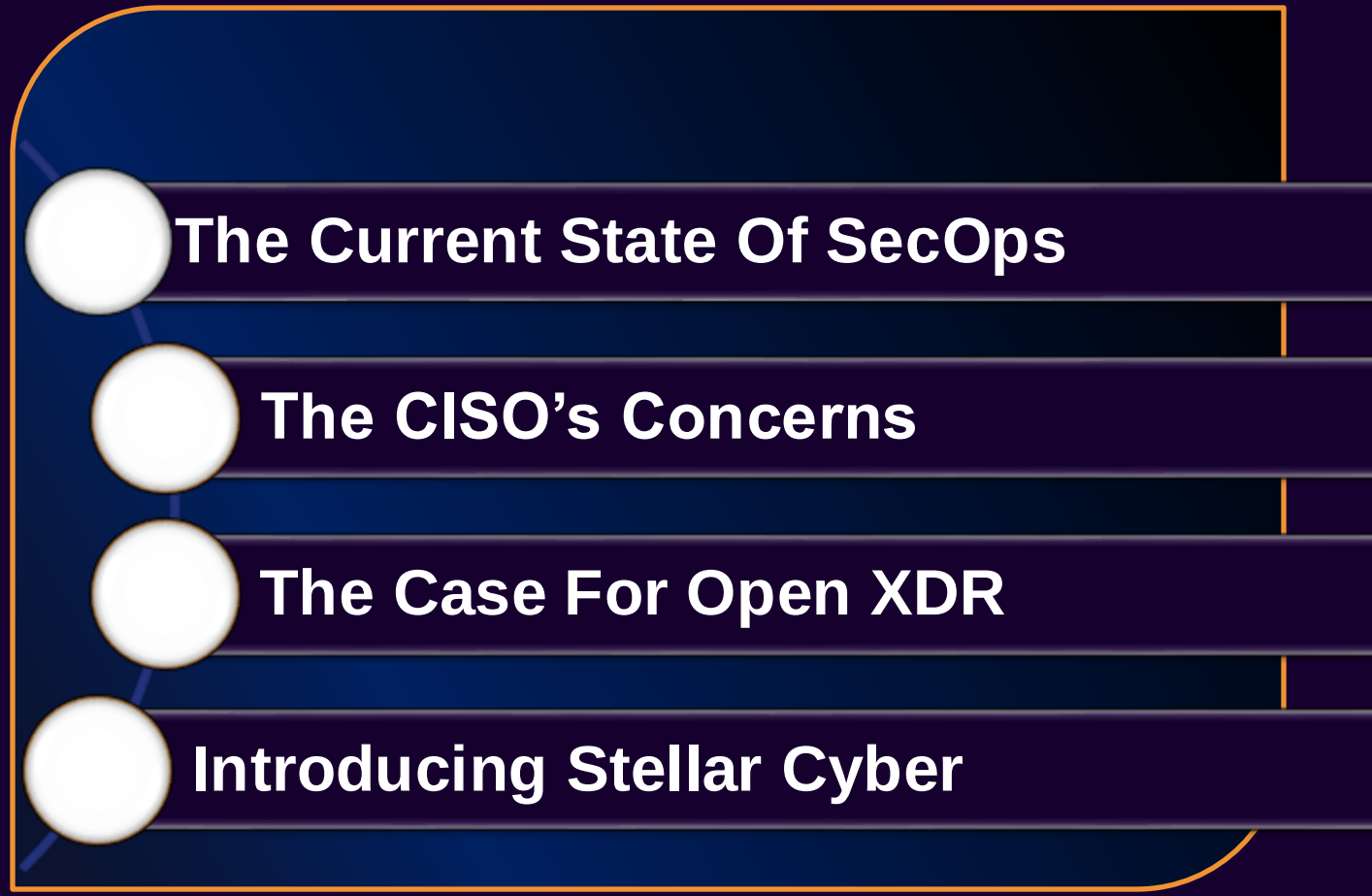
Fighting AI with AI: Achieving Cyber Resilience in the 21st Century

Miri Varbitzky
VP Sales Central & South EMEA

Agenda


The Current State Of SecOps
The CISO’s Concerns
The Case For Open XDR
Introducing Stellar Cyber

The Current State of Security Operations

Alert Overload

63%

Increase in attack surface in past three years

3

Hours spent manually triaging alerts per day

4,484

The average number of alerts generated per day

67%

Percent of daily alerts unable to investigate

STELLAR CYBER

The Current State of Security Operations

The Undeniable Truth

The Current State of Security Operations

Security Tool Explosion Continues

15–20
Small Businesses

50–60
Mid-sized Companies

>130
Enterprises

The CISO's Main Concerns

IS MY SECURITY STACK WORKING CORRECTLY?

