Introducing the Autonomous SOC

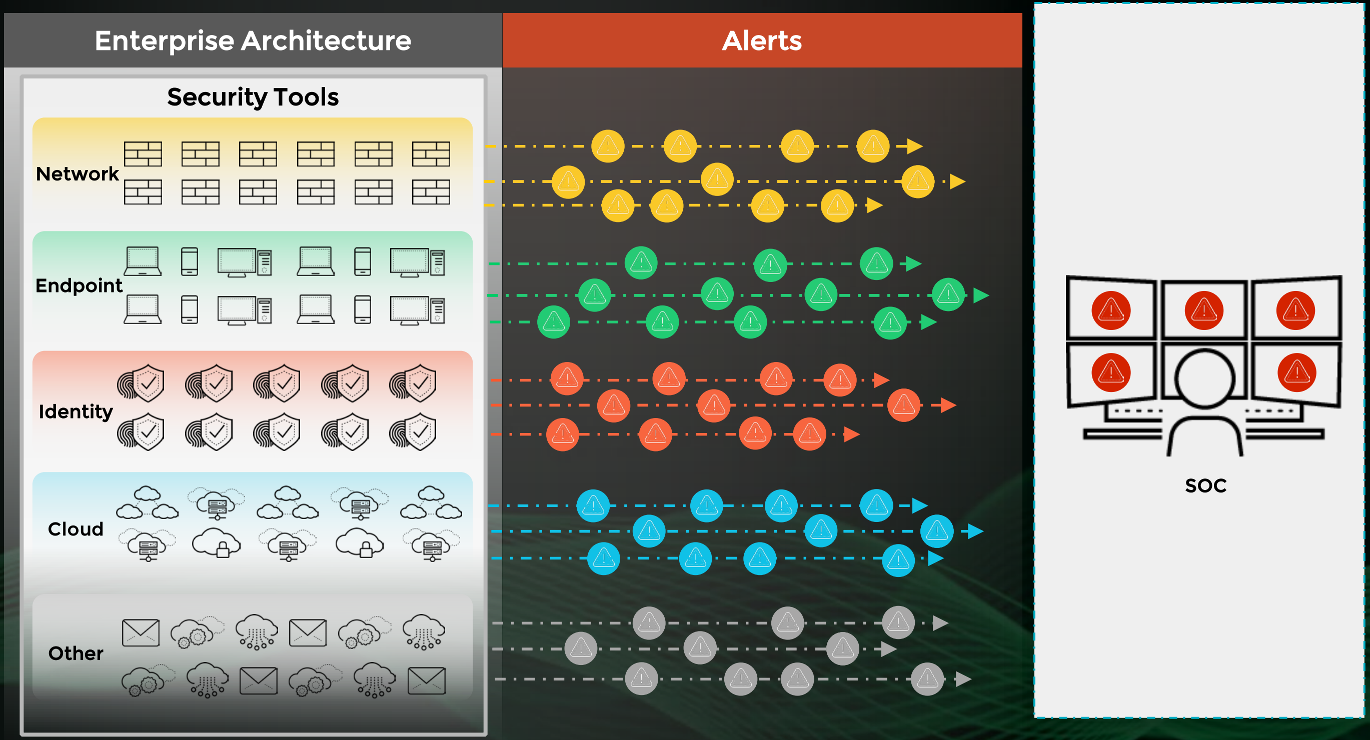
Cortex XSIAM

Ilias Polychroniadis
Regional Systems Engineer

The modern SOC challenges and the reality of the SecOps team

The misery of SecOps

The challenge: The volume of alerts is overwhelming most SOCs



Enterprise Architecture

Alerts

Security Tools

Network

Endpoint

Identity

Cloud

Other

SOC

TYPICAL INDUSTRY NUMBERS

~75

Security products to monitor assets

~11K

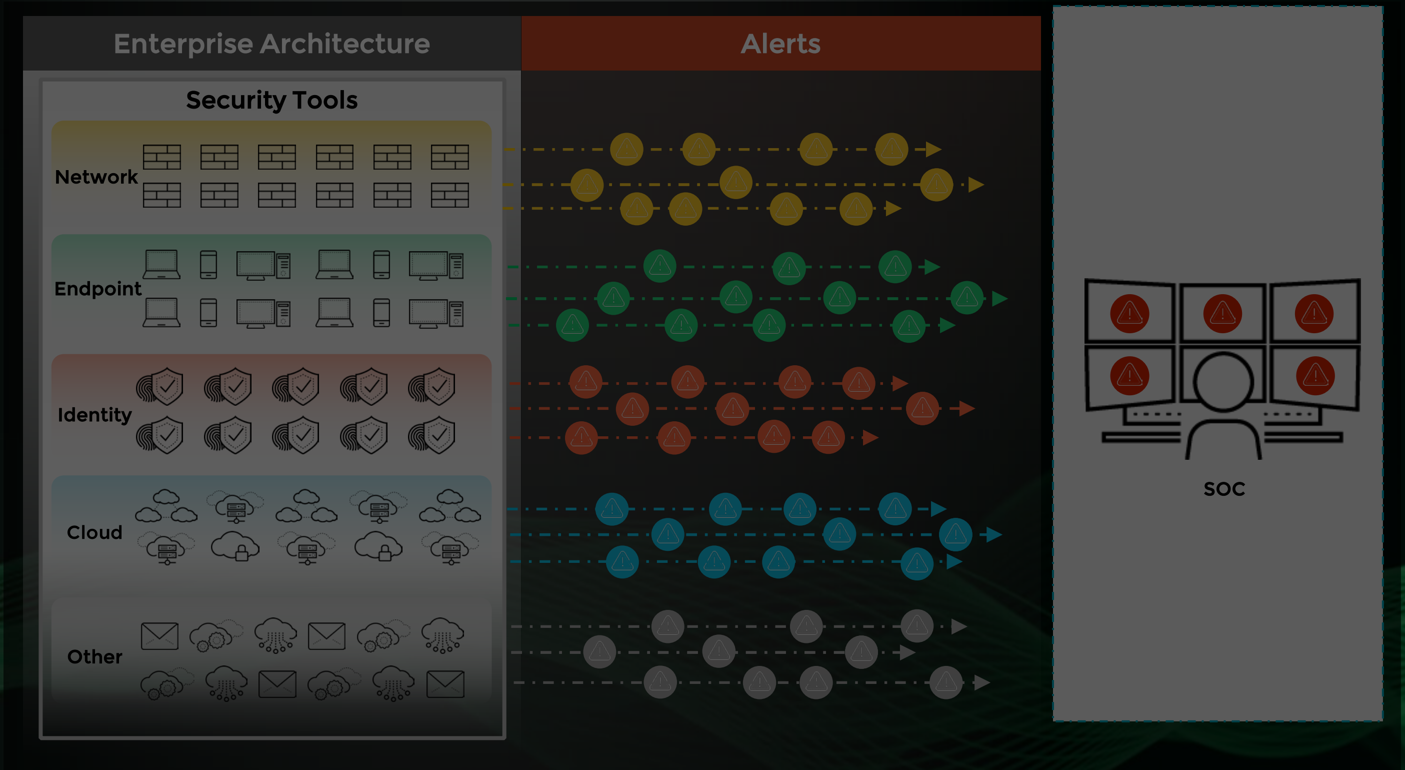
Alerts / day; only 17% touched by automation

28%

Alerts ignored

Source: Forrester (The 2020 State of Security Operations), Demisto (The State of SOAR Report, 2018)

The challenge: The volume of alerts is overwhelming most SOCs



Source: Forrester (The 2020 State of Security Operations), Demisto (The State of SOAR Report, 2018)

