



Cortex XSOAR

(formerly Demisto)

Security Orchestration, Automation
and Response (SOAR)

David Hagy
Federal Cortex Manager



Demisto Founded to address SOC challenges



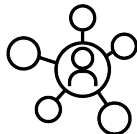
Growing Alerts

>10K alerts per week



Lack of Skilled Analysts

2 million analysts shortage



No Consistent Process

IR Process: no metrics/run over email



Long MTTR, High Risk

Weeks to resolve each detected incident



"Our response times are too long. Every lost second leads to financial and reputational damage."

- CISO



"Our security experts are overwhelmed with the growing number of alerts."

- SOC Manager



"I spend too much time switching between products to effectively respond to incidents."

- IR Analyst



Demisto Delivered:

- Workflow automation engine
- Security ticketing system
- Collaboration platform

Cortex XSOAR Adds:

- Threat Intelligence Management

***The industry's first extended security orchestration, automation and response platform with native threat intel management**



Cortex XSOAR is a workflow automation engine

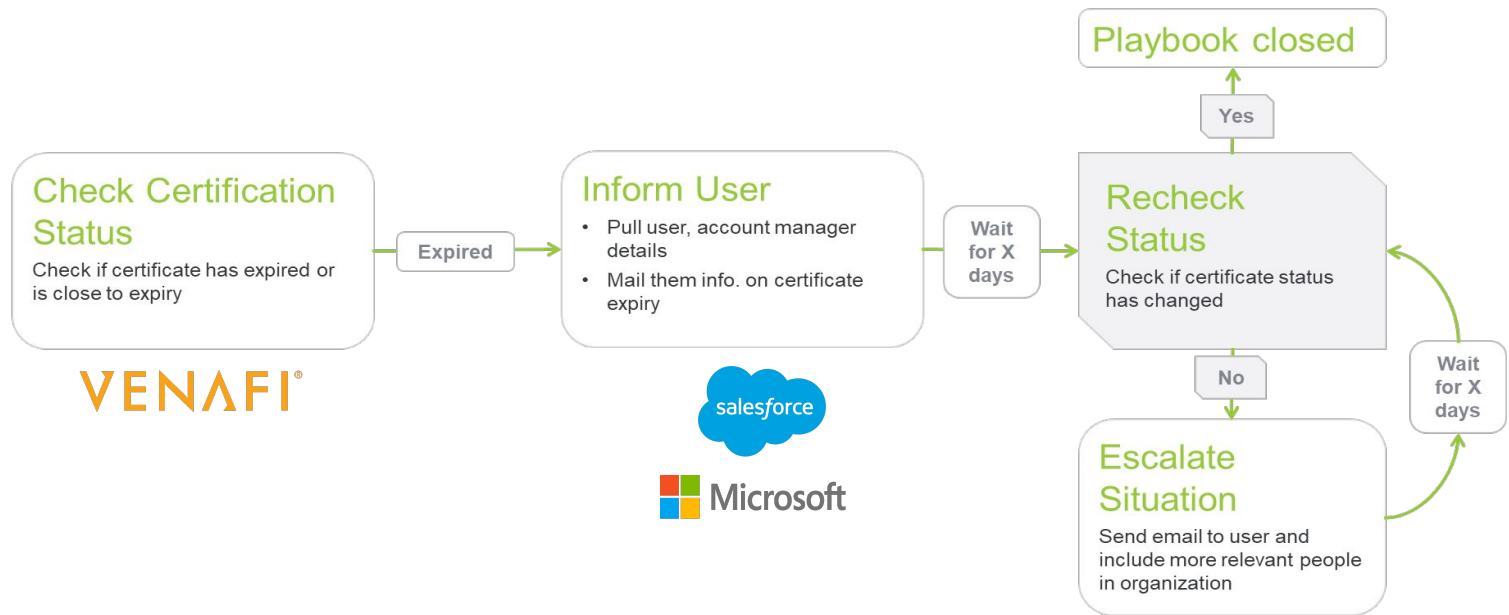
Respond to incidents with speed and scale

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

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to check for SSL certificates nearing expiry, greatly reducing both manual work and business risk stemming from out-of-date endpoints.”

