CORTEX XSIAM BY PALO ALTO NETWORKS | paloalto NETWORKS

Talking About a Revolution

Making the Unsolvable Solvable in the SOC

Version 1.1

October 2023

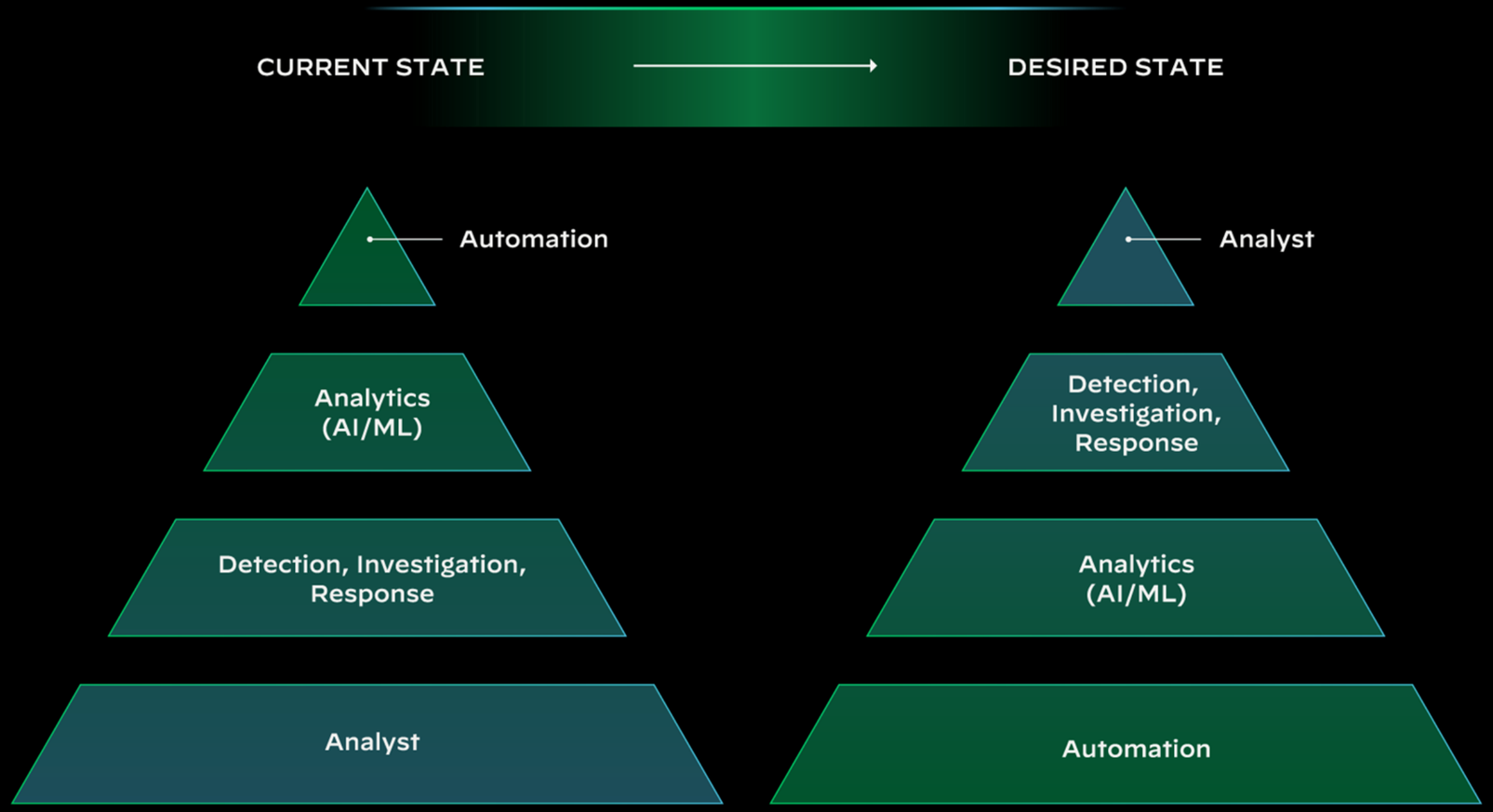
Making the Unsolvable Solvable in the SOC

The ever-expanding digital attack surface has created an urgent threat-remediation problem in cybersecurity.

Disparate detection and prevention tools generate an overwhelming number of daily alerts, surpassing what security teams can effectively handle. These disconnected alerts require extensive manual analysis and coordination among team members, resulting in enough resources only to focus on the highest-priority alerts, leaving many lower-priority ones unaddressed.

