The Modern SOC Platform

Rouzbeh Nikberg

Richard Glantz

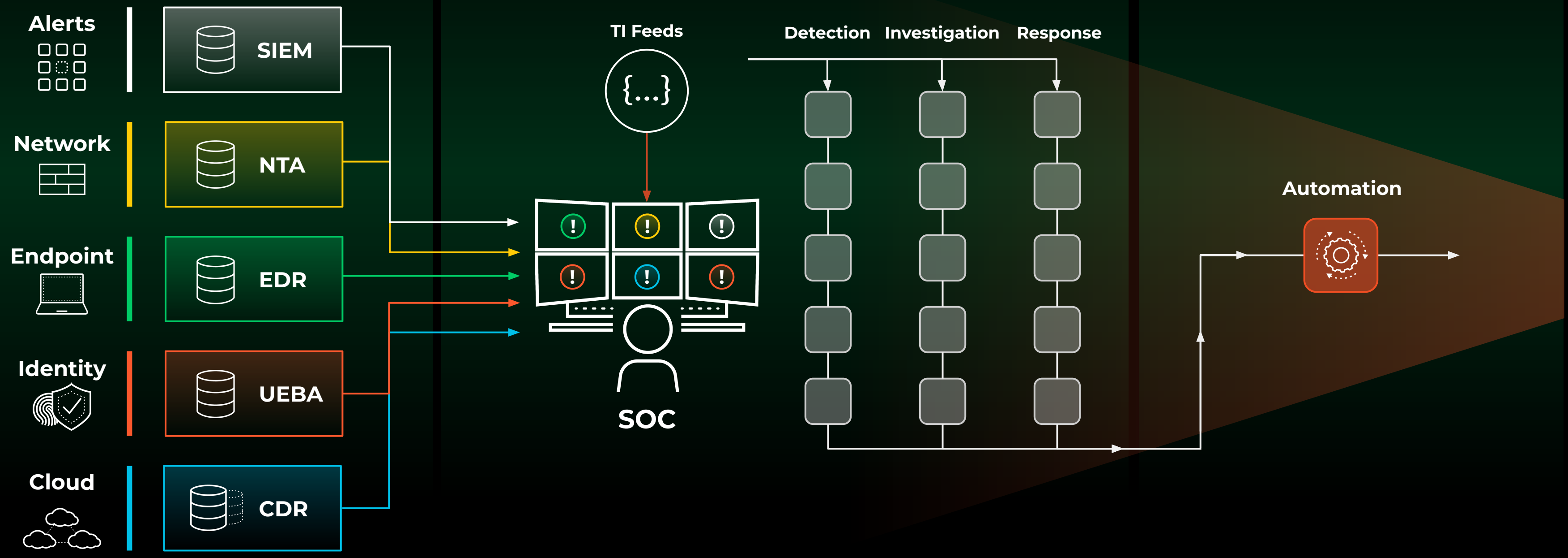
paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

