Anatomy of a Cyber Attack

Understanding The Role of Defensive Technologies and Forensic State Analysis in Breach Detection and Prevention

WHITE PAPER

Infocyte®

Table of Contents

Executive Summary

Threat Hunting is the search for unknown compromises and threats that have already bypassed prevention-oriented security controls

More than just hype, threat hunting is a legitimate and necessary tactic for modern cybersecurity practitioners. A recent threat hunting survey cited the top efficiency benefits from a threat hunting platform as reported by respondents were: improving the detection of advanced threats (72%), creating new ways of finding threats (68%), discovering threats they could not discover otherwise (67%), and reducing investigation time (66%).

And the benefits of threat hunting impact your bottom line. The 2017 Ponemon Institute report showed that how quickly an organization contained a data breach had a direct effect on the financial impact. Case in point, the cost of a data breach was nearly $1 million lower for organizations that were able to contain the breach in less than thirty days.

Looking to capitalize on the benefits, the security market has suddenly become crowded with solutions that all claim to offer threat hunting capabilities: EDR, DFIR, Behavior Analysis and FSA.

Understanding the differences between threat hunting tools and the role each plays in breach detection and prevention

Threat hunting with FSA or Forensic State Analysis offers a unique approach that is complimentary to other threat hunting approaches. It is not a replacement for alternative approaches like Endpoint Detection and Response (EDR) or Digital Forensics and Incident Response (DFIR). That said, FSA provides the most conclusive post compromise detection ability, is the easiest to use, and is by far the most cost effective approach on the market.

The purpose of this paper is to explain FSA in more detail, such that hunt practitioners, security budget decision makers, and risk management leaders can understand why deep memory state analysis provides so much promise in the fight to stop adversaries from reaching their ultimate theft or damage objectives. It also introduces Infocyte HUNT, a threat hunting tool that offers post breach detection using Forensic State Analysis (FSA) to discover hidden threats and compromises within a network.

This paper will help you understand the differences between threat hunting tools and the role each plays in breach detection and prevention, and where solutions such as Infocyte HUNT fit within the tool belt of the hunter.

Top efficiency benefits from a threat hunting platform cited by survey respondents:

- Improved detection of advanced threats (72%)
- Creates new ways of finding threats (68%)
- Discovers threats they could not discover otherwise (67%)
- Reduced investigation time (66%)[1]

The benefits of threat hunting impact your bottom line:

The cost of a data breach was nearly $1 million lower for organizations that were able to contain the breach in less than thirty days.[2]

[1] 2017 Threat Hunting Report Crowd Research Parters
[2] 2017 Ponemon Institute 2017 Cost of Data Breach Study: Global Overview.

Today's thefts have moved online where the stakes and payloads are higher:

- Company data
- Credit card numbers
- Personal data (PII)
- Corporate IP
- Critical infrastructure

The Setting

You've seen this play out in a Hollywood movie more than once. The one where there is a jewel heist from within a supposedly well-guarded building. Except today's thefts have moved online where the stakes and payloads are higher; company data, credit card numbers, personal data, corporate IP, and even access to critical infrastructure.

Let's quickly break down the story.

The antagonist. There is a hacker. He wants in. But he knows there are lines of defenses. So he must understand them, and figure out how to skirt them, at least until after the "jewel" is in hand and he is well out the door.

The protagonists. The security folks, IT team, and managed services providers whose job it is to prevent the hacker's entry, find him if he trips a wire along his journey, or investigate how he did what he did, if he somehow escapes with the jewel – so we can maybe we can stop him in his tracks, but at least learn from our "defense in depth" shortfalls.

Well, there is (arguably) a rough analogy here – but one that is good enough for our purposes. And, that analogy is to break down the anatomy of the attack into movie acts – so we can see where different "hunt tools" can be brought to bear.

Get the popcorn.

Act 1 – Attacker Entry

The first step is to get into the building. But there are system alarms, security guards at the front desk, security cameras, maybe motion sensors in a few hallways, elevator movement monitors, etc.

Action! Let's catch the attacker in the initial act – an actual breach in process!

Enter EDR.

ENDPOINT DETECTION AND RESPONSE

What if our hacker is especially crafty? What if he is equipped with evasion techniques that render your behavior monitoring defense-in-depth systems inert? Or worse, what if he knows about an entry point that you don't monitor?

