Vendor Profile

Infocyte — Automating Threat Hunting for the Rest of Us

Robert Ayoub Sean Pike

IDC OPINION

Organizations continue to struggle with finding threats hiding in the network. Many forensics-focused vendors report industry averages of over 200 days for malware to be active in a network, sitting undiscovered. While some lag might be expected for less sophisticated organizations, attackers having nearly a year on average to do what they please on a network is simply unacceptable for most organizations. Further:

- While there are tools out there to help with incident response and investigation, as well as threat hunting, the truth of the matter is that most of these tools are difficult for all but the largest enterprises to use.
- Small and medium-sized businesses also have plenty of data to lose. In fact, those small and midsize organizations are potentially even more at risk for a business-critical breach that could potentially shutter their business.

IN THIS VENDOR PROFILE

This IDC Vendor Profile analyzes Infocyte's threat hunting solution and highlights the company's differentiation factors in the market. This document also reviews key success factors including strategy, offerings, and target markets.

SITUATION OVERVIEW

Company Overview

Developed by former U.S. Air Force cybersecurity officers, Infocyte's dedicated forensics-based threat hunting platform discovers the post compromise activity of cyberattackers and malware that have bypassed other defenses. The company's unique approach to security reduces attacker dwell time to help organizations and independent assessors defend networks and critical information.

Infocyte is the result of years of experience hunting adversaries within some of the largest and most targeted defense networks in the world. This experience in building the U.S. military's first malware hunting team provides Infocyte with an unmatched level of operational expertise and equips the company with a highly refined perspective on how to tackle today's security threats.

Company Strategy

Infocyte HUNT is a cloud-delivered threat hunting solution that utilizes forensic state analysis (FSA) to perform deep host inspections of devices. Deployment models can be either agentless based, agent based, or both. Unlike other analytics solutions that focus on behavior (e.g., UEBA), Infocyte collects its own primary forensic data rather than relying on existing security logs from sensors (IDS, AV, etc.) that might have failed to alert on the attack in the first place.

The key premise behind Infocyte's approach is that a performing log analysis – the key method used by most organizations – is generally expensive, difficult to manage, and error prone. Log analysis approaches require in-depth knowledge of adversary tactics and how those tactics present themselves in the logs of security solutions. Log analysis typically requires that a product (and security analysts) performs a great deal of tuning around the exact devices and information that the solution collects, as well as then determining if devices are reporting the correct information to begin with. Log analysis approaches can be an effective security stack component for those able to commit the monetary and expert resources needed to realize full value from them. Infocyte complements and strengthens these tools via continuous, lightweight forensic inspection and baseline-independent analysis to find the threats that elude traditional log analysis – all without the need for specialized knowledge of specific attacker behaviors and tactics (TTPs).

Infocyte HUNT was designed with many principles in mind, namely independence, minimal invasiveness, and simplicity. Infocyte addresses these principles in the following ways: HUNT operates independently from other security products, it runs in a minimally invasive manner, and it is operated by a lean team and has the ability to work well in even small organizations.

Infocyte begins by assuming that endpoints are already compromised and seeks to validate that assumption using a variety of forensic and threat hunting techniques. Automated forensic collection, volatile memory inspection, threat intel enrichment, and deep analysis workflows to dig into anomalies and outliers help hunters find what purely automated detection misses.

Using FSA to Hunt for Persistent Compromises

Infocyte HUNT uses FSA to discover hidden threats and compromises within a network. It continuously inspects thousands of endpoints, spending a couple minutes on each host, and seeks to validate their state as "compromised" or "not compromised."

At the highest level, Infocyte HUNT digs deep into endpoints to validate:

- What applications and processes are running (in memory)
- What is triggered to run (through a persistence mechanism) or has run previously (via forensic execution artifacts like Microsoft Windows Shimcache)

Last, it identifies any manipulation of the operating system (OS) or active processes (e.g., what a rootkit does to hide its presence or what an insider threat might do to disable the system's security controls). This will reveal things like an OS configuration setting or an API call being hooked by a rogue/hidden process within volatile memory (e.g., rootkit).

