FEATURE OVERVIEW

Forensic State Analysis

Fast, forensic-based cyber threat hunting—pioneered by Infocyte.

WHAT IS FORENSIC STATE ANALYSIS?

Cyber threat hunting, by definition, is the proactive and systematic inspection of assets, systems, and hosts on your network in search of threats that have evaded your cybersecurity defense measures. There are two primary ways you can hunt threats: log analysis or via threat hunting software.

Threat hunting software is designed to inspect either the *network* or the *endpoints* on your network. Traditional network hunt tools scan logs/activity, but fall short when it comes to validating the compromised state of endpoints. Infocyte HUNT is the only threat hunting software that uses Forensic State Analysis (FSA) to inspect the endpoints on your network.

By hunting on your endpoints, Infocyte HUNT is more effective at finding and isolating attackers, breaches, malware, and more.

LOG ANALYSIS THREAT HUNTING

What it is: Event/activity focused, hunts on the network

What it does: Analyzes network-wide event and sensor data for anomalies and inconsistencies

What it requires: Mature centralized logging and retention of network/endpoint events, data storage, processing power

Collection: Behavior analysis and log collection focuses on:

- Network logs (flows, firewall, proxy, DNS)
- Server logs (Active, Directory, web)
- Endpoint logs (EDR logs)

Drawbacks:

Logs don't go back far enough or have limited coverage:

- The average attacker dwell time is 6 months, so you need at least 6 months of log data
- Logs must cover all network devices, as adversaries can go dark for long periods of time

Too much data is sometimes worse than none at all:

- On large networks, search querries can be expensive and time consuming
- Threat hunters must know what to look for and what search queries to use

Requires a forensics-based endpoint interrogation capability to validate anomalies.

INFOCYTE HUNT (FORENSIC STATE ANALYSIS)

What it is: Forensic, host-based hunting on each endpoint

What it does: Inspects forensic data from multiple hosts for evidence of compromise, including within live volatile memory

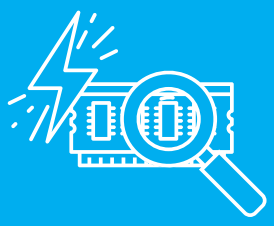
What it requires: Credentialed access to your endpoints

Collection: Infocyte HUNT deploys dissolvable or continuous agent to inspect hosts, including:

- Active Processes (modules, drivers, scripts, etc.)
- In-Memory Executable Code (volatile memory analysis)
- Auto-runs (Enumerate persistence mechanisms)
- Execution Artifacts (shim cache, prefetch, superfetch)
- OS Subversion (API hooks, configurations, disabled controls, etc.)
- Privileged Accounts
- Active Host Connections & Listeners

FORENSIC STATE ANALYSIS

Easy, lightning fast, and conclusive



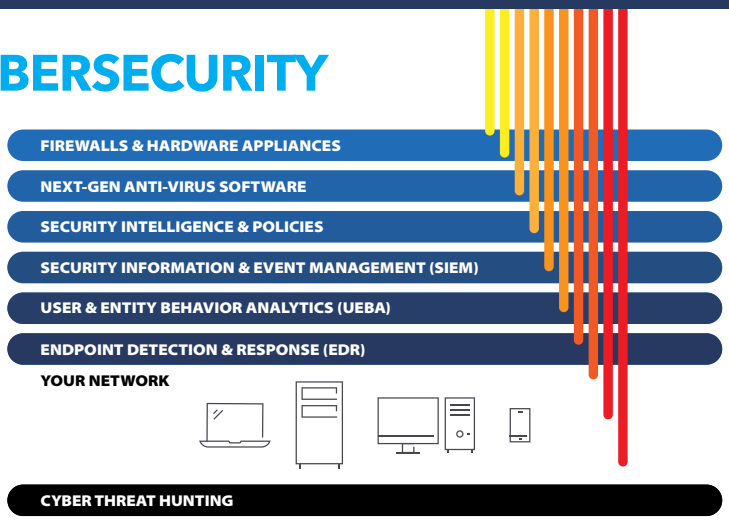
FSA is an automated approach to post-breach threat detection, enabling you to hunt cyber threats quickly and at scale. Using dissolvable and/or installed agents, Infocyte HUNT quickly collects live forensic data from your endpoints, including from both volatile and non-volatile memory. Non-memory based information is also collected to identify persistence mechanisms. This data is then analyzed using a variety of post breach analytics techniques, reputational, and multiple threat intelligence sources. Combining this live host forensic data and these analytic techniques, FSA determines the compromise state of your endpoints.

DEFENSIVE VS. PROACTIVE CYBERSECURITY

Layering defensive cybersecurity solutions is a good practice, but defensive technologies cannot prevent 100% of attacks.

Cybersecurity should be approached with the acceptance that adversaries will breach your defenses (if they haven't already). You need to be proactive, seek out the adversaries that have breached your defensive layers and eliminate them. Then, re-inspect and validate your environment, assets, and endpoints.

Infocyte HUNT assumes breach and systematically hunts the attackers, malware, and threats capable of evading even the world's best defensive technologies.



INFOCYTE HUNT

Infocyte HUNT is the only threat hunting platform that uses FSA to determine the compromise state of your endpoints and takes memory forensics to an entirely new level of scalability – enabling you to survey and analyze live memory data across thousands of endpoints simultaneously. FSA also analyzes OS and application persistence mechanisms – which can trigger the exectution of code or executables. This provides a far deeper, and more conclusive, examination of an endpoint's state.

Here are some of the functions Infocyte HUNT performs:

EVALUATING

- All active processes, loaded modules, scripts, and drivers
- All active host connections (including interprocess and redirects)

INDENTIFYING DISABLED SECURITY CONTROLS

- Disabled AV
- Reduced authentication requirement configurations
- GPO blocking, etc.

IDENTIFYING AND EVALUATING

- Memory Injected modules — Infocyte uses memory un-mapping techniques to export memory objects for offline retention and analysis
- Process Manipulation (such as Hooks, inline modifications/patching, etc.)
- Operating System Manipulation (including list modifications, hidden processes, direct kernel object manipulation)

ENUMERATING AND EVALUATING PERSISTENCE MECHANISMS

- Chronjobs
- Registry autostarts/triggers
- DLL hijacking
- WMI events
- Boot process redirection
- Watchdog processes, and more

AUDITING

- All privileged user accounts (e.g. ID rogue local administrator accounts)
- Legitimate remote administration services, such as:

Cmd	SSH	RDP
Powershell	VNC	Tunnels
NetSH	PSExec	WMI

Infocyte

3801 N. Capital of Texas Hwy.
Suite D-120
Austin, TX 78746

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

LEARN MORE ABOUT INFOCYTE HUNT

Please contact us to learn how Infocyte HUNT can help your organization identify, contain, and eradicate the cyber threats your defensive tools miss.

TRY HUNT FOR FREE »

Discover why Infocyte HUNT has been recognized as a top threat hunting solution by industry leaders.

infocyte.com