EDR products typically rely upon behavior monitoring and analysis technology for their purported "hunt" capability. Their approach is to record changes to a system (or network) as events (new process spawn, registry key change, or user privilege escalation) occur. Examples of recorded data include:

- 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 select API calls (monitoring all would be impossible)
- Network connection events, or the sampling thereof

These are valid things to monitor – provided the goal is to catch an attack in progress.

But, what if our hacker is especially crafty? What if he is equipped with evasion techniques that render your behavior monitoring defense-in-depth systems inert? You've seen this: Gas that puts the guards to sleep. Jumper wires that prevent alarms from activating. Still photos in front of the camera lens that tells the security guard in the camera room (if he's not messing around on Facebook) that all visual movement monitoring is well. Mirrors that trick laser trip wires.

Or worse, what if he knows about an entry point that you don't monitor? One that you didn't know could be breached, so you never knew to monitor it. Oops. Sounds like a zero-day.

Now we have a problem. The hacker is in the network. And, all those front line defenses set up to detect and alert on entry? Well, our guy is behind them now. So, they're kind of, to be blunt, useless.

Act 2 – The Attacker Is In. But How Would You Know?

Our guy is in. Now his goal is to sneak around until he finds the exact right room; server, network, PC. The one with the jewel in the glass case, the payload. But, this will take time. And, so he must move intelligently, staying under cover at all times. And, as he moves, he'll be searching to find keys – user passwords, admin credentials, etc. – in one 'room' that will help him enter the next (without being noticed), if he can find the right disguise.

Hold on. What if we had systematic monitoring of each and every room – or endpoint in this case? And, what if that monitoring was super sophisticated, able to see individual footprints; suspicious code, memory injected modules, process manipulations, etc. – all on a per endpoint basis? Sounds great, but that's a lot of data to collect and analyze. But, if we could do it, we'd have a great way to detect the whereabouts of the attacker who has compromised our frontline defenses.

A recent Crowd Research Partners report found that 44% of security threats go undetected by automated security tools.

To make matters worse, the average security breach goes undetected for over 6 months.[1]

This is where Forensic State Analysis (FSA) enters the picture.

FORENSIC STATE ANALYSIS

At the highest level, FSA assesses three things in detail:

- What is actively running on an endpoint
- What is triggered to run – through a persistence mechanism – on an endpoint
- The identification of any operating system (OS) manipulation, or active process, e.g., what a rootkit does to hide its presence, or what an insider threat might do to disable the system's security controls

Examples of findings include things like unusual OS configuration settings, or API calls being hooked by a rogue/hidden process within volatile memory, i.e., a rootkit.

FSA does not rely on logs or monitoring events/changes to a system. FSA assumes the device is already compromised and seeks to validate every aspect of the system as deeply as possible.

Infocyte HUNT uses FSA to discover hidden threats and compromises. It sweeps thousands of endpoints, spending a couple minutes on each host, and conclusively validates their state: "Compromised" or "Not Compromised". To accomplish that, analysis and collection includes:

1. Evaluation of all active processes
2. Evaluation of all loaded modules and drivers
3. Identification and evaluation of all memory injected modules (note: Infocyte HUNT goes well beyond simple identification here)
4. Proprietary memory un-mapping techniques – which are used to export memory objects for offline retention and analysis
5. Identification and evaluation of process manipulations, e.g., function hooks and in-line modifications / patches
6. Identification and evaluation of operating system manipulation including list modifications, hidden processes, and direct kernel object manipulations

7. Identification of disabled security controls, e.g., disabled anti-virus, reduced authentication requirement configurations, GPO blocking

8. Enumeration and evaluation of persistence including cron jobs, registry auto-starts / triggers, DLL hijacking, WMI Events, boot process redirection and watchdog processes

9. Evaluation of application execution artifacts, e.g., Prefetch, Shimcache, and SuperFetch

10. Identification and evaluation of web shells – Linux or IIS web servers

11. Auditing of legitimate remote admin services like cmd, Powershell, NetSH, SSH, VNC, PSExec, RDP, Tunnels and WMI

12. Evaluation of all active host connections, including inter-process and redirects

13. Auditing of all privileged user accounts, e.g., ID rogue local admin accounts

FSA Using Infocyte HUNT

Further, successful state analysis of a compromised machine requires the ability to bypass anti-forensics techniques. Infocyte HUNT accomplishes this by:

- Going underneath higher-level operating system APIs, and;
- Working directly with volatile memory structures.

