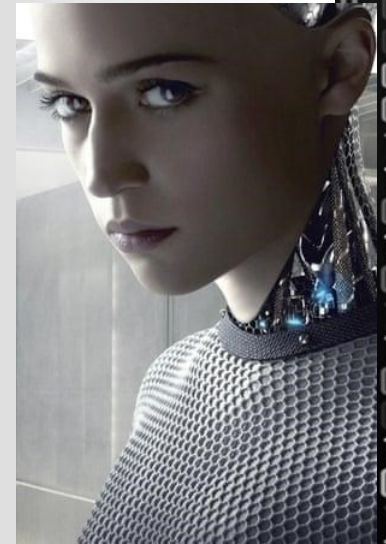




Está disposto a Sacrificar a Rainha?

Paulo Vieira- pvieira@paloaltonetworks.com





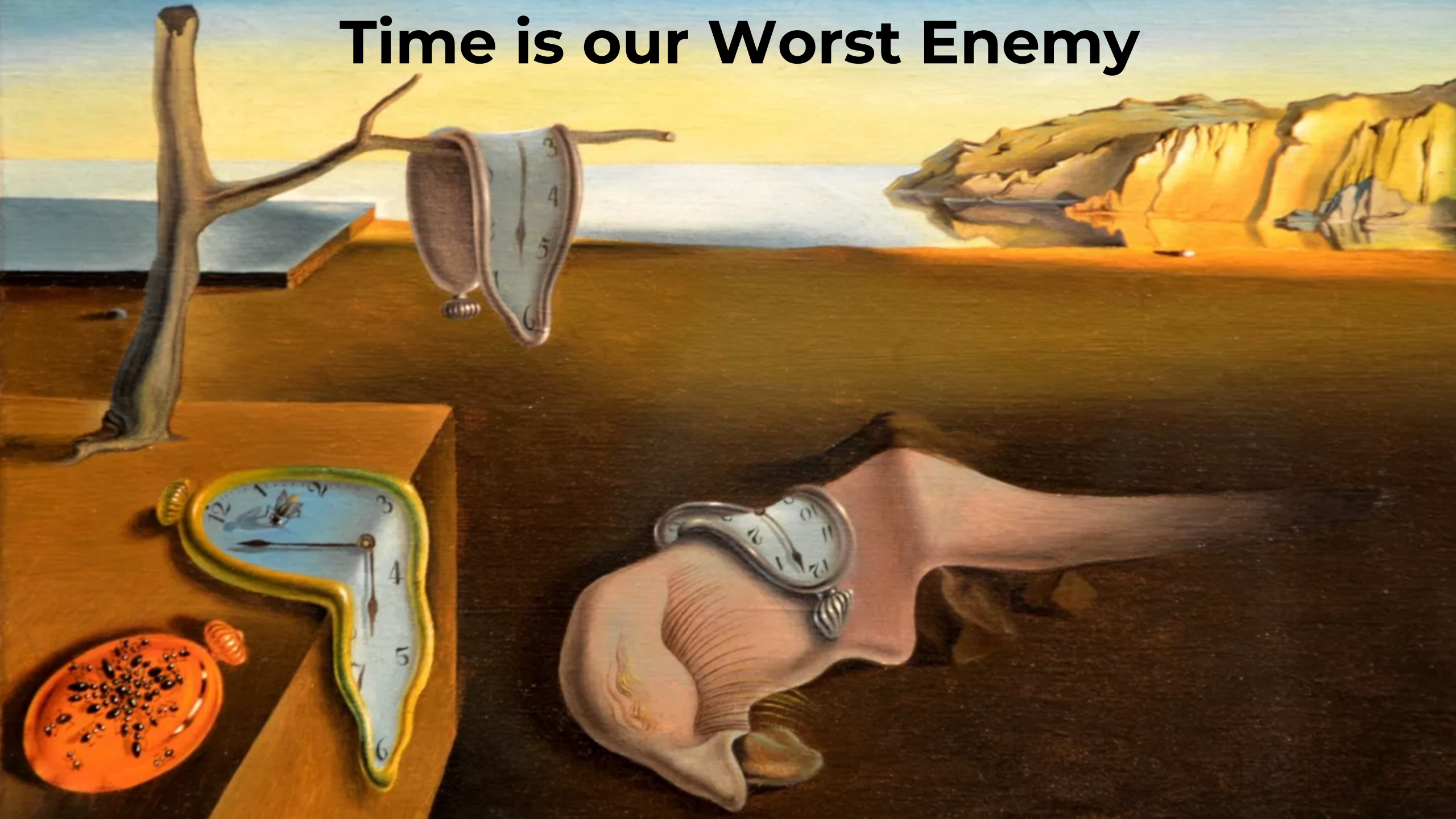