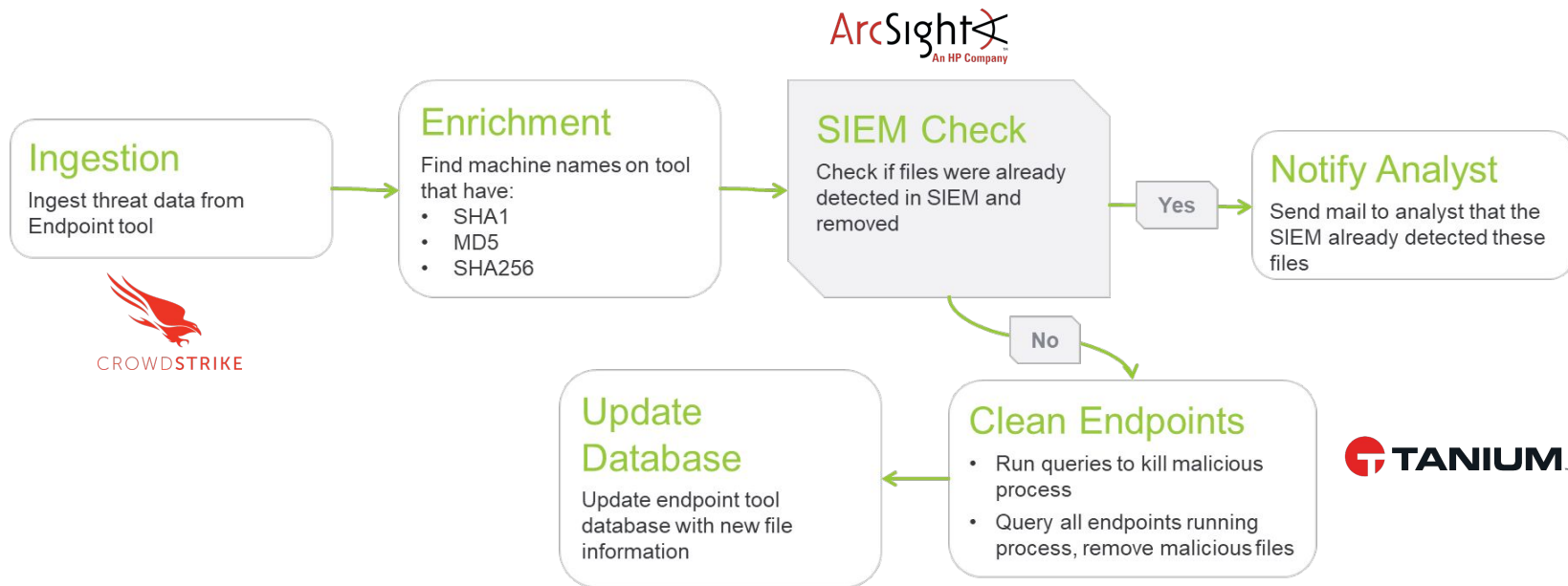
- Healthcare Company



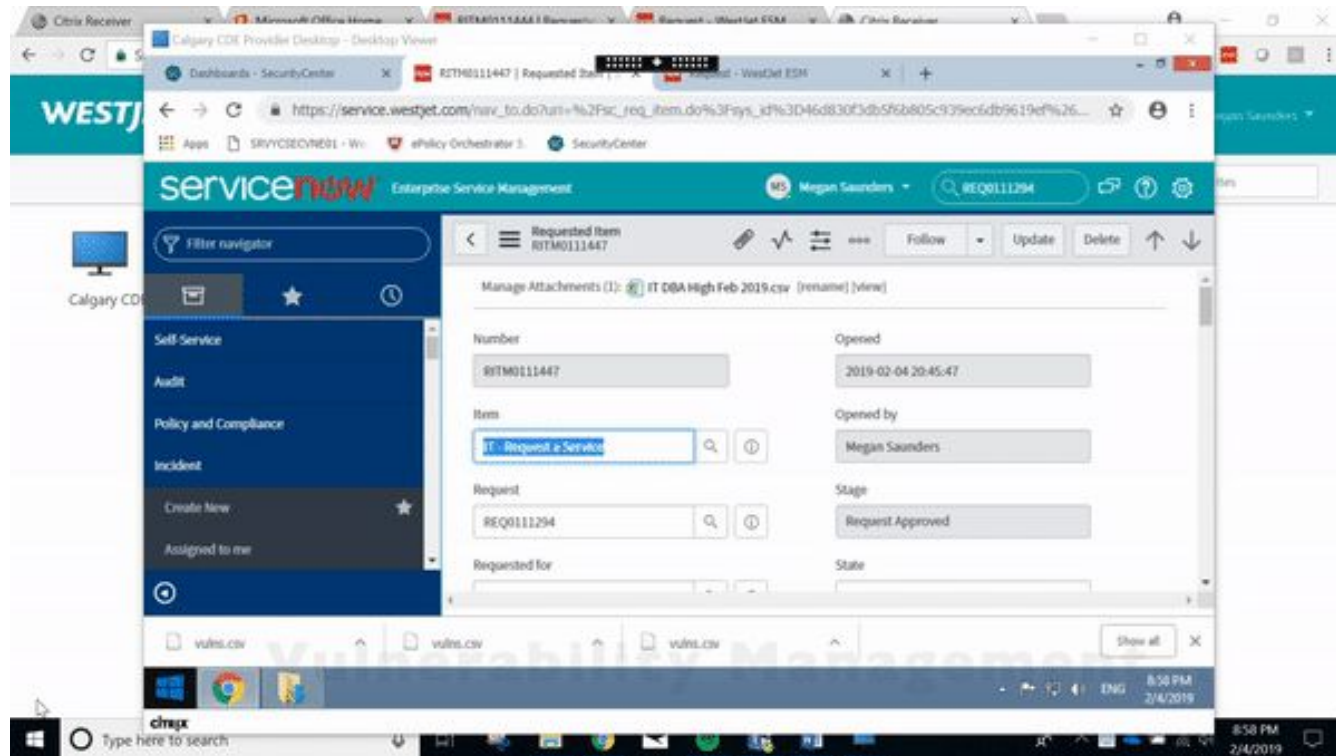
Use case: endpoint response

“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



Before Demisto



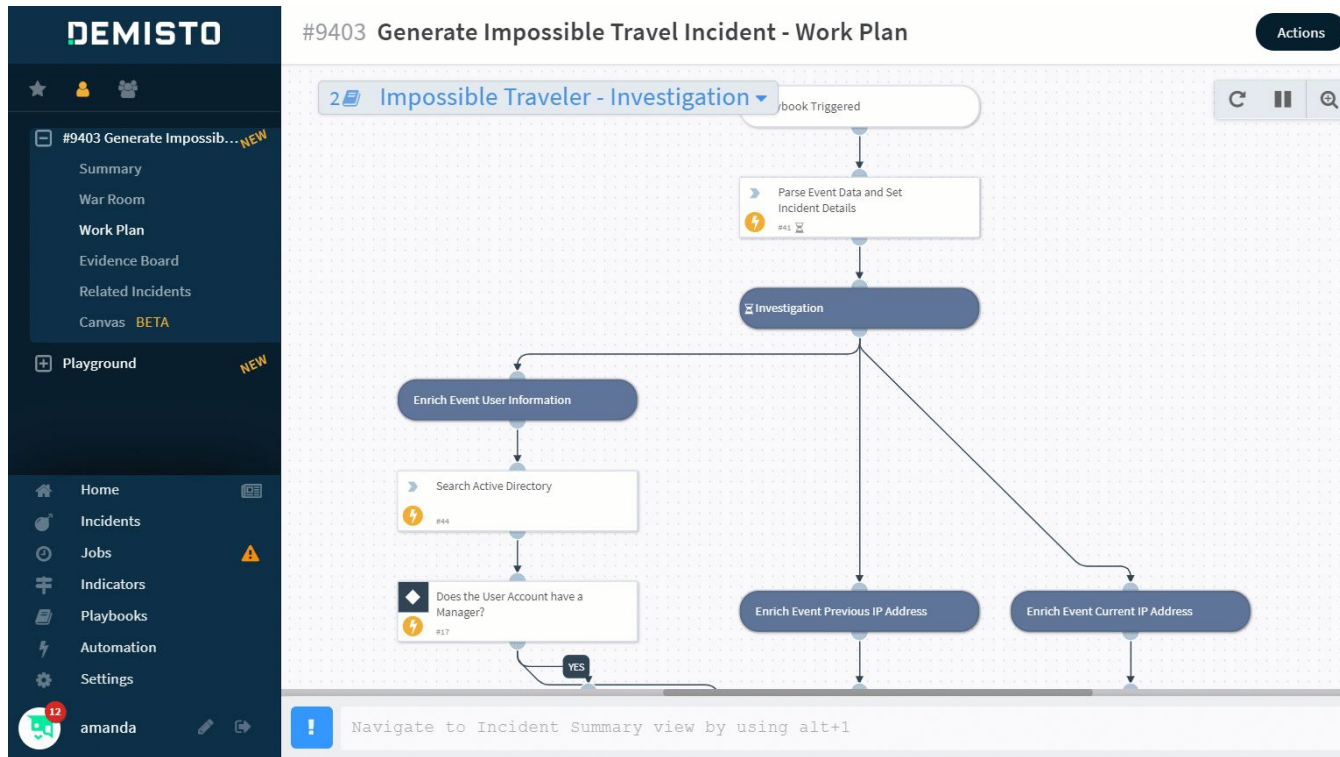
**Disparate
alert sources**

**Lack of
defined process**

**Repetitive and
manual actions**

