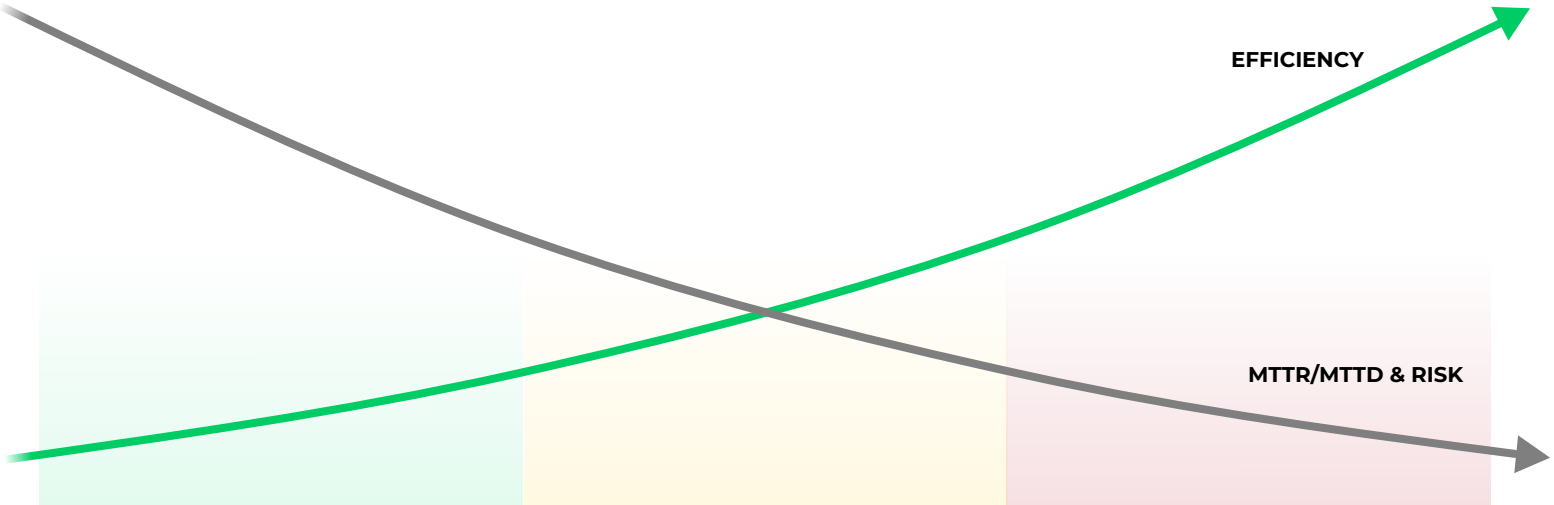
CORTEX
BY PALO ALTO NETWORKS

Shift from dozens of siloed SOC tools to Cortex

Tudor Cristea - Cortex RSM

paloalto NETWORKS

How SecOps must transform to reduce risk



Maturity	**Low** (Reactive)	**Medium**	**High** (Proactive)
Detection	RULE-BASED	CORRELATED RULE-BASED	ANALYTICS-BASED
Context	LOG AGGREGATION	SILOED DATA COLLECTION	INTEGRATED RICH DATA
Automation	NONE	PARTIAL	FULL

