Infocyte

INFOCYTE

Advanced Detection. Instant Response.

Award-winning threat detection and incident response. Reduce risk, maintain compliance, and streamline cyber-security operations across on-premise, data center, and cloud environments with Infocyte.

Solution Overview

MANAGED SERVICE

On-demand support from expert threat hunters, malware analysts, and incident responders.

RESPONSE + EXTENSIONS

Automate incident response actions and build custom Extensions on Infocyte's open MDR platform.

FORENSIC STATE ANALYSIS

Independent, automated forensic inspection of every system in your environment—physical and virtual.
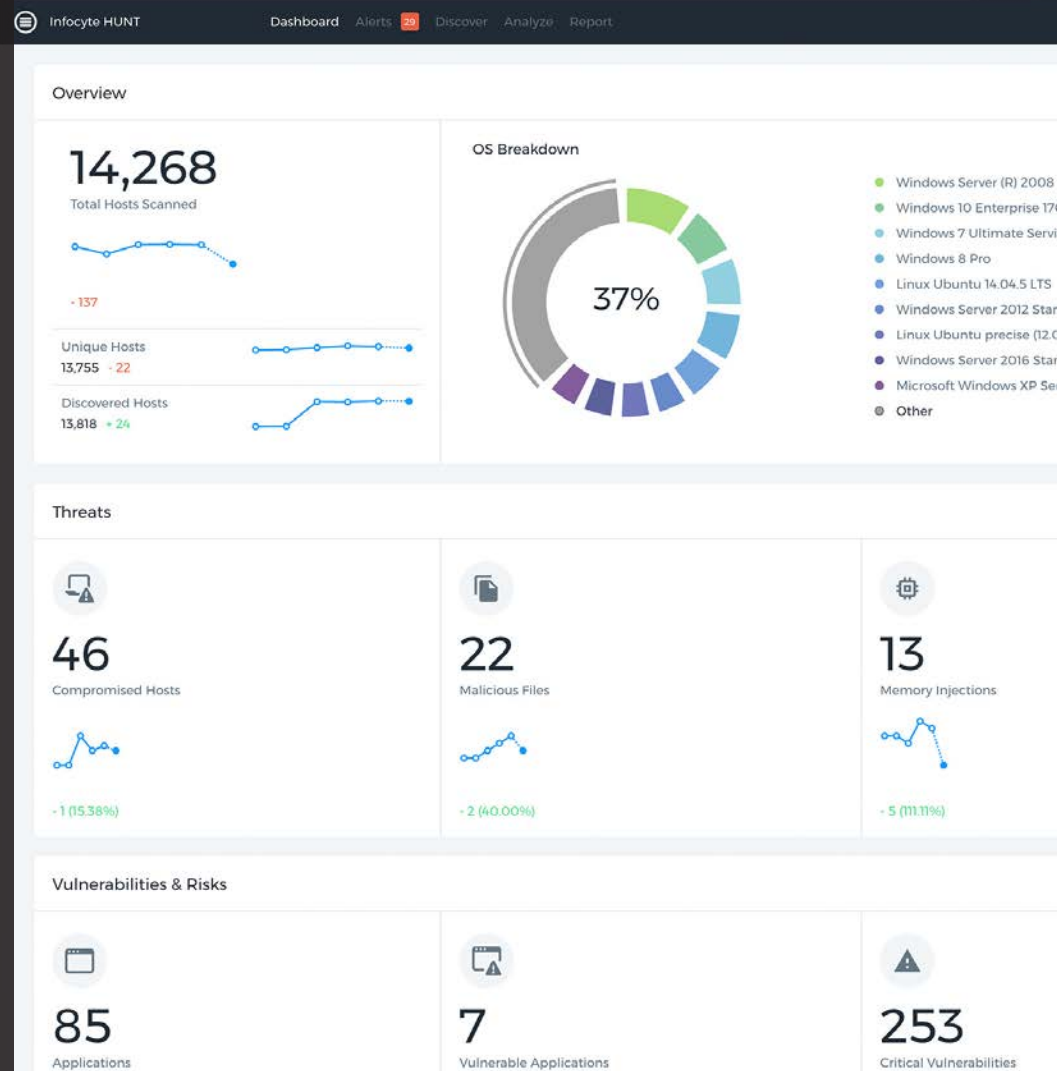
AGENTLESS OR AGENT

Deploy with zero operational impact when inspecting Windows, Linux, and Mac OS environments.

ACTIVITY TRACE

Instantly identify patient zero and respond to threats faster with automated timelining and triage.

SYNAPSE & INCYTE™

Enrich primary forensics data with multiple sources of threat intel to reduce noise and find real threats.

Infocyte HUNT — Dashboard · Alerts 29 · Discover · Analyze · Report

Overview

14,268
Total Hosts Scanned
- 137

Unique Hosts
13,755 - 22

Discovered Hosts
13,818 - 24

OS Breakdown

37%

- Windows Server (R) 2008
- Windows 10 Enterprise 170
- Windows 7 Ultimate Servi
- Windows 8 Pro
- Linux Ubuntu 14.04.5 LTS
- Windows Server 2012 Star
- Linux Ubuntu precise (12.0
- Windows Server 2016 Star
- Microsoft Windows XP Se
- Other

Threats

46
Compromised Hosts
- 1 (15.38%)

22
Malicious Files
- 2 (40.00%)

13
Memory Injections
- 5 (111.11%)

Vulnerabilities & Risks

85
Applications

7
Vulnerable Applications

253
Critical Vulnerabilities

ABOUT

Infocyte's easy-to-use yet powerful detection and response platform helps security teams reduce cyber risk, control dwell time, and stop sophisticated attacks before they start.

