AI to Improve Cyber Resilience

Shifting to Real-Time & Autonomous Security

Rabih Bou
Systems Engineer Manager

Palo Alto Networks

Zero Trust Platform

STRATA | PRISMA SASE

Best-in-class network security enabling enterprise-wide Zero Trust security

Code-to-Cloud Platform

PRISMA CLOUD

Securing the cloud by integrating app development to cloud to runtime security

AI-Driven Security Operations Platform

CORTEX

Transforming Security Operations with next-gen AI and automation

Incident Response, Advisory Services and Threat Intelligence

UNIT 42

Managed & proactive security services and world-renowned intelligence

$6.89B	**25% YoY**	**Over 65k+**	**80% G2K Customers**
FY23 Revenue	FY23 Revenue Growth	Active customers globally in 180+ countries	Half of which transact across our three platforms

We’re Going to Answer Three Questions

1

Why do Organizations Struggle to Improve Cyber Resilience?

2

How can Harnessing AI Improve Cyber Resilience?

3

What are Some Practical Examples for AI in Cybersecurity?

We’re Going to Answer Three Questions

1. Why do Organizations Struggle to Improve Cyber Resilience?
2. How can Harnessing AI Improve Cyber Resilience?
3. What are Some Practical Examples for AI in Cybersecurity?

Defining Cyber Resilience

1

Managing Business Risks

Across the entire organization including supply chain risks

2

Measuring Security & Operational Efficacy

In addressing high-risk vulnerabilities, and preventing Known/Unknown threats

3

Responding to Threats

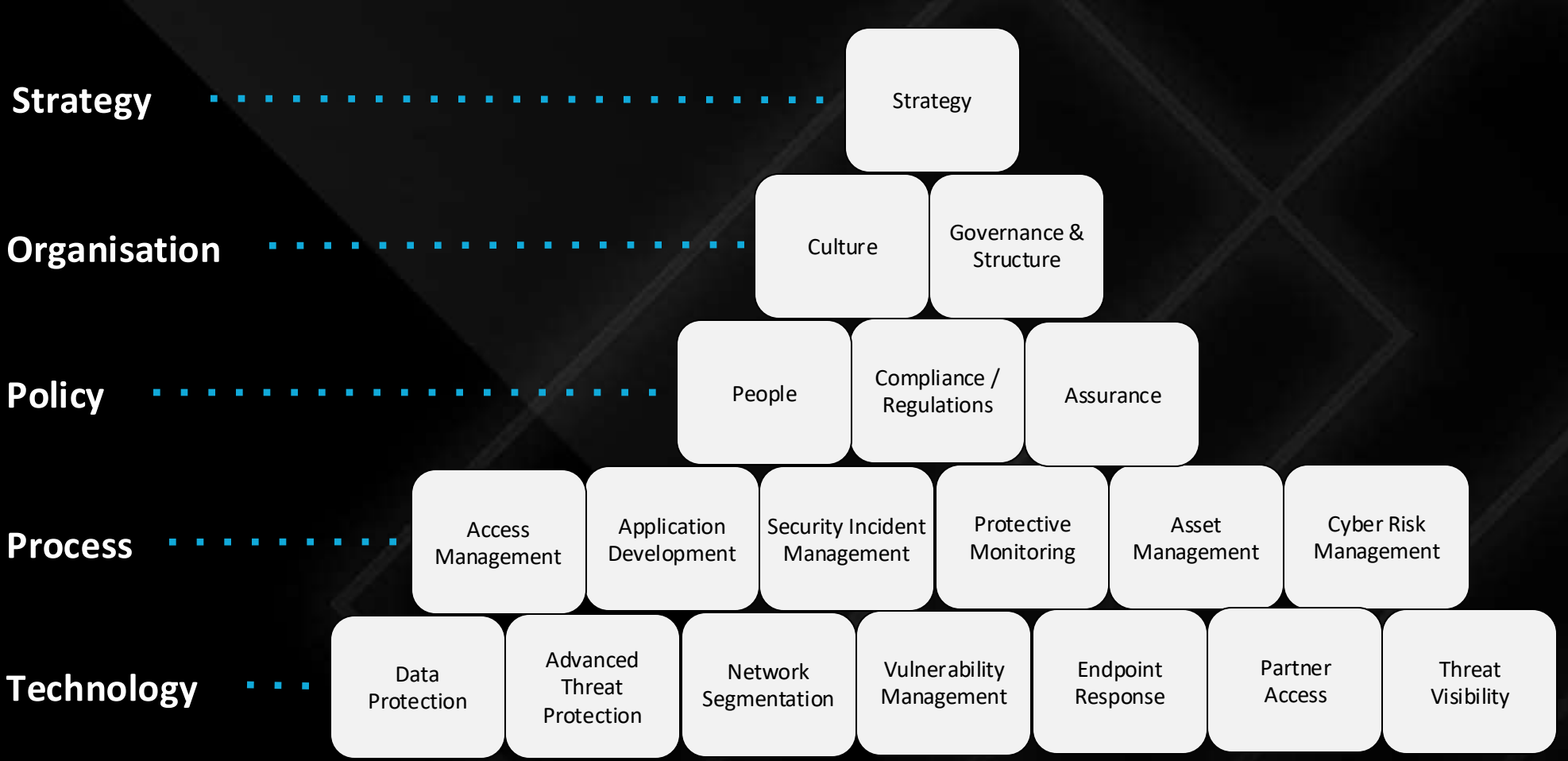
Using a threat-informed approach and automated security controls

