

## 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

The average number of alerts generated per day

4.484

67%

Percent of daily alerts unable to investigate



## The Current State of Security Operations

The Undeniable Truth

Ç Excessive Alert Volume

**{}}** 

Complexity Throughout the Tech Stack <mark>⊘</mark>×

Inadequate Analyst Capacity Increased Risk of Breach

4



### The Current State of Security Operations

Security Tool Explosion Continues

# 15-20 50-60

Mid-sized Companies

>130

Enterprises

STELLAR CYBER\*

**Small Businesses** 

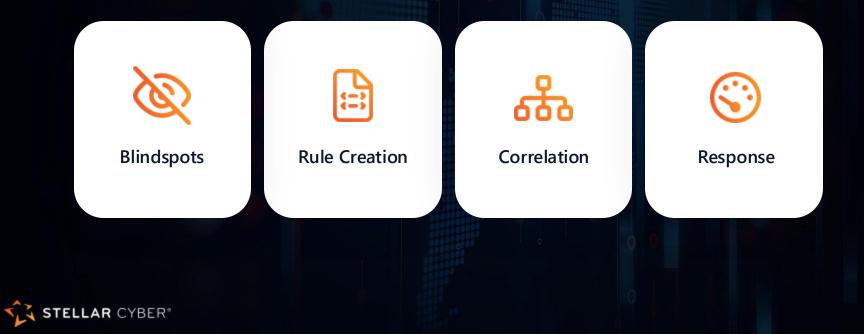
5

## The CISO's Main Concerns





### **Common SecOps Pain Points**





#### The State of Cyber Security Today



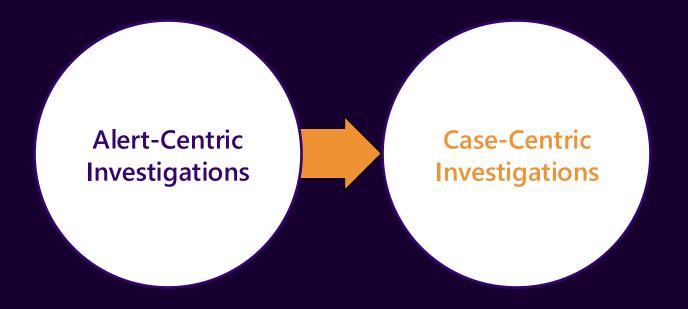






## A Modern Approach to SecOps

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



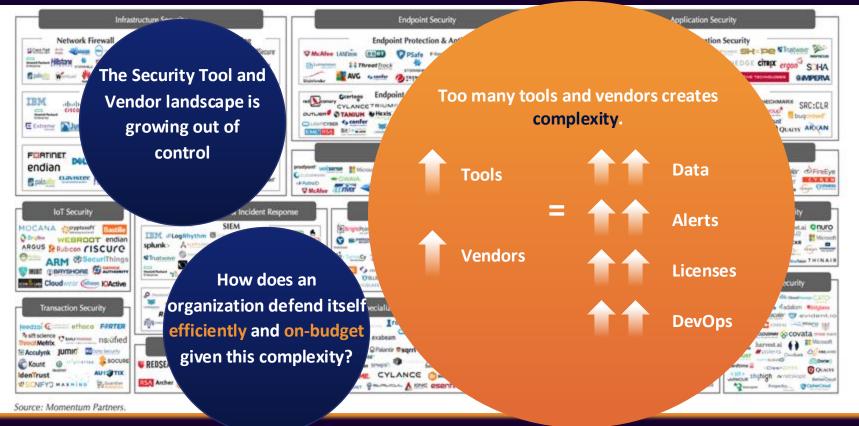
## 70% considering XDR platform



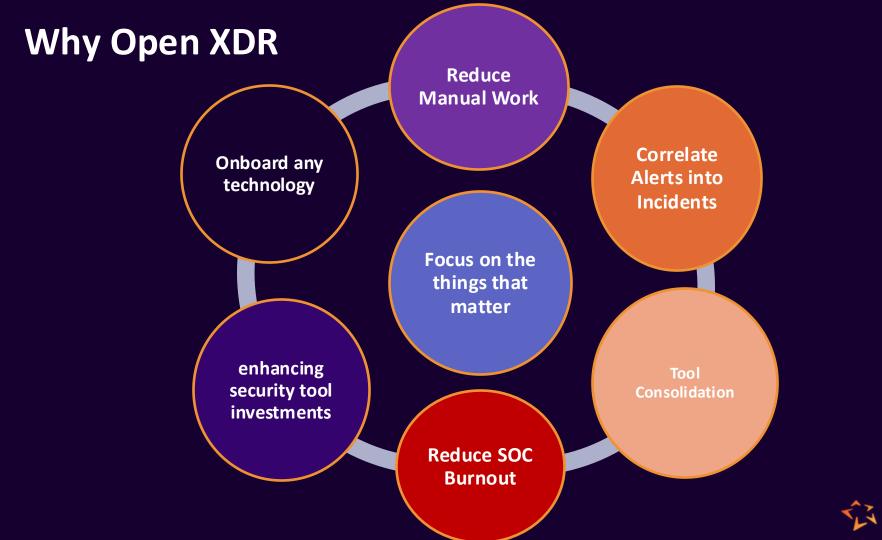




## The Case for Open XDR? The Tool Problem







# **Introducing Stellar Cyber**



▶RS:/0211TR /0 ▶RS:/0211TR /0

## **Introducing Stellar Cyber**

## Single unified Al-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<sup>™</sup> 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