**Lack of product
interconnectivity**

After Demisto



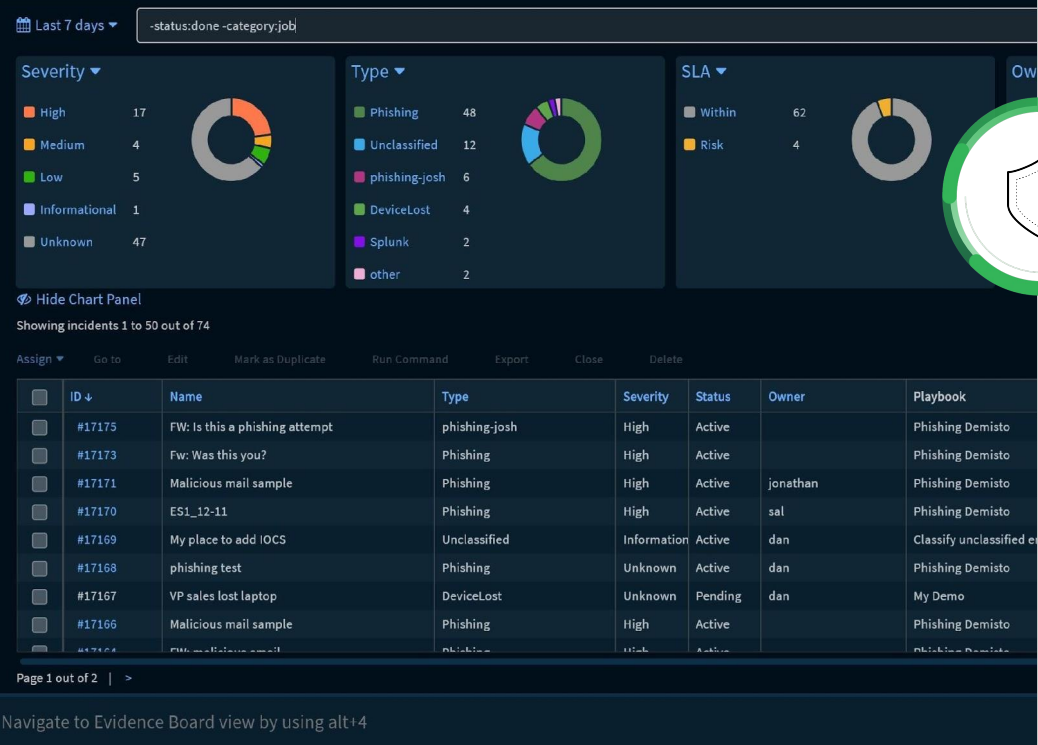
**All alerts flowing
into one console**

**Standardized
and enforceable
processes**

**Automated
high-quantity
actions**

**Cross-product
coordination**

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**




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

No filter selected

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

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

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

DBot 8:12 AM
Command: IADGetUser name="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

