



STELLAR
CYBER®

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

The Current State of Security Operations

The Undeniable Truth



Excessive
Alert
Volume



Complexity
Throughout
the Tech
Stack



Inadequate
Analyst
Capacity



Increased Risk
of Breach



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?



Common SecOps Pain Points



Blindspots



Rule Creation



Correlation



Response



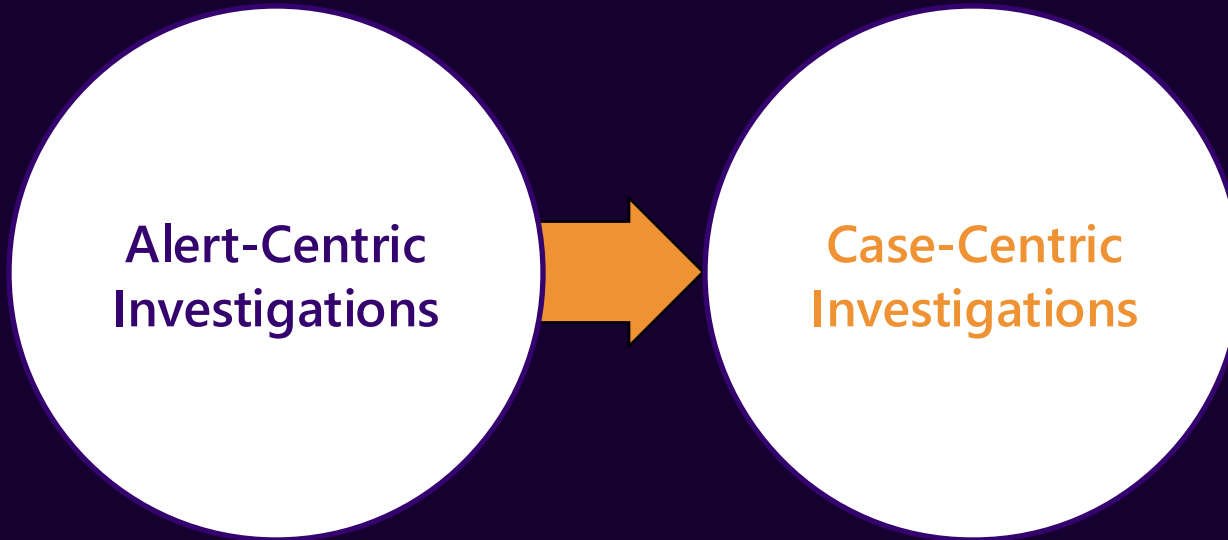
The State of **Cyber Security** Today





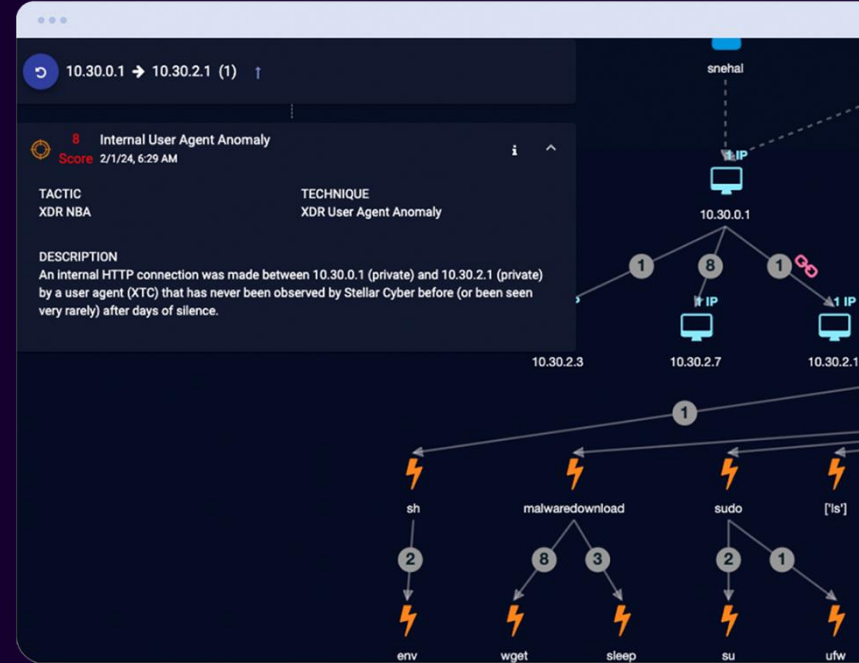
A Modern Approach to SecOps

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.