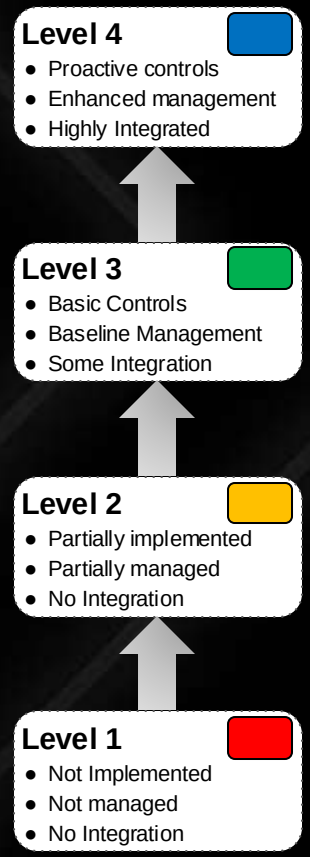
Business Risks have Evolved

$8 TRILLION

COST OF CYBERCRIME

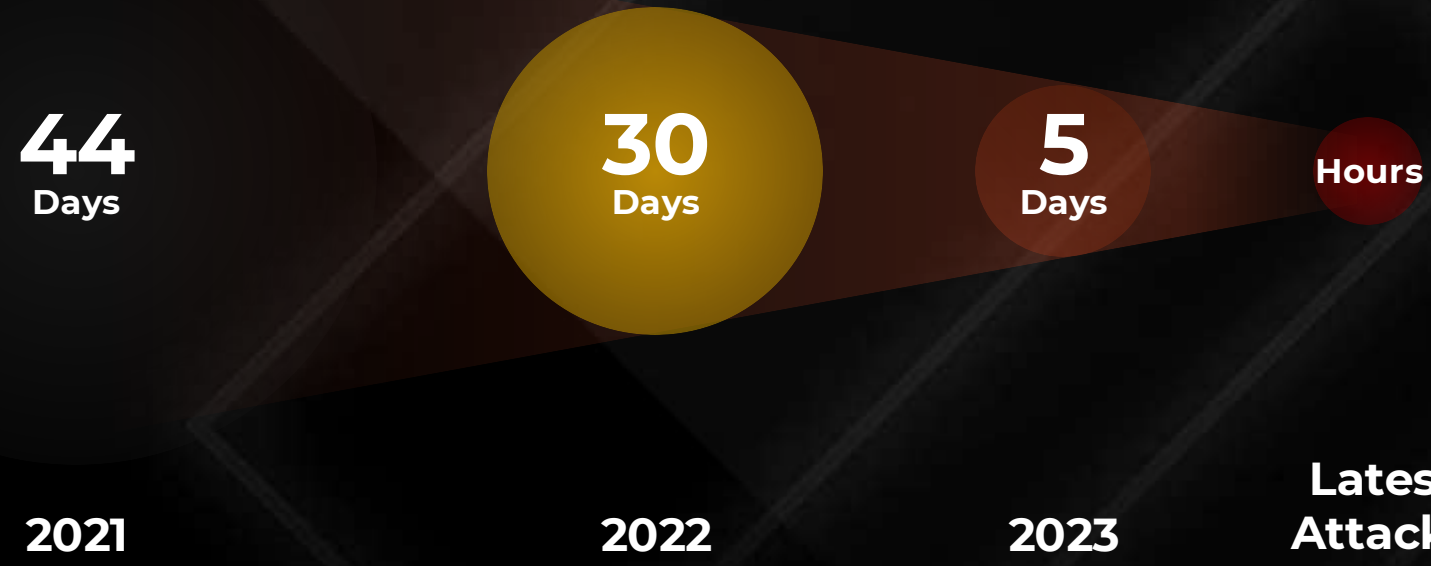
Security Frameworks Need to Adapt





Attacks Are Happening Faster Than Organizations Can Respond...

Average Days from "Compromise" to "Exfil"[1]



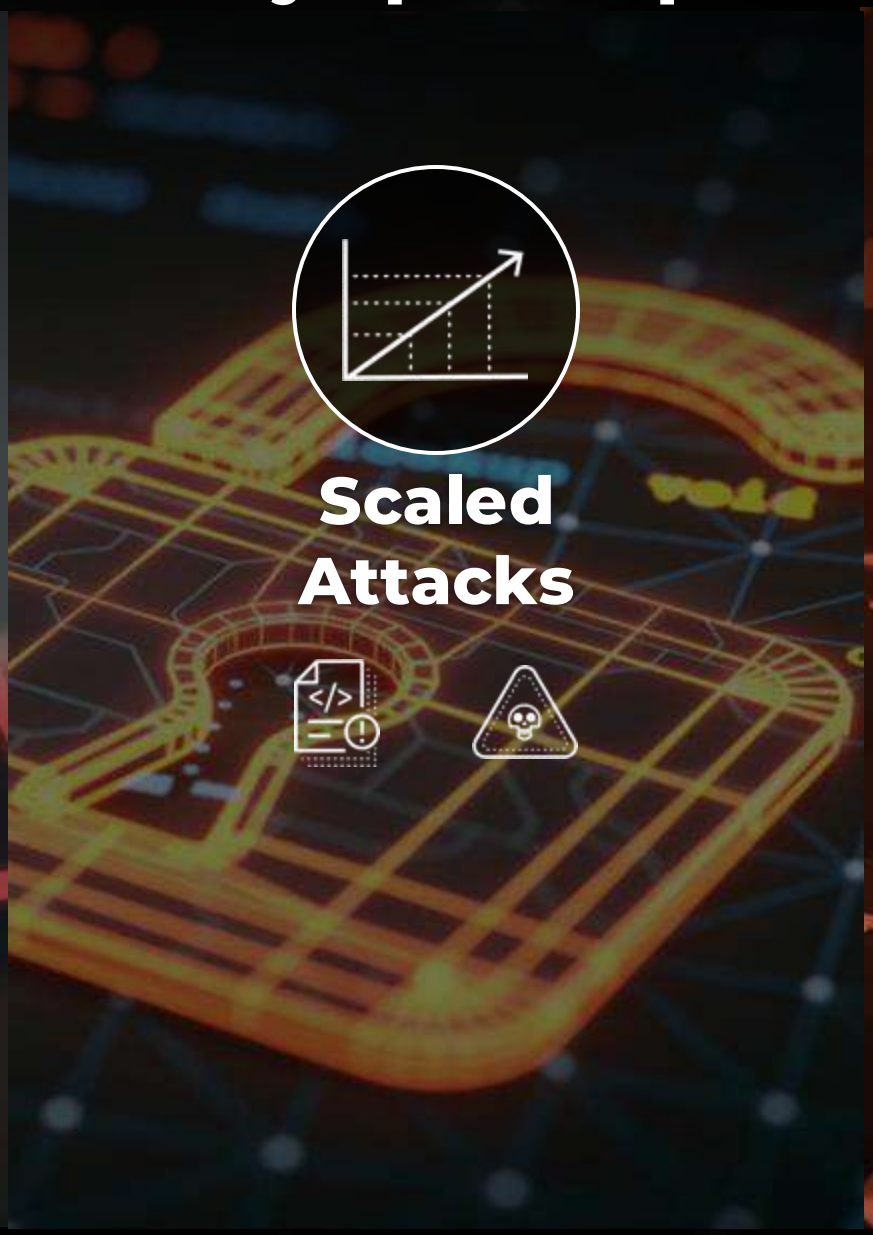
Industry average
6 DAYS
to remediate

GDPR adopted rule
3 DAYS
Data Breach Notification[2]