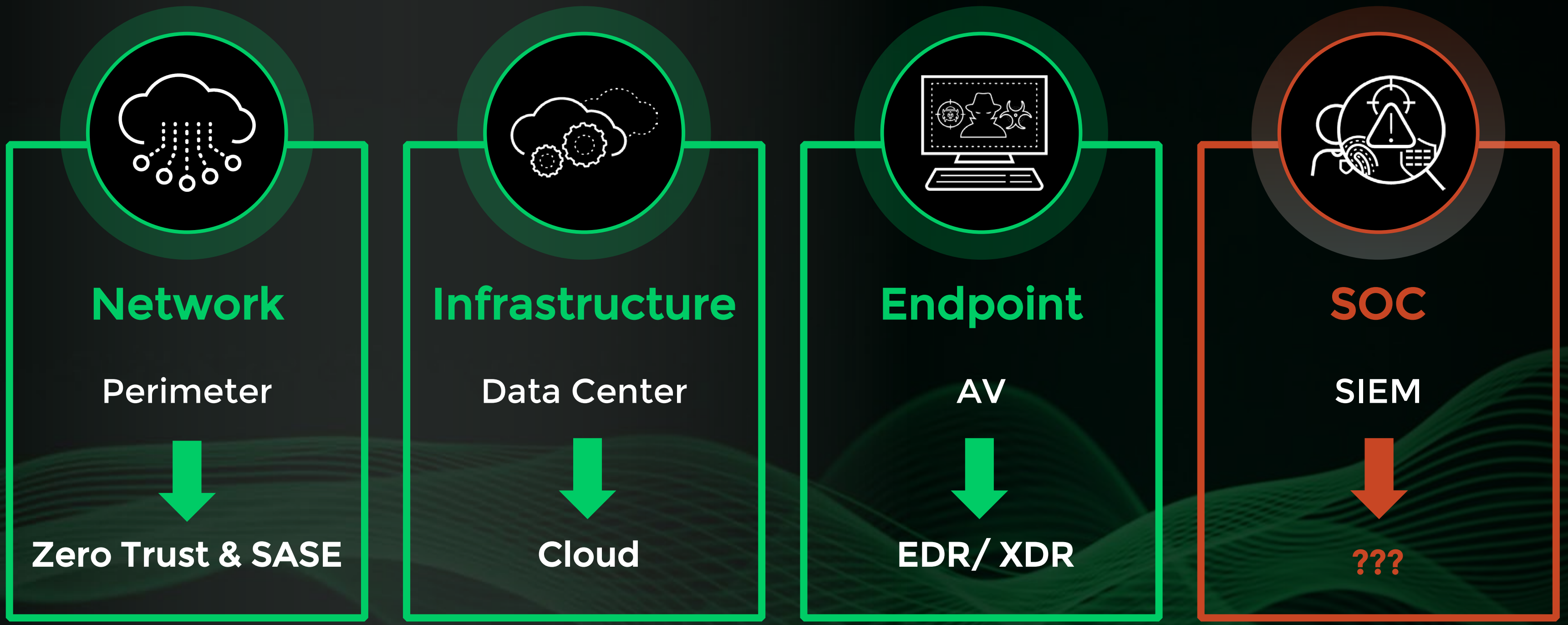
TYPICAL INDUSTRY NUMBERS

4+
Days to investigate

287
Avg days to identify and contain a data breach

<30%
of SOC teams meet their KPI goals

Most Security Real Estate Has Been Redesigned, Except...



Network

Perimeter

↓

Zero Trust & SASE

Infrastructure

Data Center

↓

Cloud

Endpoint

AV

↓

EDR/ XDR

SOC

SIEM

↓

???

Some alarming facts….

CISOs & Security Executives

- 88% consider themse moderate or high stre switch off during
- 90% said they'd ta their work-life bal
- 48% says that the s health.
- 32% admits being a relationships
- 23% needs some typ alcohol
- 97% of the C-Suite said t team could improve on delivering value for the amount of budget they receive.

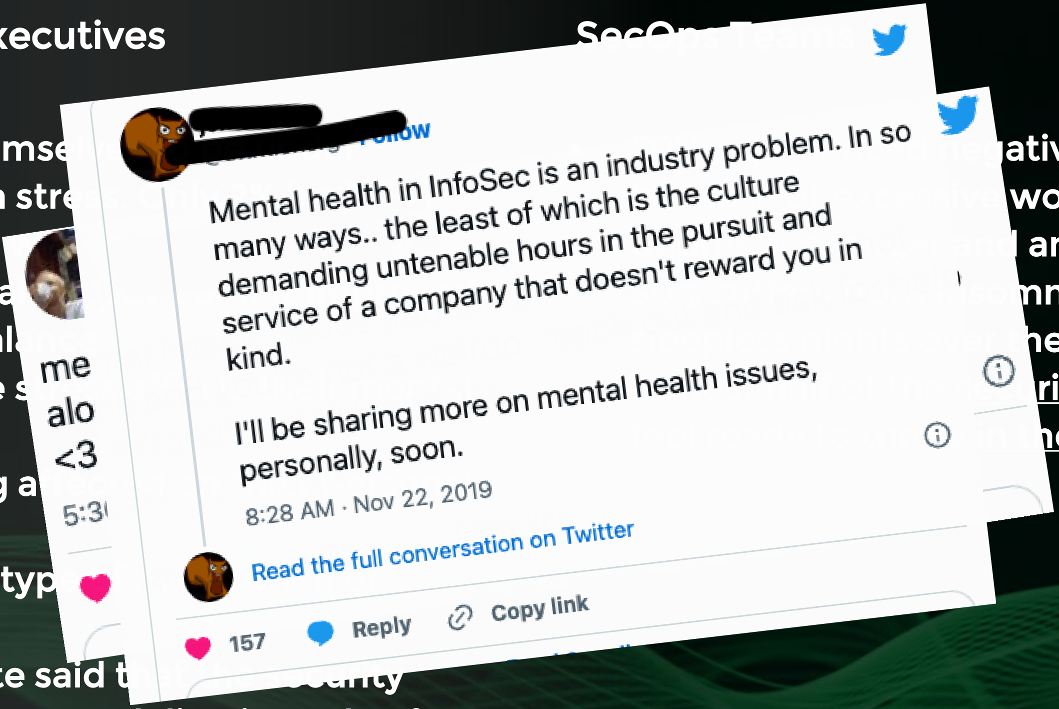
Source: Nominet CISO Stress Report (2020)

SecOps Teams

ative emotions work, including anxiety.

mnia and had he past year

rity professionals he towel...



me alo <3

5:3

[redacted] Follow

Mental health in InfoSec is an industry problem. In so many ways.. the least of which is the culture demanding untenable hours in the pursuit and service of a company that doesn't reward you in kind.

