Automating the modern SOC:

Responding and recovering from cyber incidents at machine speed

Eirik Valderhaug

Sr. Principal Systems Engineer Specialist

Cortex EMEA

Who is Palo Alto Networks?

Network Security

STRATA | PRISMA SASE

Best-in-class security delivered across hardware, software and SASE

Cloud Security

PRISMA CLOUD

Comprehensive platform to secure everything that runs in the cloud

Security Operations

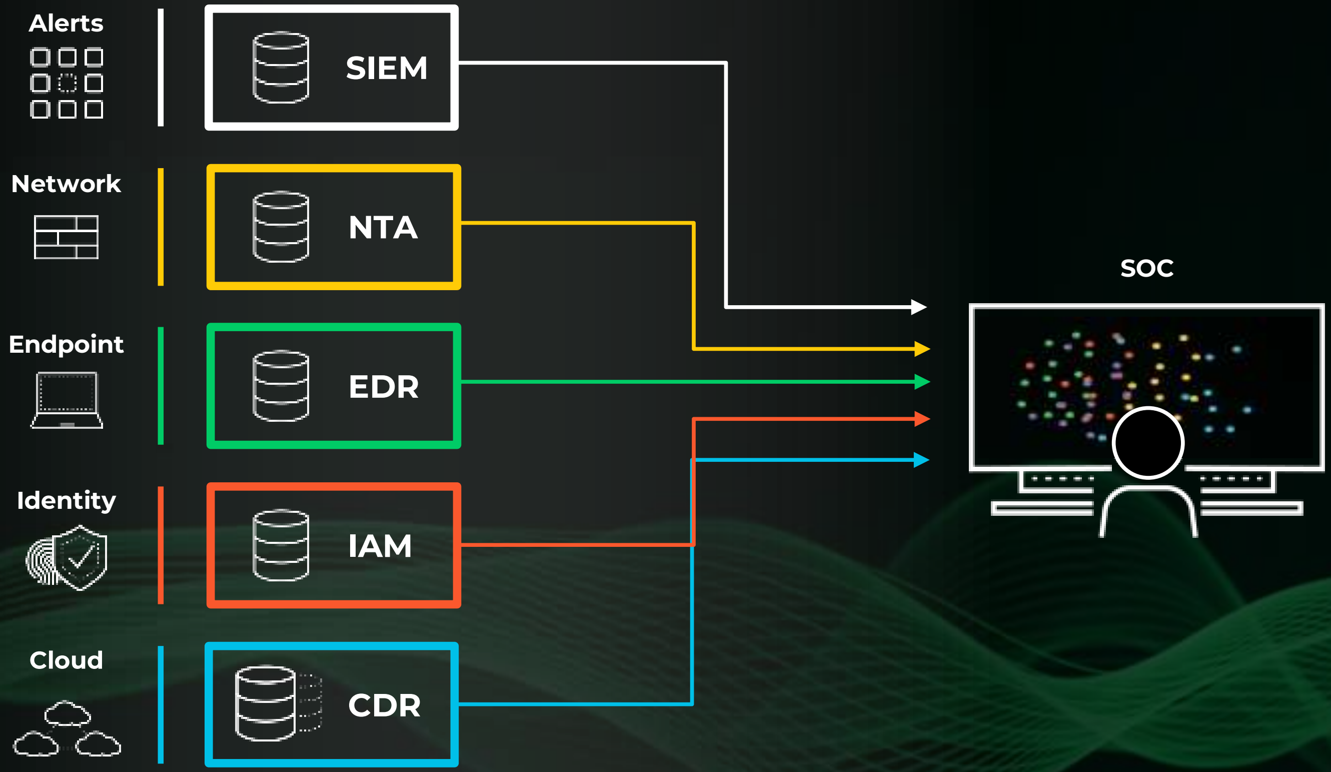
CORTEX

A new approach to SOC with fully integrated data, analytics and automation

Threat Intelligence and Advisory Services

World-renowned threat intelligence, cyber risk management and advisory services

The Problem: Too Much Info, Too Many Silos, Not Enough Insight



~11K
Alerts per day[1]

