

Transforming Your SOC

with Deloitte and Palo Alto Networks



Security Operations Centers of Yesterday



Security Operations Centers of Today



The Problems with Yesterday's SOC Architecture



Siloed Tools & Data

Weak Threat Defense

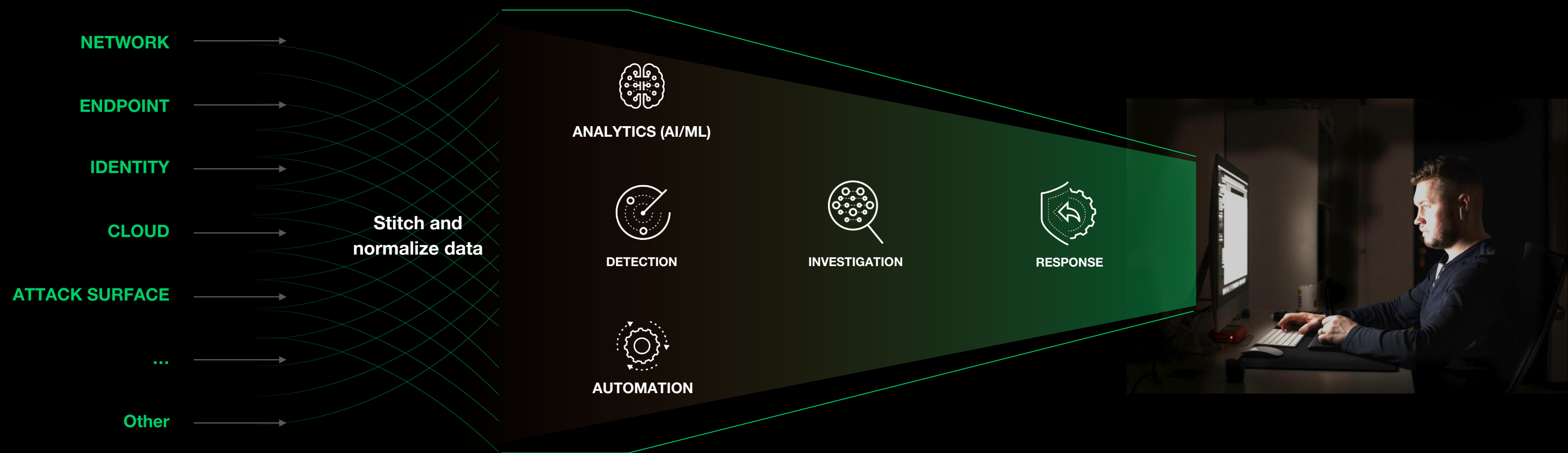
Reliance on Manual Work

11k¹ alerts per day, **23%²** are not investigated

1. Forrester: The 2020 State of Security Operations

2. ESG: SOC Modernization and the Role of XDR, October 2022

A Modern SOC requires a Single Data Platform Powered by AI




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.

Our solution is an **XSIAM-Powered** Deloitte Security **Managed Service**


SOC strategy




Governance & operating model
Deloitte.




SOC transformation advisory services
Deloitte.



Use case development / prioritization
Deloitte.



XSIAM implementation and vendor migration
 **Deloitte.**

Integration and operationalization



Integrated process & workflows
Deloitte.



Control mapping & deployment
Deloitte.



Playbook development
 **Deloitte.**



Ongoing executive status dashboards
Deloitte.

Threat detection and remediation



Policy management
Deloitte.



Threat hunting and testing
Deloitte.



Automated threat remediation




Manual threat remediation
Deloitte.

