

Cortex XSOAR

Security Orchestration, Automation and
Response (SOAR)

Running your SOC Remotely



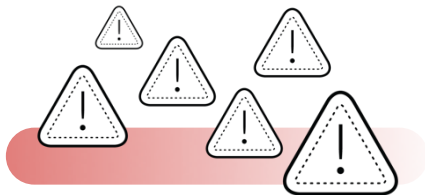
Remsis Pérez

Systems Engineer

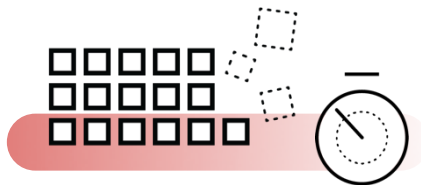
Remote SOC are the New Reality



Why do security teams struggle?



**Too much noise
(a.k.a alert fatigue)**



**Too many products
to piece together an
incident**



**Too many
manual, repetitive
actions**

BRACE YOURSELF



I find you lack of faith
AUTOMATION
disturbing

~~Varth Vader~~
Security Engineer

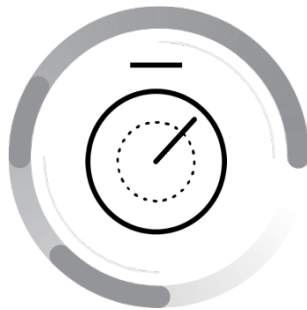
The lack of automation



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+

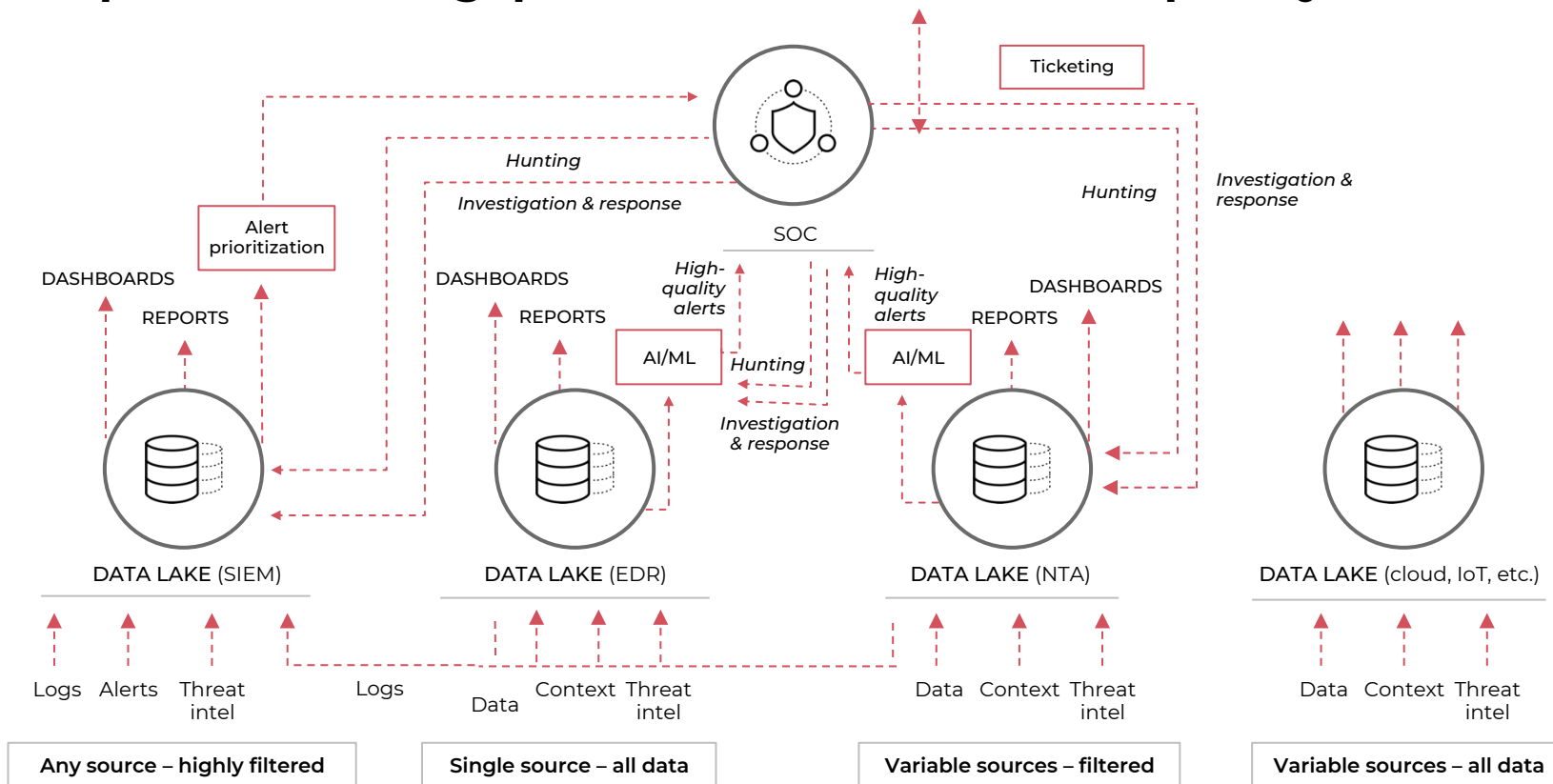


Limited Context

It takes days to understand incidents & investigate threats

4+ days

Attempts to address gaps result in even more complexity



Rewiring SecOps with Cortex



**Prevent
everything
you can**

 **CORTEX XDR**



**Everything you can't
prevent, detect and
investigate fast**

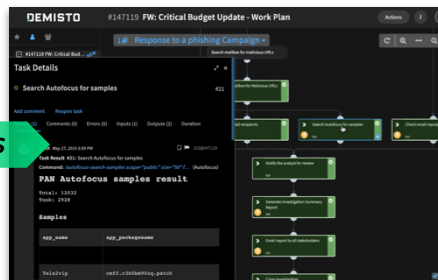
 **CORTEX XDR**



**Automate response
and get smarter with
each incident**

 **CORTEX XSOAR**
BY PALO ALTO NETWORKS

Orchestrate, manage and respond with Cortex XSOAR



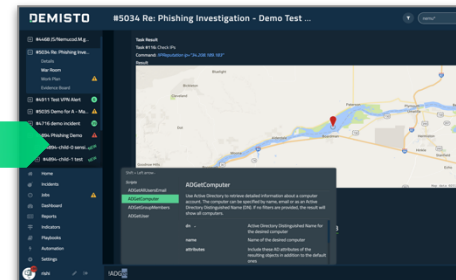
Orchestrate and automate

Playbook-based orchestration with 350+ vendor integrations



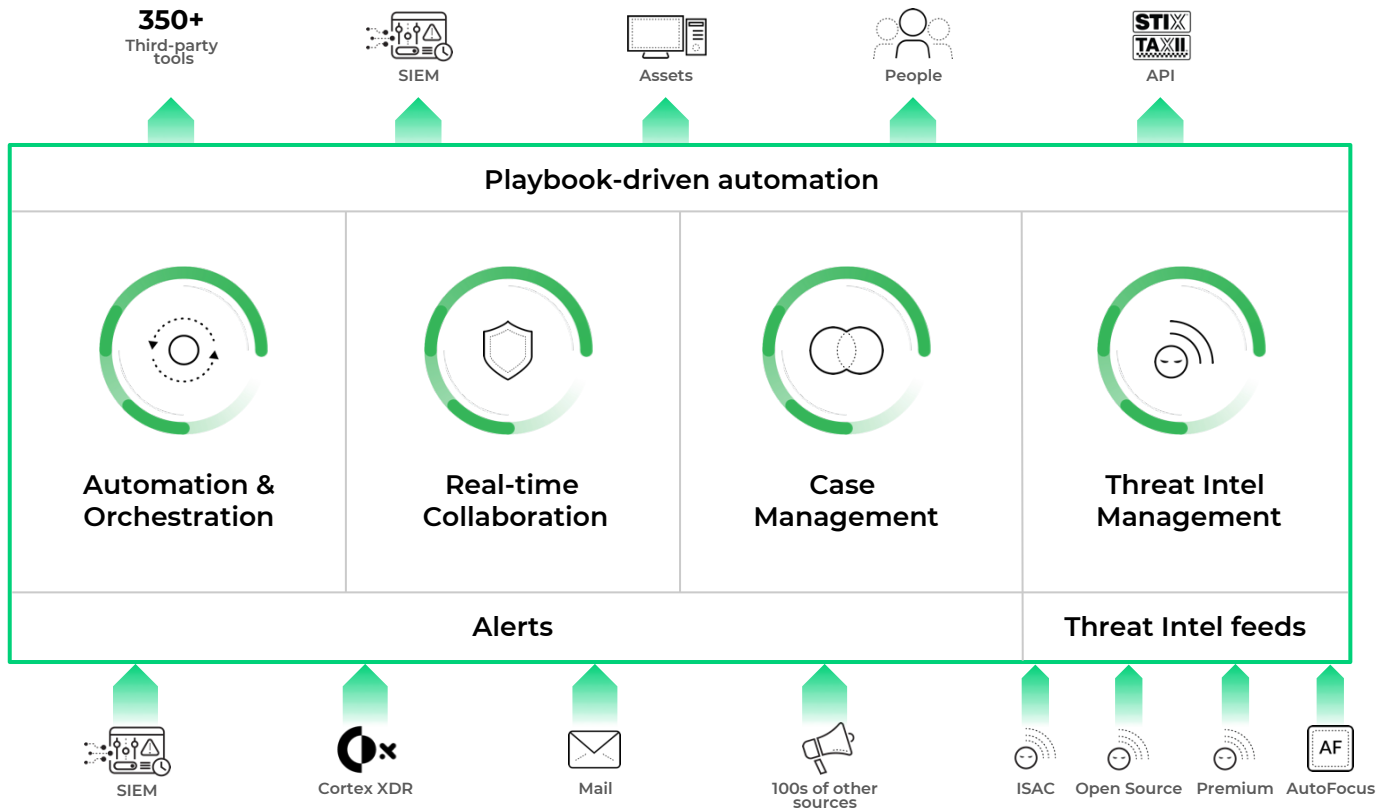
Manage and investigate

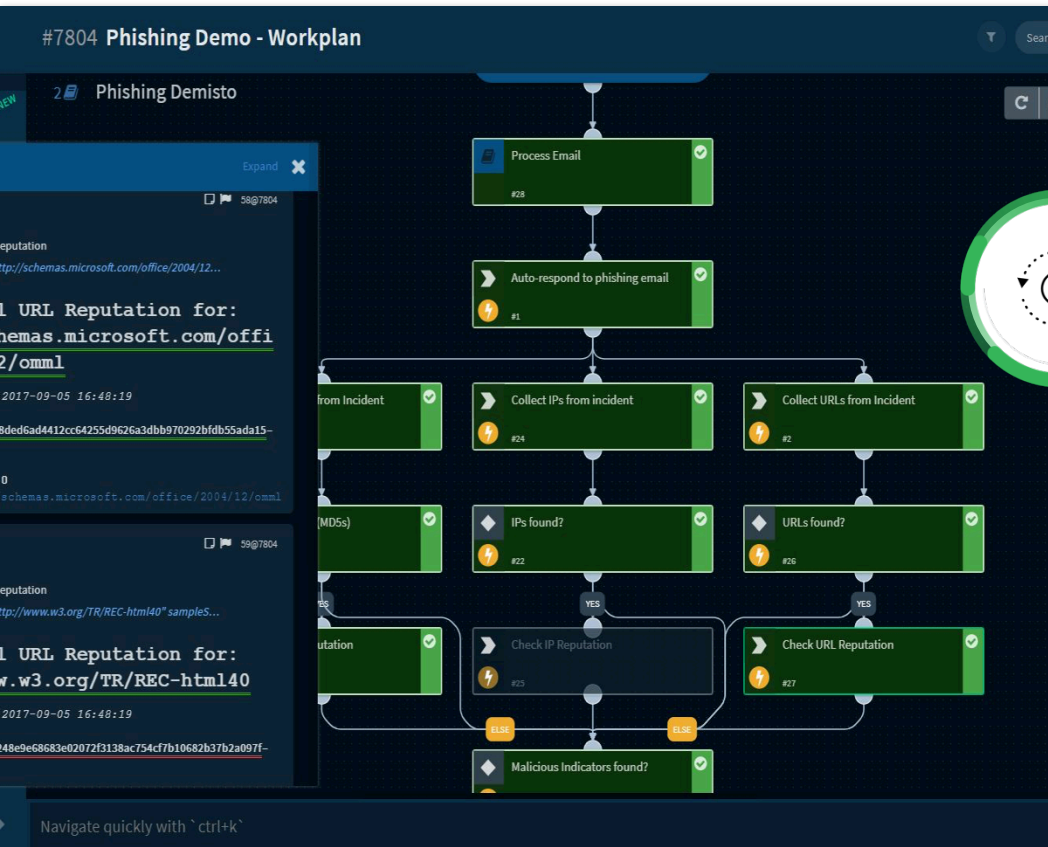
Ingest, search and query ALL security incidents



Collaborate and respond

Collaborate with team members to resolve incidents





Cortex XSOAR is a workflow automation engine

Respond to incidents with speed and scale

- **100s** of product integrations
- **1000s** of security actions
- Intuitive, **visual playbook editor**

#16958 "Event from Splunk for host " - War Room

No filter selected

abhishekiyer 8:12 AM
@rishi help me with this ip analysis

DBot 8:12 AM
rishi was added to the investigation.

abhishekiyer 8:12 AM
IADGetUser name="Jeni Russo"

DBot 8:12 AM
Command: IADGetUser names="Jeni Russo"   
Active Directory User

dn	CN=Jeni Russo,CN=Users,DC=demisto,DC=int
displayName	Jeni Russo
name	Jeni Russo
memberOf	
UserAccountControl	512
manager	CN=Janay James,CN=Users,DC=demisto,DC=int
ACCOUNTDISABLE	false
provider	activedir
mail	Jeni.Russo@demisto.int
samAccountName	DEM602894

abhishekiyer 8:13 AM

Navigate to Incident Summary view by using alt+1

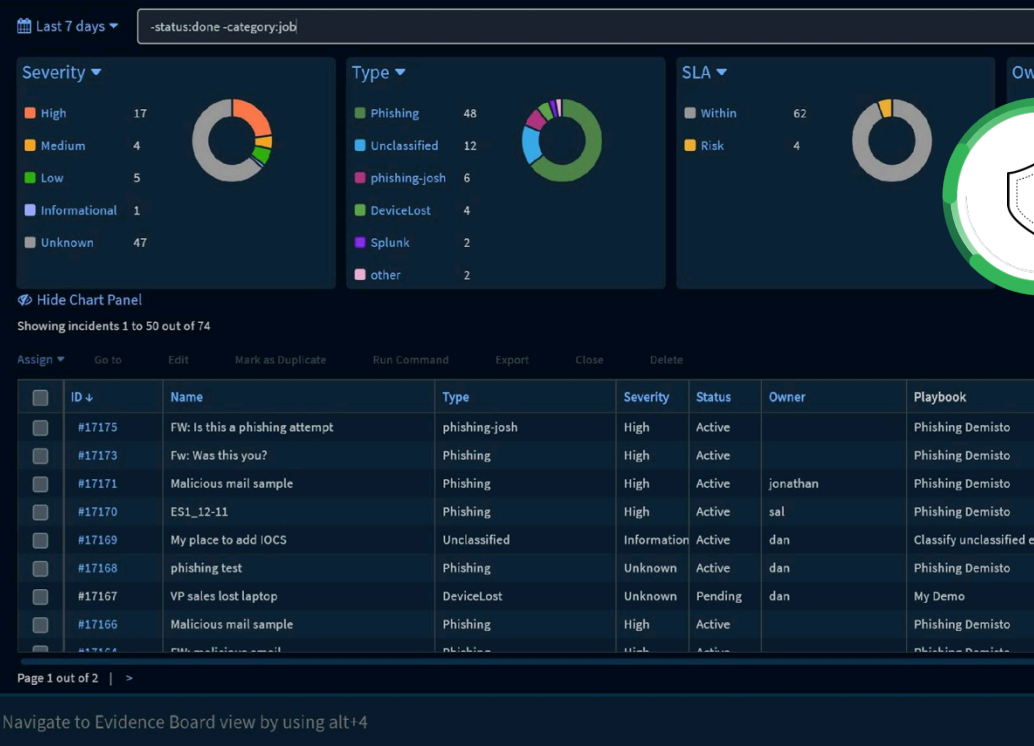


Cortex XSOAR is a collaboration platform

Improve investigation quality by working together

- **Virtual War Room** for every incident
- **ChatOps & real-time** security actions
- **Auto-documentation** of playbook & analyst actions

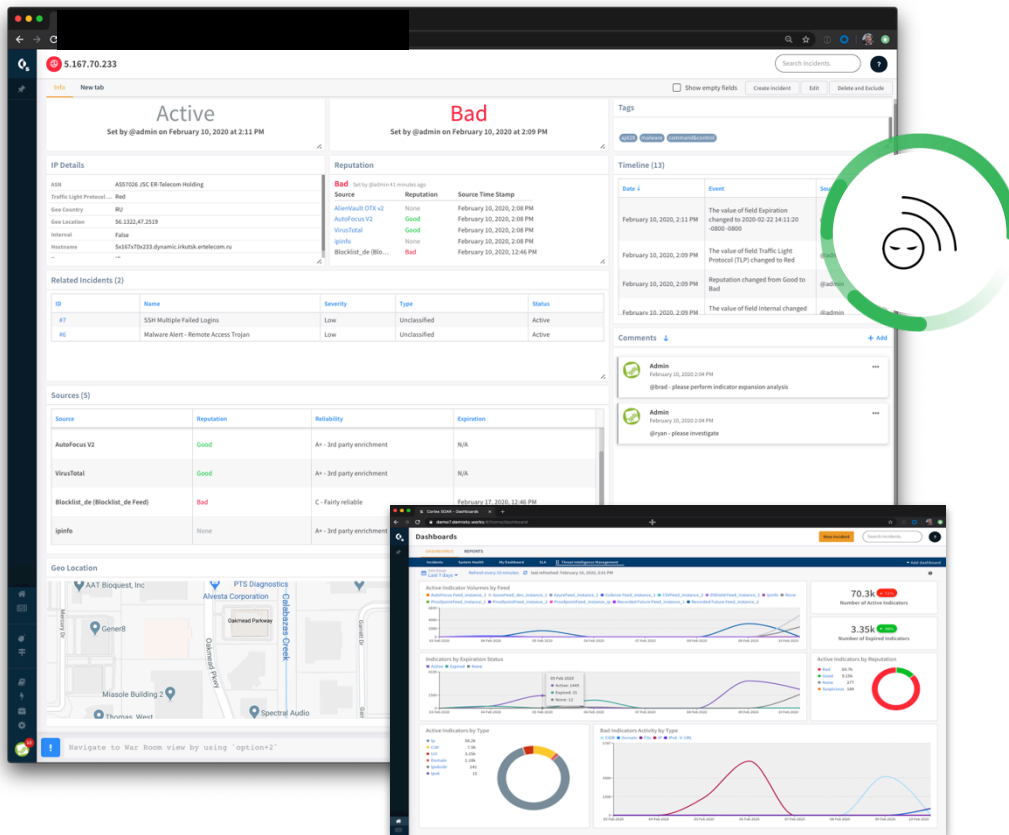
Incidents



Cortex XSOAR is a security ticketing system

Standardize process across products, teams and use cases

- Ingest, search, and query **ALL** security alerts
- **Custom views** by incident type
- Customizable **dashboards & reporting**

















































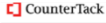

























Cortex XSOAR is a threat intel management platform

Take full control of your threat intel feeds

- Customizable **threat intel dashboards**
- **Entire indicator** lifecycle visibility
- **Instant ROI** from existing threat intel feeds

Breadth of Cortex XSOAR integrations

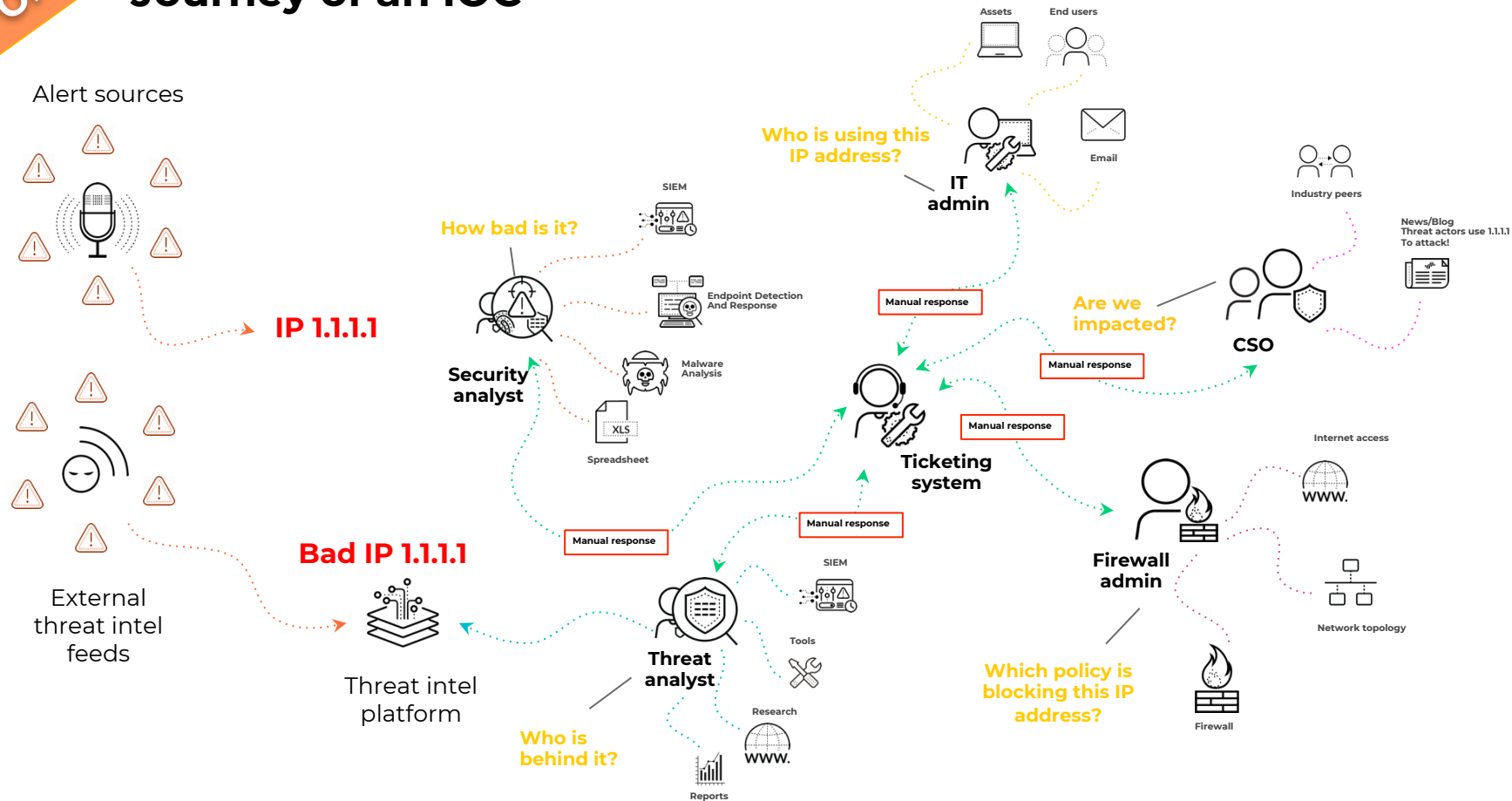
Analytics and SIEM           	Network Security        
Threat Intelligence          	Authentication    
Malware Analysis         	Email Gateway    
Endpoint         	Ticketing      
	Messaging     
	Cloud      