abbishekiyer 8:13 AM

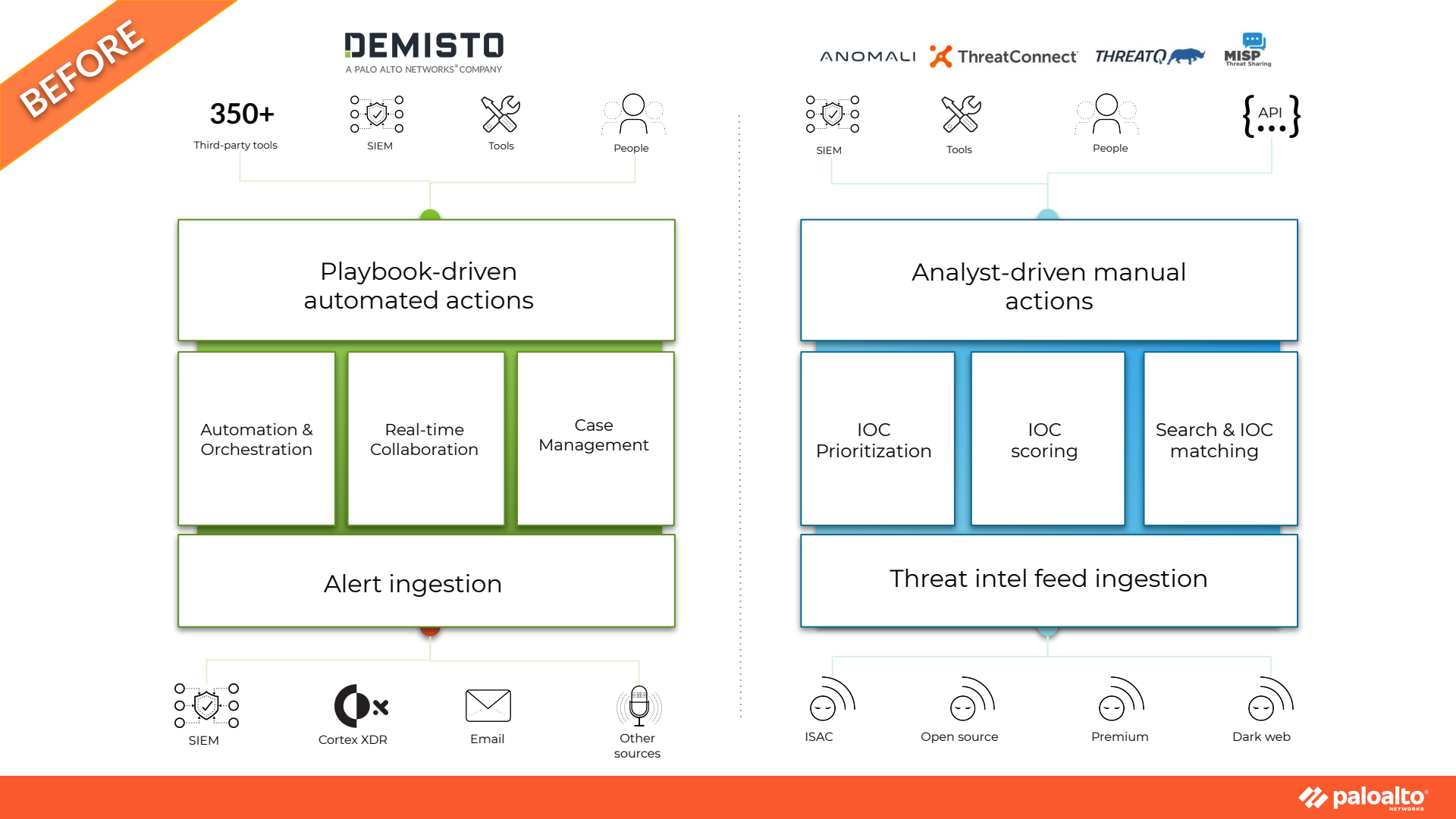
Navigate to Incident Summary view by using alt+1



