Infocyte aims to help organizations answer a critical question: Are we compromised?

Analysts - Aaron Sherrill

Publication date: Thursday, April 18 2019

Introduction

Enterprise security teams employ a variety of security tools and services to discover vulnerabilities in their organizations, but they are often unable to determine if attackers have successfully exploited these vulnerabilities to infiltrate the network and exfiltrate data. Infocyte is aiming to enable enterprises and MSSPs to detect and respond to persistent and undetected threats with its forensics-based threat-hunting and response platform designed to reduce the time, resources and expertise needed to conduct compromise assessments.

The 451 Take

Although enterprise security teams are deploying an increasing number of security tools and services, few organizations can confidently answer one critical question – is our organization compromised? According to 451 Research's Voice of the Enterprise: Information Security survey, 75% of organizations report having experienced a significant security incident in the past 12 months. For many of these organizations, the discovery of the breach or malicious activity occurred long after the threat originated. For the remaining 25% that believe they have not experienced a security incident, it is likely many are currently compromised but lack the tools and expertise to detect the threats residing in their organizations. There are many tools and services in the market aiming to help organizations detect these threats quickly, but Infocyte's unique forensics-based approach, from the cloud, independent of other security tools, should provide the company with the differentiation needed to stand out in a crowded and confusing market.

Context

Austin, Texas-based Infocyte launched in 2014 armed with the experience and expertise gained from serving on the United States Air Force Computer Emergency Response Team and helping launch the first enterprise-scoped threat-hunting team in the Department of Defense. Co-founded by Air Force

This export was generated by user rclurman@infocyte.com at account Infocyte on 5/9/2019 from IP address 24.55.33.127.

© 2019, 451 Research, LLC - A division of The 451 Group.
Using Interactive Document Server technology from Publish Interactive

alum and chief product officer Chris Gerritz and chief technology officer Ryan Morris, Infocyte offers a cloud-based cyber threat-hunting and incident response platform delivered as a service. The company reports a global customer base that spans almost every industry and every size organization. While the platform reportedly scales to enterprise levels, Infocyte says it primarily targets midmarket organizations in retail, finance, banking, insurance and health care with 1,000 to 10,000 endpoints.

Led by CEO Curtis Hutcheson, who previously served as GM for Dell Security Software, the privately held company reported substantial growth for 2018, citing 150% growth in recurring revenue over the previous year. The company has raised over $8.6m since its inception, including a $5.2m series B funding round in early 2018 led by venture firm Toba Capital.

According to Infocyte, organizations often have strong security controls around specific portions of their infrastructure, particularly those that require mission assurance. However, most organizations tend to have poor security in the outlying areas of their organization's digital footprint, making it difficult to detect indicators of compromise or breach. Infocyte said this was one of the main challenges that spurred the start of the company – how to enable breach discovery in an organization, a partner network or in a segment of a network that is not as well instrumented as the core or mission-critical network.

Infocyte believes there are multiple factors impeding organizations when it comes to breach discovery. Log digestion, retention and analysis are problematic for most organizations, with many failing or unable to gather and analyze the plethora of log data generated by an increasing number of log sources. Lack of resources, lack of expertise, disparate security tools, an expanding and diverse infrastructure and increasing threat complexity are all making it difficult to detect indicators of compromise or breach quickly and consistently. In response, according to Infocyte, many organizations are looking to security service providers for help; however, providing threat hunting, discovery and incident response capabilities often requires a significant investment in tools and expertise for service providers.

Platform

To address these challenges, Infocyte developed HUNT – a turnkey, forensics-based threat-hunting and incident response platform delivered from the cloud. The platform is designed to be independent of an organization's existing security stack, enabling it to validate existing security prevention and detection tools while also detecting, hunting and responding to threats across cloud and traditional networked endpoints and servers, containers, and serverless workloads. Infocyte offers an agentless and agent-based architecture offering enterprises the flexibility of perpetual agent-based access to endpoints or inspecting endpoints agentlessly in sensitive network segments.

The Infocyte HUNT platform provides asset and application discovery, vulnerability and compromise assessments, SIEM alert validation, alert triage and incident response capabilities. Infocyte says the threat-hunting platform uses forensic automation, memory analysis, threat intelligence, machine learning and analytics to inspect and validate endpoints, enabling organizations to automate and simplify the search for threats across the entire IT ecosystem. The platform assesses endpoints for evidence of intrusion detecting outliers and anomalies while also automating collection, enrichment and triage tasks.

Services

The company offers several service options for organizations. Infocyte professional services offers resources to help organizations launch a threat-hunting program or improve the effectiveness of their existing programs. Infocyte also provides managed threat-hunting services designed to augment customers' security teams with monthly reviews and on-demand expertise for threat

© 2019, 451 Research, LLC - A division of The 451 Group.

hunting, malware analysis and remediation. The company also touts a global partner network that is positioned to assist organizations with a range of services including deployments, training, compromise assessments and incident response services.

MSSPs

Infocyte's HUNT platform is also used by security services providers to conduct compromise assessments and perform threat-hunting or incident-response services for customers. Infocyte says MSSPs find that the platform automates traditionally resource-intensive forensic and analysis processes and improves their ability to detect post-breach activity including hidden, persistent threats that have bypassed their customers' defenses. According to Infocyte, MSSP partners can complete compromise assessments in just a few days – a significant improvement compared with traditional assessment approaches that take weeks or longer to complete.

The company says MSSPs are finding that the platform reduces the skill sets required to conduct a thorough compromise assessment, enabling providers that lack high-level threat-hunting expertise and capacity to deliver compromise assessment services to their customers. Infocyte says about 90% of its business is driven by partners – including sell-through opportunities and partners leveraging the platform to deliver threat-hunting and incident-response services.

Competition

Detecting compromise can be a difficult task and security technology and service providers take a variety of approaches to detect signs of breach, infection and other threat activity. Penetration testing, vulnerability and gap assessments, deception technologies and analytics can be effective to varying degrees but, according to Infocyte, are not effective in post-compromise situations.

Infocyte faces competition on multiple fronts, including managed detection and response (MDR) and endpoint detection and response (EDR) providers such as Expel, Red Canary, Arctic Wolf, CriticalStart, FishTech and Kudelski Security. The company will also encounter competition with security companies that offer compromise assessments through professional services engagements. FireEye, NTT Security, Booz Allen Hamilton, KPMG, Optiv, EY, IBM and LBMC offer an assortment of threat-hunting and compromise assessment services.

© 2019, 451 Research, LLC - A division of The 451 Group.

© 2019, 451 Research, LLC - A division of The 451 Group.