<https://www.demisto.com/integrations/>

Cortex XSOAR - threat intelligence management

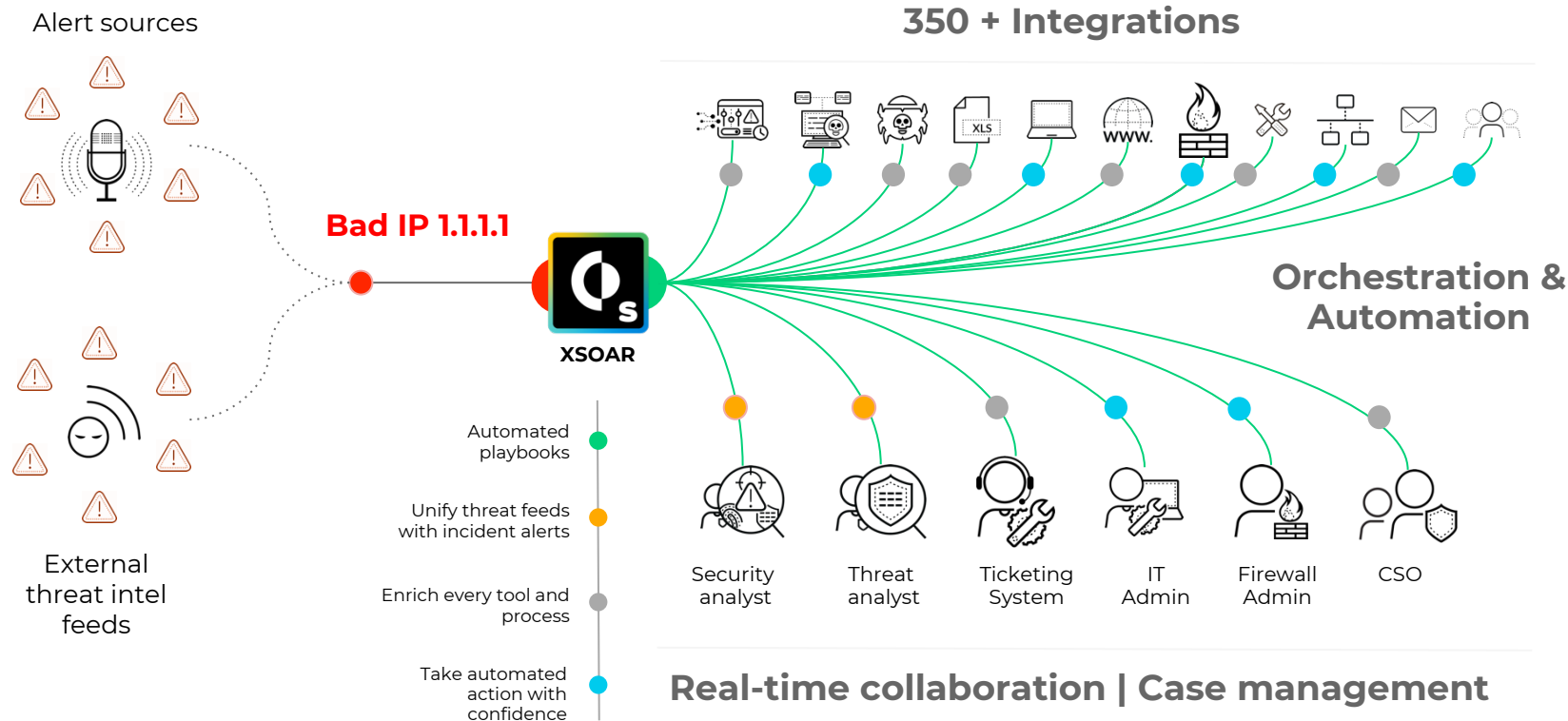
BEFORE

Journey of an IOC



AFTER

Journey of an IOC with Cortex XSOAR



Cortex XSOAR - Demo

Q&A

Best Practices for a Remote SOC

- Increased Communication
 - Video conference
 - Daily check-in
- 30/30/30 SOC Analyst Operating Model
 - ~30% Alerts
 - ~30% Hunting
 - ~30% Continuous improvement
- Metrics Reporting
 - Time to Detect, Assign & Remediate (MTTR)
 - Daily check-in
- Enable Collaboration
 - Cortex XSOAR War Room, Case Notes
- Documentation
 - Good time to review for accuracy
 - Follow Cortex XSOAR playbooks in incident response
 - Ensure Incident Response Plan (IRP) is up to date with correct contact info for key contacts
 - This should occur regardless, but in moving from onsite to remote this is good to increase frequency

Additional Resources for Cortex XSOAR (formerly demisto)

- Free Product evaluation

<https://start.paloaltonetworks.com/sign-up-for-community-edition.html>

- eBook

<https://start.paloaltonetworks.com/your-guide-to-security-orchestration>

- Gartner Report

<https://start.paloaltonetworks.com/the-hitchhikers-guide-to-soar>

- 2019 SOAR Report

<https://start.paloaltonetworks.com/the-2019-state-of-soar-report.html>

Thank you

How to use this deck

This deck is a modular master deck for Cortex XSOAR customer meetings.

If you would like create your own personal copy to customize, use File -> “Make a copy”.

Deck outline: Cortex overview, Cortex XSOAR, Threat Intel Management,.

You can find additional product slides, Cortex XSOAR for MSSPs, customer case studies, use cases with Palo Alto Networks products, and SOAR industry education in the appendix.

Latest updates

Feb 20, 2020: Updated slides to new Palo Alto Networks template and updated Demisto to Cortex XSOAR in anticipation of Cortex XSOAR announcement on Feb 24, 2020.

Note: Cortex XSOAR will be released end of March 2020.



Cortex Secures The Future

Rewiring security operations

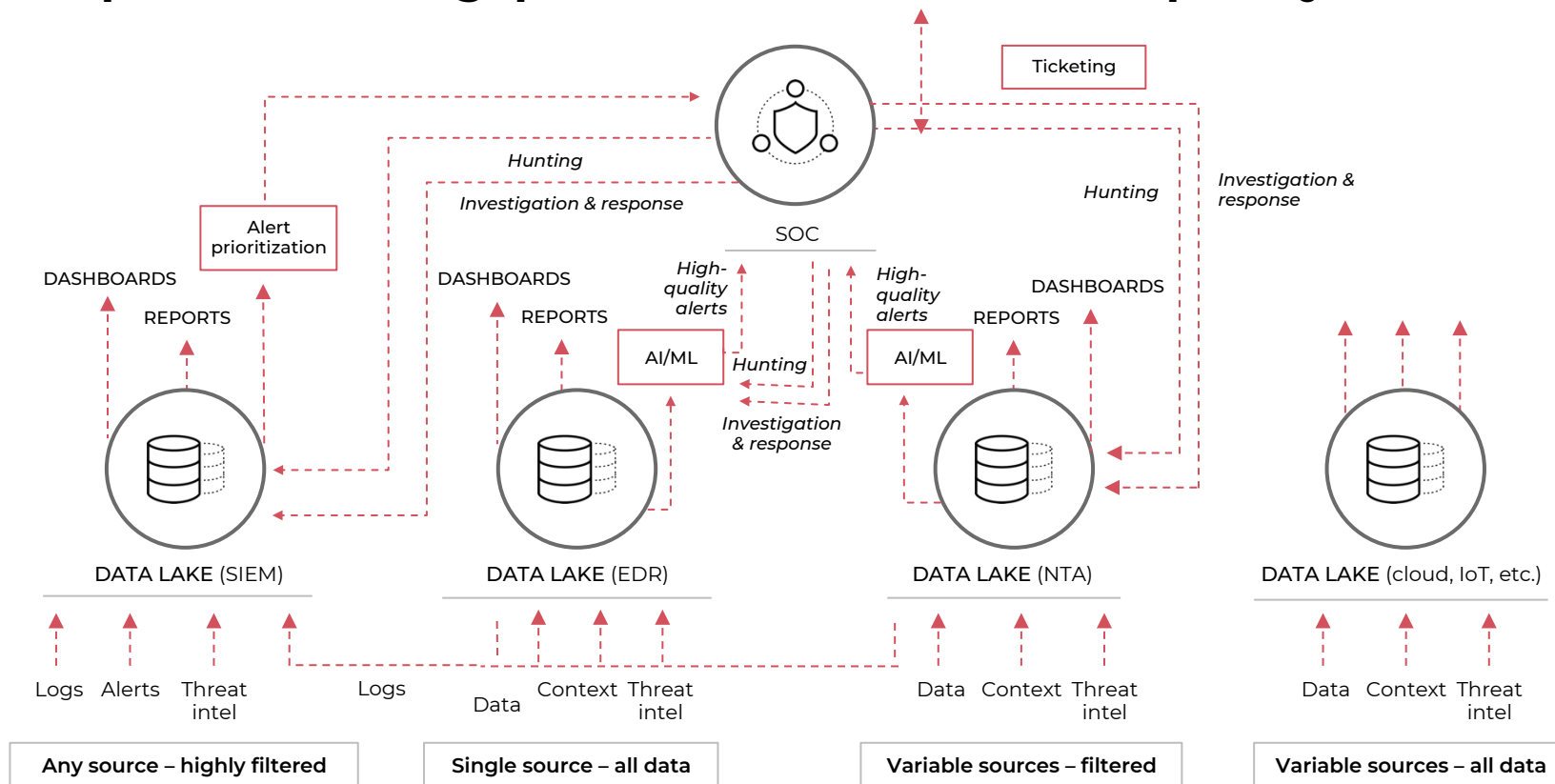


Version 1.0

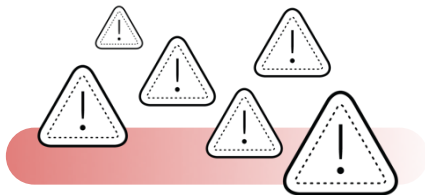
February 2020



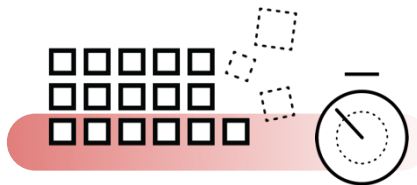
Attempts to address gaps result in even more complexity



Why do security teams struggle?



**Too much noise
(a.k.a alert fatigue)**



**Too many products
to piece together an
incident**



**Too many
manual, repetitive
actions**

Rewiring SecOps with Cortex



**Prevent
everything
you can**

 **CORTEX XDR**



**Everything you can't
prevent, detect and
investigate fast**

 **CORTEX XDR**



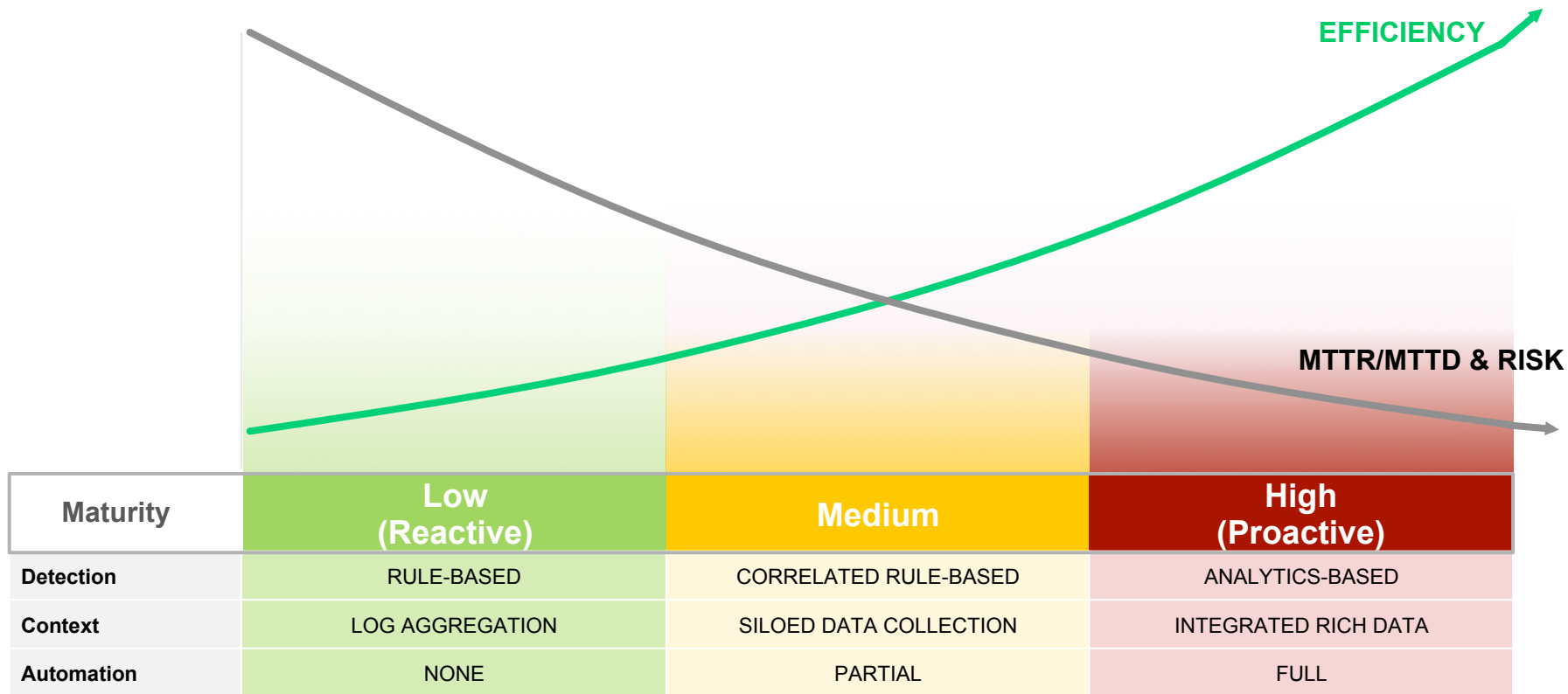
**Automate response
and get smarter with
each incident**

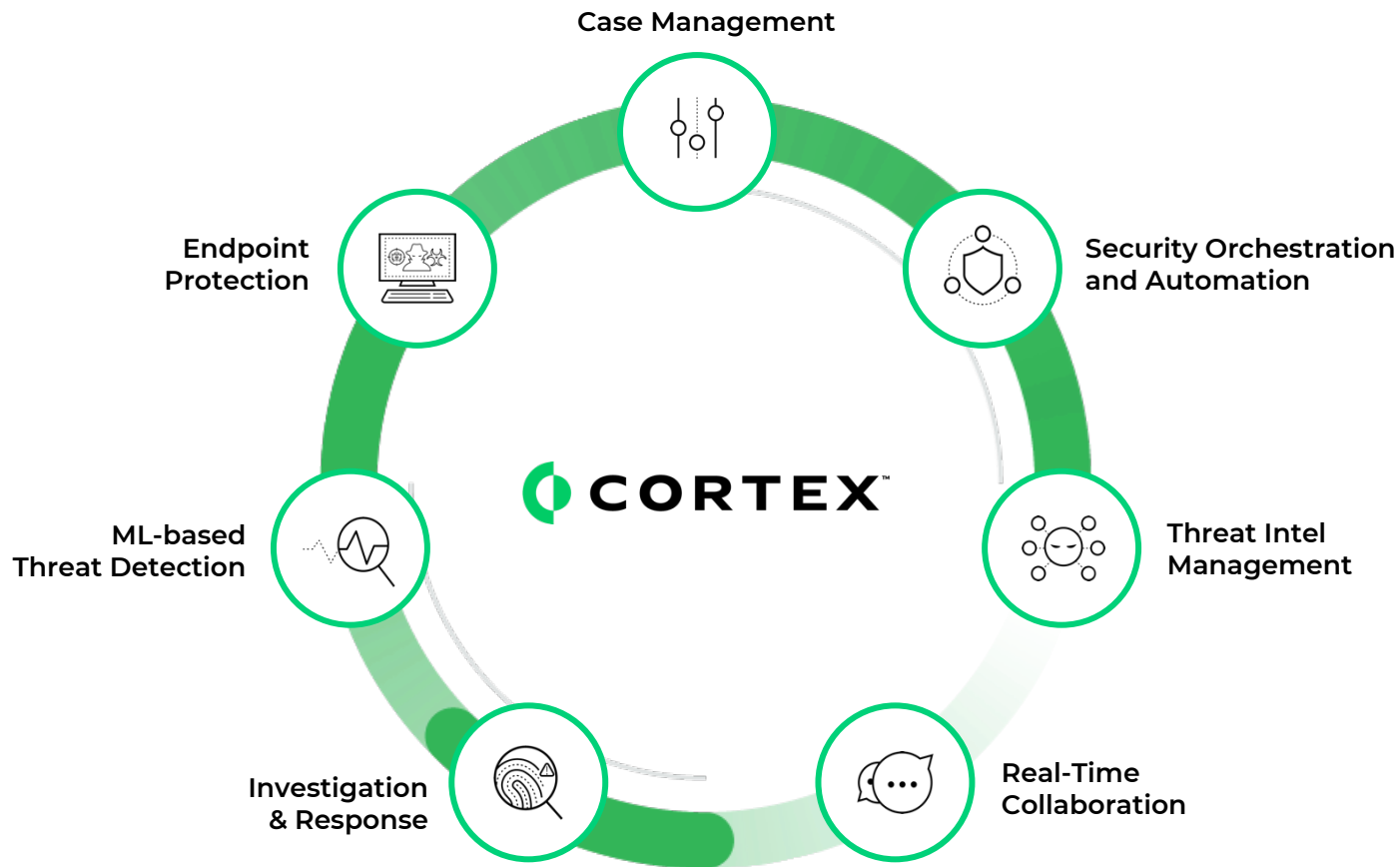
 **CORTEX XSOAR**
BY PALO ALTO NETWORKS

Our unique approach with Cortex



How SecOps must transform to reduce risk





What is SOAR?

Security **O**rchestration, **A**utomation, and **R**esponse

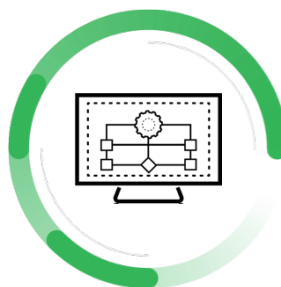


Orchestration

Playbooks, runbooks, workflows

Logically organized plan
of action

Controlling, activating security
product stack from central
location



Automation

Automated scripts

Extensible product
integrations

Machine execution of
playbook tasks

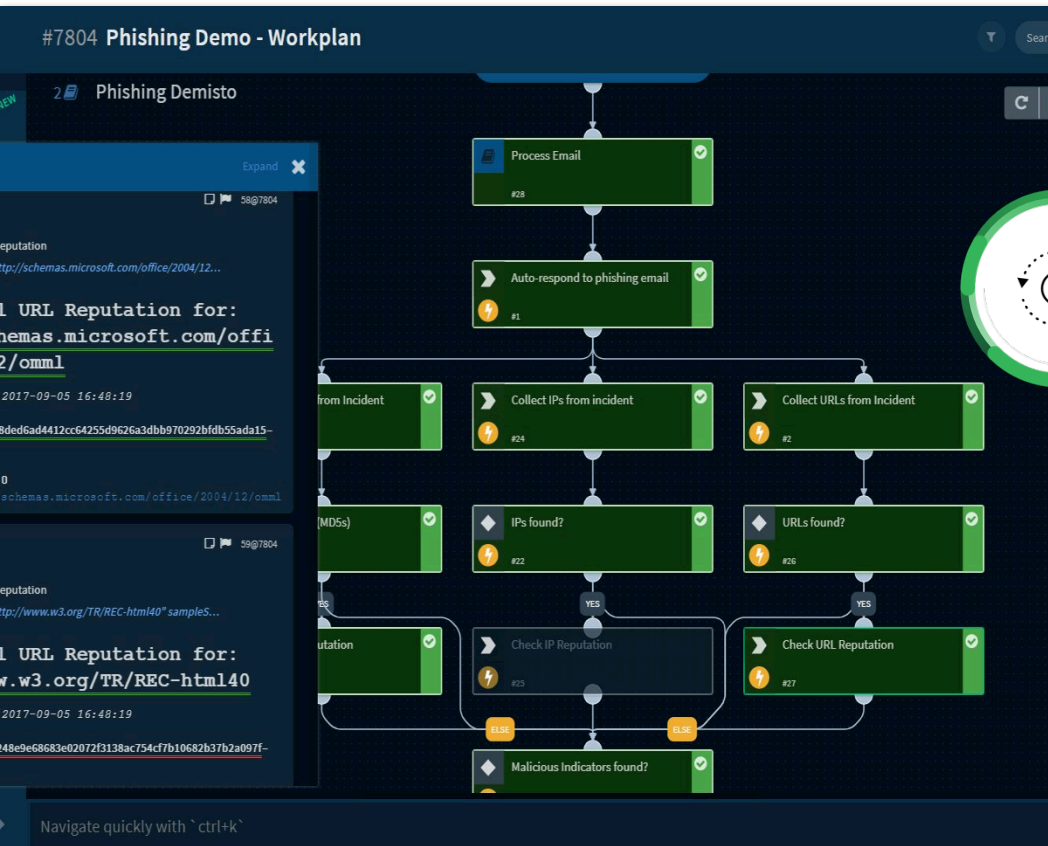


Response

Case management

Analysis
and reporting

Communication
and collaboration



Cortex XSOAR is a workflow automation engine

Respond to incidents with speed and scale

- **100s** of product integrations
- **1000s** of security actions
- Intuitive, **visual playbook editor**

#16958 "Event from Splunk for host " - War Room

No filter selected

abhishekiyer 8:12 AM
@rishi help me with this ip analysis

DBot 8:12 AM
rishi was added to the investigation.

abhishekiyer 8:12 AM
IADGetUser name="Jeni Russo"

DBot 8:12 AM
Command: IADGetUser names="Jeni Russo"   
Active Directory User

dn	CN=Jeni Russo,CN=Users,DC=demisto,DC=int
displayName	Jeni Russo
name	Jeni Russo
memberOf	
UserAccountControl	512
manager	CN=Janay James,CN=Users,DC=demisto,DC=int
ACCOUNTDISABLE	false
provider	activedir
mail	Jeni.Russo@demisto.int
samAccountName	DEM602894

abhishekiyer 8:13 AM

Navigate to Incident Summary view by using alt+1

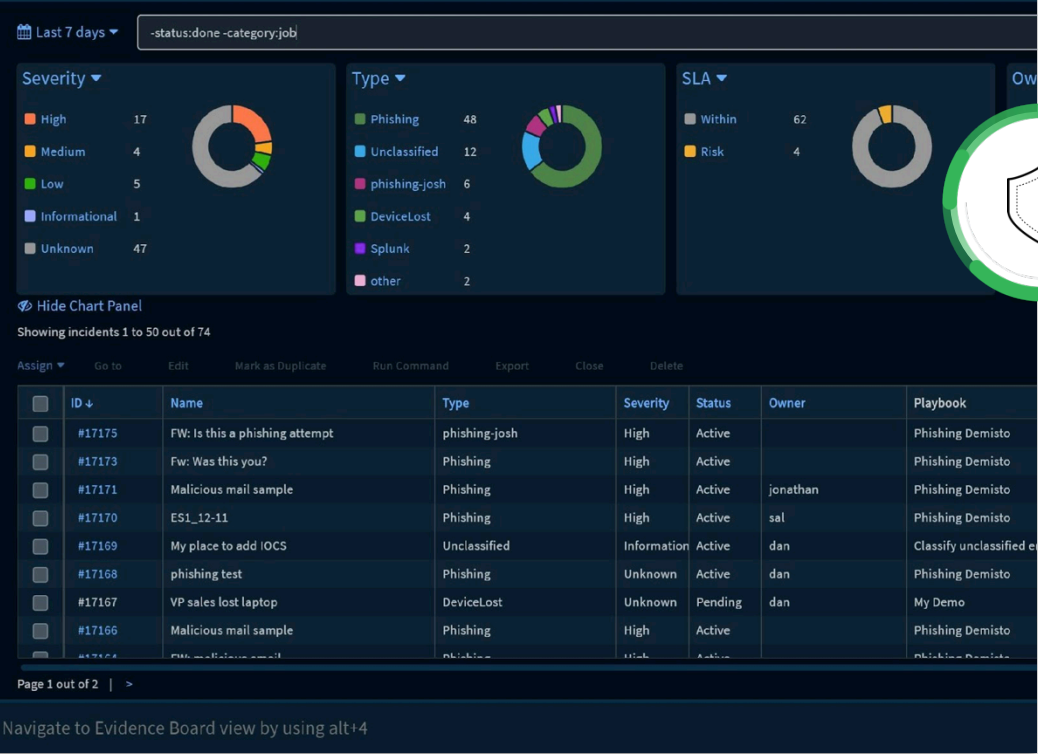


Cortex XSOAR is a collaboration platform

Improve investigation quality by working together

- **Virtual War Room** for every incident
- **ChatOps & real-time** security actions
- **Auto-documentation** of playbook & analyst actions