Reduce cyber risk, streamline security operations, strengthen their endpoint security, and reinforce your SOC with Infocyte.

- Detect and respond to advanced cyber threats

- Reduce alert noise and improve analyst efficiency

- Respond to security incidents at scale (one-to-many)

- Reinforce your cyber-security team and tools

Infocyte combines continuous process monitoring with differential forensic analysis to expose current, past, and triggered cyber attacks. Detect and respond to advanced persistent threats (APTs), file-less malware, and zero-day attackers at scale.

No other detection and response platform delivers the speed, power, and precision of Infocyte.

Learn more, request a demo, or start your free trial at infocyte.com

WHY INFOCYTE

Independent.

Independence from your existing security stack — EDR, EPP, AV, UEBA, ITSM, and SOAR — to reduce noise and improve efficacy. Detect and respond to vulnerabilities and sophisticated attackers (polymorphic, file-less, and persistent threats) traditional tools are prone to miss.

Easy to use.

Configure and deploy Infocyte from the cloud, and begin detection and response operations within minutes. An easy-to-understand interface and on-demand access to our Security Operations Center ensures your security team has the tools, technology, and experience to succeed.

Fast and lightweight.

Agentless surveys can forensically scan up to 5,000 nodes per hour. Deploy and use Infocyte across your entire IT environment — on-premise, data center, virtual and cloud architectures — without impacting network productivity or business continuity. Deploy via API in your Amazon Web Services (AWS) Cloud to assess, detect, respond to, and recover from risks, threats, vulnerabilities, and more.

Extensible.

Integrate and extend your AV, SIEM, SOAR, ITSM, and more with Infocyte. Strengthen, optimize, and streamline security operations across your entire cyber-security ecosystem. Develop, deploy, and share custom collection (analysis) and action (response) extensions, including: eDiscovery (PII forensics), host isolation, in-memory forensic analysis, and Windows Volume Shadow Copy and restoration.

AUTOMATED, INDEPENDENT, AND CLOUD-DELIVERED DETECTION & IR.

THREAT ASSESSMENTS

Independently and conclusively measure risk with asset, vulnerability, and forensic threat detection.

CONTINUOUS MONITORING

Detect, investigate, and remediate advanced cyber threats across distributed IT environments.

INCIDENT RESPONSE

Automated triage and analysis, and custom extensions help you respond at scale without additional resources.

Infocyte is the only platform featuring Forensic State Analysis, an advanced detection technique that conclusively determines the compromised state of your hosts, enabling you to identify unauthorized users, threats, and software difficult to categorize with standard monitoring and logging tools.

Perform a comprehensive survey of your entire IT environment and inspect live volatile memory, persistence mechanisms, forensic artifacts, OS integrity and more — at scale.

Start a Free Trial:

infocyte.com/trial

24x7 Managed Security Services

Infocyte Command

Reinforce your organization's cybersecurity posture with expert threat hunters, security analysts, plus first-hour incident response and tailored monthly threat intel reports.

THE INFOCYTE ADVANTAGE

FORENSIC DEPTH

- Automatically detects the post-compromise indicators AV and defensive tools often miss
- Unique, scalable volatile memory analysis finds all file-less implants—at scale
- Autostart and Forensic Artifact analysis finds threats—active, dormant, and scheduled

MANAGED DETECTION

- Automates and integrates threat hunting into your risk and vulnerability management process
- Continuously hunt or perform continuous assessments to mitigate your cyber risk
- Go beyond vulnerabilities and identify any threats that may have exploited them

EASY IMPLEMENTATION

- Lightweight agent or agentless deployment options
- Survey thousands of endpoints simultaneously vs. 'single-host' forensic tool alternatives
- Cloud-deployable, easy to assess, monitor, and respond across distributed environments
- Zero change management and no business disruption

RESPONSE READINESS

- Control dwell time to limit breach damage and costs
- Reinforce and support existing cyber defense stack
- Independently detect, investigate, and respond to cyber threats at scale (one-to-many)
- Quick access to root cause and patient zero via Activity Trace

Infocyte

ABOUT INFOCYTE

Developed by former U.S. Air Force cybersecurity officers, Infocyte's forensics-based threat detection and incident response platform discovers the post-compromise activity of hidden cyber attackers 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.

CORPORATE HEADQUARTERS

Infocyte, Inc.
3801 North Capital of Texas Hwy
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com

REDUCE RISK, MAINTAIN COMPLIANCE, STREAMLINE SECURITY OPERATIONS AND RESPOND FASTER WITH INFOCYTE.

START YOUR FREE TRIAL

Discover why Infocyte is leader in proactive threat and vulnerability detection, on-demand incident response, and instant compromise assessments.

www.infocyte.com/trial

THE CHANNEL CO.
CRN TECH INNOVATORS

SC 2017 awards
finalist

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2018

CYBERSECURITY BREAKTHROUGH AWARDS