Unfortunately, historical investigations have revealed that some of these ignored alerts are part of larger attacks, which traditional security operations centers struggle to identify promptly. The lack of context and time-consuming manual steps in the triage process lead to inefficiencies and delayed response, giving cyber adversaries an advantage.

We Need to Transition to an Analyst-Assisted Security Operation

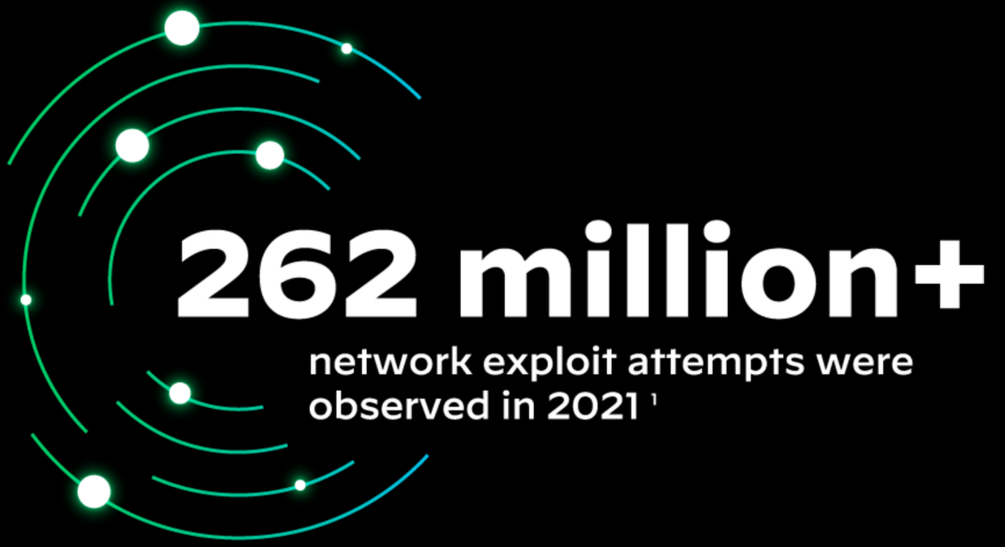


Organizations need a more efficient approach to rapidly identify and remediate threats to enhance their cybersecurity posture.

Why Can’t SOCs Stop Attacks in Real Time?

Most tools in the SOC, including SIEMs are designed for the analysts to be the intake:

- All these different data sources are using their own analytics.
- The SOC analyst has to put everything together.
- Separate workflows for detection, investigation, response.
- Automation can take care of a lot of this work but it doesn’t solve the problem.



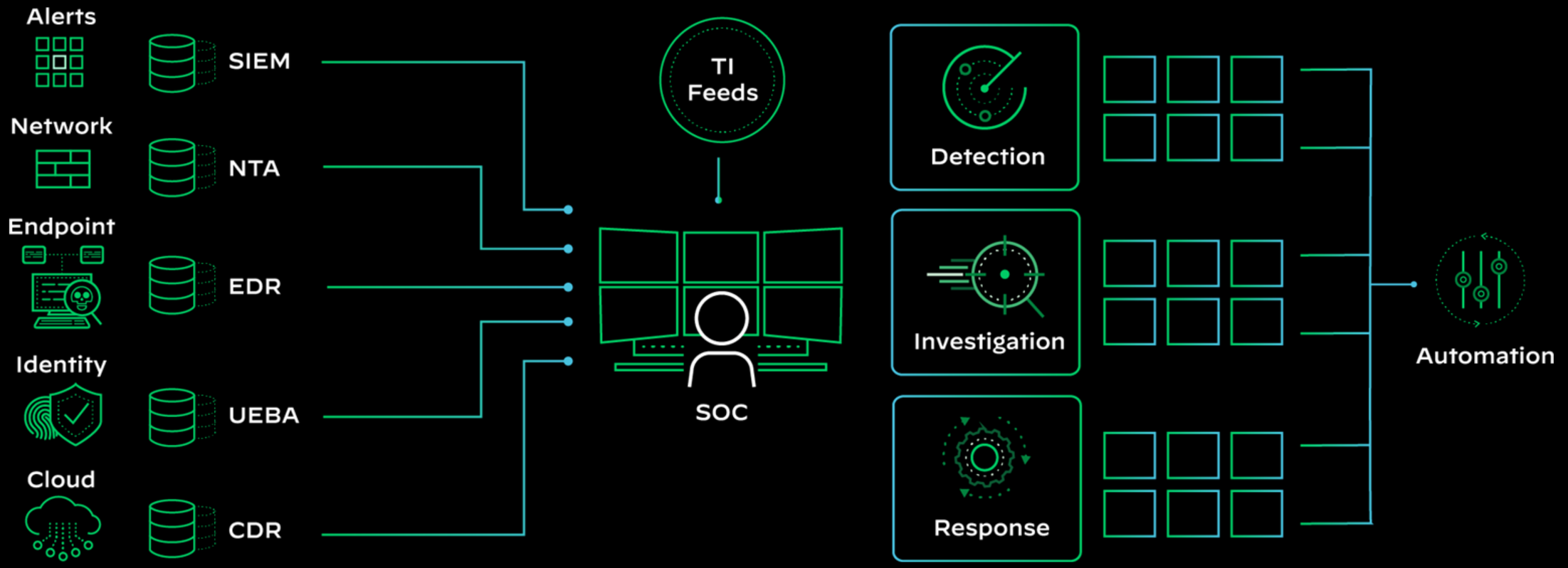
1. 2022 Unit 42 Network Threat Trends Research Report

Why Can’t SOCs Stop Attacks in Real Time?

Too many data silos make it hard to detect attacks

Teams build and maintain detection content, use multiple tools to manually investigate and respond

Automation is bolted on at the end for scale



If you always had the data to figure out what happened after the incident, why didn't you figure it out in real time? And the answer is:
Humans cannot investigate 1 million events per second. But AI can do that.

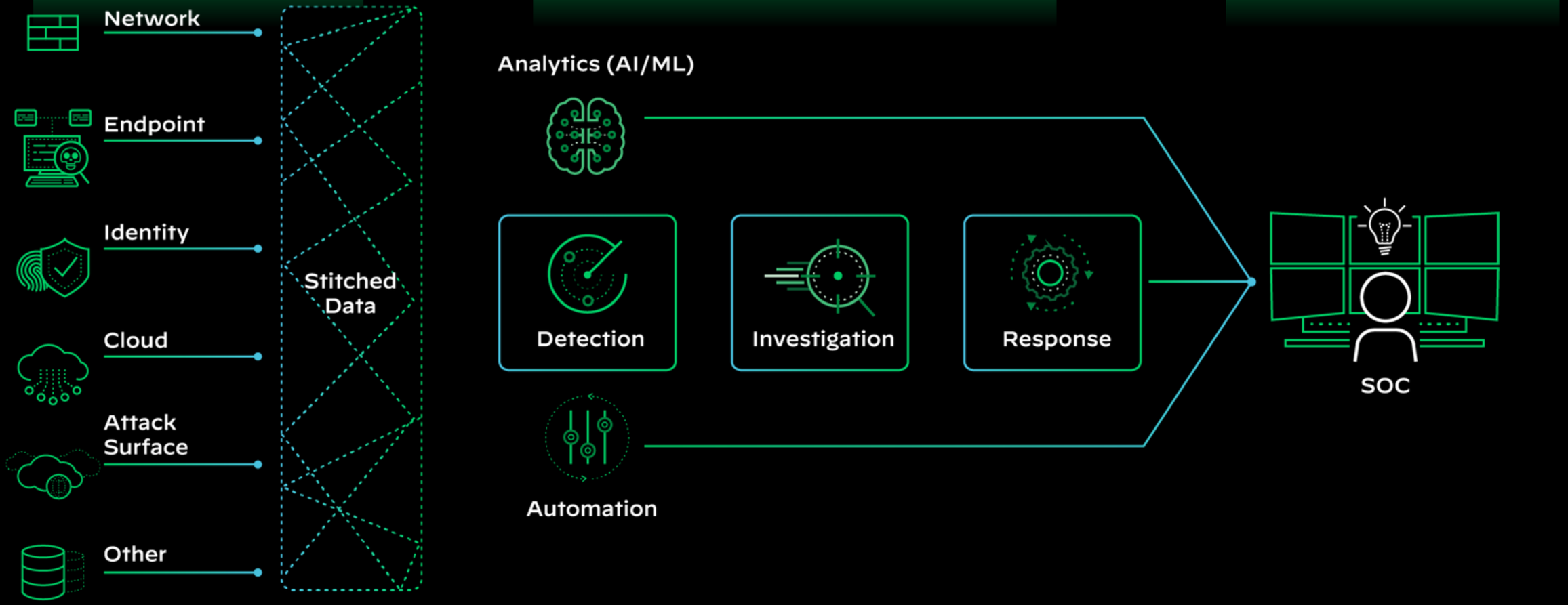
Nir Zuk
Founder & CTO, Palo Alto Networks