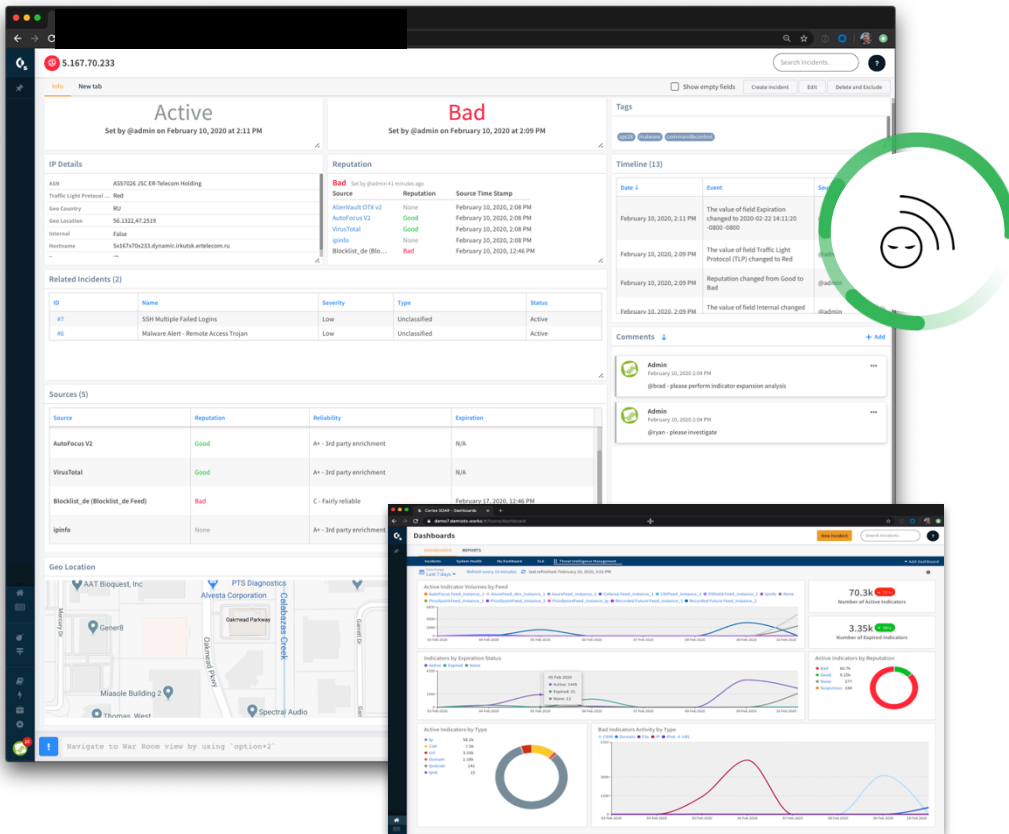
Incidents



Cortex XSOAR is a security ticketing system

Standardize process across products, teams and use cases

- Ingest, search, and query **ALL** security alerts
- **Custom views** by incident type
- Customizable **dashboards & reporting**



Cortex XSOAR is a threat intel management platform

Take full control of your threat intel feeds

- Customizable **threat intel dashboards**
- **Entire indicator** lifecycle visibility
- **Instant ROI** from existing threat intel feeds

Breadth of Cortex XSOAR use-cases



Use Case: Phishing Response

The Problem: Phishing response is hard



High Alert Volumes

Phishing attacks are frequent, easy to execute, and act as the entry vector for most security attacks



Disjointed Processes

Security teams must coordinate across email inboxes, threat intel, NGFW, ticketing, and other tools for phishing response



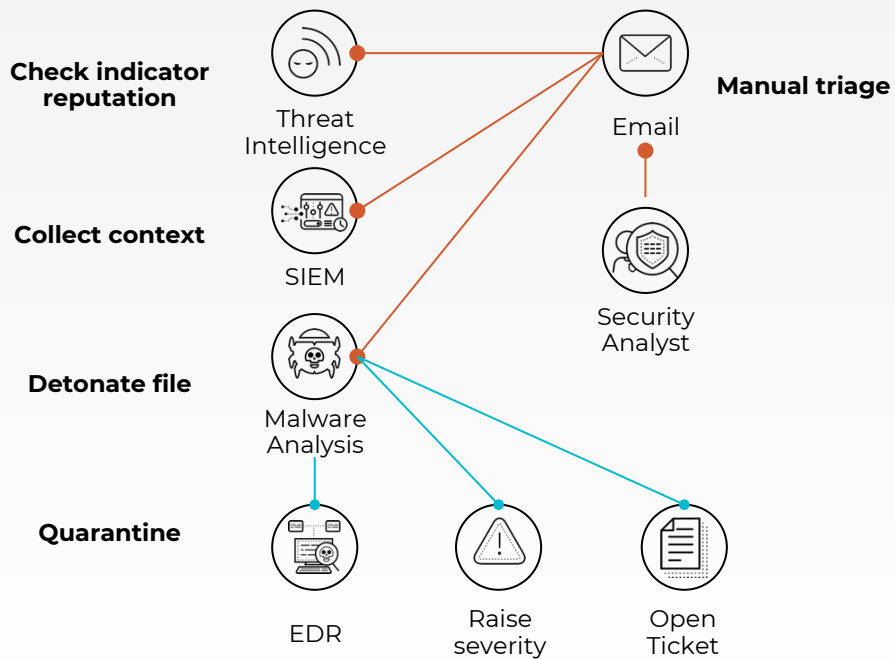
Ever-Present and Growing

95% of all attacks on enterprise networks are a result of spear phishing¹

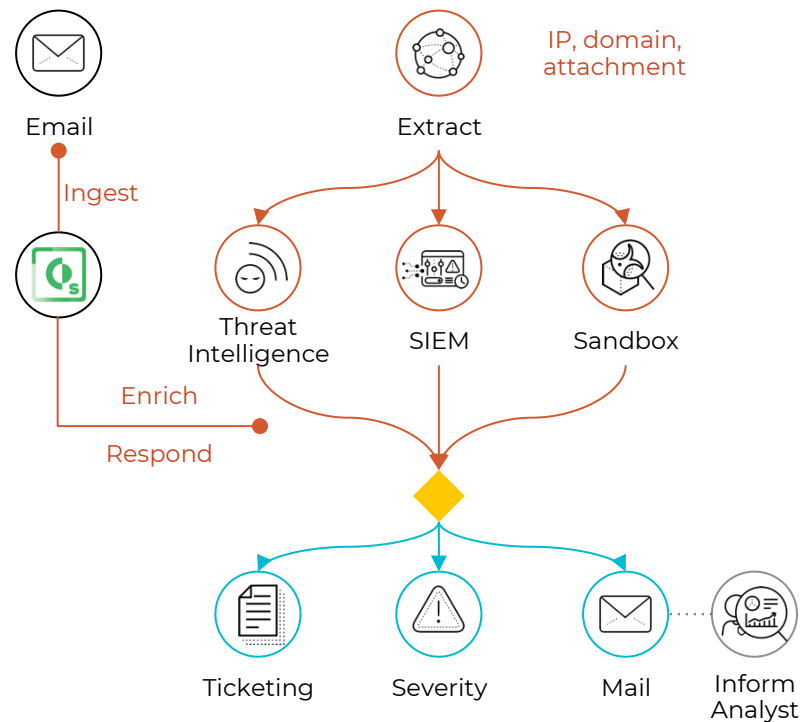
¹Source: <https://www.networkworld.com/article/2164139/network-security/how-to-blunt-spear-phishing-attacks.html>

Our Approach: Phishing response

Before



After



Key Differentiators: Automate and standardize phishing response



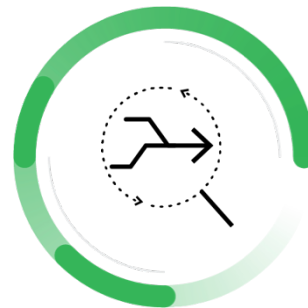
Product Integrations

Cortex XSOAR integrates with all security tools commonly used for phishing enrichment and response



Intuitive Response Playbooks

OOTB and custom task-based workflows enable security teams to coordinate across teams, products, and infrastructures



Automated Actions

1000s of automated actions across security tools make scalable phishing response a reality

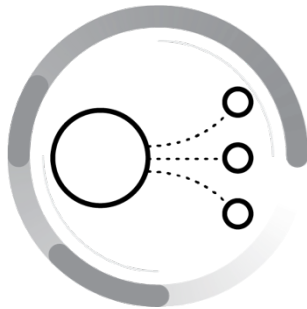
Use Case: IT & Security Processes Automation

The Problem: Processes are disjointed



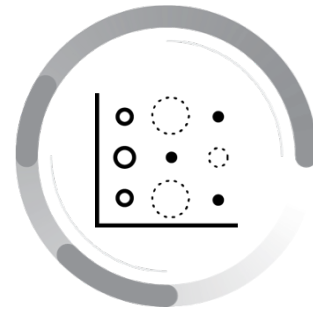
Team Silos

Managing and responding to security incidents involves end users, IT team, NOC team, and other stakeholders



Shifting Context

Coordinating across security tools involves shifting context, leading to rework and fragmented documentation

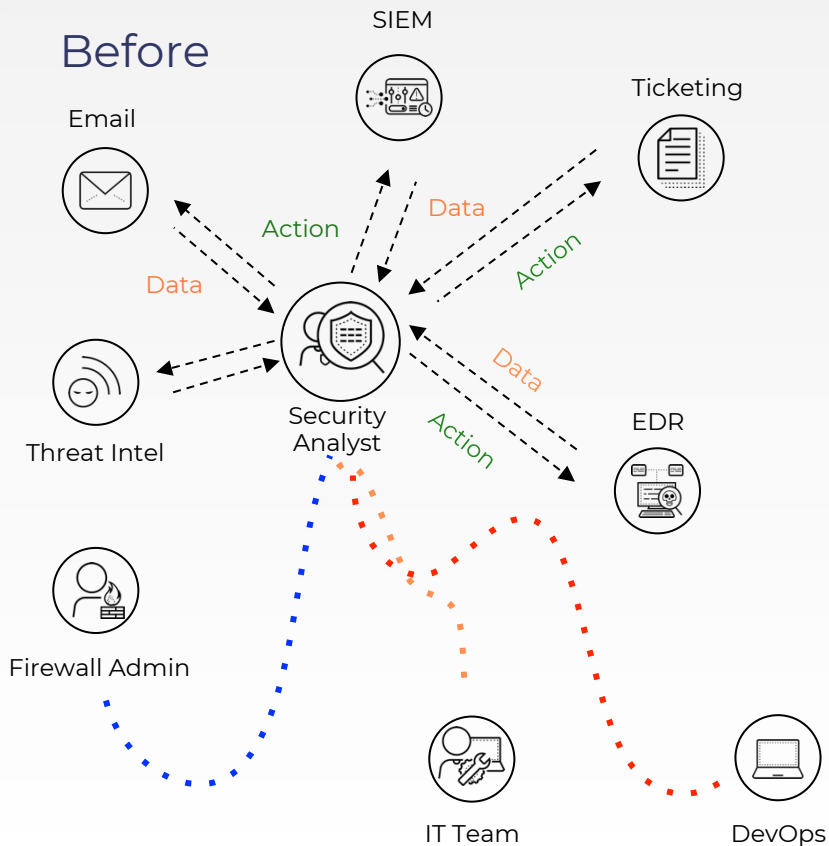


Lack of Metrics

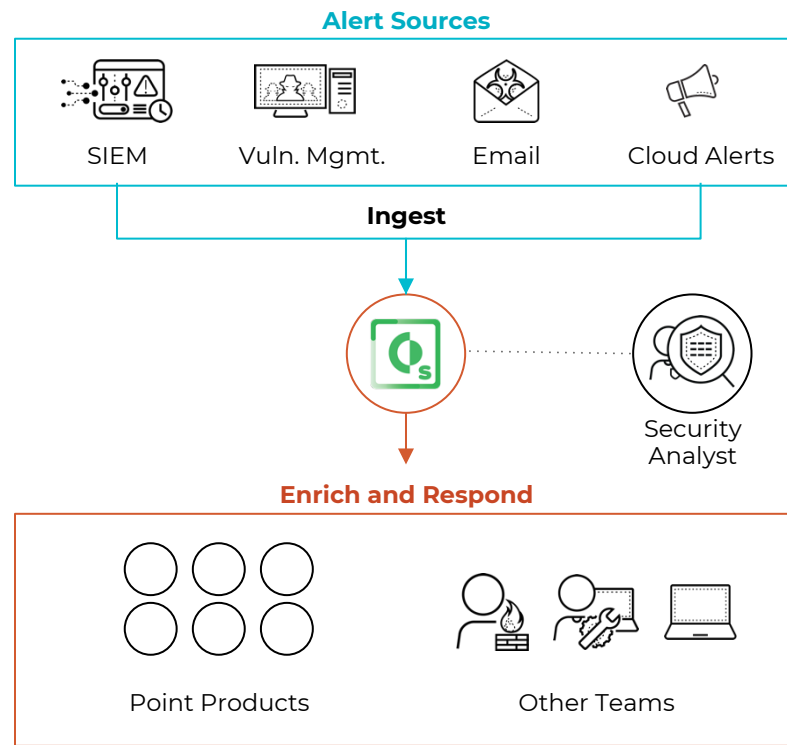
Security teams lack the time, flexibility, and centralized data to visualize relevant metrics and track performance

Our Approach: Security processes

Before



After



Key Differentiators: Centralized incident management with security context



Cross-team Communication

Communicate with end users, security teammates, and other teams, both in real-time and through automated tasks



Security Focused Context

Ingest all security alerts for centralized view and context across the incident response lifecycle



Granular Dashboards

View cross-sections of incident, indicator, and analyst data with custom, widget-driven dashboards and reports



“

Cortex XSOAR's process modularity and automation has helped us stay agile as we onboard new technologies. Cortex SOAR is really the constant 'sheet music' that keeps our security orchestra going.

”

Sean Hastings, Senior Information Security Analyst

“
Launched in 2015, [Cortex XSOAR] rapidly became one of the most visible security orchestration, automation and response (SOAR) vendors, outshining vendors launched years earlier. An early focus on user interface (and not just the APIs), its inclusion of machine learning, usable Slack integration, and sizable stable of out-of-the box integration with tools and online services makes it a popular SOAR tool.
”

Anton Chuvakin, Ex-Research VP, Gartner

Cortex SOAR successfully maps with all of Gartner's recommended capabilities for SOAR vendors.

View Full PDF



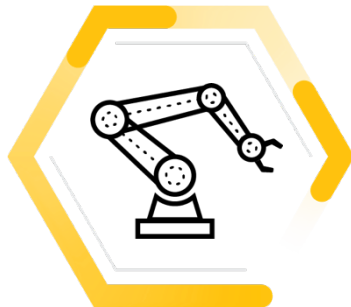
"Cool Vendor" in Security Operations and Vulnerability Management, 2018

Cortex XSOAR value



**Standardize and
scale processes**

Reduced weekly
alerts from
10,000 to 500



**Lower response times
with automation**

Reduced response
times from
3 days to 25 minutes



**Coordinate actions
across security products**

Automated 30% of
incidents for
1 FTE time saved

*Real stats from Cortex XSOAR customers

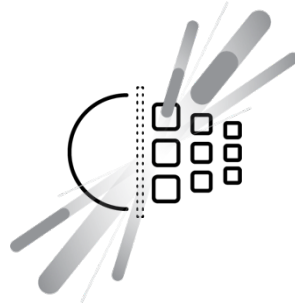
Cortex XSOAR - threat intelligence management

Why analysts struggle with Threat Intelligence Platforms



Lack of control

Threat feeds force analysts to manually tune and score IoCs to match their environment



Siloed workflows

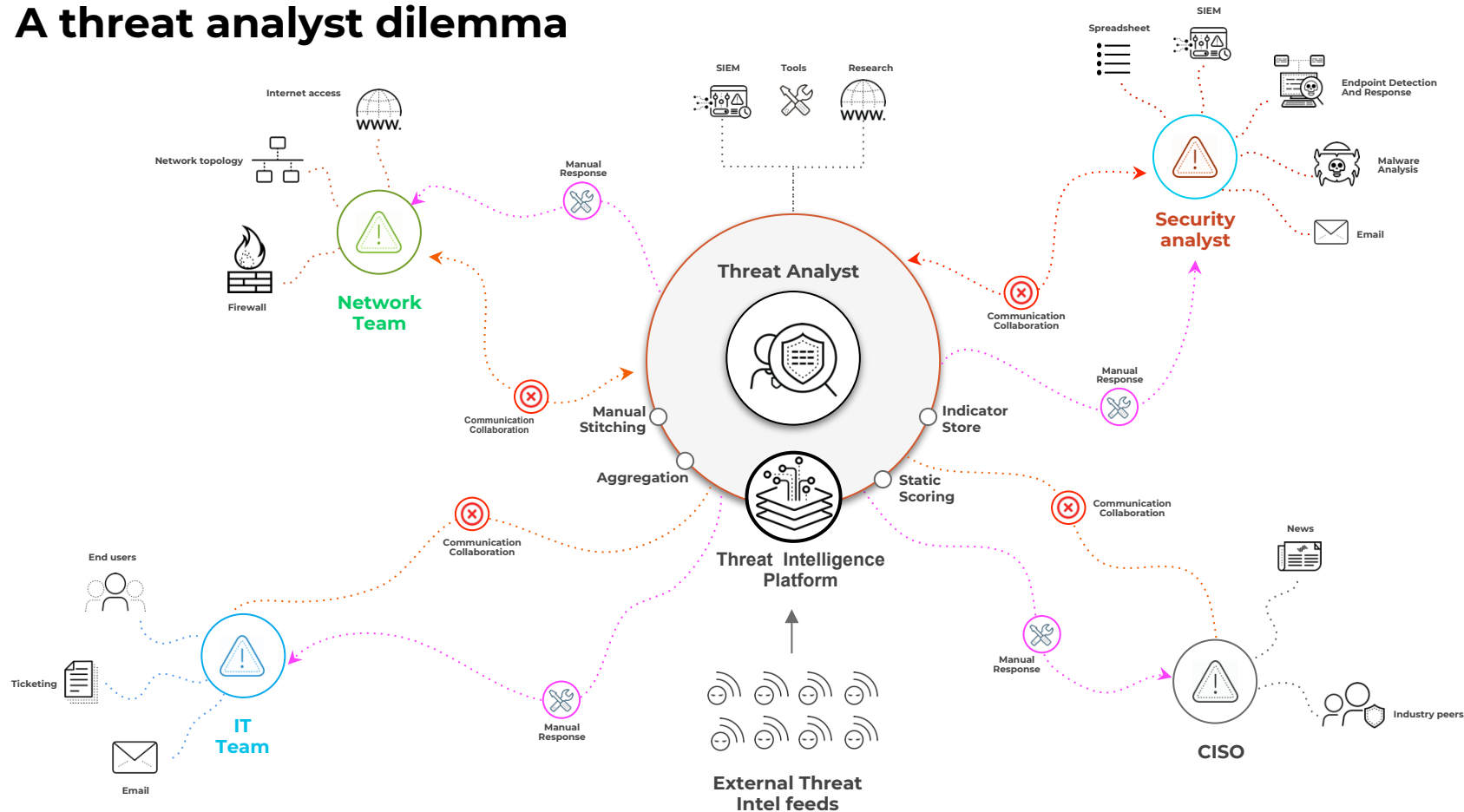
Incidents and threat intel are broken across tools, people and processes



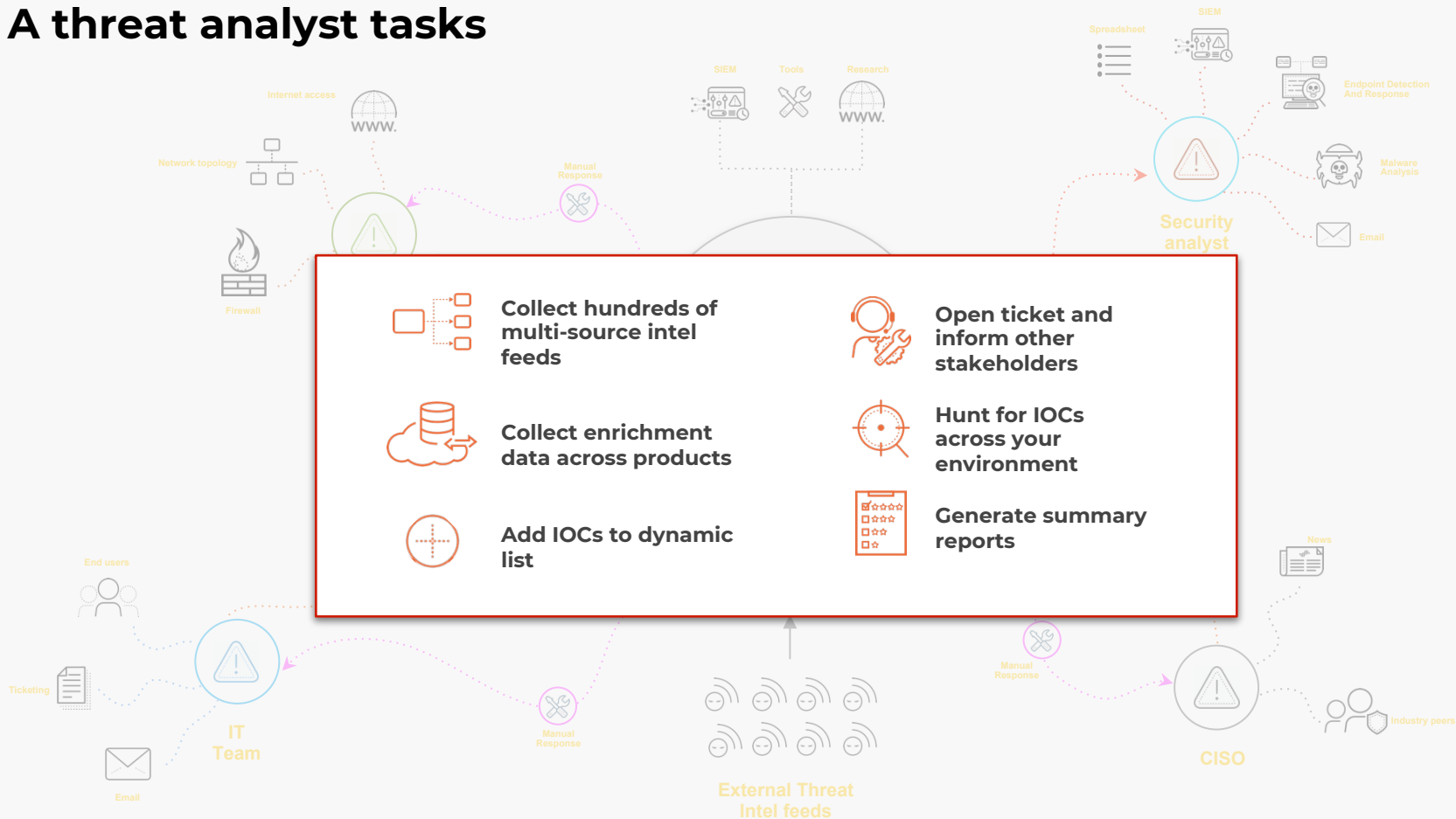
Hard to operationalize

Putting threat intel into action is highly manual and repetitive

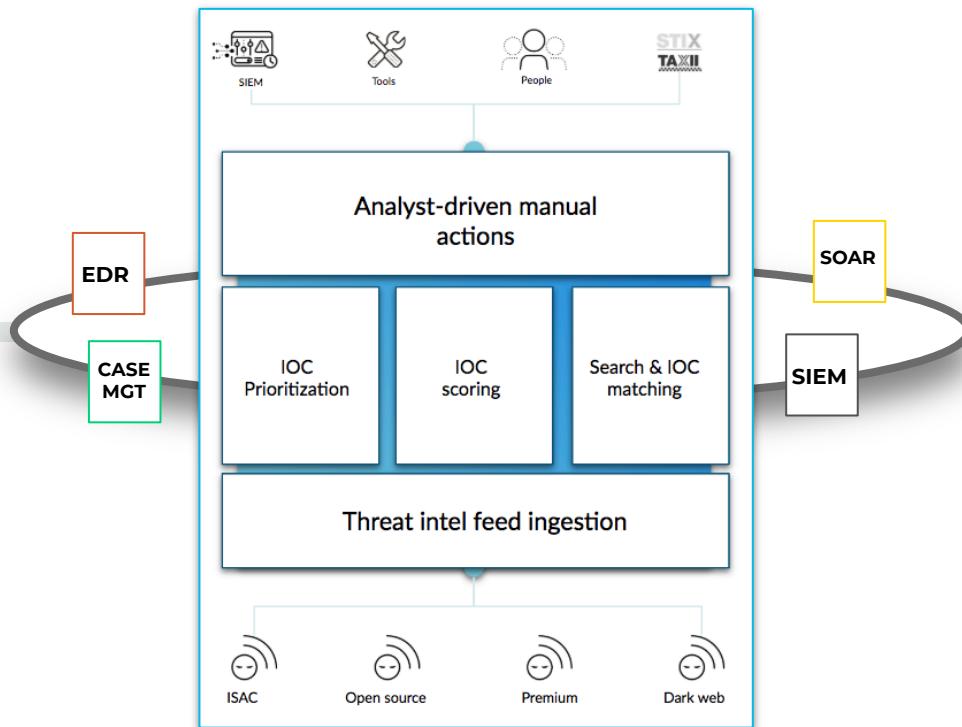
A threat analyst dilemma



A threat analyst tasks



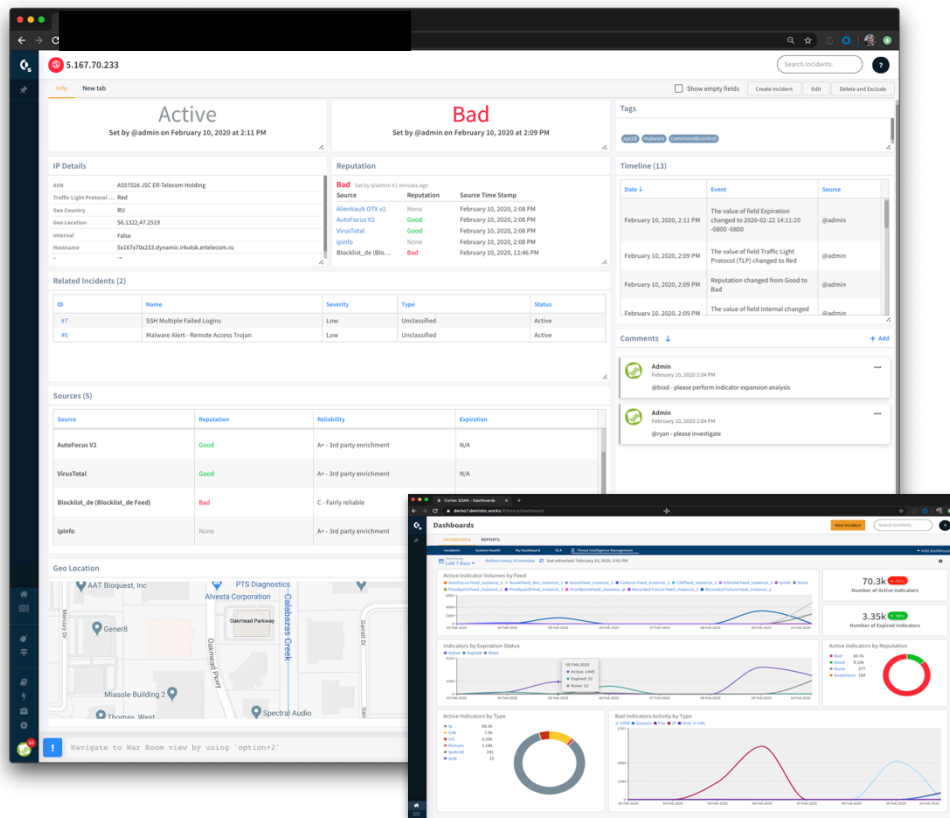
Existing Threat Intelligence Platform are siloed