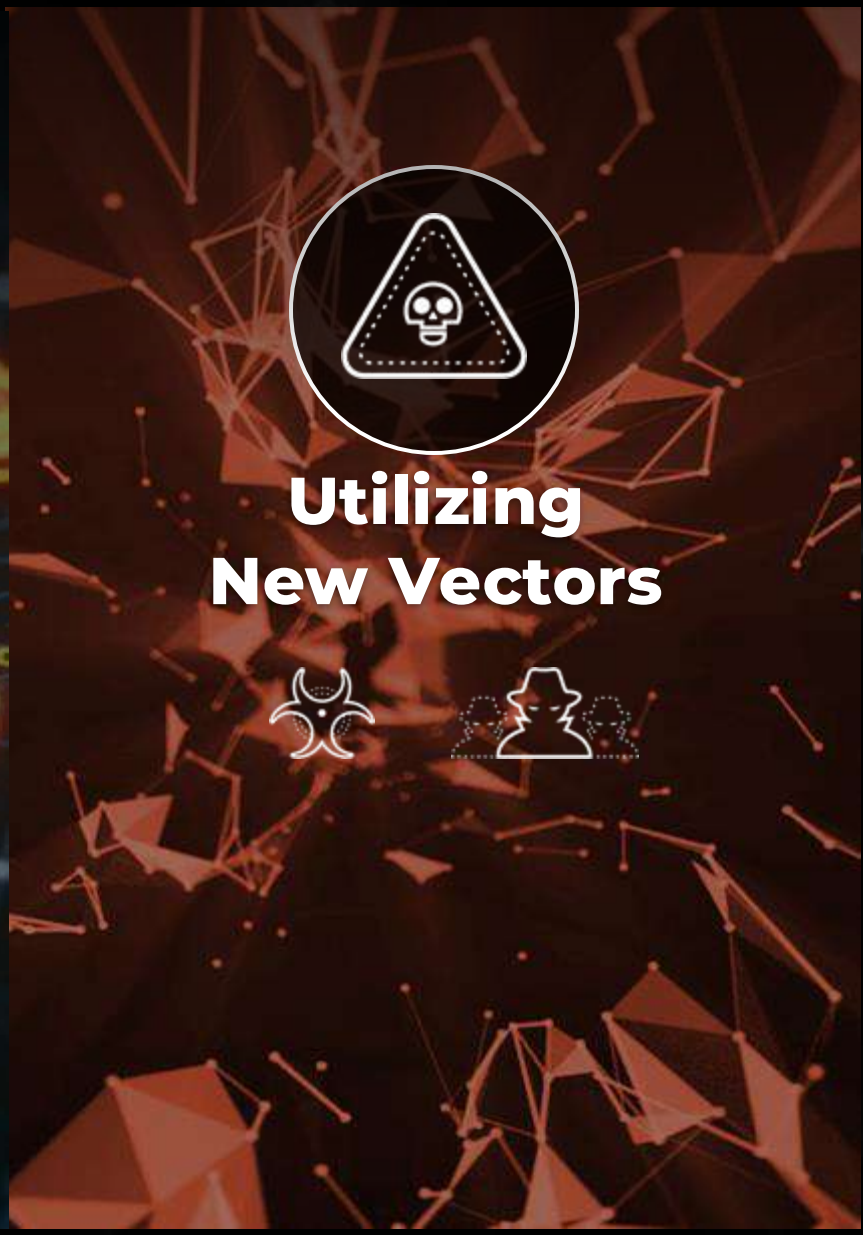
Sources:
1) Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;
2) Under the GDPR Notification Rules, an incident that causes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

...and AI Will Only Speed Up Attackers

Accelerated Attacks



Scaled Attacks



Utilizing New Vectors

Example Client: Dealing with Complexity

Typical industry approach requires 10+ point products per Digital Initiative

We’re Going to Answer Three Questions

1

Why do Organizations Struggle to Improve Cyber Resilience?

2

How can Harnessing AI Improve Cyber Resilience?

3

What are Some Practical Examples for AI in Cybersecurity?

Artificial Intelligence Primer

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.

Machine learning is a type of ANI that provides computers with the ability to identify specific patterns without being explicitly programmed to identify them.

