DEMISTO

The Four Crucial Capabilities of a Modern Incident Management Platform

Modern threats demand a reimagined incident management function

Incident Management Essentials

Security incident management platforms have been around for a few years and the market has advanced to an extent that some feature-sets have become points-of-parity across vendors.

In their report 'Innovation Insight for Security Orchestration, Automation and Response[1]', Gartner writes:

> "This major function [incident management and collaboration] is complex. It deals with the life cycle of the incident from the moment an alert is generated, to the initial triage, to the validation of true/false positive, to the hunting and finally the remediation."

Before we go over modern incident management capabilities, let's highlight essential features that most incident management systems include today.

Process documentation:

The need for consistent, transparent, and documented processes has always been a core driver for incident management solutions. Full case management capabilities that map the entire lifecycle of an incident, enable reconstructed timelines of actions taken, and support post-incident reviews are a base expectation from incident management vendors today.

SLA tracking:

The lack of robust measurement is often overlooked, but remains a major challenge facing security teams that necessitates demand for incident management tools. Granular tracking of incident and analyst metrics, auto-documentation of all actions for future analysis, and dashboards and reports to visualize underlying data are industry standards for incident management.

Role-based access control:

As Security Operations Centers (SOCs) start to face incidents with varying levels of sensitivity, individual user-based identity management is no longer enough to control privacy and access. Role-based access control (RBAC) is a mechanism through which SOCs can tailor permissions to their security risk tolerance and organizational hierarchies.

SIEM data ingestion:

SIEMs are usually the 'digital brains' of any organization, collecting logs and event data across sources and correlating information across all security relevant data. Any incident management platform worth its salt ingests this already-sifted data from SIEMs for further case management, triage, and resolution.

Process Documentation	SLA Tracking	RBAC	SIEM Ingestion
Case Management	Metric Tracking	Custom Roles	Rule-Based Ingestion
Incident Timelines	Auto Documentation	Tailored Permissions	Bidirectional Integrations
Post-Incident Reviews	Bespoke Dashboards	Transferability	Flexible Mapping
Workflow Formalization	Incident Reports	Regulatory Compliance	Audit Trails

[1] Gartner Innovation Insight for Security Orchestration, Automation and Response (ID: G00338719). Neiva, C., Lawson, C., Bussa, T., & Sadowski, G. (2017, November 30).

Incident Management Reimagined

The cybersecurity landscape is changing at breakneck pace. The expansion of attack surfaces has resulted in a constantly shifting digital warzone, 'short tail' threats now help attackers lay the groundwork for more malicious campaigns, and the percentage of malicious attachments in spam is increasing globally. **Organizations need to adopt a newer, more evolved form of incident management** in the face of these attack mechanisms.

Let’s look at the four critical capabilities of a modern incident management platform.

Customization is king

With such a wide variety of attack types, indicators, and mechanisms prevalent today, incident management with be-all and end-all standardization may no longer be the ideal option. An incident management platform with a base of standardization and **added layers of user customization** is likely to be preferred amidst unpredictable attacks.

Customization options within a modern incident management platform should include:

Regulations and Standards:

