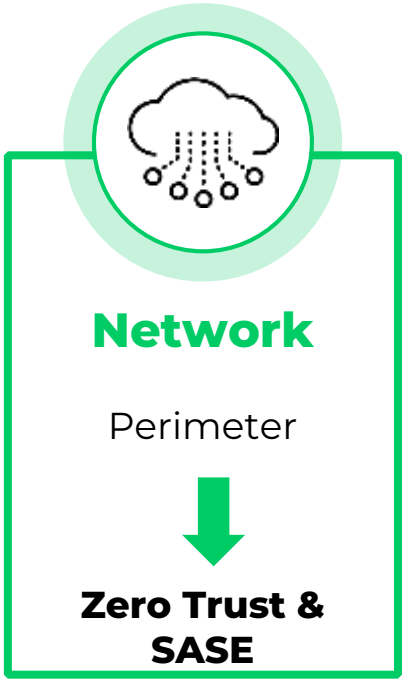
Goodbye, SIEM.
Hello, XSIAM.

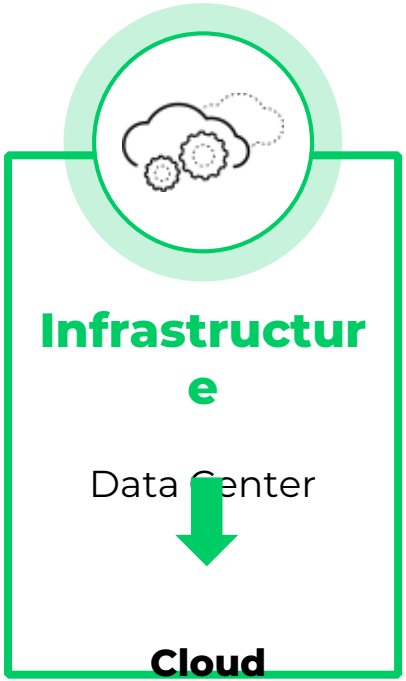
The Modern SOC, Reimagined

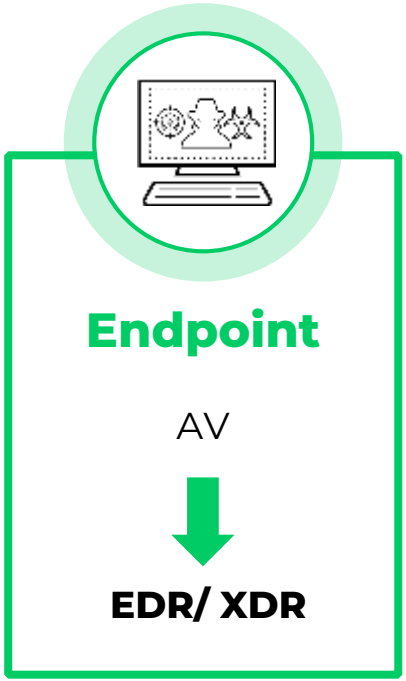
Thomas Maxeiner
Sr. Manager System Engineering, Cortex
Central & Southern Europe

