DEMISTO

An Ideal Match with Gartner's SOAR Recommendations

Technology Convergence

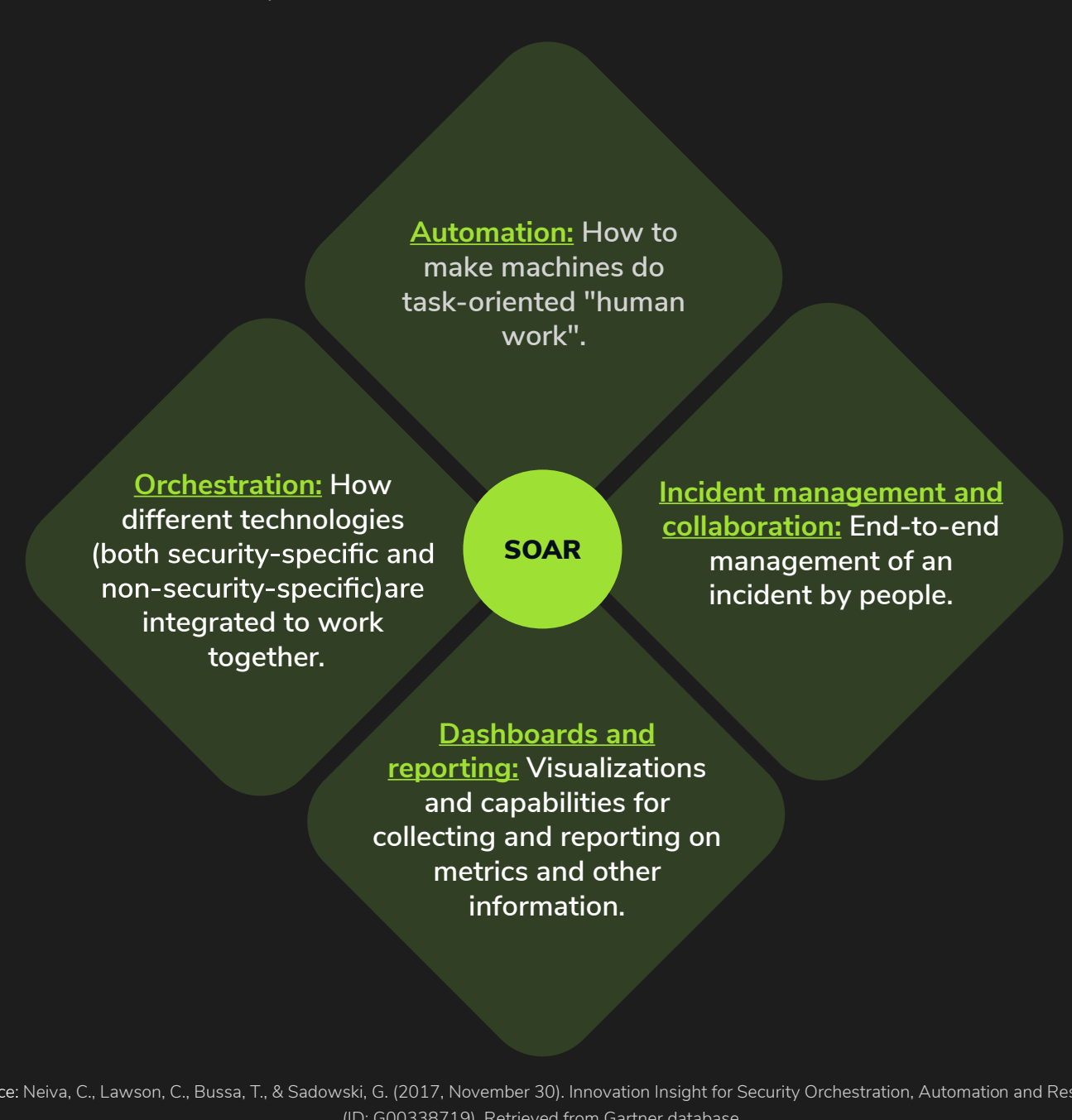
Gartner has tracked the evolution of SOAR (Security Orchestration, Automation, and Response) and defines the ideal SOAR solution as a convergence of three previously distinct technology markets: security orchestration and automation, security incident response platforms, and threat intelligence platforms.