This process of hunting with FSA is performed in five steps:

1. Inspect endpoints and collect forensic data
2. Enrich that data with threat intel
3. Triage leads with hunt-tailored learning algorithms
4. Investigate suspicious findings
5. Remediate

This is a highly differentiated approach from the behavior analysis techniques used by endpoint detection and response (EDR) or user behavior analytics (UBA) products, which only record the changes to a system or network as events (e.g., a new process spawning, a registry key change, or a user elevating privileges). FSA digs much deeper into each host.

Perhaps the most important aspect of ensuring that the state analysis of a compromised machine is successful is being able to bypass anti-forensics techniques. This is accomplished by going underneath higher-level operating system APIs and working directly with volatile memory structures – both of which Infocyte HUNT does.

FUTURE OUTLOOK

Security products vendors can differentiate themselves first and foremost by simplifying what has become a highly complex mix of technologies, services, and approaches. The forensics and incident investigation market continues to show strong growth because it is continually a challenge to address the advanced attack landscape of today. The adversaries are smarter, faster, and growing daily, therefore challenging organizations to keep up. On top of the complex nature of attacks, there is also a more pragmatic aspect to forensics and incident investigation today. Regulatory compliance mandates and cyberinsurance are beginning to require forensic evidence in order to prove or disprove an incident. To maximize participation in forensics and incident investigation deals, vendors should consider the following:

- Identify an area or areas of expertise, and build a case for differentiation and value, recognizing the effort and investment required to stay at the bleeding edge. Creating value is key as many end users are perplexed with the vast amounts of forensic and log data that is being presented to them.
- Understand the maturity curve of the market, and educate enterprises about the need for a modern approach to forensics and incident investigation. Many practitioners have a severely outdated view of forensics, believing that it is difficult and complex and requires extensive expertise to operate successfully. There is a critically important need for vendors to provide simplified forensics workflows as well as provide definitive information as to whether a host is compromised or clean.

Finally, there are number of secondary measures that can be adopted by forensic and incident investigation vendors to address some of the confusion and concerns of customers in the market today:

- Share best practices and use cases to demonstrate time- and money-saving benefits resulting from real-time or near-real-time detection and response.
- Emphasize big-picture thinking that positions forensics and incident investigation as necessary for business continuity and places it at the core of IT operations and budgeting.
- Propose modular, flexible solutions that protect existing investments and enable tight integration with existing solutions versus point solutions.
- Offer (or partner to offer) hosted or managed services, a delivery model that is preferred by an increasing number of enterprises.
- Provide scalability by investing in the infrastructure to provide real-time data to organizations.
- Continue to invest in customer support and build out a superior technical support team that can address complex customer requirements and issues.

By engaging a vendor like Infocyte, enterprises can quickly get alerted and respond to a lurking attacker and gain visibility into advanced threats. These capabilities can quickly bring value to understaffed organizations.

ESSENTIAL GUIDANCE

Advice for Infocyte

Infocyte has tremendous forensic capabilities and comes from a DoD pedigree, giving it credibility in the market. However, the space for security products is crowded, and given the reputation of threat hunting as an advanced toolset, Infocyte has its hands full in conveying the messaging and effectiveness to organizations that might believe that they simply cannot do forensics in-house. There are a few key areas where Infocyte needs to invest and align its focus on in order to be successful in this very crowded space:

- **Educate the market:** As stated previously, forensics and incident response are generally viewed as functions that are highly complex and require a great deal of hands-on experience. Infocyte has developed a product that can do much of the heavy lifting remotely for an organization.
- **Focus on midsize businesses and smaller enterprises:** Midsize businesses and smaller enterprises have the most to gain from Infocyte HUNT. These organizations still have valuable assets to protect and often have the same regulatory requirements as larger organizations but often without the staff or expertise that larger organizations might have.
- **Partner with managed security service providers (SPs) and other technology partners:** Infocyte has a unique value proposition that can be leveraged by managed security SPs and other dedicated security partners. Infocyte has an opportunity to add significant capabilities to providers that can easily augment a security analyst's daily functions. Also, by adding technology ecosystem partners, Infocyte can ensure that its product works seamlessly with infrastructure and endpoint security products that have already been invested in by end-user organizations.

LEARN MORE

Related Research

- *Worldwide Security and Vulnerability Management Forecast, 2018-2022: SVM Vendors Fight Off New Market Entrants* (IDC #US43491618, July 2018)
- *Worldwide Security and Vulnerability Management Market Shares, 2017: Defending the Boundaryless Network* (IDC #US42049417, July 2018)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com