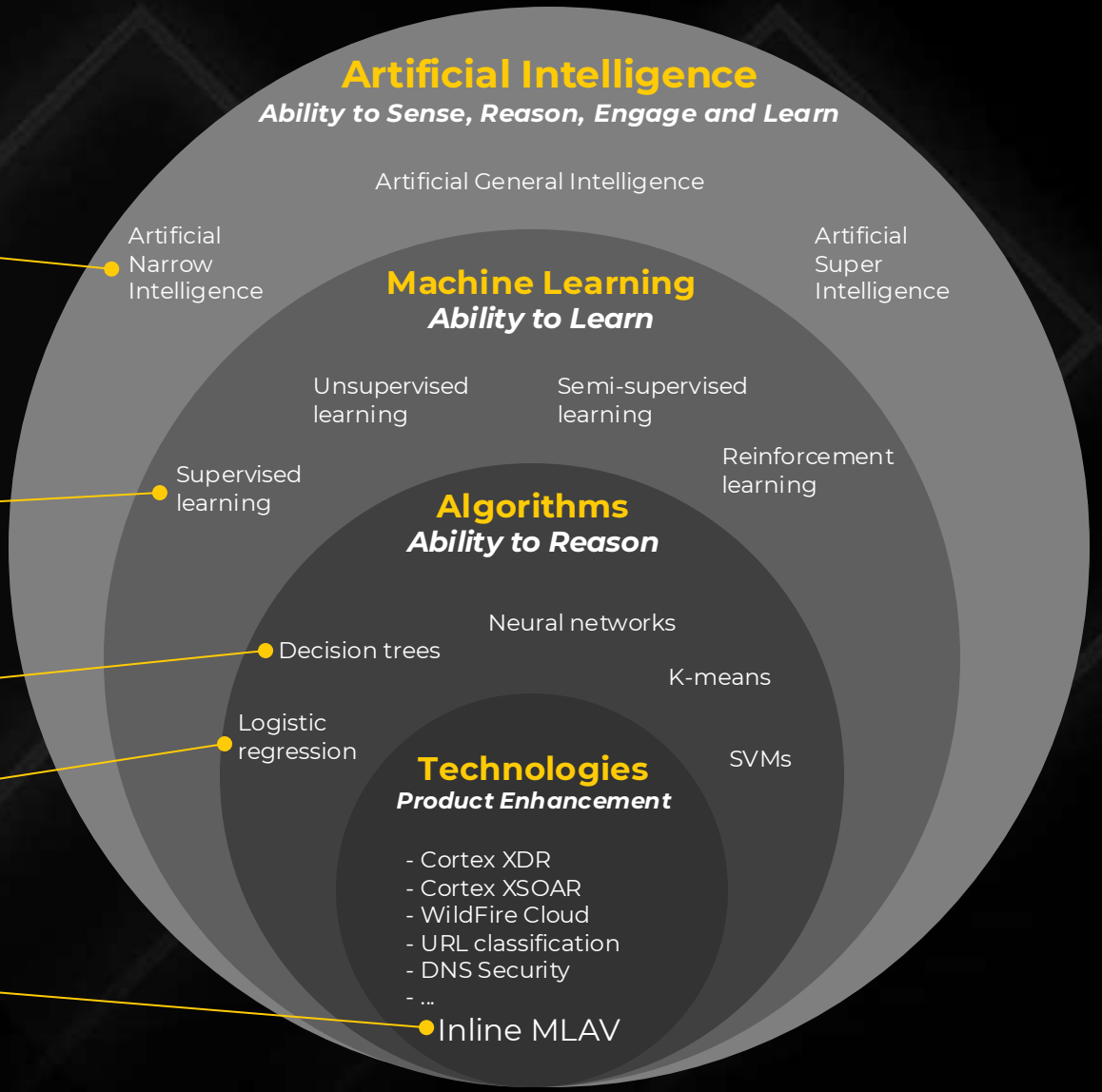
In **Supervised Learning**, the training set you feed to the algorithm includes the desired solutions, called labels.

Classification predicts a *class label*, which is a choice from a predefined list of possibilities. **Binary classification** is the special case of distinguishing between exactly two classes.

A **Decision Tree** is a binary tree data structure used to make a decision. They serve as the base model for more powerful ensemble algorithms such as Random Forest and **Gradient-Boosted Trees.**

Logistic regression is a linear classifier that predicts probabilities.

Inline MLAV is a classic supervised machine learning binary classifier. This classification occurs at line speed (as the file is being transmitted) by making a single pass over each file or piece of network traffic followed by a verdict.



AI can Improve Resilience and Reduce Risk

Real-Time Threat Prevention & Sandboxing

Block Sophisticated Attacks without Human Intervention

Increase Effectiveness and Efficiency of Security Teams

AI Rapid Response Reduces Impact of a Cyber Attack

Improved Cyber Resilience & Reduced Risk

Predictive Risk Management

Reduce Operational Cost

Consolidate with AI-Driven Security Platforms

Proactively Identify Compliance Gaps and Suggest Remedies

We’re Going to Answer Three Questions

1

Why do Organizations Struggle to Improve Cyber Resilience?

2

How can Harnessing AI Improve Cyber Resilience?

3

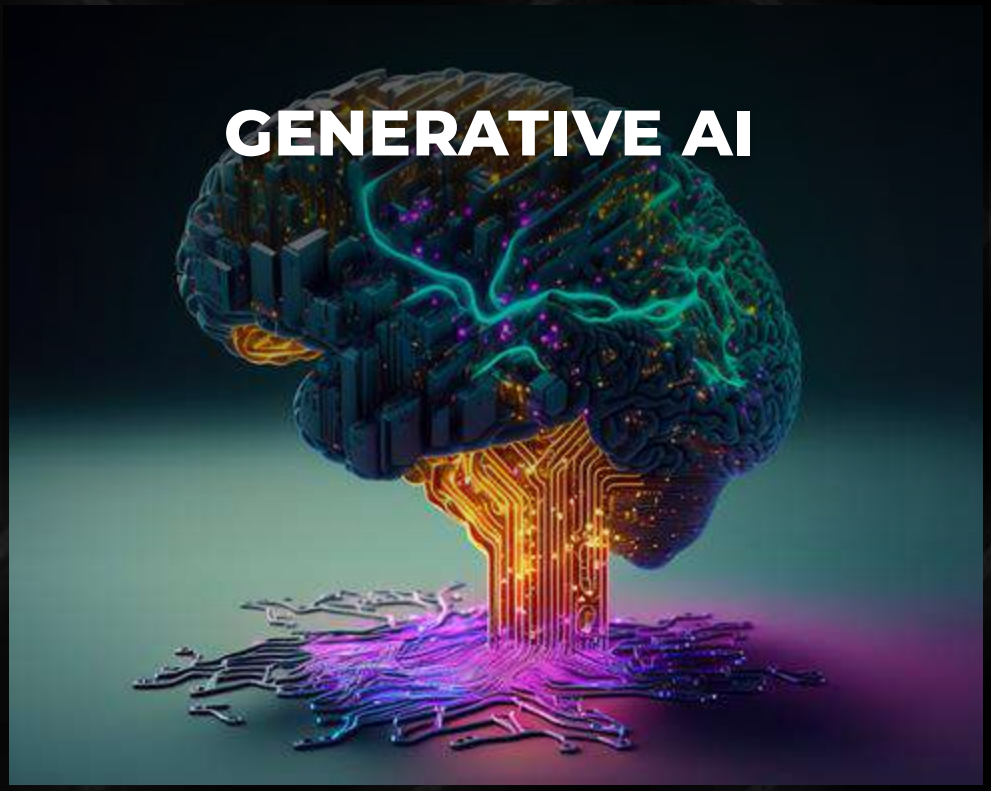
What are Some Practical Examples for AI in Cybersecurity?