We Must Transform the SOC to be AI-Driven, Analyst Empowered

Massive amounts of data improve detection efficacy

Machines automate detection, investigation, and response and make recommendations

Empowered analysts become more proactive



Shifting Our Mindset

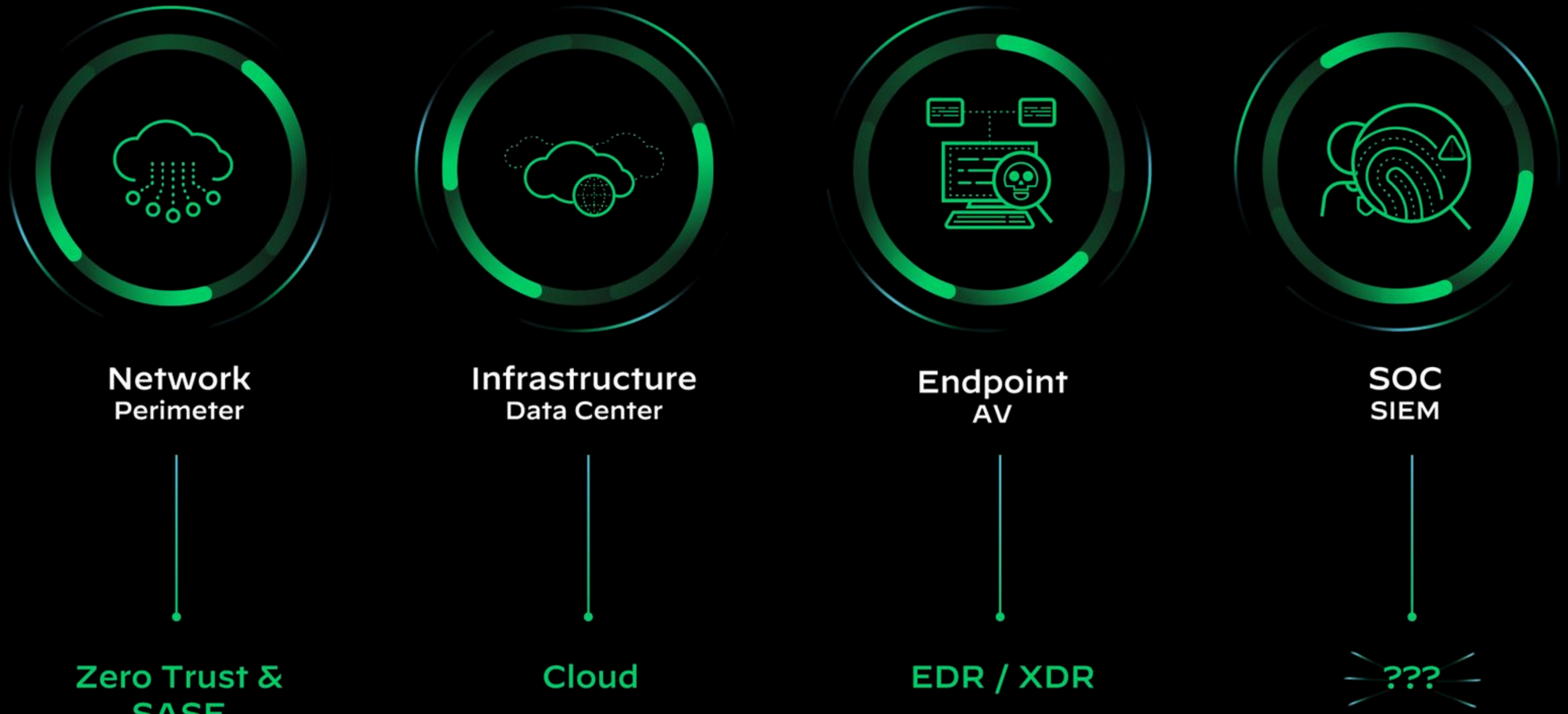
In cybersecurity, we need to prioritize human-readable alerts to ensure effective analysis. Currently, we rely on a small portion of pre-processed and pre-filtered data that analysts can handle. However, this approach is not enough.