SOC technology stack



SIEM




EDR




SOAR




ASM

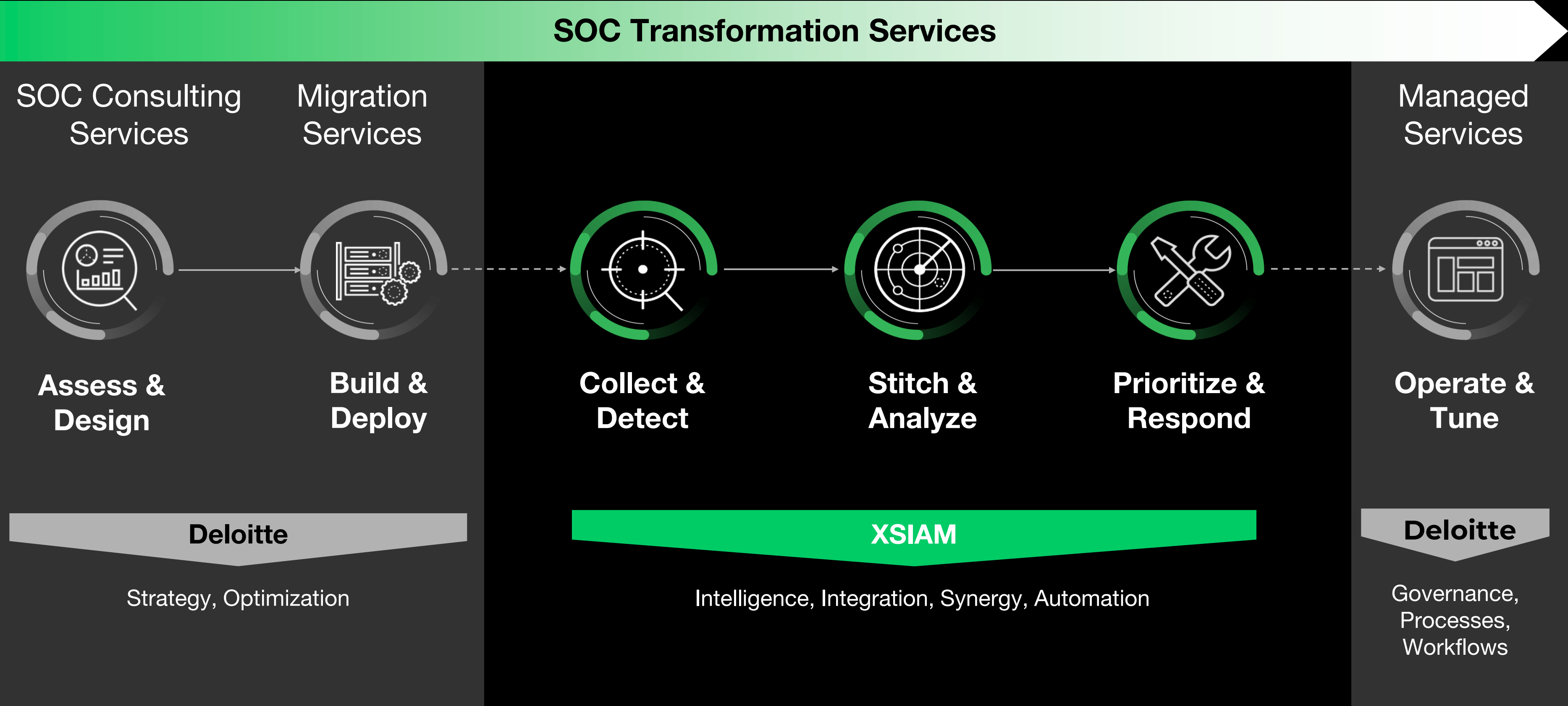



UBA




TIP


Deloitte can help you maximize your XSIAM investment



XSIAM Drives Three Key Security Outcomes



Simplifies security operations with a converged platform.



Stops threats at scale with AI-driven outcomes.



Accelerates incident remediation with an automation-first approach.

Simplify Security Operations With a Converged Platform



See all your data

Centralize, stitch, and correlate all security data.

Reduce operational complexity

Converge SOC capabilities and data processing into one platform.