Cortex XSOAR is a collaboration platform

Improve investigation quality by working together

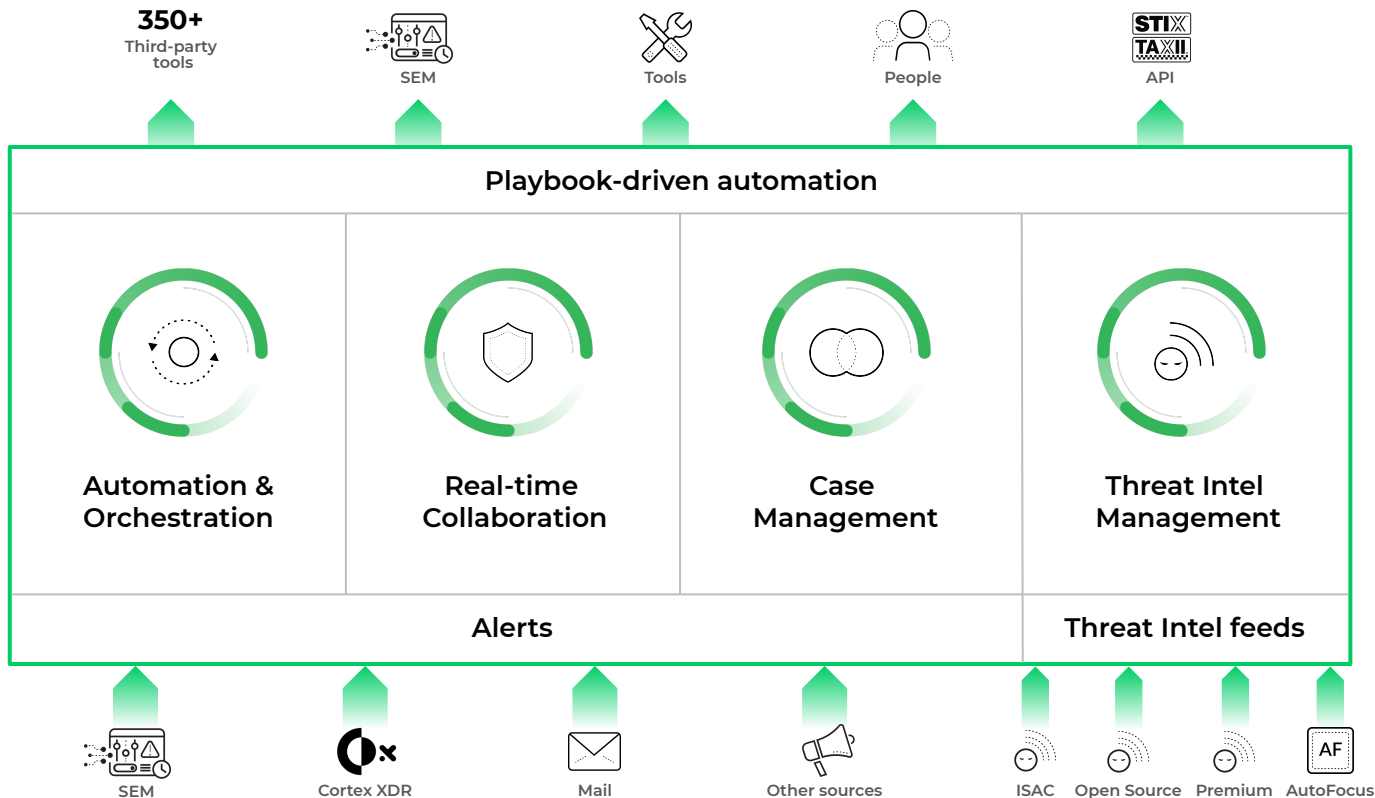
- **Virtual War Room** for every incident
- **ChatOps & real-time** security actions
- **Auto-documentation** of playbook & analyst actions

