Infocyte®

Threat Hunting Using Forensic State Analysis

FORENSIC STATE ANALYSIS (FSA)

Forensic State Analysis is something completely different from endpoint monitoring or behavior analysis. And no, it's not just an Indicator of Compromise (IOC) scanner. IOC scanners are cute, but they are far too superficial to hunt for, and find, a wide range of persistent threats resident within a network. However, a comprehensive FSA tool will come as close as one can get to being able to say, "this endpoint is clean". Endpoint monitoring tools like EDR will never be able to make that claim. It's simply not their designed function.

Infocyte recently attended the 2017 SC Magazine's Awards Ceremony as a nominee for the Best Forensics Solution. It's certainly an honor to be nominated for this award. But frankly, we're a bit of an anomaly in this category. Let me explain. Unlike the other solutions, like Guidance Software's Encase, Infocyte HUNT is not a pure forensics solution. On the contrary, what we have done is novel among commercial cybersecurity products. We have morphed endpoint digital forensics for proactive and scalable threat hunting (the search for unknown compromises/threats that have already bypassed other security controls).

We call it Forensic State Analysis (FSA).

Now, skeptics might stop reading right here and suggest the digital forensics incident response (DFIR) community and top tier incident response (IR) firms like Mandiant have been doing something similar for years. Hold up, keep reading - I promise you this is not the same thing.

Our finalist nominated solution, Infocyte HUNT, is an agentless endpoint hunting platform that uses FSA to discover hidden threats and compromises within a network. It sweeps thousands of endpoints, spending a couple minutes on each host, and conclusively validates their state: "Compromised" or "Not Compromised".

At the highest level, we dig deep into an endpoint to validate 1) what is actively running, and 2) what is triggered to run (through a persistence mechanism). Next, we work to identify 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, i.e., rootkit.

Note this is starkly different from the behavior analysis techniques used by your Endpoint Detection and Response (EDR) or User Behavior Analytics (UBA) products - which only records 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.

To illustrate, let's take a closer look at the differences.

State vs Behavior Analysis

These days, the security industry is quite enamored with behavior analysis and detection. Some believing (wrongly) it's the only way to detect advanced threats. To wit, we occasionally get asked by analysts and prospects alike, "How does Infocyte do behavior analysis if it's agentless?" The answer is: we don't. Other than sandboxing during binary analysis phases, we don't use behavior detection techniques at all.

Forensic State Analysis is something completely different from endpoint monitoring or behavior analysis. And no, it's not just an Indicator of Compromise (IOC) scanner. IOC scanners are cute, but they are far too superficial to hunt for, and find, a wide range of persistent threats resident within a network. However, a comprehensive FSA tool will come as close as one can get to being able to say, "this endpoint is clean". Endpoint monitoring tools like EDR will never be able to make that claim. It's simply not their designed function. EDR tools monitor endpoints for behaviors indicating there is an attack, they don't perform forensic validation of cleanliness. As an analogy, EDR and behavior monitoring's entire premise is centered on the idea that if you are monitoring all the doors, nobody could possibly be in the house. Breach after breach has proven that to be false.

And yes, I said "clean". I know, I know. Security cynics will cry "Blasphemy!" I get it. Even our CTO would quickly agree with you that nothing is foolproof. But, stay with me here. Let's look at this from a business perspective. When the President of the United States stays in an overseas hotel, a team of Secret Service agents arrives in advance and sweeps for bugs in the presidential quarters. Do they expect their equipment will find every unknown spy technique? Of course not. But a room swept for bugs using a reasonably comprehensive process is exponentially safer than an un-swept room.

By comparison, if you are a CISO, your job is to satisfactorily and cost-effectively de-risk operations within an organization. Knowing that, each week, all networked information systems were forensically validated - and they have a high confidence their operations, emails, or financial trades aren't being monitored gives an increasingly nervous board or C-suite a degree of confidence about moving forward without being paralyzed by fear being hacked. That has value.

So what is the difference on the technical level? It starts with what kind of data is being collected and analyzed.

Behavior Analysis

In behavior monitoring and analysis - such as what an EDR product does - collection and analysis is event-centric. Examples include the recording of:

- Process Execution Events (occasionally with command line used, if enabled)
- Process Changes (elevation of privileges, process crashes, etc.)
- Select Registry Changes/Writes
- Select Disk Writes (i.e. download/user folders, windows folder, etc.)
- File Creation Events
- Monitoring of select API Calls (monitoring all would be impossible)
- Network Connection Events (or sampling thereof)

Now, let's be fair. These are all good things to monitor – if you want to catch an attack in progress.

Forensic State Analysis

In contrast, FSA does not rely on logs or monitoring events/changes to a system. Instead, FSA assumes the device is already compromised and seek to validate every aspect of the system as deep as possible. To accomplish that, analysis and collection includes:

- Evaluating All Active Process
- Evaluating All Loaded Modules and Drivers
- Identifying and Evaluating Memory Injected Modules (Note: Infocyte goes way beyond identification here. We use proprietary memory un-mapping techniques to export memory objects for offline retention and analysis)
- Identifying and Evaluating Process Manipulation (Function Hooks, Inline modifications/patching, etc.)
- Identifying and Evaluating Operating System Manipulation (List modifications, hidden processes, Direct kernel object manipulation)
- Identifying Disabled Security Controls (disabled AV, reduced authentication requirement configurations, GPO blocking, etc.)
- Enumerating and Evaluating Persistence (cronjobs, registry autostarts/triggers, DLL hijacking, WMI Events, boot process redirection, watchdog processes, etc.)
- Evaluating application execution artifacts (Prefetch, Shimcache, and SuperFetch)

- Identifying and Evaluating Web Shells (Linux or IIS web servers)
- Auditing legitimate Remote Admin services (cmd, Powershell, NetSH, SSH, VNC, PSExec, RDP, Tunnels, WMI)
- Evaluating all Active Host Connections (include interprocess and redirects)
- Auditing all privileged User Acccounts (ID rogue local admin accounts, etc.)

Perhaps the most important aspect of ensuring 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.

Why you need it

We aren't suggesting that FSA replaces the need for centralized logging or real-time behavior monitoring. On the contrary, they are highly complimentary – filling the gap in post-compromise detection. For the mature enterprise SOC already hunting, Infocyte HUNT enables you to do away with the custom scripts and other one-host-at-a-time DFIR processes you use to validate suspicious behaviors your team detects. Now you can iteratively and effectively sweep all endpoints to find entrenched threats and beachheads hiding on any of your endpoints. Many SOCs are probably already doing a lighter version of this now using a custom tool set or scripting out an endpoint querying tool - which, unfortunately, won't bypass anti-forensics.

Beyond improving your monitoring and hunt processes, FSA enables entirely new use cases:

- Laptops, mobile devices, and other transient systems not previously under management can now be validated as they come on the network
- Systems without endpoint monitoring (due to policy, mismanagement, or tampering) can be identified and periodically assessed
- For organizations that don't have enough historical logs or ability to convert big data into definitive action, FSA is a huge bang for the buck
- For consultants and IR professionals, FSA is the fastest and easiest way to perform a compromise assessment or threat hunting engagement service. Further, using an agentless method like Infocyte HUNT negates the need for most change management processes, significantly simplifying your engagements

There are a multitude of reasons to incorporate FSA into your security operations process. **Ready to see for yourself? Contact us.**

Adapted from blog post posted February 14, 2017 by Chris Gerritz, Founder of Infocyte

Infocyte®

CORPORATE HEADQUARTERS
110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc