

Zero Trust

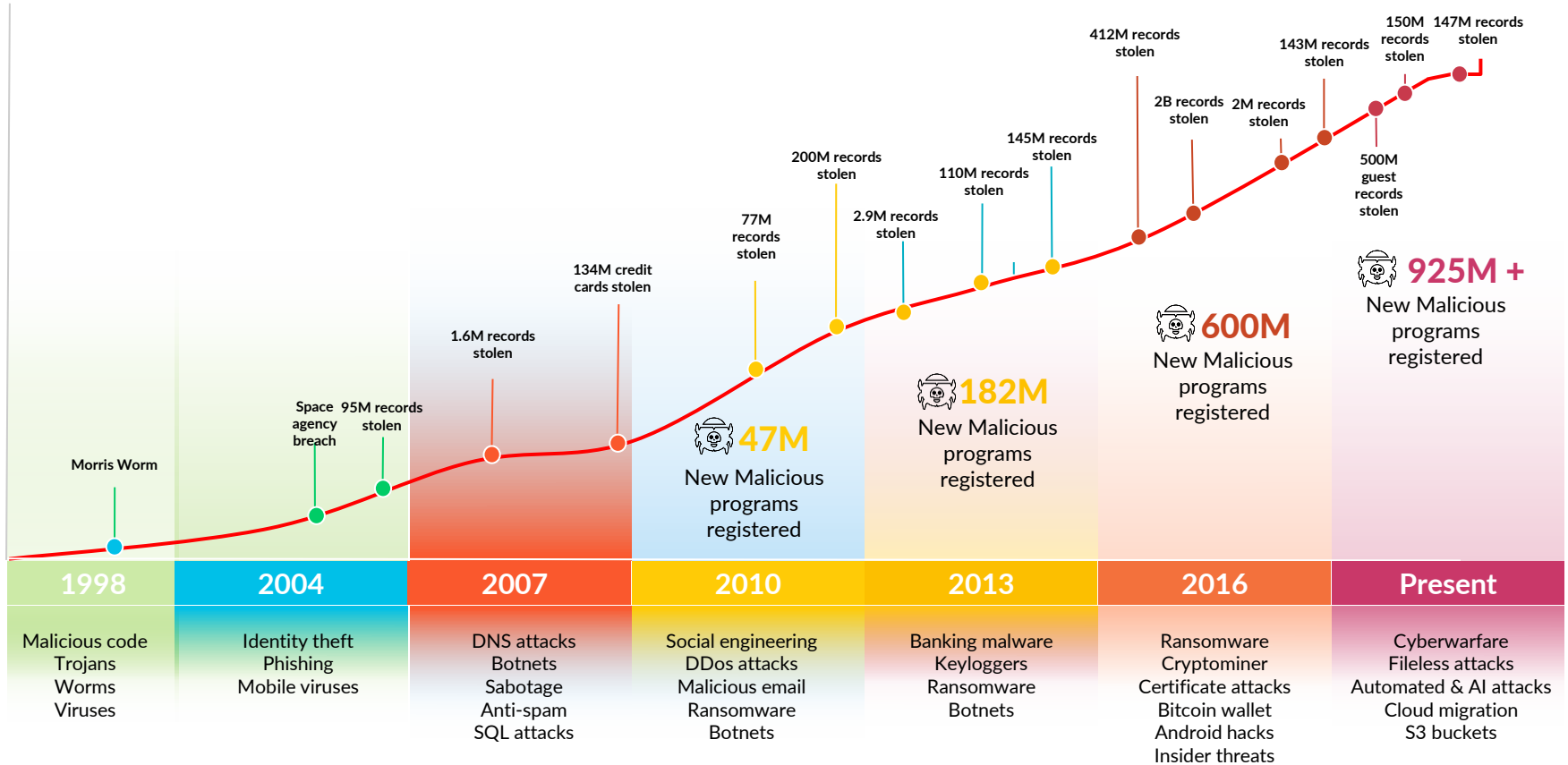
Security Orchestration and Automation

Feb 2024

Matt Thorn
Cortex SE



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

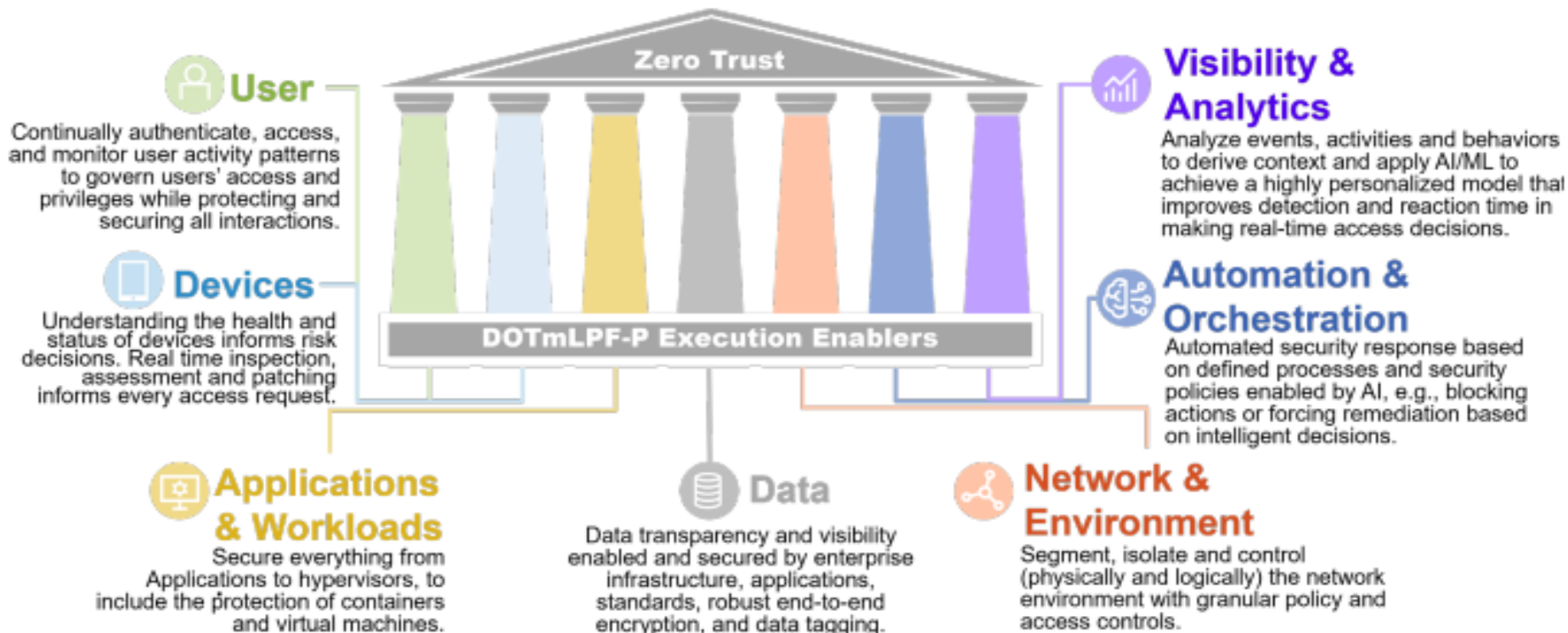
Defending DoD networks with high-powered and ever-more sophisticated perimeter defenses is no longer sufficient for achieving cyber resiliency and securing our information enterprise that spans geographic borders, interfaces with external partners, and support to millions of authorized users, many of 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:

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Google

404. That's

The request
we know.

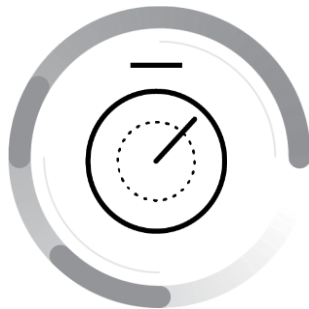
Why security teams struggle



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+

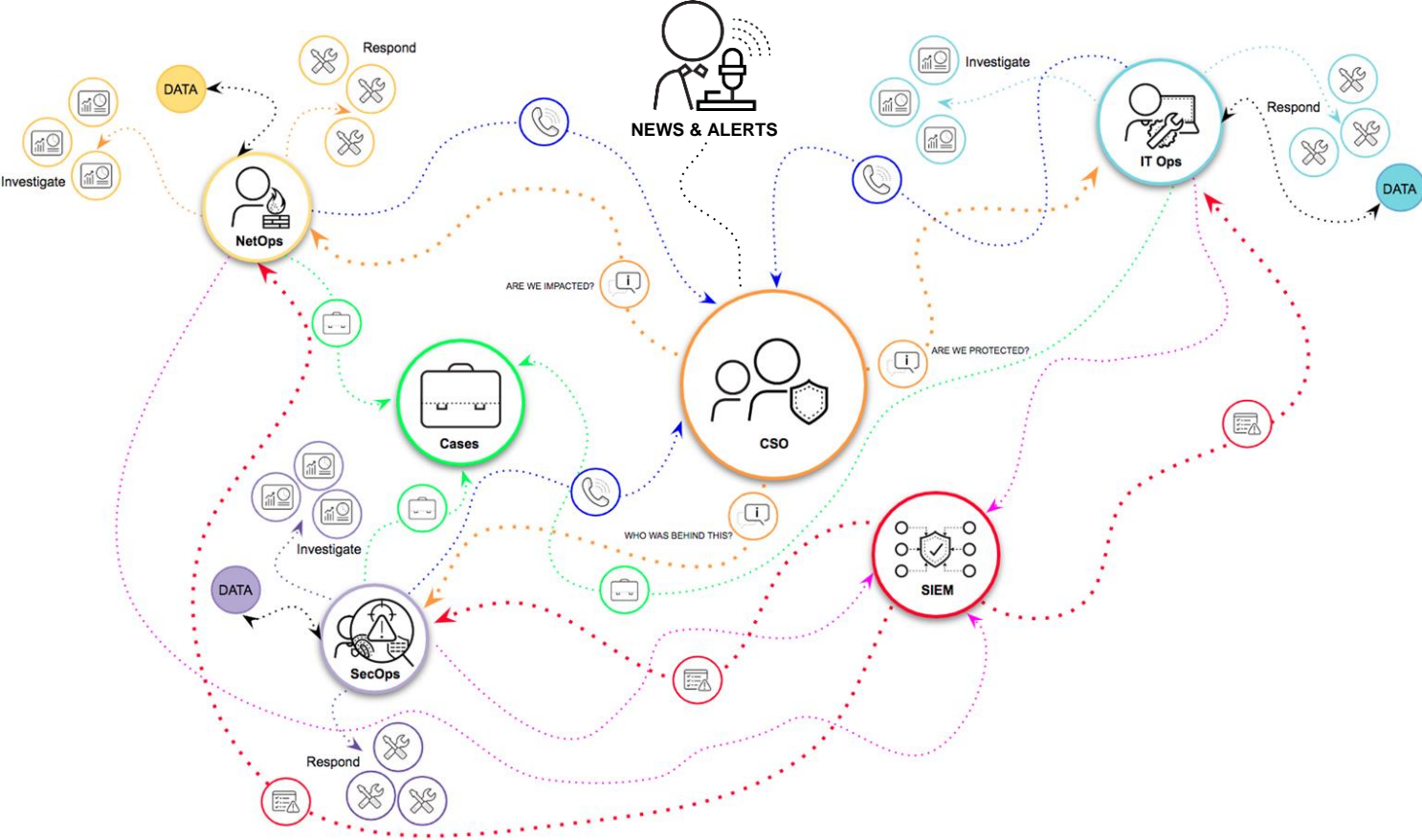


Limited Context

It takes days to understand incidents & investigate threats

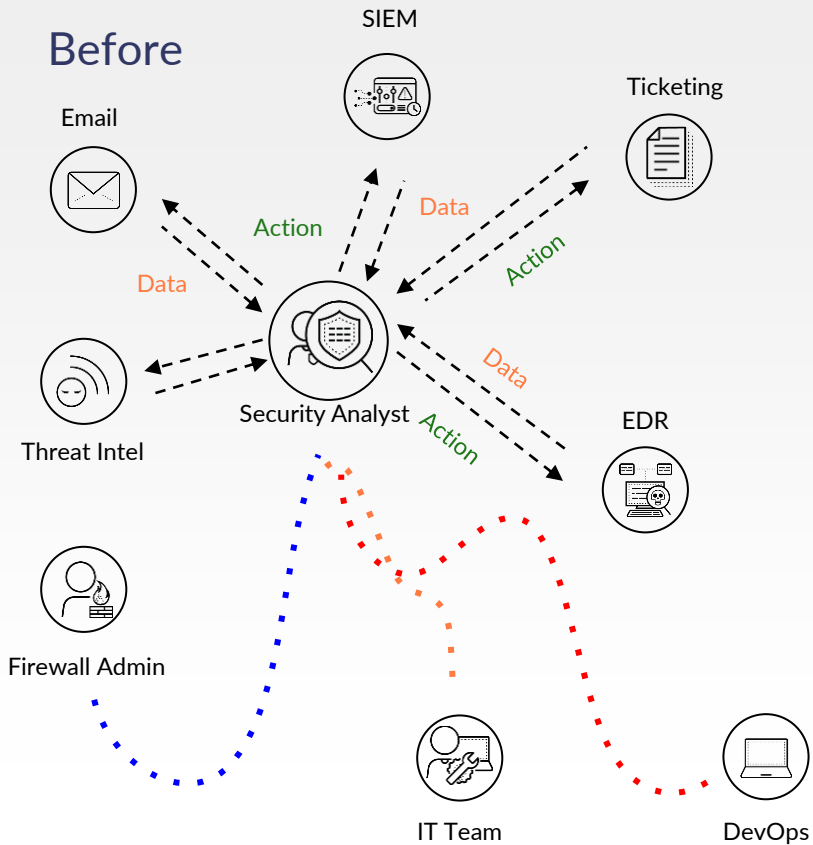
4+ days

The reality of security operations...