FORTUNE 50 RETAILER

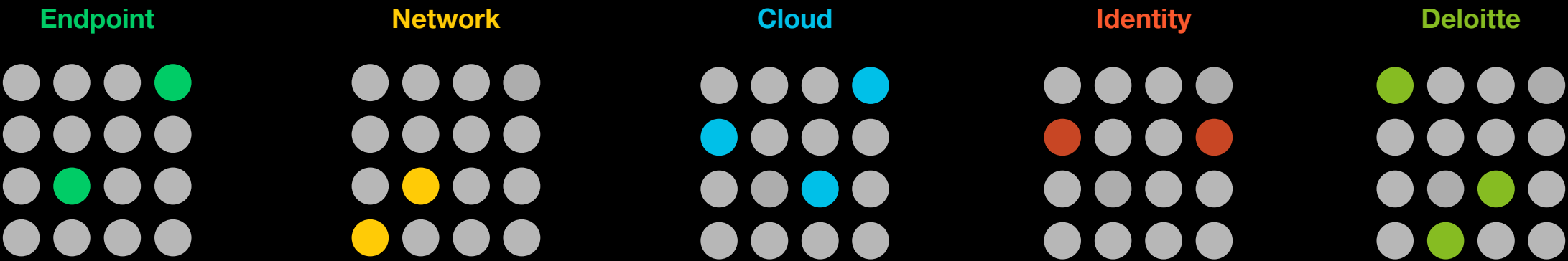
Expands visibility with additional data

From **20TB**...
per day

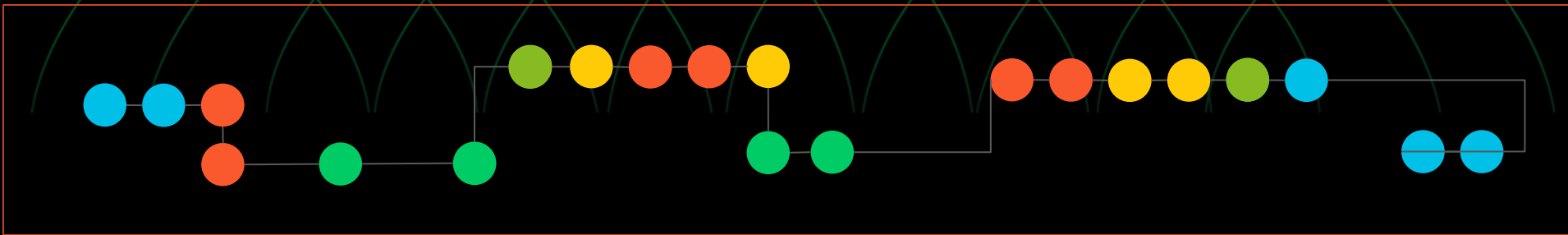
...to **60 TB**
Analyzed per day in XSIAM
using 1000+ built-in ML
models



Stops Threats at Scale **with AI-Driven Outcomes**



Data stitching creates high quality intelligence from siloed alerts



Accelerate threat analysis

Leverage AI/ML to analyze and act on data at scale from across your organization

Better detection and response

Stitched data provides the entire story for any given incident for complete context.

