DEMISTO

Company Overview

From the War Room to the Board Room

Improve Security Incident Response

About Demisto

Demisto has your back in the war against hacker attacks.

Security teams must battle a growing number of complex incidents with fewer resources, while facing increasing pressure from executives to protect the company brand.

But you will win the war with your **secret weapon**: Demisto.

The Demisto platform scales incident investigation, response and reporting by:

- Providing a **comprehensive Incident Case Management** system with SLA management, analyst assignments and metrics tracking,
- Enabling **full incident automation** where appropriate and providing a clearly **defined workflow via a playbook** which analysts use to document the investigation
- Empowering analysts with effective **collaboration** and **machine learning** based suggestions.

Risk Reduction

By using Demisto, the volume of alerts requiring active human review can be reduced by as much as **95%**. One **Demisto** customer reported taking an original incident volume of 10,000 alerts per week down to 500 or less. This leaves more time to examine more complicated events, while leaving no alert behind.

Headquarters

10061 Bubb Road, Ste. #300
Cupertino, CA 95014

Benefits

- Dramatically reduced response time
- Consistent and accurate IR process
- Increased analyst productivity
- Reduced SOC costs

Products

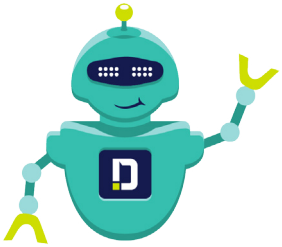
- Demisto Enterprise
- Demisto Free Edition (same great product; some limitations)

Partners

Demisto.com/partners

Product Overview

Demisto's orchestration engine is designed to automate 100's of security tasks across 100+ security products and weave the human analyst tasks and workflows with ease. Collaborative and interactive interface enables security operations team to investigate, track evidences and entire incident life cycle with a complete auditable trail. All the information captured as part of the investigation is indexed and available at analyst's fingertips to hunt and respond to threats.



Demisto Enterprise is powered by DBot, that learns from the real-life analyst interactions and past investigations in customer environment. Machine learning powered DBot enhances security operations by helping SOC teams with analyst assignment suggestions, playbook enhancements, incident and indicator correlation and best next steps for investigations.

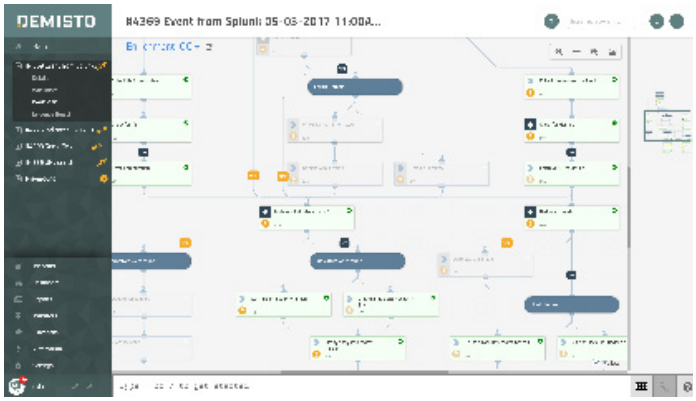


Figure 1. Demisto Enterprise Interactive playbook orchestrating security incidents.

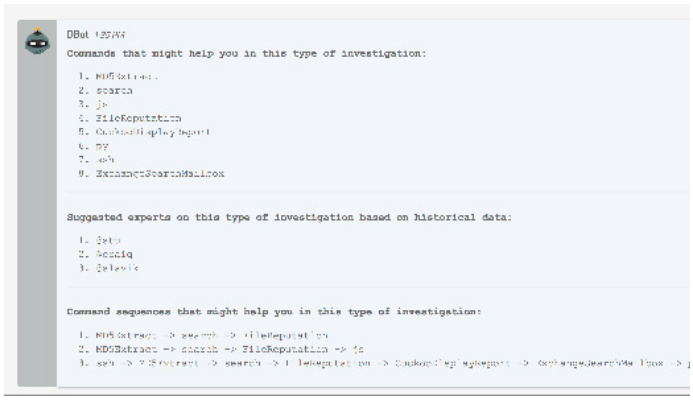


Figure 2. DBot provides machine learning suggestions so the platform (and you) get smarter with every incident.

Technology Partners

Demisto Enterprise integrates with a growing list of products, including security solutions as well as collaboration and notification platforms. By integrating with Demisto, partners enable their products with the industry's first Bot-powered security operations platform for automating playbooks and response tasks, and detecting duplicate incidents.