# Zero Trust

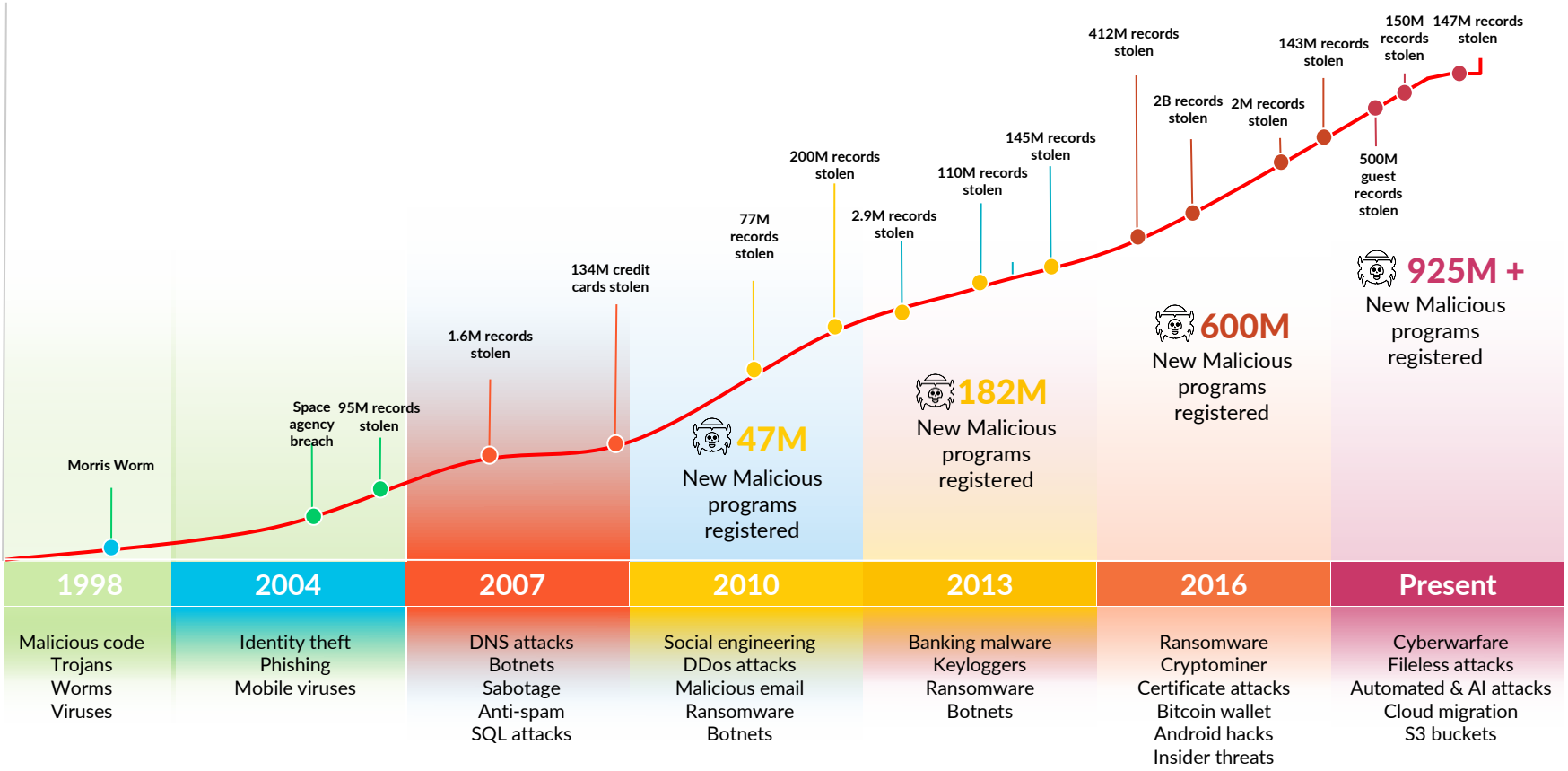
## Security Orchestration and Automation

Feb 2024

Matt Thorn
Cortex SE

paloalto NETWORKS | CORTEX

# We all know the problem



# The DoD CIO says We Need to Transition to Zero Trust Architecture

The rapid growth of these offensive threats emphasizes the need for the Department of Defense (DoD) to adapt and significantly improve our deterrence strategies and cybersecurity implementations.

# The DoD CIO says We Need to Transition to Zero Trust Architecture

Our adversaries are in our networks, exfiltrating our data, and exploiting the Department's users.