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

67% want an open suite of products



70% considering XDR platform

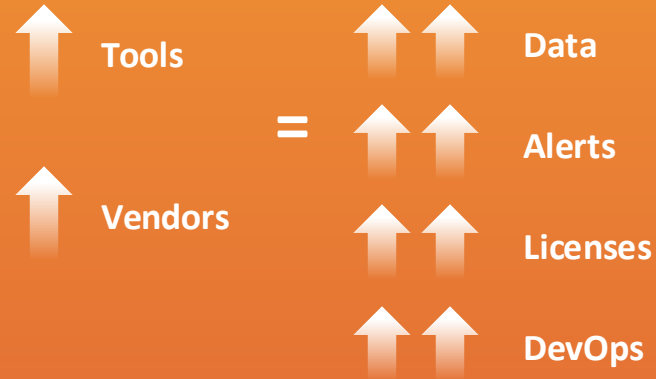


The Case for **Open XDR**? The Tool Problem

The Security Tool and Vendor landscape is growing out of control

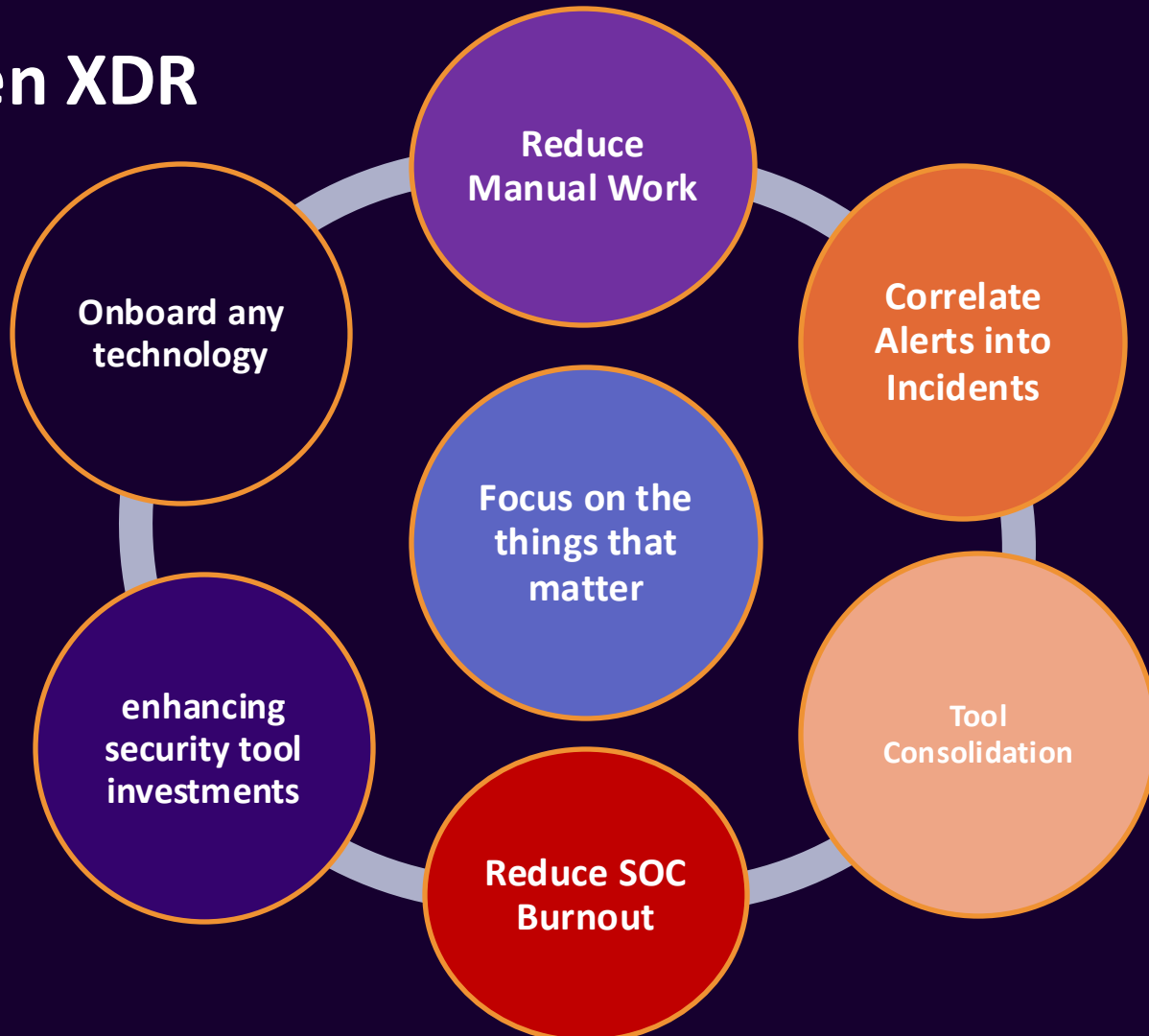
How does an organization defend itself **efficiently** and **on-budget** given this complexity?