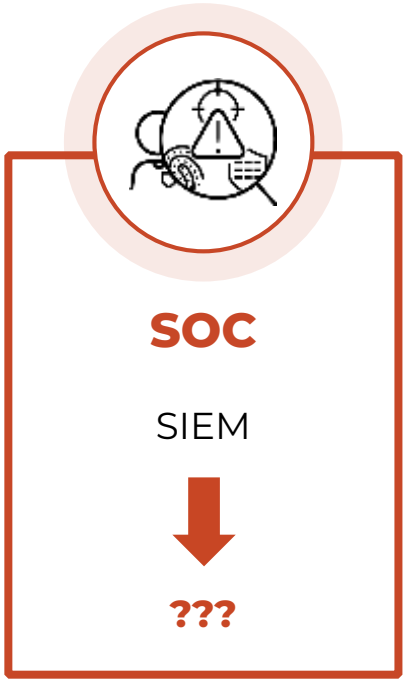
paloalto | CORTEX

Most Security Real Estate Has Been Redesigned, Except…





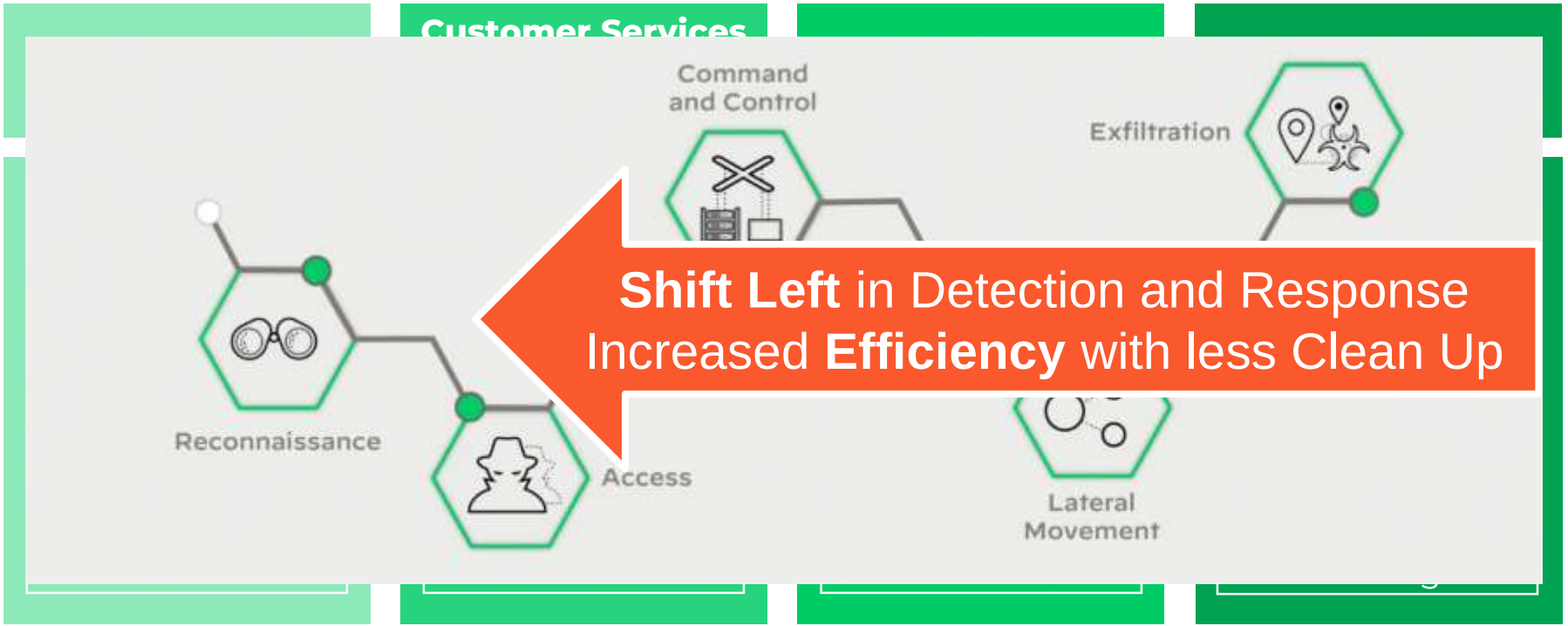




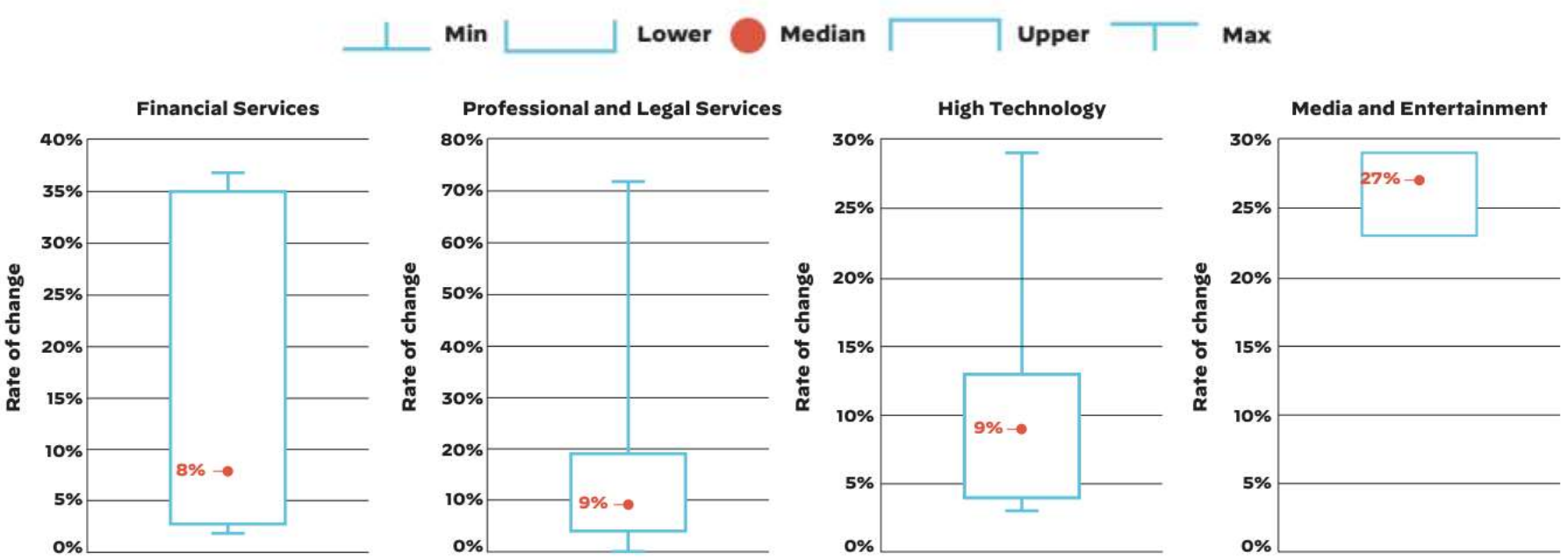
Digital Transformation: Every Project generates more Data

Digital Workplace Mobility / Cloud	Customer Services Continuous DevOps	Industrial IT-OT Converge	R&D Innovation
Windows 10 / 11	Cloud (SaaS, IaaS)	Critical Infrastructure	Collaboration
Mobile	Shadow IT	SCADA	Container
MAC OS / Linux	SDN	Manufacturing	M&A Infrastructure
Legacy OS	Cloud Storage	Medical Devices	Smart Technologies

Adversaries use the full Attack Surface to get in



How much does the attack surface change over a month?