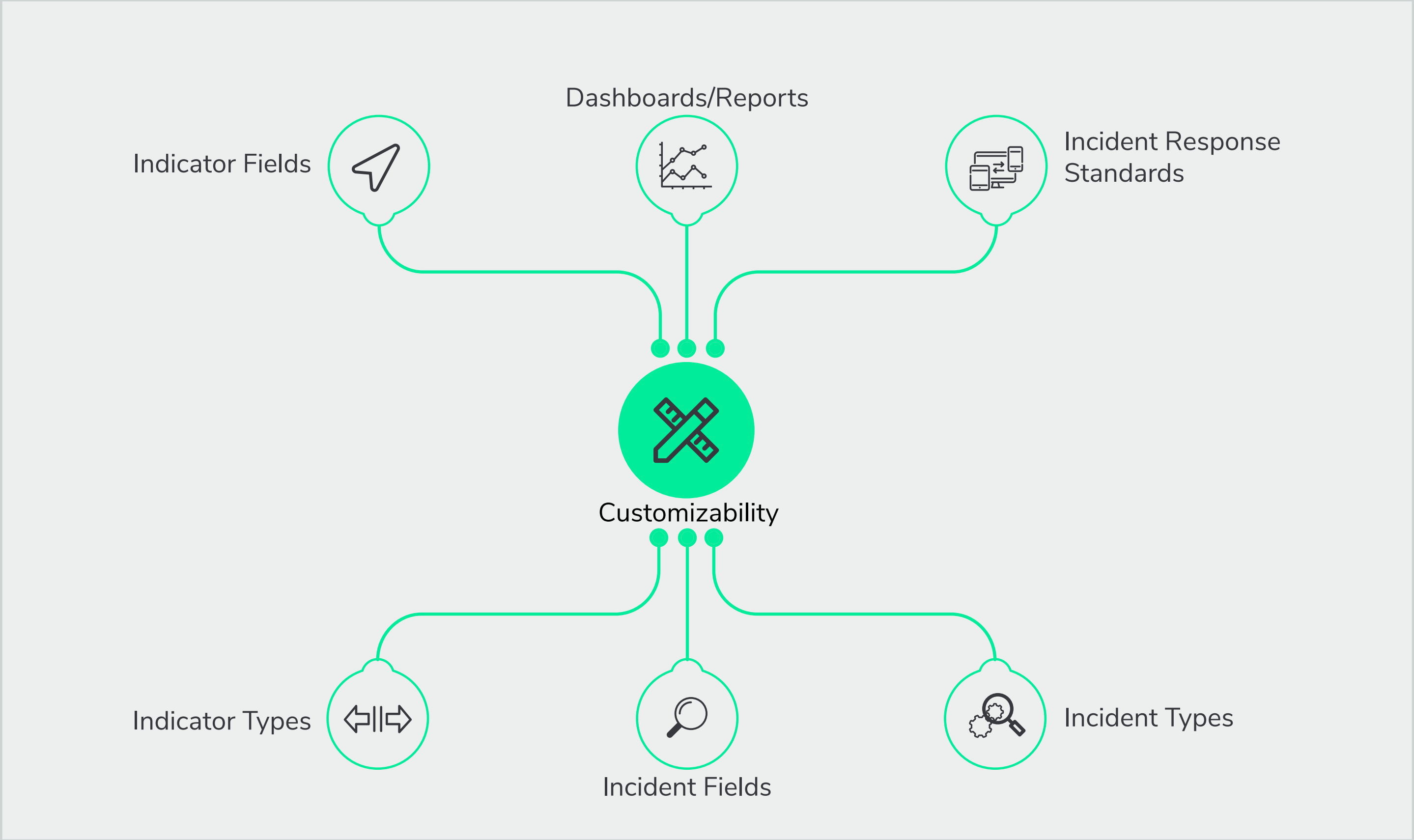
With multiple industry standards and frameworks present today (NIST, CERT, SANS, etc.) and regulatory requirements like the GDPR (General Data Protection Regulation) on the horizon, incident management platforms cannot afford to be married to a single standard anymore. Apart from availing templates aligned to popular standards, SOCs should be enabled to tailor their incident management platform to custom standards as required.

Incident Types and Fields:

SOCs are perennially one step away from facing new attacks without any prescribed response measures. Locking in pre-defined incident types in such a nebulous battlefield is a mistake. Incident management platforms should allow for creation of custom incident types as well as incident fields and labels, so that unknown attack types are quickly categorized and SOCs can be ready the next time they manifest themselves.

Indicator Types and Fields:

A wide variety of attacks might be defined by the same set of malicious indicators, but a lack of indicator visibility and control results in repetitive response actions for each attack that could otherwise have been avoided or automated. Incident management platforms should enable creation of custom indicator types and fields in addition to automatically logging all indicators that show up within incidents.



Everything is connected

Product proliferation is one of the main challenges facing SOCs today Analysts have to coordinate a vast security product suite while responding to incidents; this coordination involves repeated context and console switching that leads to 'dead time', shaving off vital seconds from incident response time.

Today, incident management solutions that **align strongly with other security functions** will rise to the top of user needs.