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 SAYS	DEMISTO HAS
Security Orchestration and Automation	✓	✓
Incident Management and Response	✓	✓
Threat Intelligence	✓	✓

Mapping Functional Components

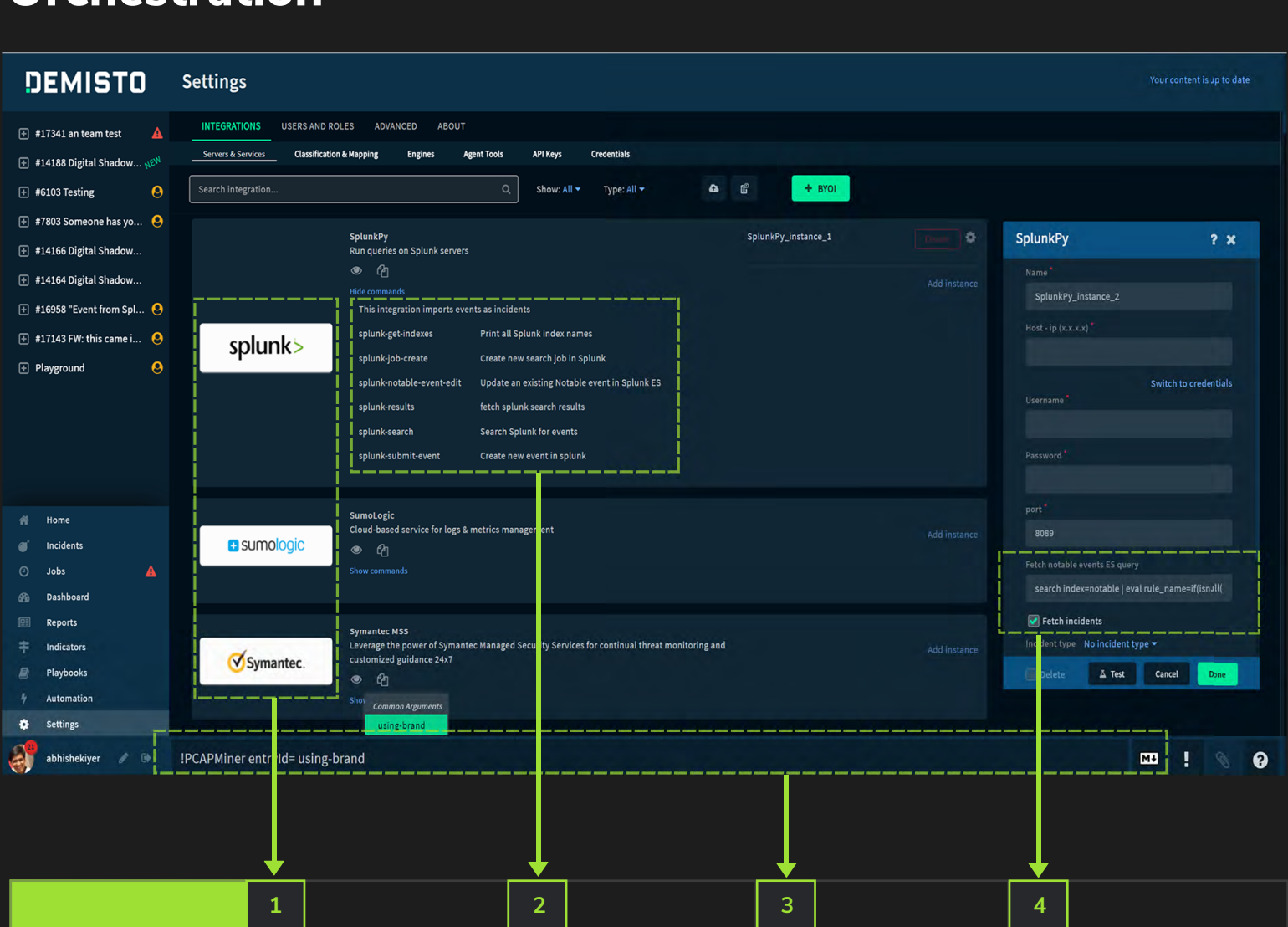
Gartner has prescribed four should-have components for SOAR solutions, and summarized capabilities within those components.