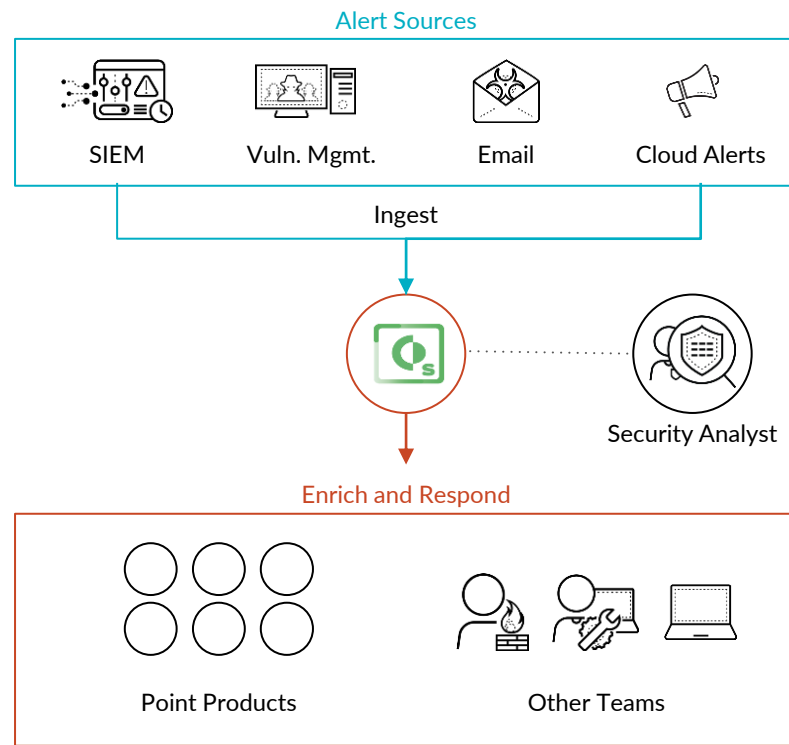


Security Processes Automation

Before



After



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



Threat Intelligence



Malware Analysis



Endpoint



Network Security



Authentication



Email Gateway



Ticketing



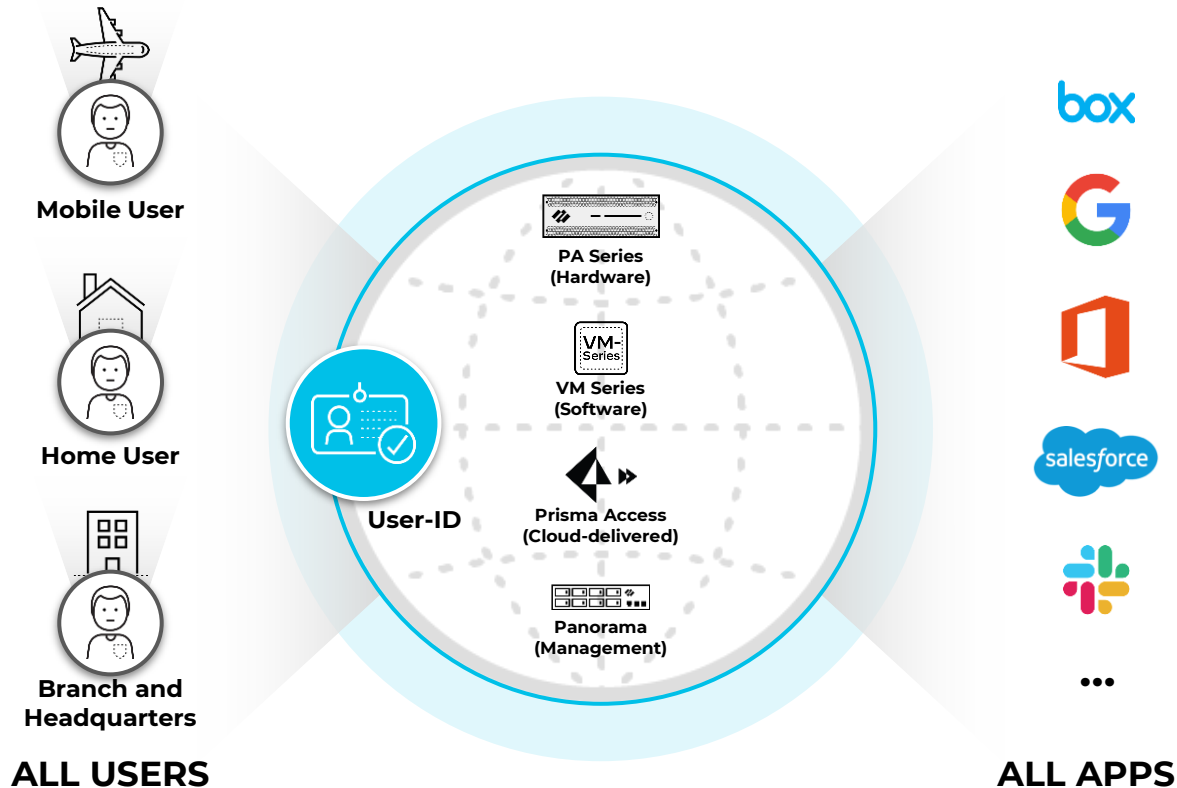
Messaging



Cloud



...and 100s more!



