For internal use only

DEMISTO
A PALO ALTO NETWORKS® COMPANY

DEMISTO BATTLECARD

At a Glance

Respond to incidents with **speed and scale**

Standardize processes across products and teams

Improve investigation quality by **working together**

Get smarter with every security incident

Intelligent Automation

- Playbooks primed for automation with 100s of integrations and 1000s of security actions.
- Engage analysts through manual tasks and end users through mail response and analysis.
- Visual playbook editor with flexibility to create new playbook tasks, nest, and carry over.
- High availability and failover, easy to troubleshoot and start over from any point in the playbook.
- Machine-powered suggestions for related incidents and common indicators across incidents.

Incident Management

- Six different persona-based incident views.
- Full customization: incident and indicator types, labels, layouts, automations, and more.
- Auto-documentation of all incidents and investigations for comprehensive SLA tracking.
- Evidence timeline to enable incident reconstruction.
- Customizable dashboards and reports with widget library to quantify performance, gain metric visibility.
- Windows/Mac/Linux OS dissolvable agents to collect data from endpoints.

Threat Management and ML

- Central indicator repository with auto-detection and STIX import., intuitive search and query capabilities.
- Historical correlation of all indicators across incidents.
- Ability to schedule playbooks for threat hunting.
- **Machine Learning:**
- Simplified workflow creation through playbook task parameter suggestions.
- Enhance analyst productivity through incident ownership/expert/security command suggestions.
- Improve enrichment through related and duplicate incident detection.

Interactive Investigation

- ChatOps-powered virtual 'War Room' where analysts can collaborate in real-time and run security actions.
- Related Incidents investigative toolkit that provides customizable map of related incidents across time.
- In-house security bot (DBot) that helps run commands, suggests analyst ownership and future course of action.
- Externally installable chatbot that allows mirroring investigations on Slack.
- Evidence gathering and auto-documentation with rich text markdown and highlightable notes.

Elevator Pitch

Demisto Enterprise is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines full case management, intelligent automation, and collaborative investigation to serve security teams across the incident lifecycle. Demisto helps SOCs reduce alert fatigue, improve analyst productivity, and run more efficient security operations.

Value to the Business

- Reduce response times.
- Lower alert volume.
- Increase security team productivity.
- Improve return on existing security investments.

SOAR Drivers

Rising security alerts	Security teams review **12,000 alerts per week** on average[1]. High volume of false positives is a related challenge.
Skills shortage	Security analysts are tough to hire, train, and retain. It takes **8 months** to train new security analysts, and **25% of them leave within 2 years**[1].
Product proliferation	Security teams need to use a variety of tools, each with different context and value. Coordinating among these tools involves tab switching and dead time.
Piecemeal processes	Over **50% of security teams polled either don't have processes, or rarely update the processes they have**[1]. This leads to increased error rate, quality variance, and lack of compliance.
Lots of data but little follow-up	Security products provide lots of granular data but there's rarely a way to drive that data to response. "We have all this data. So what?"

Popular SOAR Use Cases

Phishing enrichment and response	IOC enrichment across sources
Malware analysis	Rapid IOC hunting
Failed login checks	Logins from unusual locations
Vulnerability management	Endpoint protection (quarantining)
Setting incident severity	Endpoint diagnostics and kickstart
Cloud security actions (security group management, deprovisioning instances)	Firewall management (changing rules, adding IOCs to blacklists)

SOAR Benefits

Unify security infrastructures: Coordinate enrichment and response by gathering intelligence from multiple products on a single console.

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

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

Increase analyst productivity: SOAR frees up analyst time for more important decision-making, proactive tasks, and charting future security improvements rather than getting mired in grunt-work.

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

Customer Success Stories

- Esri used Demisto playbooks to **reduce alert volume by 95%**.
- An app development customer was able to reduce average times for a process from **4 hours to 10 minutes** using a Demisto playbook.
- A Fortune 500 pharma company used Demisto's phishing email classifier to detect **90% of incoming phishing emails**.