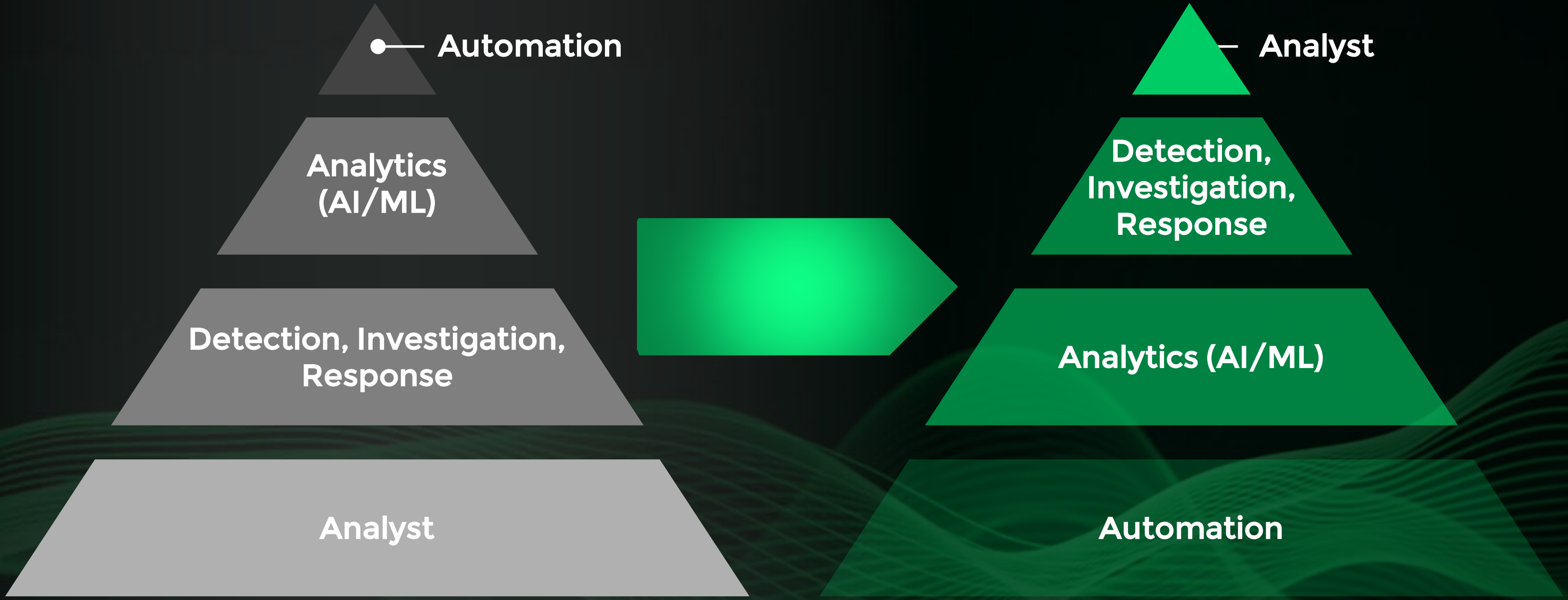
I'll be sharing more on mental health issues, personally, soon.

8:28 AM · Nov 22, 2019

Read the full conversation on Twitter

The Next Generation SOC needs to be Machine-led, Human Empowered

The Transition to Analyst-Assisted Security Operations



Automation

Analytics (AI/ML)