Cortex Vision for Proactive Security

SCOPE and **PROTECT** your attack surface

PREVENT everything you can

Everything you can't prevent, **DETECT** and **INVESTIGATE** fast

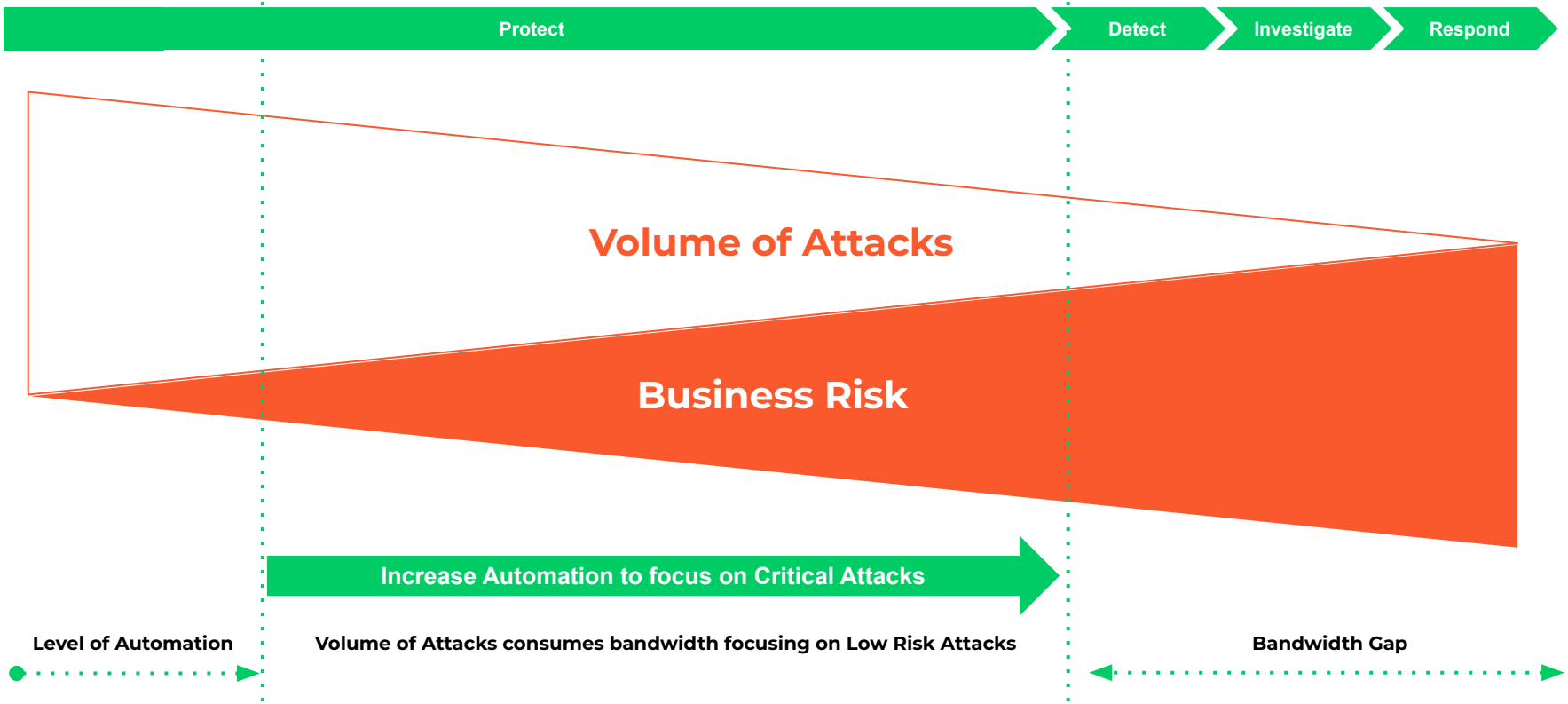
AUTOMATE response and get smarter with every incident

A day in Our SOC

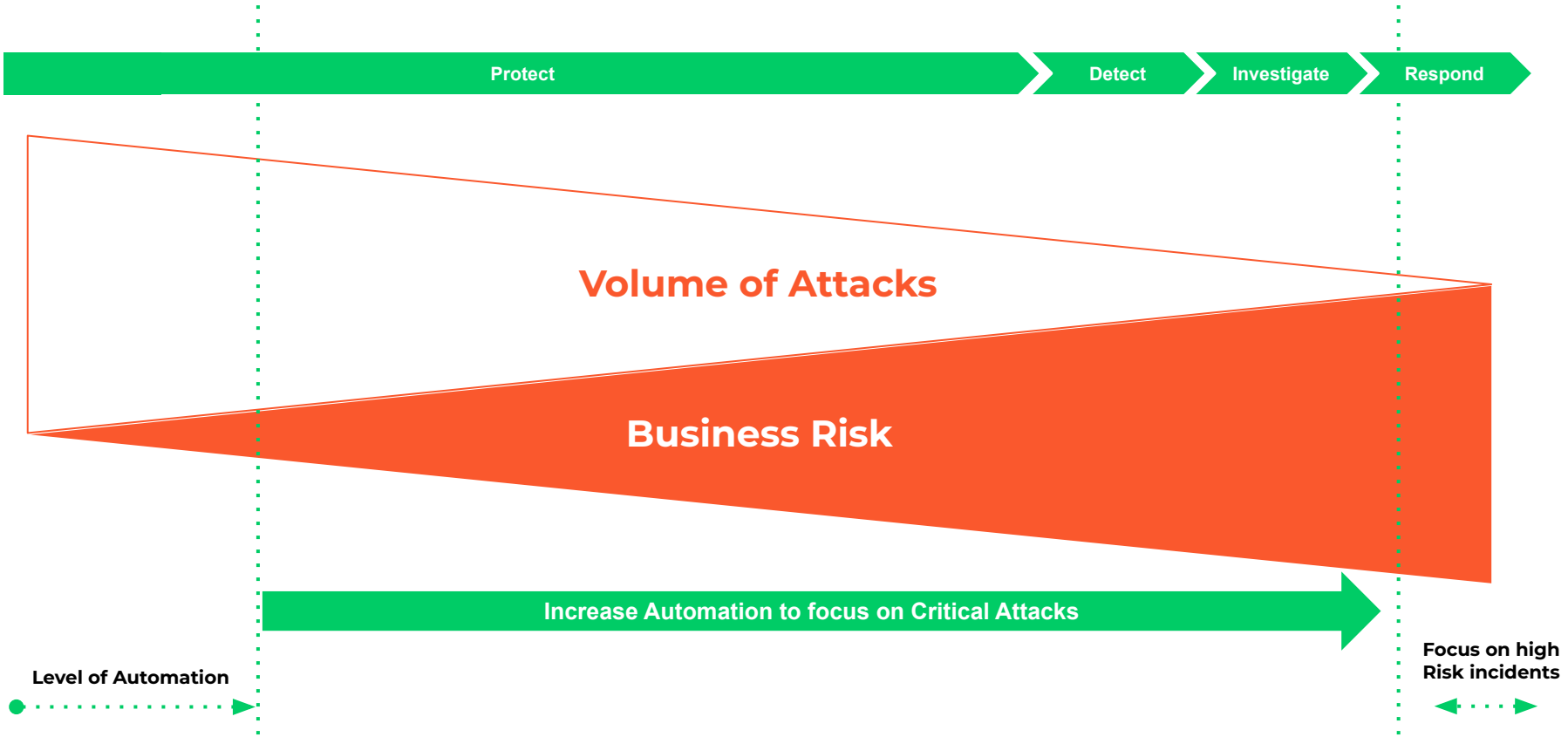
Transform Your Security Architecture for better Outcomes

