Gartner

Emerging Tech: Security — Cloud Investigation and Response Automation Offers Transformation Opportunities

Published 5 June 2023 - ID G00782893 - 14 min read

By Analyst(s): Lawrence Pingree, Mark Wah

Initiatives: Emerging Technologies and Trends Impact on Products and Services

Cloud investigation and response automation is emerging to automate the investigation and collection of digital forensics in the cloud. Product leaders must adopt transformative cloud technologies to address demand for expanding data collection, analysis, collaboration and future business models.

Overview

Key Findings

- Runtime visibility and threat detection are critical aspects of investigations into breach events and help characterize and validate attack methodologies for forensics and incident response activities.
- Threat detection capabilities are overlapping in multiple areas of security, causing customers to stretch to understand how providers fit across their product needs.
- Expanding data sources and SaaS delivery in forensics are transforming incident characterization and analysis speed and improving efficiencies in incident response.

Recommendations

Product leaders interested in emerging technologies in data forensics and incident response should:

- Seek to expand both runtime and threat detection capabilities to characterize threats leading to breach incidents quicker through both technology OEMs and partnerships.
- Prioritize API integration partnerships and OEMs due to overlapping threat detection use cases, such as cloud infrastructure and SaaS.

- Work to expand your scope of data collection across both cloud-native and SaaS solutions to interconnect activities and provide efficient delivery of post-collection analysis efforts for target incident response (IR) and forensics roles.

Strategic Planning Assumption

- By 2026, SaaS-delivered, cloud-native offerings will replace at least 30% of traditional on-premises-delivered software and hardware-based forensic acquisition solutions, up from only 5% today.

Analysis

Technology and Trend Description

Cloud investigation and response automation (CIRA) is an emerging technology that forensically collects, analyzes and applies analytics and machine learning on cloud and various forensic data sources. The defining goal with these offerings is to forensically analyze incidents, find and collect related files and correlate log events in support of comprehensive investigations of confirmed threats. These tools are also leveraged for human resource violations and legal cases and data breach events for legal cases or law enforcement.

The latest emerging providers' CIRA-focused tools are extending forensic collection and analysis across an expanding set of end-user endpoints, cloud workloads, cloud-native infrastructure and services, and SaaS environments. CIRA tools provide more-focused support for IR and forensic workflows; artifact discovery, collection and analysis; artifact management; data life cycle handling; and chain of custody for investigation and forensic use cases. Modern capabilities are emerging, including the use of AI and deep learning for extending data artifact preprocessing, event processing and workflow automations. This document presents three critical insights about CIRA and their impacts on product leaders, summarized in Figure 1.