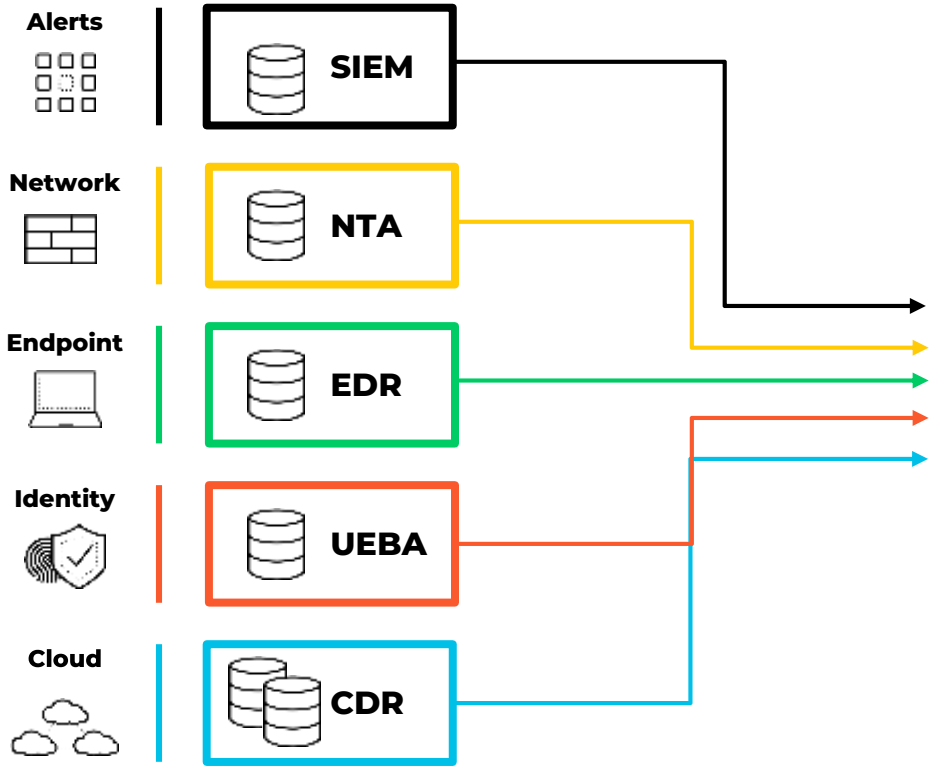
4% - 35%

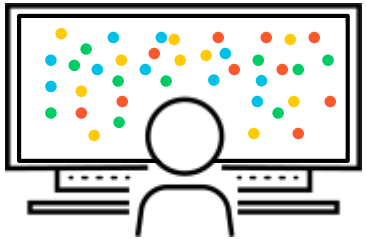
5% - 70%

4% - 28%

24% - 28%

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





~11K
Alerts per day

4+
Days to investigate

< 30%
of SOC teams meet KPI goals

212
Days of dwell time

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

EDR and SIEM Products Have Not Adequately Solved the Problem

EPP / EDR

Deep analytics and threat detection

Lacks coverage and context for entire environment

EDR

Endpoint

Lack of Analytics

Lack of Data and Context

SIEM

No Endpoint

Lack of Analytics

SIEM

SIEM / SA

Mile-wide, inch-deep understanding of data

Deficient analytics and detection

Lack of workflows

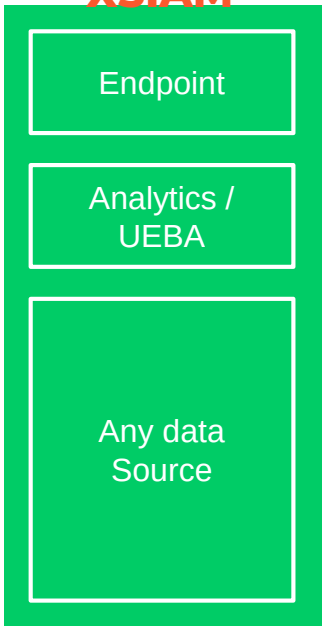
Lack of control points to remediate

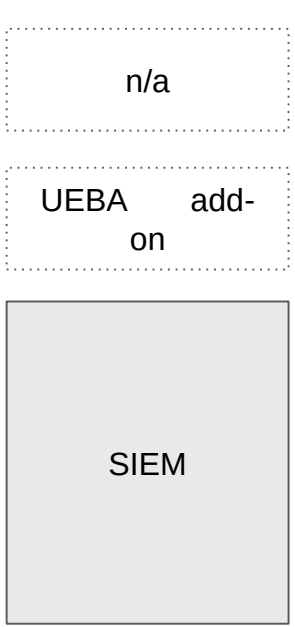
XDR is designed to increase SOC efficiency

Detection
- Data Stitching to tell the complete attack story “Causality Chain”

Investigations
- Complete Incident, instead of multiple Alerts
- Build-in analytics will stitch anomalies over multiple days

Response
- Native Actions (Endpoints, Firewalls, Cloud, OT)
- Live terminal and Host Restore





Detection
- Static Correlation Rules only triggered if all criteria is met (if, then, else conditions)

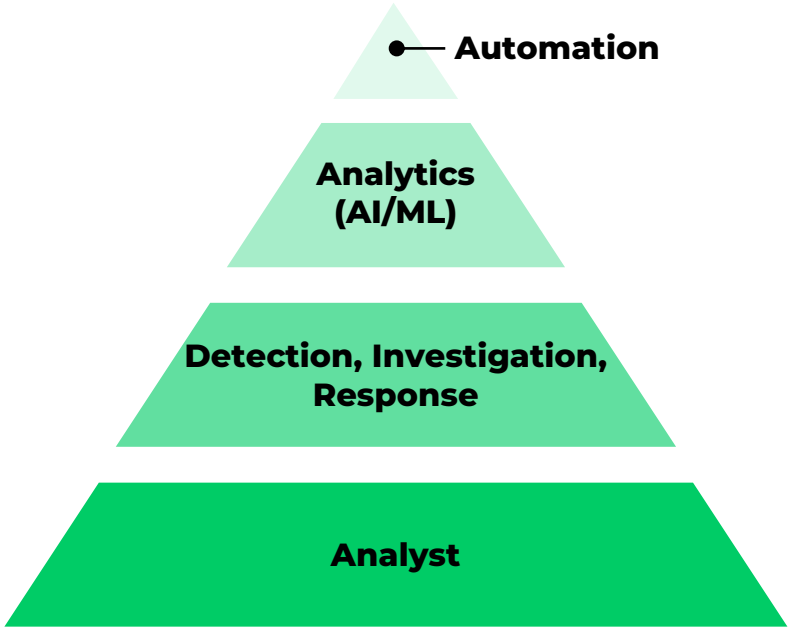
Investigations
- Lack of analytics means investigations are manual to put alerts in context