# The DoD CIO says We Need to Transition to Zero Trust Architecture

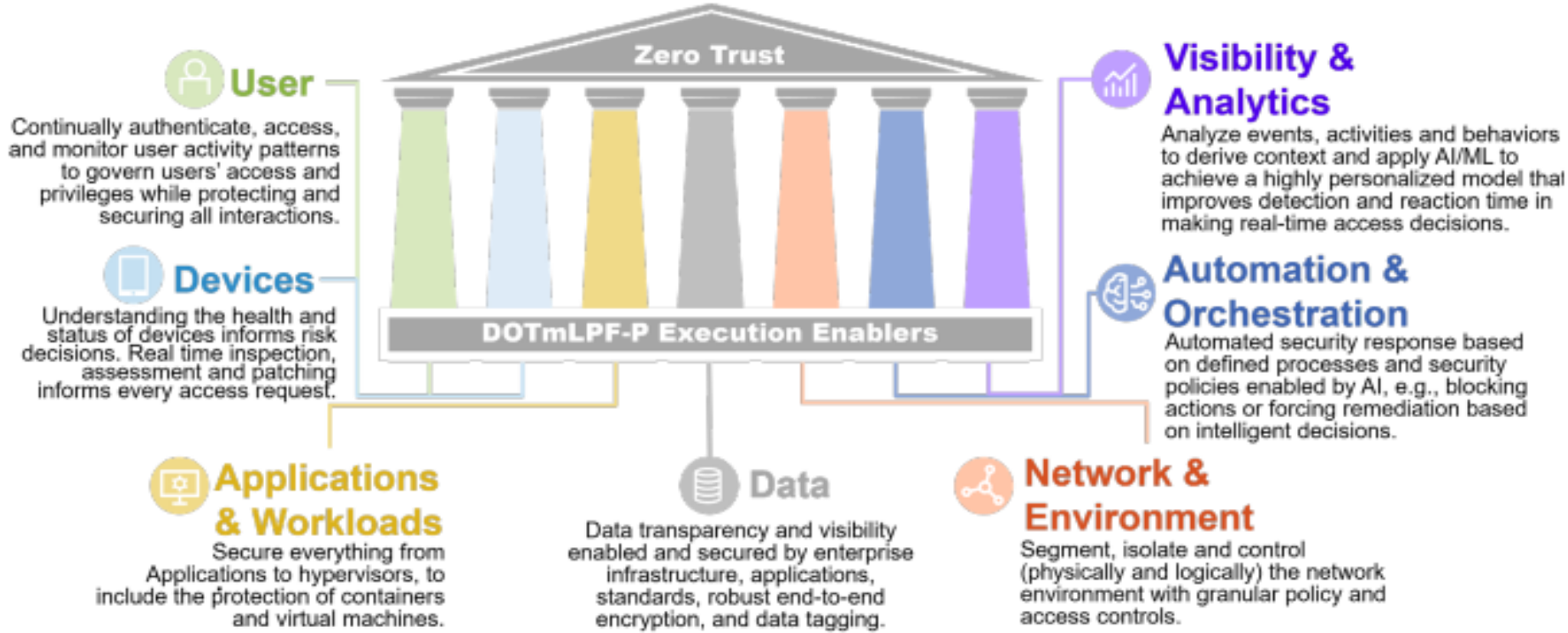
Defending DoD networks with high-powered and ever-more sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our information enterprise that spans geographic borders, interfaces with external partners, and support to millions of authorized users, many of which now require access to DoD networks outside traditional boundaries, such as work from home.

# The DoD CIO says We Need to Transition to Zero Trust Architecture

To meet these challenges, the DoD requires an enhanced cybersecurity framework built upon Zero Trust principles that must be adopted across the Department, enterprise-wide, as quickly as possible...