To improve our security strategy, we must shift our mindset. Instead of making analysts the front end of the process, we should leverage automation and ML/AI to handle the initial data influx. By feeding vast amounts of data to these systems, we can run detection engines, investigations, and response capabilities on the resulting analytics and automations.

Analysts then take on a supervisory role, making crucial decisions and investigating data that seems anomalous or doesn't align with the automated findings. This necessitates building a robust platform that embraces this new approach to cybersecurity, which is why we created Cortex XSIAM.

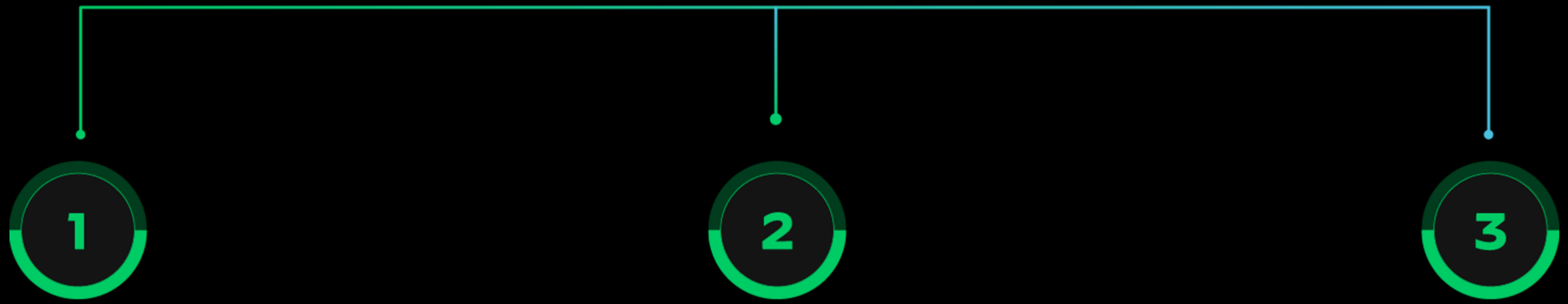
The Need for Change

Most security real estate has been redesigned except:



The Need for Change

The SIEM market has been slow to evolve, with limited incentive for vendors to invest in significant changes to their products and solutions. There are several reasons for this technological inertia, including:



Integrating SIEM solutions with other security tools, such as EDR systems, IDS, and NTA tools, poses challenges as each of these tools require their own enablement, turning, maintenance, and validation that outputs are correctly still found in the SIEM.

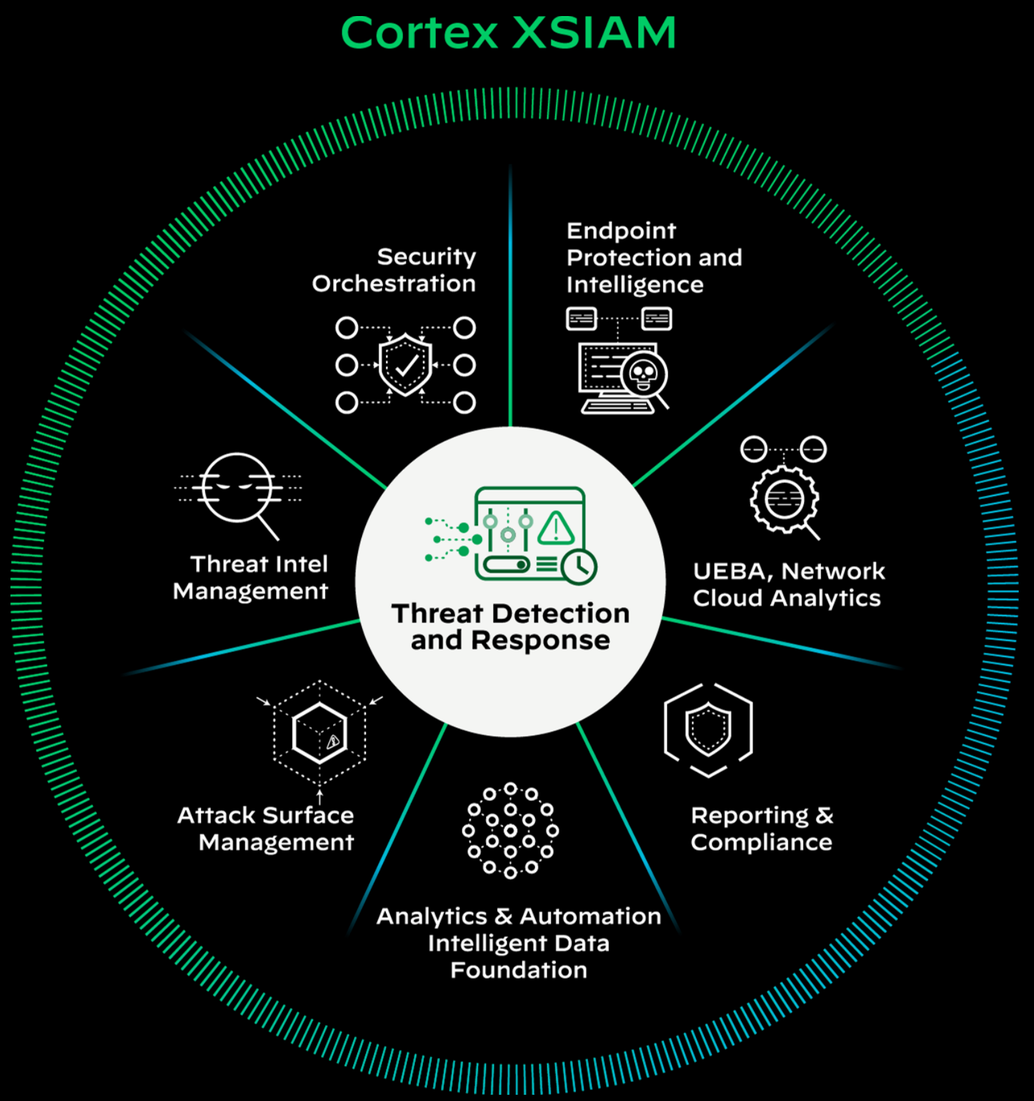
Customized SIEM solutions tailored to specific needs may necessitate time-consuming and costly reconfiguration, making it difficult or impossible to pivot when the business needs.