So you see, post compromise detection is different from finding an attack in progress. And yet, that difference remains an area of confusion for many. In fact, prospects and industry analysts often ask, "How does Infocyte perform behavior analysis if it is agentless?"

Well, it doesn't.

With the exception of sandboxing during binary analysis phases, Infocyte HUNT does not use behavior detection techniques at all.

Given the extensive endpoint state collection and analysis performed by FSA, it comes as close as possible to being able to assert 'this endpoint is clean'. Or, in our movie parlance, 'this room is clean.'

EDR will never be able to make this claim. It is simply not designed to do so. Again, EDR tools monitor endpoints for behavior indicating an attack is underway. They do not perform forensic validation of endpoint (room) cleanliness.

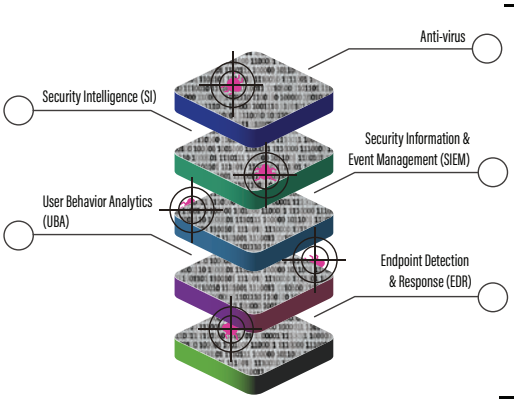
To further drive the point, EDR, and its behavior monitoring feature set, is centered on the premise that if you monitor all doors and windows, no unwanted person could possibly be inside the house. Breach after breach has clearly proven this to be patently false.

Now, no one is suggesting that FSA is somehow perfect. However, it should be clear that analyzing the state of affairs of a room past the point of entry delivers unique and compelling value.

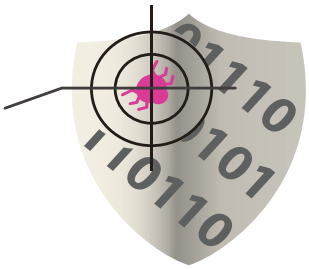
Here's an example that fits our story. When the President of the United States stays in an overseas hotel, a team of Secret Service agents will arrive in advance, and sweep the presidential quarters for bugs.

Will their equipment find every unknown spy technique? Probably not. The security personnel at the hotel can be the most sophisticated in the industry, have all the latest locks on the doors, security cameras, and exterior defenses a hotel could possibly use (similar to EDR). And yet, the secret service is still going to sweep the room for bugs and verify no intruders are currently in the room (FSA). A room swept for bugs, using a reasonably comprehensive process, is far safer than an un-swept room.

Forensic State Analysis provides a safety net, should prevention and monitoring fail to discover the threat



Infocyte HUNT Uses FSA to Detect Breaches & Malware Defensive Technologies Miss



As a security pro your job is to satisfactorily and cost-effectively de-risk operations within an organization. If all endpoints are forensically validated on a weekly basis, there is a much higher confidence that operations, emails, financial trades, etc. aren't being illicitly monitored. There is a much higher chance that the burglar will not achieve his final objective of getting that jewel.

And, this validation will provide business assurance to your increasingly nervous board and executive team – the ones who will lose their jobs if that jewel gets stolen.

Act 3 – We Found Our Attacker. Now What?

You just cannot afford to do DFIR on every endpoint at a high enough frequency to detect an attack in progress, let alone the more difficult work of sweeping an entire building for post compromise detection.

There are only three ways this can end:

1. Our hacker gets in, gets out with the jewels and we never saw him.

   In fact, we are so weak at security, we don't even recognize the jewel is gone until six months after the fact. Sadly, many corporate cyber security stories play out this way. Why? Well first, they trusted defense-in-depth. Second, in a corporation, there isn't just one jewel. There are hundreds to thousands of them. Intellectual property repositories. Credentials left and right. Personal privacy records by the truckload. Payment card data. In fact, there are so many, that we don't even know where they all are at a given point in time.

2. We catch our hacker as he enters, i.e., while his entry attack is underway.

   Great. He got past our prevention investment which is where we spend most of our budget, wrongly, given modern burglar sophistication. But, thankfully, he tripped a behavioral wire. We detected this "indicator of compromise". And then, we had our really bright security analyst (who is rare, busy, and very expensive) take a look at this indicator, match it up to a lot of other big data, and conclude – correctly (this time) that it is in fact a real burglar, and not the janitor.