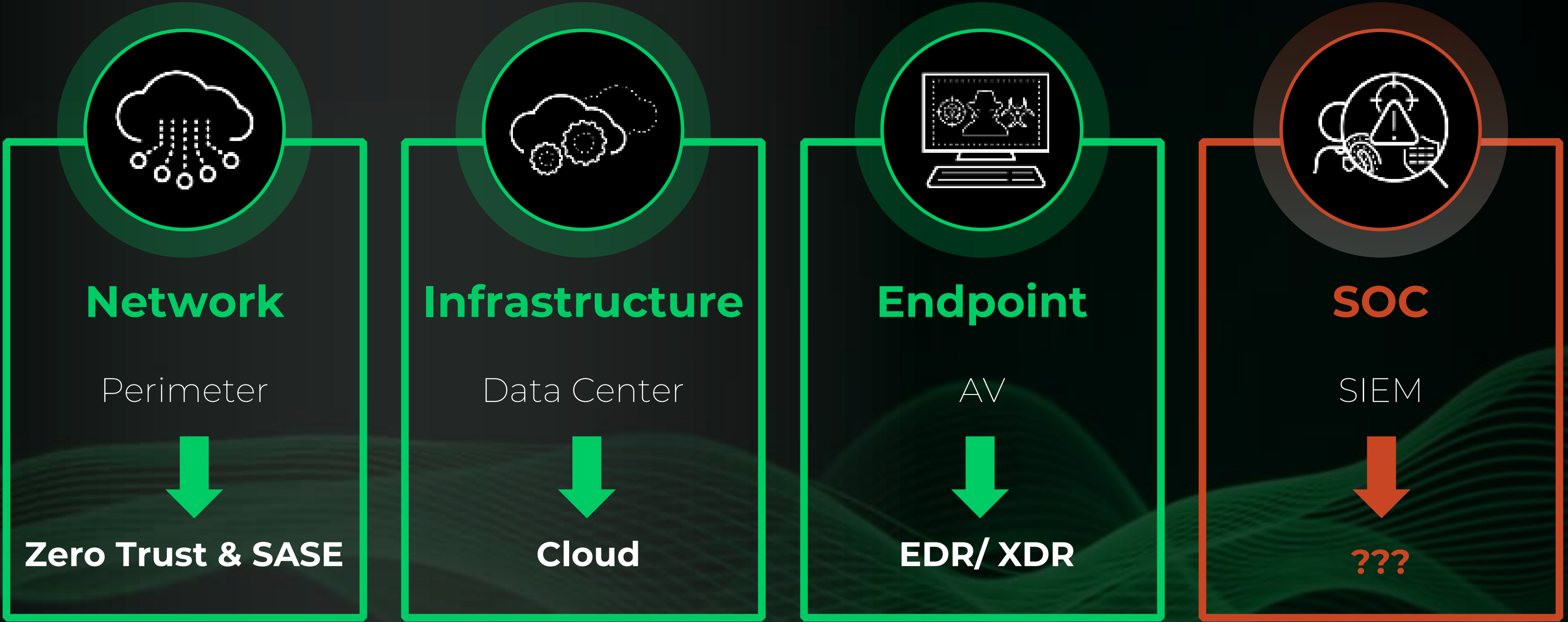
4+
Days to investigate[2]

< 30%
of SOC teams meet KPI goals

207
Days of dwell time[3]

[1] Forrester, The 2021 State of Security Operations
[2] The State of SOAR Report
[3] 2022 Ponemon report