paloalto NETWORKS

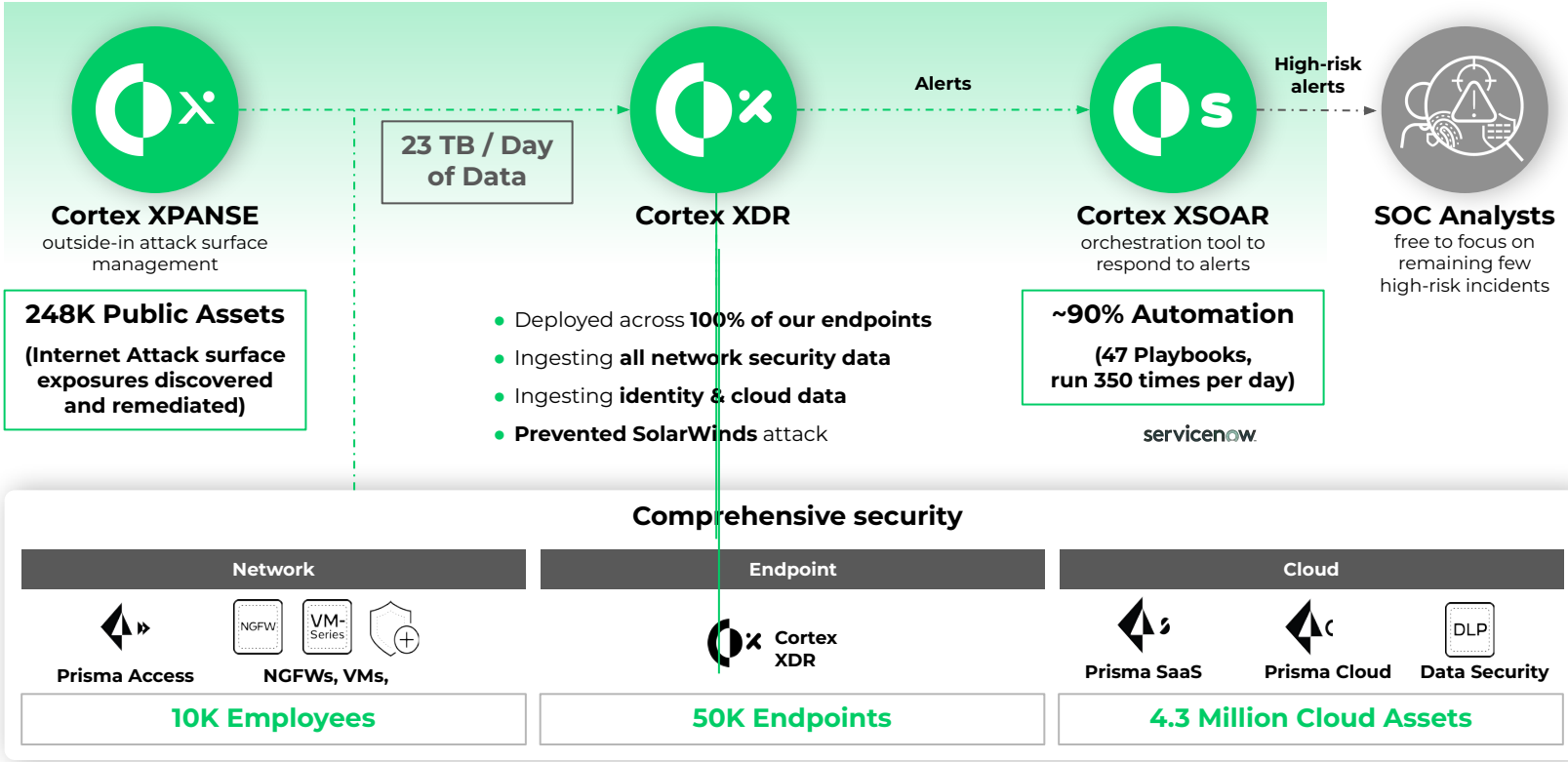
Increase Automation to address Volume and Risk at the same time