# That means

## DoD CIO – Zero Trust Strategy



# Because...

## So we need to focus on:

# Why security teams struggle

## Rising Alerts

Too many alerts & not enough people to handle them

**174k**

## Lack of Time

Repetitive & manual actions across siloed tools take too much analyst time

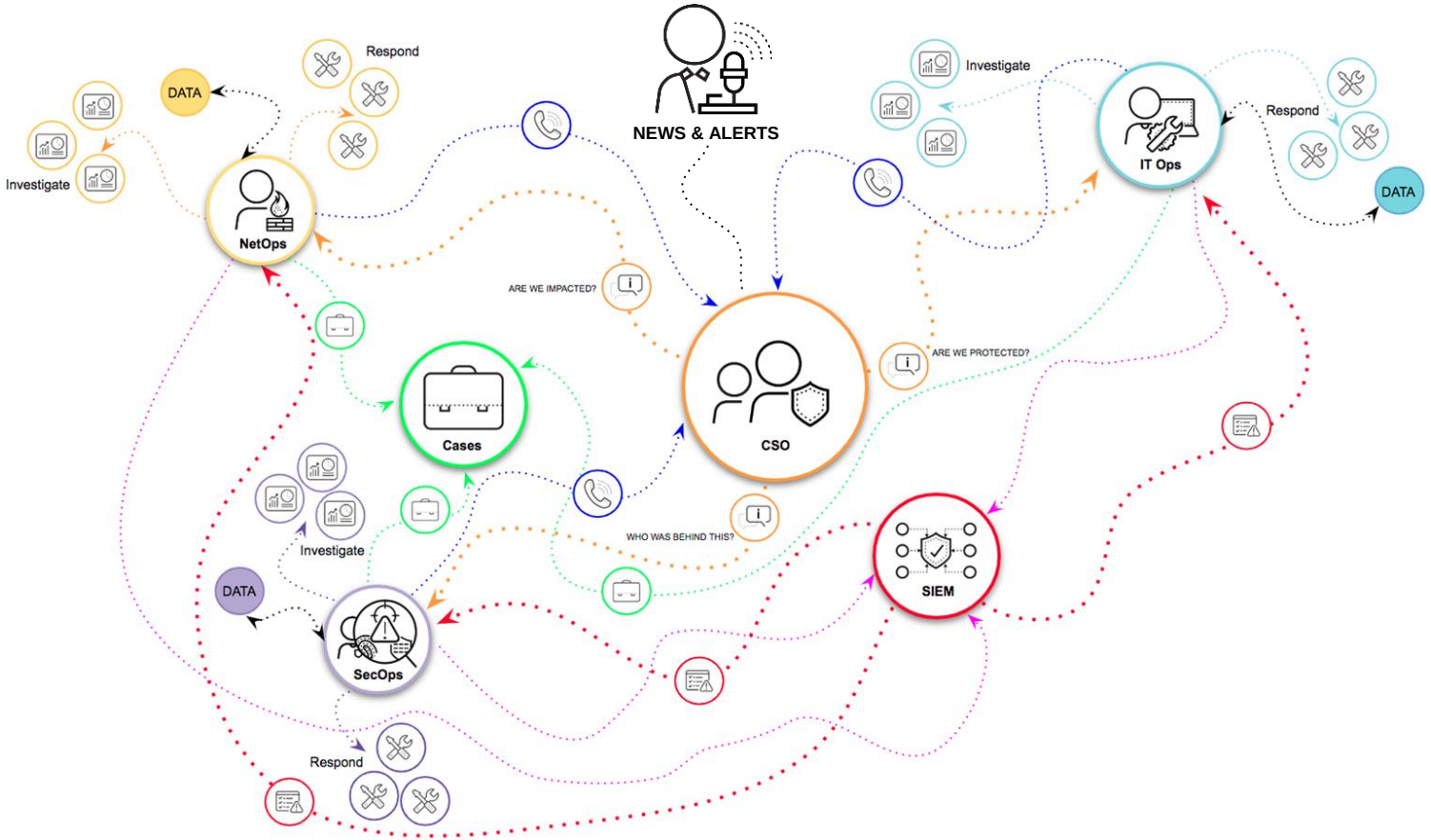
**30+**

## Limited Context

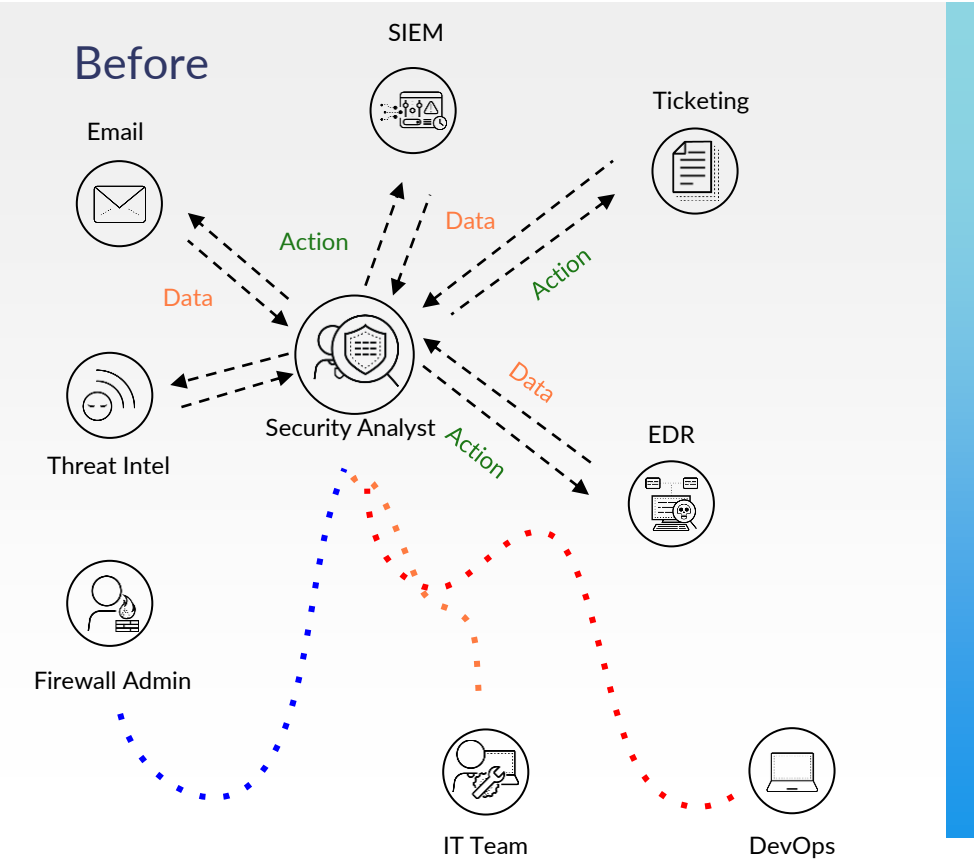
It takes days to understand incidents & investigate threats

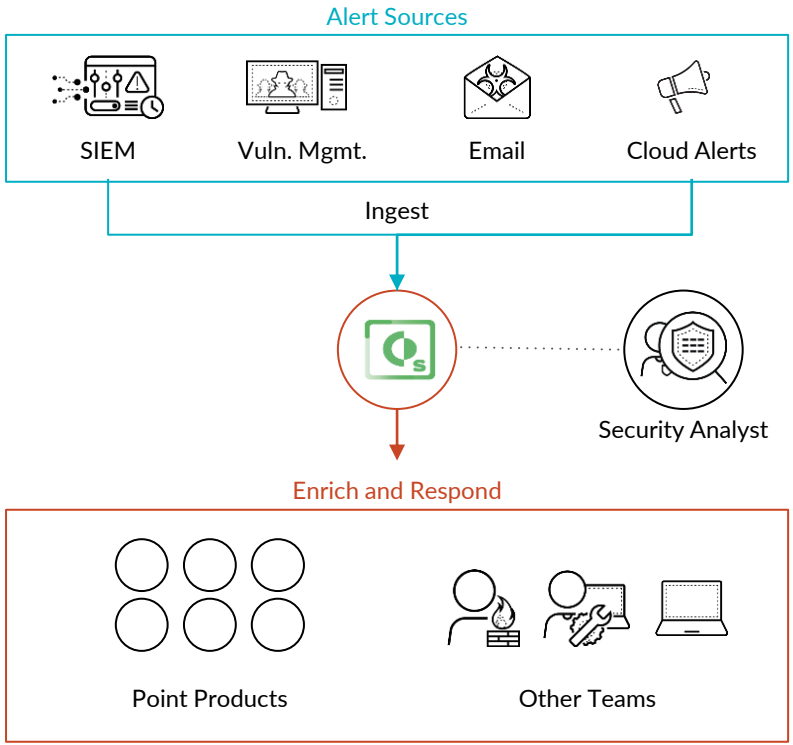
**4+ days**

# The reality of security operations...



# Security Processes Automation



# Your SecOps Team Today

"Incident information is difficult to compile and keep a record of."