Dynamic protection

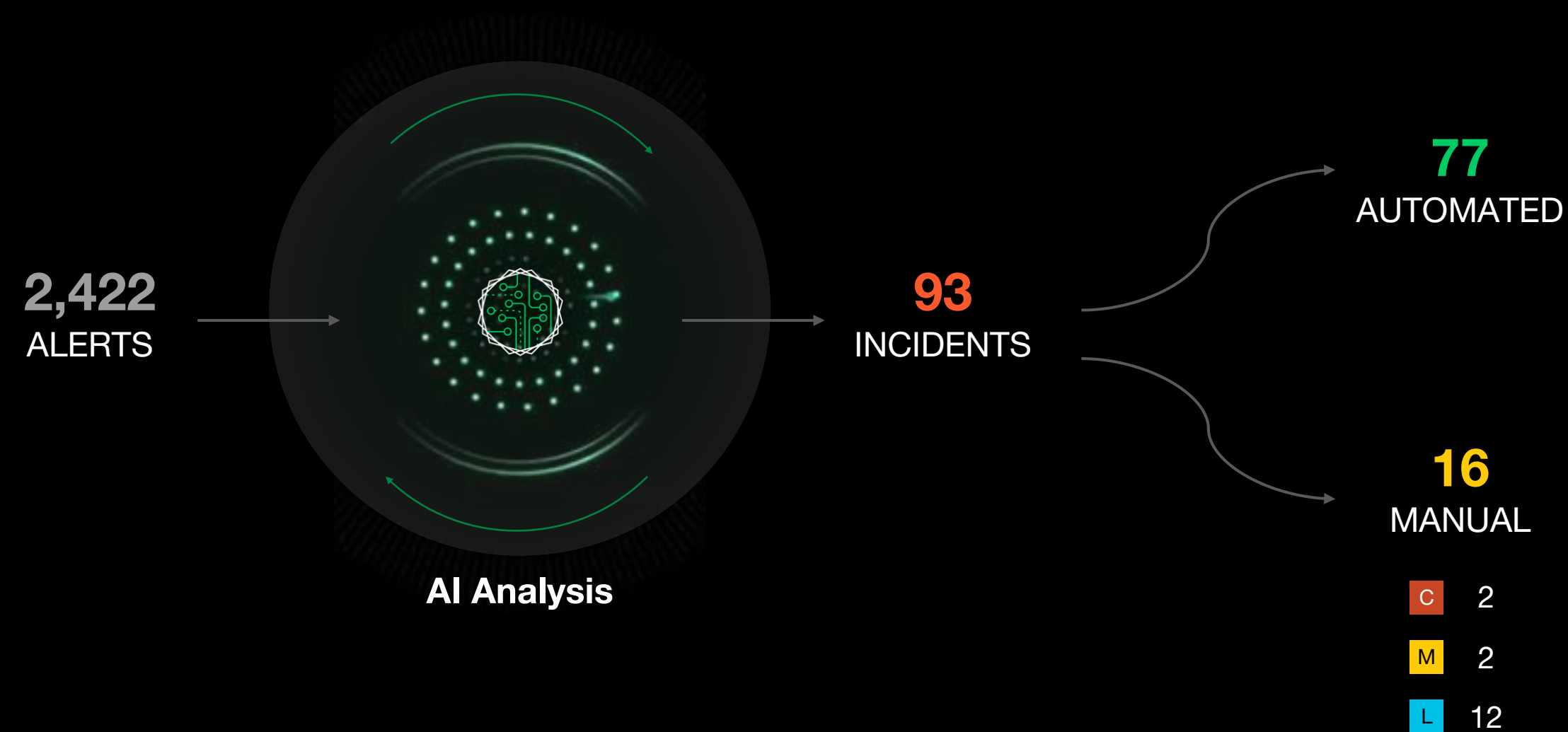
Protection adapts to the evolving threat landscape and infrastructure behavior.

Example use case:
OIL & GAS COMPANY

Reduction in false positives

From **~1,000**... incidents flagged per day
...to **~250** incidents flagged per day

Accelerate Incident Remediation With an Automation-First Approach



Reduce manual effort

Shift to a machine-led, human-empowered SOC model decreasing the manual load on analysts.

Faster detection and response

Apply automation to accelerate resolution of security incidents.

Continuous Improvement

Increase opportunities for automation as XSIAM recommends future actions.

