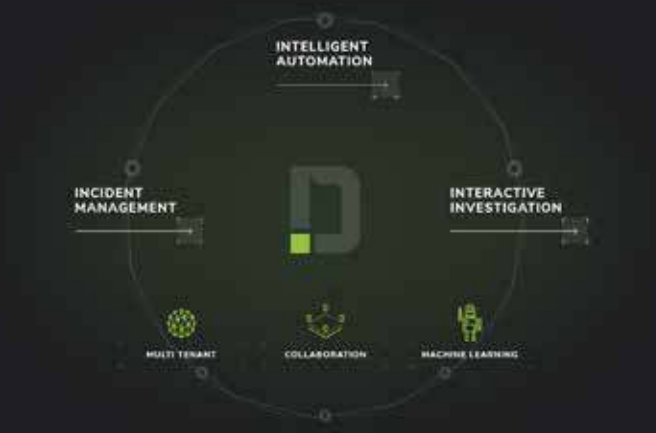
DEMISTO ENTERPRISE

DEMISTO



The Operating System for Enterprise Security

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

Intelligent Automation and Orchestration: Automatable playbooks, allows for end user and analyst participation, high availability and failover, cross-correlations

Interactive Investigation: ChatOps-powered War Room, investigative toolkit for related incidents, real-time analyst collaboration and hand-offs

Flexible and scalable deployment: Solution available as cloud-hosted 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 SOC's Challenges

In this landscape of ever-evolving and complex threats, SOC employees face challenges across the board. Tier-1 analysts are drowning in alerts and performing time-consuming tasks like weeding out false positives, actioning repetitive responses, and keeping up with alerts from disparate security tools.

KEY BENEFITS

Consistent, transparent, and documented processes

- Playbook-driven response actions and investigation queries
- Auto-documentation of all investigations and historical searches
- Automatic detection of duplicate investigations
- Search across investigations, indicators, and evidence

Quicker resolution times and better SOC efficiency

- Customizable playbook portfolio to automate redundant and repeatable steps
- Virtual "War Room" for joint, real-time investigations
- Granular tracking of incident and analyst metrics

Improved analyst productivity and enhanced team learning

- Collaborative platform allows analysts to share insights and information
- Enables analyst training based on past investigations
- ML-powered insights for task-analyst matching, response actions, and linked incidents

Tier-3 analysts are faced with the challenge of finding contextual needles in haystacks of noise. They find it difficult to coordinate the multiple security products at their disposal in the most effective way. Amidst this workload, they can't find time to train junior analysts and bring them up to speed.

SOC Managers have trouble in quantifying the ROI that security tools bring to their SOC. They also constantly face SLA pressures in the face of incomplete metric tracking and documentation. Finally, the threat of the analyst skills gap always hangs over their head; any senior analyst leaving the organization can result in a fatal loss of expertise and a step back for the SOC.

This is where Demisto Enterprise comes in – a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines incident management, intelligent automation and orchestration, and interactive investigation to serve security teams across the incident lifecycle.

Complete Incident Management

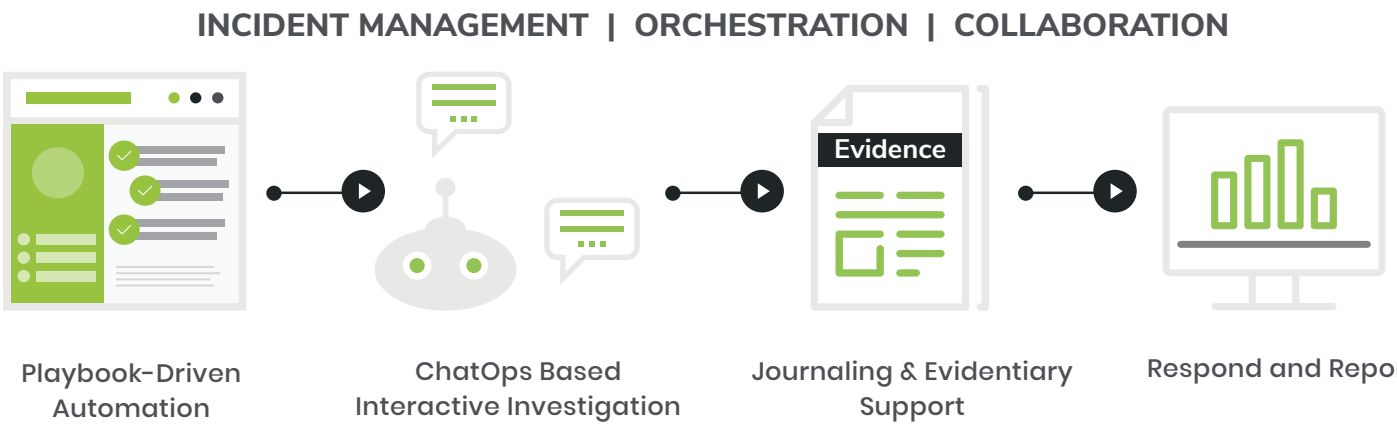
Demisto's platform helps you manage all aspects of the incident lifecycle:

- Open and extensible platform powered by 100s of 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 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.
- Strong search capabilities that provide auto-detection of duplicate and related investigations.
- Comprehensive dashboards and customizable reports to quantify performance and archive results.
- Windows/Mac/Linux OS dissolvable agents to collect data from endpoints.
- Mobile application providing personalized dashboards, task lists, and executable incident actions on the go.