Security orchestration:

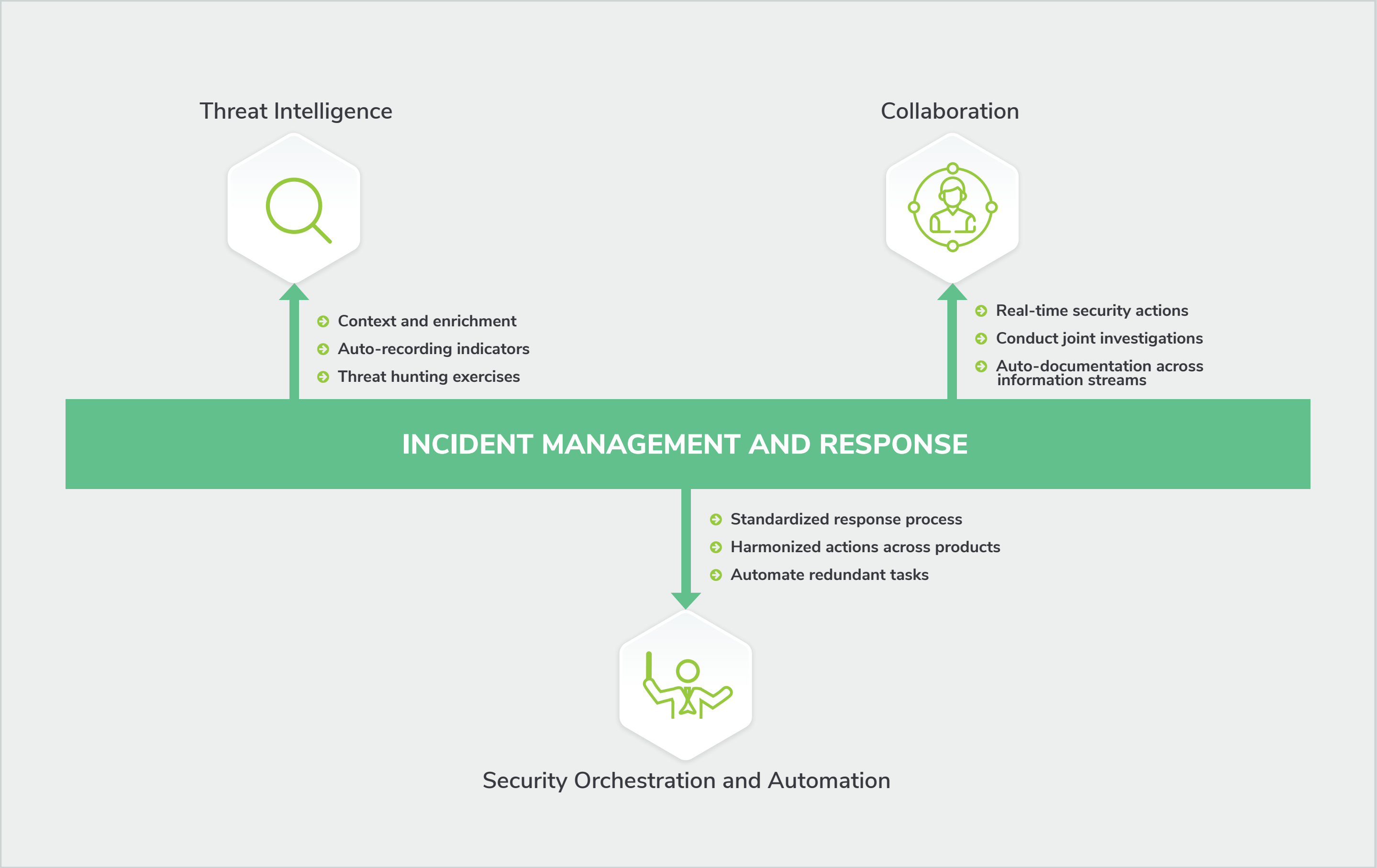
If incident management platforms have native security orchestration or integrate with third-party security orchestration platforms, analysts can benefit from harmonizing actions across their security product stack in a single window, preventing the need to switch screens and collate information from disparate sources.

Collaboration:

If analysts perform actual investigations on the incident management platforms but converse with each other using an isolated collaboration tool, the wealth of data that can be gleaned from their conversations is lost. Incident management platforms with native collaboration suites or integrations with third-party collaboration tools result in a capturing of all those analyst comments. This not only lets analysts work on a single console while also conversing with the team, but also aids in knowledge management by building a repository of information within the organization.