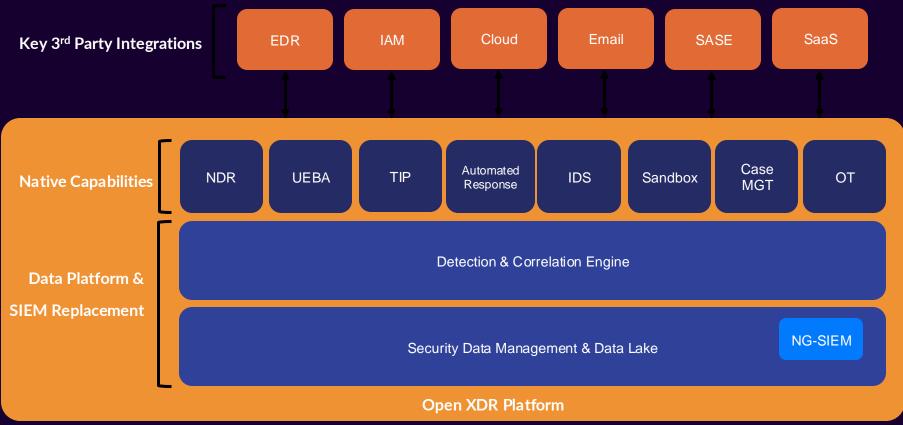
#### **Automate Response**

and take decisive

action fast

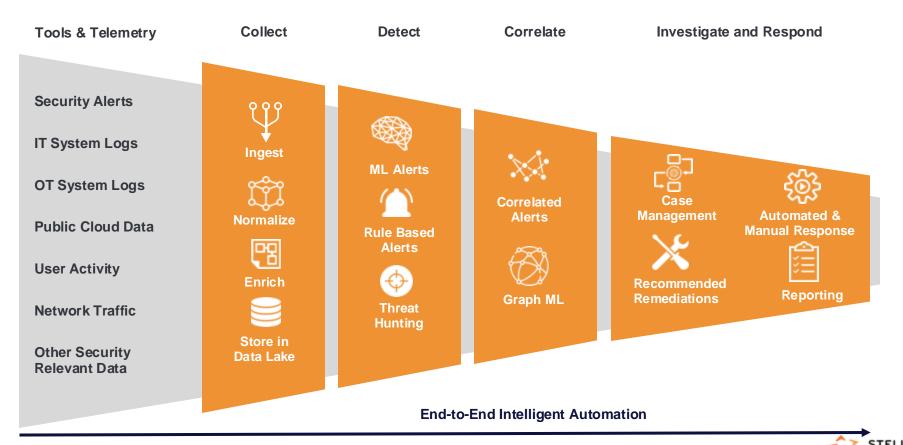


## **OPEN XDR - Single Platform, Single License**





## 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**





## **Selected Use** Cases

(Technology Partners)



Oracle		Blackberry	<b>Check Point</b>	
<text><text><text><list-item><list-item><list-item><list-item><list-item><table-row><table-cell></table-cell></table-row><table-row><table-cell><table-cell></table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row><table-row><table-cell></table-cell></table-row></list-item></list-item></list-item></list-item></list-item></text></text></text>	Image:	Cyberson Stellar Cyber and BlackBerry partner for Al-powered security operations platform, has partnered with BlackBerry to accelerate the adoption of Al-powered security	<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	
F5 Netw	orks	SonicWall	Garland (OT)	



Imperi, normalize, and annoh all security data including analysismi, natwork, and could and data site a single repositivy.
 Automatically detects and constitutes alors, single appropriate yorld metables alors, any property multi-metables alors, anyping driven by machine teering.

contenties freed mestigations a writing with contential data and unstated incidents.

 Coharood violidity reduces the roll of demaging leases.
 Damatic honese in security analysis' productivity and efficiency Fedure stacker deal time, wormany stack impact

CORTEX XSOAR

## Stellar Cyber + SonicWall 8 SOLUTION AT A C **ESET**

eser Ideanced Thread Datason

Subol Business Date 15

ESET Benefits

STRLAR

CYBER"

Stellar Cober Benefits

	STELLAR CYBER'	GARAND			
	Open XDR Platform	Network Visibility			
