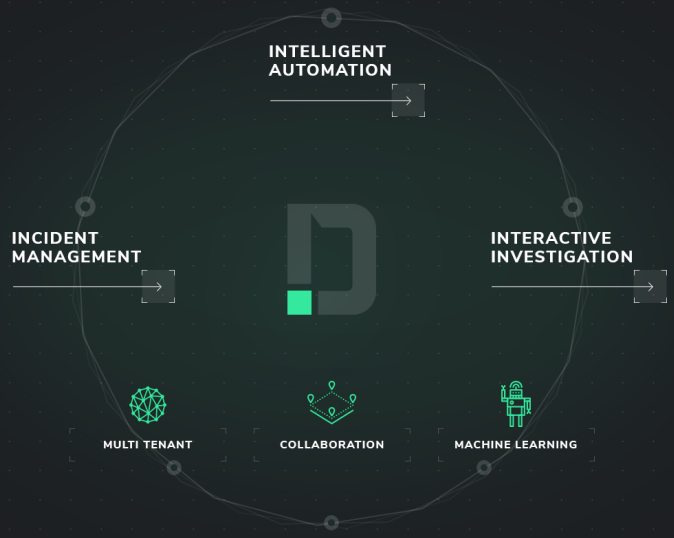
DEMISTO ENTERPRISE FOR INCIDENT MANAGEMENT



The Connecting Fabric For Your Security Infrastructure And Teams

Complete Incident Management: Comprehensive SLA tracking and metrics, evidence collection and journaling, regulatory compliance

Primed for Full Customization: Custom incident types and fields, ingestion from multiple sources, flexible playbooks for process workflows, bespoke searches and queries

Continuous Improvement and Learning: Machine learning powered insights on incident owner/task assignment, related incidents, false positive and duplicate detection

Incident Management, Reimagined

In this landscape of ever-evolving and complex threats, SOC employees face challenges across the board. One major challenge is finding a balance between standardized incident response for high-quantity attacks and customized response for sophisticated, one-off attacks.

There is also a lack of focus on continuous improvement and learning, with most of the time being spent fighting daily fires.

This is where Demisto Enterprise for Incident Management comes in.

Our full incident management capabilities weave in security orchestration and automation for quicker triage, response, and coordination in the face of rising attack numbers.

KEY BENEFITS

Consistent, Transparent, and Documented Processes

- Playbook-driven response actions and investigation queries.
- Auto-documentation of all investigations and historical searches.
- Search across investigations, indicators, and evidence.
- Granular tracking of incident and analyst metrics.

Tailored Incident Response and Monitoring

- Custom incident ingestion rule sets and sources.
- Unique incident-specific fields, views, and response workflows.
- Analyst-level tracking of task assignment and response actions.
- Quick pivot searches and queries to focus on incident subsets.

Improved Analyst Productivity and Enhanced Team Learning

- Visual maps of related incidents for quick detection of duplicates.
- Collaborative platform allows analysts to share insights and information.
- ML-powered insights for task-analyst matching, ownership, and response actions.
- Enables analyst training based on past investigations.

Flexible and Scalable Deployment

- Solution available as SaaS or on-premise deployment.
- Supports full multi-tenancy with data segregation and scalable architecture.
- Engine proxy to handle segmented networks.
- Chatbot installable in non-Demisto chat systems (Slack mirroring).

A high focus on customization – from granular metrics and response workflows to incident types and reports – allows users to tailor response to attack types. Machine learning insights also prime users for continuous learning, with suggestions for incident ownership, task assignment, related incidents, and indicator cross-correlation.

Complete Incident Management

Demisto's platform manages all aspects of the incident lifecycle:

- Open and extensible platform of 140+ integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, and more.
- Intuitive drag-and-drop playbooks to automate SOC processes and standardize workflows.
- Auto-documentation of all incidents and investigations for comprehensive SLA tracking.
- Central indicator repository that enables pivoted searches around indicators and threat hunting exercises.
- Windows/Mac/Linux OS dissolvable agents to collect data from endpoints.

Customization Across Incident Lifecycle

Demisto's end-to-end flexibility lets users tailor response to attack:

- Custom incident types, streamlined ingestion, and classification make Demisto a powerful central alerts repository.
- Custom incident fields, indicator types, and indicator fields result in SOC agility, increase reaction effectiveness.
- Strong search and query capabilities that enable quick drill-down into incident subsets.
- Comprehensive dashboards and customizable reports to quantify performance and archive results.

Intelligent Automation and Orchestration

Demisto's incident management dovetails with orchestration and involves an ideal interplay between people, process, and technology:

- Playbook portfolio primed for automation with 140+ integrations and 400+ security actions.
- Dynamic playbooks that engage analysts through manual tasks and end users through mail response and analysis.
- Flexibility to create new playbook tasks/blocks and carry them over across playbooks.
- Playbooks have high availability and failover, easy to troubleshoot and start over from any point in the playbook.

Continuous Learning

Demisto's machine learning base powers proactive improvement and decreases resolution time:

- 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 incident ownership, and task assignment.
- Externally installable chatbot that allows mirroring investigations on Slack.
- Evidence gathering and auto-documentation with rich text markdown and highlightable notes.

DEMISTO FOR INCIDENT MANAGEMENT

Unified Platform

Complete platform unifying incident management, security orchestration, and collaboration

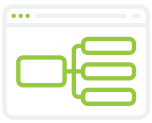
Full Customizability

Flexibility in ingestion sources, incident types, incident fields, response playbooks, and reports

Continuous Learning

ML-powered insights for incident ownership, analyst-task matching, and analyst actions

Flexible Deployment



On-premise and SaaS deployments with full multi-tenancy and three layers of isolation

Intelligent Automation

Interweaving automated and manual tasks through playbooks with 140+ integrations and 400+ actions

SLA Confidence

Auto-documentation with full SLA tracking, granular analyst and incident metrics, dashboards and reports

System Requirements

Demisto Enterprise Server:

- Physical or virtual server
- Linux OS: Ubuntu 14.04 and 16.04, Centos 7.x (ask us about other distros and versions)
- 8GB RAM minimum (16GB desired)
- 8 CPU cores minimum (16 desired)

Demisto Engine:

- Linux OS: Ubuntu 14.04 and 16.04, Centos 7.x (ask us about other OSs, distros and versions), Windows
- 4GB RAM minimum
- Dual core CPU minimum

About Demisto

Demisto helps Security Operations Centers scale their resources, improve incident response times, and capture evidentiary support while working and solving problems the way humans are wired to – together. Demisto Enterprise is the first comprehensive, Security Operations Platform to combine intelligent automation with collaborative, human social learning and experience. Demisto's intelligent automation is provided by DBot which works with your team via a new concept, Security ChatOps, for fully automated, playbook-based workflows, cross-correlation, information sharing and curation from investigation-through-response and beyond. Demisto is backed by Accel with offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.