ARE THERE ASSETS THAT ARE UNPROTECTED IN MY ENVIRONMENT?

WILL A KEY RESOURCE LEAVE THE TEAM UNEXPECTEDLY?

AM I ALREADY BREACHED AND DO NOT KNOW IT?

AM I MISSING CRITICAL ALERTS?

STELLAR CYBER

Common SecOps Pain Points

Blindspots

Rule Creation

Correlation

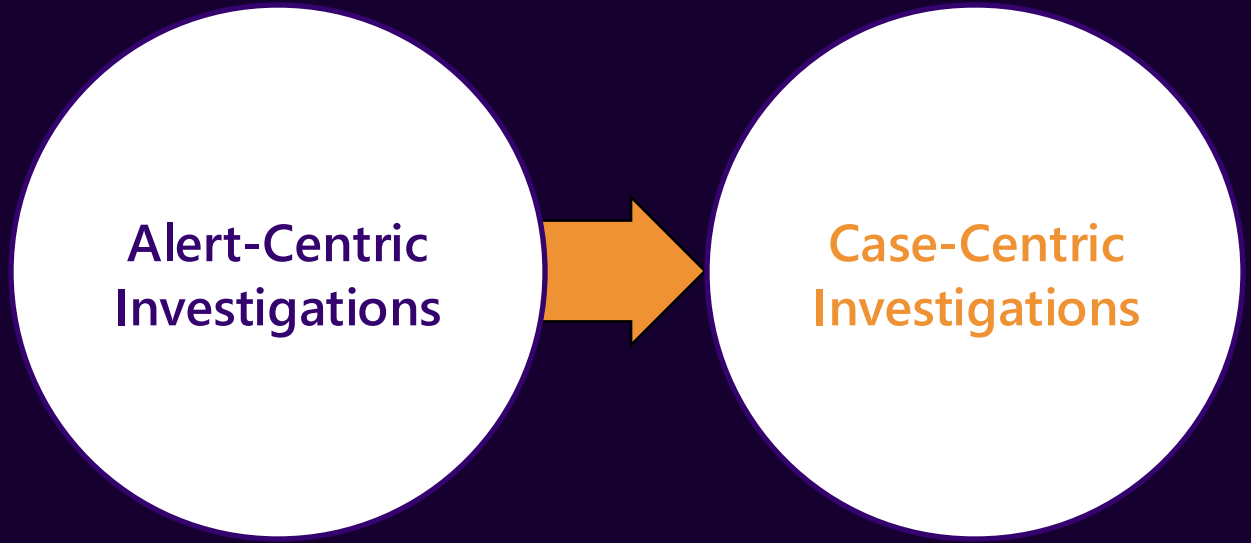
Response

The State of Cyber Security Today

STELLAR CYBER

A Modern Approach to SecOps

The time to evolve security operations is now



Case Centric Investigation

- **Ingest, normalize**, and **enrich** alerts and logs from
any data source
- **Using AI**, cases are **automatically** created, grouping related alerts/events
- Complete investigations and **respond directly from the platform**

A single case could include 50 or more related events.