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



Network

Perimeter

↓

Zero Trust & SASE

Infrastructure

Data Center

↓

Cloud

Endpoint

AV

↓

EDR/ XDR

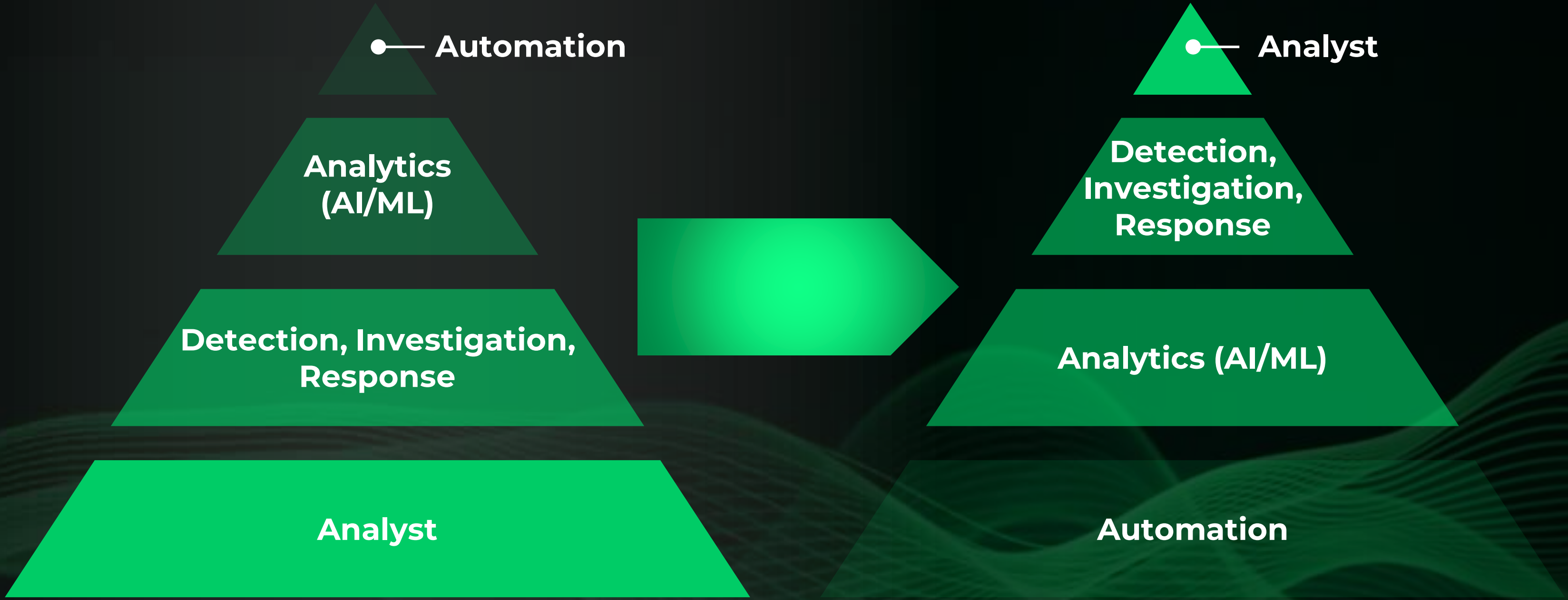
SOC

SIEM

↓

???

We Need to Transition to Analyst-Assisted Security Operations


Automation
Analytics (AI/ML)
Detection, Investigation, Response
Analyst
Analyst
Detection, Investigation, Response
Analytics (AI/ML)
Automation

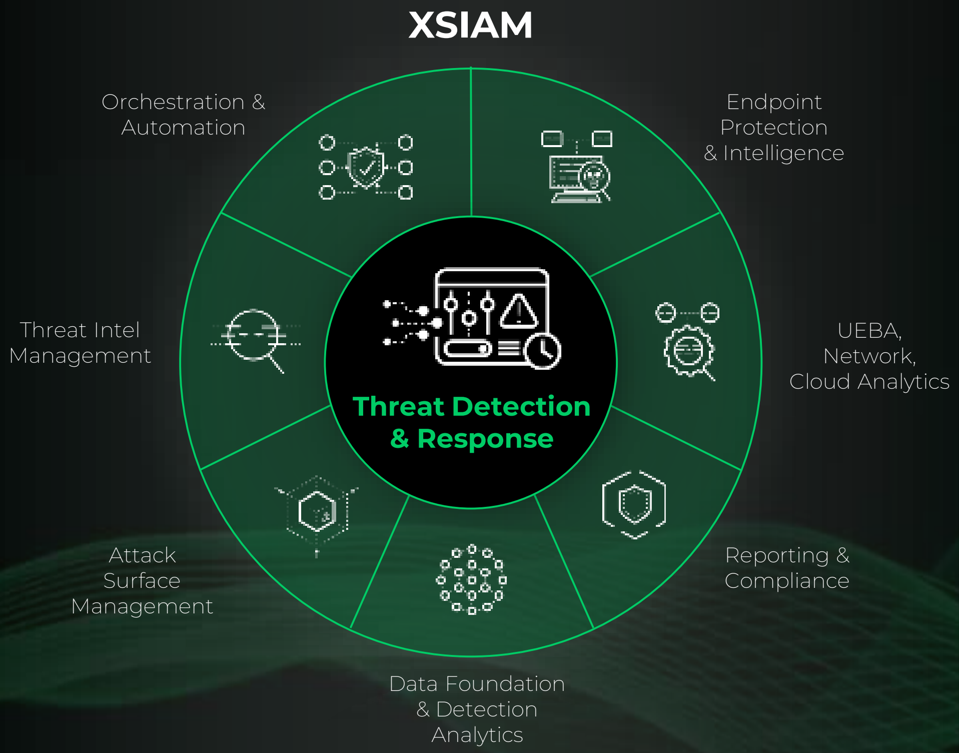
XSIAM: Designed Around Three Key Concepts