"Communicating with end users and other teams takes up a lot of my time."

"We receive hundreds of alerts a day...user issues, network traffic, malware alerts, cloud security alerts."

"There are so many tools and the solutions I use require a lot of brain power and so many clicks."

"Small team and we are on-call 24/7 even on holidays."

"I have no way of filtering through duplicate alerts."

# Breadth Your SecOps Team is probably dealing with Today

## Analytics and SIEM

CORTEX · DEVO · exabeam · FORTINET · JASK · LogRhythm · McAfee · MICRO FOCUS · Radar · splunk> · sumologic

## Threat Intelligence

paloalto · ALIEN VAULT · ANOMALI · COFENSE · CYMON · DOMAINTOOLS · FORSIGHT SECURITY · OpenPhish · Recorded Future · VirusTotal

## Malware Analysis

paloalto · CISCO · cuckoo · FIREEYE · INTEZER · JoeSecurity · KOODOUS · REVERSING LABS · SNDBOX

## Endpoint

CORTEX · Carbon Black. · CounterTack · CROWDSTRIKE · cybereason · CYLANCE · SentinelOne · Symantec. · TANIUM

## Network Security

paloalto · Check Point · F5 · PROTECTWISE · Signal Sciences · zscaler · VECTRA · tufin

## Authentication

CYBERARK · DUO · Active Directory · okta

## Email Gateway

BitDam · mimecast · proofpoint. · Symantec.

## Ticketing

cherwell · easyVISTA · freshdesk · Jira Software · salesforce · zendesk

## Messaging

Exchange · pagerduty · slack · twilio · zoom

## Cloud

CORTEX · PRISMA · aws · Google Cloud · Microsoft · netskope

**...and 100s more!**


**Zero Trust requires implementing a policy of least privilege**

You need to verify and validate your users everywhere at all times throughout your security architecture where you block and allow access.

**Palo Alto Networks introduced User-ID to write identity-based policies more than a decade ago.**

# How to begin?

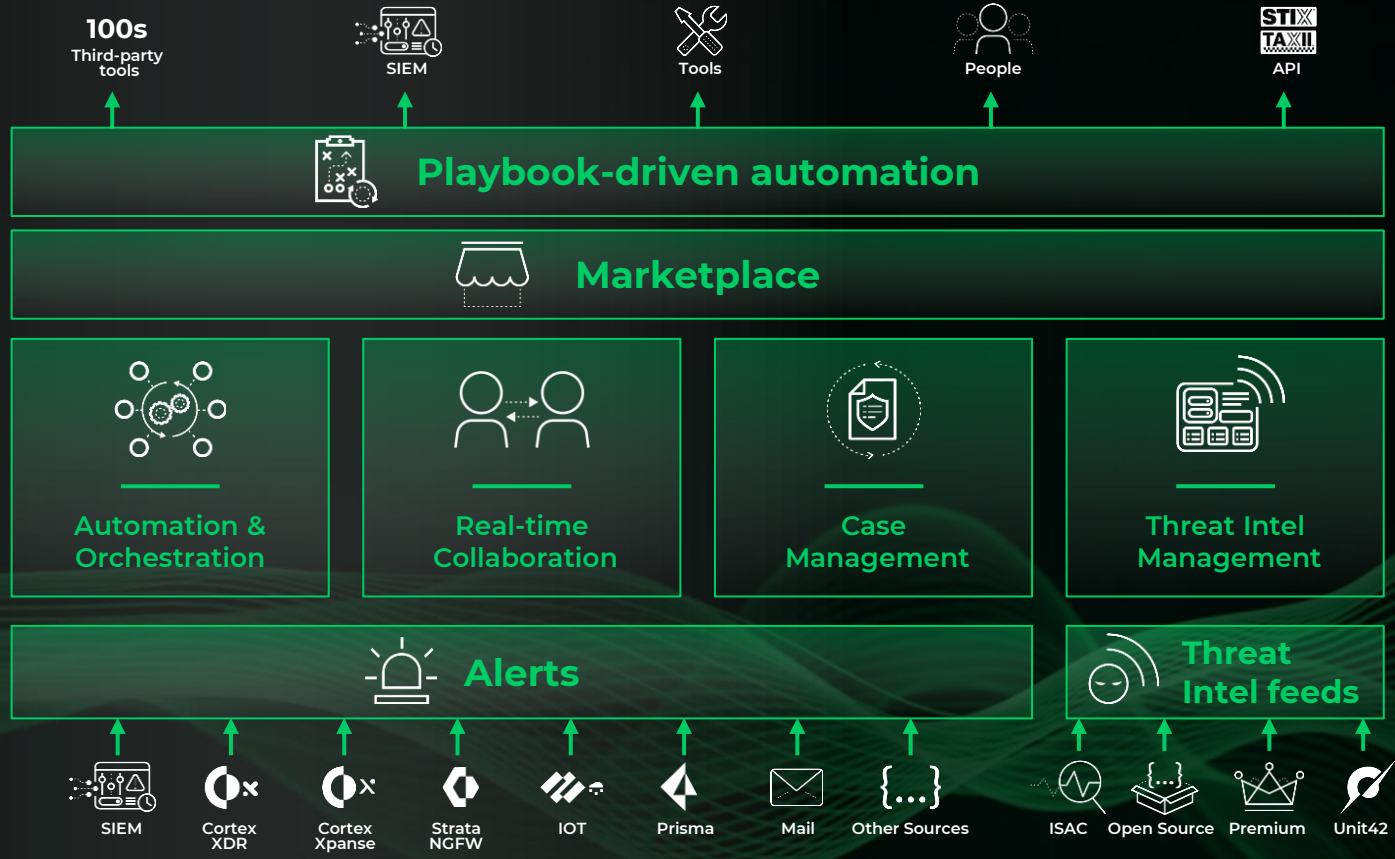
Integrate disparate technologies to enforce cohesive, ubiquitous security policy