Cortex XSOAR Threat Intel Management Module



Take full control of your threat intel feeds



Aggregate, parse, de-duplicate and manage indicators at scale

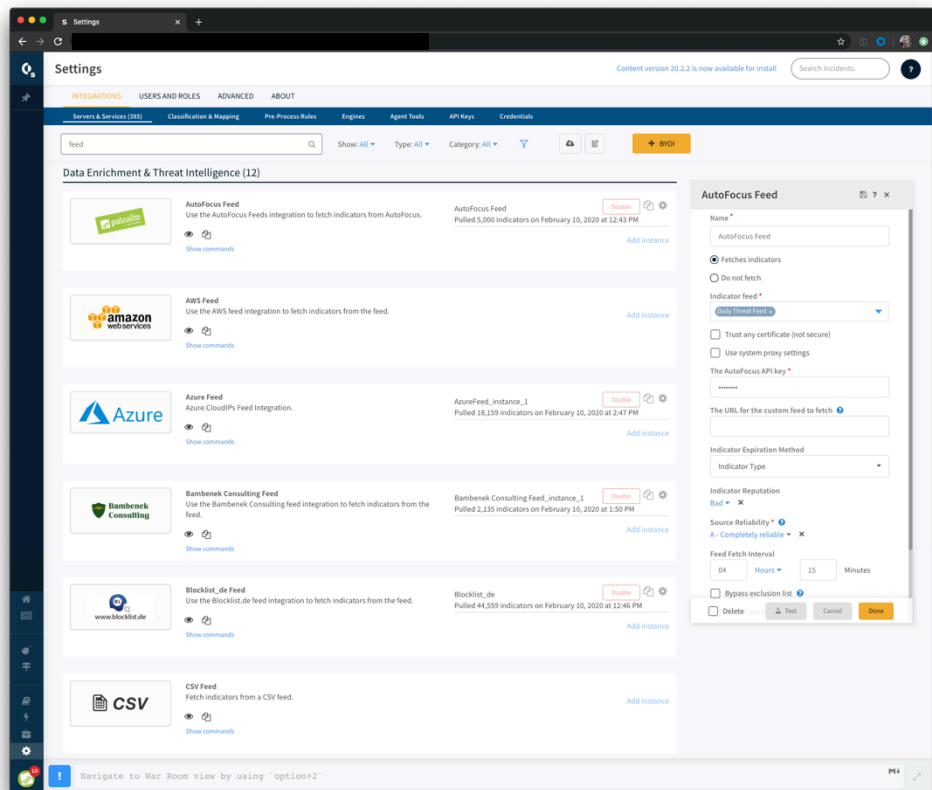


Take charge of your threat data with playbook-based IOC scoring



Get instant ROI on your existing threat feeds

Make smarter decisions by enriching and prioritizing indicators



Reveal critical threats by layering third-party threat intel with internal incidents

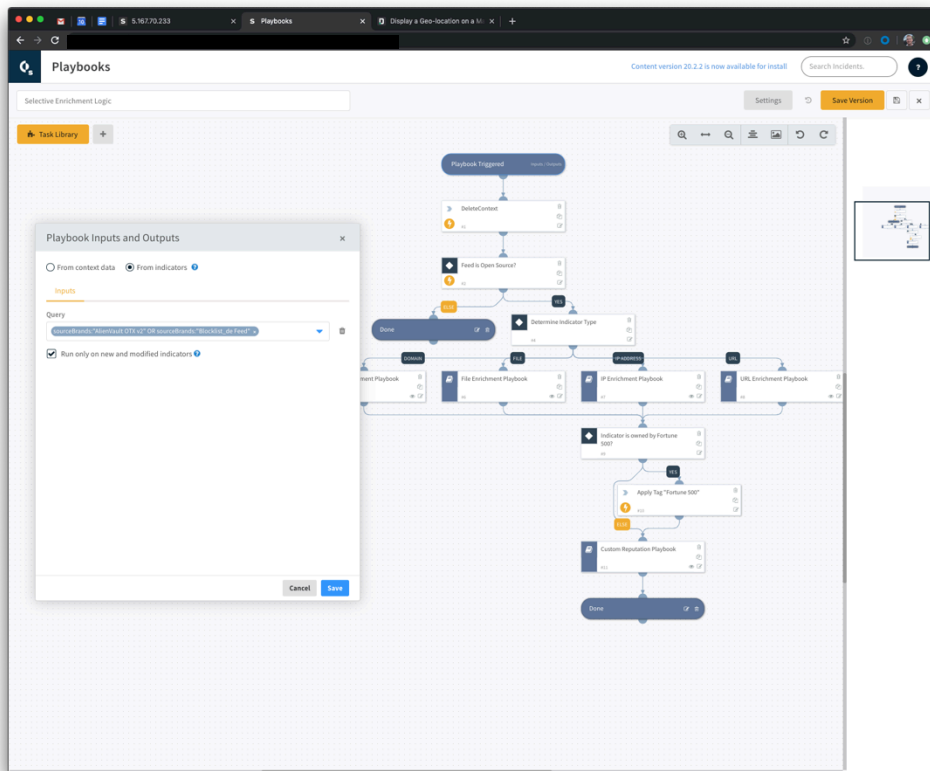


Supercharge investigations with built-in threat intelligence from AutoFocus



Enrich any detection, monitoring, or response tool

Close the loop between intel and action with automation



Take actions to shutdown threats with playbook-driven automation

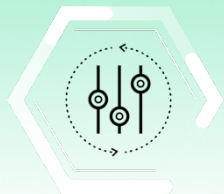


Expand the scope of your investigations by sharing threat intel



Extend the value of your SOAR platform with native threat intel management

Cortex XSOAR native Threat Intel Management use cases



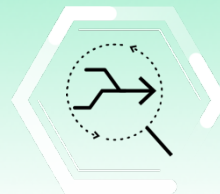
Indicator
Prioritization



Whitelist
Administration



Incident Enrichment



Automated
Threat Hunting



AutoFocus
Integration

Cortex XSOAR native Threat Intel Management key takeaways



Take full control of your
threat intel data



Unify external threat intel
data with internal
incident alerts



Make smarter decisions
with enrichment and
prioritization



Act fast and with
precision via automated
playbooks

Additional Slides

Cortex XSOAR - Licensing & pricing

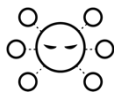
Cortex XSOAR + TIM	Cortex XSOAR Starter	Cortex TIM
Base Platform: \$250K/year Includes: XSOAR Starter + TIM + 4 full users	Base Platform: \$125K/year Includes 2 full users	Base Platform: \$125K/year Includes 2 full users <ul style="list-style-type: none">Includes AutoFocus threat intel feed with 5K/Day API query submissions
<ul style="list-style-type: none">Additional full user: \$20K/yearAudit user: \$6K/year (view only mode)Volume tiered full user modelHosting is 10% of the list priceCustomer support: Standard included, Premium 20% of list price per year <p>NOTE: These prices reflect ONLY North America pricing.</p>		

Threat Intelligence Platforms are an incomplete puzzle

What is possible



Static IOC
scoring



External intel
aggregation



Manual
enforcement

What is missing?



User-driven
automation



Real-world
context



Scalable
enforcement

Why it matters



Gain confidence



Smarter incident
response



Act with machine
speed

Intelligent automation: #NoCodePromise



Visual playbooks to discover automations and connect tasks



Human readable and machine context output



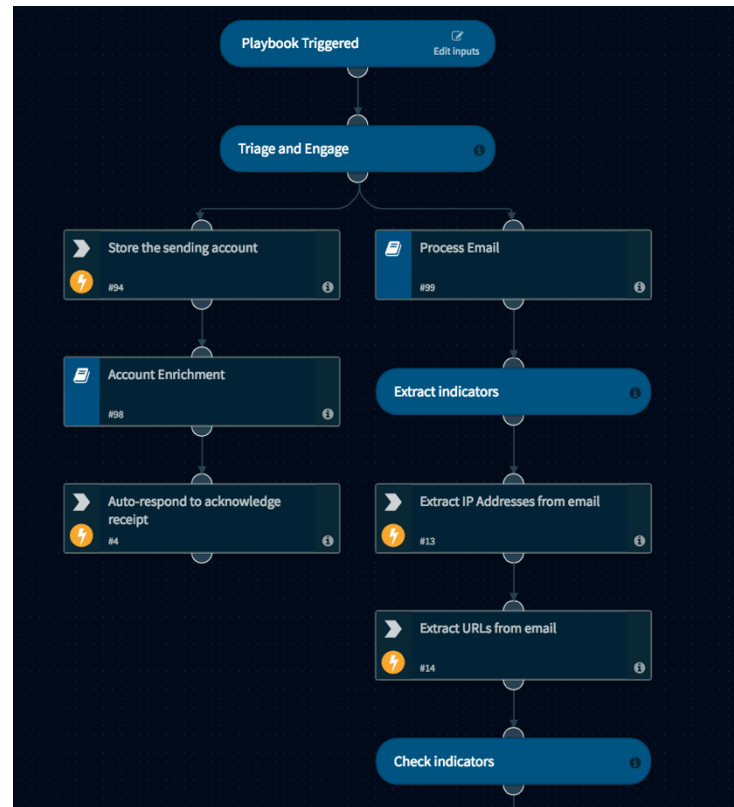
Review live playbook runs with outputs and errors



Avoid scripting for parsing, filtering, loops, and arrays



UI-based filters, transformers, and pre-process rules



Comprehensive incident management



Workflows, SLAs, incident assignment, and metrics



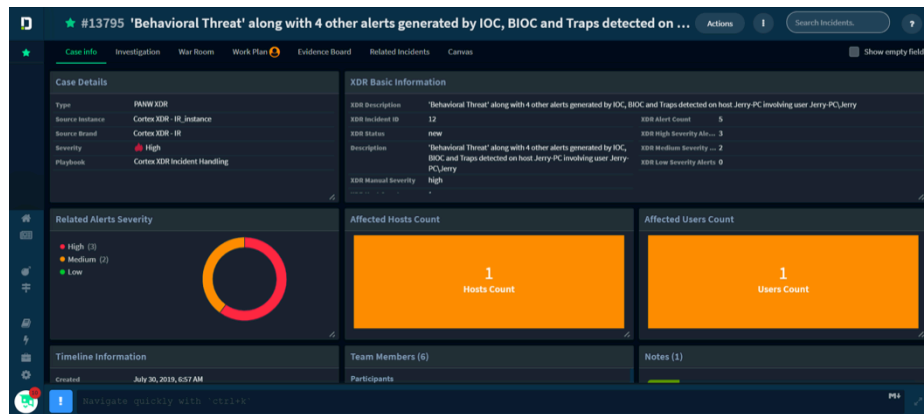
OOTB and custom incident types, fields, and summary layouts



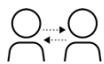
Mobile application support for incident management on-the-go



Granular dashboards and reports with user-driven widget library



Real-time interactive investigation



Collaborate with peers on joint investigations



Chat with DBot for executing and documenting deep investigation tasks



Analyze and investigate with historical information across incidents



Correlate and analyze indicators across incidents

The screenshot displays the Palo Alto Networks Cortex XDR interface. At the top, a header bar shows the indicator `ca8f71715c280b00969df13de3c11df7a1d07b1b` with a 'Delete and Whitelist' button. Below this, the 'Reputation' is set to 'Bad' and 'Known History' shows '34 Incidents'. A list of related incidents is provided, including '#7965 Phishing Demo 9_28', '#8116 Phishing Incident', '#8122 Phishing Example 03-10-2017', '#5652 Fw: Demo Phishing SC', and '#8191 SC1 10-05'. A section titled 'Select a script to execute:' lists 'FileReputation', 'SplunkSearch', and 'WildfireReport'. The main panel displays a table of metadata for the indicator:

Key	Value
city	Mountain View
country	US
hostname	google-public-dns-a.google.com
ip	8.8.8.8
lat	37.3846, -122.0840
org	AD15149 Google LLC
phone	650
postal	94035
region	California

Below the table, a map shows the location of Mountain View, California, with a red pin. The bottom of the interface includes a navigation bar with the text 'Navigate to Evidence Board view by using "alt+4"'.

Mobile app: incident management on the go



Agile incident management

- Personalized dashboards for data visibility
- Incident summaries for at-a-glance oversight



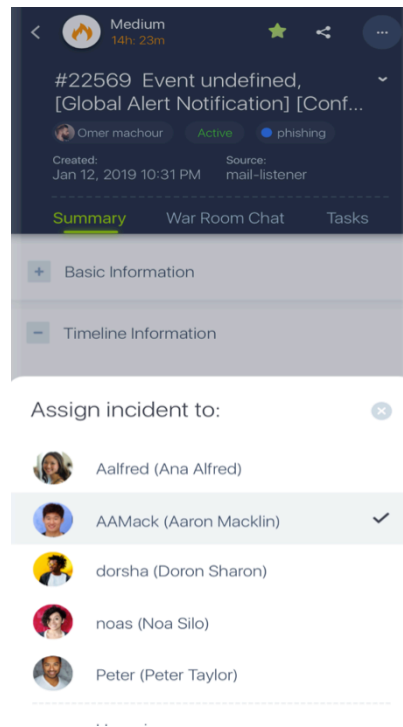
Keep response running

- Assign incidents, set severity
- View curated task lists, pending tasks

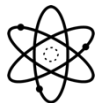


Connect with context

- Access relevant security information
- War Room with chat capabilities



Get smarter with each incident



DBot learns from historical actions



Suggest incident assignments



Identify experts for each type of incident

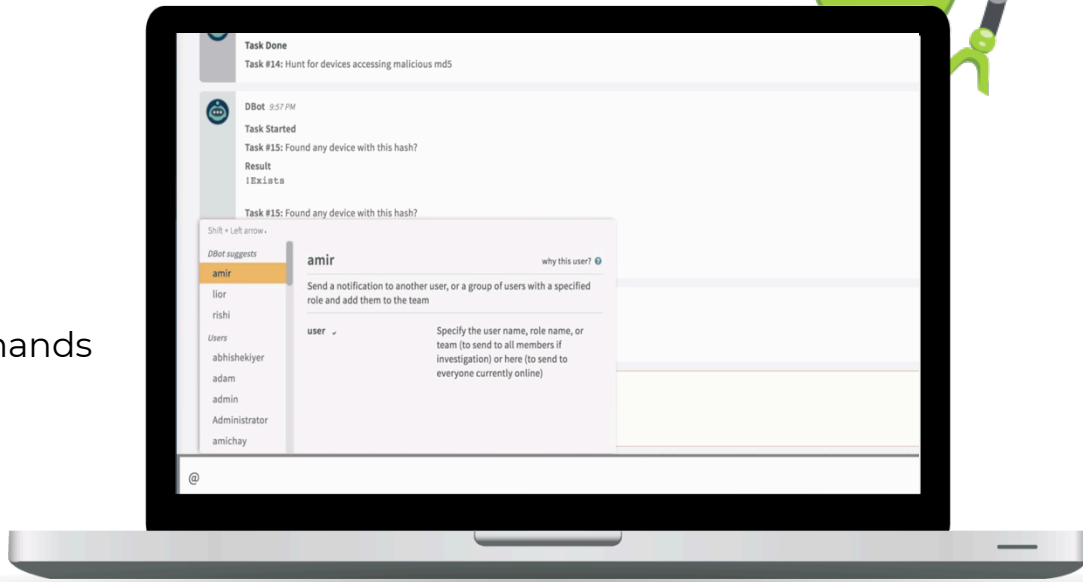


Suggest commonly used commands during investigation

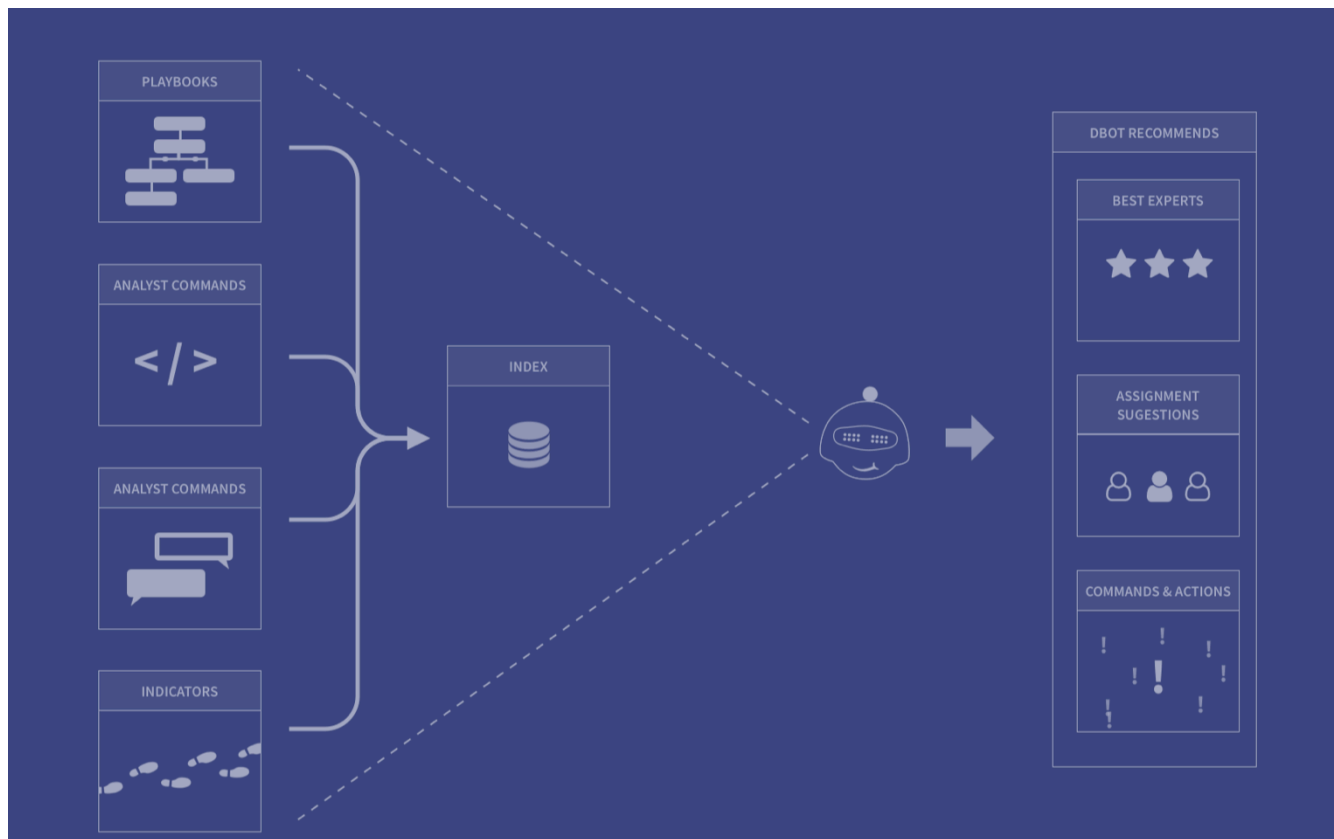


Identify related and duplicate incidents

DBot: Force multiplier
for your analysts



Cortex XSOAR machine learning



ML-Based phishing classifier



Cortex XSOAR phishing email classifier model helps teams categorize incoming emails as 'Valid', 'Scam', 'Spam', or 'Malicious'.

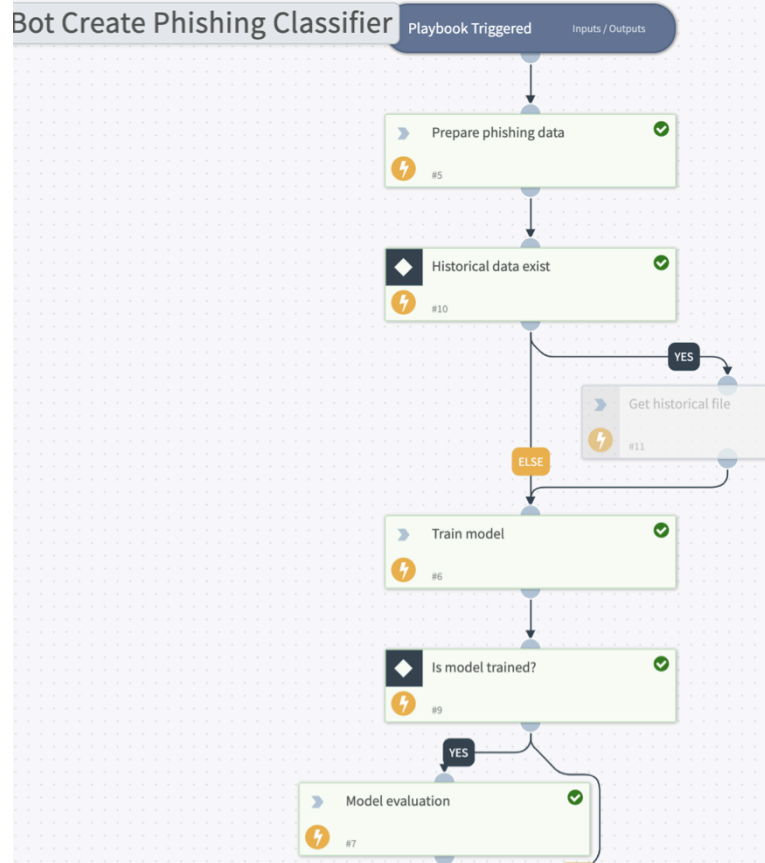


Collected labeled emails from existing customers and used text classification, explainability.

