An Ideal Match with Gartner's SOAR Recommendations Technology Convergence

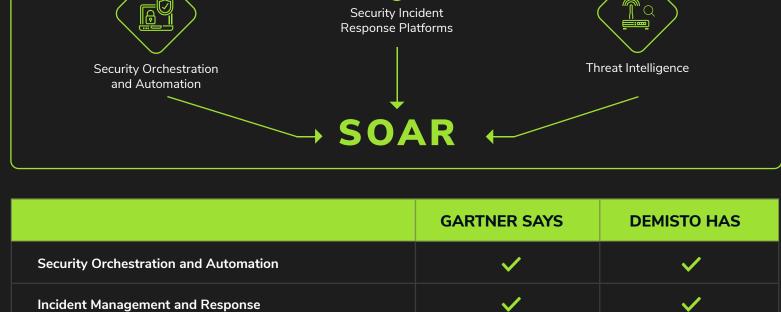
ideal SOAR solution as a convergence of three previously distinct technology markets: security orchestration and automation, security incident response platforms, and threat intelligence platforms. Demisto Enterprise is the only security operations solution with native incident management and

collaboration, security orchestration and automation, and threat intelligence woven into one platform.

Gartner has tracked the evolution of SOAR (Security Orchestration, Automation, and Response) and defines the

DEMISTO

Security Incident
Response Platforms



Threat Intelligence	~	✓
Mapping Functional Compone	ents	
Gartner has prescribed four should-have components		d summarized
capabilities within those components.		

Automation: How to make machines do task-oriented "human work".

Orchestration: How

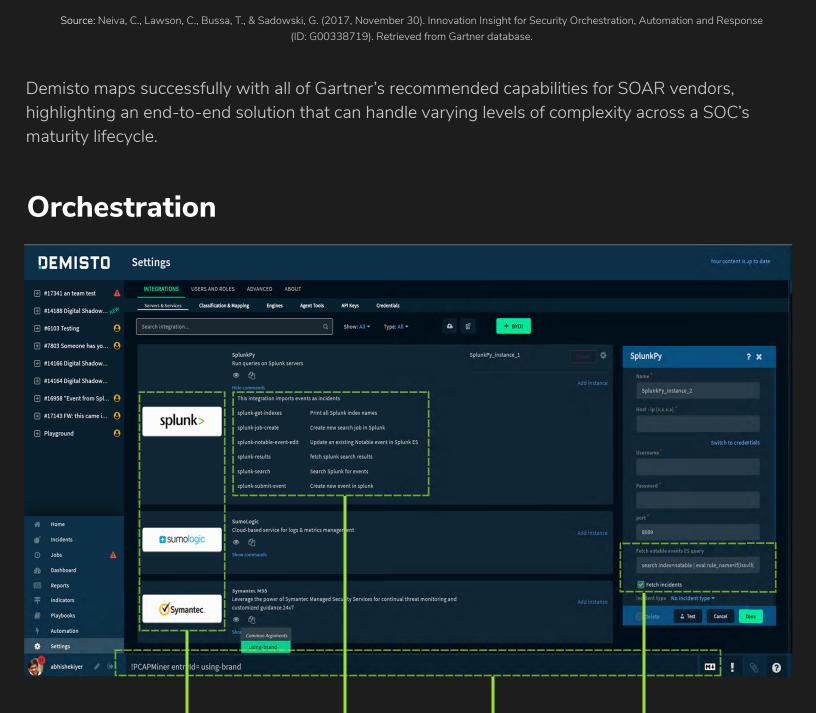
together.

different technologies
(both security-specific and non-security-specific) are integrated to work

| Collaboration: End-to-end management of an incident by people.

Dashboards and reporting: Visualizations and capabilities for collecting and reporting on metrics and other information.

Incident management and



Abstraction layer

✓ 1000s of automation

✓ Logical expressions

scriptlets invokable

Bidirectional integration

✓ Many bidirectional

pull capabilities

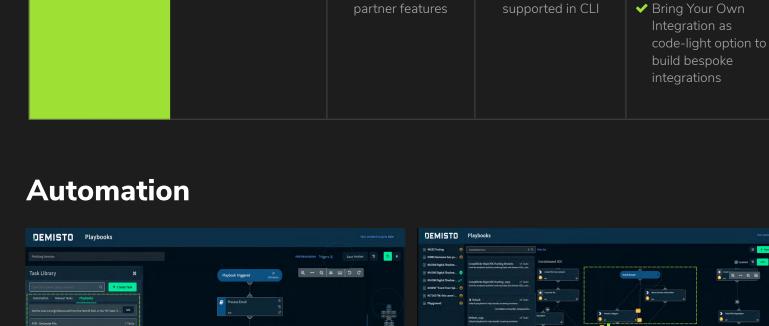
partner integrations

capability

M#

3

0



Feature-rich

integrations

✓ Multiple API calls

integration that

leverages all

(and growing) per

1

Out-of-the-box

integration connectors

Extensible network

integrations

with 100s of partner

GARTNER

RECOMMENDS

DEMISTO HAS

GARTNER

Multi-level automation Playbooks Workflows **RECOMMENDS** ✓ Playbooks interweave ✓ GUI-based drag-and-drop ✓ Full workflow capability **DEMISTO HAS** ✓ Workflows can have automated and manual tasks ✓ Ability to create custom manual ✓45+ OOTB playbooks automated and manual ✓ Open playbook standards tasks and place sub-playbooks within playbooks product functions **Incident Management and Collaboration** Journaling and Evidentiary Support DEMISTO #17113 Phishing demo 12/6_1 - Evidence Board ☐ #17113 Phishing demo. Evidence Board Attacker's server 1/1/2018 (2) (#2765) MLWR file Marked Date January 11, 2018 3:26 AM etched January 11, 2018 3:24 AM (#2742) Attacker's Ip ⊕ #6103 Testing #7803 Someone has y... (#2758) Attacker's server 12/23/2017 (1) (#2739) C2 server