Automate manual and redundant processes

Orchestrate the technologies and user as well as analysts and operators efforts to support the Zero Trust tenants

Do not Automate what you cannot properly Orchetsrate and you cannot Orchestrate what you do not sufficiently Integrate

# Integration: The first step to Orchestration



# You will need to unlock your SOC with Orchestration and Automation

**Automate** manual tasks so your analysts can focus on what's critical

**Reduce** the number of alerts your team needs to touch

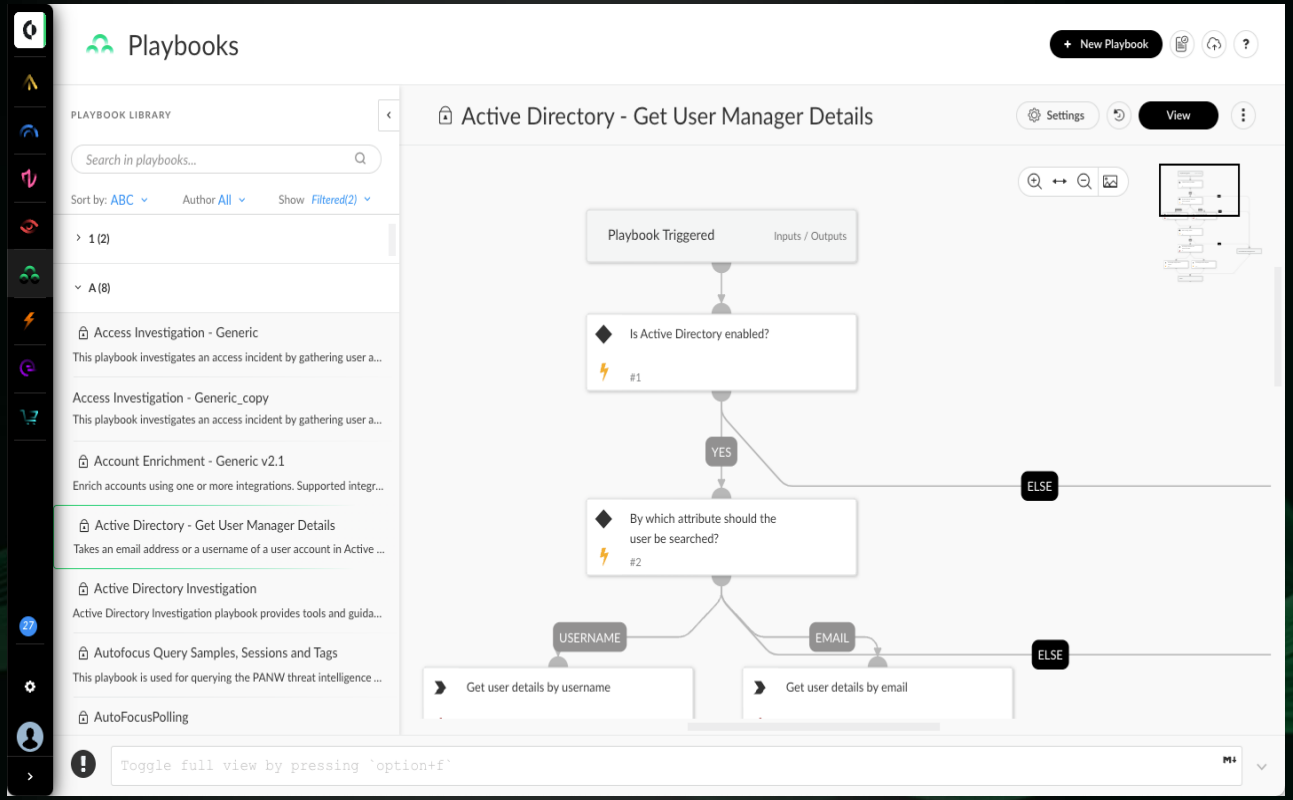
**Manage** and **act** on your threat intel