3. We catch our attacker – who cleverly got past all of our prevention and entry detection mechanisms – but was not able to evade our FSA hunting methods.

In any of these outcomes, the third act is all about accosting him if we can, and then once the dust settles, figuring out how he got that far – so we have a clue about how to prevent that movie from going to a sequel.
This is where Digital Forensics Incident Response (DFIR) comes in.

DIGITAL FORENSICS INCIDENT RESPONSE

Digital Forensics and Incident Response (DFIR) is the procedure of investigating security alerts or suspicions of malicious activity in a computer network. By examining a breach or an attacker's infiltration in detail, a skilled forensic analyst can come to understand misconfigurations, lack of security measures that might have allowed the attack to take place, and attack details that can assist remediation.

DFIR solutions are fabulous. It's the blue light in the forensic specialist's hand that finds all kinds of nasty evidence at the scene of the crime. It goes down to the granular level of DNA analysis of a hair.

There is just one problem. DFIR is designed to focus on the deep data collection and analysis of a single endpoint at a time – and by yet another highly skilled, highly specialized, and, therefore, very expensive analyst.

You just cannot afford to do DFIR on every endpoint at a high enough frequency to detect an attack in progress, let alone the more difficult work of sweeping an entire building for post compromise detection.

The End. What Did You Learn?

Act 1 is pretty straightforward. Stop him from entering via prevention. Or detect his entry via indicator of compromise and/or behavioral analysis. That can work. But, as we know, often it does not. So this act is not that “intriguing”.

Act 2. He got in. He is smart. He is crafty. He knows when to move and when to lay low. Ah, now we have an interesting story. Game on. If you are using FSA and Infocyte HUNT, that is.

Act 3. Frankly, boring. Yeah, it’s cool to know how the guy did what he did, but the damage is done if he succeeded.

The hero of the story is FSA. But, FSA is not a replacement for centralized logging or real-time behavior monitoring. These compromise discovery approaches have their place. But, they are complimentary to FSA post-compromise detection. Let’s look closer.

For mature audiences (enterprise SOCs) that have already adopted hunting:

- FSA enables the elimination of custom scripts and/or single-host-at-a-time DFIR processes used to validate suspicious behaviors detected by your team
- FSA enables hunt teams to iteratively and effectively sweep all endpoints to find entrenched threats and beachheads hiding on any of your endpoints

Now, many SOCs are likely already doing a lighter version of the above, but with a custom tool set or scripting out an endpoint-querying tool. Not only are these approaches difficult to scale and maintain, they will have limited effectiveness – as they are unable to bypass anti-forensics safeguards.

For newer moviegoers (i.e. newer or smaller Hunt teams), FSA provides, by far, the biggest bang for the buck. Infocyte HUNT incorporates the FSA methodology to automate the majority of the workflow and analysis for you. It finds relatively conclusive results. It does not require a department full of hard to hire, hard to retain, expensive specialists.

Finally, whether you have a sophisticated SOC, or are just at the early stages of learning to hunt, Infocyte HUNT not only supercharges your monitoring and threat hunting processes, it enables entirely new use cases:

- Laptops, mobile devices, and other transient systems not previously under management can now be validated as they join the network
- Systems without endpoint monitoring (due to policy, mismanagement, or tampering) can be identified and periodically assessed
- Organizations that don't have sufficient historical log data, or the ability to convert big data into definitive action, realize huge value from FSA
- Consultants and IR professionals now have access to the fastest and easiest way to perform a compromise assessment or threat hunting engagement service

Parting Thoughts

Movies are fun. We all love them. Cyber attacks are not fun. They will cost you money, your company’s reputation – even your job. You don’t have time to waste on rabbit hole analyses. You don’t have enough staff. You’ll never have enough budget.

Infocyte HUNT is the industry’s leading Forensic State Analysis platform. No security hunt team should be without it. Security is a tough game. And certainly, other tools have their place. But, Infocyte HUNT with its ability to perform post breach detection in a fast, effective and budget friendly manner – is your best possible threat hunting investment.

About Infocyte

Developed by former US Air Force cybersecurity officers, Infocyte's hunt technology fills a void left by today's real-time detection solutions. By focusing on the post-compromise activity of persistent attackers and insider threats, Infocyte's unique approach to security helps organizations defend their networks and critical information.

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