Threat intelligence:

Although SIEMs perform initial incident enrichment and correlation, analysts often need to buttress that with additional context gleaned from threat intelligence platforms. Incident management platforms with basic native threat intelligence and integrations with third-party threat intelligence platforms will ensure that analysts get accurate, actionable context from multiple sources while dealing with incidents.


Threat Intelligence
Collaboration
Context and enrichment
Auto-recording indicators
Threat hunting exercises
Real-time security actions
Conduct joint investigations
Auto-documentation across information streams
INCIDENT MANAGEMENT AND RESPONSE
Standardized response process
Harmonized actions across products
Automate redundant tasks
Security Orchestration and Automation

Always be learning

Analysts and SOC Mangers are so caught up with daily firefighting and moving from incident to incident that opportunities to learn from and improve upon response processes remain unexplored. Modern incident management solutions will be **intelligent enough to learn from analyst actions** and provide actionable insights to improve both analyst-level and business-level response metrics.

Machine learning capabilities within modern incident management platforms should include:

Incident ownership:

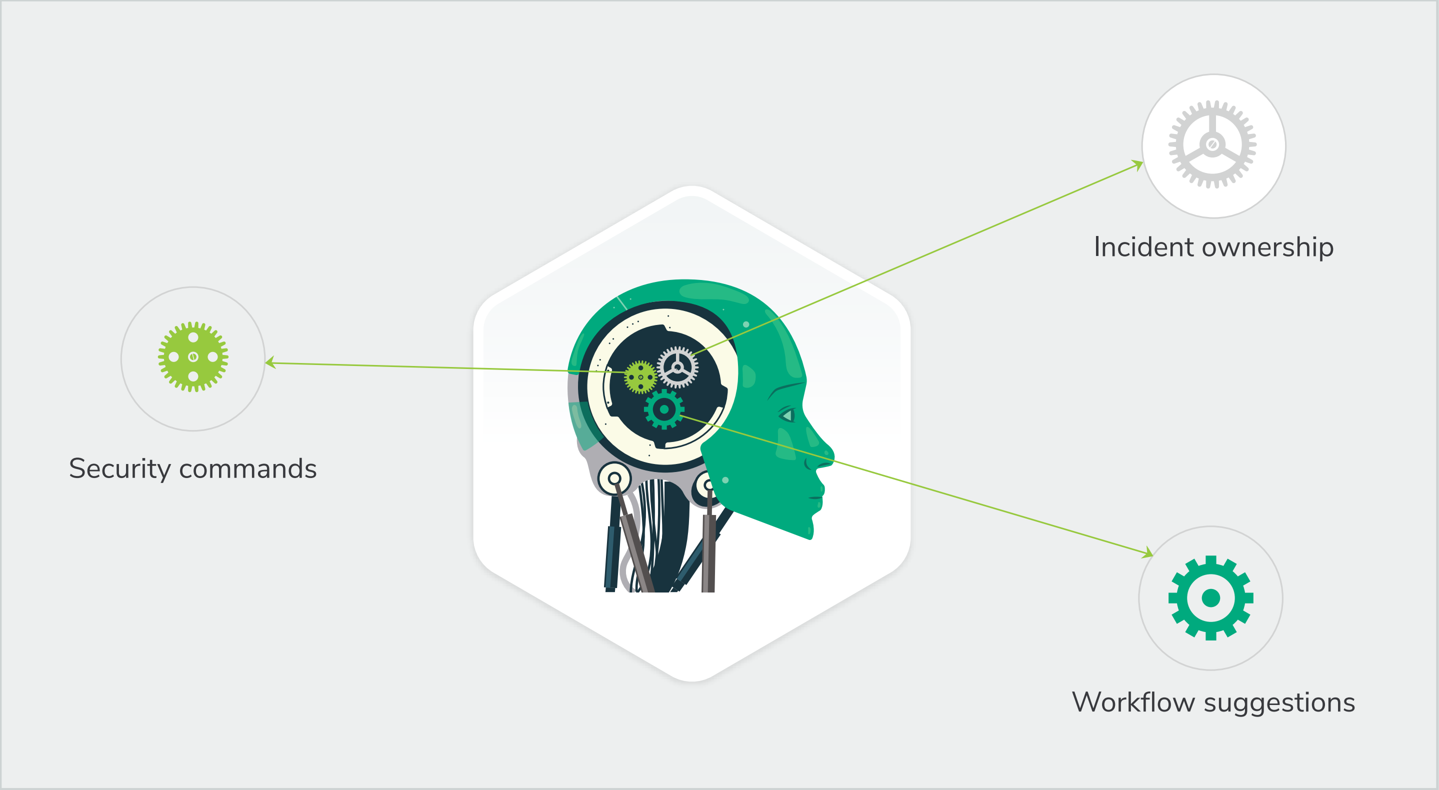
With analysts busy in daily battles, measurement of most effective incident ownership takes a backseat. Modern incident management platforms should be able to analyze incident data and recommend ideal incident-analyst pairings with time, ensuring that analysts are always handling incidents at optimal capacity.