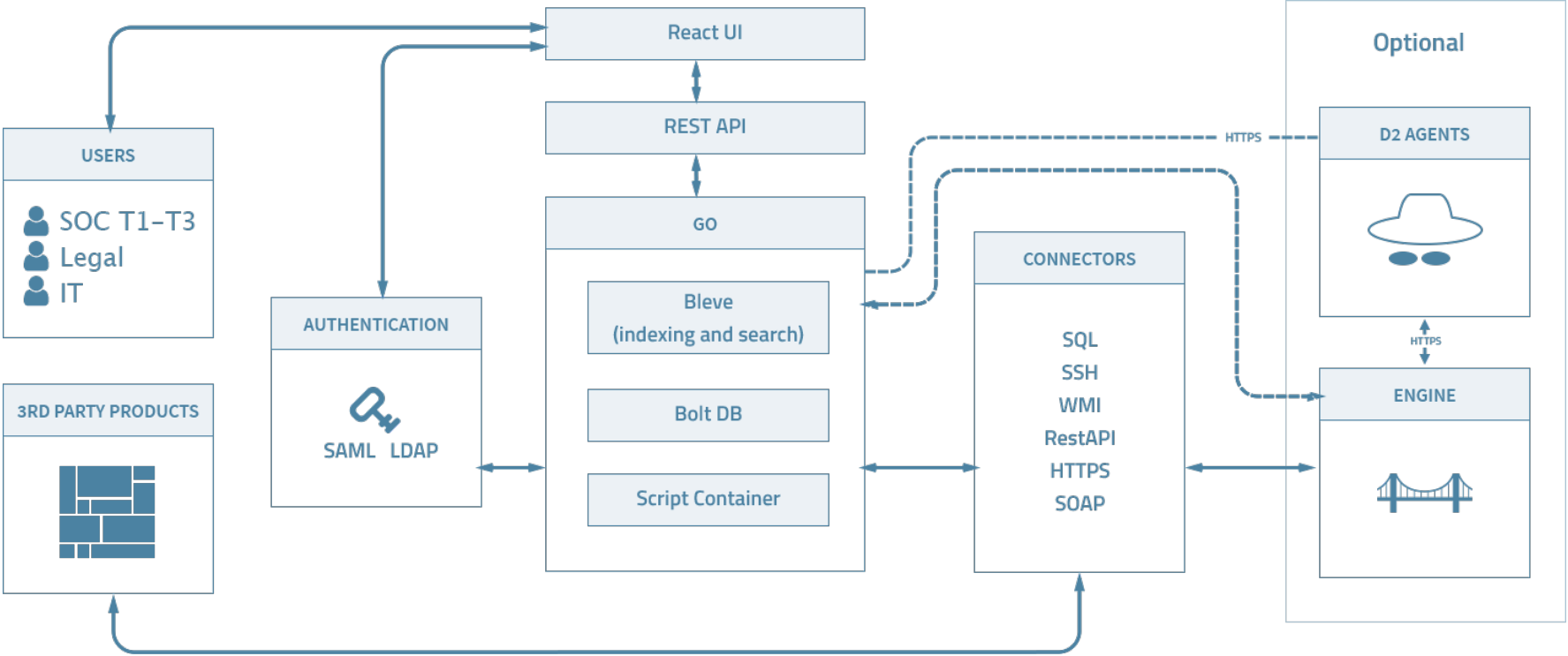


Model also available as a service through AWS SageMaker.

More info: <https://blog.demisto.com/building-a-phishing-email-classifier-in-demisto>



Cortex XSOAR architecture



How Cortex XSOAR deploys

Cortex XSOAR can be deployed both on-premise and as a cloud-hosted offering. The platform supports native multi-tenancy for MSSPs, providing three layers of isolation to maintain data integrity while simplifying communication across tenants.

Customer on-premise
server



Customer virtual or cloud

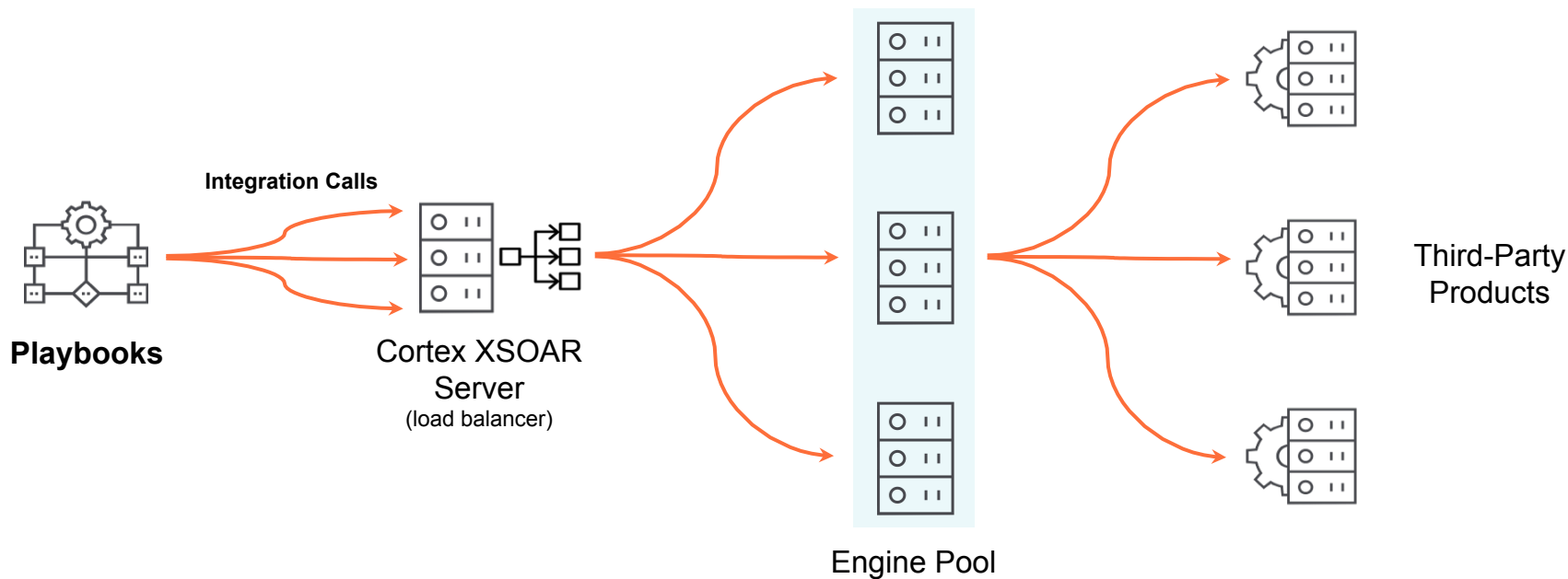


Hosted solution

aws



Engine load balancing



Rapid horizontal scalability

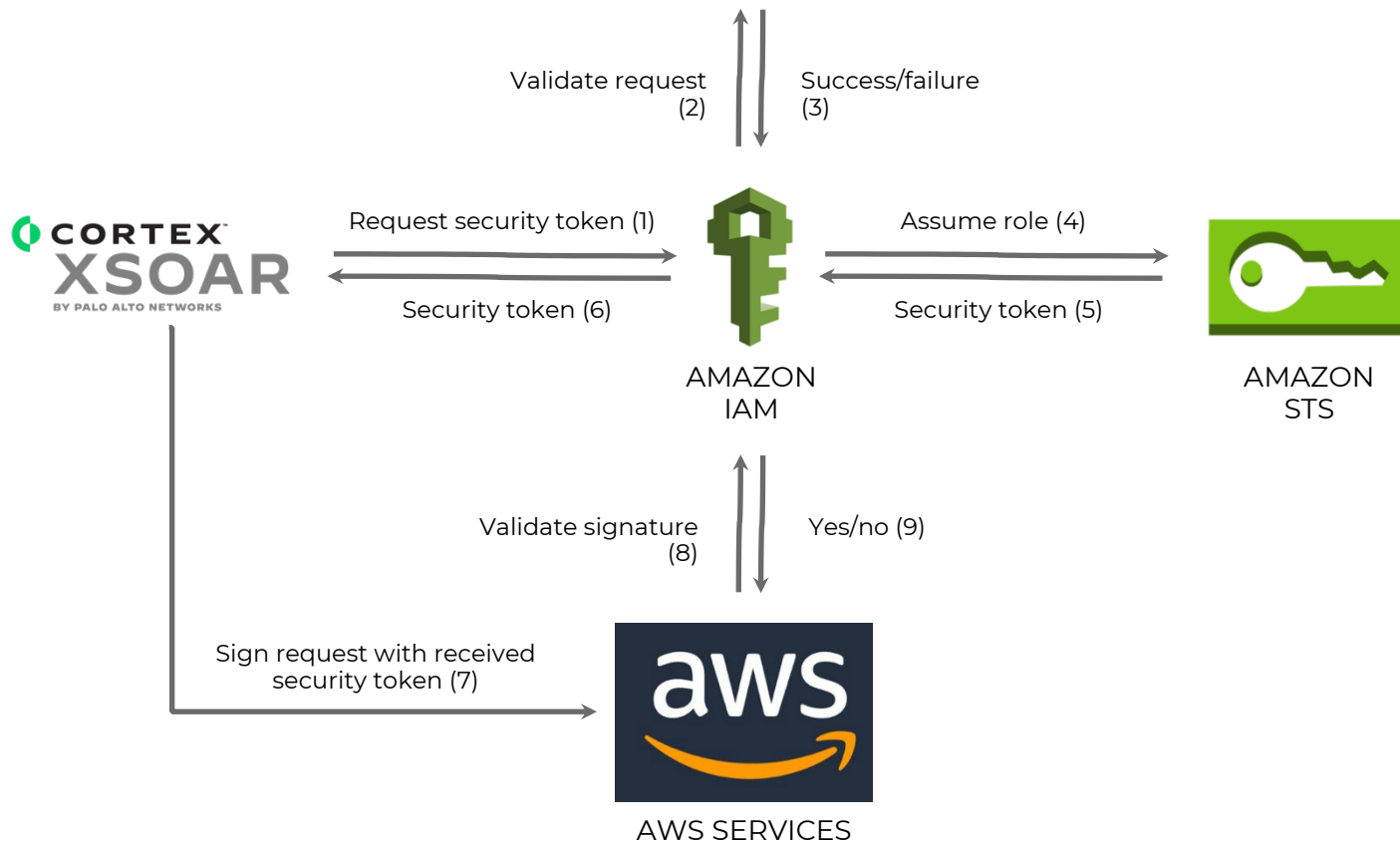


Increased redundancy



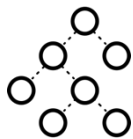
Improved performance

Keyless automation on the cloud



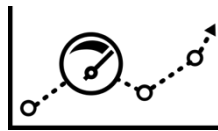
Cortex XSOAR for MSSPs

MSSP SOC challenges



Disparate Security Tools

Context switching across tools and tenants wastes time



Scaling Service Delivery and Customers

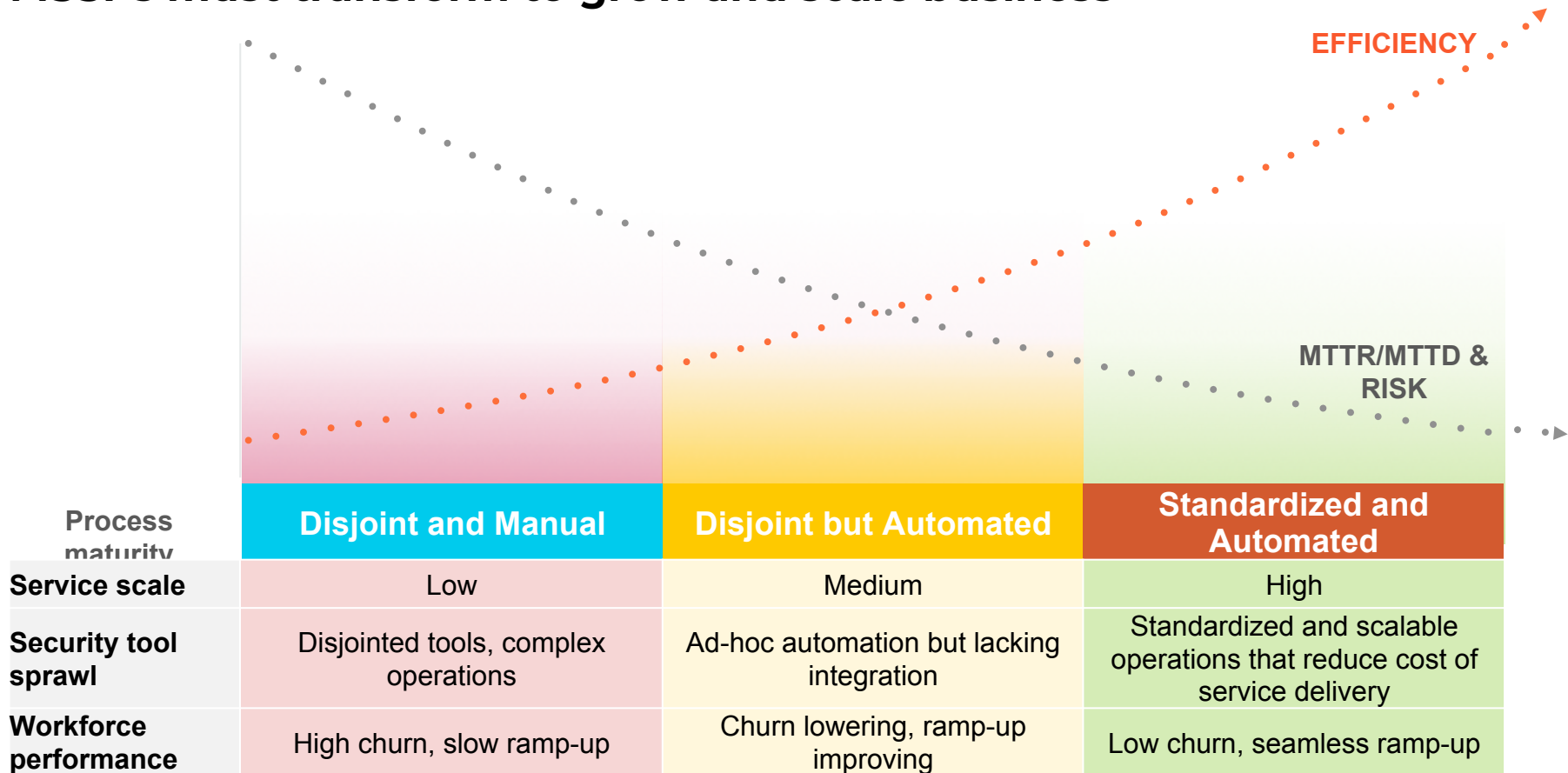
Adding analysts before adding customers is unsustainable



Analyst Onboarding and Churn

Repetitive, manual processes hinder productivity

MSSPs must transform to grow and scale business



Cortex XSOAR deployment for MSSPs

Cortex XSOAR can be deployed both on-premise and in the cloud (private and public). The platform is also primed with native multi-tenancy for MSSPs that scales horizontally, provides three layers of isolation, and maintains data integrity while simplifying communication across tenants.

MSSP on-premise server/
Private Cloud



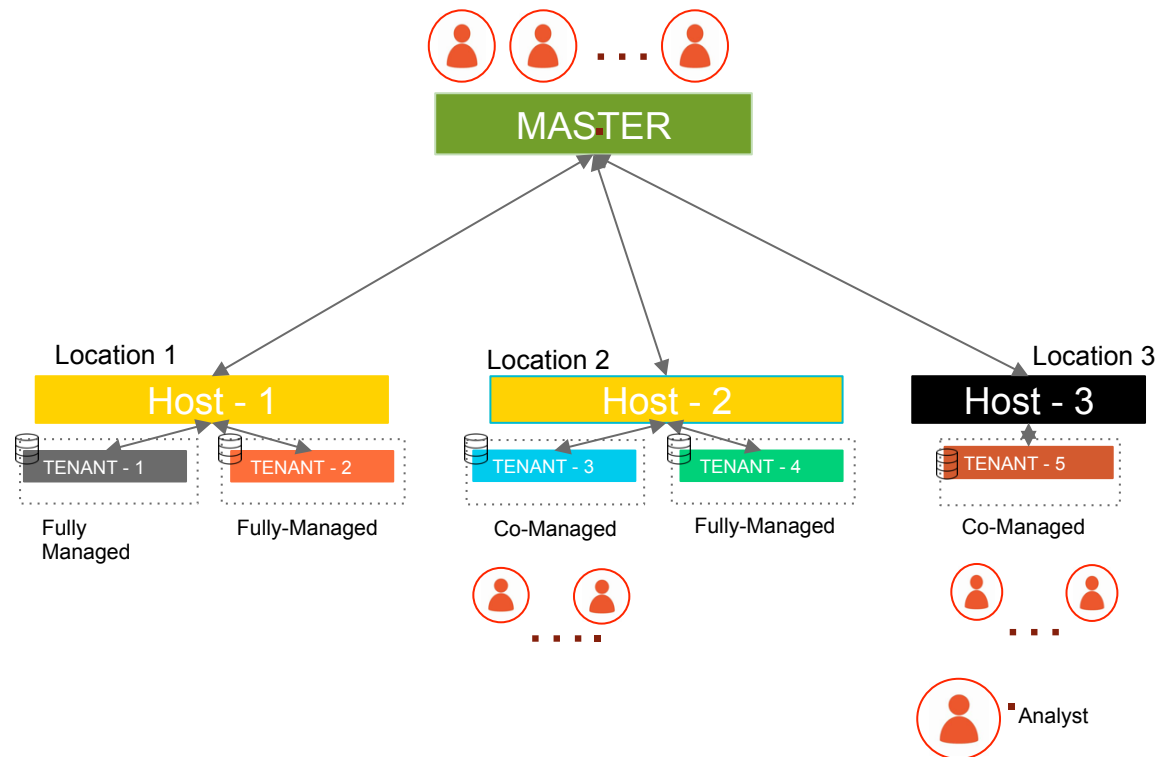
MSSP deploying in
Public cloud



Customer on-premise server



Cortex XSOAR multi-tenancy for MSSPs



Deployment flexibility

- Both fully managed and co-managed models.
- Horizontal scaling to 100s of tenants.
- Complete data separation between tenants.

Content and tenant customization

- Integrations, playbooks can be deployed at the master level or the tenant level.
- Customized dashboards, reports per tenant.
- RBAC for analysts and customer accounts.

Deployment with hosts

- Tenants can be on the same host as master or can be on other hosts.
- The hosts can be geographically dispersed.
- Hosts can be physical/virtual compute resource.

Cortex XSOAR for MSSPs



Flexibility and scale

- On-prem and cloud-hosted deployment options.
- Horizontal scalability across 100+ tenants.
- Data, execution, and network isolation for tenants.



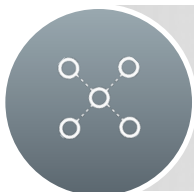
Automated, streamlined processes

- Playbooks to automate well known processes.
- Machine learning algorithms suggest incident experts, commonly used security commands, workflow tasks/inputs.



Quick and simple deployment

- Extensible product integration network, setup.
- Internal SDK, service support, and PyCharm plug-in for custom integrations.



Collaboration enables customer trust

- Handle distributed SOC teams and hand-offs with increased efficiency.
- Collaborate with customers and SMEs via Demisto War Room.

Improve analyst productivity

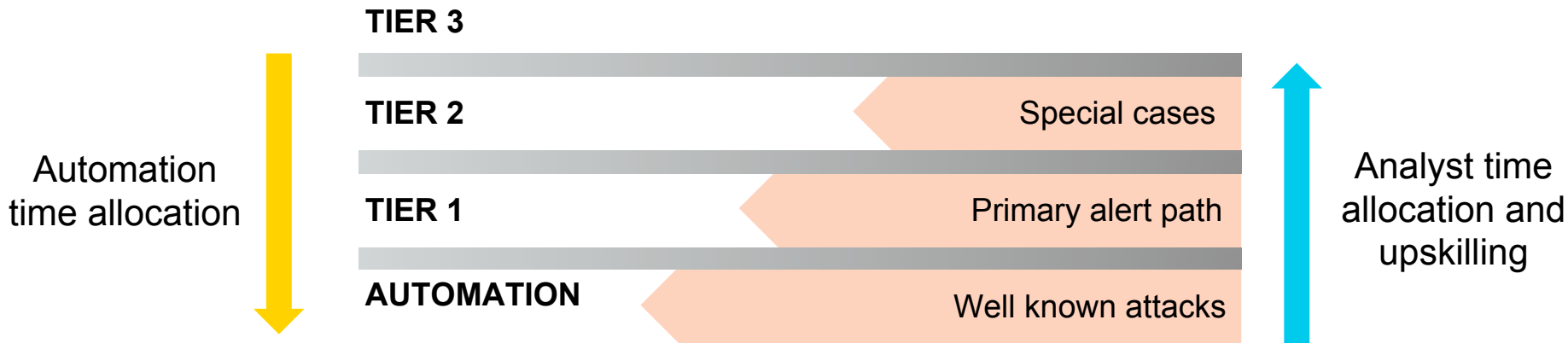
Enhanced service scale

Single pane of glass

Deliver better MTTD/MTTR

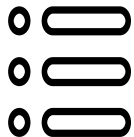
Reduce cost of service delivery

Reduce cost of SOC service delivery with automation



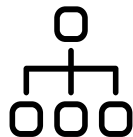
With automation, analyst time commitment will shift towards investigation and mitigation rather than triage and repetitive task execution

Improve analyst productivity with enhanced processes



Process repeatability

Standardized processes will ensure **quicker analyst onboarding** and **modular IR execution** for complex incidents



Unified workflows

With time, more products and tasks will come under the ambit of automation, leading **broader and deeper playbooks**

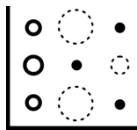


Continuous learning

Machine learning algorithms will suggest incident **owners and experts**, commonly used security **commands**, workflow tasks and **related incidents**

Consistent workflows, automation, auto documentation and machine learning simplify analyst onboarding, making them productive from day one.