Source: Neiva, C., Lawson, C., Bussa, T., & Sadowski, G. (2017, November 30). Innovation Insight for Security Orchestration, Automation and Response (ID: G00338719). Retrieved from Gartner database.

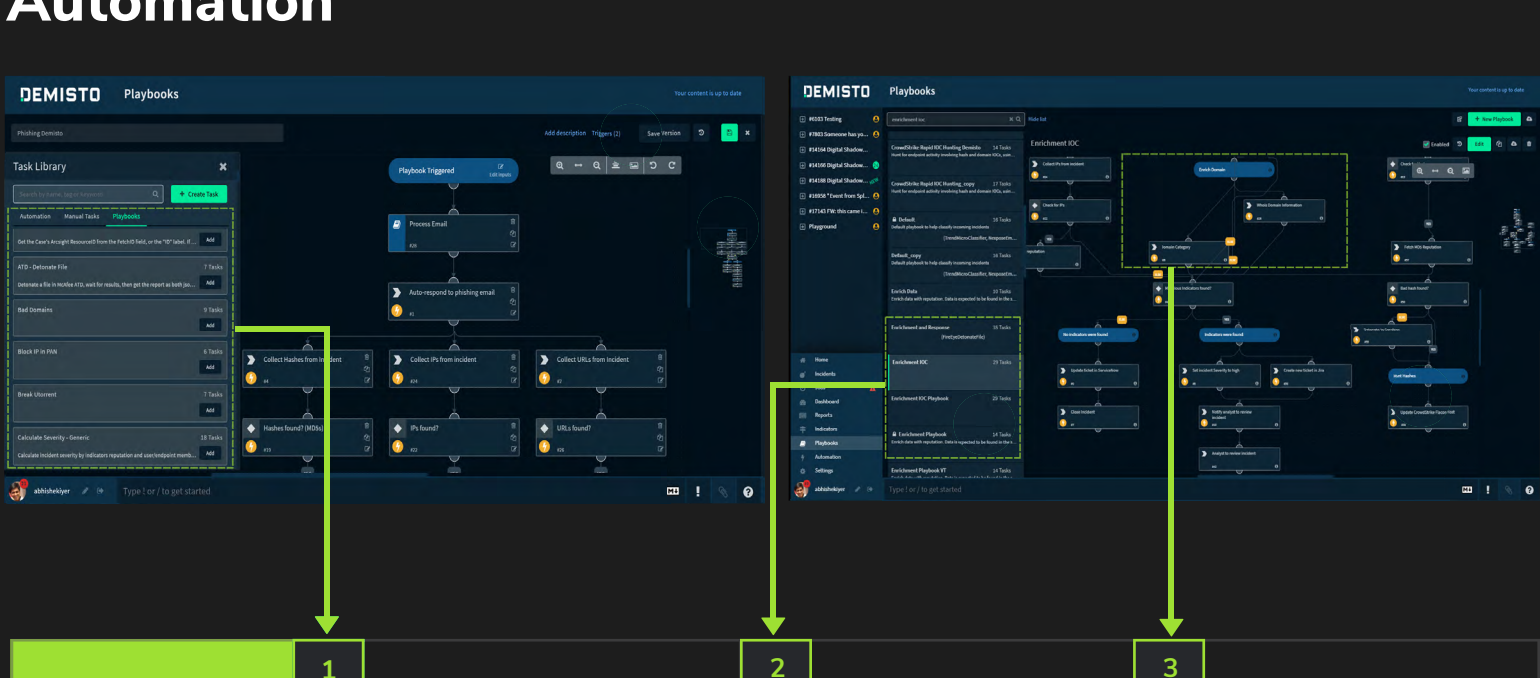
Demisto maps successfully with all of Gartner's recommended capabilities for SOAR vendors, highlighting an end-to-end solution that can handle varying levels of complexity across a SOC's maturity lifecycle.