Workflow suggestions:

Response workflows are different for each incident and each SOC, traditionally built from collective knowledge and best practices. An intelligent incident management platform will learn from incident data and suggest leaner, more effective workflows with time, ensuring that SOCs are always on the path of further improvement.

Security commands:

Even though incident management platforms help standardize initial response, analysts still have unique investigation procedures as they move deeper into the incident. If the platform learns from this set of analyst actions and suggests commonly used security commands with time, all analyst response procedures can coalesce into one lean, efficient, repeatable workflow.



Flexible deployment

As security becomes more pervasive across organizations, it becomes necessary for solution providers to match organizational vagaries. The most pertinent among these vagaries is how an organization deploys its computing power. Companies may install some services on premise, have other services on the cloud, and isolate networks different business segments to maintain security and compliance.

For an incident management solution to be successfully deployed across an organization, it must be **flexible in its deployment options.**

Tailored deployment:

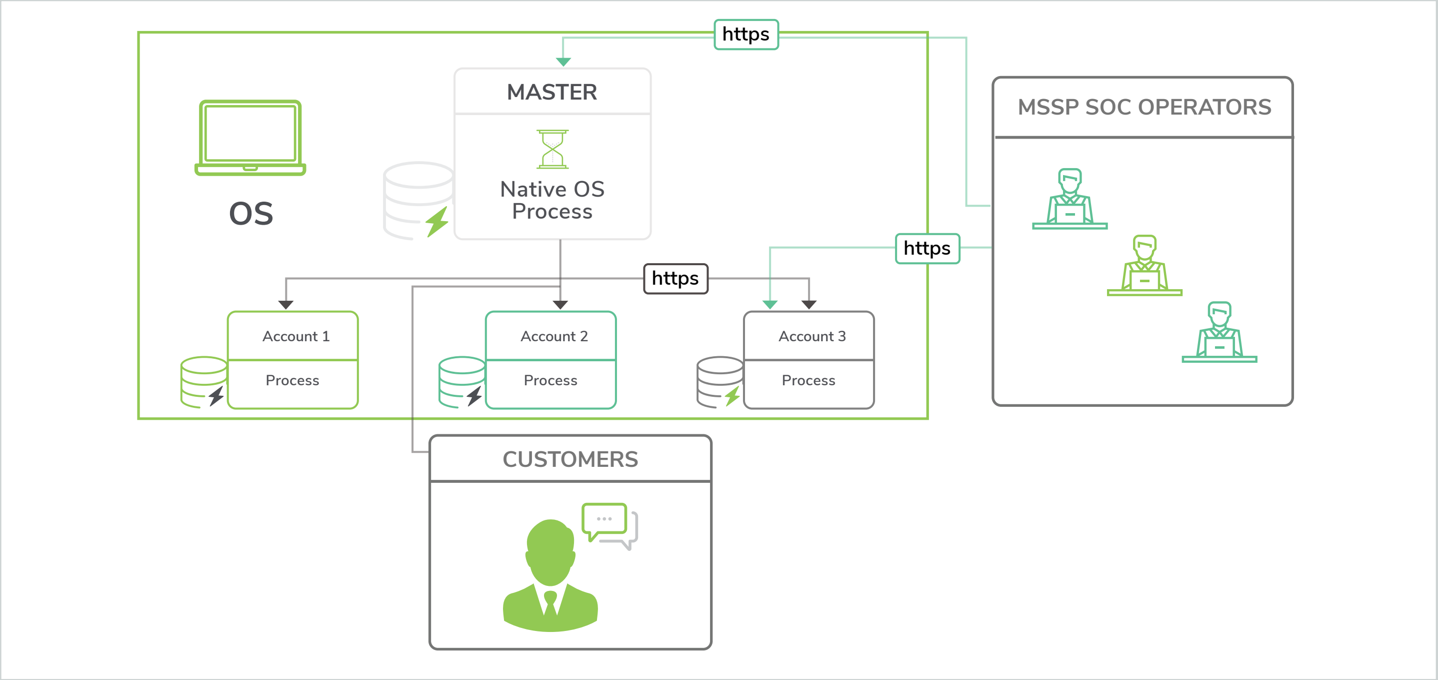
Modern incident management platforms must possess deployment options tailored to the organization. With multiple deployment options sometimes required across one organization, it's essential that on-premise, cloud, and hybrid selections be available if required.