DEMISTO

a

#16958 "Event from Splunk for host" - War Room

Available of the Indiana Survey along the Indi

DBot suggests

CloseInvestigation

IPReputation

LoadJSON

PCAPMiner

0

GARTNER

DEMISTO

```
Collaboration
                       Incident timeline
                                                           Historical records
  RECOMMENDS

✓ Evidence board for each incident

✓ War Room: analysts conduct

✓ Auto-documentation of
  DEMISTO HAS
                          stores key artifacts for current
                                                             playbook tasks, analyst tasks,
                          and future analysis

✓ Related Incidents with

                                                             War Room
                                                                                              security products (ChatOps)
                          time-based radial map of related
                          incidents, ability to link and map
                          duplicates
Case Management
```

ADGetUser

nestedSearch

Directory Distinguished Name (DN).

Use Active Directory to retrieve detailed information about a user

account. The user can be specified by name, email or as an Active

user query)

Enter 'true' to allow nested groups

Include these AD attributes of the

search as well (only works on a single

Active Directory Distinguished Name for

If no filter is provided, the result will show all users.

GARTNER Post-incident reviews Knowledge management Role-based access control **RECOMMENDS** ✓ Library for playbooks, ✓ Parent and child account ✓ Post-closure scripts **DEMISTO HAS** Evidence timeline to automation scripts privileges for automations, ✓ Auto-documentation of all capture key incident playbooks, incident types, actions and comments reports ✓ Customizable reports per ✓ Machine learning trains on analyst actions for insights **Analytics and Investigation Support** Task Details 0 Collect URLs from Incident? Fetch URL Reputation #27 Delete and Whitelist X Results (10) Errors (0) Inputs (1) Outputs (2) Comments (0) Bad -4 Incidents **DBot** 11:19 AM 39@17221 Go to related investigation: Select a script to execute: Task #27: Fetch URL Reputation SplunkSearch A Command: !URLReputation url= http://0551gx.cn/i9jnrc" OpenPhish Database - URL Query No matches for URL http://0551gx.cn/i9jnrc Bad url found? DBot 11:19 AM 40@17221 **Task Result** Task #27: Fetch URL Reputation Command: !URLReputation url="http://0551gx.cn/i9jnrc"

Enrich Domain

1

Unassigned 40

dan

guy shriki

GARTNER

RECOMMENDS

Basic native threat intelligence

✓ Central indicator repository with

STIX upload, auto-detection of

AlienVault url response http://0551gx.cn/i9jnrc

Incident correlation

✓ Cross-correlation of artifacts across incidents

✓ Visual map of related incidents with ability to link and mark as duplicates

DEMISTO

digital shadows_

Google

Third-party threat intelligence network

✓ Extensive threat intelligence partner network

✓ Orchestrate actions as playbook tasks or run commands

355

306

MB !

Alert - suspicio...

CISO level reporting

abhishekiyer

GARTNER

RECOMMENDS

DEMISTO HAS

Threat Intelligence

GARTNER

RECOMMENDS

DEMISTO HAS

	✓ Ability to schedule threat hunt playbooks and proactive respo		r Room
	ards and Reportin	ng	
#6103 Testing	Refresh every 10 minutes Refresh now 127 30% 67 34% 121 391% New Incidents Pending Incidents New Investigati	The state of the s	39 56% \$1.55m SLA About to End Saved by DBot
### ##################################	Re: Inv 94 Mess 19 days past SLA Re: Inv 94 Mess 19 days past SLA	Active Incidents by Type ▼ Unclassified 28 Phishing 16 DeviceLost 8 Splunk 6	Mean Time to Resolution (AVG) ② 1 10 7 DANS HOURS MIN
	SLA About to End "Event from Spl 2 days to SLA "Event from Spl 2 days to SLA "Event from Spl 2 days to SLA	□ IOCHunt 4 □ other 5	Top Closing Analyst DBot 43 sal 7 amir 5 DemoPri≠ I Top Busy Investigations (Activities)
Home Incidents	Load and SLA	Incident Types by Severity All ▼	FW: malicious e 430 Suspicious IOCs 367

26

SOC Manager level reporting

nformation2l

nknown 70

DEMISTO HAS ✓ Number/types of incidents, open/close status ✓ Number of analysts, number of incidents per analyst ✓ Efficiency metrics: MTTR, Top performing analysts, money saved through automation To see Demisto in action

Analyst level reporting

SCHEDULE DEMO

DOWNLOAD COMMUNITY EDITION