GLANCE of Second Se	<ul> <li>Ingelt's convertings, end enrobus of point security data, including OC andiputes, serving, hold, and point as single resolution, reading any DED.</li> <li>Sing a point of some data data data sequere data for a single account data data sequere data for the main account data data to account data for a main data data to account account data for a main data data to account sequere data for a main data data to account security determine.</li> <li>Provides accounted and main data points and/other</li> </ul>	<ol> <li>Providen SO/D: particular Software (Section Prima descept particular Software) (Section Prima and Prima and Prima Prima Prima particular software) (Section Prima particular software) (Section Prima particular software) (Section Prima Prima Prima Prima Prima Prima Software) (Section Prima Prima Software) (Section Prima Prima Software) (Section Prima Prima Software) (Section Prima Software) (Section Prima Prima Prima Prima Prima Software) (Section Prima Software) (Section Prima Prima Prima Prima Software) (Section Prima Pri</li></ol>			
	Benefita	Benefits			
No a ring e latara l'Arr distante ringiling condating del restaring del restaring	Enhanced validity releases the risk of damaging trench     Damartic increases in security analysity polasticity and ethosing     Paulue structure deal time, minimizing ethnic input	Complete visibility regardless of the native architecture constraints     Police product natives, mandating to scale are provided natives, mandating of the seq product or strange in underlying often Records complete particular of XMP and The			
doorait Britstolar Laithtean Jastinet	<ul> <li>Imprive ROI of your soluting security stack assestment is IT and OT</li> </ul>	Bolar probats • Zen harbean adazriptan fee			
dina,	STELLAR CYDER"	www.statheriphet.al ( asterdist			