**Speed** incident investigation and reduce MTTR

**Orchestrate** incident response across **all** your security tools

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

# Automate Your Manual Workflows

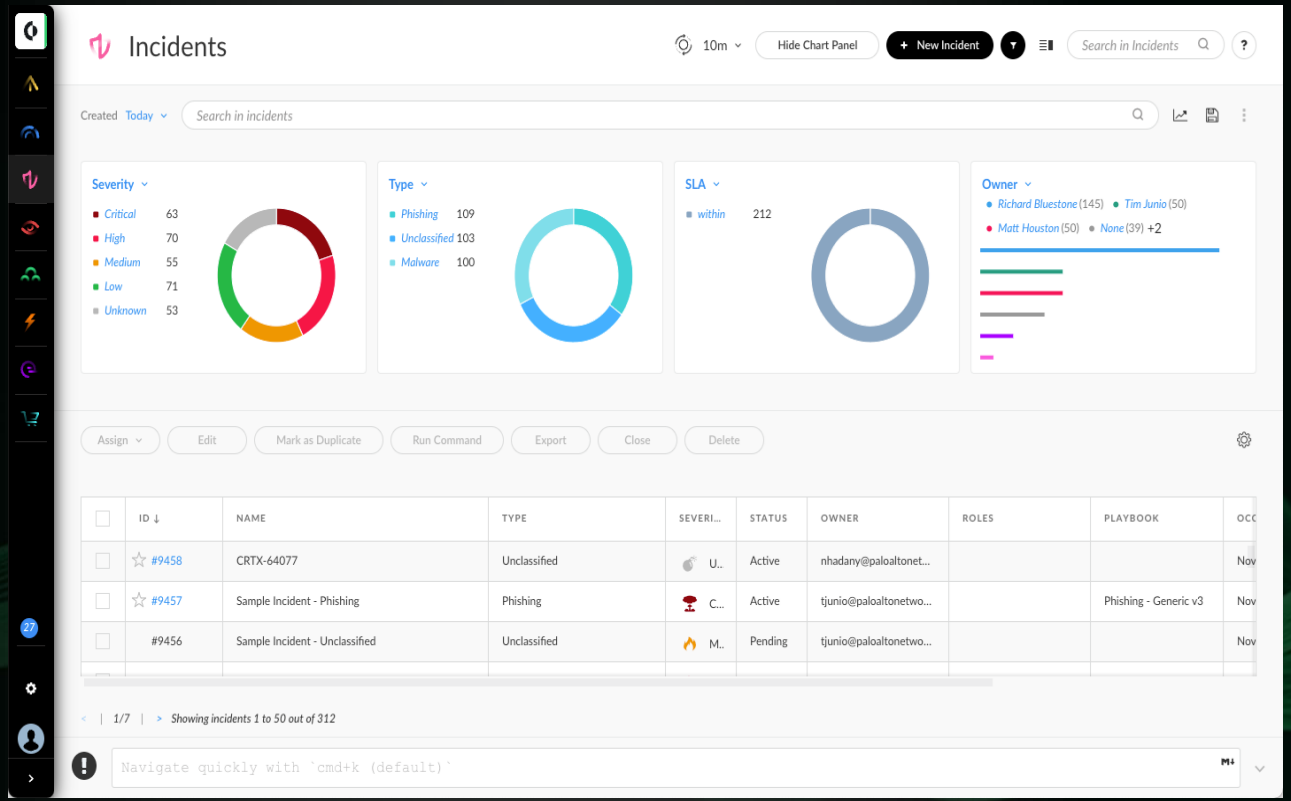



## Eliminate repetitive, time consuming tasks

- **You will need** integrations & automation packs
- **You will leverage** security actions for DIY playbooks
- Seek drag & drop style, modular **visual playbook editor** for **code-free** editing

paloalto NETWORKS | CORTEX

# Automations Speed Your Incident Investigations

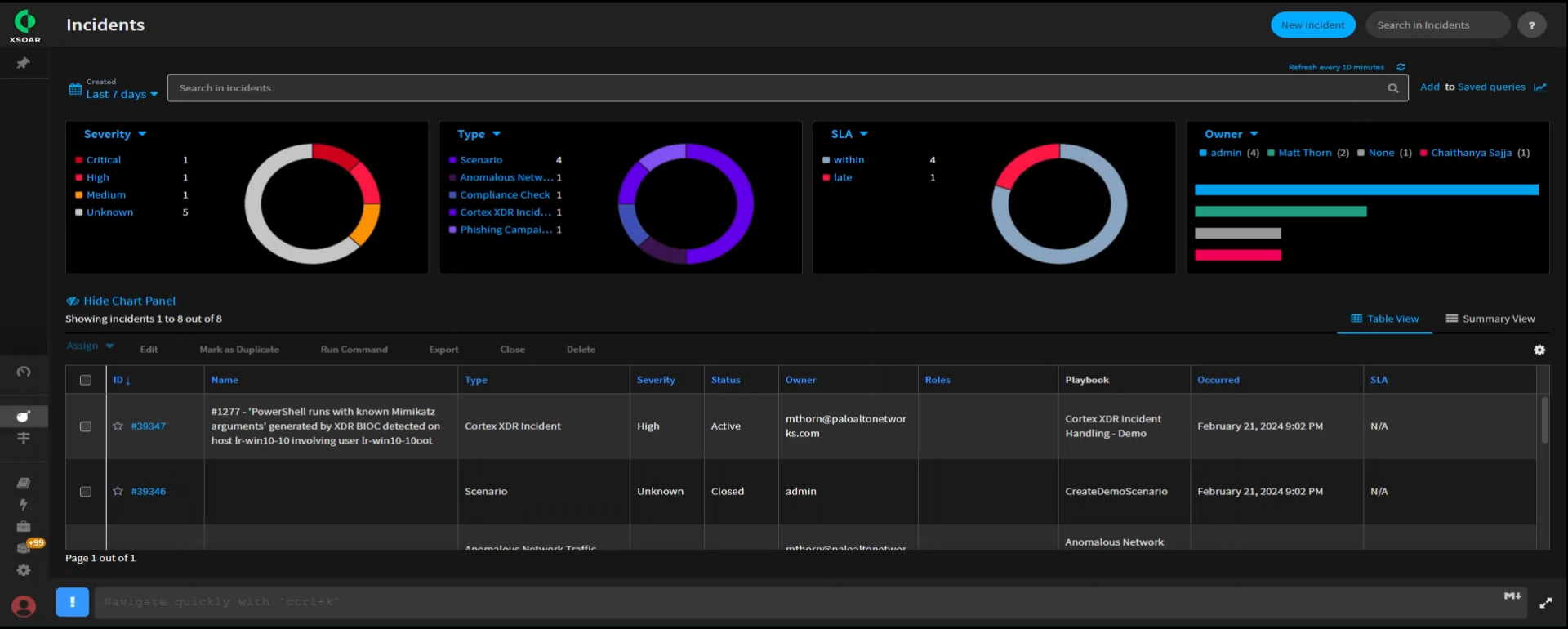



## Utilize real-time collaboration across teams

- A **Virtual War Room** for incident investigation & collaboration
- Use **ChatOps & CLI** for on-the-fly investigation
- **Auto-documentation** for knowledge sharing & audit reporting is essential
- **Machine learning** to aid analysts response quicker