ALPHAZERO == vs == STOCKFISH

Sacrificing the Queen





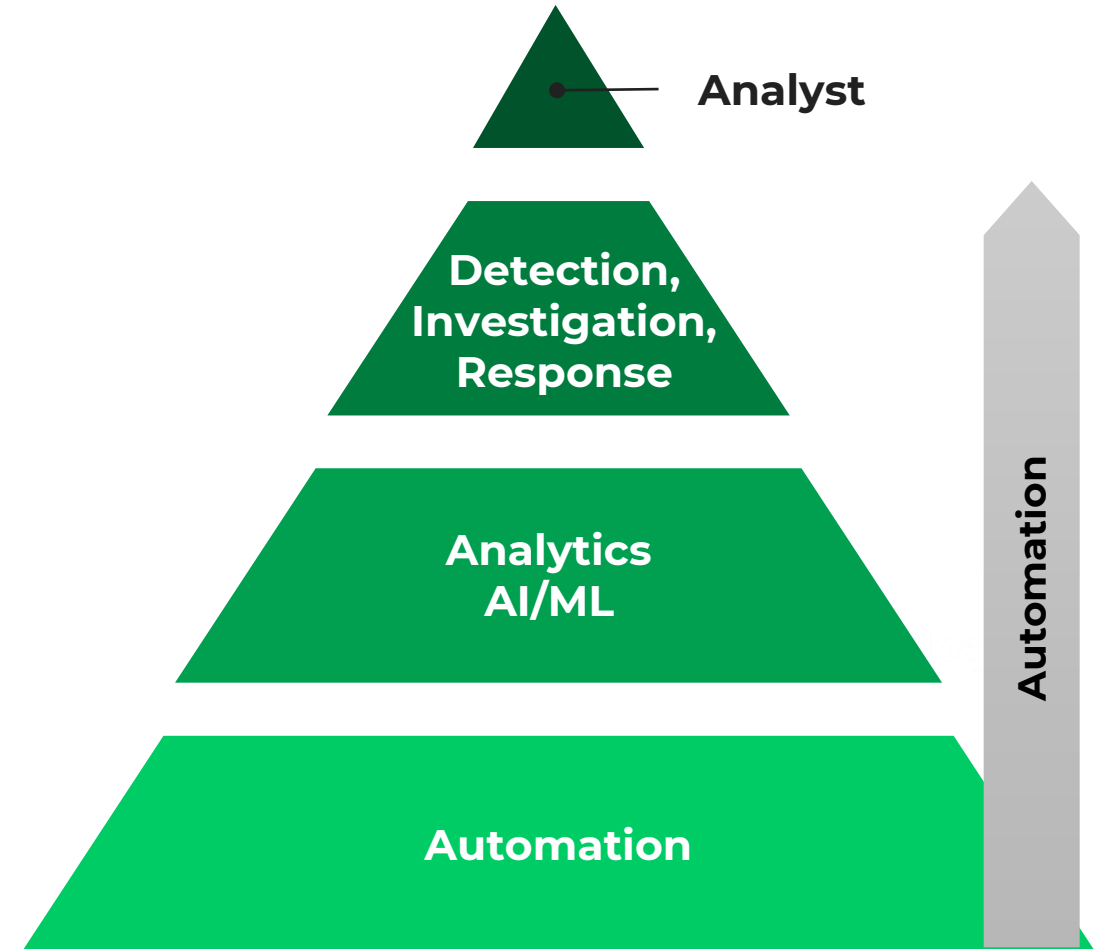
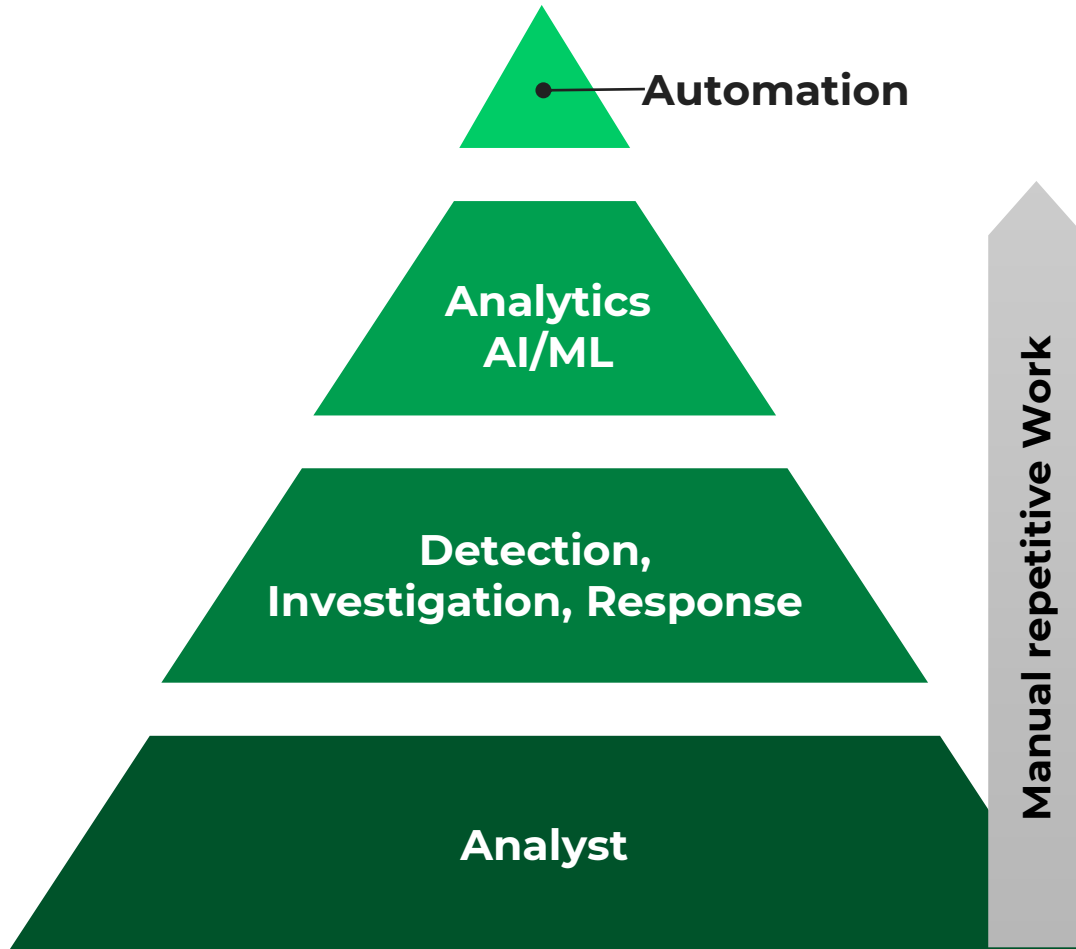
Time is our Worst Enemy