STELLAR CYBER

Organizations are Replacing Standalone Security Point Tools with Integrated, Multi-product Platforms

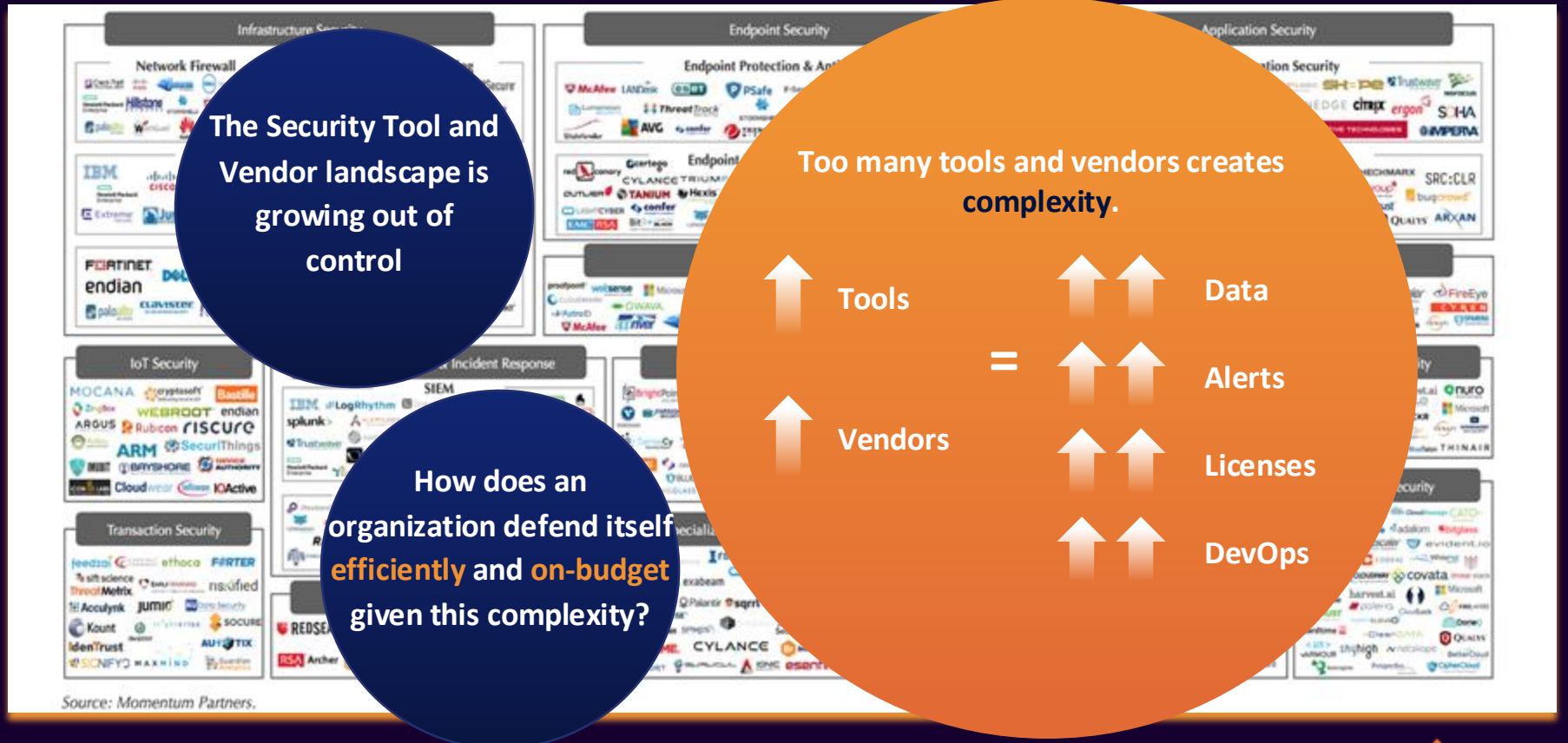
67% want an open suite of products

70% considering XDR platform

Enterprise Strategy Group by TechTarget

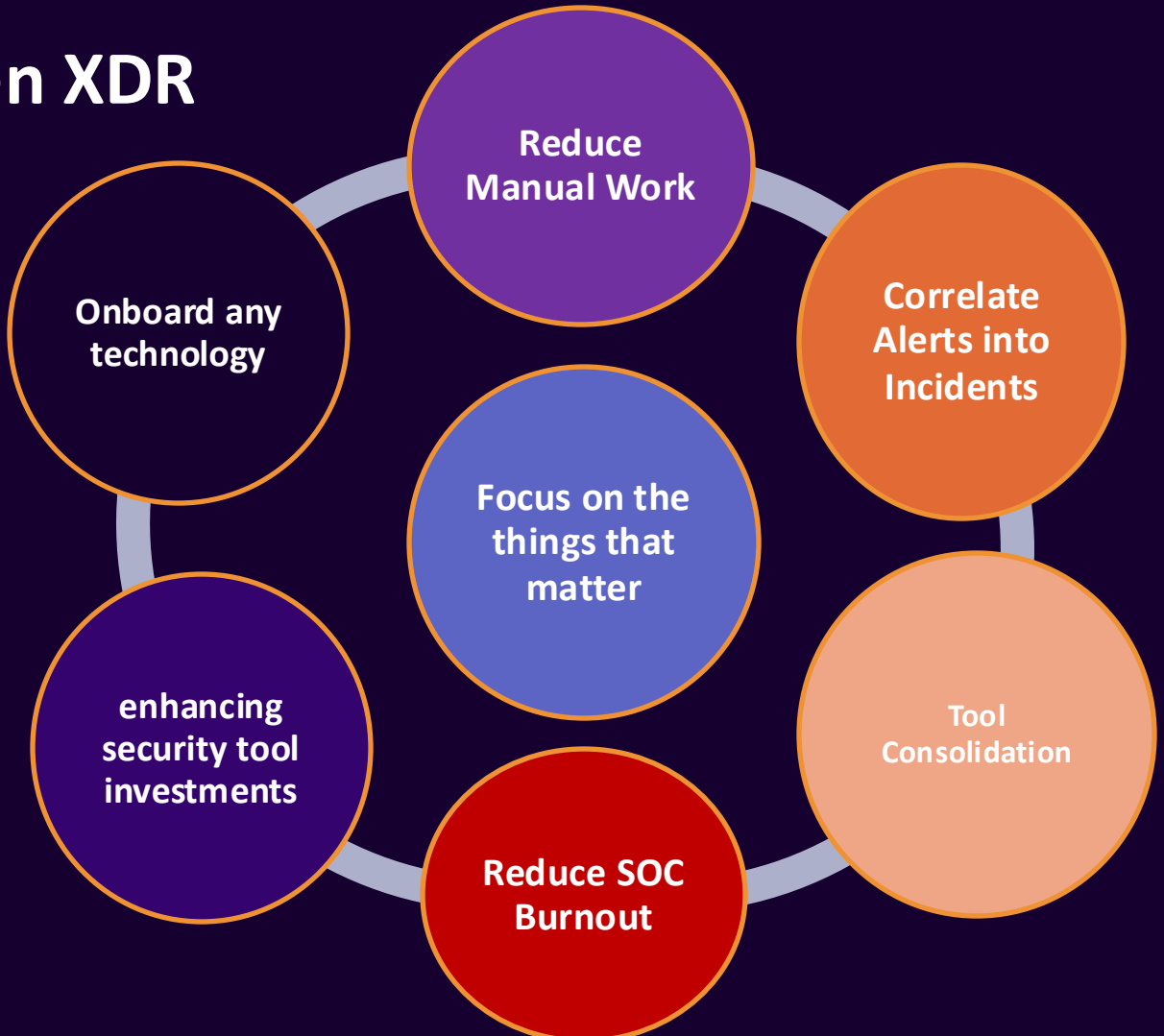
STELLAR CYBER

The Case for Open XDR? The Tool Problem



STELLAR CYBER

Why Open XDR


Reduce Manual Work
Correlate Alerts into Incidents
Tool Consolidation
Reduce SOC Burnout
enhancing security tool investments
Onboard any technology
Focus on the things that matter