Diversify revenue streams with Cortex XSOAR value-added services



Tiered Services

Tiered SOC services based on the ability to deliver consistent and improved SLAs



Co-Management

Offer co-management of SOC services through Demisto's multitenancy



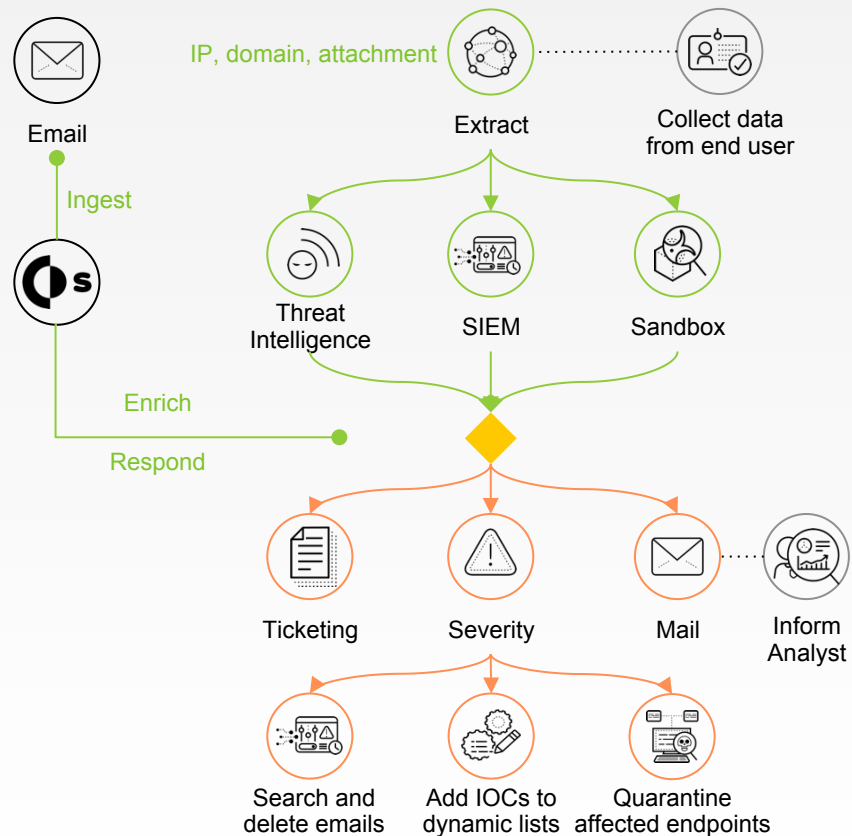
SOAR-as-a-Service

SOAR-as-a-service to existing SOC management and SOC-as-a-service customers

New value-added services increase both revenue potential for MSSPs and effectiveness for end users

Additional Use Cases

Phishing enrichment and response



Visual playbook editor to define custom processes & tasks



Automated data collection from end users & stakeholders



Review live playbook run outputs & simplify task management

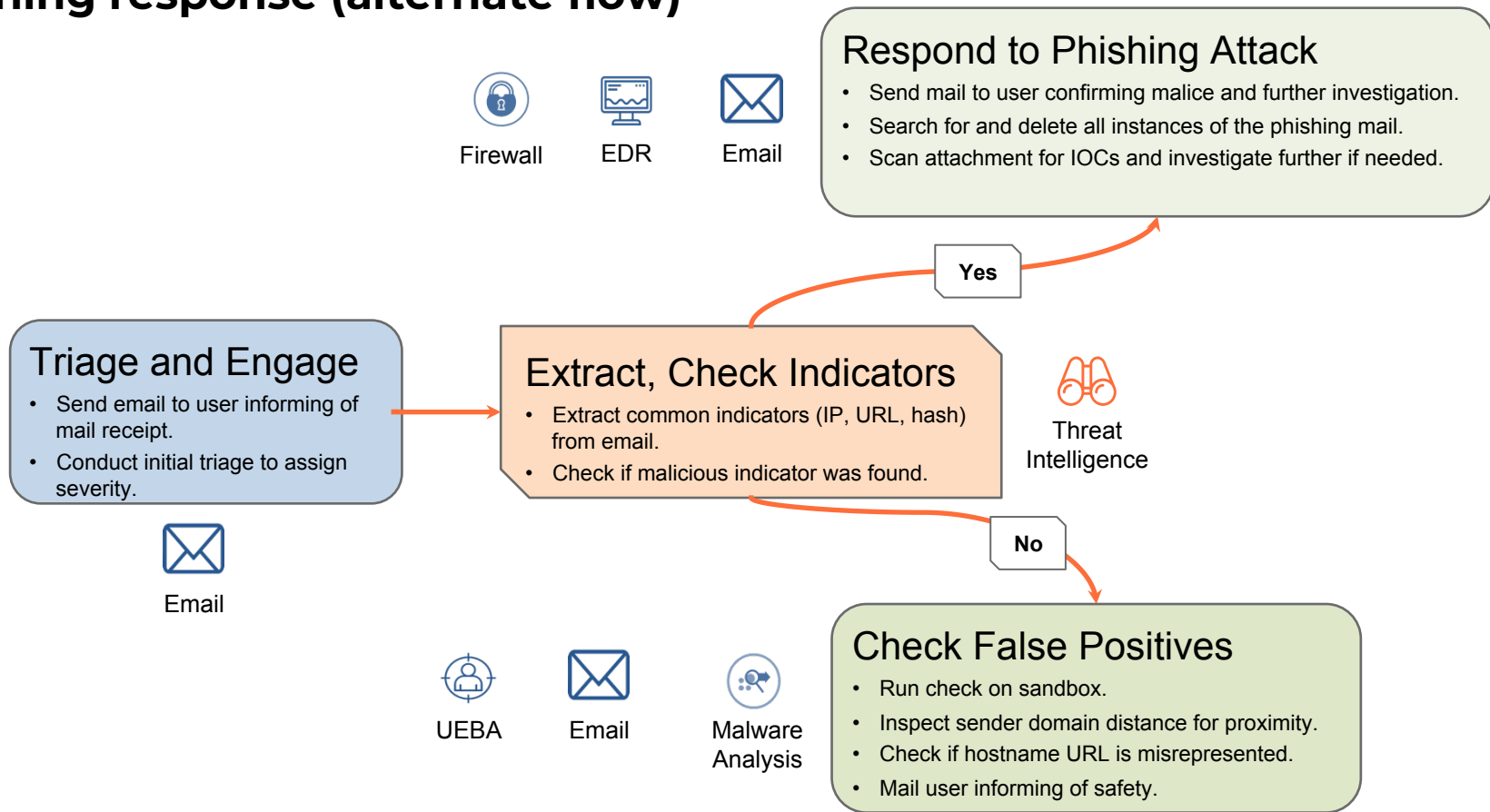


350+ integrations that increase breadth & depth of response



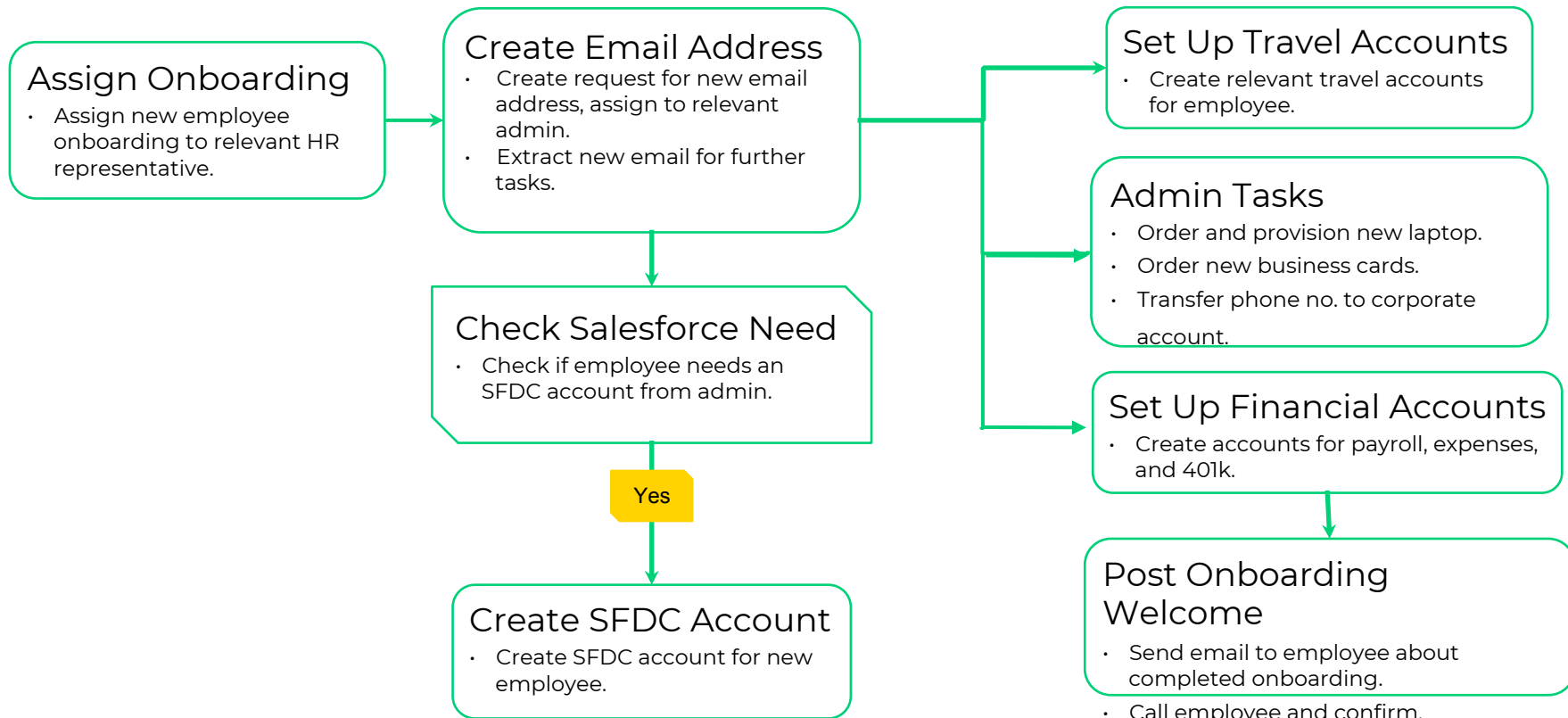
Automated tasks for searching/deleting emails, adding IOCs to lists/groups

Phishing response (alternate flow)



Employee onboarding

Cortex XSOAR used this playbook to onboard new employees (back when we were a startup)



Rapid IOC hunting

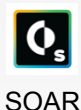
Ingest

- Ingest list of IOCs as attached csv/text files.



Extract IOCs

- Extract IOCs from the csv/text file using Regular Expression.



Hunt IOCs Across Tools

- Check how many threat intelligence tools are deployed and hunt for extracted IOCs on those tool databases.

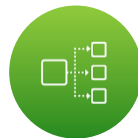


Update Databases

- Update databases with new IOC information whenever relevant.



Close Playbook



Upload STIX files and execute playbooks in real-time (as Demisto 'Jobs')



Any combination of automated and manual tasks guiding users through hunting process



Wide no. of integrations with threat intel and endpoint products



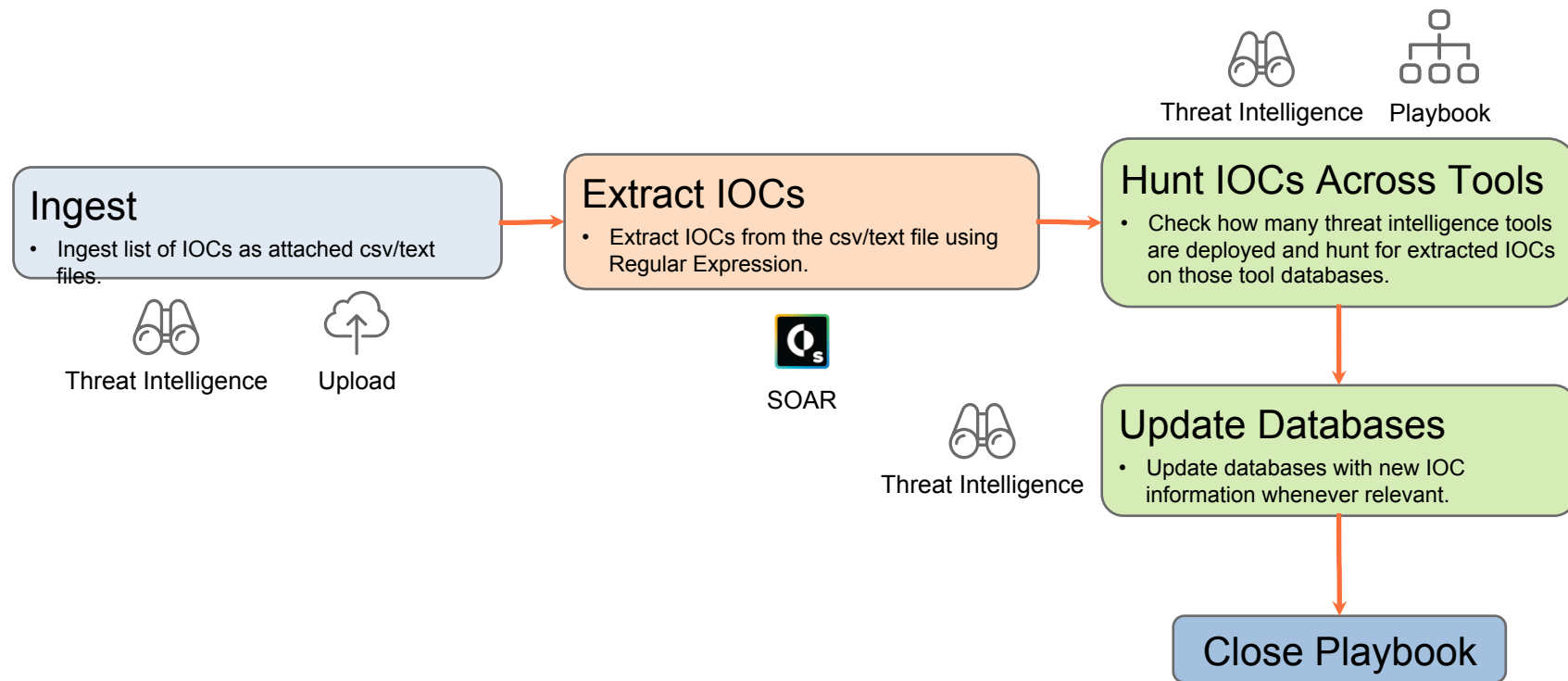
Correlation of indicators across incidents and a dedicated indicator repository



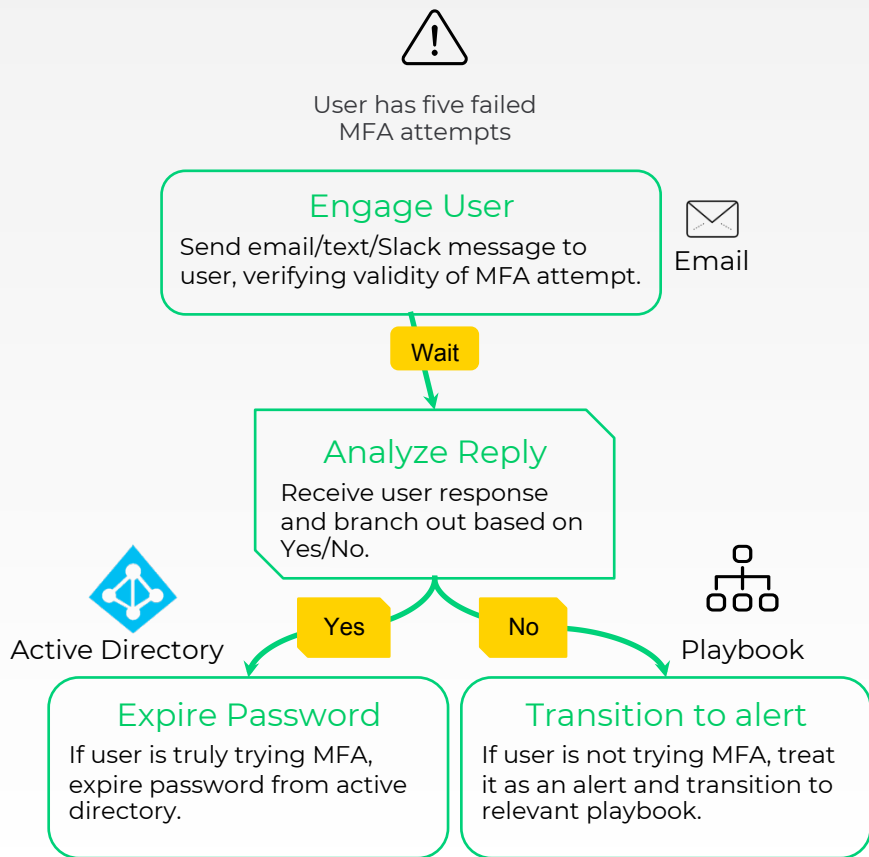
Nested threat hunting playbook helps user transition from other processes to hunting

Rapid IOC hunting (alternate flow)

SOAR playbooks can be **proactively scheduled** or **run in real-time** to conduct threat hunting exercises



User access - MFA failure



Modular playbooks can perform multiple checks & filters



Automated data collection from end users & other stakeholders



Integrations with email, Active Directory, Slack etc. for end-user communication



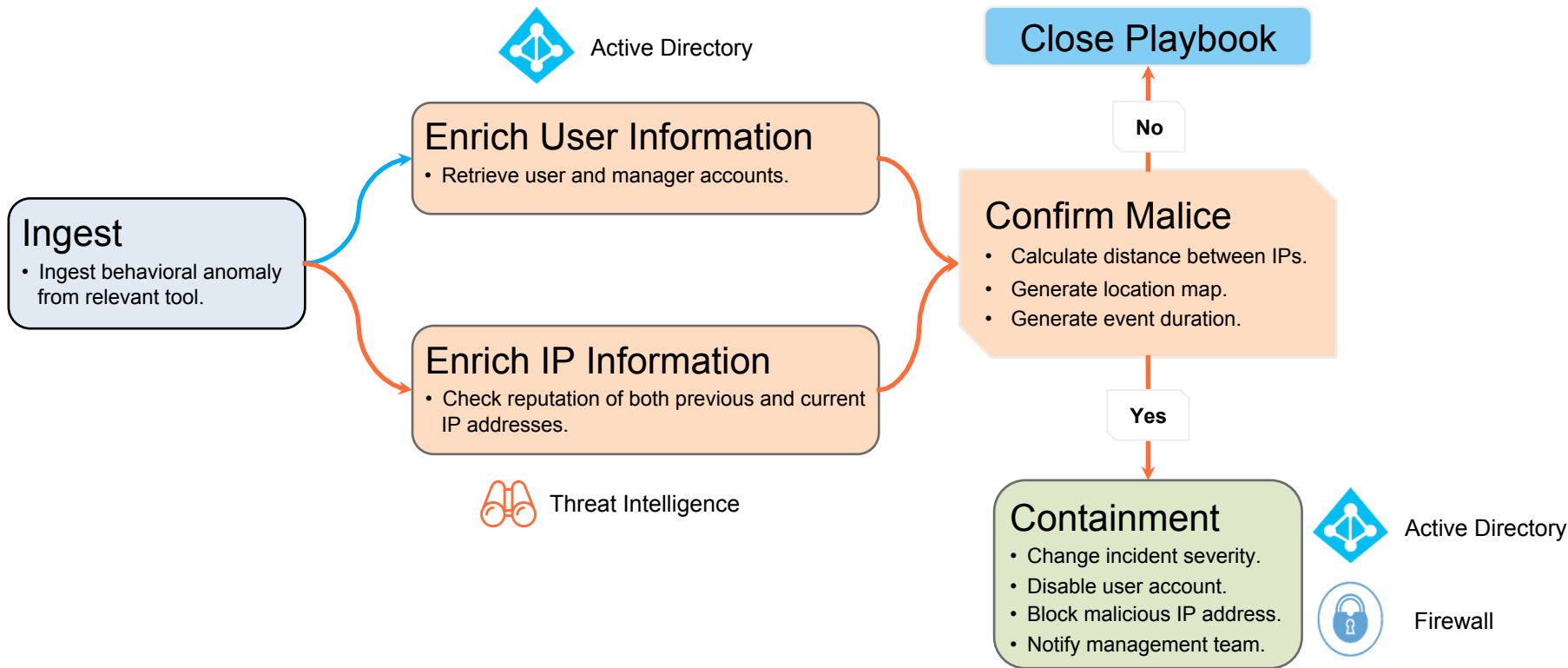
300+ integrations that increase breadth & depth of response



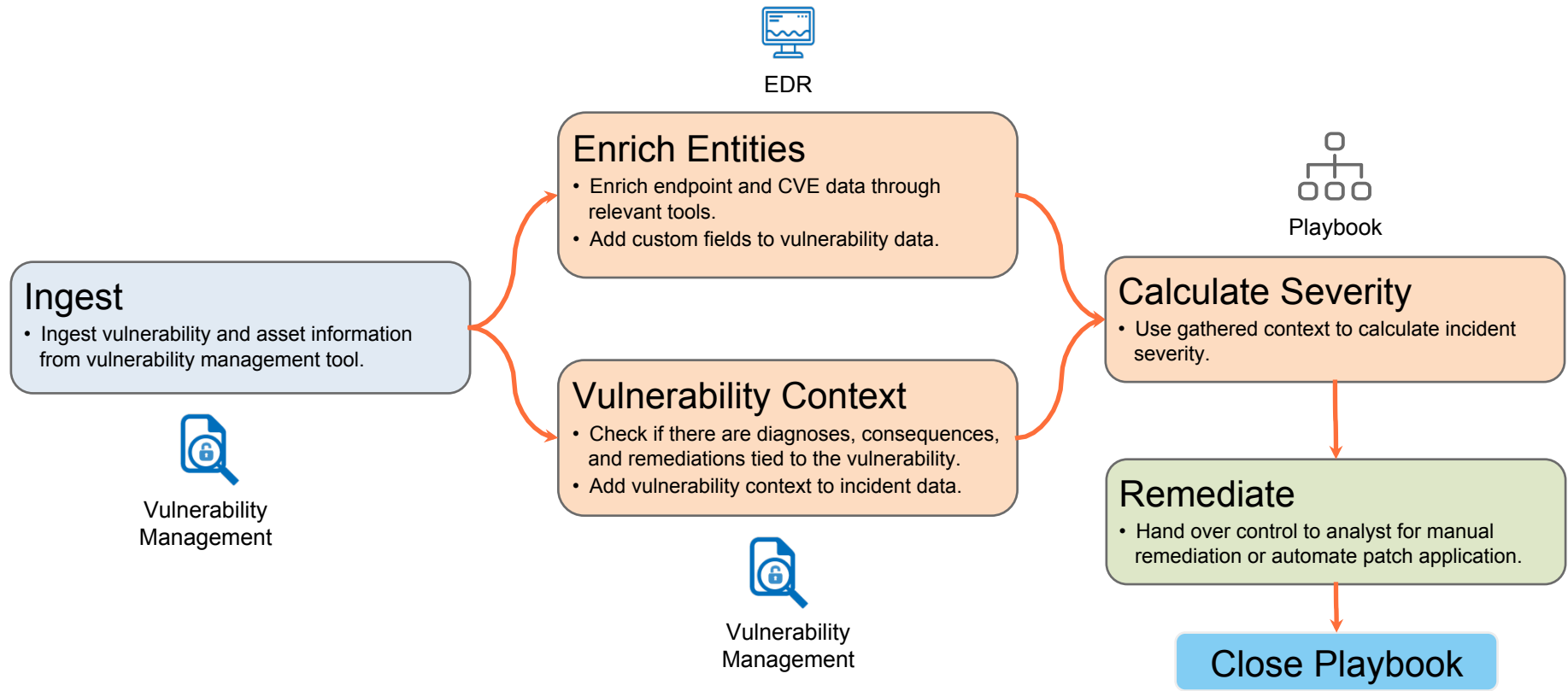
Nested playbooks helps security team transition to IR if it's a genuine alert

Impossible traveler

Use case: Two IP addresses tied to the same user are far apart.