SIEM solutions that were commonly employed to meet regulatory compliance requirements oftentimes were just configured for that purpose and fail to detect modern threats.

The Urgency for Radically Reimagined Cybersecurity

Cortex XSIAM harnesses the power of machine intelligence and automation to radically improve security outcomes and transform the SecOps model.

XSIAM puts the SOC in full control of enterprise security—endpoint to cloud—centralizing data and security functions to outpace threats, accelerate response, and dramatically streamline analystand SOC team activities.



The Urgency for Radically Reimagined Cybersecurity

1. Replace out-moded SIEM to centralize and act on true security intelligence.
2. Consolidate disparate SOC tools for efficient and cost-effective operations team-wide.
3. Get machine-driven security at scale, while analysts focus on high value tasks.
4. Extend SOC visibility and control to cloud and dynamic internet resources.
5. Depend on threat detection that's proven to protect the entire enterprise — endpoint to cloud.
6. Protect endpoint targets from laptops to datacenter systems to cloud workloads.

Centralize, automate, and scale operations to protect your organization

Time Savings: Traditional SIEM vs XSIAM

SIEM XSIAM

Threat Detection Development

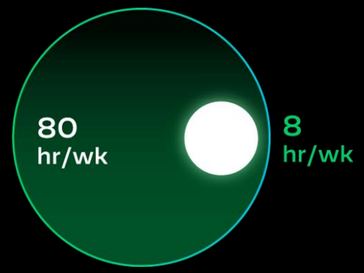
Continuous processes to create new alerts that adapt to changing threat landscape.

100
hr/week saved

Outsourced most threat detection development to XSIAM research team.

Alert Tuning

Continuous processes to improve alerts based on historic fidelity.



72
hr/week saved

Outsourced tuning of endpoint alerts to XSIAM research team.

System Maintenance

Log parsing, server patching, etc.

No change

Analytics

Creation of advanced alerts that take into account complex statistics and machine learning.

