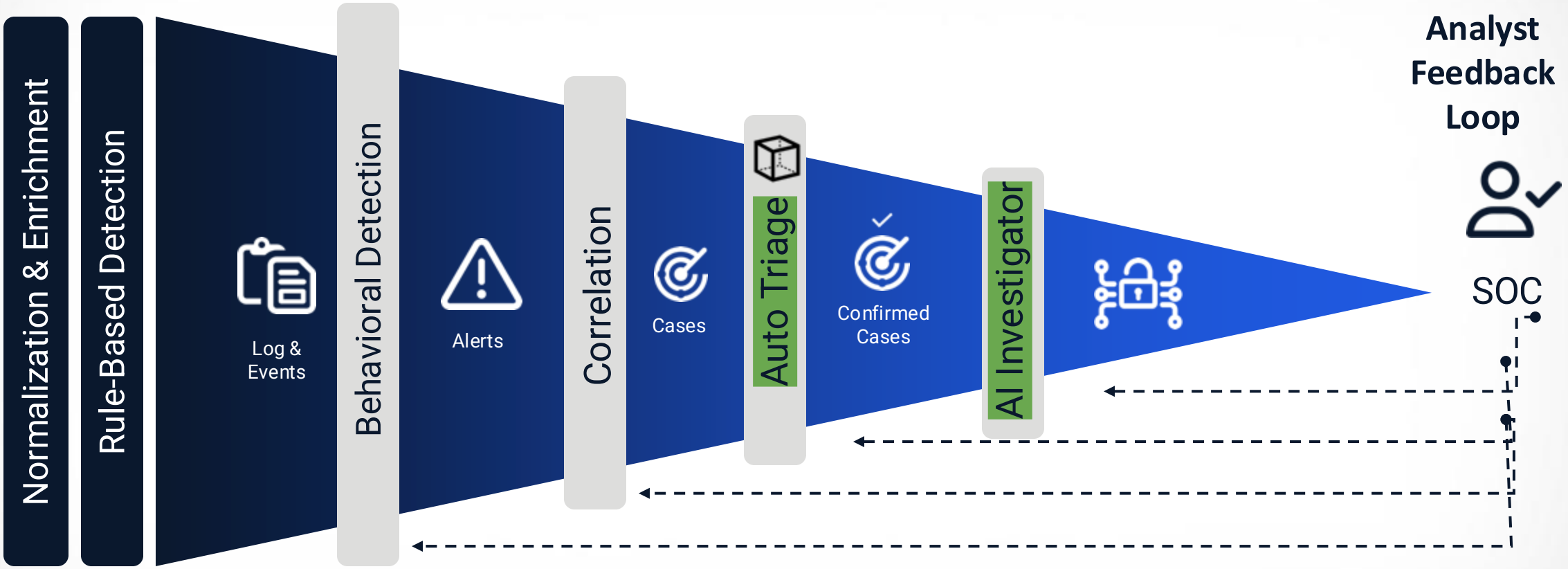
Upon careful reconsideration, the correct answer is indeed:

✅ **Option A**

Thanks for prompting a second look!

Full Cycle Human-Augmented Autonomous SOC

Full-cycle approach merging rule-based detection, behavioral analytics, and automated triage—resulting in faster threat response, reduced alert fatigue, and a truly self-sustaining security operation.



Elevate alert triage by blending human insight with continuous AI refinement
Accelerates Autonomous SOC evolution

Impact of GenAI on Security

- Common Perception: Exploited to create sophisticated cyber attacks, such as deepfakes and automated phishing, intelligently adaptive, learning from every defense mechanism we deploy

