DEMISTO | SNDBOX

Automated Malware Analysis and Response

Benefits

- Execute SNDBOX's cutting-edge malware analysis within Demisto in real-time.
- Orchestrate SNDBOX malware analysis with other security processes through task-based playbooks.
- Reduce time to resolution by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

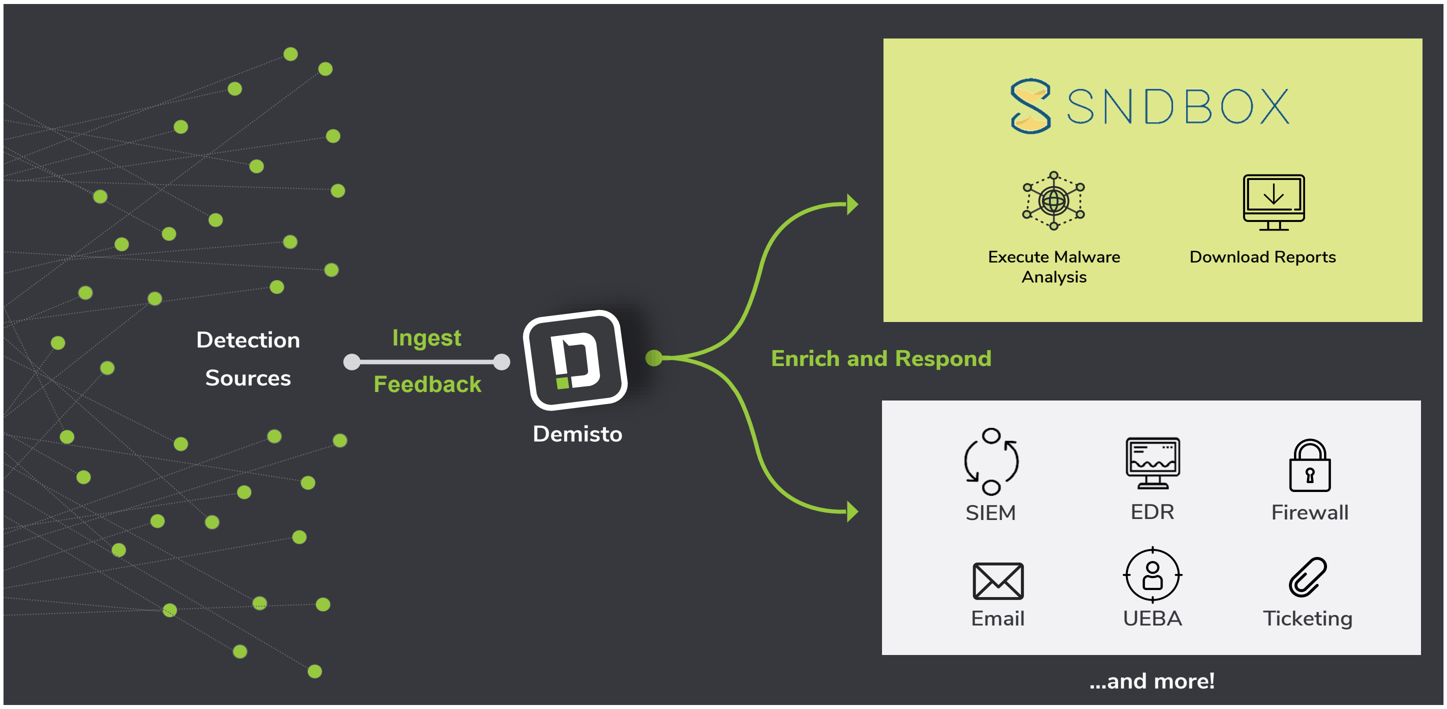
- Products: Demisto Enterprise, SNDBOX
- Platform: Platform independent

In today's security landscape, threat actors use multiple entry vectors and attack techniques to target organizations. With so many moving parts, security teams struggle to reconcile data between isolated malware analysis tools and other security products. They lose valuable time shuttling between screens and executing repeatable tasks while the attack continues to manifest. Analysts need a platform that unifies data from malware analysis products and other sources on one console, resulting in rich incident context and accelerated response without tab-switching and manual rework.

Joint users can combine SNDBOX's AI-powered malware analysis capabilities with Demisto's security orchestration and automation features to standardize their response processes, increase analyst productivity, and reduce time to detection and remediation.

Integration features

- Orchestrate SNDBOX malware analysis actions along with actions from other security products in one window through Demisto playbooks.
- Submit samples to SNDBOX for analysis and download reports from within Demisto in real-time.
- Leverage hundreds of Demisto product integrations to further enrich SNDBOX data and coordinate response across security functions.
- Run thousands of commands (including for SNDBOX) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



Detection Sources

Ingest

Feedback

Demisto

Enrich and Respond

SNDBOX

Execute Malware Analysis

Download Reports

SIEM

EDR

Firewall

Email

UEBA

Ticketing

...and more!