Increase Automation to address Volume and Risk at the same time



Palo Alto Networks SOC: Eating our own dog food



SOC Playbooks in Cortex XSOAR

Incident Playbook

1. Cortex XDR Incident
2. Prisma Saas Alert
3. Prisma Cloud Alert
4. Okta Alert
5. WinEvent Alert
6. Linux Alert
7. Proofpoint Alert
8. G-Suite Alert
9. GCP Alert
10. Support Requests
11. NGFW Alert
12. Abuse Reports
13. Bishop Fox Alert
14. Expanse Alert
15. Monitoring Alert
16. Password Spray Alert

Analysis Subplaybooks

Upon Trigger

1. Calculate Severity
2. Get JIRA ticket info
3. Get user details
4. Get host details

Gather Details

1. URL Enrichment
2. Domain Enrichment
3. User Enrichment
4. Email Address Enrichment
5. Host Enrichment
6. Attachment Enrichment
7. IP Enrichment
8. Related email search
9. Related log search
10. Forensic capture
11. Ask user a question

Response Subplaybooks

Containment Subplaybooks

1. Lock AD user account
2. Lock AD service account
3. EDL Block (IP/Domain/URL)
4. PAN-DB re-categorization
5. Block email sender
6. Quarantine email
7. Quarantine files
8. Quarantine device
9. Disable project

Eradication/Remediation Subplaybooks

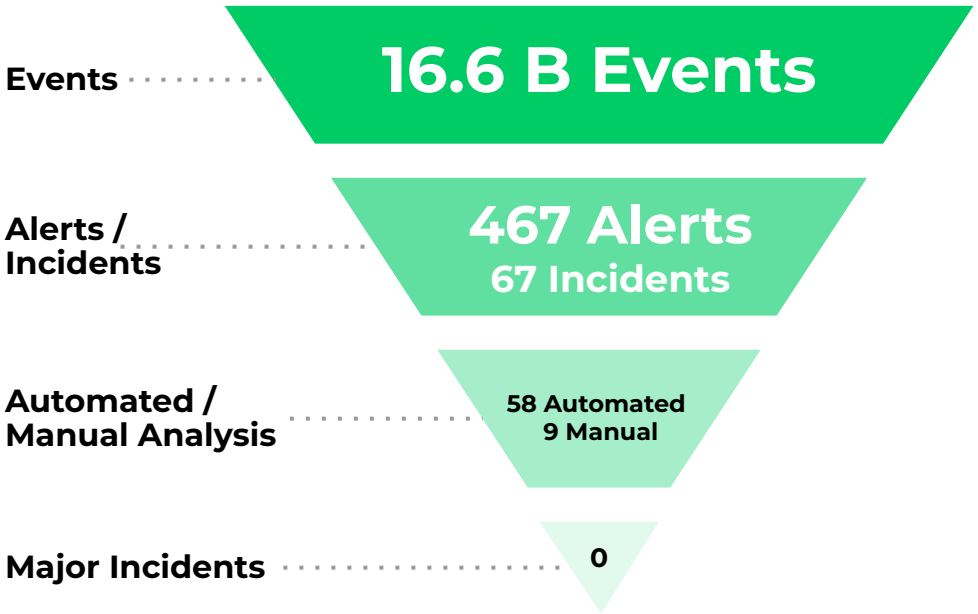
1. Re-image request
2. Search and destroy
3. External website takedown
4. Revoke physical badge access
5. Kill sessions