Detection, Investigation, Response

Analyst

Analyst

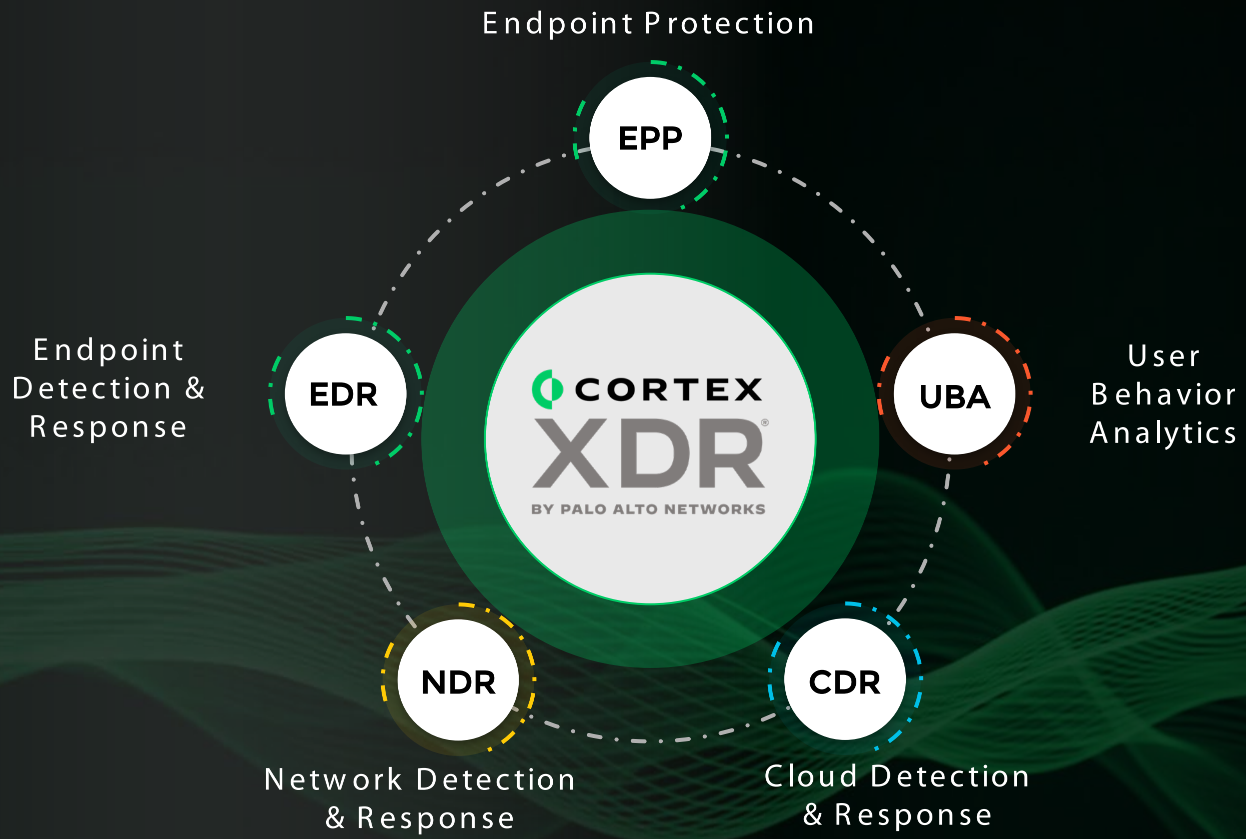
Detection, Investigation, Response

Analytics (AI/ML)