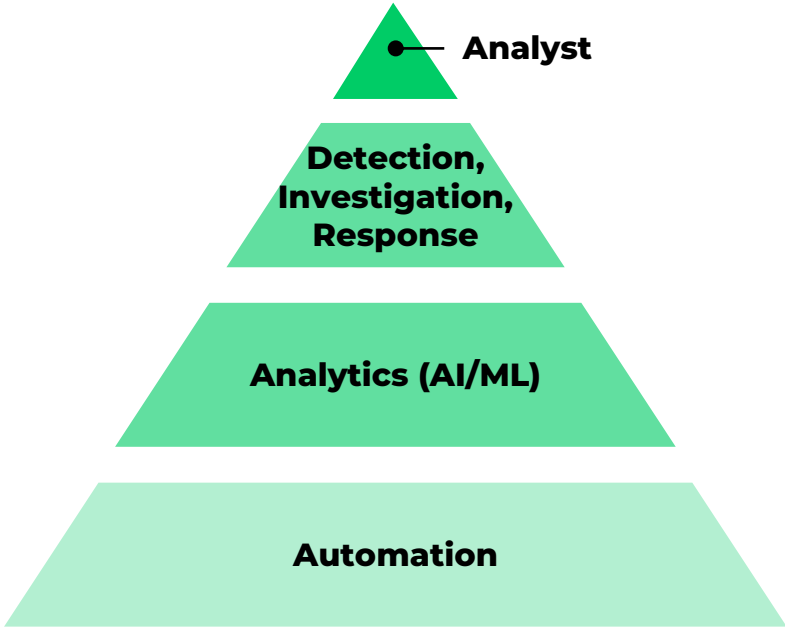
Response
- API based integrations with Endpoint vendors
- Limited actions

Cortex XSIAM

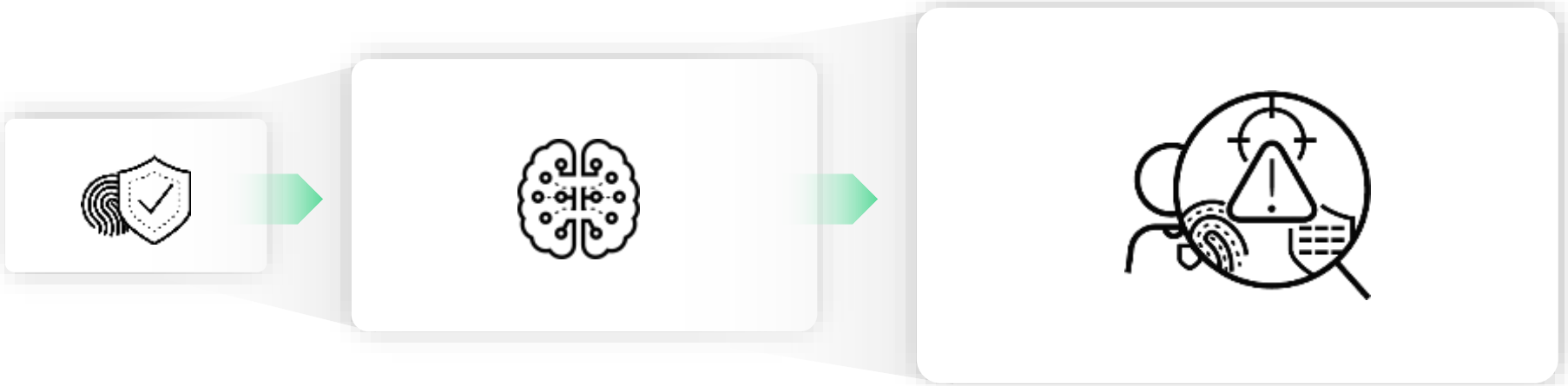
The Autonomous Security Platform
Powering the Modern SOC.