Introducing Stellar Cyber

Introducing Stellar Cyber

STELLAR CYBER

Stellar Cyber Driving a Modern Approach to SecOps

Hundreds of Integration Partners

Stellar Cyber Driving a Modern Approach to SecOps

Industry Recognition

Gartner®

2023 XDR Market Guide

2024 NDR Market Guide

2024 Hype Cycle™ for Security Operations

STELLAR CYBER®

STELLAR CYBER OPEN XDR

SIMPLIFIES THE COMPLEXITY OF SECURITY OPERATIONS

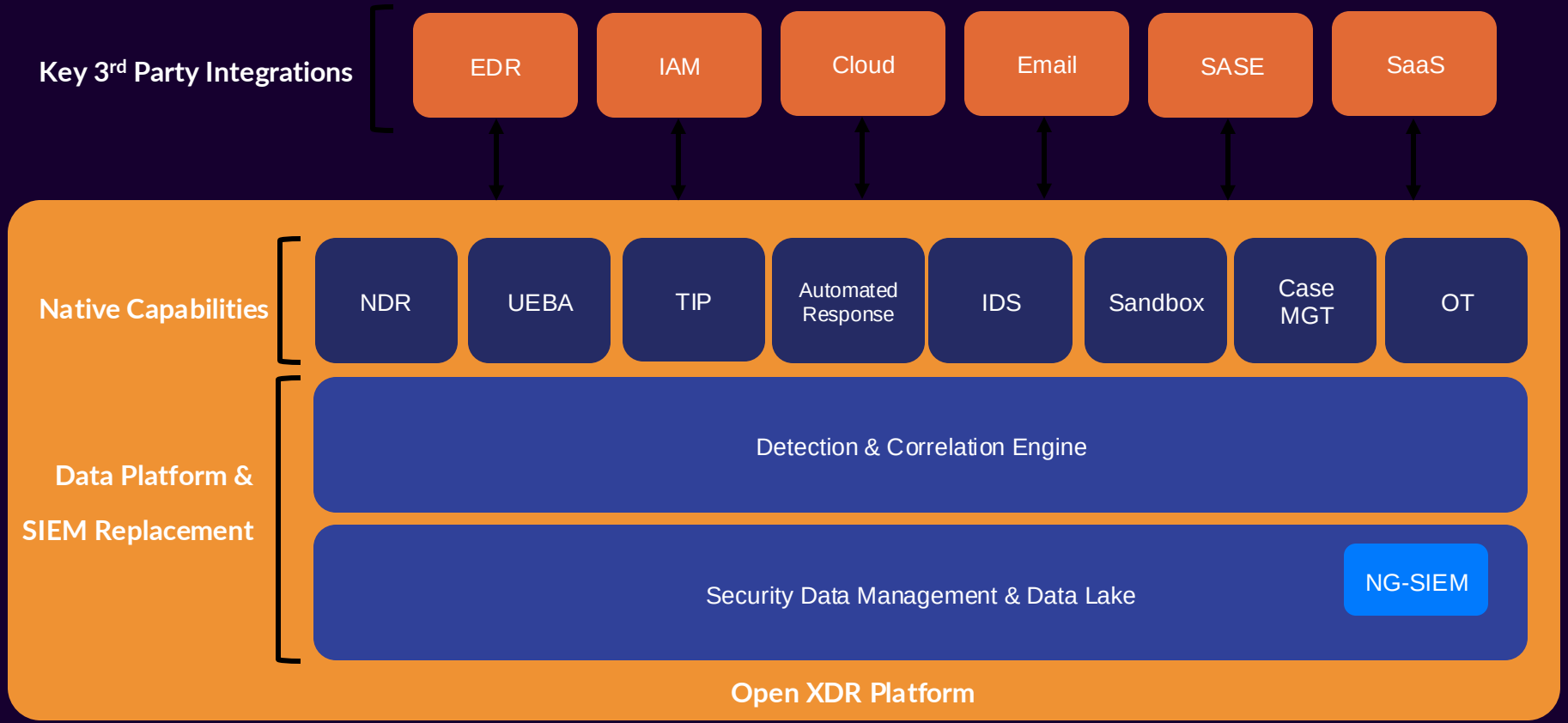
Simply Connect all your existing tools into the Stellar Cyber Open XDR Platform