How the World is Changing with AI

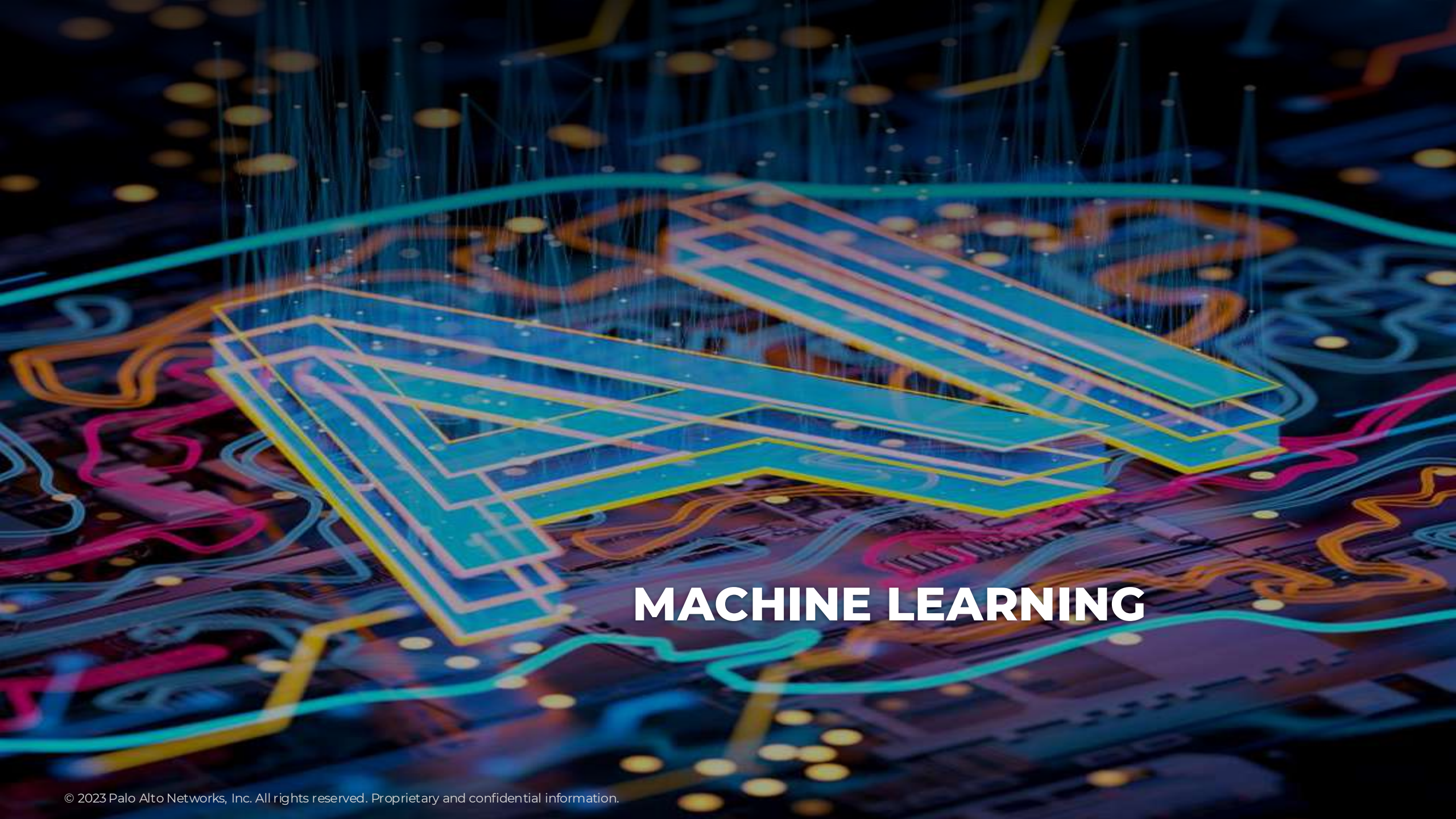
MACHINE LEARNING

Deterministic models focused on **targeted, well-defined tasks** requiring high accuracy & precision

GENERATIVE AI



General-purpose, versatile models for **generating creative & non-deterministic content** from human language prompts



1. AI Prevents Threats Inline

AI-Enabled Cloud-Delivered Security

- Advanced Intrusion Prevention
- Advanced URL Filtering
- Advanced WildFire (Sandboxing)
- DNS Security
- Data Loss Prevention
- SaaS Security
- IoT Security
- AIOps