Orchestration



	1 Out-of-the-box integration connectors	2 Feature-rich integrations	3 Abstraction layer	4 Bidirectional integration capability
GARTNER RECOMMENDS	Out-of-the-box integration connectors	Feature-rich integrations	Abstraction layer	Bidirectional integration capability
DEMISTO HAS	✓ Extensible network with 100s of partner integrations	✓ Multiple API calls (and growing) per integration that leverages all partner features	✓ 1000s of automation scriptlets invokable across platform ✓ Logical expressions supported in CLI	✓ Many bidirectional partner integrations with both push and pull capabilities ✓ Bring Your Own Integration as code-light option to build bespoke integrations

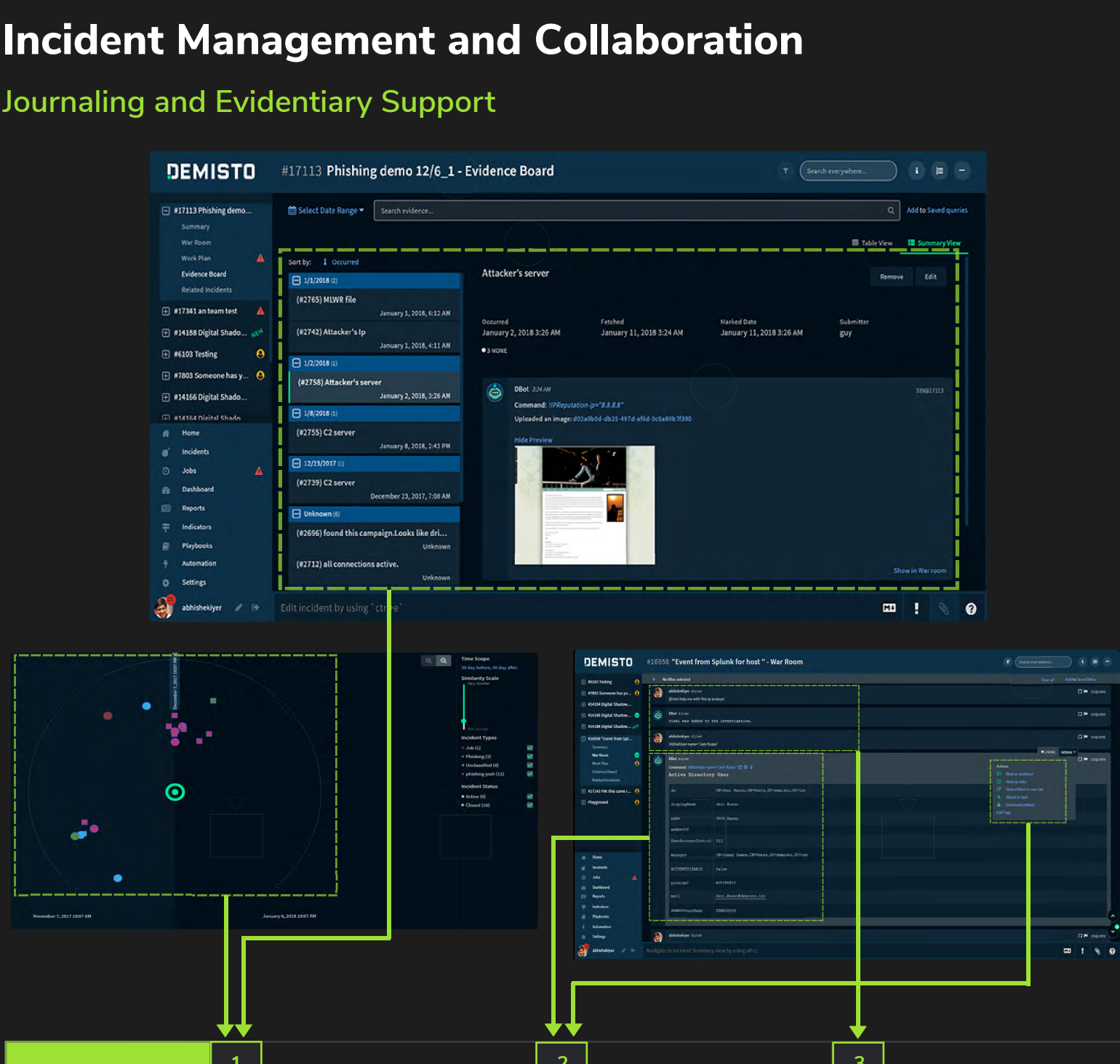
Automation



	1	2	3
GARTNER RECOMMENDS	Multi-level automation	Playbooks	Workflows
DEMISTO HAS	✓ Playbooks interweave automated and manual tasks ✓ Ability to create custom manual tasks and place sub-playbooks within playbooks	✓ GUI-based drag-and-drop playbook editor ✓ 45+ OOTB playbooks ✓ Open playbook standards	✓ Full workflow capability ✓ Workflows can have automated and manual tasks across security product functions