Post-Incident Metrics

1. Metrics incl. effort
2. Record alert fidelity
3. Timeline

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

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



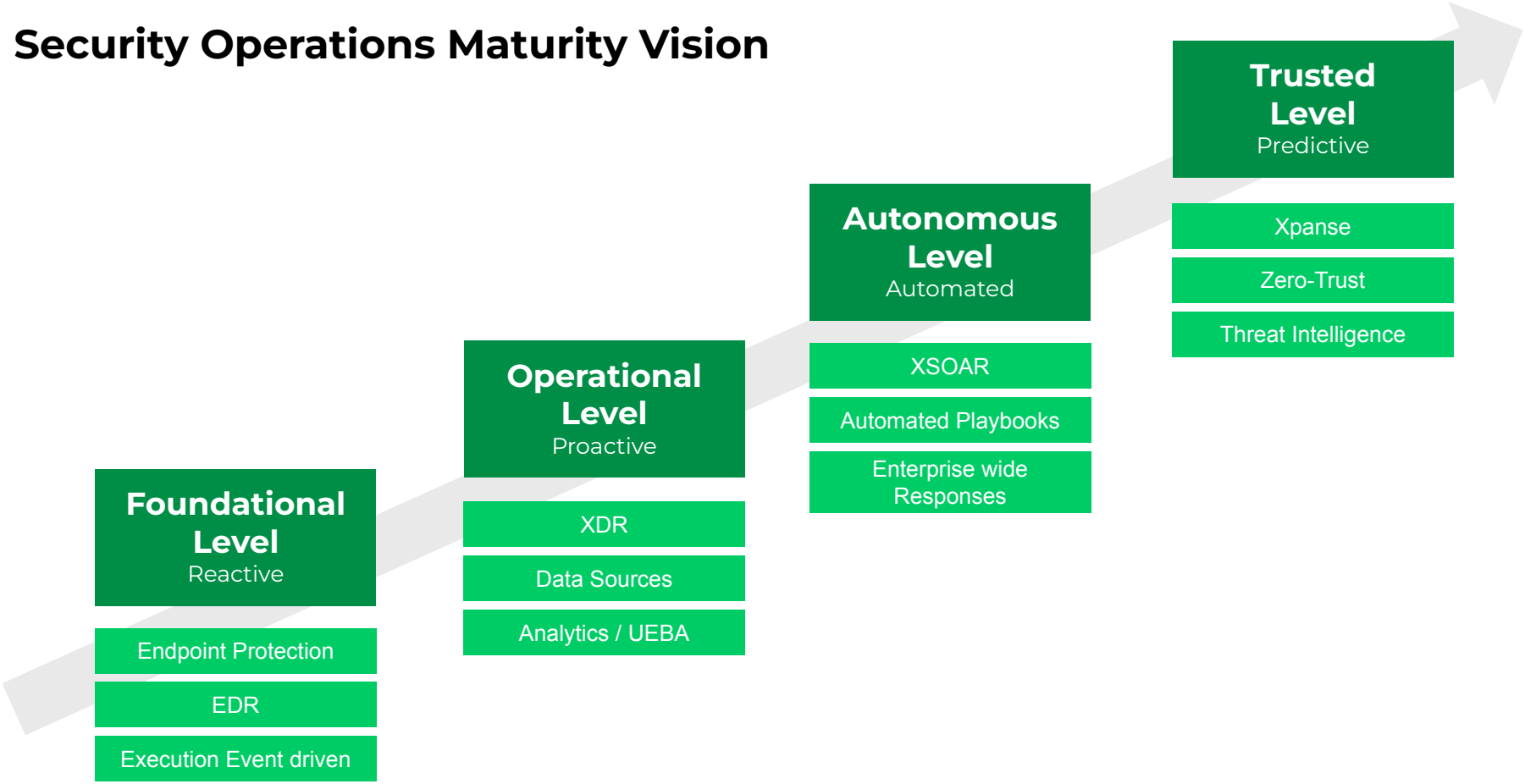
10
SECONDS

Mean Time to Detect

1
MINUTE

Mean Time to Respond
(High priority alerts)

Security Operations Maturity Vision



Protect

Next Gen Endpoint & EDR to provide prevention and detection capabilities in one Platform

Detect & Investigate

Broad Context and strong Analytics to under the Attack Story faster

EDR and SIEM Products Have Not Adequately Solved the Problem

EPP / EDR

Deep analytics and threat detection

Lack coverage and context for entire environment

EDR

Endpoint

Lack of Analytics

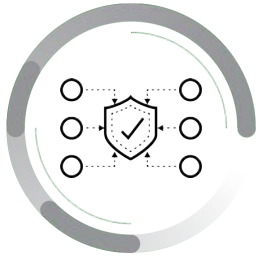
Lack of Data and Context

SIEM

No Endpoint

Lack of Analytics

SIEM



SIEM

Mile-wide, inch-deep understanding of data

Deficient analytics and detection

Lack of workflows

Lack of control Points to remediate

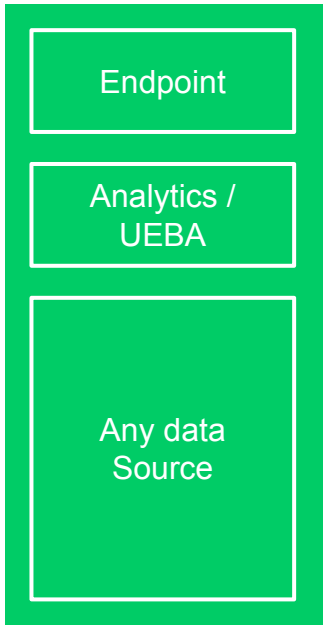
XDR is designed to increase SOC efficiency

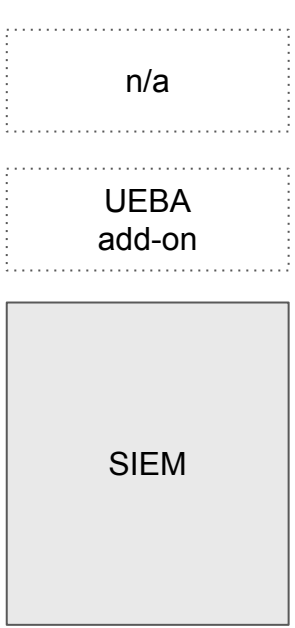
Protection
- Modern EPP Platform

Detection
- Data Stitching to tells the Story automatically
- Stitching means one unique event and not multiple log files (ML optimized)