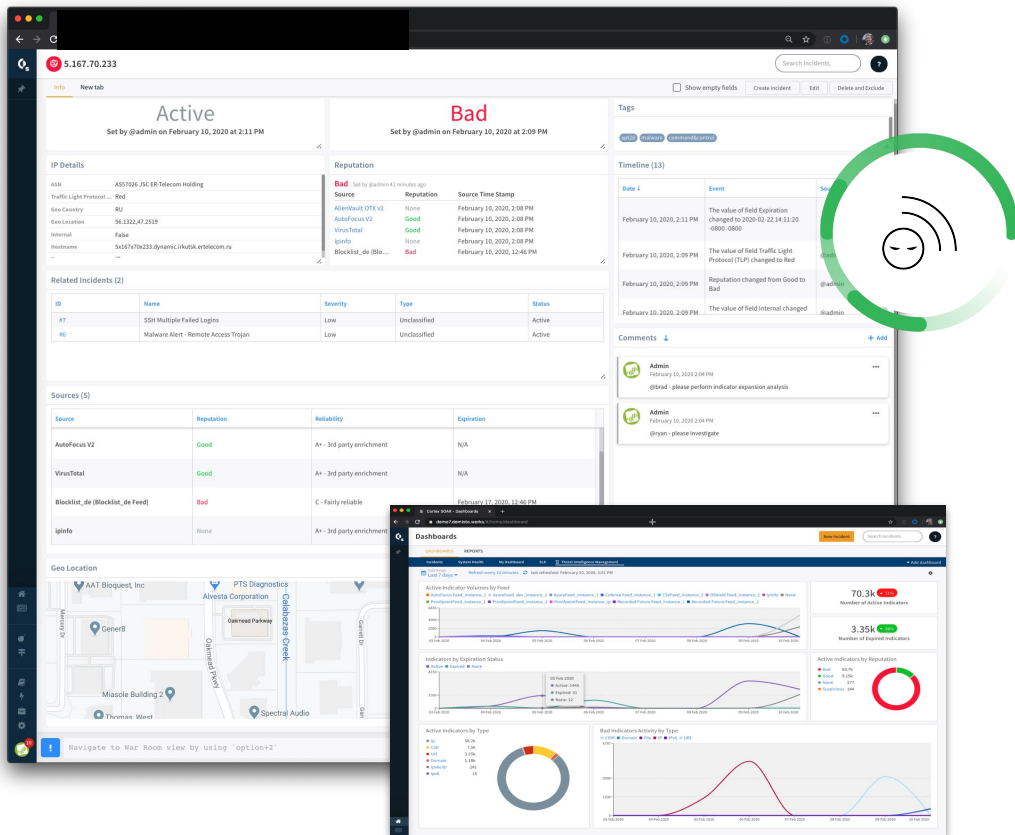


AFTER

CORTEX XSOAR

BY PALO ALTO NETWORKS













































































Cortex XSOAR is a threat intel management platform

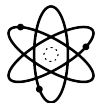
Take full control of your threat intel feeds

- **Automate** repetitive daily indicator management tasks
- **Get Instant ROI** from existing threat intel feeds
- **Gain confidence** in incident response decisions

Breadth of Cortex XSOAR integrations (400+)

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

Get smarter with each incident



DBot learns from historical actions



Suggest incident assignments



Identify experts for each type of incident

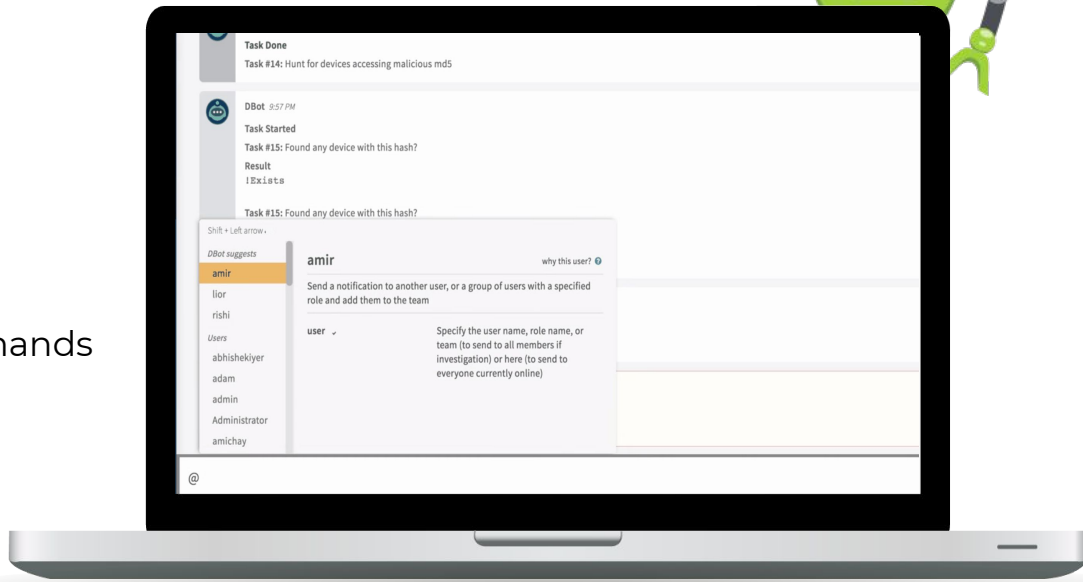


Suggest commonly used commands during investigation



Identify related and duplicate incidents

DBot: Force multiplier
for your analysts



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



Thank you