**Journaling & Evidentiary Support**

**INCIDENT MANAGEMENT & COLLABORATION**

**AUTOMATION**

include various forms of threat intelligence integration for this purpose. Threat intelligence is becoming a significant resource for detecting, diagnosing and treating security incidents. Gartner* notes the following capabilities:

- NETWITNESS
- RSA

Gartner has tracked the evolution of SOAR (Security Orchestration, Automation and Response (ID: G00338719)).


* RSA NetWitness Orchestrator provides:

- **Auto-detection of indicators, search and query**
- **Threat intelligence woven into one platform**
- **Native incident management and collaboration**
- **Security incident response platforms**
- **Security orchestration and automation**

Gartner's research highlights an end-to-end solution that can handle varying degrees of automation. **RSA NetWitness Orchestrator** is designed to work together with other security tools and products. It supports product functions like workflows, integration capabilities, full workflow capability, and cross-correlation of artifacts across incidents.

**TO SEE RSA NETWITNESS ORCHESTRATOR IN ACTION**

- **Visual map of related incidents with ability to link and mark as duplicates**
- **Cross-correlation of artifacts across incidents**
- **Workflows can have full automation scriptlets invokable in the cloud**
- **Logical expression supported in CLI**
- **40 OOTB playbooks**
- **400+ automation scripts**
- **Many bi-directional integrations**

**ORCHESTRATION & AUTOMATION**

**ENGAGEMENT & REPORTING**