Investigations
- Build in analytics will stitch anomalies over multiple days
- Workflows which are design to understand the complete picture easily

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





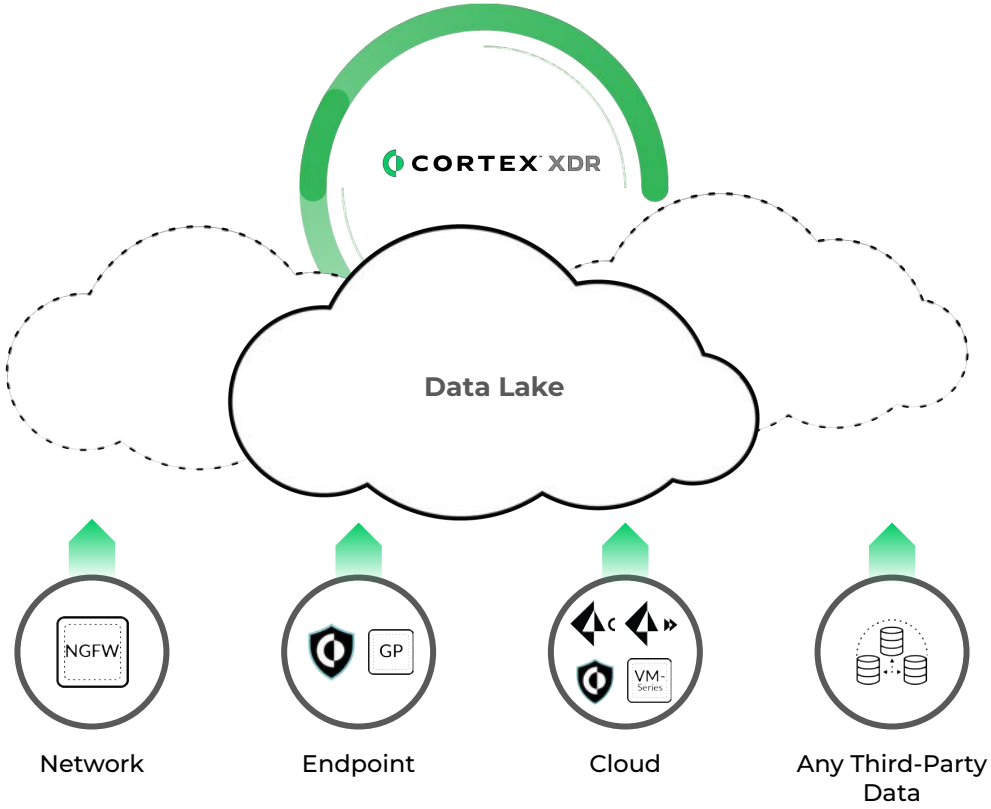
Protection
- Not available

Detection
- Static Correlation Rules “Known Bad”
- Only triggered if all criteria is met (if, then, else conditions)
- Historic data, Not real time

Investigations
- Lack of analytics means investigations are manual
- Lack of Context (alert that people work on PII data but they are in customer service)

Response
- API based integrations with Endpoint vendors
- Limited actions

Shift-Left in Detection with broad Sensor Network and Context

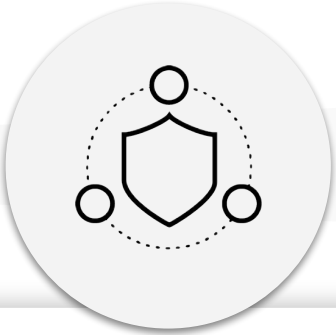


Response & Automation

Prioritized and Automated Responses to reduce Risk and MTTR

Protect | Detect | Investigate | **Respond** | Predict

Cortex XSOAR: Striving to automate everything

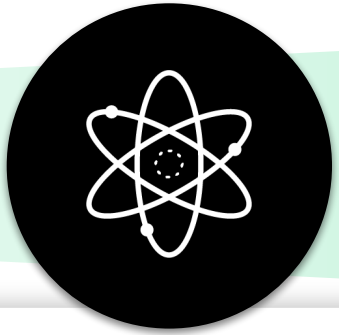


SOC Automation

- Threat Intel Enrichment
- Phishing Response
- SIEM Enrichment
- Automated Threat Hunting