Too many tools and vendors creates complexity.



Source: Momentum Partners.

Why Open XDR



Introducing Stellar Cyber

Introducing Stellar Cyber

Single unified AI-driven platform
to detect, correlate, and respond to threats fast.



Collect & Normalize

Ingest, normalize, and enrich security alerts, logs, and telemetry from any product



Detect & Correlate

Uses AI to automatically analyze and correlate collected data to identify cyber threats



Investigate & Respond

Enables your security team to complete effective investigations fast

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 OPEN XDR

SIMPLIFIES THE COMPLEXITY OF SECURITY OPERATIONS

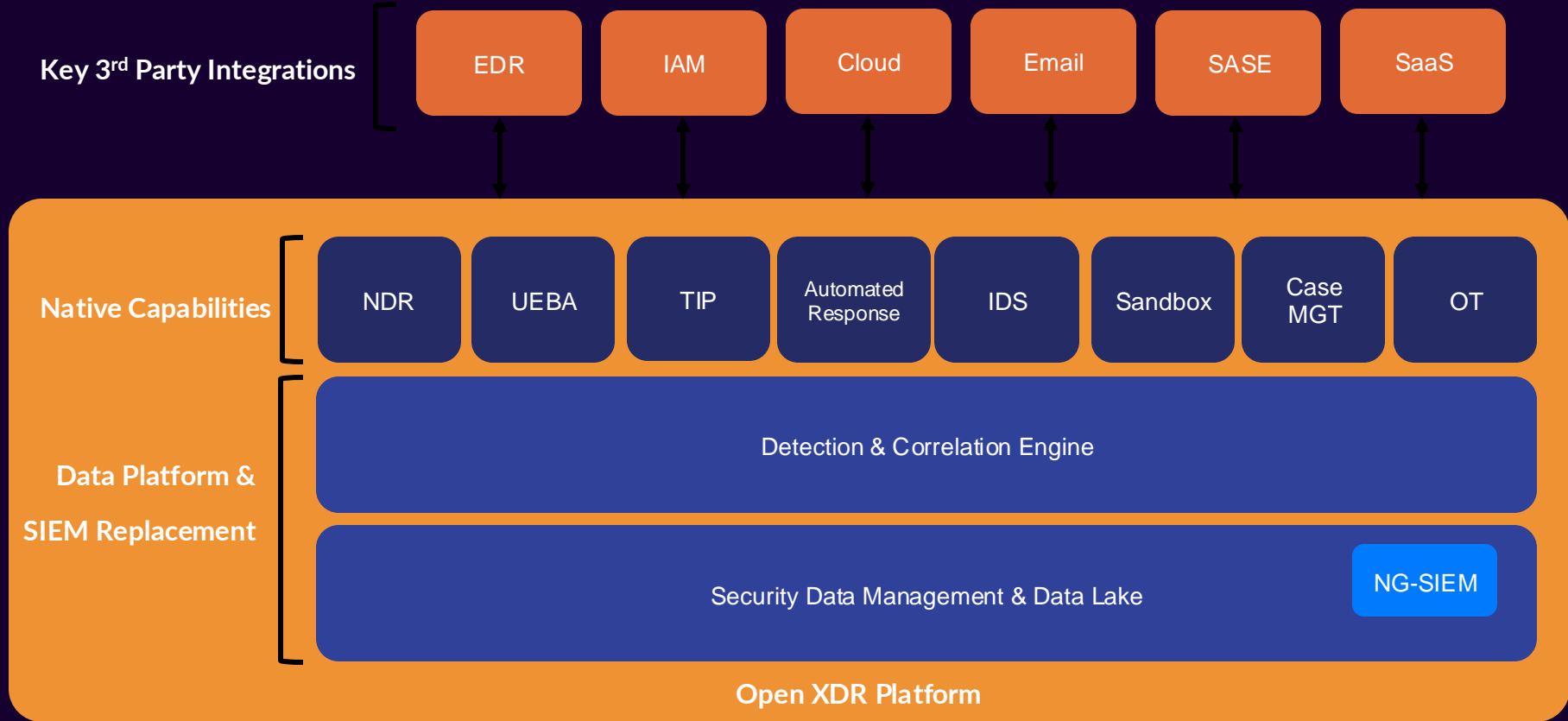


Simply Connect all your existing
tools into the Stellar Cyber Open
XDR Platform

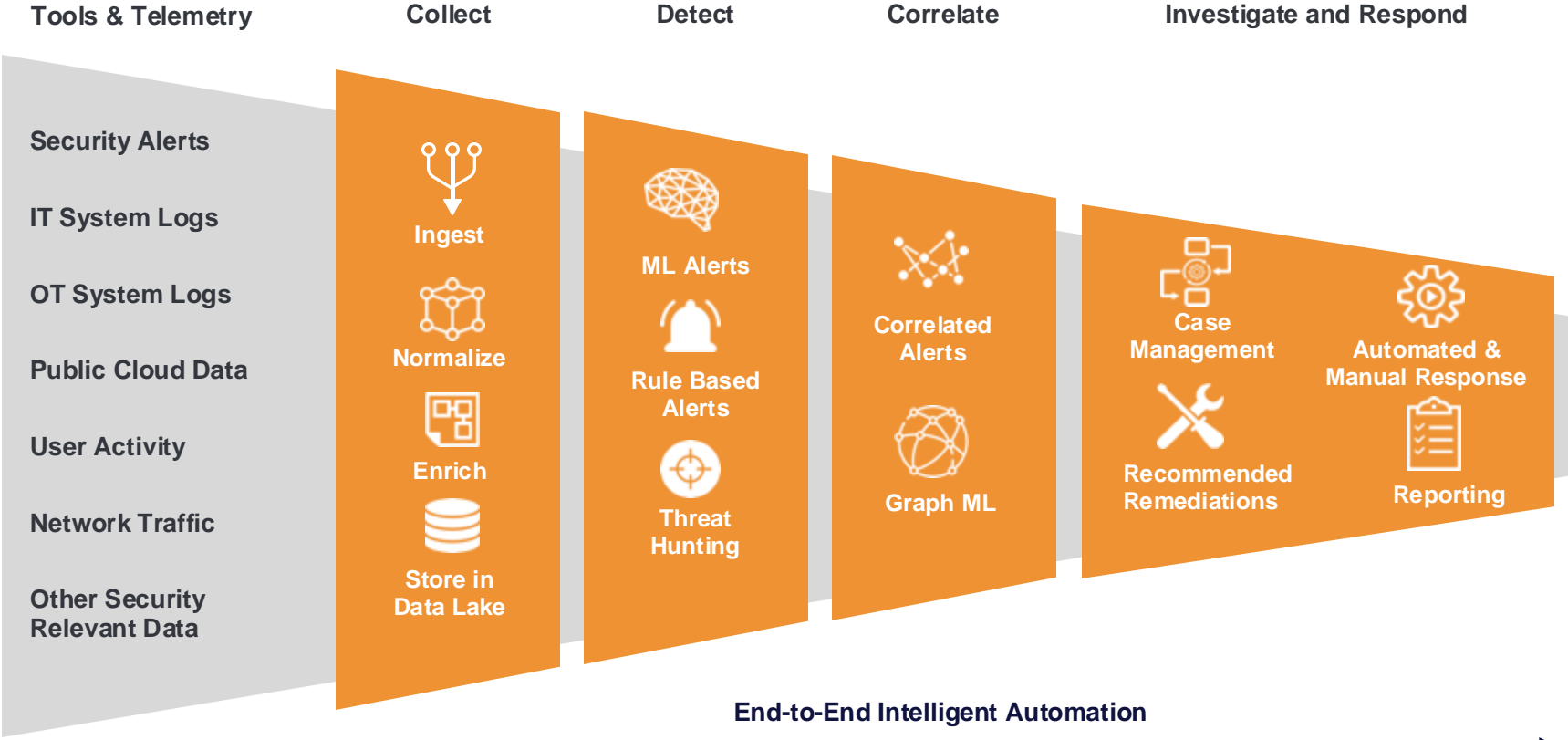
Automatically Identify
and **Correlate** threats using
intelligent data analysis

Automate Response
and take decisive
action fast

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

Enterprise



Financial Services



Education



Government



Manufacturing



Utilities



Selected Use Cases (Technology Partners)

Oracle

Stellar Cyber XDR Report

The report provides a comprehensive overview of the organization's security posture, including a detailed analysis of alerts, a breakdown of incidents, and a summary of response actions. The dashboard highlights key metrics such as the number of alerts generated, the number of incidents identified, and the number of response actions taken.

Blackberry

Stellar Cyber and BlackBerry partner for AI-powered security

Stellar Cyber, a next-generation security operations platform, has partnered with BlackBerry to accelerate the adoption of AI-powered security.