paloalto NETWORKS | CORTEX

# Automations make Zero Trust viable



# Automate ZTNA for your SOC

## Common SOC Use Cases

- Rapid Breach Response
- Phishing Response
- Indicator Enrichment
- Malware investigation & Response

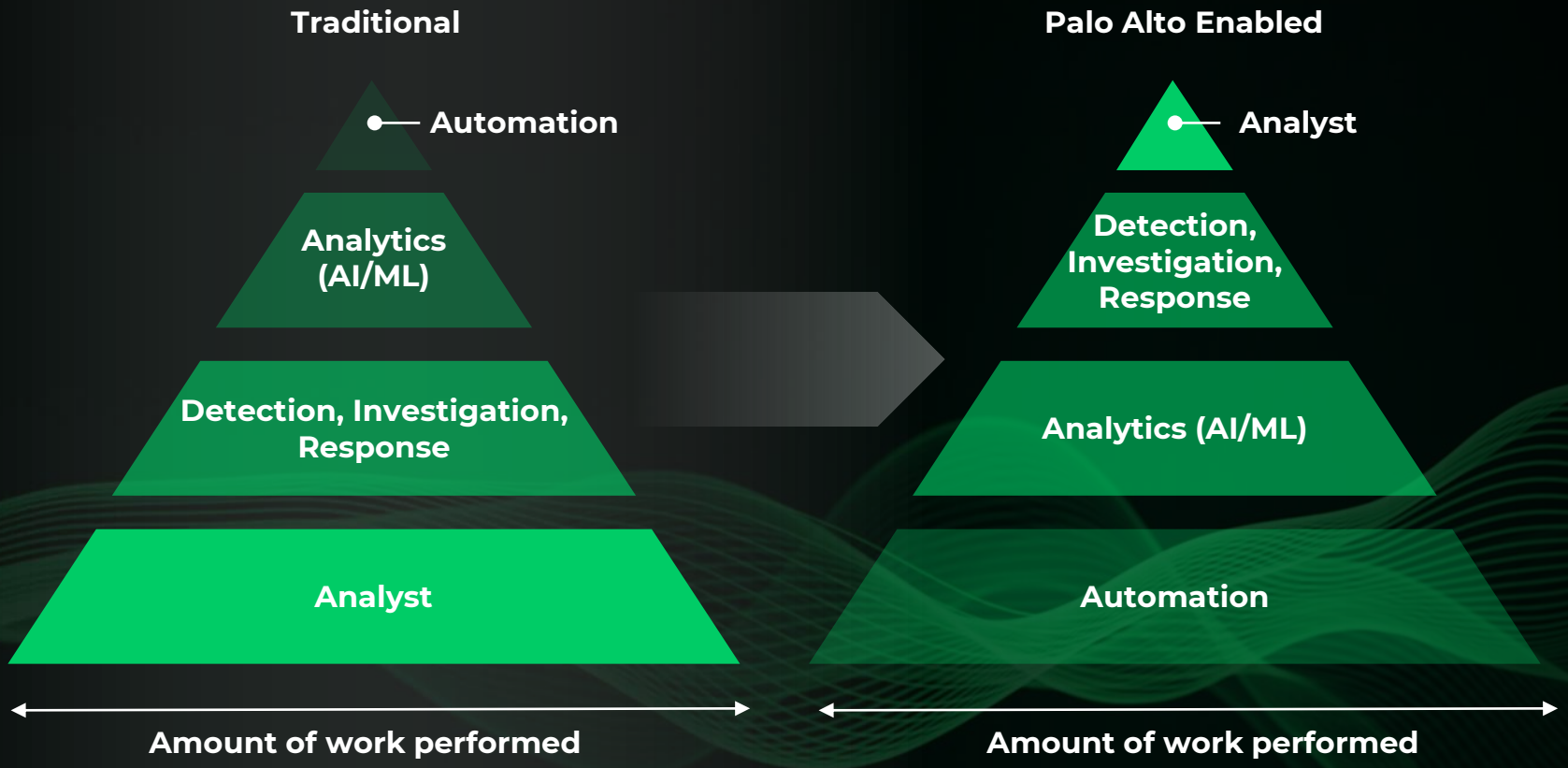
## Extended Security Automation

- Cloud Security
- Threat Feed Management
- Remote User Access
- Vulnerability Management