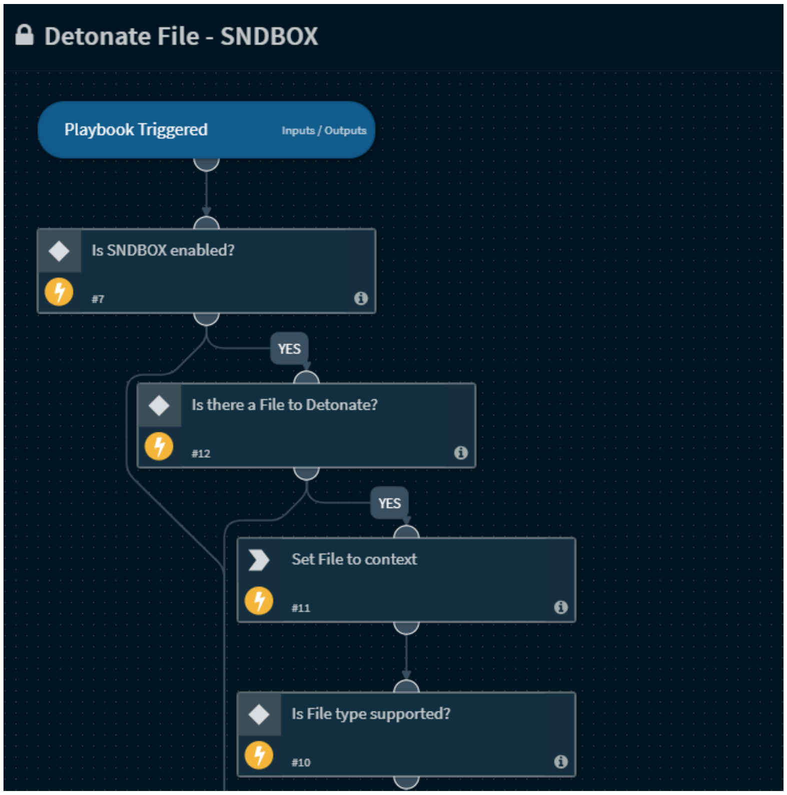
USE CASE #1

AUTOMATE MALWARE ANALYSIS AND RESPONSE

Challenge: As alert numbers grow, analysts find it tough to keep up with the repetitive, high-quantity tasks that encompass malware triage and analysis for further study. This can eventually lead to increased error rate, incomplete investigations, and alerts slipping through the cracks.

Solution: SOCs can have standardized playbooks that run automatically and query SNDBOX for malware analysis. These playbooks can perform checks to initiate triage, run detonation actions, and return the reports to the analysts for subsequent investigation. By aligning malware analysis with other concurrent security functions, these playbooks ensure that security teams have central visibility over incident response processes.

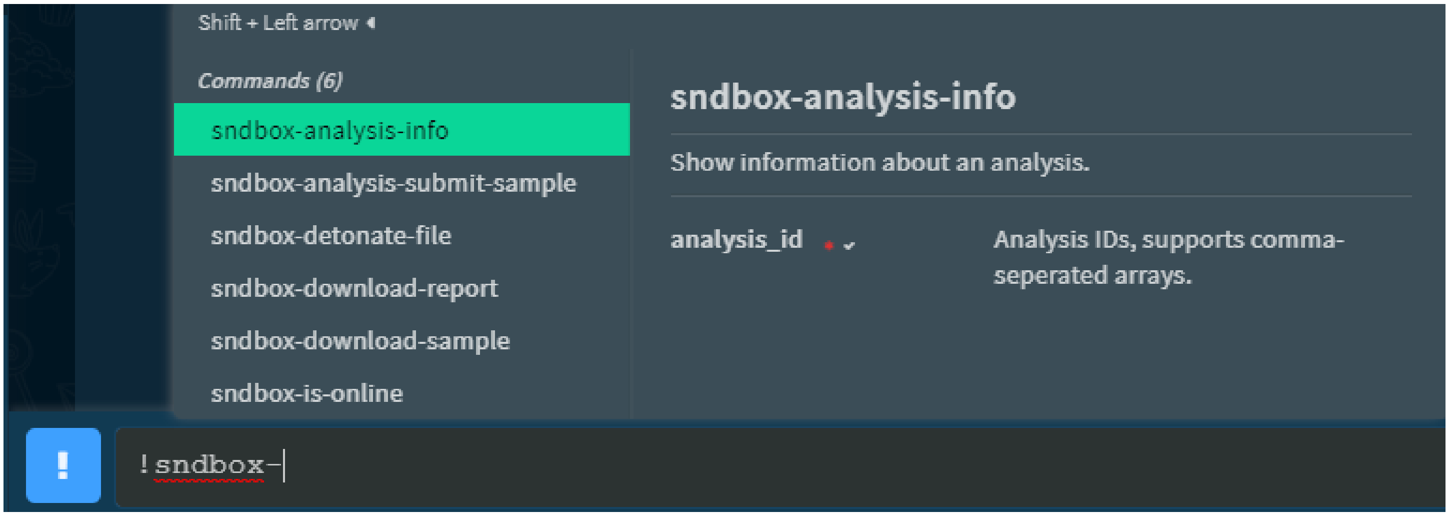
Benefit: Analysts will save time and eliminiate redundant effort by automating triage and detonation tasks, saving their energies for more nuanced and sophisticated investigation actions. This will also ensure standardized response, reduced error rate, and no alerts slipping through the cracks.



USE CASE #2 INTERACTIVE INVESTIGATIONS FOR DEEPER MALWARE STUDY

Challenge: While conducting joint investigations, analysts struggle with attaching task-level accountability, documenting actions in one source, and learning from each other's actions to reduce marginal time to incident resolution.

Solution: After playbook execution, analysts can conduct joint investigations in the Demisto War Room and run SNDBOX-specific commands in real-time. For example, analysts can run the sndbox-analysis-submit-sample command to submit a sample to SNDBOX for analysis. Security teams can also run commands from hundreds of other products in the War Room, ensuring a unified platform for collaboration, investigation, and documentation of actions.



```
sndbox-analysis-info
sndbox-analysis-submit-sample
sndbox-detonate-file
sndbox-download-report
sndbox-download-sample
sndbox-is-online
```

sndbox-analysis-info

Show information about an analysis.

analysis_id	Analysis IDs, supports comma-seperated arrays.

```
! sndbox-
```

Benefit: All participating analysts will have full task-level visibility of the process followed, be able to run and document commands from the same window, and eschew the need for collating information from multiple sources for documentation.