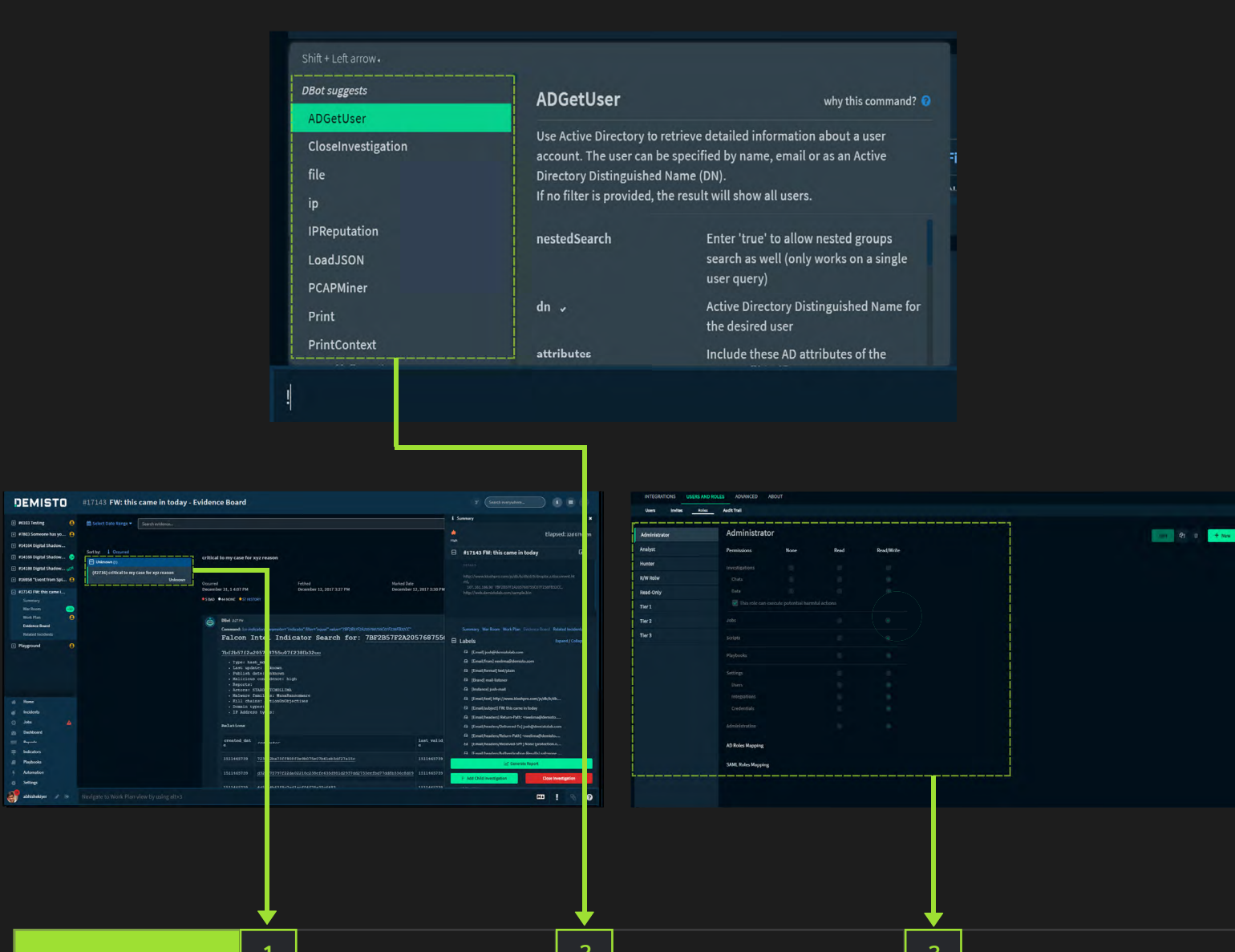
Incident Management and Collaboration

Journaling and Evidentiary Support



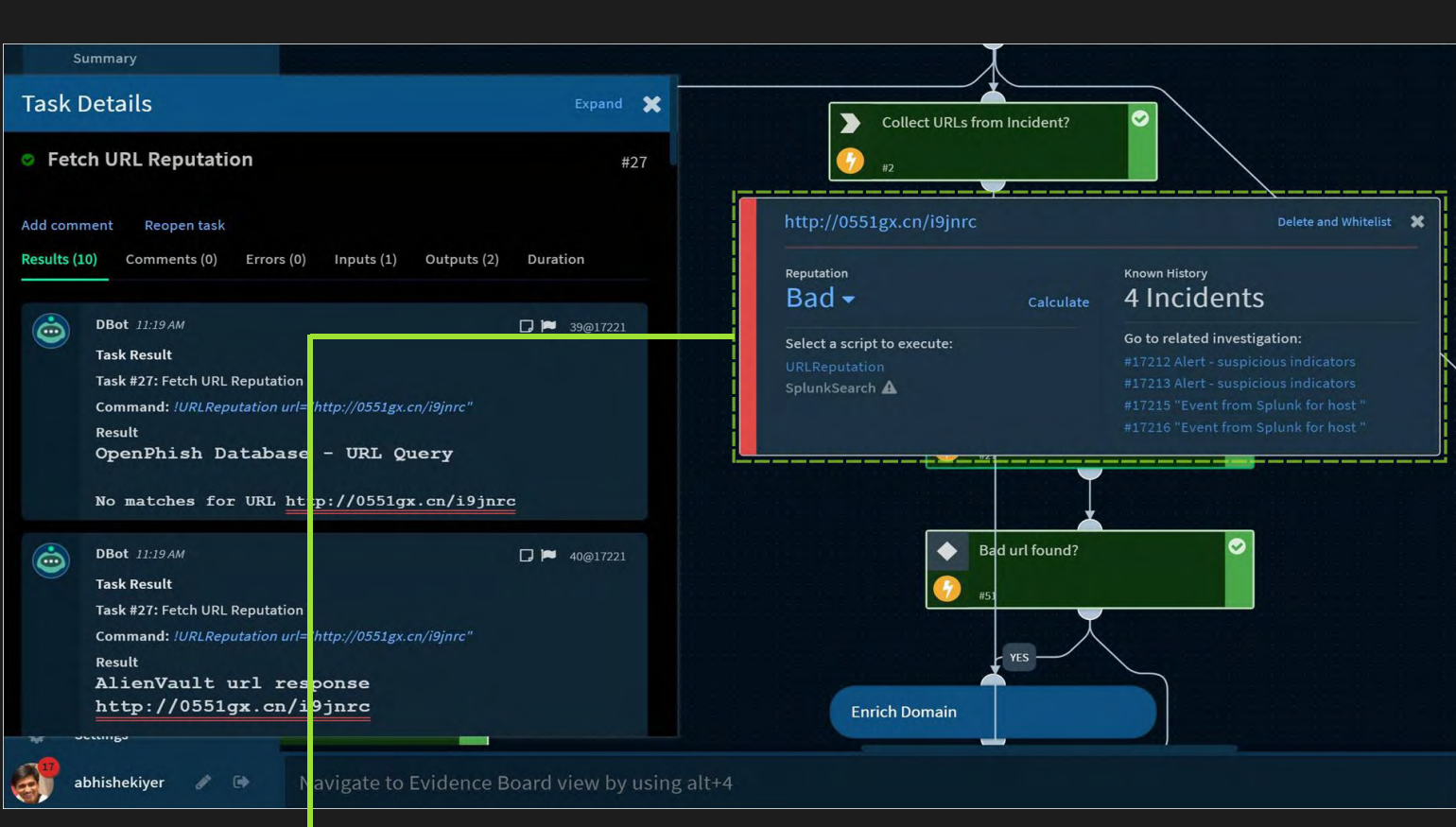
	1	2	3
GARTNER RECOMMENDS	Incident timeline	Historical records	Collaboration
DEMISTO HAS	✓ Evidence board for each incident stores key artifacts for current and future analysis ✓ Related Incidents with time-based radial map of related incidents, ability to link and map duplicates	✓ Auto-documentation of playbook tasks, analyst tasks, comments, live commands in War Room	✓ War Room: analysts conduct joint investigations, interact with chatbots, and other security products (ChatOps)