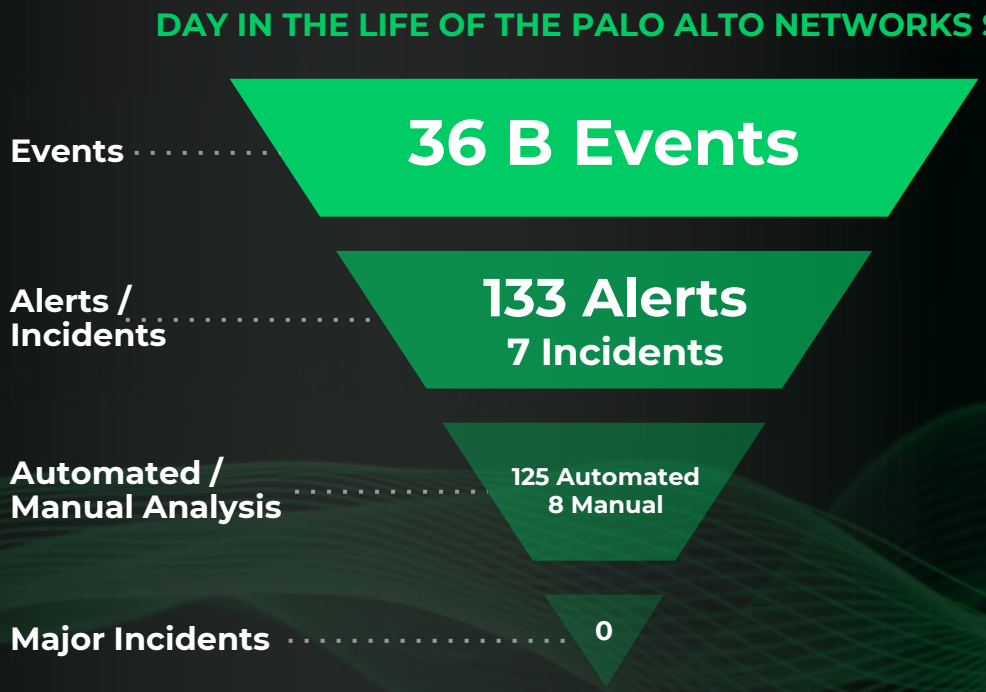
## Enterprise Security Automation

- Network Security
- Security Compliance
- Identity & Password Management
- Other Security and IT Use Cases

# We Need to Transition to Analyst-Assisted Security Operations



# The Proof: We have achieved a 1 min. response time




**10 SECONDS**

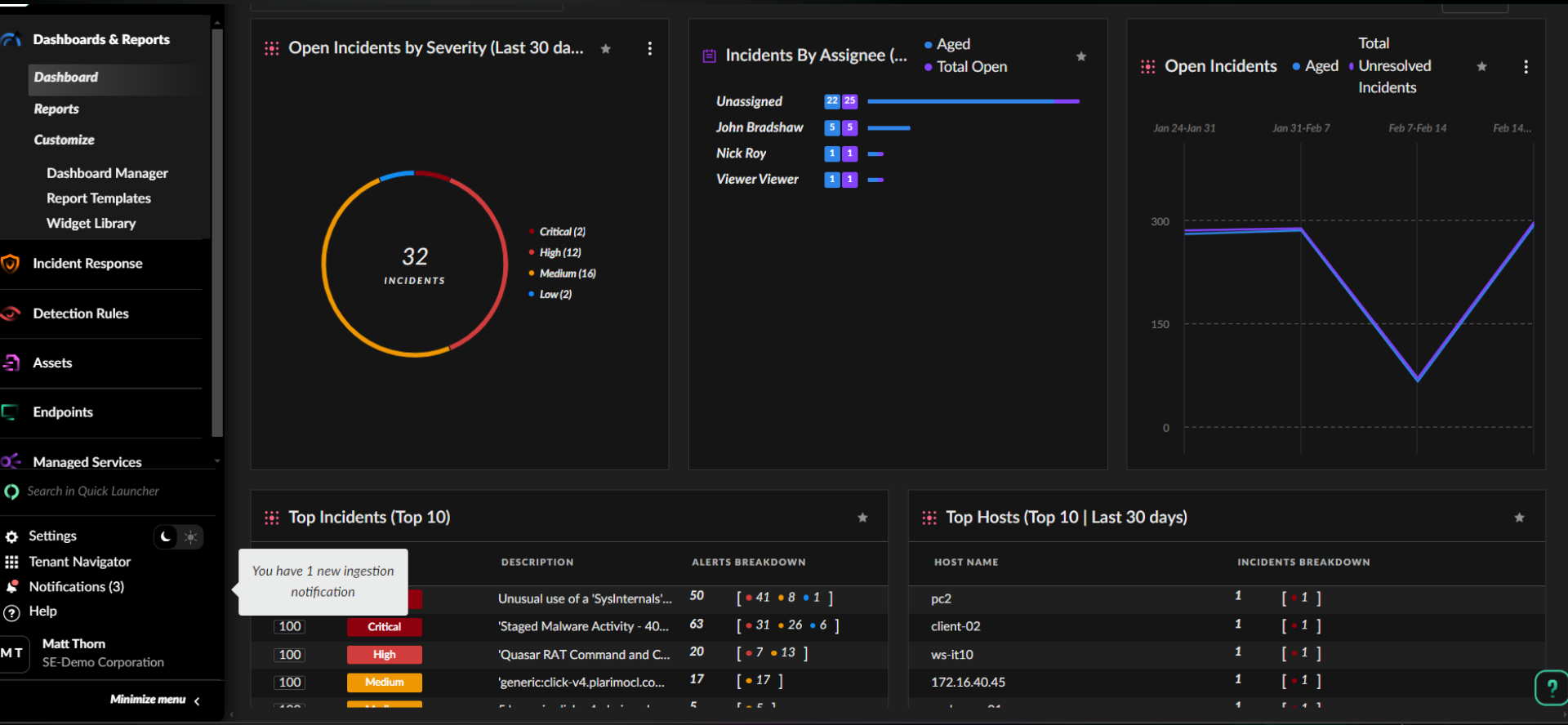
**Mean Time to Detect**

**1 MINUTE**

**Mean Time to Respond**
(High priority)

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

# Because, ultimately, we should not be focusing on these



# We really need to focus on

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

# Thank you