Check Point

CHECK POINT + STELLAR CYBER

Stellar Cyber, a next-generation security operations platform, has partnered with Check Point to accelerate the adoption of AI-powered security.

F5 Networks

Stellar Cyber + F5 Networks

The integration allows for the collection and analysis of network logs from F5 devices, providing a comprehensive view of network activity and potential threats.

SonicWall

Stellar Cyber + SonicWall

The integration allows for the collection and analysis of network logs from SonicWall devices, providing a comprehensive view of network activity and potential threats.

Garland (OT)

Stellar Cyber + Garland (OT)

The integration allows for the collection and analysis of network logs from Garland devices, providing a comprehensive view of network activity and potential threats.

Cortex XSOAR

Stellar Cyber + Cortex XSOAR

The integration allows for the collection and analysis of network logs from Cortex XSOAR devices, providing a comprehensive view of network activity and potential threats.

ESET

Stellar Cyber + ESET

The integration allows for the collection and analysis of network logs from ESET devices, providing a comprehensive view of network activity and potential threats.

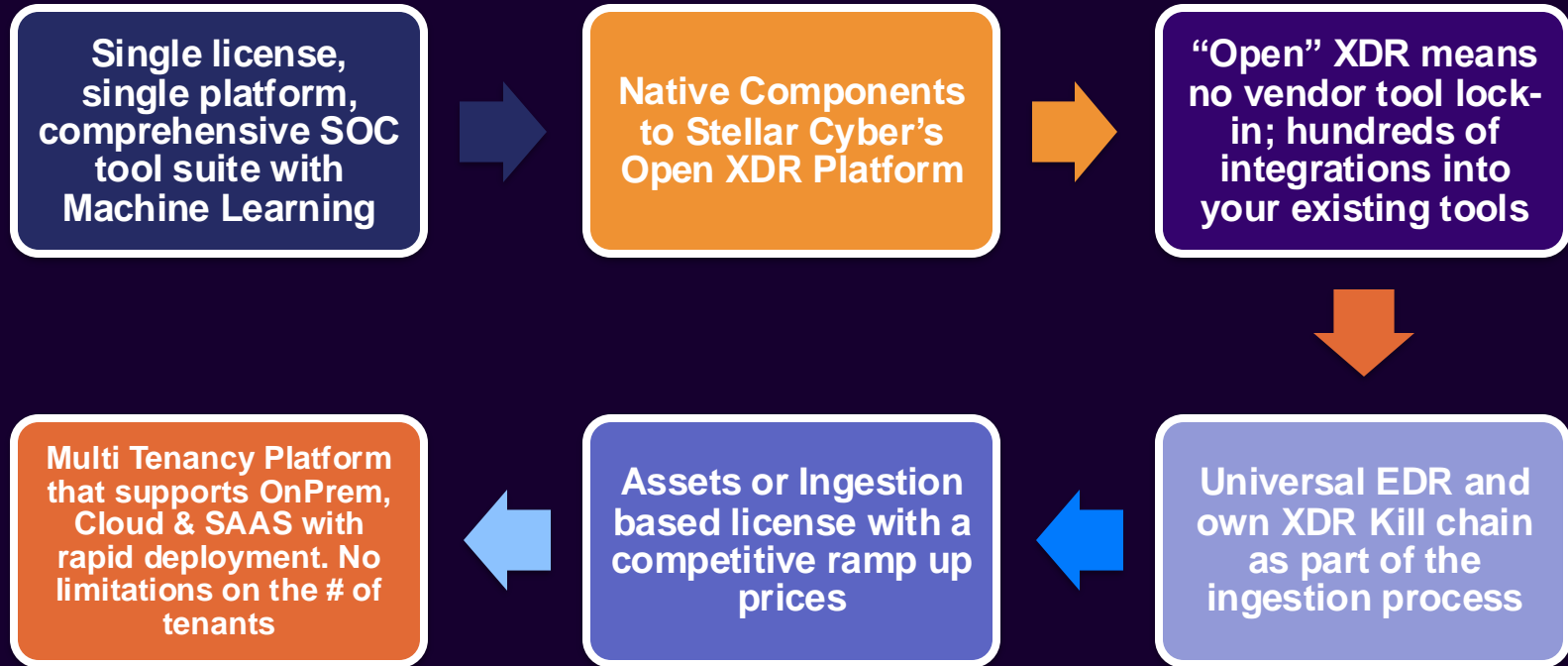
Trellix

Stellar Cyber + Trellix

The integration allows for the collection and analysis of network logs from Trellix devices, providing a comprehensive view of network activity and potential threats.



Stellar Cyber Key Differentiators



Thank You!