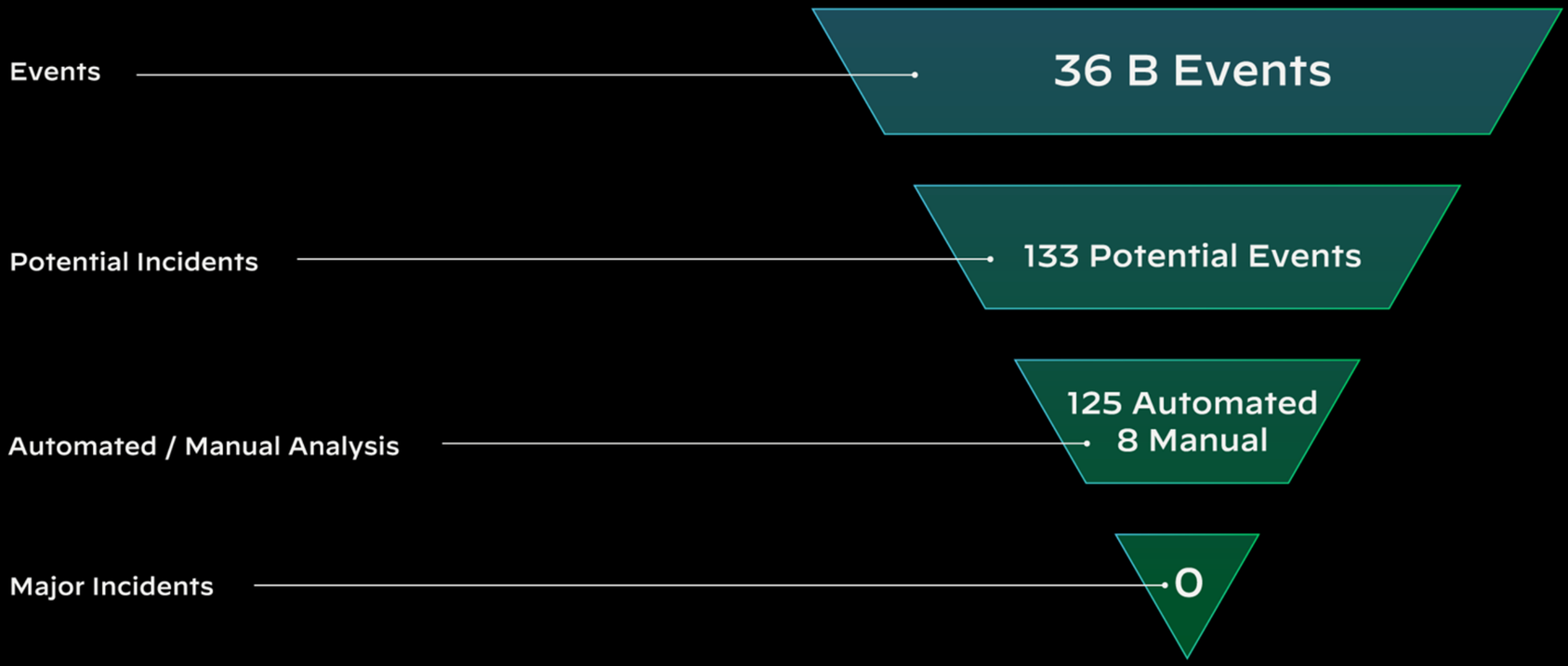
SIEM [Capability gap]
Requires add-on package and building your own machine learning model. Normalization is difficult.

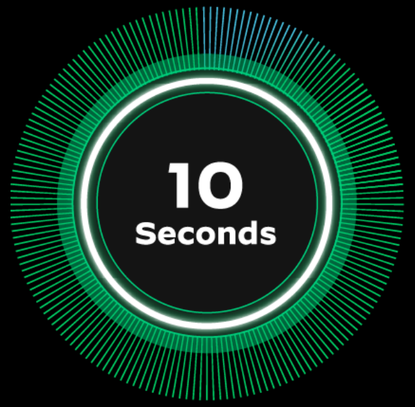
XSIAM [New capability]
XSIAM has automated baselining and anomalous alerting through statistics and ML.

Time-Saving Results:
4.5 FTE Total Effort Reduction

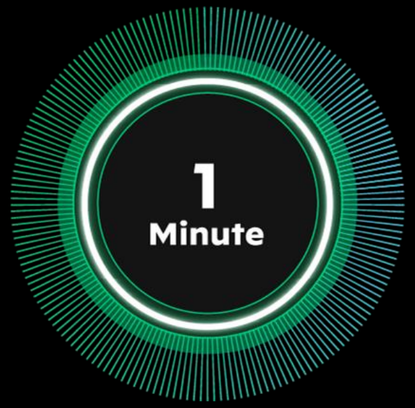
paloalto NETWORKS | CORTEX

What Our SOC has Achieved with Cortex XSIAM:





Mean Time to Detect



Mean Time to Respond
(High Priority)

paloalto NETWORKS | CORTEX

More than Alerts & Logs: Cortex XSIAM Highlights

An Intelligent Data Foundation:

- Simplified connection and collection for any data source.
- Automatic data normalization and enrichment.
- Stitches data for rich analytics and investigation context.
- Built on a cost-effective, scalable cloud architecture.

