Mapping Functional Components

Journaling and Evidentiary Support

An Ideal Match with Gartner’s (ID: G00338719). Retrieved from Gartner database.

Demisto Enterprise is the only security operations solution with native incident management and orchestration and automation, security incident response platforms, and threat intelligence platforms.

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

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.

**Technology Convergence**

- **Orchestration:**
  - Related Incidents with War Room
  - Visual map of related incidents with ability to link and mark as duplicates
  - Cross-correlation of artifacts across incidents
  - Ability to schedule threat hunting
  - Central indicator repository with integrations
  - Multiple API calls
  - Extensible network
  - Out-of-the-box playbooks, incident types, privileges for automations
  - Parent and child account
  - Auto-documentation of all product functions
  - Library for playbooks, incident types, privileges for automations
  - Integration as code-light option to build bespoke
  - Many bidirectional integration
  - Bidirectional integration

- **Case Management:**
  - Historical records Collaboration
  - Analyst level reporting SOC Manager level reporting CISO level reporting
  - Number/types of incidents, duplicates
  - Post-incident reviews Role-based access control Knowledge management
  - Post-closure scripts
  - Argument maps
  - Investigation timeline
  - Visualizations
  - Analytics to archive logs reports
  - Auto-documentation of all

- **Analytics and Investigation Support:**
  - Post-closure scripts
  - Argument maps
  - Investigation timeline
  - Visualizations
  - Analytics to archive logs reports
  - Auto-documentation of all

- **Automation:**
  - Duplicates
  - Time-based radial map of related
  - Stores key artifacts for current and future analysis
  - Playbooks and proactive response
  - Indicators, search and query within playbooks
  - Ability to create custom manual
  - Evidence timeline to
  - Post-closure scripts

- **Dashboards and Reporting:**
  - Incidents per analyst
  - Money saved through automation
  - Parent and child account
  - Auto-documentation of all

- **Threat Intelligence:**
  - Basic native threat intelligence
  - Third-party threat intelligence network
  - Different technologies
  - Orchestration:
    - Integrated to work together.

**Gartner Says Demisto Has**

**Feature-rich Orchestration:**

- Orchestrate actions as playbook tasks or run commands
- Integrations
- Abstraction layer
- Logical expressions
- 45+ OOTB playbooks
- Open playbook standards
- 100s of partner integrations
- Many bidirectional integration
- Multiple API calls
- Extensible network
- Out-of-the-box playbooks, incident types, privileges for automations
- Parent and child account
- Auto-documentation of all product functions
- Library for playbooks, incident types, privileges for automations
- Integration as code-light option to build bespoke
- Many bidirectional integration
- Bidirectional integration

**Dashboard and Reporting:**

- Incidents per analyst
- Money saved through automation
- Parent and child account
- Auto-documentation of all

**Case Management:**

- Historical records Collaboration
- Analyst level reporting SOC Manager level reporting CISO level reporting
- Number/types of incidents, duplicates
- Post-incident reviews Role-based access control Knowledge management
- Post-closure scripts
- Argument maps
- Investigation timeline
- Visualizations
- Analytics to archive logs reports
- Auto-documentation of all

**Analytics and Investigation Support:**

- Post-closure scripts
- Argument maps
- Investigation timeline
- Visualizations
- Analytics to archive logs reports
- Auto-documentation of all

**Automation:**

- Duplicates
- Time-based radial map of related
- Stores key artifacts for current and future analysis
- Playbooks and proactive response
- Indicators, search and query within playbooks
- Ability to create custom manual
- Evidence timeline to
- Post-closure scripts

**Threat Intelligence:**

- Basic native threat intelligence
- Third-party threat intelligence network
- Different technologies
- Orchestration:
  - Integrated to work together.

An Ideal Match with Gartner’s (ID: G00338719). Retrieved from Gartner database.

Demisto Enterprise is the only security operations solution with native incident management and orchestration and automation, security incident response platforms, and threat intelligence platforms.

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

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.

**Technology Convergence**

- **Orchestration:**
  - Related Incidents with War Room
  - Visual map of related incidents with ability to link and mark as duplicates
  - Cross-correlation of artifacts across incidents
  - Ability to schedule threat hunting
  - Central indicator repository with integrations
  - Multiple API calls
  - Extensible network
  - Out-of-the-box playbooks, incident types, privileges for automations
  - Parent and child account
  - Auto-documentation of all product functions
  - Library for playbooks, incident types, privileges for automations
  - Integration as code-light option to build bespoke
  - Many bidirectional integration
  - Bidirectional integration

- **Case Management:**
  - Historical records Collaboration
  - Analyst level reporting SOC Manager level reporting CISO level reporting
  - Number/types of incidents, duplicates
  - Post-incident reviews Role-based access control Knowledge management
  - Post-closure scripts
  - Argument maps
  - Investigation timeline
  - Visualizations
  - Analytics to archive logs reports
  - Auto-documentation of all

- **Analytics and Investigation Support:**
  - Post-closure scripts
  - Argument maps
  - Investigation timeline
  - Visualizations
  - Analytics to archive logs reports
  - Auto-documentation of all

- **Automation:**
  - Duplicates
  - Time-based radial map of related
  - Stores key artifacts for current and future analysis
  - Playbooks and proactive response
  - Indicators, search and query within playbooks
  - Ability to create custom manual
  - Evidence timeline to
  - Post-closure scripts

- **Dashboards and Reporting:**
  - Incidents per analyst
  - Money saved through automation
  - Parent and child account
  - Auto-documentation of all

To see Demisto in action sidewalks: Weather Map