We Need to Transition to Analyst-Assisted Security Operations





Cortex: A Path to the Automated SOC



Cortex EDR
Advanced Endpoint Protection

Real-time endpoint analysis for malware/ threat prevention

Cortex XDR
Extended Detection & Response

Endpoint+network+cloud data stitching and analytics for enterprise-wide threat detection

Cortex XSIAM
Security Operations Platform

XDR+automation, extensible detection and data, compliance audit, advanced intelligence

XSIAM: THE AI-DRIVEN SOC PLATFORM FOR THE MODERN SOC

Cortex XSIAM

Forensics | Investigation & Response | Case Management | Dashboard & reporting | Cloud SOC | Compliance

Process Automation & Orchestration | Playbooks | Host Insights | Asset Discovery & Mgmt

Threat Intel Mgmt | Endpoint Security | External Exposure Mapping | Network, Cloud, and Identity Analytics | (Customizable) Correlation Rules

Behavior Analytics on Telemetry

Embedded Automation & Analytics

Data Processing & Integration

Palo Alto Networks Threat Intelligence

Data Lake


Identity


Cloud Platforms


Endpoint Security

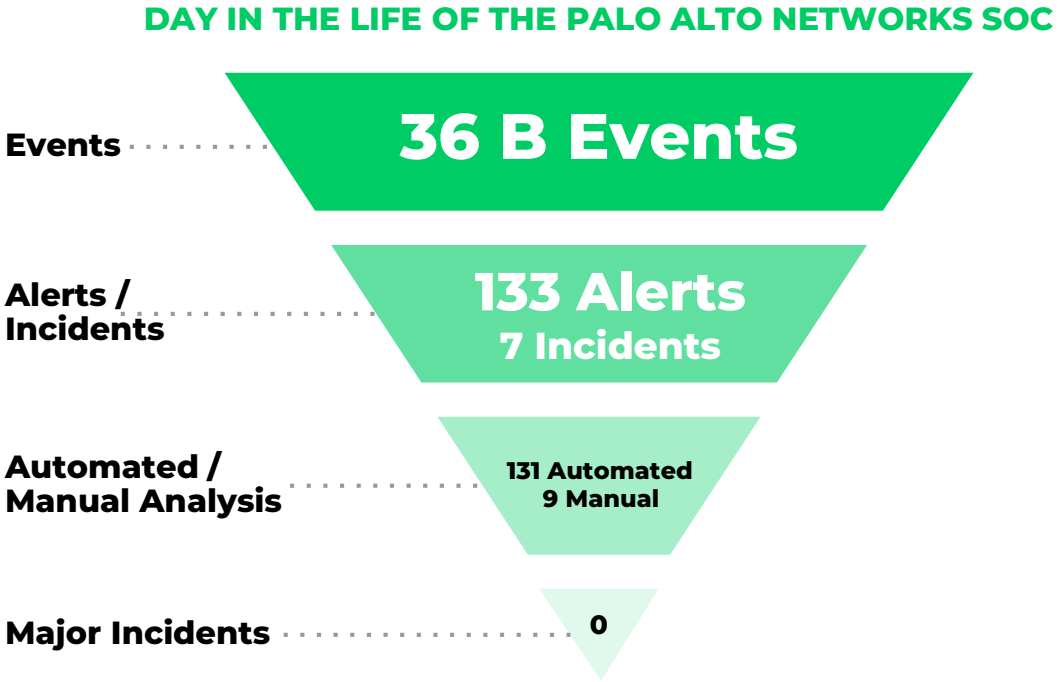

Servers & DB


Threat intel feeds


Network security


Any data

Palo Alto Networks SOC: Industry-leading 1 min response time



10
SECONDS

Mean Time to Detect

1
MINUTE

Mean Time to Respond
(High priority alerts)

paloaltonetworks.com