Intelligent Data & Analytics

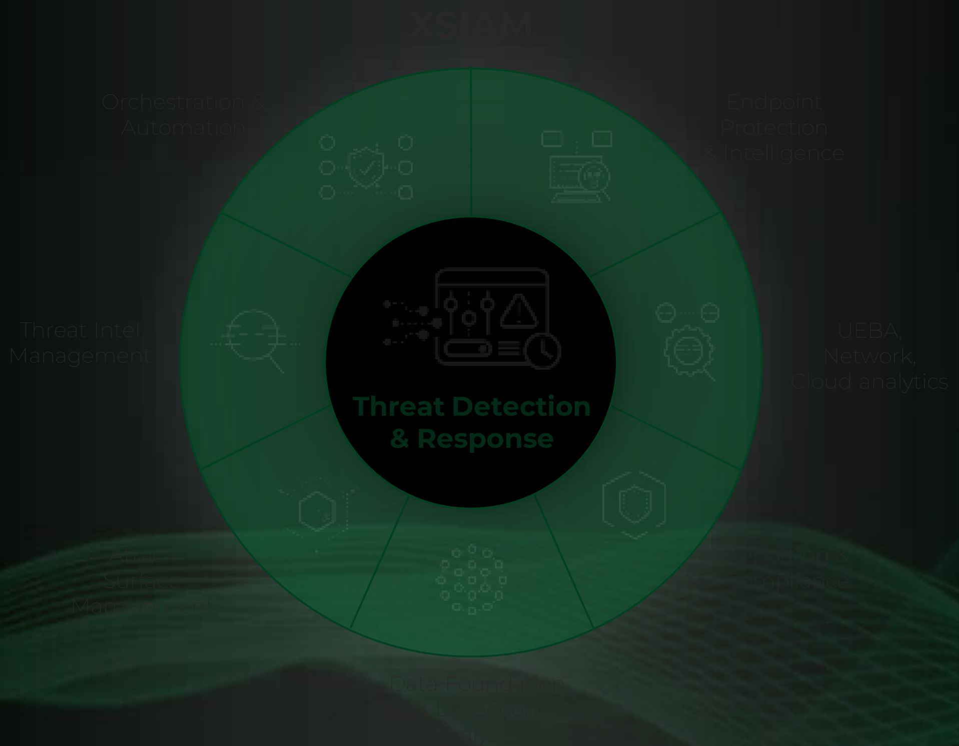
Automation First

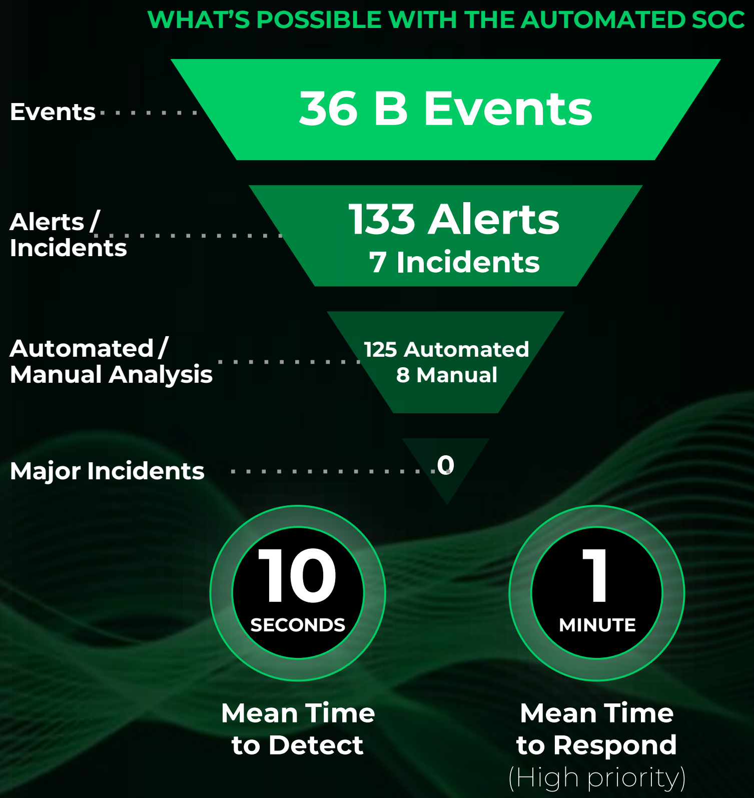
Proactive Security

XSIAM Is the Next Big Transformation in Security Operations


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

XSIAM Is the Next Big Transformation in Security Operations


XSIAM
Orchestration & Automation
Endpoint Protection & Intelligence
Threat Intel Management
Threat Detection & Response
UEBA, Network, Cloud analytics
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