Hardware NGFW | **Software NGFW** | **SASE**

NGFW

A **Leader** in Gartner Magic Quadrant Network Firewalls

Deep Learning On Live traffic

Gartner

SD-WAN

A **Leader** in Gartner Magic Quadrant WAN Edge Infrastructure

6x Faster Compute for ML in the Cloud

Ultra-low latency global network

Gartner

SSE

A **Leader** in Gartner Magic Quadrant Security Service Edge

Gartner

Outcomes

95%
Common File-Based Threats Prevented

1.5m
New Attacks Detected Daily

SASE

ONLY Leader in Gartner Magic Quadrant Single-Vendor SASE

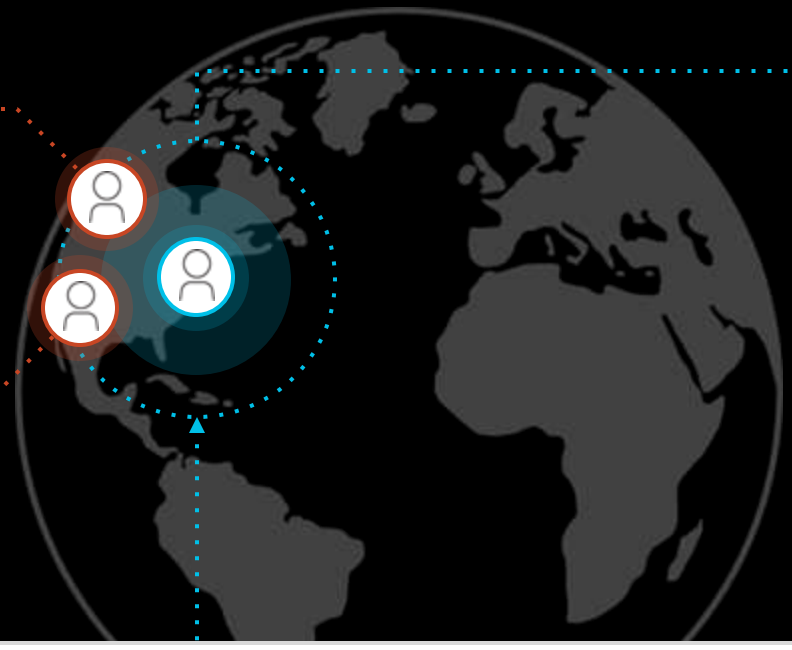
8.6B
Attacks Blocked Daily

Gartner

2. AI Deflects Incidents & Forecasts Capacity

Users experiencing authentication failures

Users are unable to access business critical apps

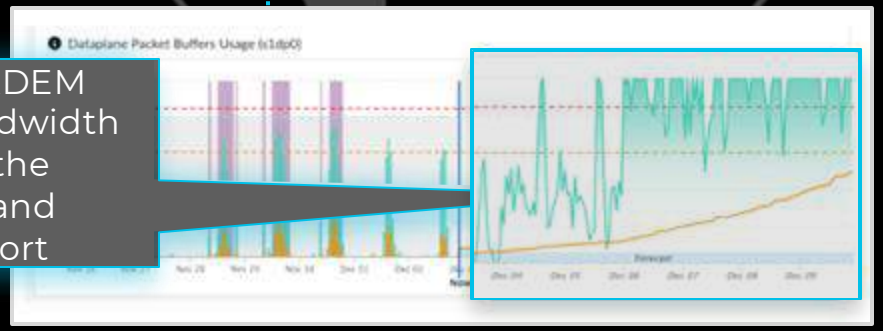


ADEM

AI-powered DEM notifies IT: Regional internet provider has an outage in Santa Clara, San Jose, Milpitas in California starting 10:17AM PST

IT proactively notifies nearby users, preempting tickets.

AI-powered ADEM forecasts bandwidth saturation in the next 28 days and alerts IT Support



Outcomes

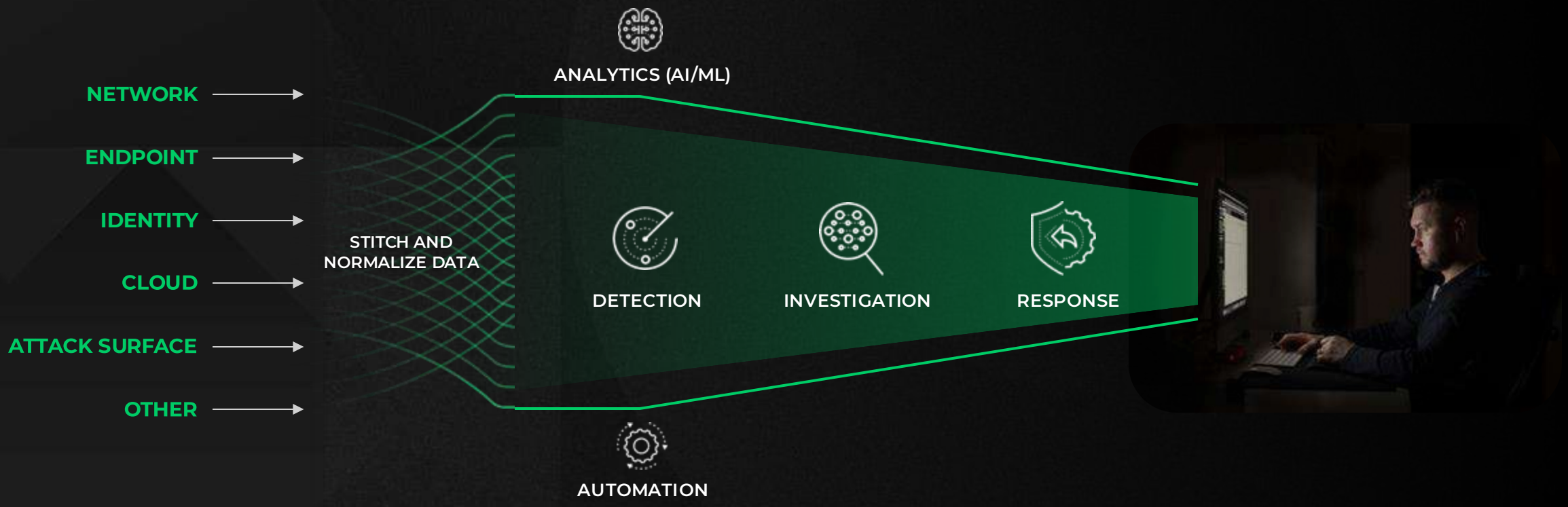
- **Proactive IT**
- **Deflect tickets**

3. AI Delivers the Autonomous SOC

Massive data enhanced with stitching and correlation dramatically reduces the # of alerts

Machines automate detection, investigation, and response and make recommendations