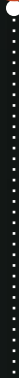
Zero Trust requires implementing a policy of least privilege

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

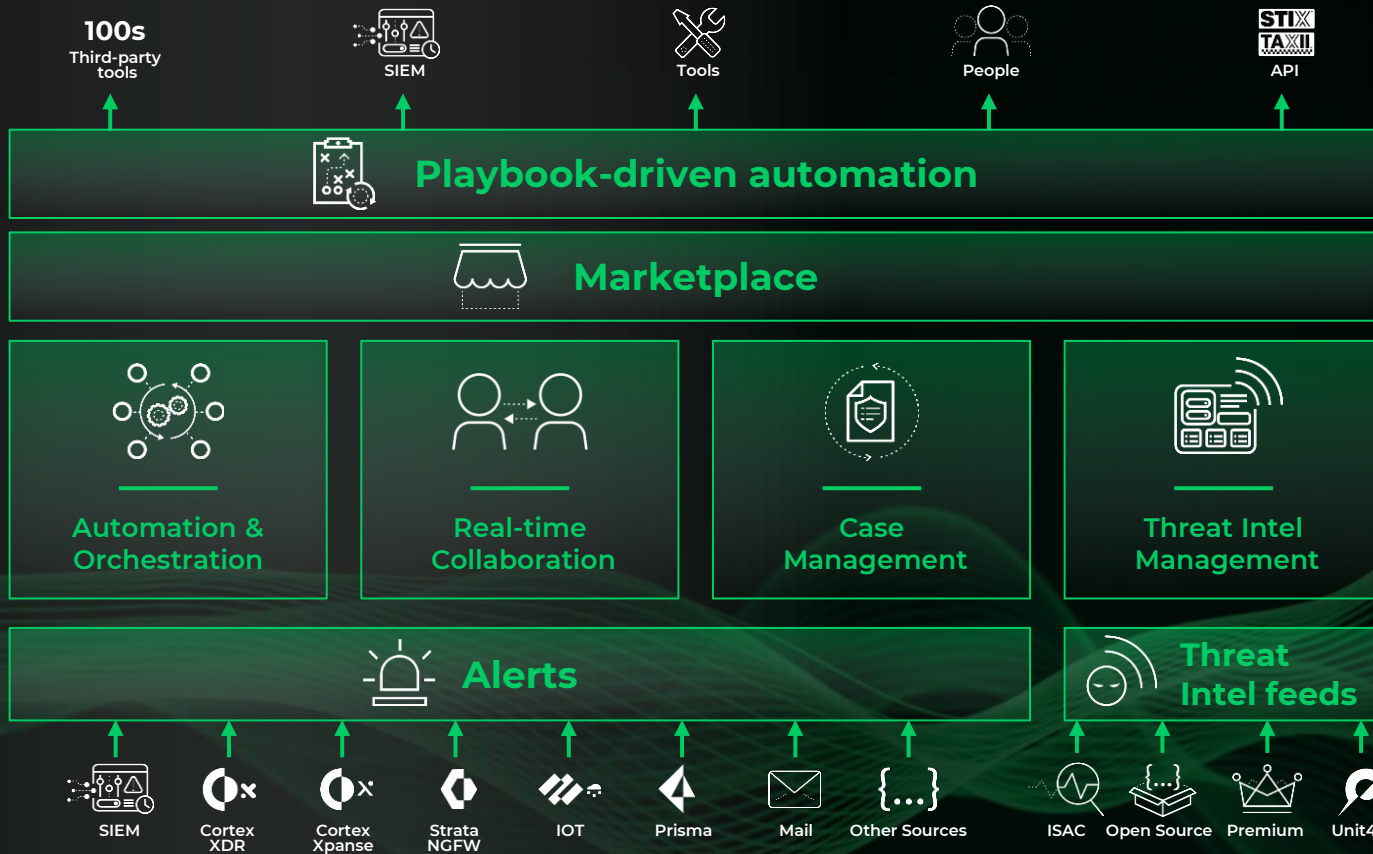


Automate manual and redundant processes

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 Orchestrate 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