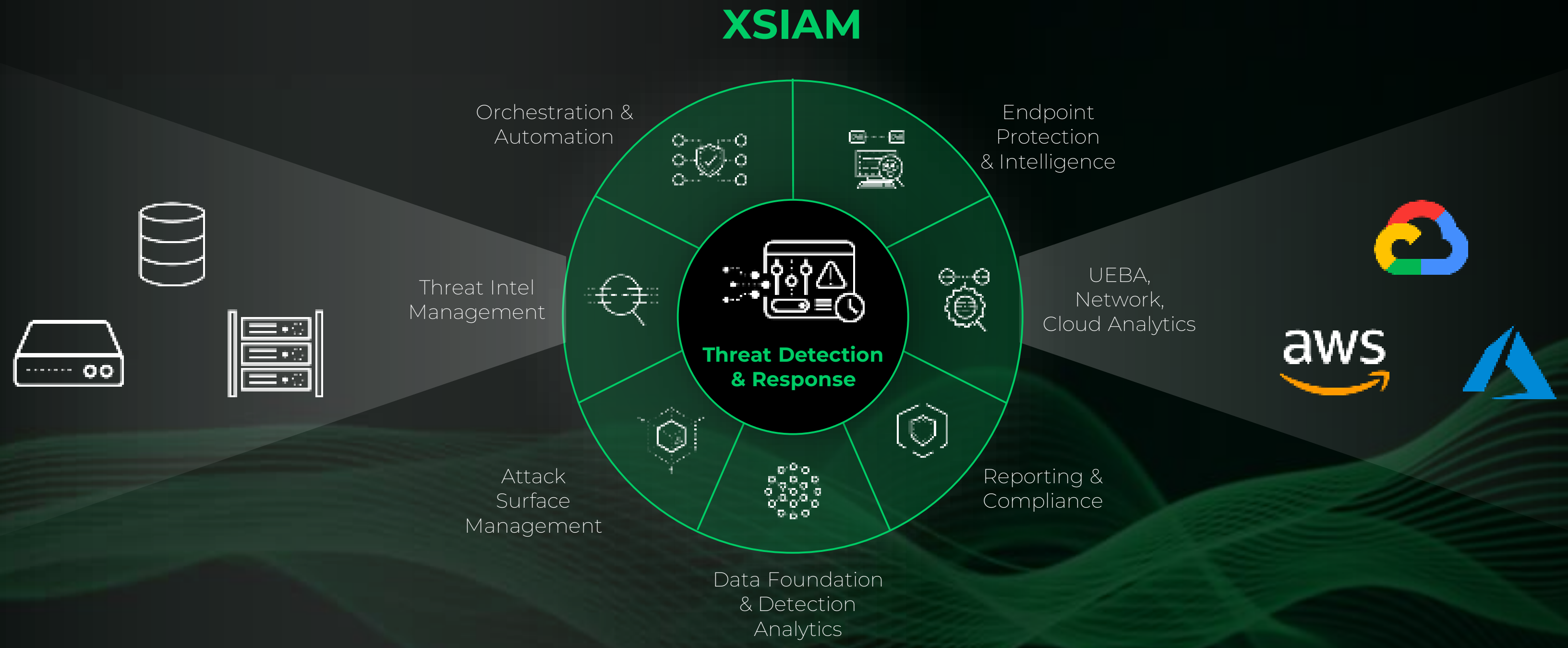
Automated / Manual Analysis — 125 Automated, 8 Manual

Major Incidents — 0

10 SECONDS — Mean Time to Detect

1 MINUTE — Mean Time to Respond (High priority)

XSIAM: Security Operations from Data Center to Cloud


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
aws

An Easy Journey to the XSIAM Vision

Improve analyst experience and increase productivity

Reveal advanced attacks with industry-leading threat intelligence

Simplify new data source onboarding vs. SIEM

Thank You