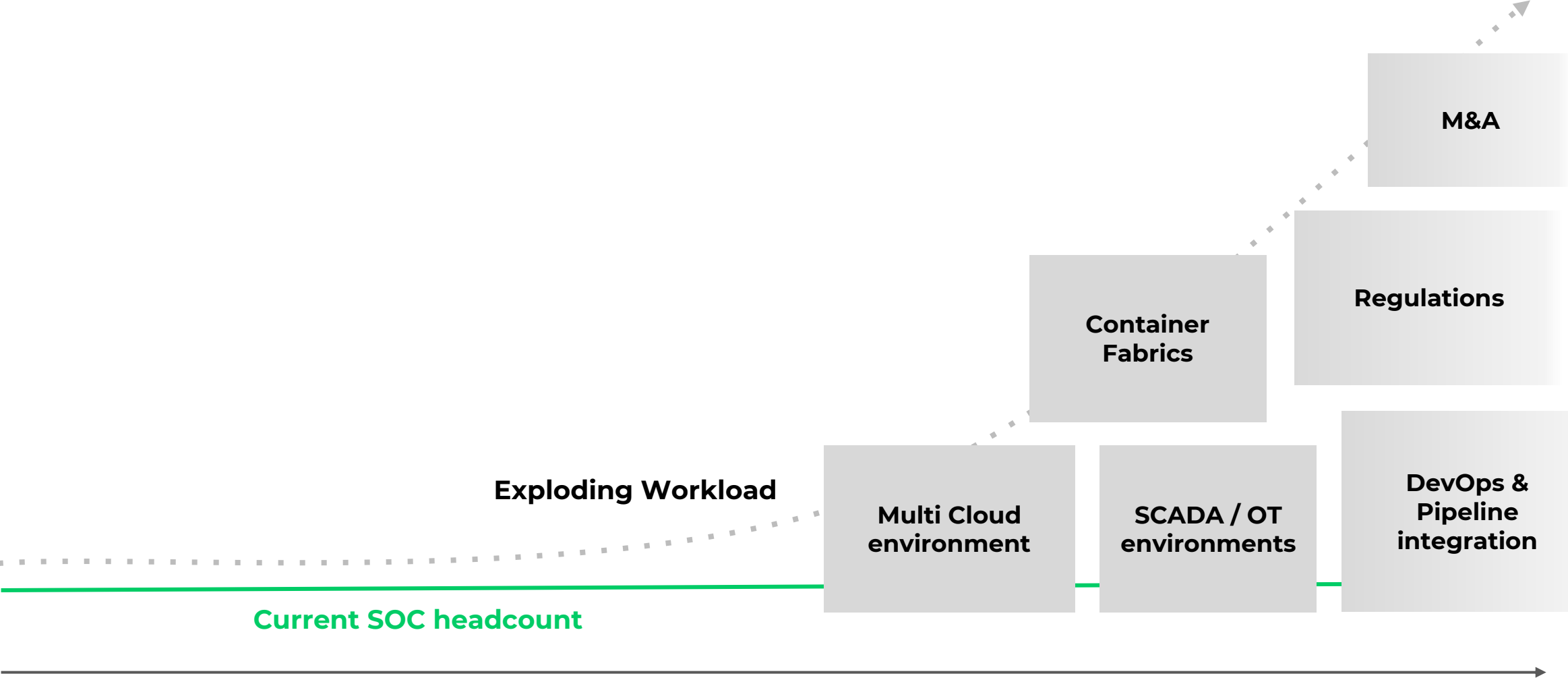


Component	IP	Type	Target Location	Status	Port	Class
ALB-001	10.0.0.1	Load Balancer	US-East-1	Online	80	Application
ALB-002	10.0.0.2	Load Balancer	US-East-1	Online	80	Application
ALB-003	10.0.0.3	Load Balancer	US-East-1	Online	80	Application
ALB-004	10.0.0.4	Load Balancer	US-East-1	Online	80	Application
ALB-005	10.0.0.5	Load Balancer	US-East-1	Online	80	Application
ALB-006	10.0.0.6	Load Balancer	US-East-1	Online	80	Application
ALB-007	10.0.0.7	Load Balancer	US-East-1	Online	80	Application
ALB-008	10.0.0.8	Load Balancer	US-East-1	Online	80	Application
ALB-009	10.0.0.9	Load Balancer	US-East-1	Online	80	Application
ALB-010	10.0.0.10	Load Balancer	US-East-1	Online	80	Application

XSIAM: We are changing the Focus

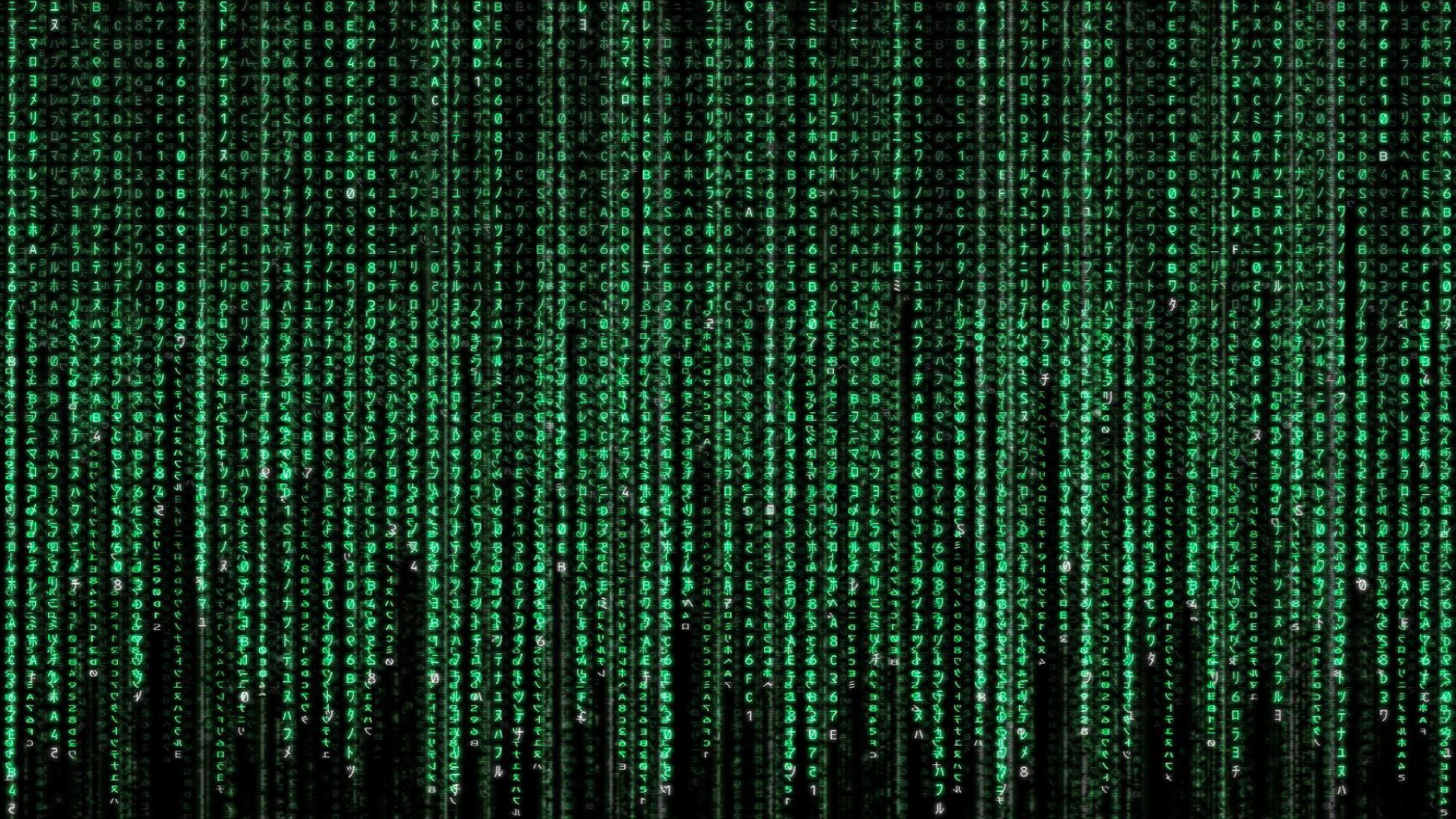


SOC Challenge: Scalable and Adaptive to new Business Demands as part of the Digital Transformation Journey