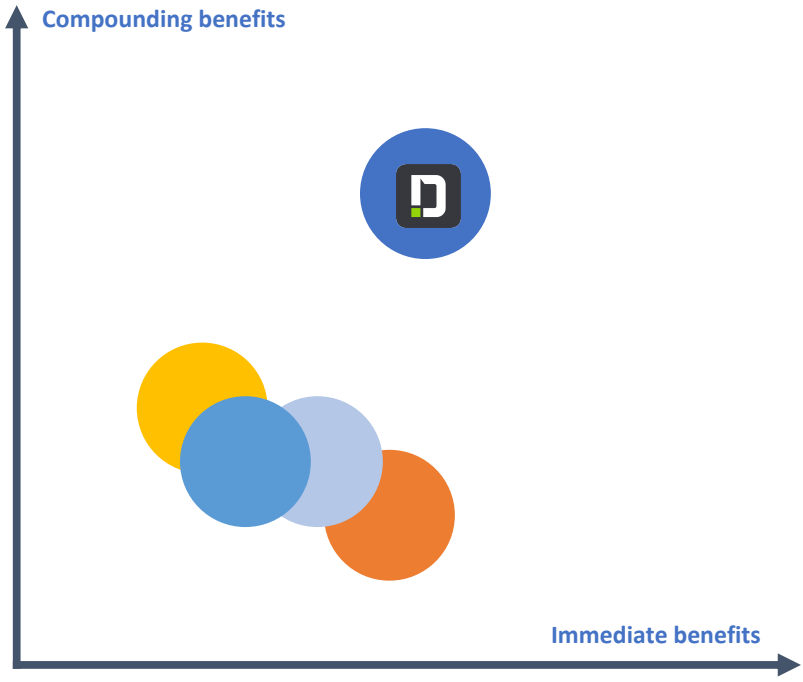
DEMISTO
A PALO ALTO NETWORKS® COMPANY

Competitive Landscape

Incident Response Platforms	Ticketing Systems	SIEMs with Automation	Homegrown / Generic
Phantom Swimlane CyberSponse Siemplify	IBM Resilient ServiceNow Remedy HP ServiceManager	Splunk + Phantom LogRhythm Exabeam JASK	The Hive MISP Spreadsheet tool Email

Demisto Differentiators

Unified Platform	Interactive Investigation	Continuous Learning
More capabilities for the same price (orchestration, incident management, collaboration) on one platform.	Virtual War Room enables real-time collaboration, command execution, and documentation.	Demisto's machine learning helps increase analyst productivity and efficiency of SecOps with personalized suggestions.
Transparent Pricing	**Architecture Security**	**Flexible Deployment**
Demisto's user-based pricing doesn't charge for any actions (automations) and aligns with predicted budgets.	Demisto's code is written and executed in dockers, ensuring maximal security and privacy.	Demisto can be deployed on-premise or hosted on the cloud. It's also available as a multitenant solution.
Flexible Automation	**Customizability**	**Indicator Management**
Demisto playbooks can have automated and manual tasks, engage end users, and are easy to nest/troubleshoot.	Create new incident types/fields, indicator types/fields, summary layouts, dashboards, and reports.	Demisto automatically captures indicators tied to incidents, correlates them, and is primed for threat hunting operations.



Immediate and compounding value

Immediate
- Flexible deployment
- Intuitive visual automation
- Extensible partner network
- Internal SDK for custom integrations
- OOTB playbooks

Compounding
- Machine learning
- Customizable incident management
- Granular performance measurement
- Use cases outside of IR: SecOps, cloud security, IT operations
- Horizontal scalability
- Bimonthly content updates
- Agile product enhancements

Target Buyers and Decision Makers	Security analyst (Tiers 1-3), SOC manager, Incident responder, CISO

Objection Handling and FAQs

We don't need automation.	- Besides automation, Demisto's platform has **incident management** and **collaboration**, resulting in a complete tool for security operations. - Demisto playbooks can be **fully manual** as well.
We already have Splunk, so why should we not go with Splunk + Phantom?	- Demisto is a better SOAR solution than Phantom has a very good Splunk integration. - Many existing Demisto customers use Splunk. - Better than Phantom: Flexible automation; Collaboration; Machine Learning; User-based Pricing; Code in Docker
We already have an in-house / homegrown solution.	- These tools are difficult to maintain and scale with time, and don't adapt to new technologies quickly. - Demisto can integrate with your homegrown tool to begin with and plug in any gaps. - Manual playbooks in Demisto are easier to reuse, transfer, and are primed for eventual automation. - Demisto provides support for transfer of in-house playbooks (if and when you transfer).
Tool X has more integrations than Demisto.	- Demisto has 100s of integrations and counting. We add new integrations every 2 weeks. - If there's user/customer need, we can add a new integration in 2-3 days. - Through **BYOI (Build Your Own Integrations)** and the PyCharm plugin, users can add their own integrations.
We have enough tools, we don't need another tool.	- Demisto acts as a central hub for your security operations and unifies actions across all other security products in your SOC. - Using Demisto enables you to get the **best out of existing security investments**.
We're only looking for a ticketing system right now.	- Demisto has full-fledged incident management and ticketing that's dynamic (customizable), can adapt to emerging threats (mobile app), and connects with all the tools in your security stack. - This incident management is closely tied with automation and orchestration, enabling your SOC to mature.
This will create more work for my team.	- Automated playbooks **reduce alert volume**, false positives, and the need to perform redundant tasks, freeing up analyst time. - War Room enables collaboration and joint investigations, **reducing analyst rework**.
We are not a Palo Alto Networks shop, so we won't get value from Demisto.	- Demisto has an **extensible and neutral** integration network with 100s of integrations and 1000s of security actions across products. We already integrate (or will do so) with any product you use, whether it is a Palo Alto Networks product or not.