CYBER'	New source the region and position?			
Open XDR Platform	Network Visibility			
spectr, normalizer, end ancidera ell pro- mescritri dari, incluídez QC existences, norman, la del part de la collador manchine, indexise granno (ECE) esta paramitter con el canolador alcini en a paramitter con el canolador alcini en a paramitter con esta de la collador de destator en paramitter con esta con el consolito, la collador de la collador de la collador esta paramitter en la collador de la collador esta paramitter en la collador de la collador esta paramitter esta collador de la collador esta esta o maní-free	<ul> <li>Provide 2055 scraphters starter's existing strengts threads 15470 (Start Access Threads address at Machine Inselfs);</li> <li>Optimise strengts manufacture phares programme sharts Threads Theorem (Start Access Strength and Start Provide Start Strength Access Start and Address Testing Access Start Access and Address Testing Access Access Access (Start Start Access Access Access Access Access Control Start Access Access Access Access Access (Start Access Access Access Access Access Access Access Access Access Access Access Access Access Access Access Access Access Access Acce</li></ul>			
Benefits	Benefits			
Orberted sinklify reduces the risk of damaging based. Descriptions is peoply analysis' production of the second strategy based antitude desk from, minimizing strain langues result inputs regione RFO at junc exciting executing strain mentment in IT and GT	Complete visibility regardless of the setwork architecture usuarization.     Further ground nations maintening to state up to any sparse architecture is underlying of statements Reduce averaged stated or maintening through samplete particulation of SAP and Passlel Botter grounders     Taminations subscripting feas			
STOLAR				

Т	rel	li	x			
-				-		
	Trellix and Stellar Cyber Joint Solution					
About Stellar Cyber	In today's dynamic cyberaecurty landscape, organizations field increasingly periodicated threats that reacting advanced toda and increasingly					
Station Cyber General a Realitie, easy to use, attractive accurity spectrum protection, engowering team security seams to take control of their security seams in take NAC- SIMA NDD, OLBA, TO YMA LDS, and metricipent automation, Station Cyber seamines investigation methodes	Insports, and Insighton By containing Table wedgets success, include catarians to warm with three contained to include the device of national warms, induced price allow a sector bar balance and a contained warms that data and to the table of balan participes, balance does not contain contains, contained and the table and balan wards projektion to the balance or several and table tables and table and and a participes to balance or several and tables and the balance of an application. The balance or several and tables categories participes to balance through there capabilities and balance data categories and an application to execute condense to the balance data categories to investigate security condense to the balance data categories to investigate					
Androg down attacker dwell time while involutions security analyst productivity	This is precisely what the Stellar Cyber SecCys, Plantoni delivers, With Stellar Cyber, you can ingest data from any data source into the plantoni where automated inomalization, processing, and threat committion occur.					
About Trellix	automatically					
Palitic is redefining the future of observation to with its even and	Stallar Cyter SecOps Hatlum					
native extended detection and response (XSR) pratform, helping organizations to pain confidence in	Ten botten	Links	Detect	Canadama	manifugate and Temporal	
the protection and realitation of their operations. Thelia and its	Trellix		2	-	and the second s	
partner ecolytism, accelerates innovation through intertime teaching advantation, ampointering over 40,000 customers with firing accurity	Kenselig Islams If Barlans Logis 24 Tgolans Logis Public Group Gala Galactic Ratific Vice Autority Websath Ratific Other Angelig		={i 0 i	1.1	×	
Learn More	Annual test					
Contact your Trelle representative or channel partner for more information, or your and	hater Berefits in	Lube:				
		intry tre	ands "line of	sight" visites	lly scross the arrive att	



## **Stellar Cyber Key Differentiators**

Single license, single platform, comprehensive SOC tool suite with Machine Learning

Native Components to Stellar Cyber's Open XDR Platform



"Open" XDR means no vendor tool lockin; hundreds of integrations into your existing tools

Multi Tenancy Platform that supports OnPrem, Cloud & SAAS with rapid deployment. No limitations on the # of tenants



Universal EDR and own XDR Kill chain as part of the ingestion process



# Thank You!