More than Alerts & Logs: Cortex XSIAM Highlights

Outpaces Threats:

- Cloud and attack surface visibility and threat detection.
- Specialty endpoint, network, cloud, UEBA analytics.
- Real-time behavioral analysis and methods across all data.
- Continuous intel and learning from 85,000 customers.

More than Alerts & Logs: Cortex XSIAM Highlights

Accelerates Response:

- Alert grouping, incident enrichment and prioritization.
- Auto-execution of common activities.
- Intelligent in-line playbook functions and rich library.
- Unifies and automates broad SOC functions.

Automation: More Than Workflow

When we talk about automation, we don’t just mean workflow automation, i.e. automating what a human analyst does with an alert. We also mean native automation embedded into the product to normalize and stitch events together into an “attack story,” to create new detectors to dispatch alerts, etc.

With XSIAM, we have built this native automation in addition to workflow automation. In some areas, we’ve combined the two. For example, XSIAM can recommend new playbooks or response actions based on machine learning, thereby making workflow automation (SOAR) more powerful.

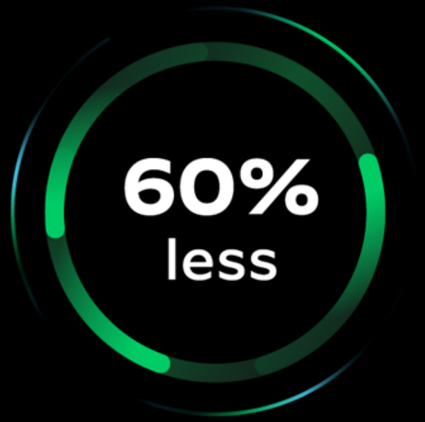
Our SOC XSIAM Experience

Server Maintenance

No server patching

Simple agent upgrades

Engineers can focus on expanding data collection vs. being a “server janitor”



Detection Engineering

Access to expert research

Frequent content updates

Automated feedback loop and ML results in better detections

Faster Data Onboarding

Native integrations

Vendor agnostic

Increased scope and visibility

Better Analyst Experience

Fewer browser tabs

Faster query building

Simple user interface

But Don’t Just Take Our Word for It

While XSIAM is delivering exponential improvements in the Palo Alto Networks SOC, our primary objective is to innovate to outpace cyberthreats, so customers can embrace and deploy our technology with confidence.

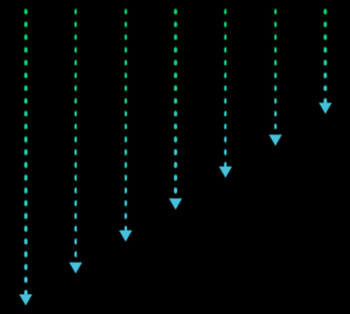
Recent customer success metrics provide evidence that XSIAM is doing just that.

MTTR

270x Faster

Added 10x more data yet improved MTTR from
3 days to 16 minutes

Services Company

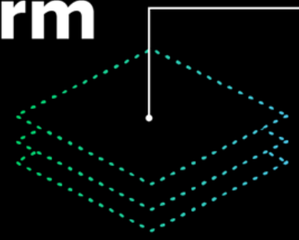


75% Reduction
in incidents requiring investigation from
~1000 a day to ~250 a day, eliminating false positives and duplicates

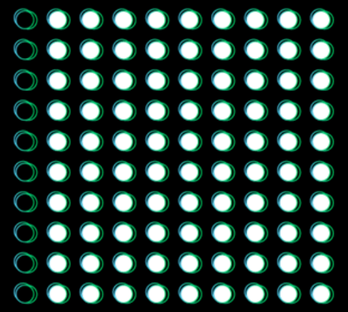
Oil & Gas Company

Boyne Resorts

Added 20 more data sources
Into 1 Platform
streamlining and improving investigations



Imagination Technologies



10x Improvement in incident closure rate from less than
10% to 100%

paloalto NETWORKS | CORTEX

With XSIAM, we have more visibility and faster investigations. Seamless data onboarding and automation setup are gamechangers.

Senior Network Lead
at resort chain

Thank You

To learn more about the transformative security outcomes you can experience with XSIAM, learn more in our e-book:

[Cortex XSIAM, The Machine Led, Human Empowered Security Platform]

paloaltonetworks.com