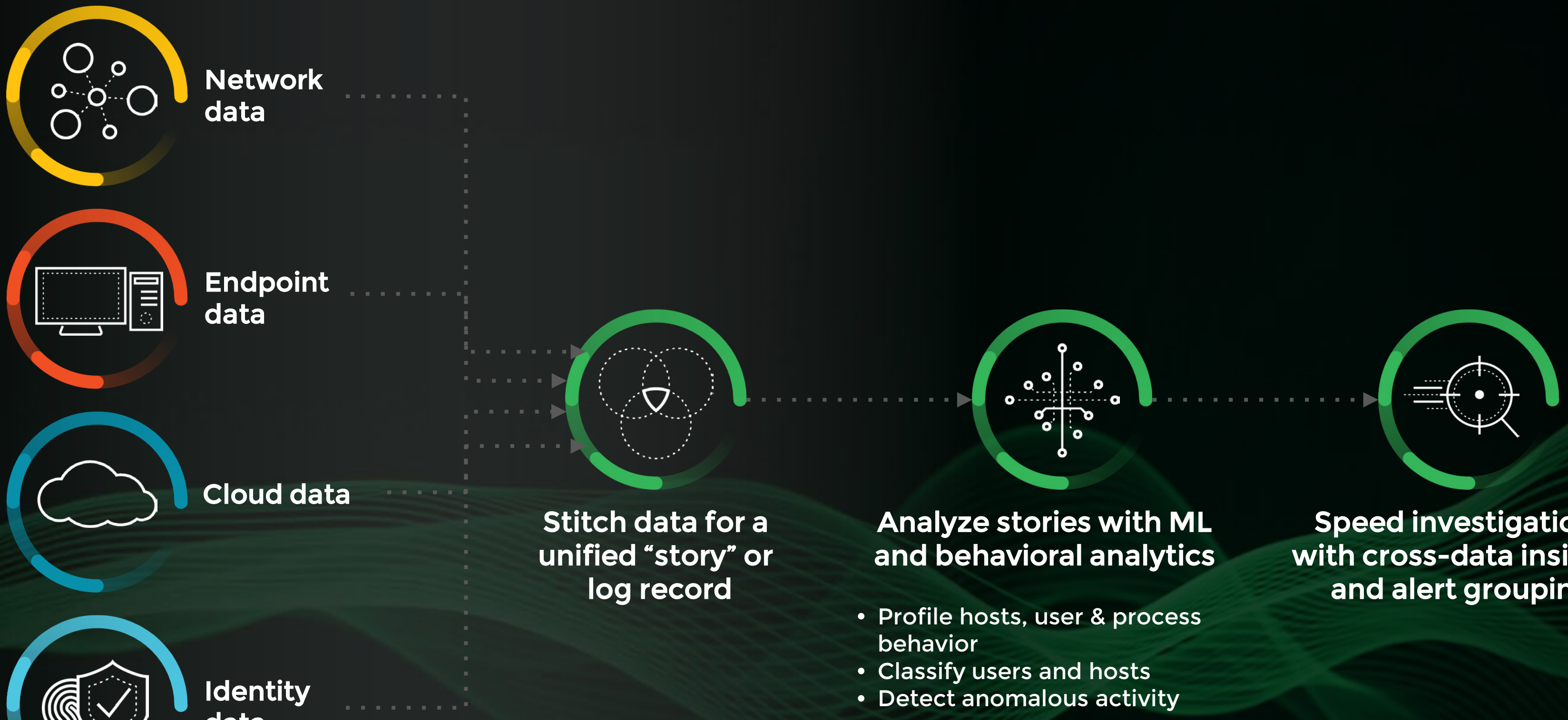
Automation

Introducing the Autonomous SOC

Cortex XDR: Breaks down data and product silos



Cortex XDR: Detect and Investigate Threats with Cross-Data Analytics & Insights