Automatically Identify and **Correlate** threats using intelligent data analysis

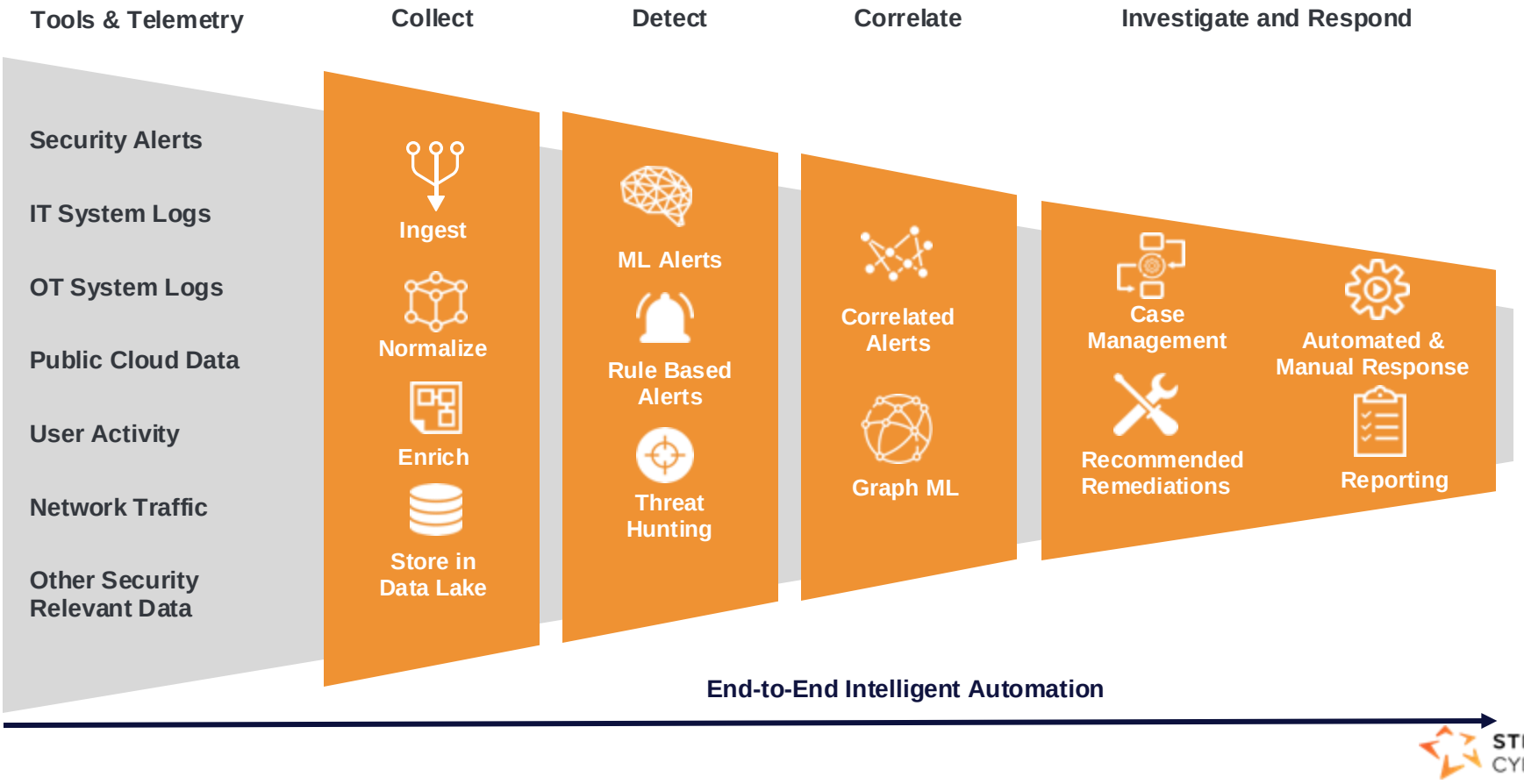
Automate Response and take decisive action fast

STELLAR CYBER

OPEN XDR - Single Platform, Single License



Stellar Cyber Open XDR Platform – Single Platform, Single License



Stellar Cyber for OT Environments

Combining IT and OT security in a single platform gives security teams a permanent advantage over attackers who frequently attempt to exploit weaknesses and vulnerabilities identified in an IT environment to move laterally into an OT environment to carry out an attack, and vice versa.