- REALITY: **Human Factor is still the number one issue**

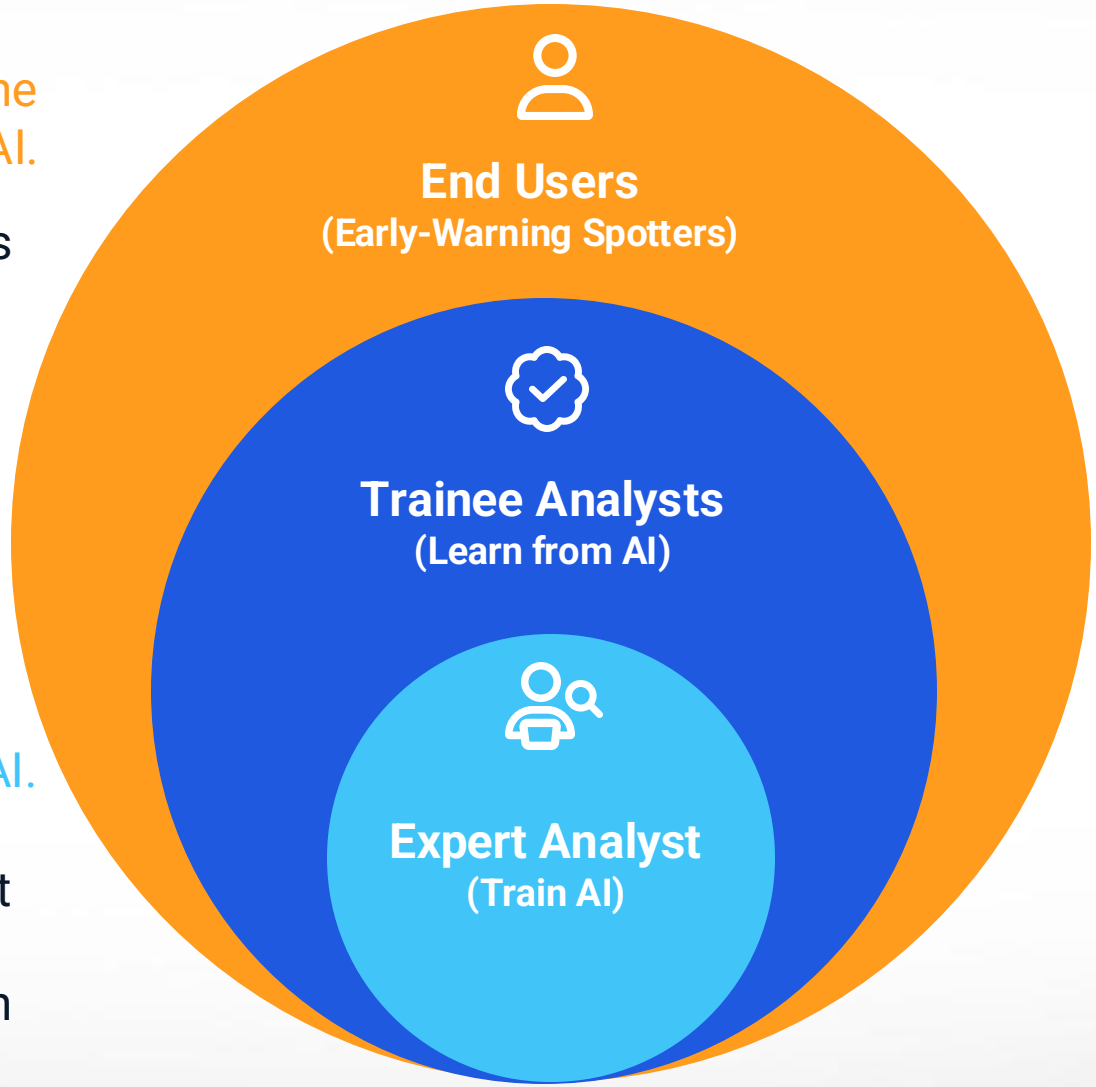
  - One in five people click on AI-generated phishing emails
  - CEO Fraud on the rise: Spear-phishing > Business Email Compromise schemes > Wire Fraud

Autonomous SOC ≠ Humans Replaced

Humans at the core, supported by and collaborating with AI at every critical step.

Provide immediate, frontline threat feedback and context to AI.

e.g. Report suspicious phishing emails to AI



Validate, assist, and teach the AI.

e.g. Provide direct feedback to AI to improve detection

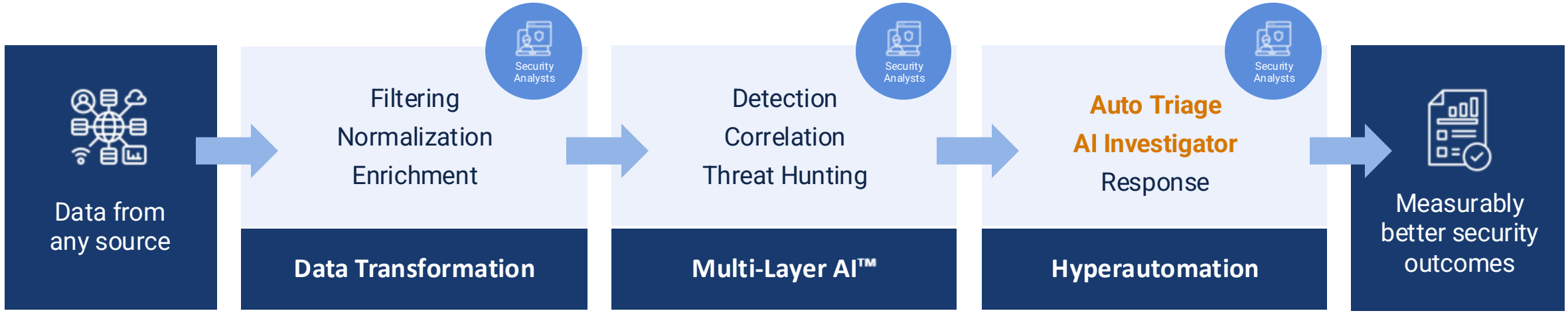
Learning from AI through investigation.

e.g. Guided by AI step-by-step explanations, build intuition around threat actor Tactics, Techniques, and Procedures (TTPs),

STELLAR CYBER®

Our Vision

We are a **full cycle autonomous security operations platform** that empowers security teams to elevate past the limitations and inefficiencies embedded in their security stack.



OPEN • UNIFIED • HUMAN-AUGMENTED

Thank you!

awei@stellarcyber.ai