Network data

Endpoint data

Cloud data

Identity data

Stitch data for a unified “story” or log record

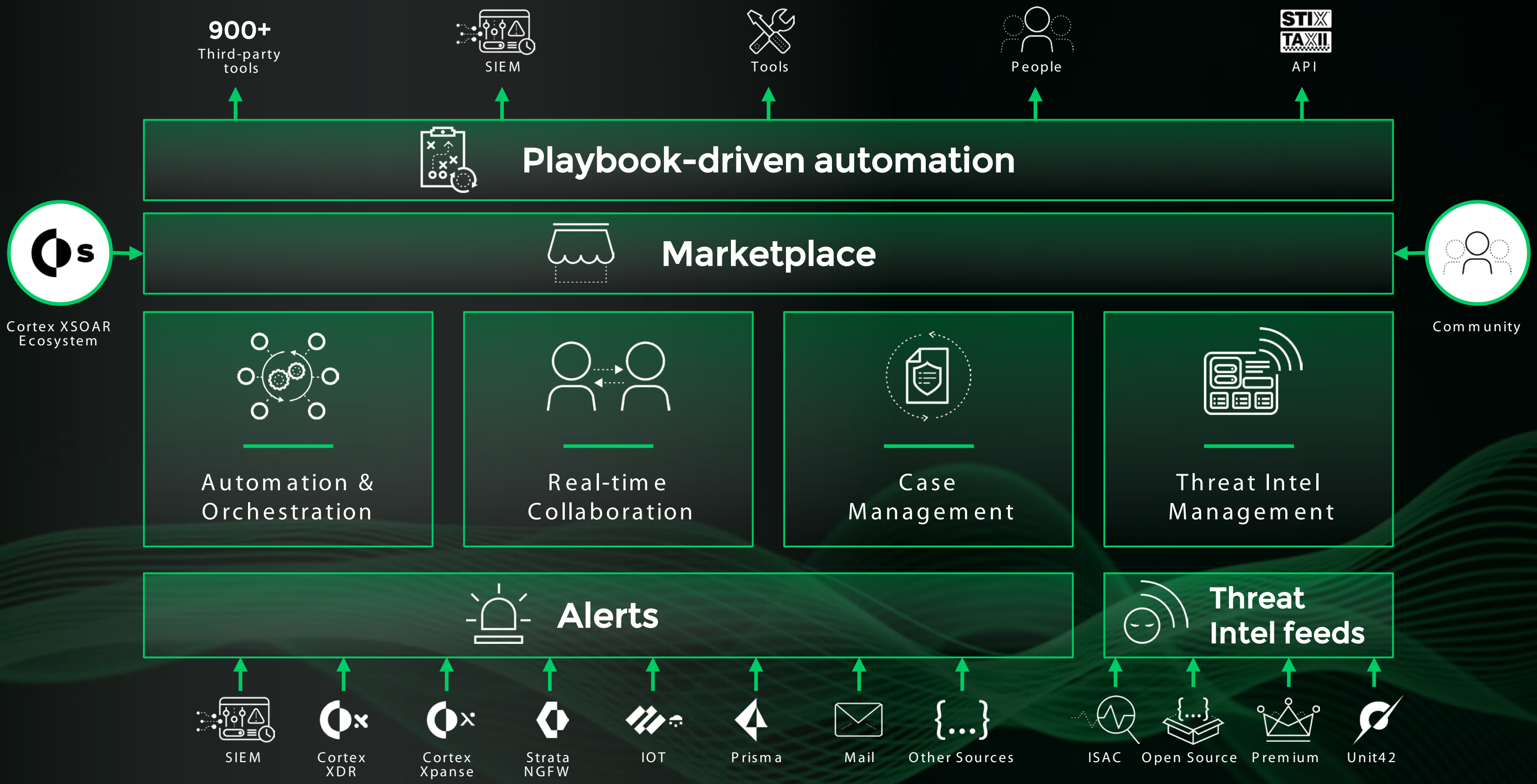
Analyze stories with ML and behavioral analytics