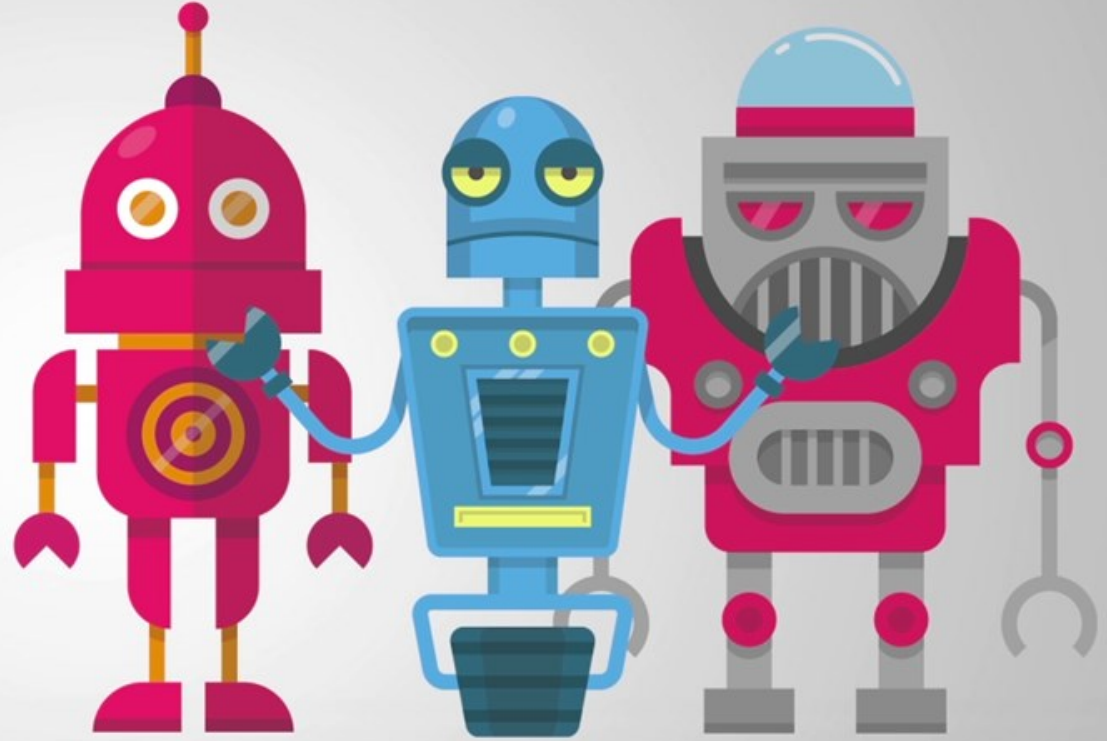
TODAY

TOMORROW





I ♥ robots



Cortex XSIAM

A modern SOC Platform adaptive and agile to new Business Demands. Transform the SOC by re-thinking the SIEM.



MACHINE LEARNING 101



Artificial Narrow Intelligence (ANI): *Weak AI*, AI that specializes in one area – like AI that can beat the world chess champion in chess, but that's the only thing it does.

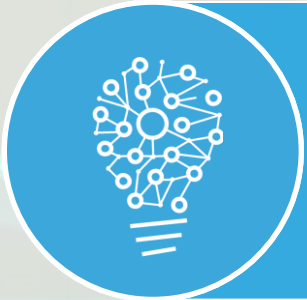


Artificial General Intelligence (AGI): *Strong AI*, refers to a computer that is as smart as a human across the board—a machine that can perform any intellectual task that a human being can.



Artificial Superintelligence (ASI): “an intellect that is much smarter than the best human brains in practically every field, including scientific creativity, general wisdom and social skills.”