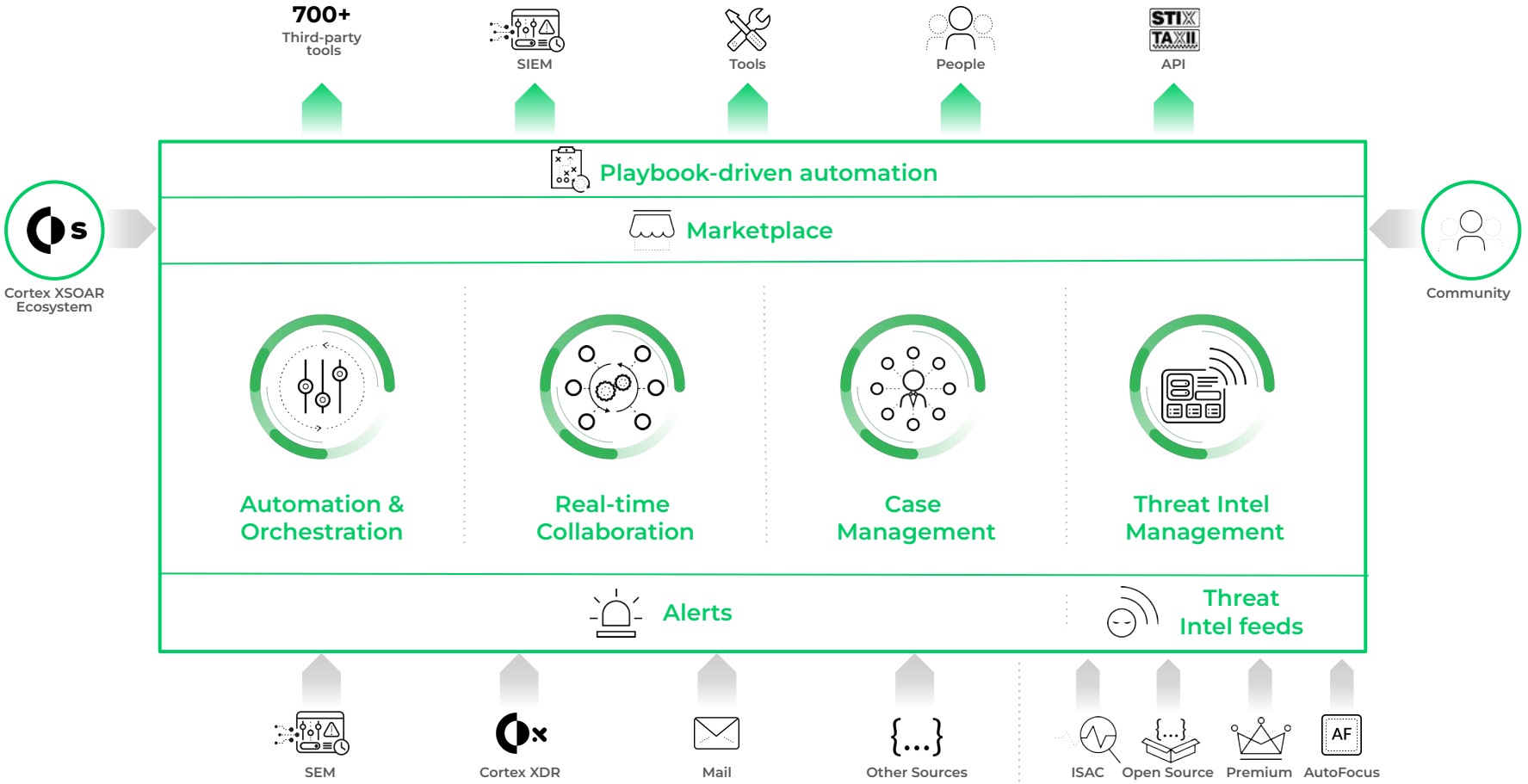
Extended Security Automation

- Vulnerability Management
- Cloud Security
- Complete Threat Intel Management
- IoT Security