Empowered analysts become more proactive

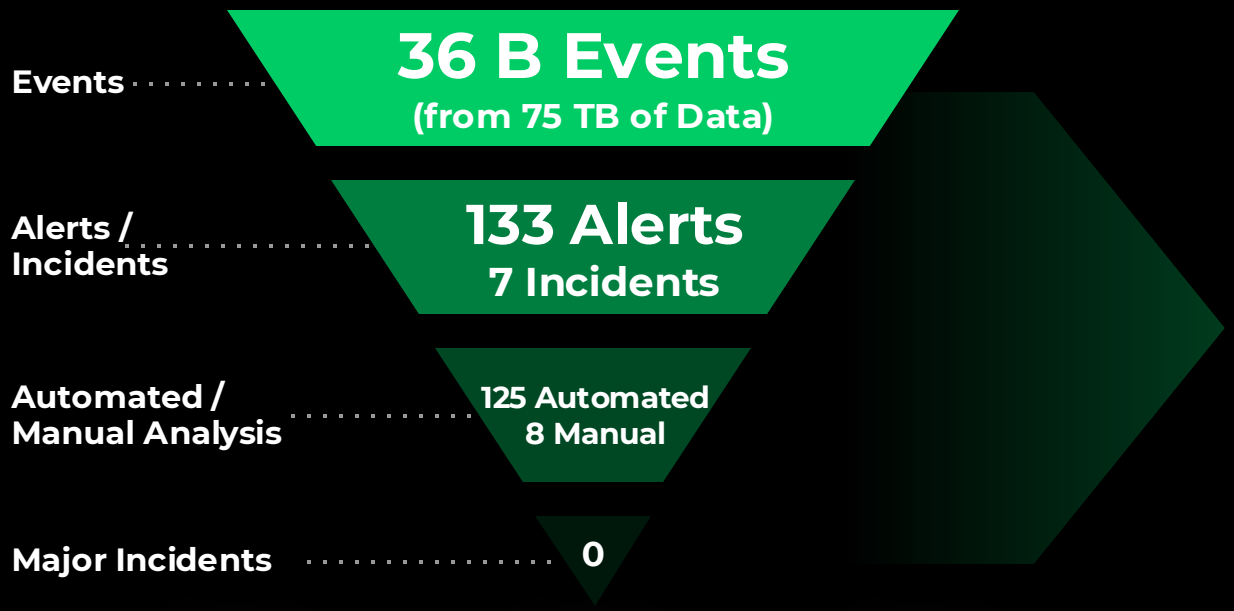


Outcomes from Delivering the Autonomous SOC

Cortex XSIAM

The autonomous security platform for the modern SOC

A Day in the life of the Palo Alto Networks internal SOC



10 SECONDS
Mean Time to Detect

1 MINUTE
Mean Time to Respond (High priority)

10 FTE
Staff Automation Savings (per Annum)

Early Customer Results

>4.86 PB/day of Data ingested

1000+ AI Models applied **to detect attacks**

AI smart scoring and automation to accelerate investigation and response

Early XSIAM customers seeing **mean time to respond reduction from weeks/days to hours/mins**

Palo Alto Networks: 10 Years+ of *Machine Learning*

2013

Wildfire
AI-driven malware detection

2018

CASB
ML-powered data protection to help find and eliminate dangerous misconfigurations.

Cloud UEBA
ML-driven suspicious user login and activity detection in the cloud

2019

Demisto/ XSOAR
Automated incident response

Zingbox
AI-driven IoT device discovery for security

2020

ML-Powered NGFW
Inline ML to stop Zero Day attacks

Xpanse
Leverage ML to catalog entire Internet

Cloud Threat Detection
AI-powered malicious network activity identification in the cloud

2021

AI-Powered ZTNA
AI-Powered Autonomous Digital Experience Management to proactively remediate issues