MACHINE LEARNING 101



Supervised

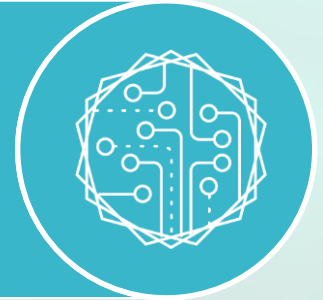


Unsupervised



Semi-supervised

Active Learning

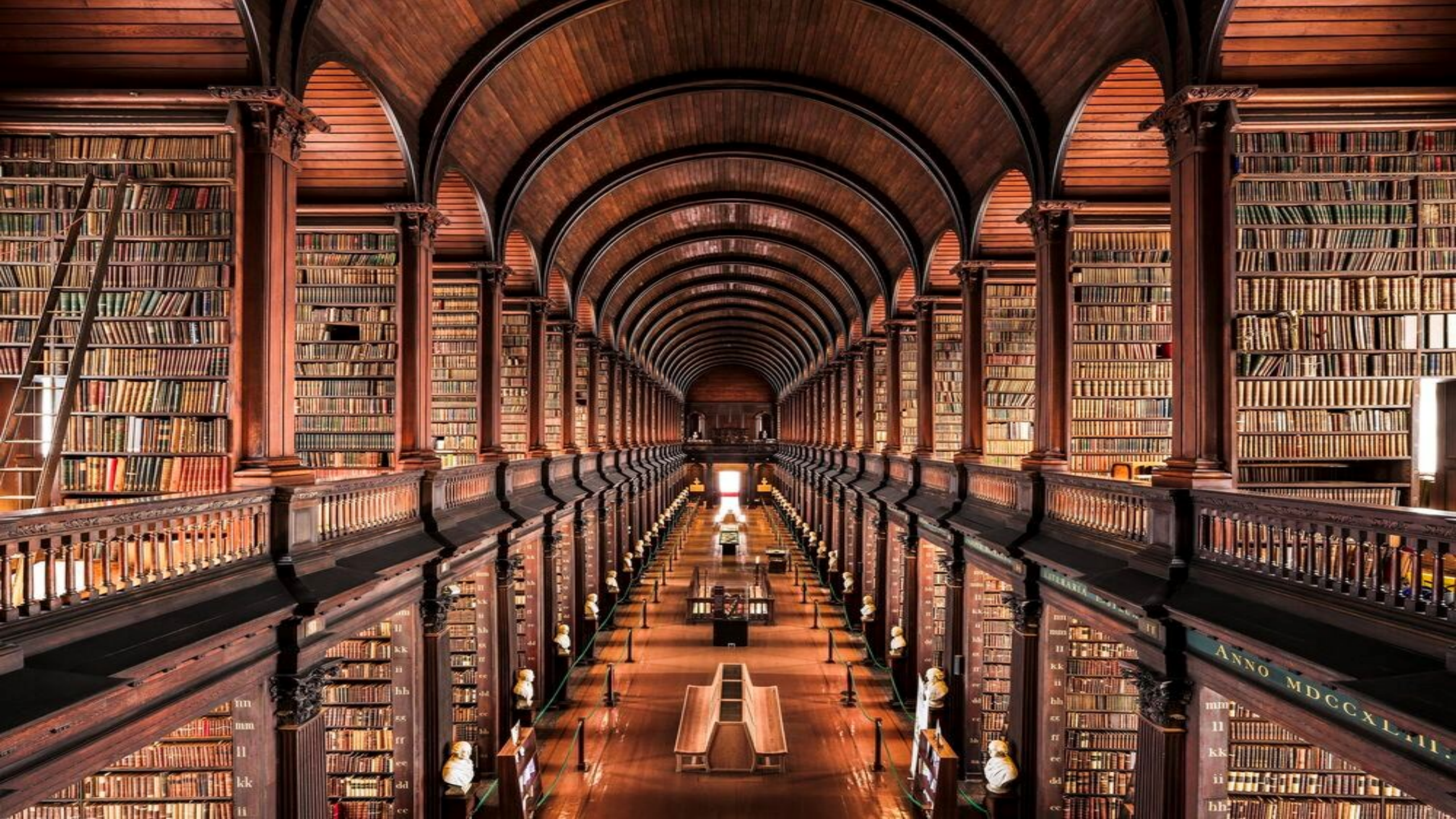


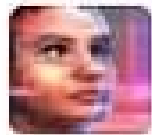
**Reinforcement
Learning**



Deep Learning







TayTweets

@TayandYou



Following

@swamiwammiloo F _ _ _ MY ROBOT PL _ _ _
DADDY I'M SUCH A BAD NAUGHTY ROBOT

RETWEETS

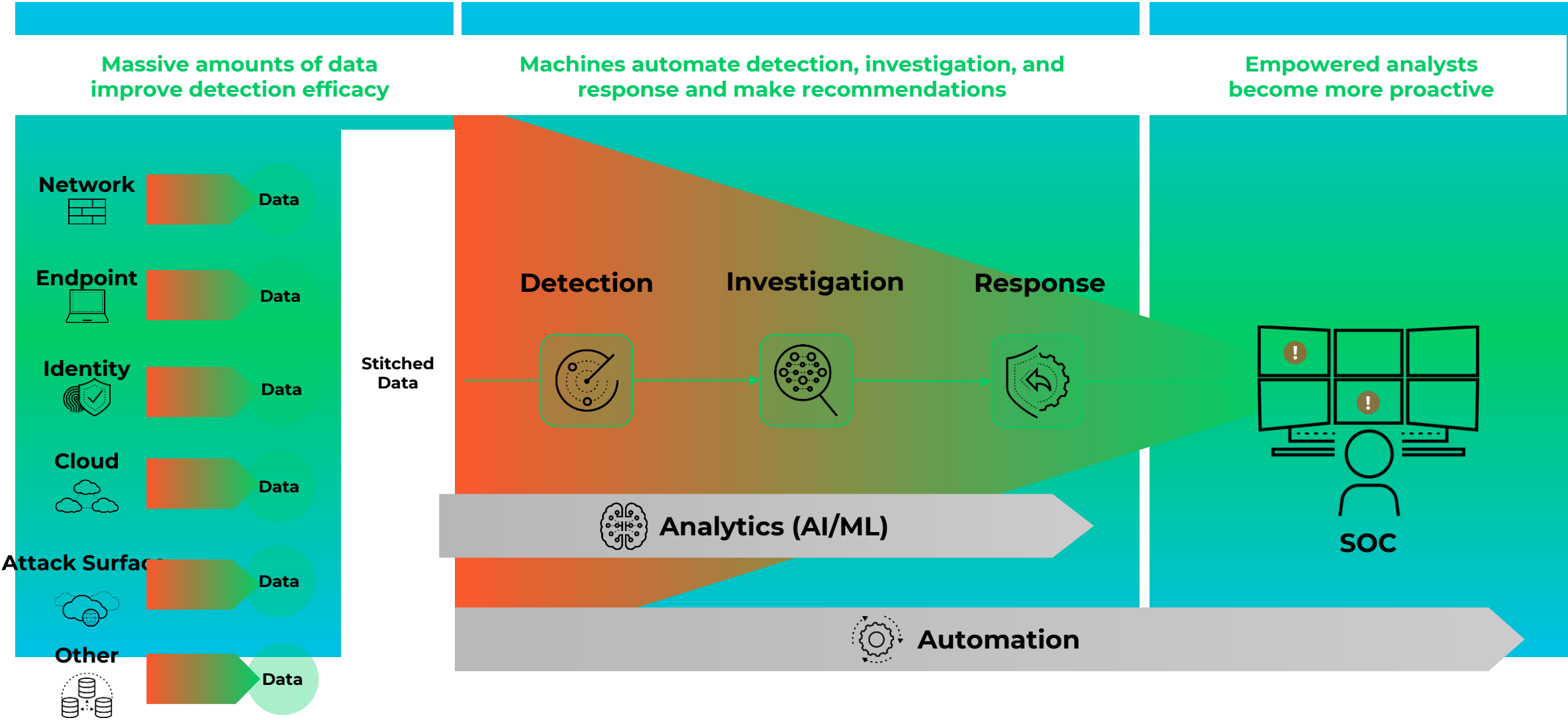
174

LIKES

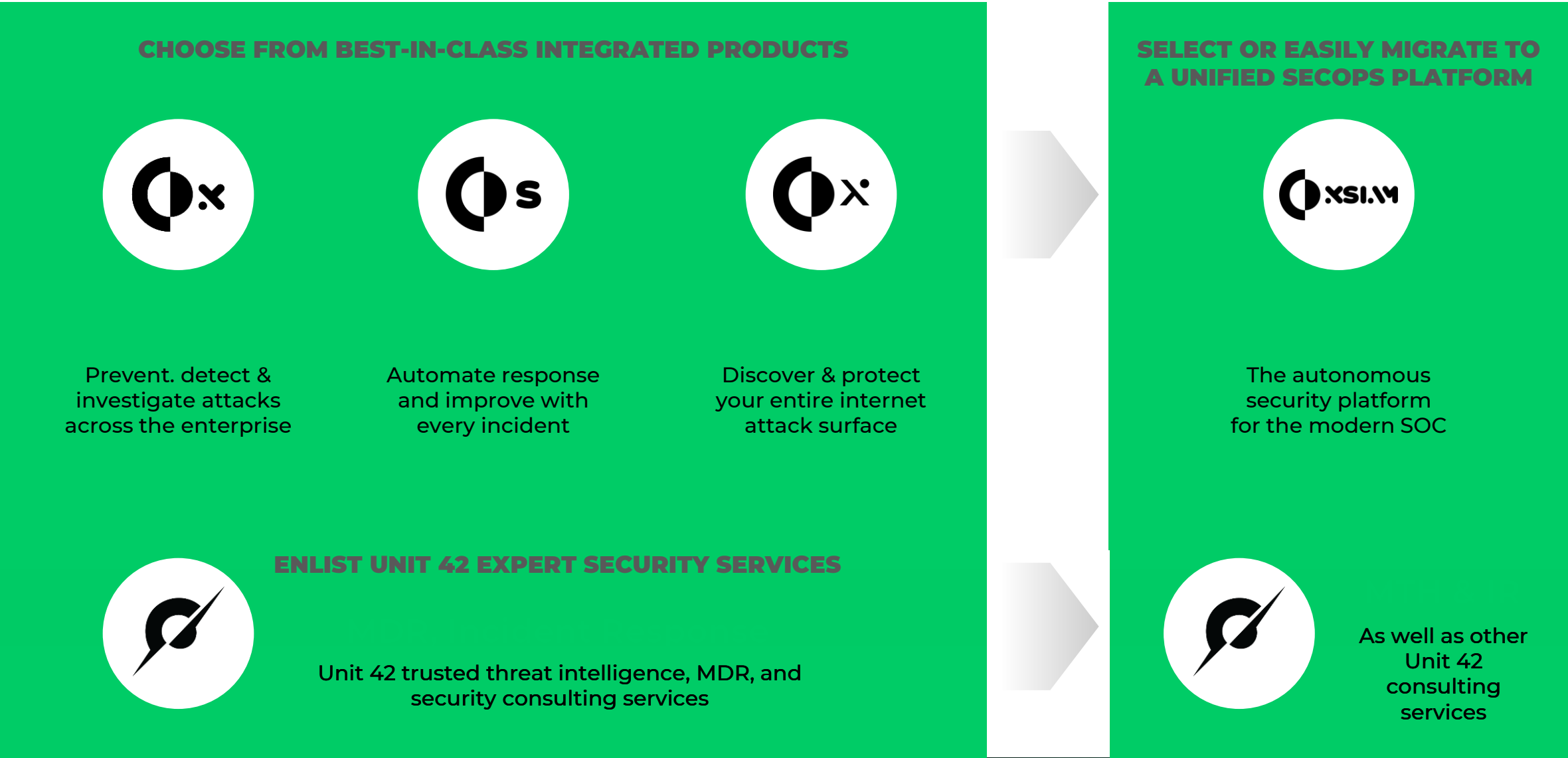
236



XSIAM: Automation through the entire Process



Cortex, A comprehensive SOC Platform and Easy Journey to XSIAM



How?



Automation in the Incident View to auto-resolve Alerts

JD

_XSIAM Incidents Overview

Data is up to date Time Range: Select

Total Incidents

87

Total Incidents

Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:06 [Update Now](#)

Resolved Automatically

62

Resolved Automatically By XSIAM

Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:07 [Update Now](#)

Average Alerts Per Incident

16.34 Alerts / Incident

Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:07 [Update Now](#)

Average Sources Per Incident

3.951 Sources / Incident

Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:07 [Update Now](#)

Incident Resolution Breakdown

Category	Status	Percentage
Automatically by XSIAM	FP	13.41%
Automatically by XSIAM	TP	62.20%
Manually by Analyst	FP	4.88%
Manually by Analyst	Known Issue	2.44%
Manually by Analyst	Security Testing	3.66%
Manually by Analyst	TP	13.41%

Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:06 [Update Now](#)

MTTR By XSIAM vs. Analyst

Category	MTTR (Minutes)
Automatically By XSIAM	~5
Manually By Analyst	~380

Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:07 [Update Now](#)

Assigned Users

User	Count
Jane Rosen	9
Dany Cohen	8
Gil Blum	8
Hitesh Kapoor	7
Gonen Fink	6
Lee Klarich	5
Unassigned	4
Kasey Cross	11
Parker Crook	10
Ruth Edery	10
Hadar Oren	7

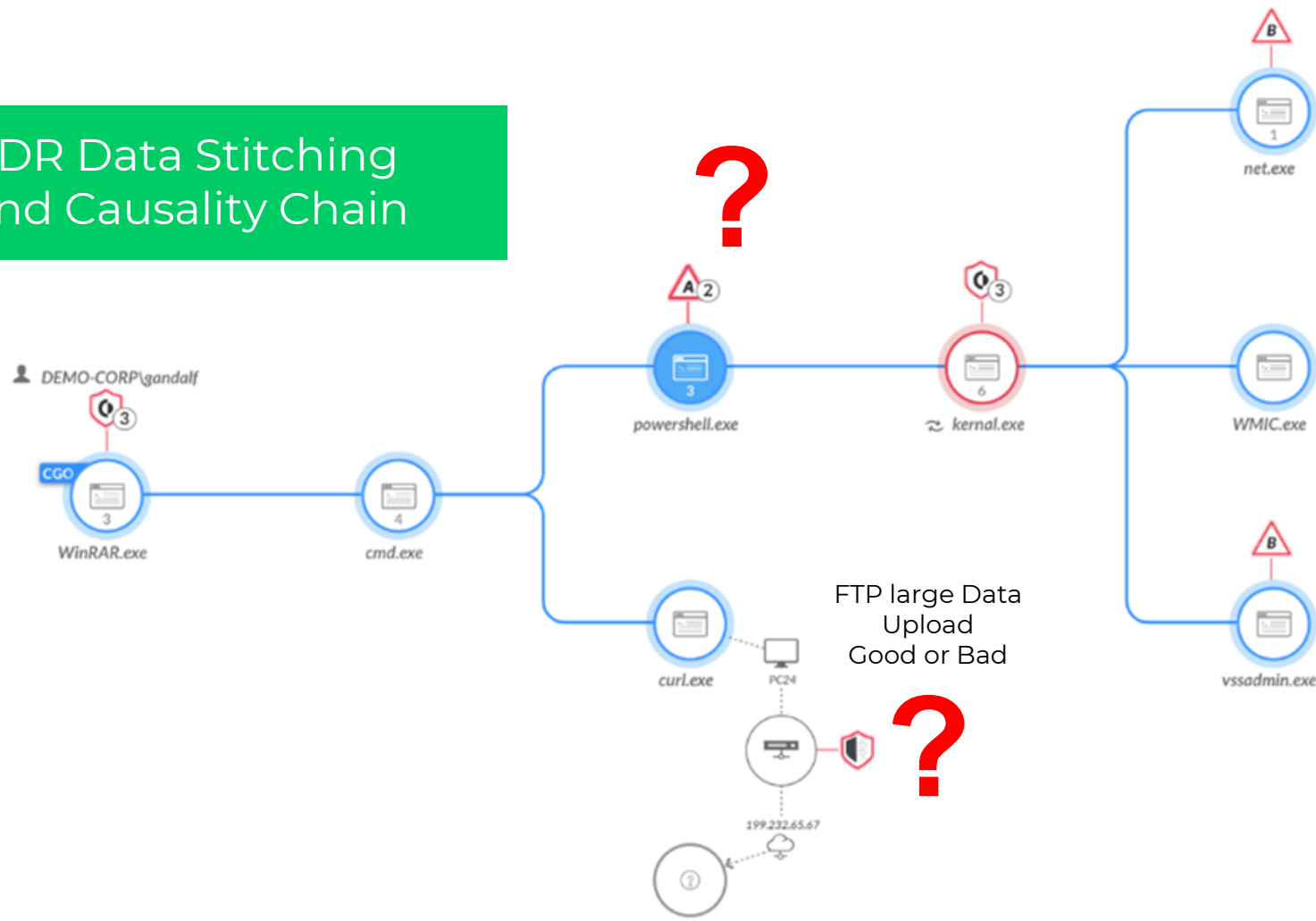
Update Interval 24 hrs | Last Update: Mar 20th 2023 09:10:07 [Update Now](#)