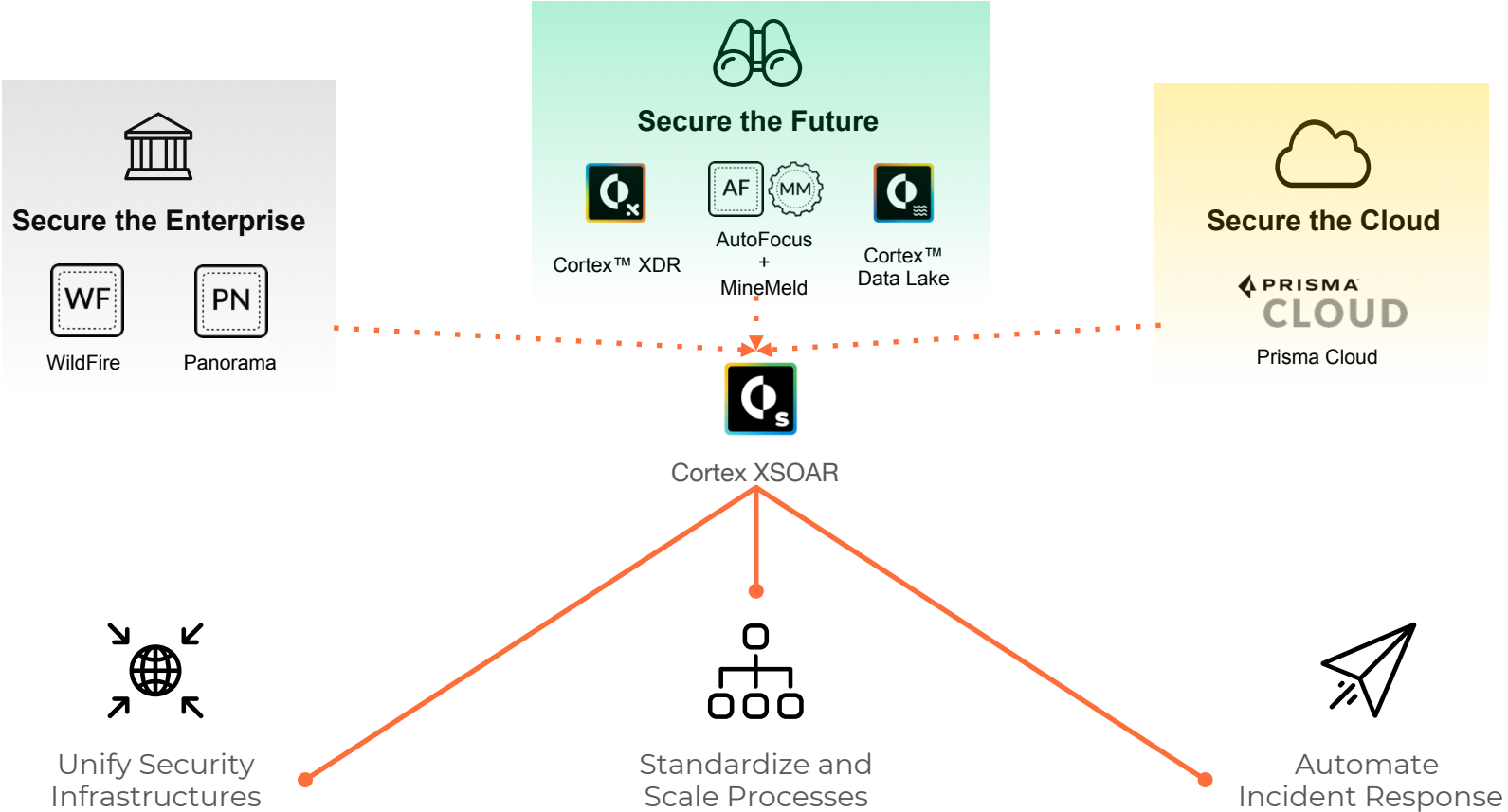


Vulnerability management



Cortex XSOAR & Palo Alto Networks

Cortex XSOAR and Palo Alto Networks

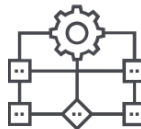


Integration features

Cortex XSOAR and Palo Alto Networks products



Ingest data
into Demisto



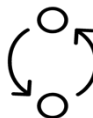
Trigger
automated
playbooks



Collaborate in
War Room



Unify
workflows
across products



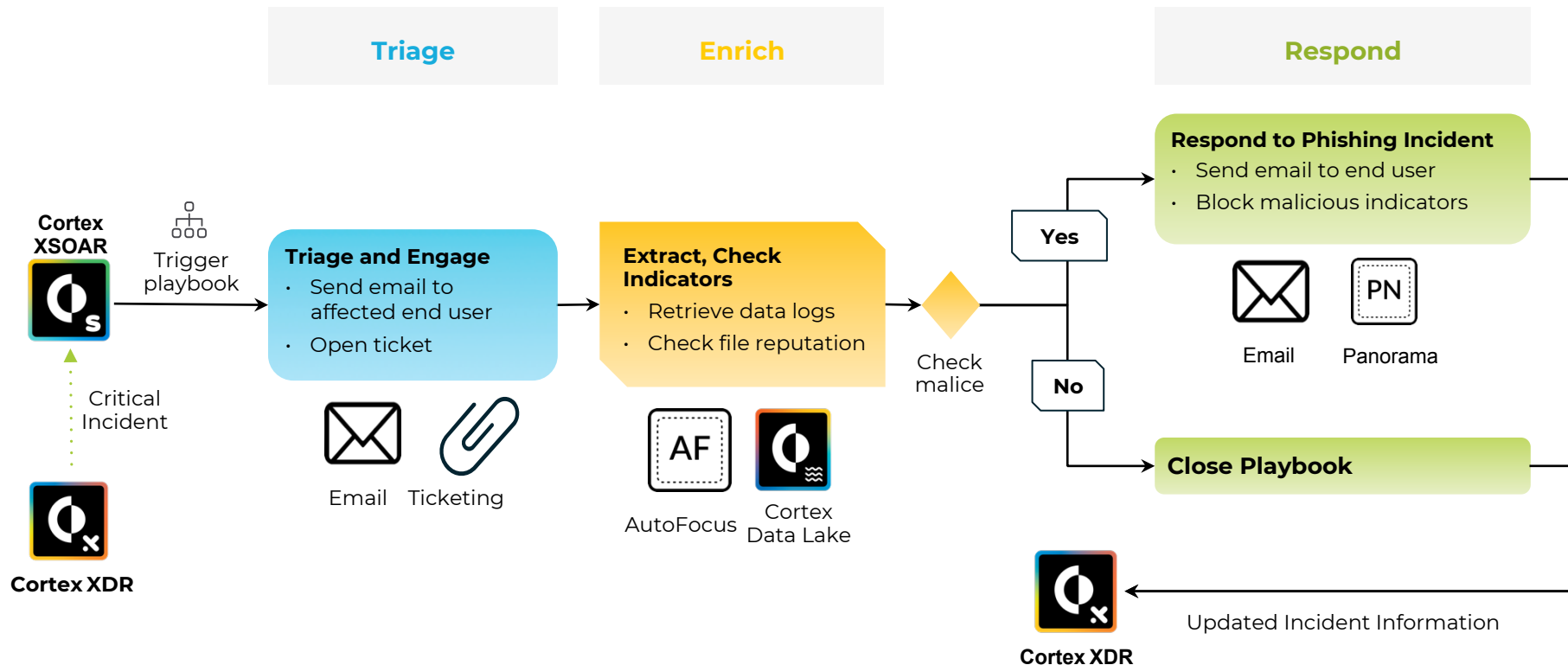
Cross-correlate
indicators



Run **real-time**
commands

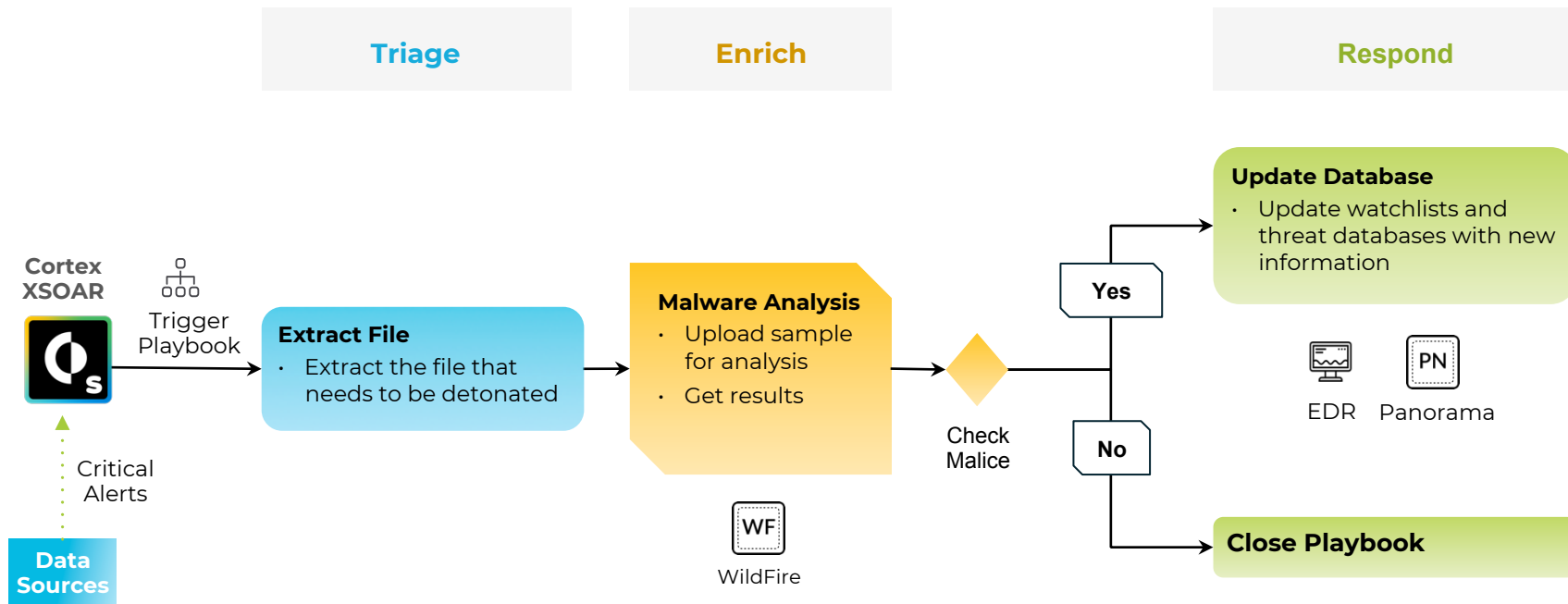
Cortex XSOAR and Cortex XDR use case

Phishing alert with drive-by download that initiated port scan



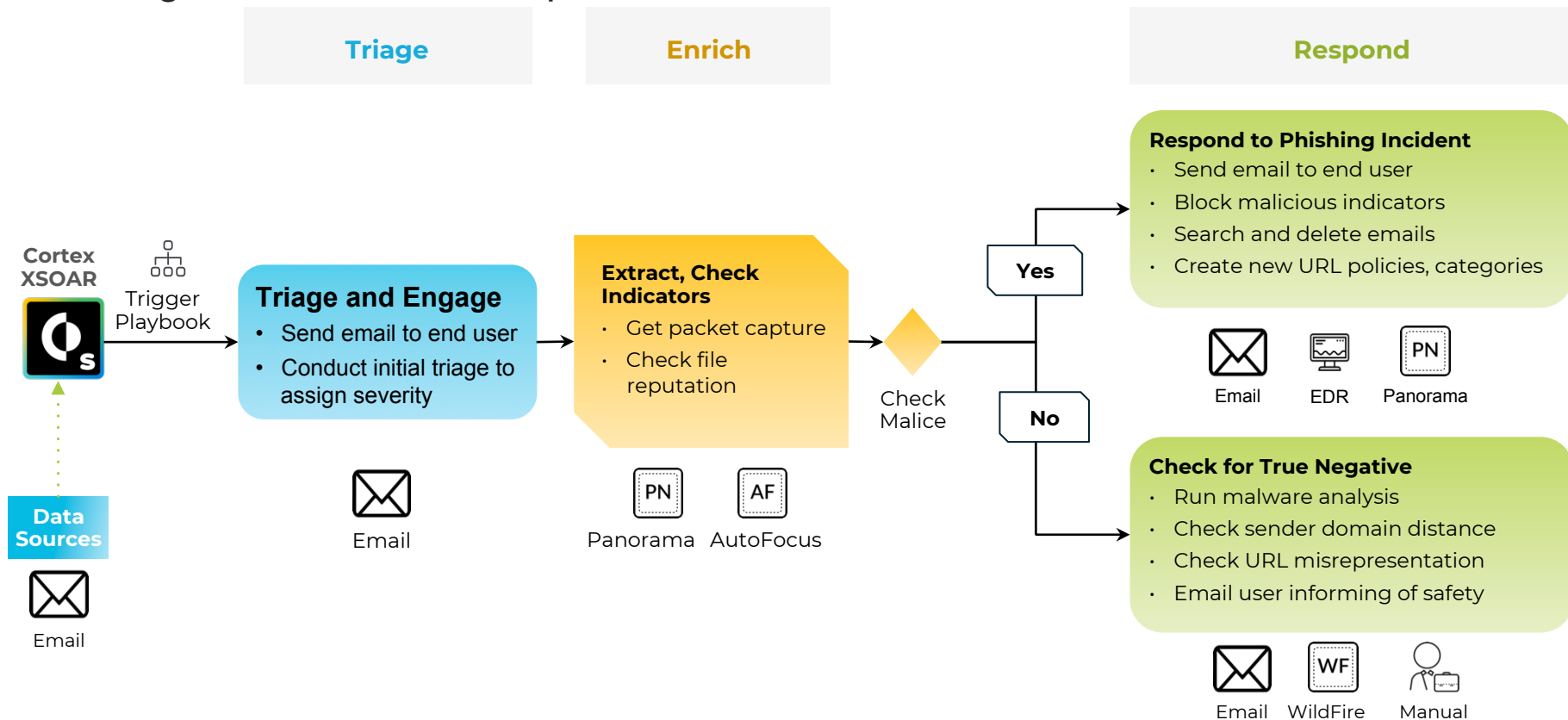
Cortex XSOAR and WildFire use case

Automated malware analysis and response



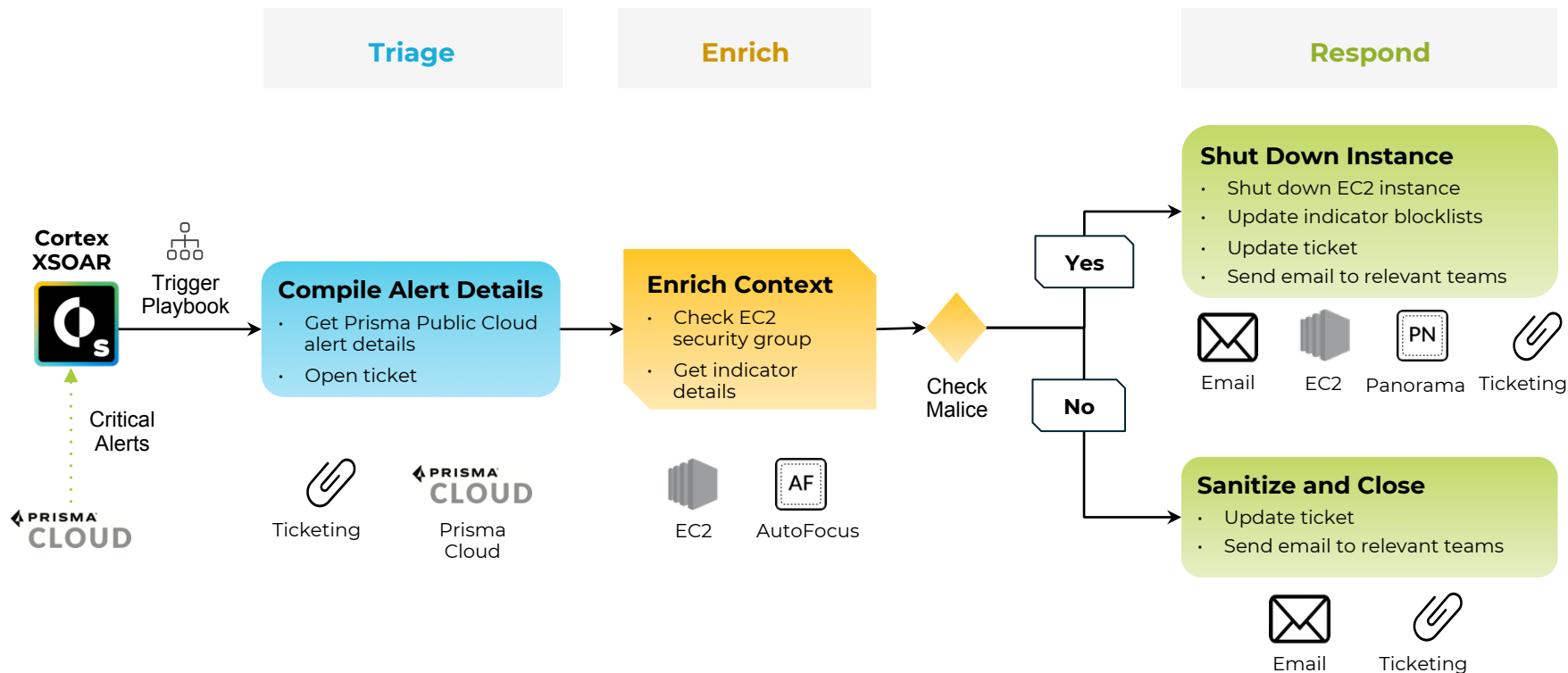
Cortex XSOAR and Panorama use case

Phishing enrichment and response

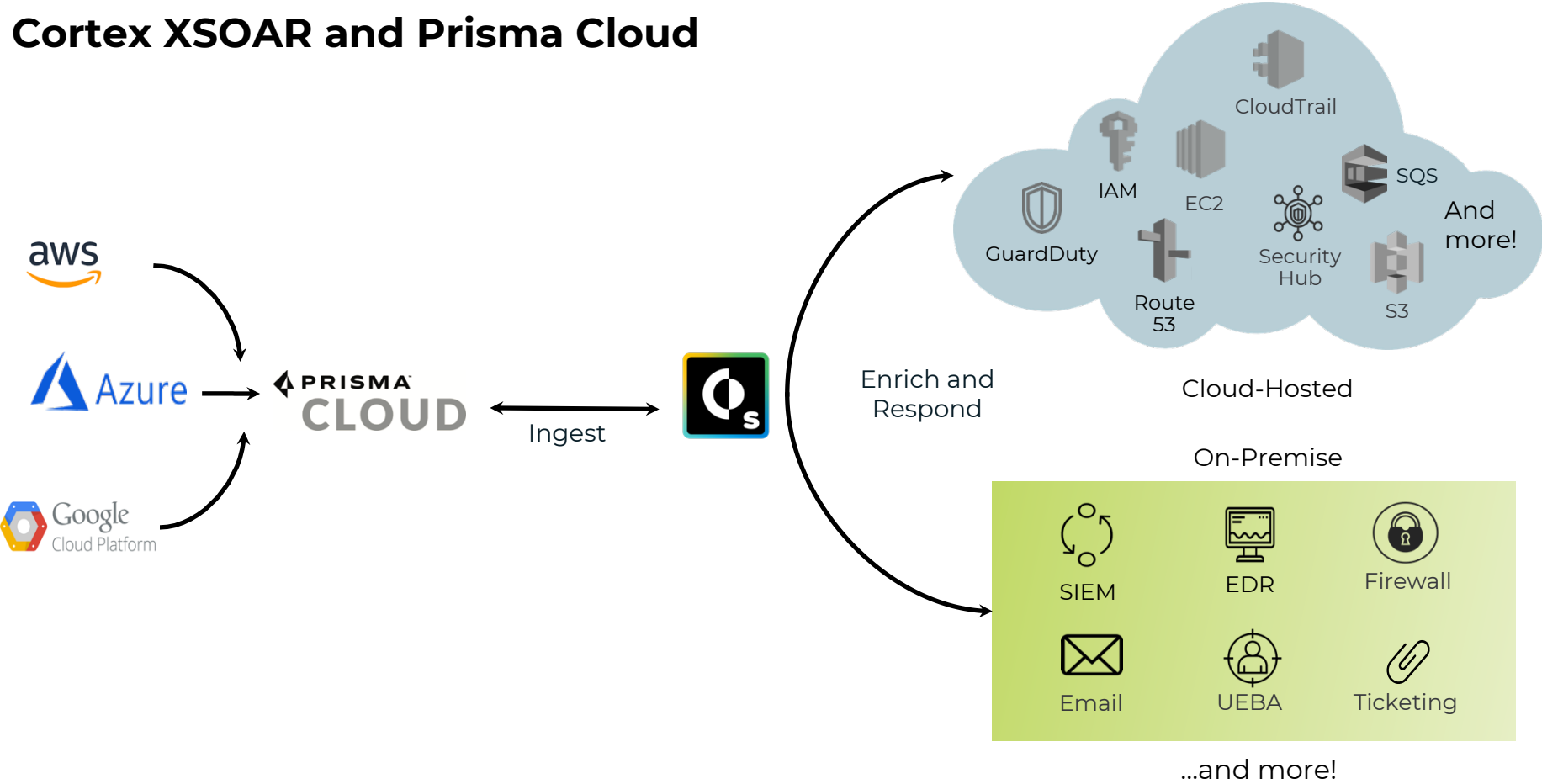


Cortex XSOAR and Prisma Cloud use case

Malicious traffic to internet-exposed database instance



Cortex XSOAR and Prisma Cloud



SOAR Industry Overview

SOAR market evolution

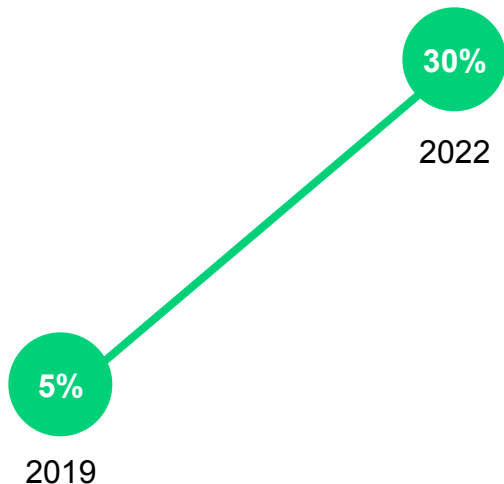


Increased Adoption

Organizations leveraging SOAR (Security Orchestration, Automation, and Response) solutions will **rise from 5% now to 30% by 2022**.

Technology Convergence

The ideal SOAR solution is a **convergence of three previously distinct technology markets**: security orchestration and automation, security incident response platforms, and threat intelligence platforms.



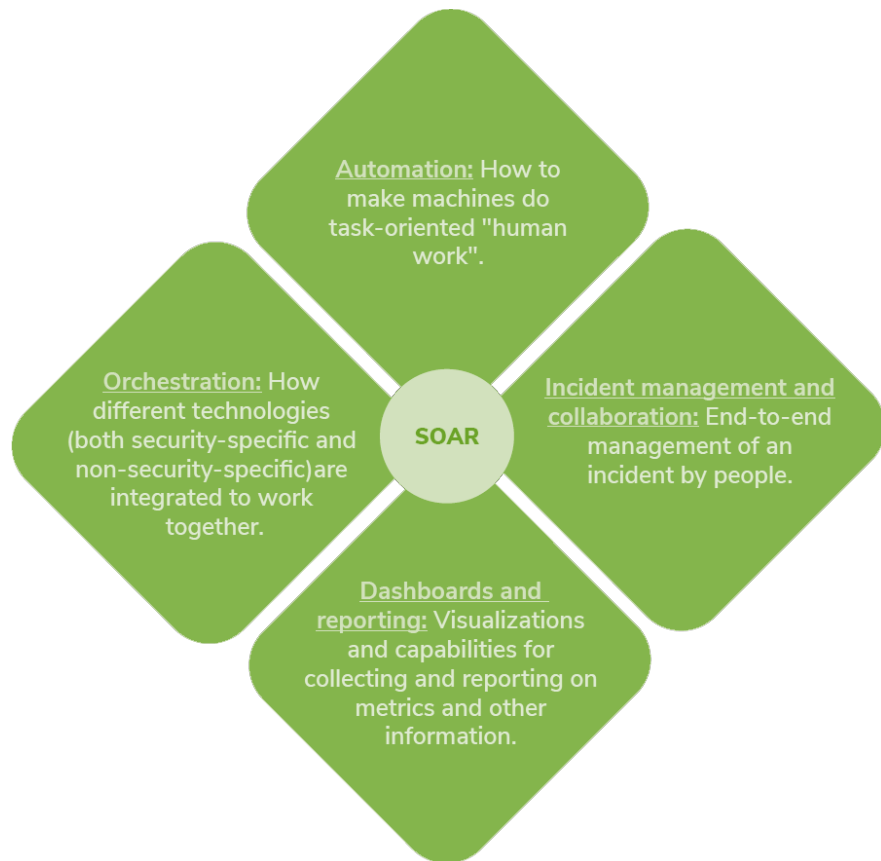
Source: Neiva, C., Lawson, C., Bussa, T., & Sadowski, G. (2017, November 30). Innovation Insight for Security Orchestration, Automation and Response (ID: G00338719). Retrieved from Gartner database.

A perfect SOAR match

Cortex XSOAR successfully maps with all of Gartner's recommended capabilities for SOAR vendors.

[Click here to view full PDF](#)

End-to-end solution that can handle varying levels of complexity across a SOC's maturity cycle.



Source: Neiva, C., Lawson, C., Bussa, T., & Sadowski, G. (2017, November 30). Innovation Insight for Security Orchestration, Automation and Response (ID: G00338719). Retrieved from Gartner database.

Analyst momentum



Demisto named by Gartner as a **"Cool Vendor"** in Security Operations and Vulnerability Management, 2018



Launched in 2015, Demisto rapidly became one of the most visible security orchestration, automation and response (SOAR) vendors, outshining vendors launched years earlier. An early focus on user interface (and not just the APIs), its inclusion of machine learning, usable Slack integration, and sizable stable of out-of-the box integration with tools and online services makes it a popular SOAR tool.”

Anton Chuvakin
Ex-Research VP, Gartner

SOAR drivers



Growing alerts

>12K alerts per week



Limited visibility

Expanded threat surface



Lack of skilled analysts

2 million analysts shortage



Disparate infrastructures

Coordination challenge across product consoles



No consistent process

No metrics, fragmented documentation



Long MTTR

Increased business risk: weeks to resolve incidents

Who's selling SOAR?