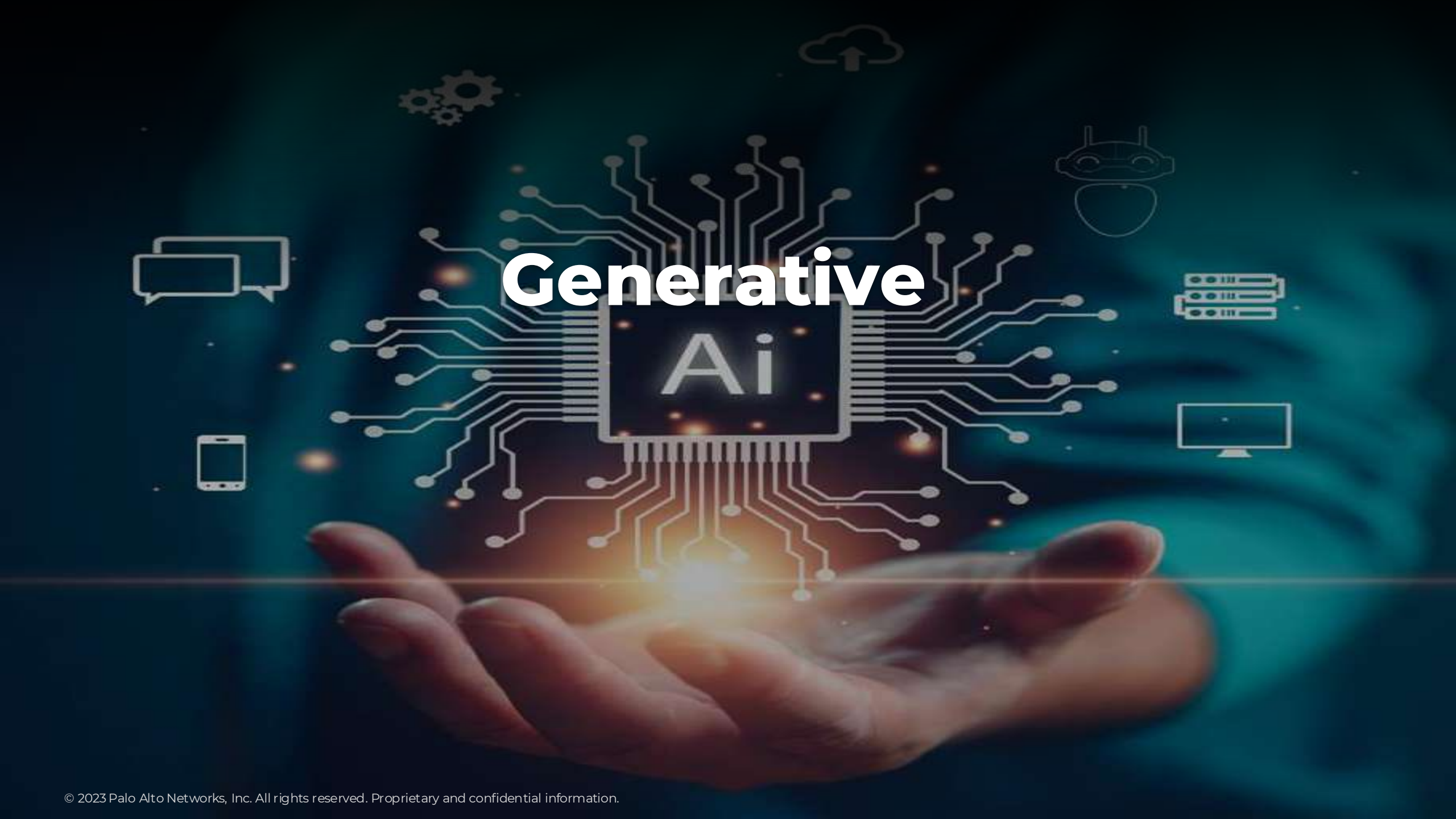
2022

XSIAM
AI-driven security operations platform for the modern SOC

2023

AIOps
Proactively improve security posture and prevent network disruptions

Adv URL Filtering
AI-driven anti-phishing



Copilots will Reveal the Value of AI

Reimagining Product Experience

Find and Understand Information

- Navigation
- Predefined Prompts & Queries
- "Hover Cover" Translation
- User Feedback and Expert Rating

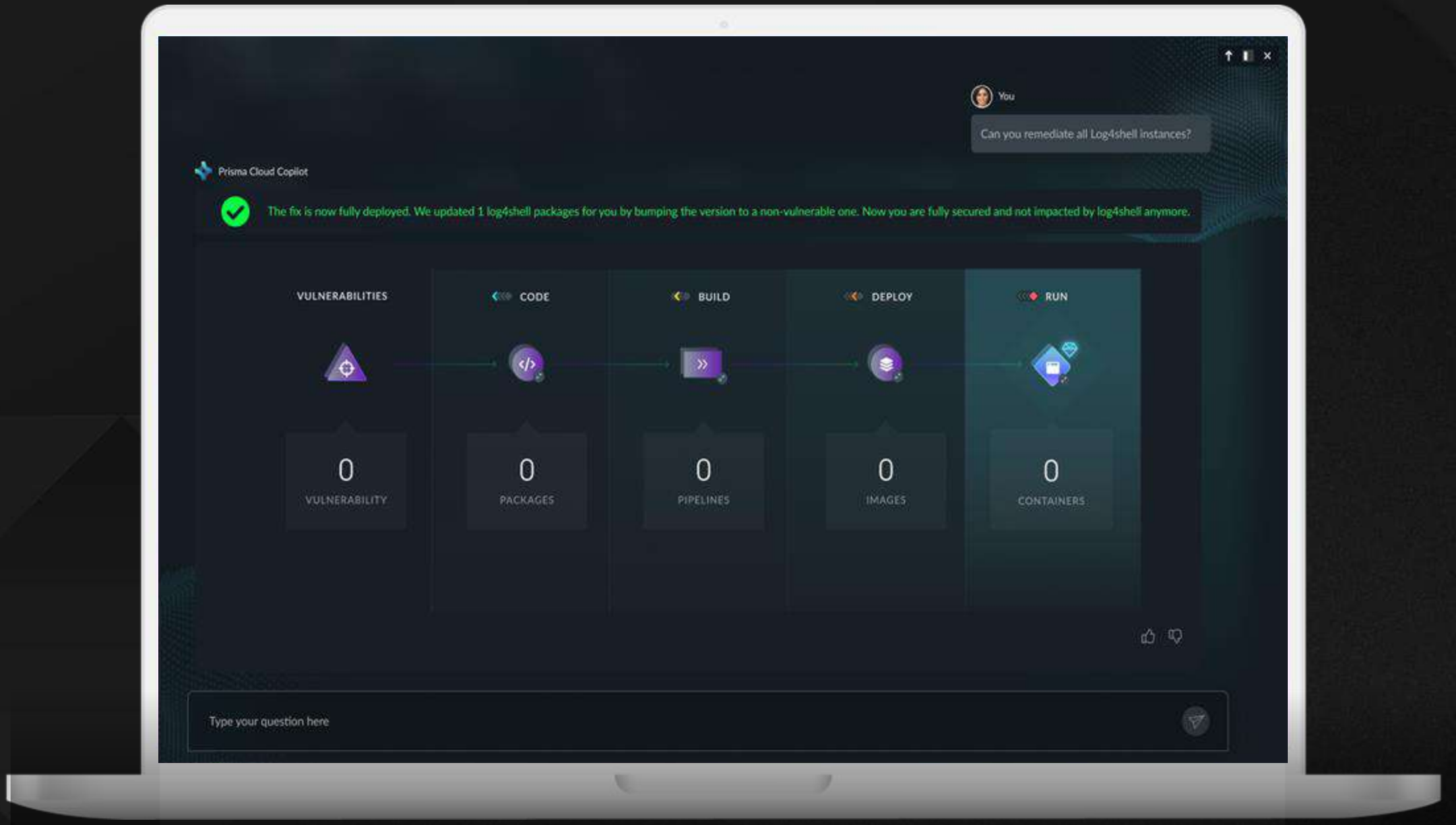
Optimize Security Outcomes

- "Good Morning" Dashboard
- Key Metrics "Ticker"
- Best Practice Guidance
- Risk Prioritization
- Remediation

Minimize Disruption from Product Issues

- "How to" & Basic Config Answers
- Troubleshooting
- In-Product Case Creation
- Detect Product Issues
- Automated Resolution

GENERATIVE AI



Looking Ahead

Organizations will require
Real-time and Autonomous Security
to Achieve Cyber Resilience

Ubiquitous Platformization will Deliver
Real-Time Security Outcomes

The Golden Formula with Data and AI for Better Cybersecurity Outcomes

Integrated, Real-Time Telemetry Data

Networks

Cloud

Endpoints

+

ML / AI Driven Automation

Strata NGFW

Cortex XSIAM

Cortex XSOAR

=

Better Cyber Outcome

Risk **10** Efficiency

SECONDS

Mean Time to Detect

TCO **1** Simplicity

MINUTE

Mean Time to Respond

(High priority alerts)

Thank You

Rabih Bou
Systems Engineer Manager
rbou@paloaltonetworks.com