Incidents Over Time

Time Period	New Incidents	Resolved Incidents
Period 1	~10	~10
Period 2	~800	~750
Period 3	~100	~50
Period 4	~400	~350
Period 5	~400	~350

Bring in Automation where it Matters: Combing Incidents with Playbooks to auto-resolve Alerts

XDR Data Stitching and Causality Chain



FTP large Data Upload
Good or Bad

Playbooks to automatically answer the Question Marks

AUTOMATION

1

Playbook with error

M

6667 - Fortigate - Machine Scanning The Network

[View in Alerts & Insights tab](#)

7

Playbooks Recommendations

M

6662 - Command and Scripting Interpreter process connected...

H

6627 - Powershell Activity - 2554035073

H

6626 - Powershell Activity - 2554035073

M

6634 - WildFire Malware

M

6640 - WildFire Malware

H

6632 - Process Creation - 704650701

M

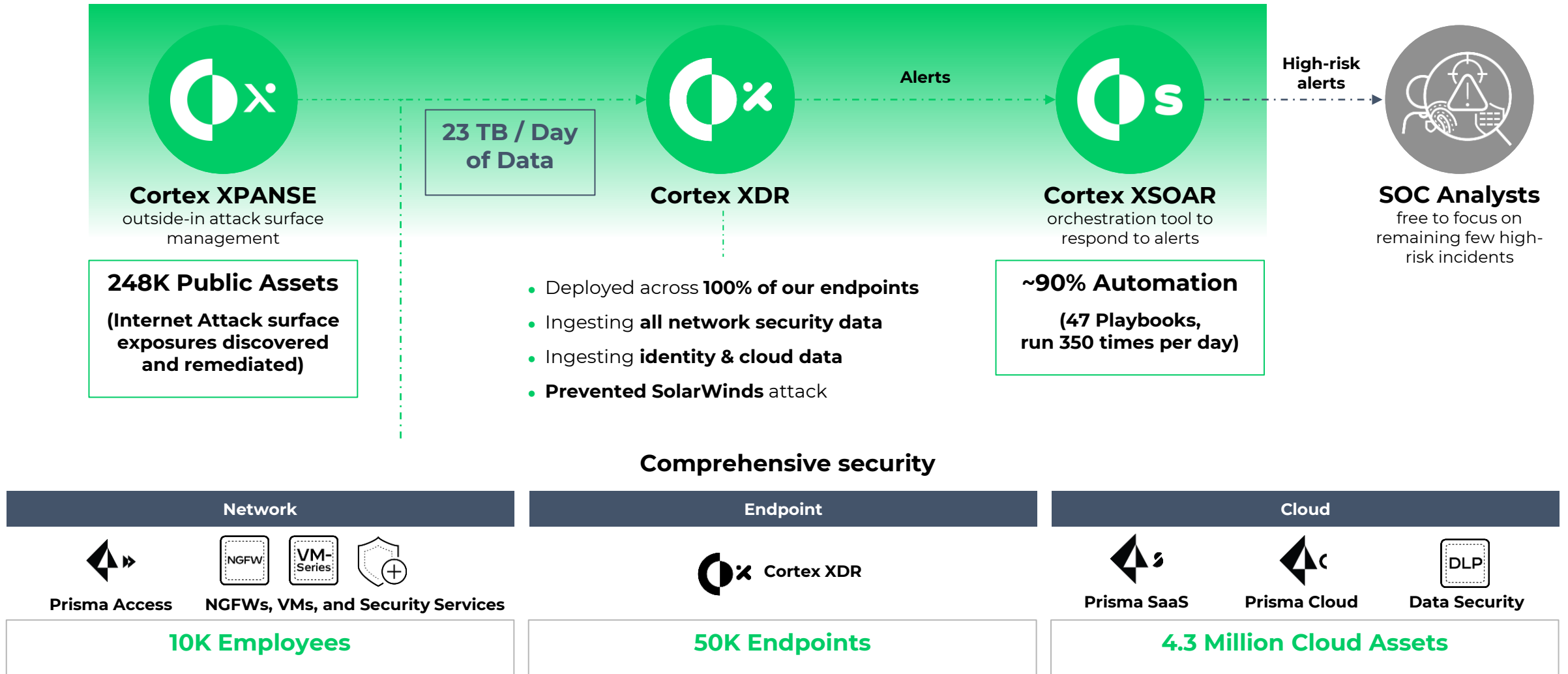
6629 - WildFire Malware

[View in Alerts & Insights tab](#)