Multi-tenancy:

Organizations sometimes prefer to outsource security operations to a Managed Security Services Provider (MSSP) or utilize the same SOC for different business units. In these situations, an incident management platform primed for multi-tenancy with full master-child separation guarantee will result in the greatest SLA confidence for customers.

Tri-layered isolation:

For best-in-class privacy and security, platforms need three levels of isolation if they're multi-tenant: data isolation (to preserve integrity of data in child accounts), execution isolation (to prevent common execution across child accounts), and network isolation (to preserve security of segmented networks). An incident management platform with all three levels of isolation embedded within its multi-tenancy stack will possess a critical advantage.



While evaluating incident management platforms, SOCs should consider both essential features and modern differentiators to ensure a maximal return on investment and overall improvement in security posture. The Vendor Qualification Criteria document given on the next page will help form an initial guideline upon which SOCs can build their own custom evaluation checklist.

Vendor Qualification Criteria

Points-of-parity

Process documentation:

- Does the platform support full case management?
- Does the platform enable reconstructed incident timelines?
- Does the platform have workflow capabilities? (combination of automated and manual tasks, live run of actions, one-source documentation)
- Does the platform support post-incident reviews?

SLA tracking:

- Does the platform track both incident and analyst level metrics?
- Does the platform automatically document all commands, comments, and actions?
- Does the platform allow for custom dashboard creation with widgets and templates?
- Does the platform include custom reports that can both be spun up in real time and scheduled?

Role-based access control:

- Does the platform enable creation of custom organizational roles?
- Does the platform allow for flexible permissions and authorizations per role?
- Does the platform allow for transfer of roles and permissions to other (both security and non-security) platforms?
- Does the platform have checks and balances for specific industry regulations?

SIEM ingestion:

- Does the platform allow for rules-based data ingestion from SIEMs?
- Does the platform contain bidirectional integrations with SIEMs, allowing for push and pull of data?
- Does the platform facilitate flexible label mapping with the data labels of SIEMs?
- Does the platform create audit trails to highlight data flow and maintain accountability?

Points-of-difference

Customization capabilities:

- Does the platform contain response templates for specific standards such as NIST, CERT, etc.?
- Does the platform enable creation of custom incident response standards?
- Does the platform allow for creation of custom incident types?
- Does the platform allow for creation of custom incident fields and labels?
- Does the platform allow for customized incident summary layout?
- Does the platform allow for creation of custom indicator types?
- Does the platform allow for creation of custom indicator fields and labels?

Integrations across security functions:

- Does the platform contain native security orchestration and integrations with security orchestration platforms?
- Does the platform contain native real-time collaboration and integrations with collaboration platforms?
- Does the platform contain native threat intelligence and integrations with threat intelligence platforms?

Continuous learning:

- Does the platform contain learning mechanisms to give insights into analyst productivity?
- Does the platform contain learning mechanisms to give insights into response efficiency?
- Does the platform contain learning mechanisms to give insights into effective security commands?

Flexible deployment:

- Is the platform available as an on-premise, cloud, or hybrid solution?
- Is the platform equipped with data, execution, and network isolation for maximal privacy?
- Is the platform designed for multi-tenancy with full master-child separation?
- Does the platform have an engine (proxy) to deal with segmented networks?
- Does the platform have dissolvable agent for conducting operations without violating firewall rules?

More helpful resources:

Looking for Incident Report Best Practices?

GET THE TEMPLATE

Ready to know more about Security Orchestration?

GET GARTNER REPORT