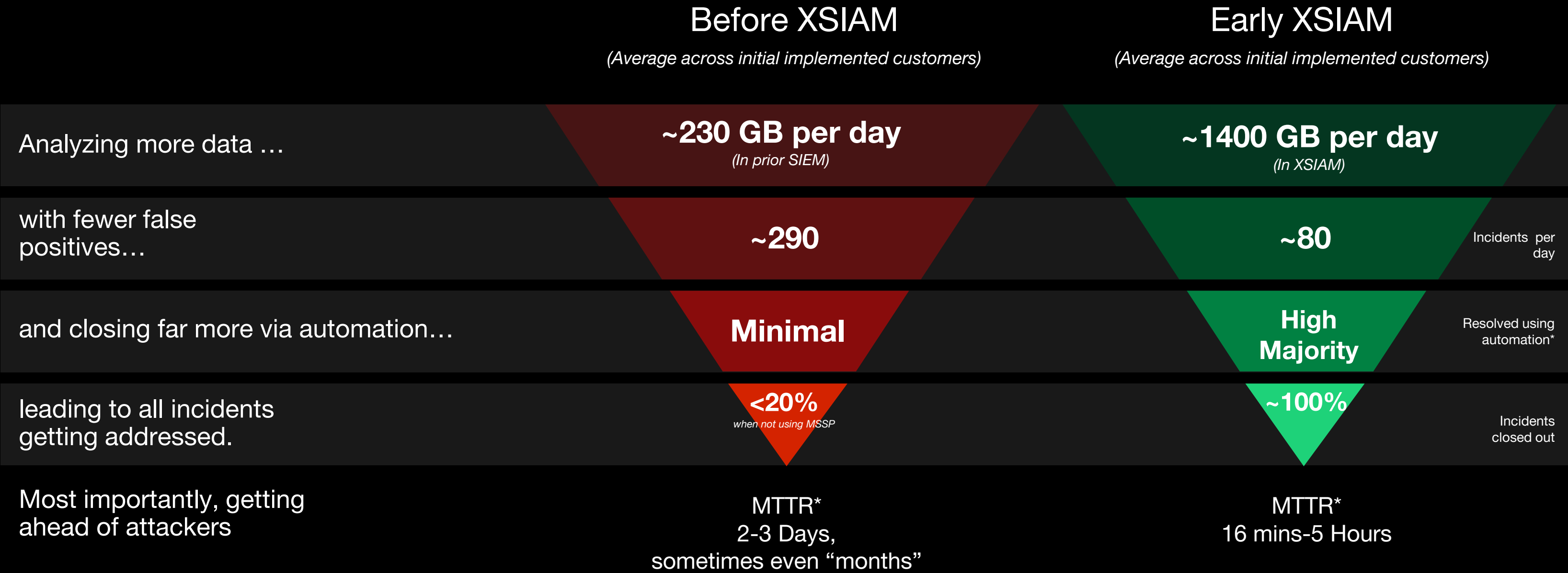
IT SERVICES COMPANY

Dramatically faster incident response

From **~2 days**
Median Time to Resolution

...to **15 minutes**
Median Time to Resolution

XSIAM is Already Driving Amazing Outcomes for Customers



“

XSIAM is the best single pane of glass I’ve seen in cybersecurity. We went from looking at 10 data stores to just XSIAM in our investigations.

– SOC Leader, XSIAM Customer

Cortex offers best-in-class SOC products, Deloitte is a Recognized MSS Leader



Cortex XDR
Named Strong Performer in the
Forrester Endpoint Security
Wave™, Q4,2023.



Cortex Delivers 100% Protection and
Detection in MITRE Engenuity



Cortex XSIAM Leader &
Outperformer, GigaOm Radar Report
2023



Cortex XDR
EPP Magic Quadrant
coming Dec



Cortex XDR
Voice of the Customer for Endpoint Protection
Platforms (2023)



Cortex XSOAR: Outperformer Leader in the
GigaOm Radar for SOAR 2x in a row

Cortex Xpanse: Only Two-Time Leader and
Outperformer In the GigaOm ASM evaluation



Cortex XSOAR: Overall Leader in the
KuppingerCole Leadership Compass
for SOAR two times in a row



2023 CYBERSECURITY WINNER
Best AI/Machine Learning/Autonomous Solution –
Palo Alto Networks, Cortex XSIAM



#1 ranked Globally in Security Consulting
12 years in a row
Source: Gartner Market Share Security Consulting Services, Worldwide, 2022



A Leader in Worldwide Cybersecurity
Risk Management Services
Source: IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment, by Phillip D. Harris, October 2023, IDC # US49435222



A Leader in Worldwide Managed Cloud Security Services
Source: IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment, by Cathy Huang, September 2022, IDC # US48761022

- **30+ year history** providing cybersecurity services and support, including 10+ years of delivering managed services
- **2,700+ cyber clients** from enterprise to mid-enterprise across all major industries, focused on trusted, transformative relationships
- **Access to 25K+ cyber practitioners worldwide** with depth and breadth of technology, business, and industry knowledge and experience
- **Global \$5B** hyperscale investment in Cyber, Cloud, and AI – focused on solutions, talent, acquisitions, and ecosystem
- **3 Cybersphere centers** providing 24x7x365, globally consistent & reliable operational support and solution delivery, augmented by network of in-region delivery centers
- **Access to an expansive global network** enabling contextualization of services by combining the strength of the a leading professional services organization with in-depth knowledge & experience in local markets

Thank You

paloaltonetworks.com

deloitte.com

This presentation contains general information only and Palo Alto and Deloitte are not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Palo Alto and Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.