Case Management



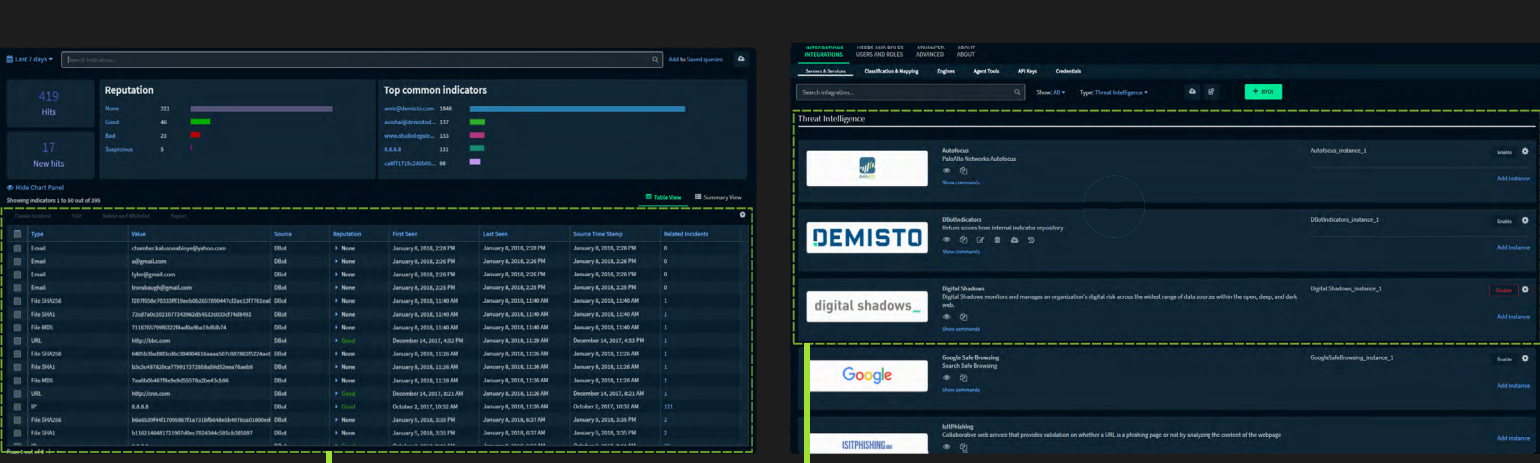
	1	2	3
GARTNER RECOMMENDS	Post-incident reviews	Knowledge management	Role-based access control
DEMISTO HAS	✓ Post-closure scripts ✓ Evidence timeline to capture key incident takeaways ✓ Customizable reports per incident	✓ Library for playbooks, automation scripts ✓ Auto-documentation of all actions and comments ✓ Machine learning trains on analyst actions for insights	✓ Parent and child account privileges for automations, playbooks, incident types, reports

Analytics and Investigation Support



	1
GARTNER RECOMMENDS	Incident correlation
DEMISTO HAS	✓ Cross-correlation of artifacts across incidents ✓ Visual map of related incidents with ability to link and mark as duplicates

Threat Intelligence



	1	2
GARTNER RECOMMENDS	Basic native threat intelligence	Third-party threat intelligence network
DEMISTO HAS	✓ Central indicator repository with STIX upload, auto-detection of indicators, search and query ✓ Ability to schedule threat hunting playbooks and proactive response	✓ Extensive threat intelligence partner network ✓ Orchestrate actions as playbook tasks or run commands interactively from War Room

Dashboards and Reporting

	1	2	3
GARTNER RECOMMENDS	Analyst level reporting	SOC Manager level reporting	CISO level reporting
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

SCHEDULE DEMO

DOWNLOAD COMMUNITY EDITION