Intelligent Automation and Orchestration

Demisto's orchestration involves the ideal interplay between people, process, and technology:

- Playbook portfolio primed for automation with 100s of integrations and 1000s of 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; it's simple to troubleshoot and start over from any point in the playbook.
- Machine-powered suggestions for related incidents and common indicators across incidents.



Interactive Investigation

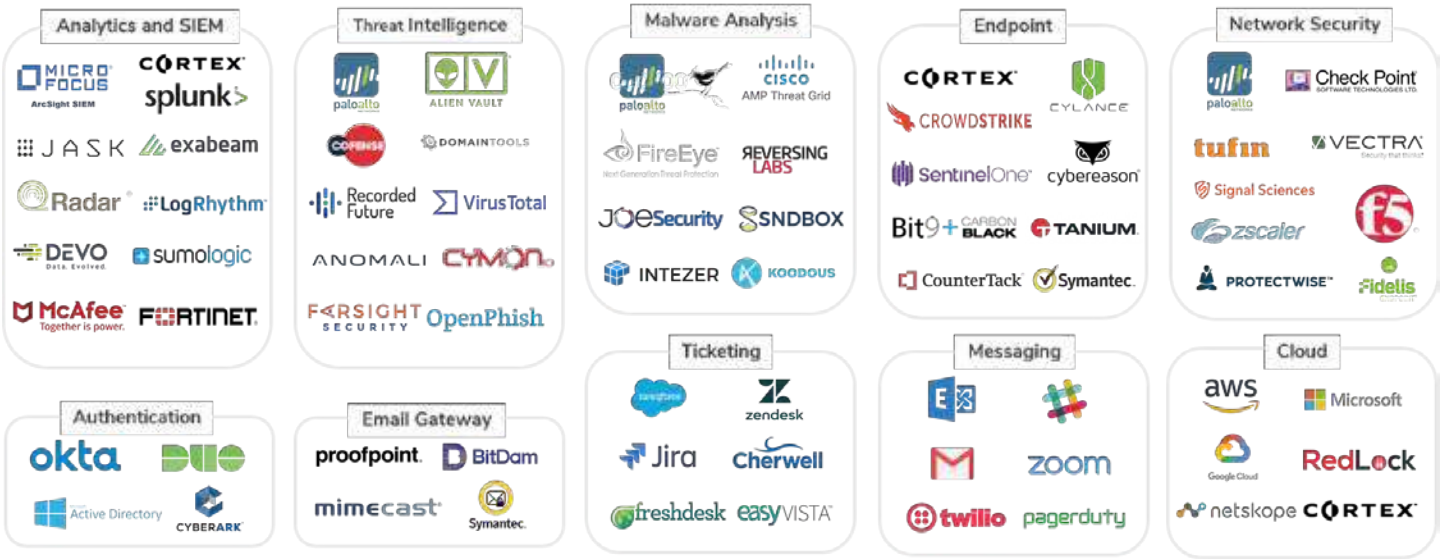
Demisto's interactive investigation features help analysts collaborate productively and get smarter with each incident:

- 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.
- Evidence gathering and auto-documentation with rich text markdown and highlightable notes.

Machine Learning Powered DBot

In addition to solving a SOC's current, pressing problems, Demisto Enterprise also leverages the power of machine learning through DBot to act as a force multiplier and prime SOCs for the future. ML-supported suggestions are present in incident ticketing, task-analyst matching, response actions, analyst ownership, and related incidents. Machine learning cuts across all three pillars of incident management, intelligent automation and orchestration, and interactive investigation. As both DBot and analysts grow smarter with each incident, the marginal time to predict, contain, and respond to threats decreases.

Some of our Integrations...



...AND MORE!

System Requirements

1. Demisto Server:

Operating System Requirements

Demisto server is compatible with several Linux operating systems. Verify which operating systems are supported for your version of Demisto.

	v3.6	v4.0	v4.1	v4.5
CentOS	✓	✓	✓	✓
Ubuntu 14.04	✓	✓	✓	✓
Ubuntu 16.04	✓	✓	✓	✓
Ubuntu 18.04	✗	✗	✓	✓
Ubuntu 18.10	✗	✗	✓	✓
RHEL v7.x	✓	✓	✓	✓
Oracle Linux	✓	✓	✓	✓
Amazon Linux 2	✓	✓	✓	✓
SUSE Enterprise	✓	✓	✓	✓
openSUSE	✓	✓	✓	✓
Fedora	✓	✓	✓	✓

IMPORTANT:

- RHEL and Oracle Linux require Docker Enterprise Edition (Docker EE).
- Ubuntu 14.04 requires Linux kernel 4.x.

Hardware Requirements

Component	Minimum	Recommended
CPU	8 CPU cores	16 CPU cores
Memory	16 GB RAM	32 GB RAM
Storage	500 GB SSD	1 TB SSD with minimum 3k dedicated IOPS

2. Demisto Engine:

Operating System Requirements

Demisto Engine is compatible with Windows, Mac, and Linux operating systems. Verify which operating systems are supported for your version of Demisto.

	v3.6	v4.0	v4.1	v4.5
MacOS	✓	✓	✓	✓
Windows	✓	✓	✓	✓
Linux	✓	✓	✓	✓

Hardware Requirements

Component	Minimum	Recommended
CPU	8 CPU cores	16 CPU cores
Memory	16 GB RAM	32 GB RAM

About Demisto

Demisto, a Palo Alto Networks company, is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform that combines playbook orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com

Want to find out more?

To learn more, speak to a member of the Threatscape team via info@threatscape.com or on 0203 653 0000 (UK) or 01 901 7000 (Ireland)

Threatscape