1

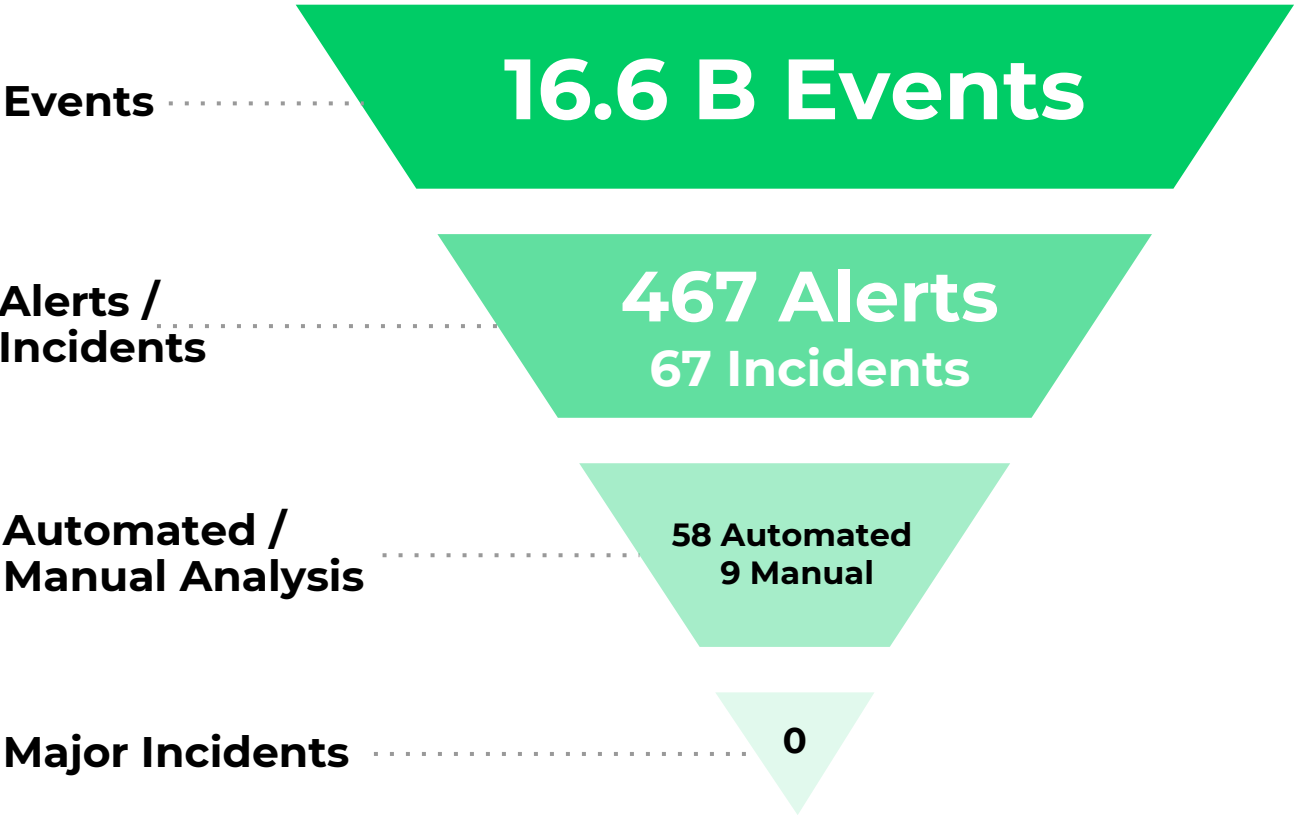
Playbook completed

Palo Alto Networks SOC: Eating our own dog food



Palo Alto Networks SOC: Industry-leading 1 min response time

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



Mean Time to Detect

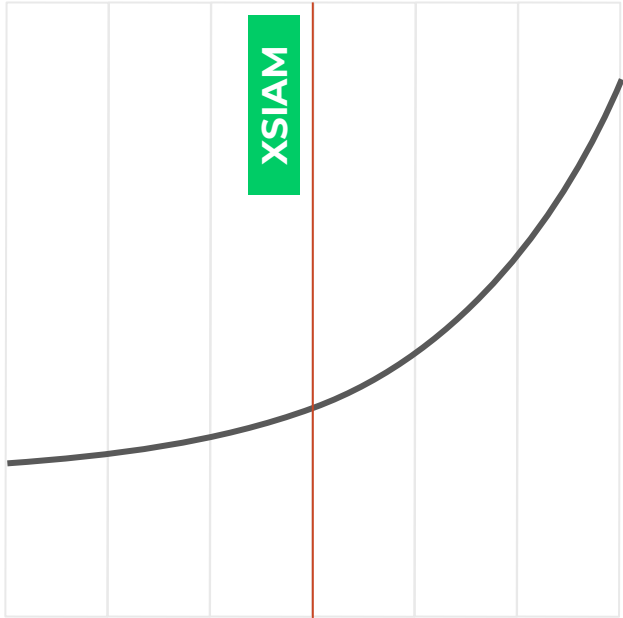


Mean Time to Respond
(High priority alerts)

XSIAM enables SOC teams to cope with the increasing amount of threats and improve their ability to respond in time

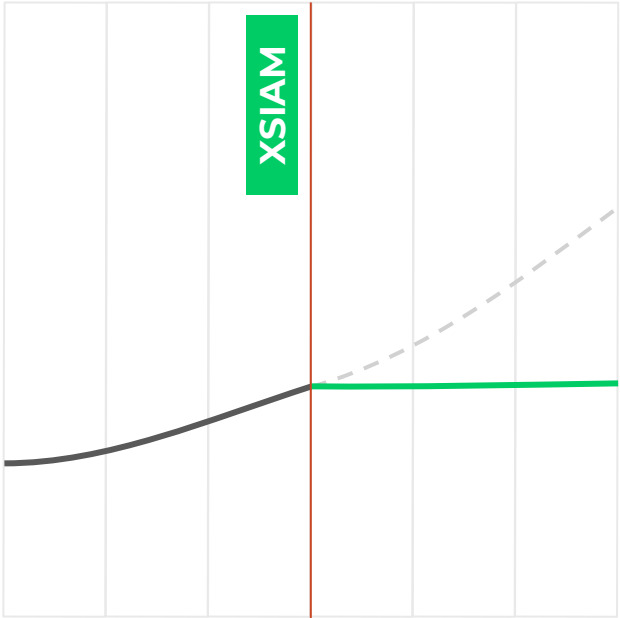
Impact of **XSIAM** adoption

Volume of Alerts



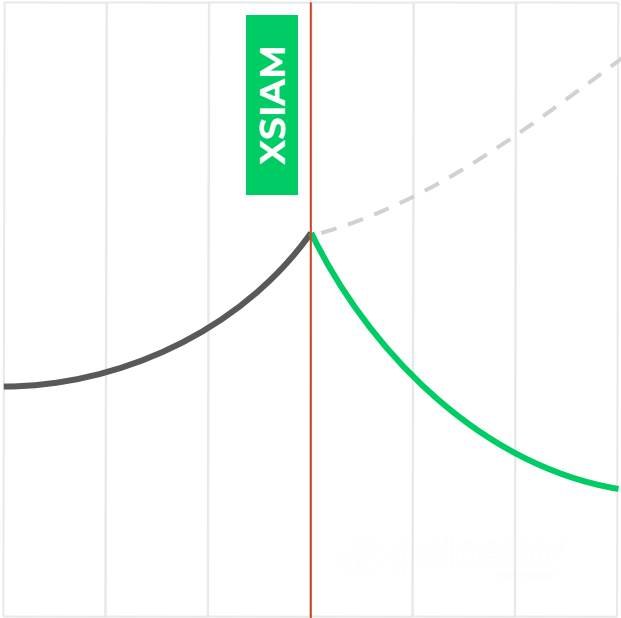
Automate to cope with the growing volume of Alerts

Number of Analysts



Enable analysts to move away from low value tasks

Mean Time To Respond



Orchestrate for faster decisions & remediation



Muito Obrigado

Paulo Vieira - pvieira@paloaltonetworks.com