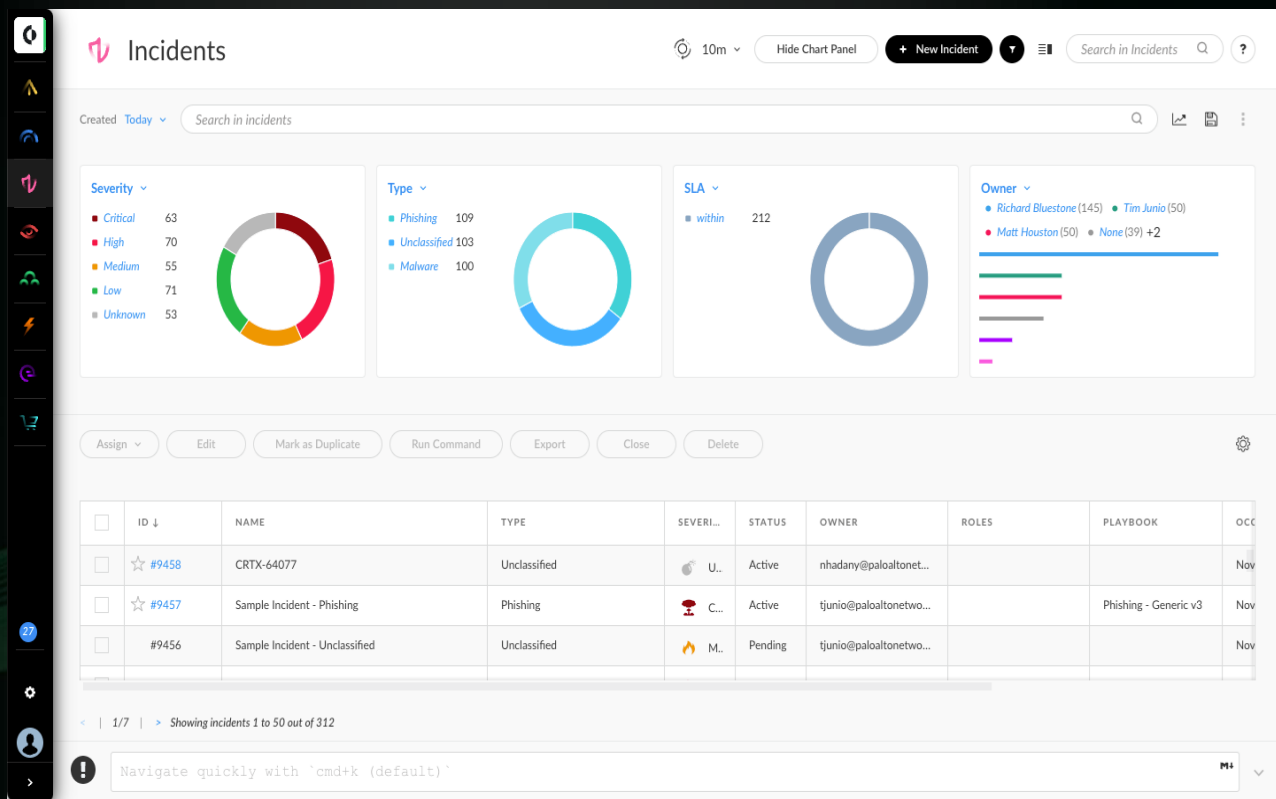
Automate Your Manual Workflows

The screenshot displays the Palo Alto Networks Playbooks interface. On the left is a 'PLAYBOOK LIBRARY' sidebar with a search bar and a list of playbooks, including 'Active Directory - Get User Manager Details'. The main area shows a detailed view of this specific playbook, titled 'Active Directory - Get User Manager Details'. The workflow is visualized as a flowchart starting with 'Playbook Triggered', followed by a decision diamond 'Is Active Directory enabled?'. If 'YES', it proceeds to another decision diamond 'By which attribute should the user be searched?'. This second diamond has two paths: 'USERNAME' leading to 'Get user details by username' and 'EMAIL' leading to 'Get user details by email'. There are also 'ELSE' paths from both decision diamonds. The interface includes a top navigation bar with '+ New Playbook', 'Settings', and 'View' buttons, and a bottom status bar with a toggle for full view.

**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

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

Automations make Zero Trust viable

Incidents

New Incident Search in Incidents ?

Created Last 7 days Search in incidents Refresh every 10 minutes Add to Saved queries

Severity

- Critical 1
- High 1
- Medium 1
- Unknown 5

Type

- Scenario 4
- Anomalous Netw... 1
- Compliance Check 1
- Cortex XDR Incid... 1
- Phishing Campal... 1

SLA

- within 4
- late 1

Owner

- admin (4)
- Matt Thorn (2)
- None (1)
- Chaitanya Sajja (1)

Hide Chart Panel Showing incidents 1 to 8 out of 8

Table View Summary View

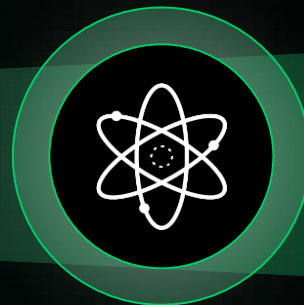
Assign Edit Mark as Duplicate Run Command Export Close Delete