The Current State of the SOCs

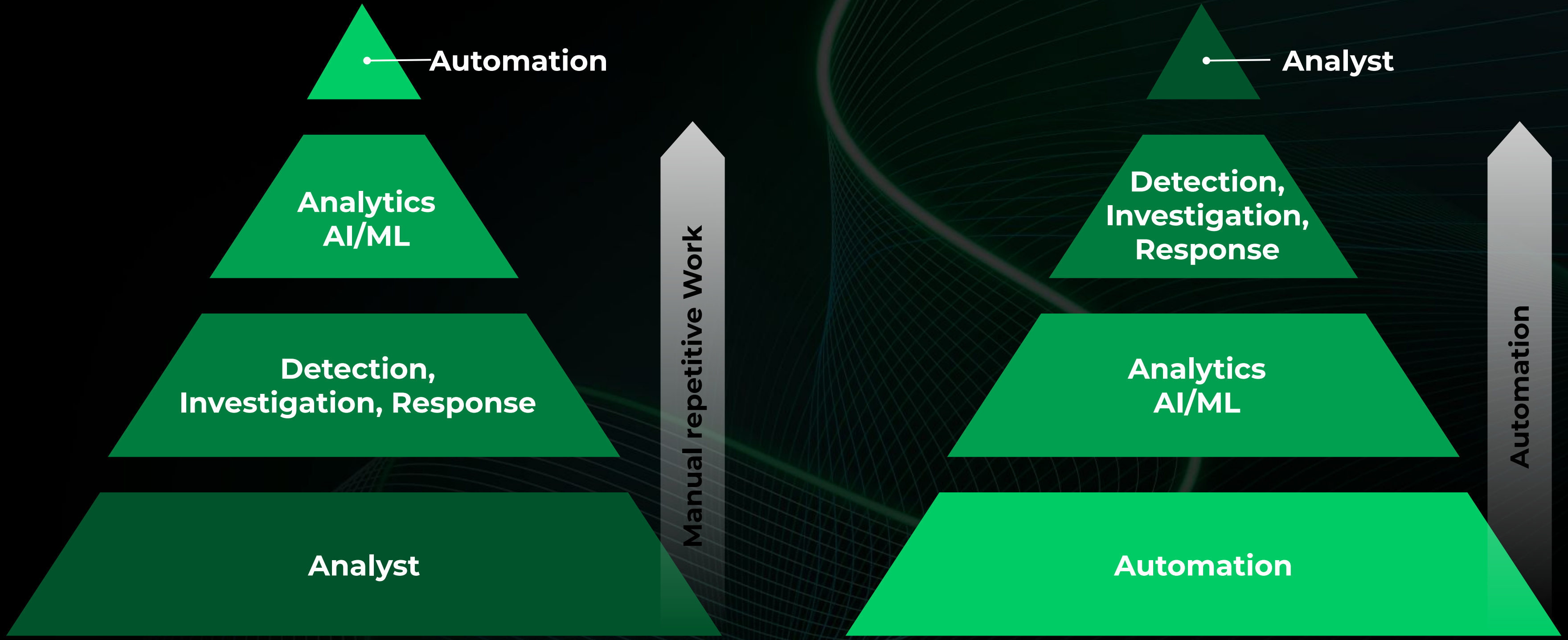
Too many data silos make it hard to detect attacks

Teams build and maintain detection content, use multiple tools to manually investigate & respond

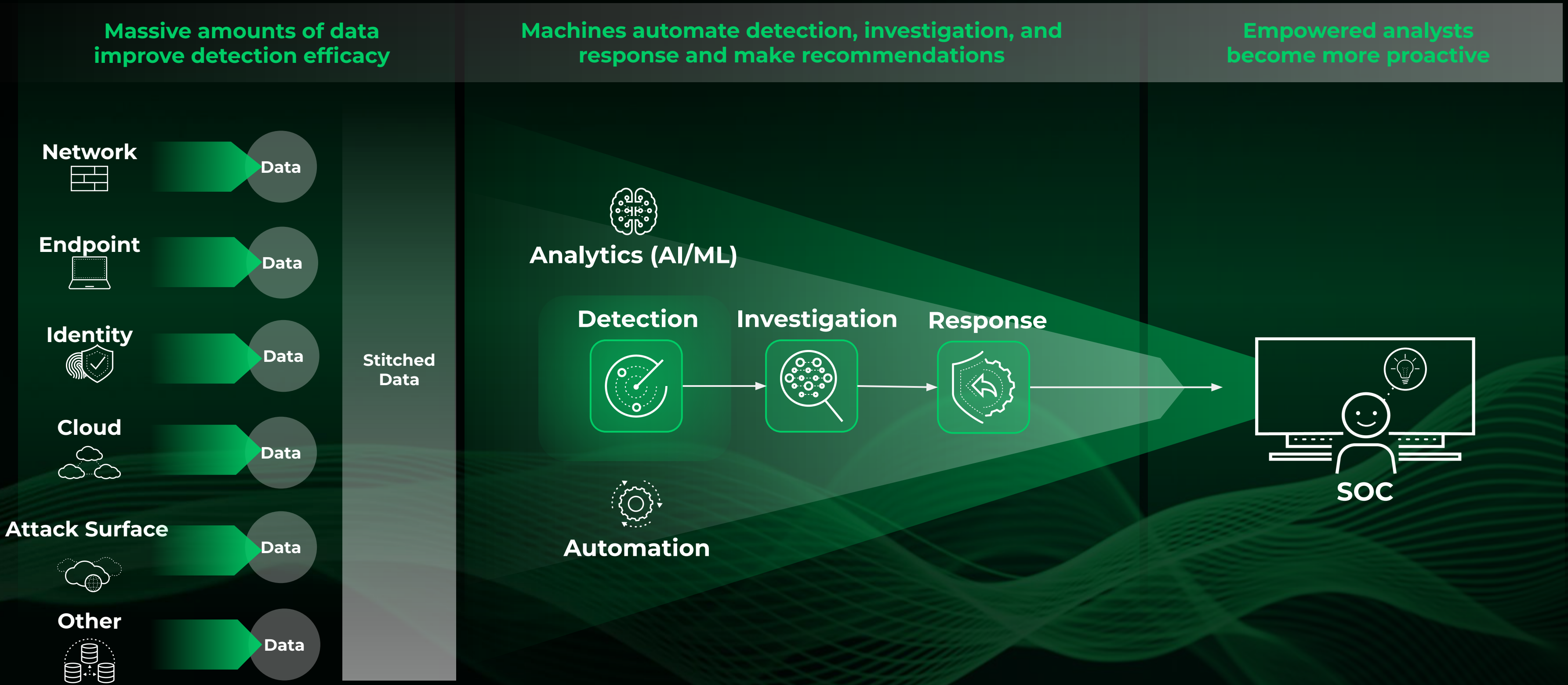
Automation is bolted on at the end to scale it