- Profile hosts, user & process behavior
- Classify users and hosts
- Detect anomalous activity

Speed investigations with cross-data insights and alert grouping

* Cloud data includes Prisma Access, VM Series, and cloud flow logs

Cortex XSOAR



900+ Third-party tools

SIEM

Tools

People

STIX TAXII API

Playbook-driven automation

Cortex XSOAR Ecosystem

Marketplace

Community

Automation & Orchestration

Real-time Collaboration

Case Management

Threat Intel Management

Alerts

Threat Intel feeds

SIEM

Cortex XDR

Cortex Xpanse

Strata NGFW

IOT

Prisma

Mail

Other Sources

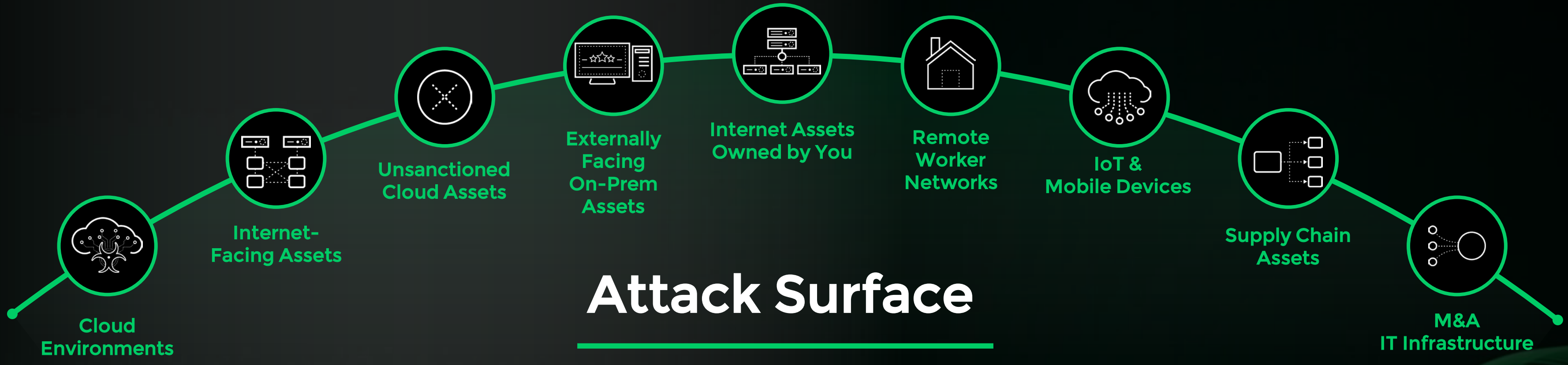
ISAC

Open Source

Premium

Unit42

Cortex Xpanse: Proactively Find and Shut Down Risks



Cloud Environments

Internet-Facing Assets

Unsanctioned Cloud Assets

Externally Facing On-Prem Assets

Internet Assets Owned by You

Remote Worker Networks

IoT & Mobile Devices

Supply Chain Assets

M&A IT Infrastructure

Attack Surface

Discover Exposed Assets & Risky Services

Continuously Monitor Attack Surface

Quickly Mitigate & Block Access

Cortex XSIAM

Extended Security Intelligence & Automation
Management

The Autonomous Security Platform
Powering the Modern SOC.

