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

Demisto Enterprise is an ideal SOAR solution as a convergence of three previously distinct technology markets: security operations, incident management, and threat intelligence.

**Playbooks**

Feature-rich, open playbook editor built on Python and supporting multiple API call integrations, with 100s of partner features supported in CLI

**Dashboards and Reporting**

Out-of-the-box analyst level reporting, SOC Manager level reporting, CISO level reporting

**Analytics and Investigation Support**

Central indicator repository with STIX upload, auto-detection of indicators, search and query

**Incident Management and Collaboration**

Cross-correlation of artifacts across incidents, ability to schedule threat hunting, central indicator repository with STIX upload, auto-detection of indicators, search and query

**Automation**

Logical expressions, 1000s of automation scripts invokable

**Orchestration**

Bidirectional integration, many bidirectional partner integrations

**Case Management**

Multi-level automation, duplicates, incident correlation, incident history, open/close status

**Threat Intelligence**

Extensible network, basic native threat intelligence, third-party threat intelligence network

**SCHEDULE DEMO**

To see Demisto in action.