ID	Name	Type	Severity	Status	Owner	Roles	Playbook	Occurred	SLA
#39347	#1277 - 'PowerShell runs with known Mimikatz arguments' generated by XDR BIOG detected on host lr-win10-10 involving user lr-win10-10oot	Cortex XDR Incident	High	Active	mthorn@paloaltonetworks.com		Cortex XDR Incident Handling - Demo	February 21, 2024 9:02 PM	N/A
#39346		Scenario	Unknown	Closed	admin		CreateDemoScenario	February 21, 2024 9:02 PM	N/A
		Anomalous Network Traffic			mthorn@paloaltonetworks.com		Anomalous Network		

Page 1 out of 1

Navigate quickly with Ctrl+K

Automate ZTNA for your SOC



Common SOC Use Cases



Rapid Breach Response



Phishing Response



Indicator Enrichment



Malware investigation & Response

Extended Security Automation



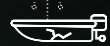
Cloud Security



Threat Feed Management



Remote User Access



Vulnerability Management

Enterprise Security Automation



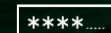
Network Security



Security Compliance

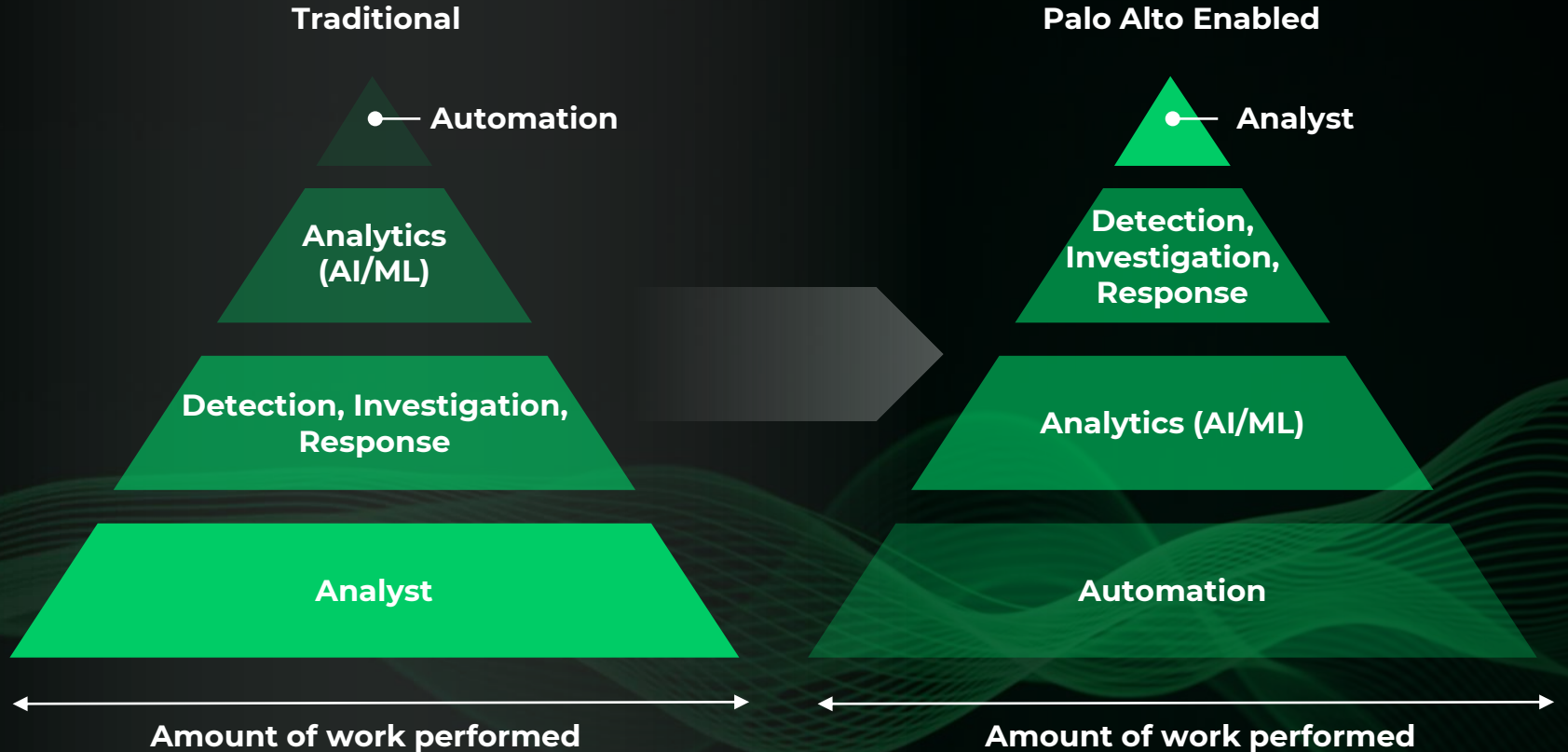


Identity & Password Management



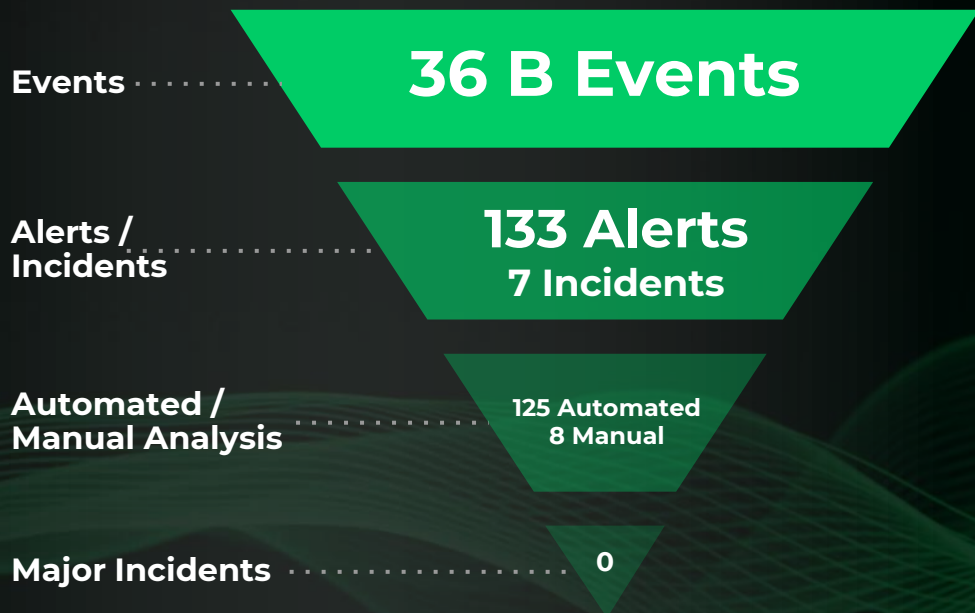
Other Security and IT Use Cases