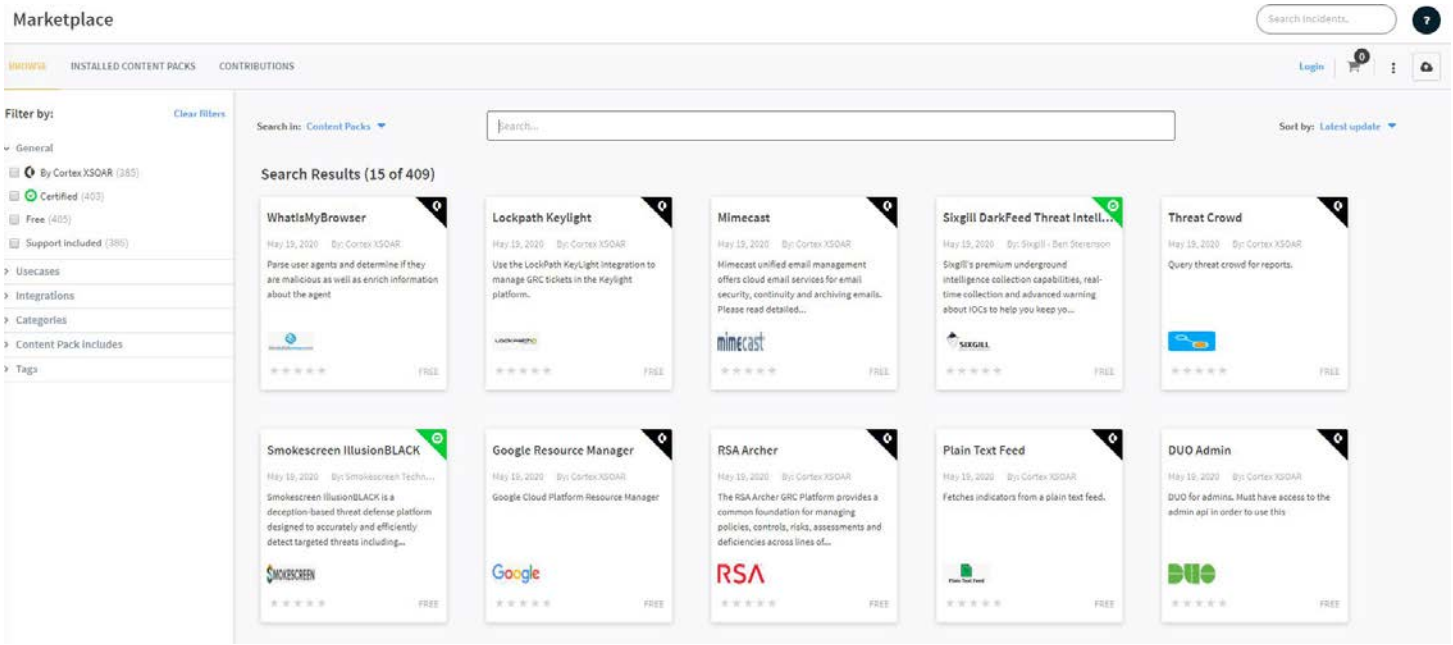


Enterprise Security Automation

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



Cortex XSOAR Marketplace - Largest SOAR Ecosystem



550+
Content Packs

700+
Partner Integrations

150+
New integrations last year

Predict

Predicative Security with continuous Attack Surface Management & automated responses

Protect | Detect | Investigate | Respond | Predict

What businesses need is

A continuous, real-time, and updated view of their attack surface to discover, evaluate and mitigate exposures of their internet-connected assets.

Managing your Attack Surface with Xpanse

Discover

Continuously indexing the entire internet discovering all connected devices and exposed services.

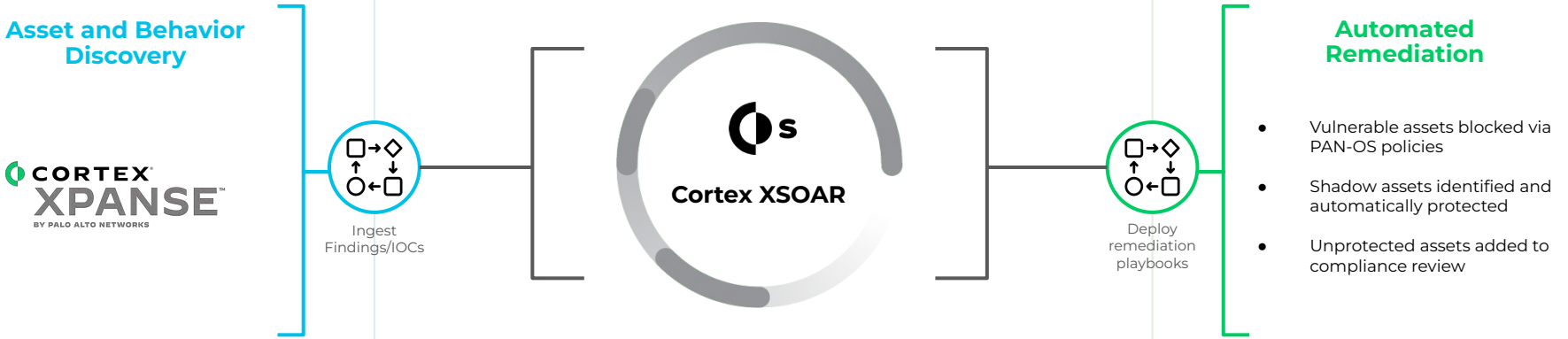
Evaluate

Supervised ML engines power high-accuracy attribution and perpetual risk identification.

Mitigate

Automated policy-driven remediation leveraging existing processes and platforms.

Automate attack surface remediation with Xpanse and XSOAR



01 Ingest discovered unknown assets such as IP ranges, domains, and certificates and risky unknown communications

02 Coordinate across different points of enrichment (firewall, SIEM, internal databases), triage incidents based on severity, and deploy remediation playbooks

03 Automated remediation with intelligent ML powered playbooks

CORTEX
BY PALO ALTO NETWORKS

Thank you

Tudor Cristea

paloalto NETWORKS