Palo Alto Networks is changing the Focus



We Must Transform the SOC to be Machine-led, Human Empowered



Massive amounts of data improve detection efficacy

Machines automate detection, investigation, and response and make recommendations

Empowered analysts become more proactive

Network – Data

Endpoint – Data

Identity – Data

Cloud – Data

Attack Surface – Data

Other – Data

Stitched Data

Analytics (AI/ML)

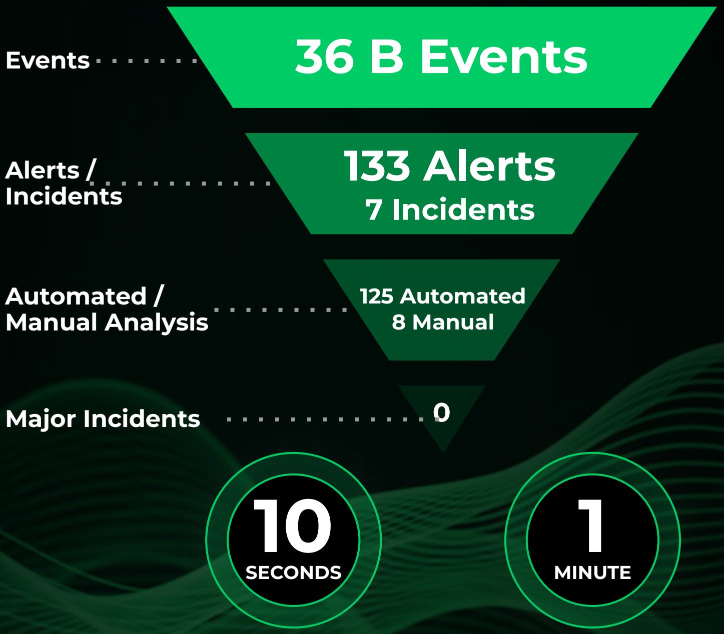
Detection → Investigation → Response → SOC

Automation

The Palo Alto Networks “Realtime” SOC Use Case

XSIAM
Orchestration & Automation
Endpoint Protection & Intelligence
Threat Intel Management
UEBA, Network, Cloud analytics
Threat Detection & Response
Attack Surface Management
Reporting & Compliance
Data Foundation & Detection Analytics

WHAT’S POSSIBLE WITH THE AUTOMATED SOC



Events · · · · · · 36 B Events

Alerts / Incidents · · · · · · · · · · 133 Alerts 7 Incidents

Automated / Manual Analysis · · · · · · · · 125 Automated 8 Manual

Major Incidents · · · · · · · · · · · · · 0

10 SECONDS

Mean Time to Detect

1 MINUTE

Mean Time to Respond (High priority)

Tack!