We Need to Transition to Analyst-Assisted Security Operations



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

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



Mean Time to Detect



Mean Time to Respond
(High priority)

Because, ultimately, we should not be focusing on these

Dashboards & Reports

- Dashboard
- Reports
- Customize
 - Dashboard Manager
 - Report Templates
 - Widget Library

Incident Response

- Detection Rules
- Assets
- Endpoints

Managed Services

Search in Quick Launcher

Settings

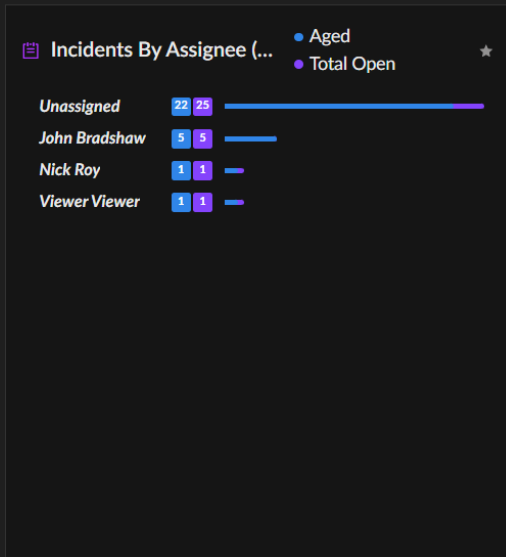
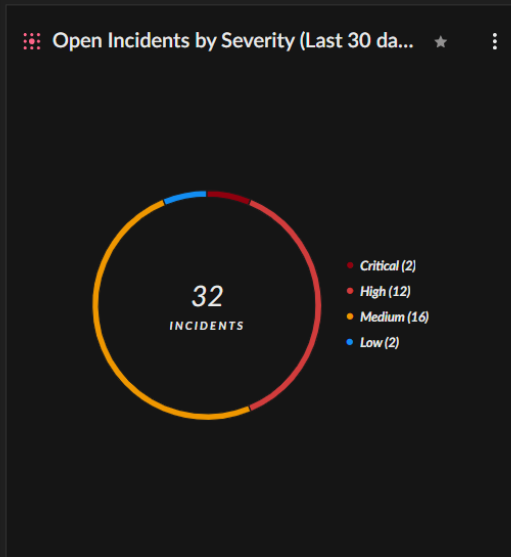
Tenant Navigator

Notifications (3)

Help

M T Matt Thorn
SE-Demo Corporation

Minimize menu <



Top Incidents (Top 10) ★

You have 1 new ingestion notification

	DESCRIPTION	ALERTS BREAKDOWN
100	Unusual use of a 'SysInternals...	[41 8 1]
100	'Staged Malware Activity - 40...	[31 26 6]
100	'Quasar RAT Command and C...	[7 13]
100	'generic:click-v4.plarimocl.co...	[17]
100		[5]

Top Hosts (Top 10 | Last 30 days) ★

HOST NAME	INCIDENTS BREAKDOWN
pc2	1 [1]
client-02	1 [1]
ws-it10	1 [1]
172.16.40.45	1 [1]
	1 [1]

We really need to focus on





Thank you