Fragmented market



Different pricing outlooks



Tough to compare

Ticketing Systems



SIEM Vendors →

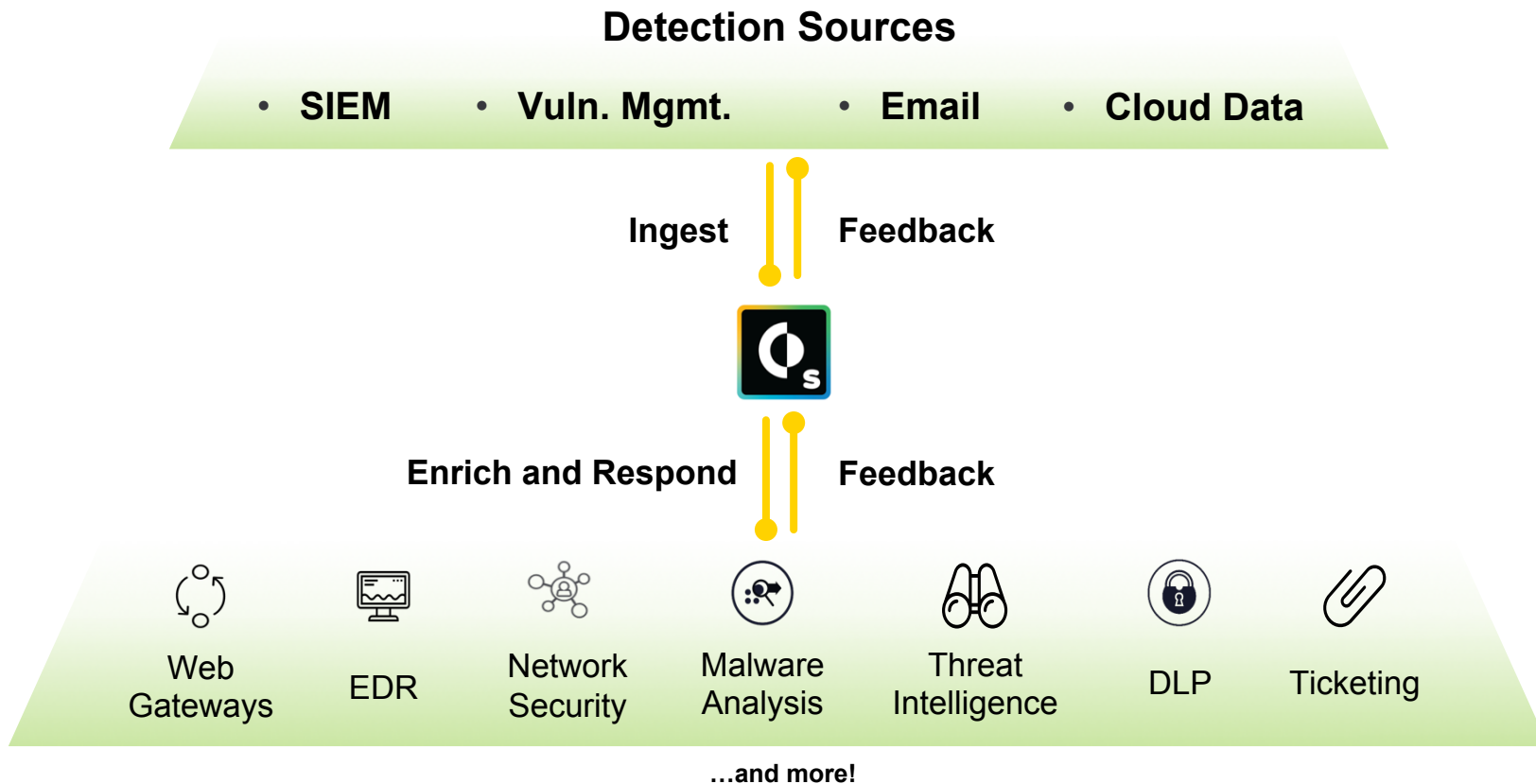
SOAR

← Threat Intel Tools



Orchestration Platforms

How SOAR works



SOAR benefits



Unify Security Infrastructures

Coordinate enrichment and response by gathering intelligence from multiple products on a single console



Increase Analyst Productivity

SOAR frees up analyst time for more important decision-making, and proactive tasks rather than getting mired in grunt-work.



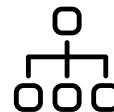
Accelerate Incident Response

By automating low-level manual tasks, SOAR can reduce incident response times and improve accuracy.



Leverage Existing Investments

Through automation and minimized console-switching, SOAR enables coordination across multiple products and greater value from existing security investments.



Standardize And Scale Processes

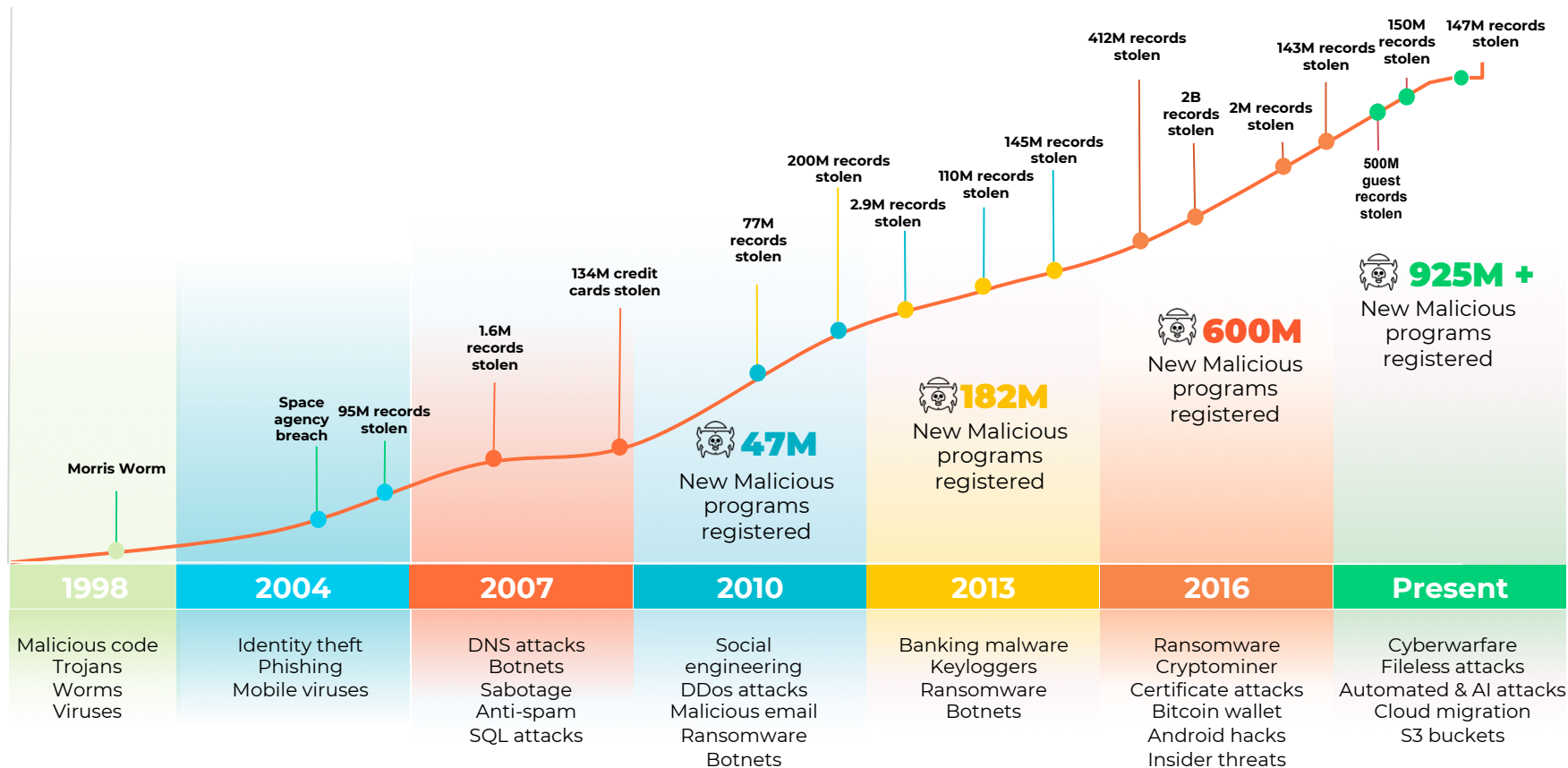
Through playbooks, SOAR standardizes incident enrichment and response processes that increases the baseline quality of response and is scalable.



Improve Overall Security Posture

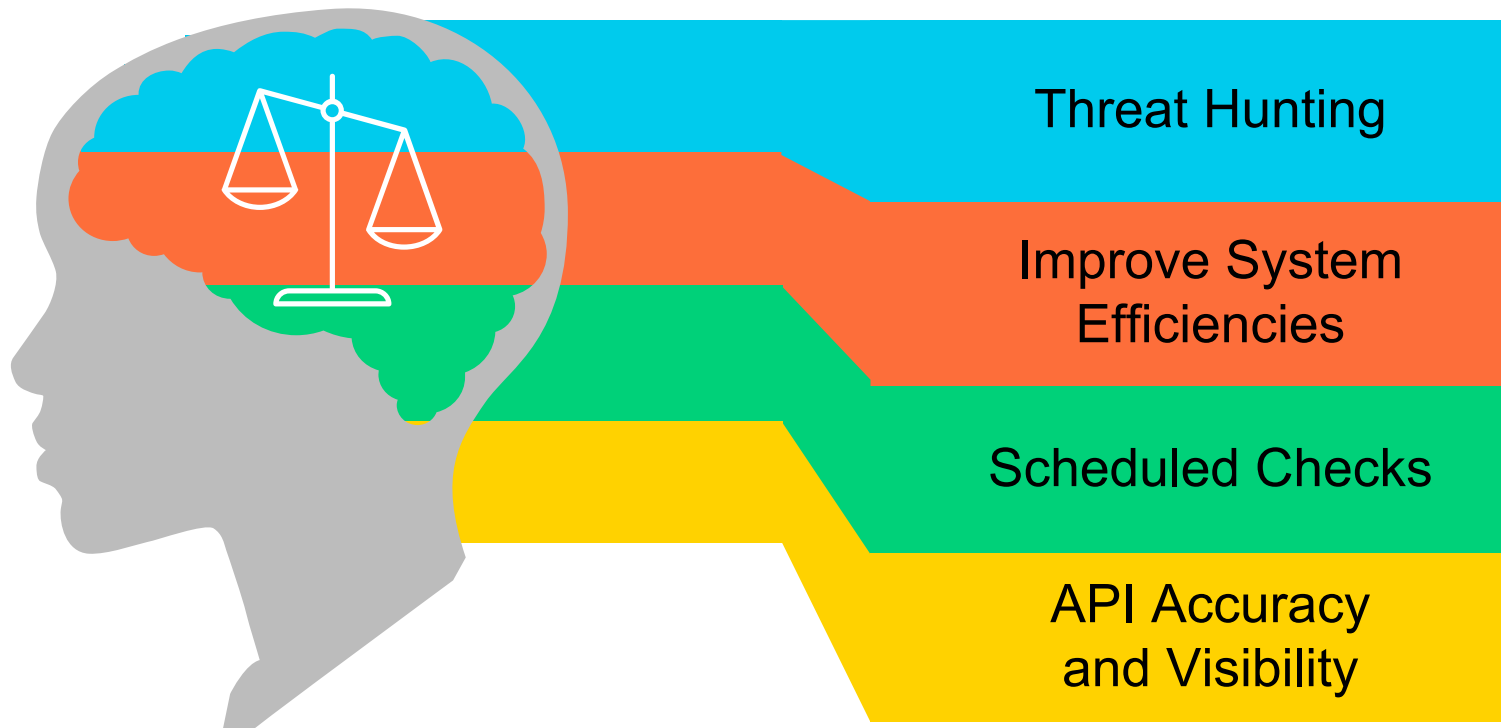
The sum of all aforementioned benefits is an improvement of the organization's security posture and a corresponding reduction in security and business risk

As threats escalate, SecOps is more important than ever



Immediate ROI

SOAR frees up L2/L3 analyst time to conduct more proactive operations and value-added tasks



Compounding ROI

ROI from SOAR will compound over time due to effects such as learning, repeatability, and process standardization

Process Repeatability



Standardized processes will ensure **quicker analyst onboarding** and **modular IR execution** for complex incidents

Unified Workflows



With time, more products/tasks will come under the ambit of automation and lead to creation of **broader, all-encompassing playbooks**

Continuous Learning



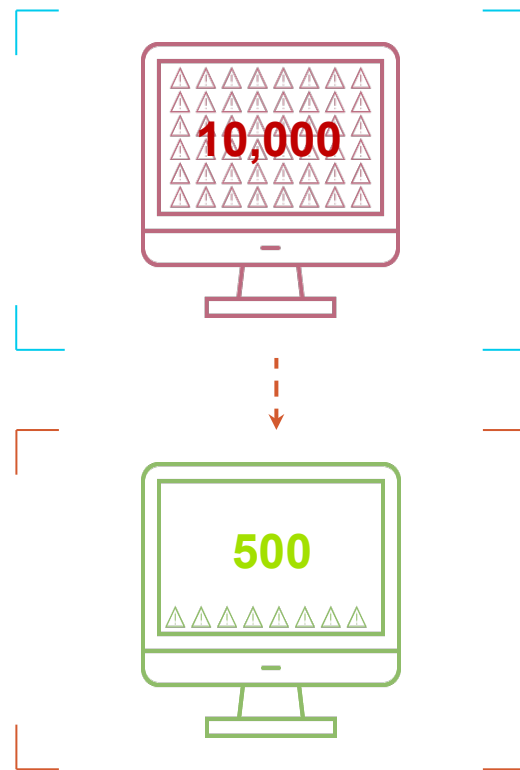
Machine learning algorithms will suggest incident **owners and experts**, commonly used security **commands**, workflow tasks/inputs, and **related incidents**

User Case Studies

Reduced alerts



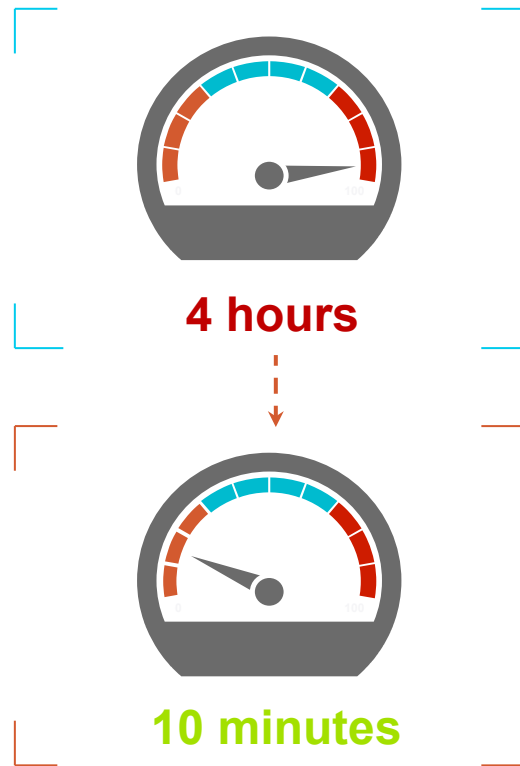
We were struggling with 10,000 alerts per week, including a host of duplicates and false positives. Cortex XSOAR's automated playbooks, cross-correlation, and real-time collaboration helped reduce our alert load to 500 (a **95% decrease**) largely due to speedy resolution of false positives.



Accelerated response



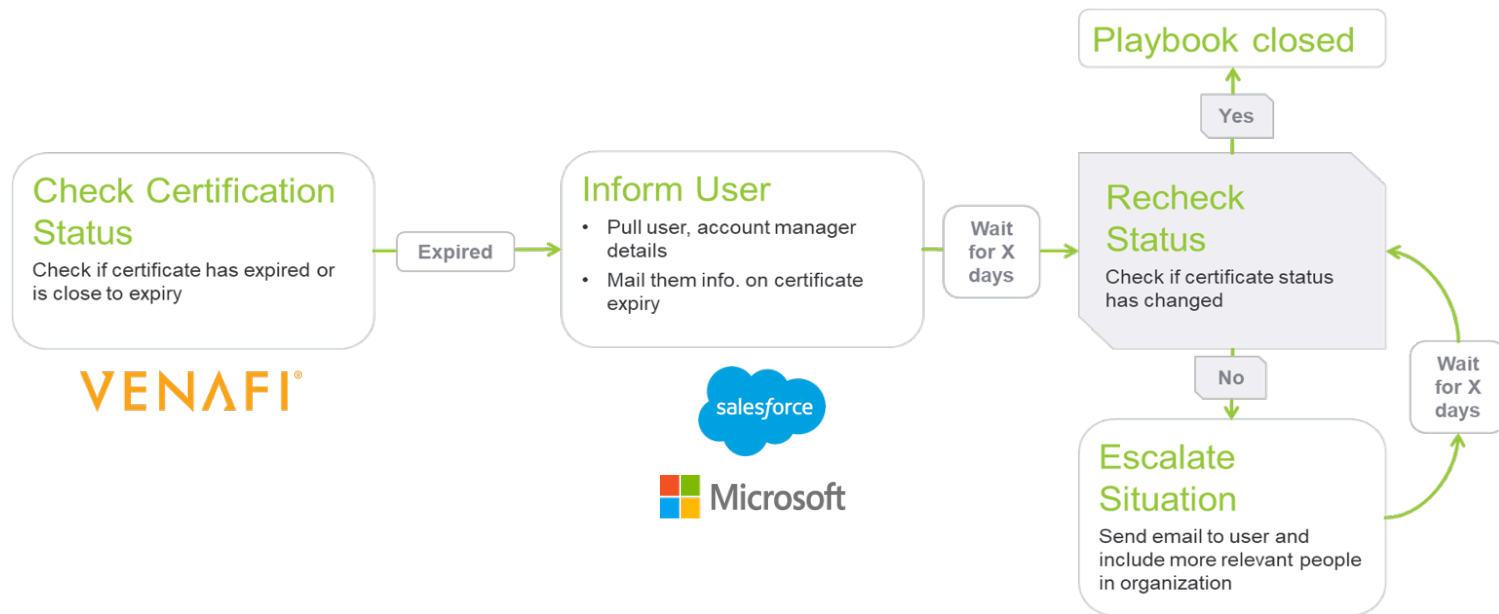
We were challenged by resolution times and needed an ‘action center’ to respond to alerts detected by their SIEM logging tools. We used Cortex XSOAR as a connective fabric between all security products, creating playbooks that standardized and scaled response. We were able to shave time for a common incident occurrence from **4 hours to 10 mins**.



Use case: SSL certificate checks

“We were having trouble maintaining the integrity of SSL certificates across endpoints. We scheduled a Cortex XSOAR playbook to run at timely intervals and query all endpoints to check for SSL certificates nearing expiry, greatly reducing both manual work and business risk stemming from out-of-date endpoints.”

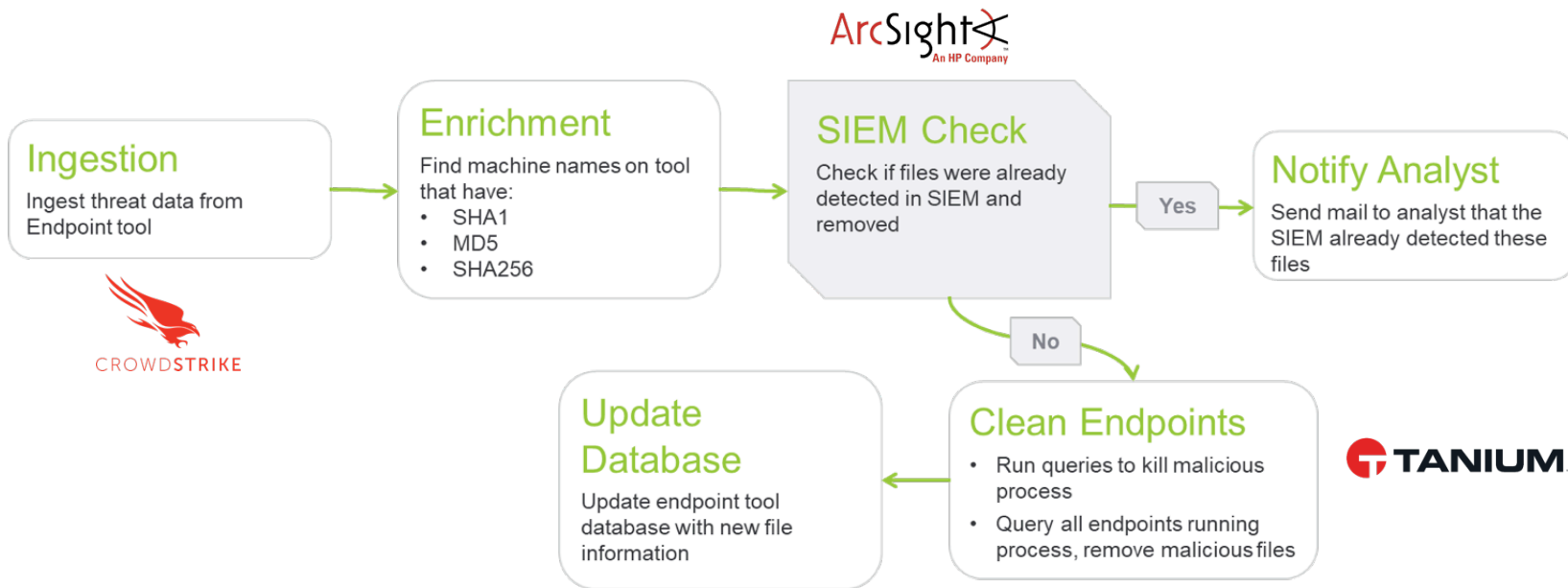
- Healthcare Company



Use case: endpoint response

“Our trouble was reconciling SIEM data with threat intelligence to take action. We used Cortex XSOAR as the connecting grid between products, executing a playbook that identified unprotected endpoints missed by our SIEM, quarantined the endpoints, and updated external databases with new IOC information.”

- High-Tech Conglomerate



Case study: The Pokemon Company International

Goals —●



Keep pace with rapidly scaling cloud environment



Automate everything that humans don't need to do



Provide value to other technology departments

Use Cases —●



EC2 and account compromise



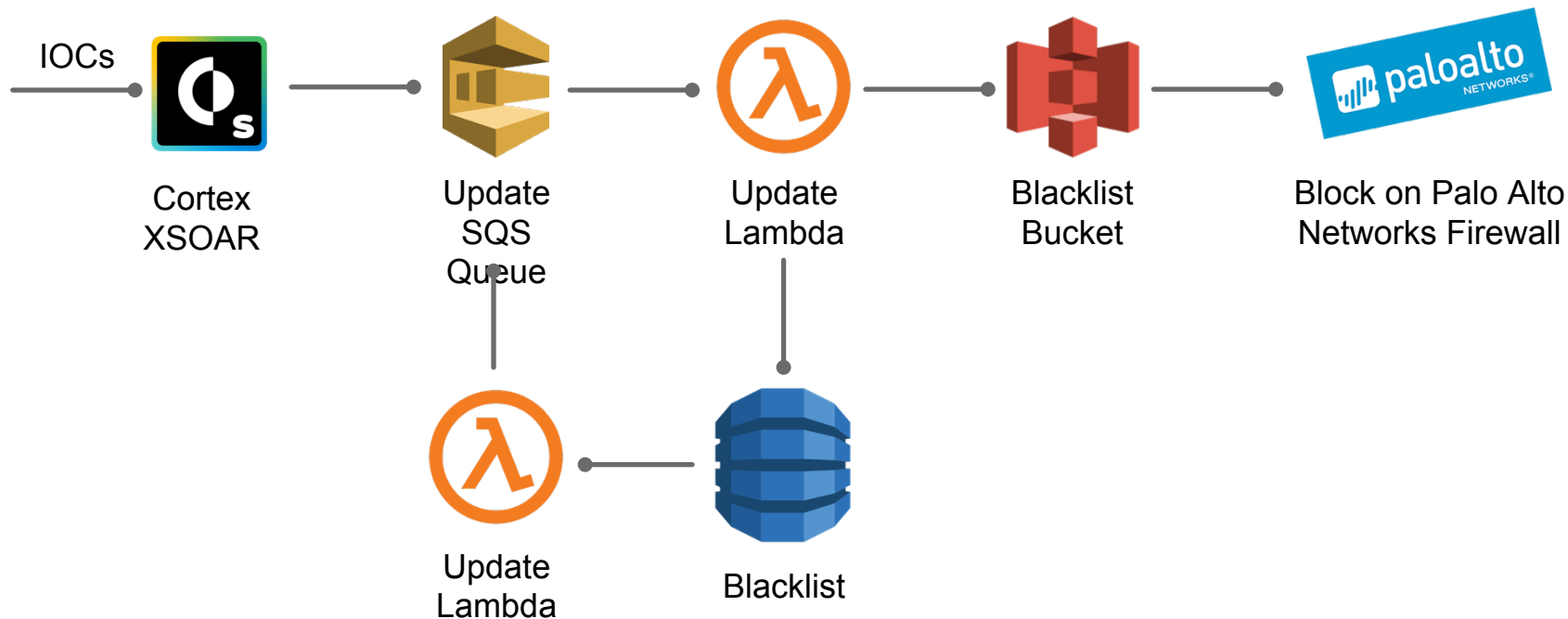
Phishing enrichment and response



Employee offboarding

Case study: The Pokemon Company International

As part of the phishing response playbook that Pokémon deployed, Cortex XSOAR automated extraction of IOCs before pushing those IOCs to blacklists across both cloud and on-premise environments.



Thank you