XSIAM: Designed Around Three Key Concepts

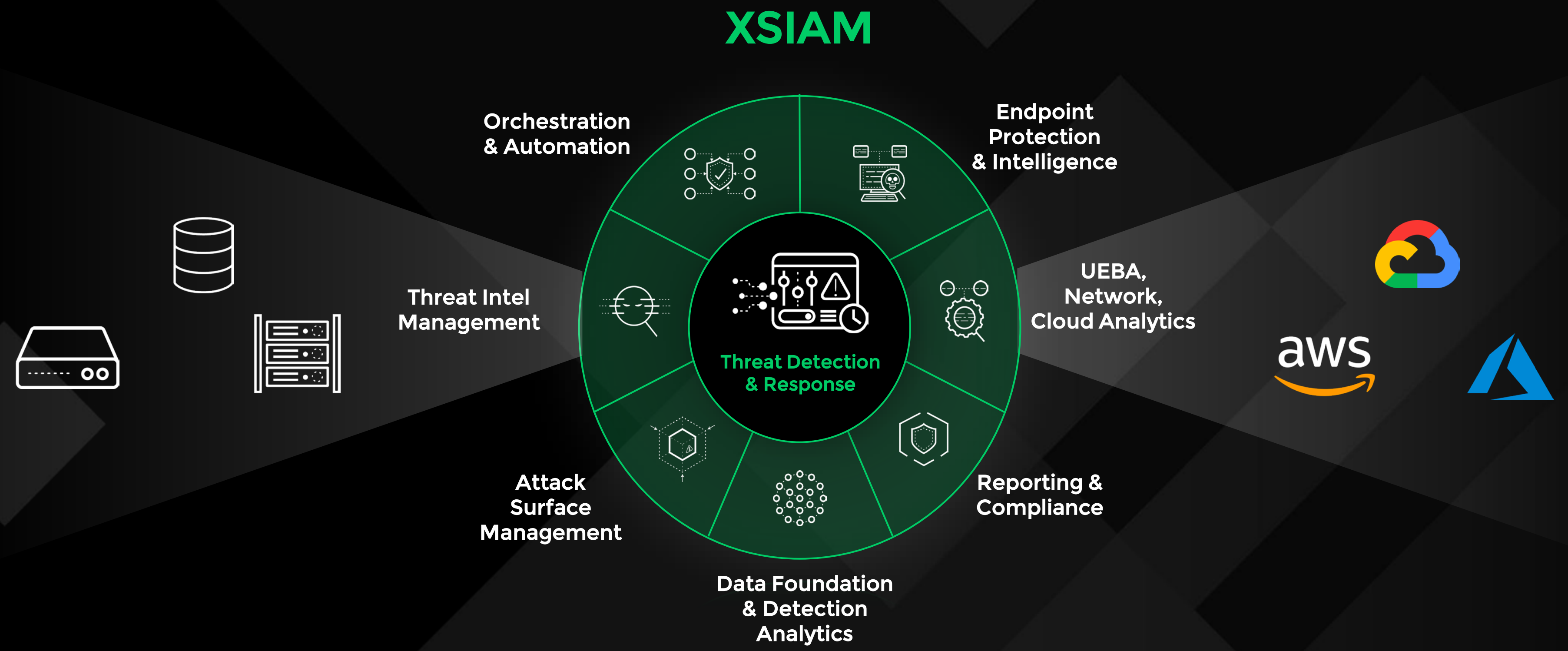
Intelligent Data & Analytics

Automation First

Proactive Security

XSIAM delivers a transformation in detection and response, analyst experience, and continuous risk reduction.

XSIAM: The Next Big Transformation in Security Operations



XSIAM

Threat Detection & Response

Orchestration & Automation

Endpoint Protection & Intelligence

UEBA, Network, Cloud Analytics

Reporting & Compliance

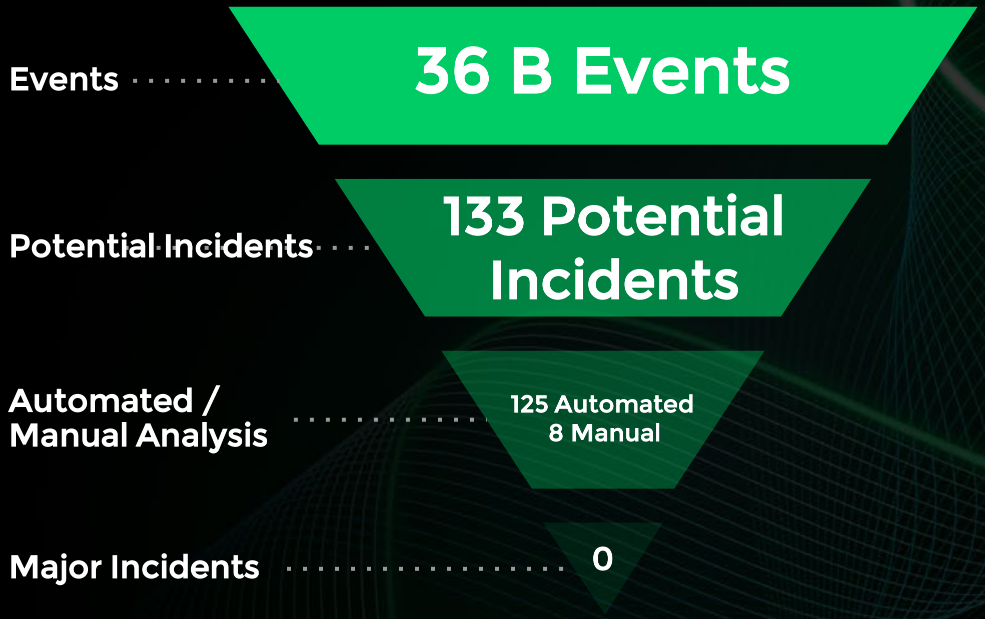
Data Foundation & Detection Analytics

Attack Surface Management

Threat Intel Management

The Proof: We have Achieved a 1 min. Response Time

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



Events — 36 B Events

Potential Incidents — 133 Potential 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)

Less Busywork.

More Security.

Thank you :)

paloalto NETWORKS