With Stellar Cyber, security teams can now automatically detect the following:

- Many flavours of SCADA protocols
- SCADA network segmentation violations
- Network attacks
- Malicious or suspicious file transfers
- Anomalous communication
- IT-to-OT breaches

Selected Enterprise Customers

STELLAR CYBER

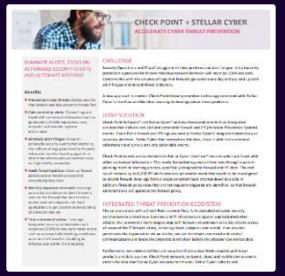
Selected Use Cases

(Technology Partners)

Oracle

Blackberry

Check Point



F5 Networks

SonicWall

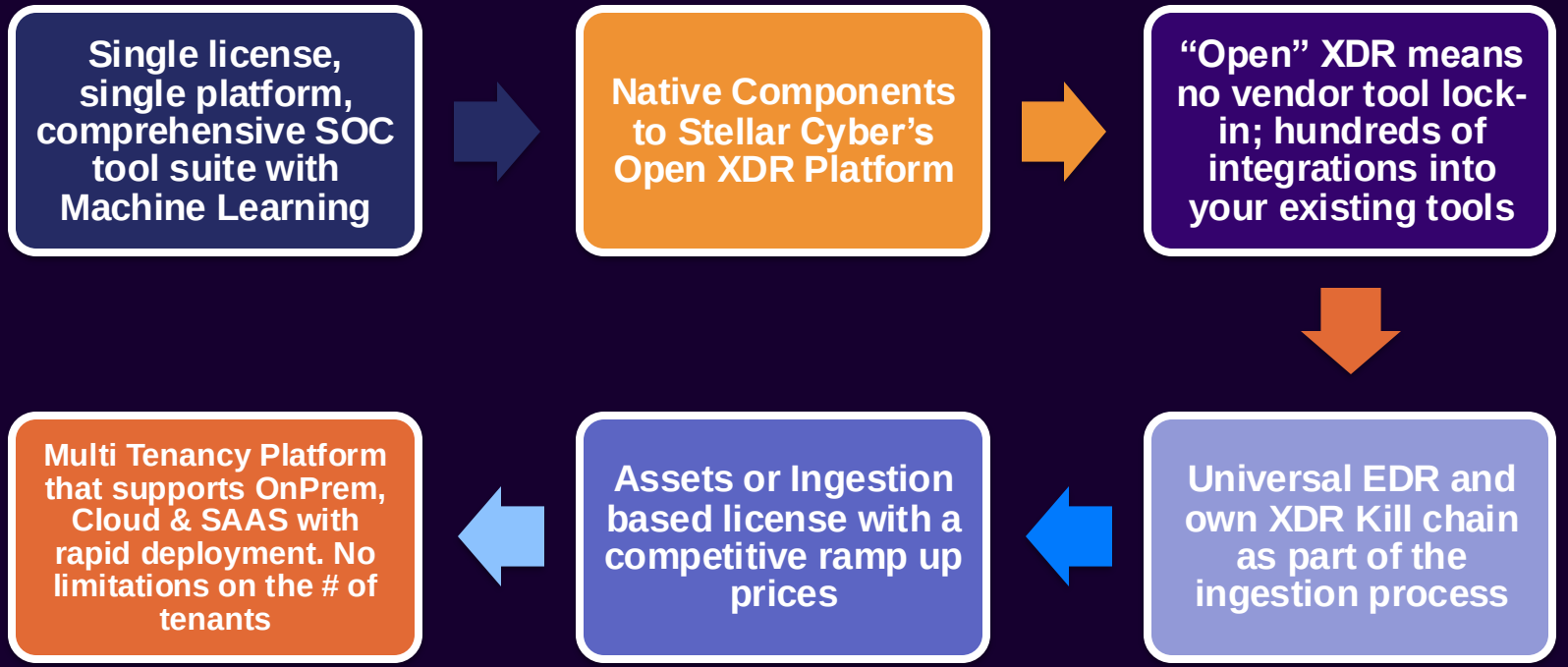
Garland (OT)

Cortex XSOR

ESET

Trellix

Stellar Cyber Key Differentiators



Thank You!

STELLAR
CYBER®