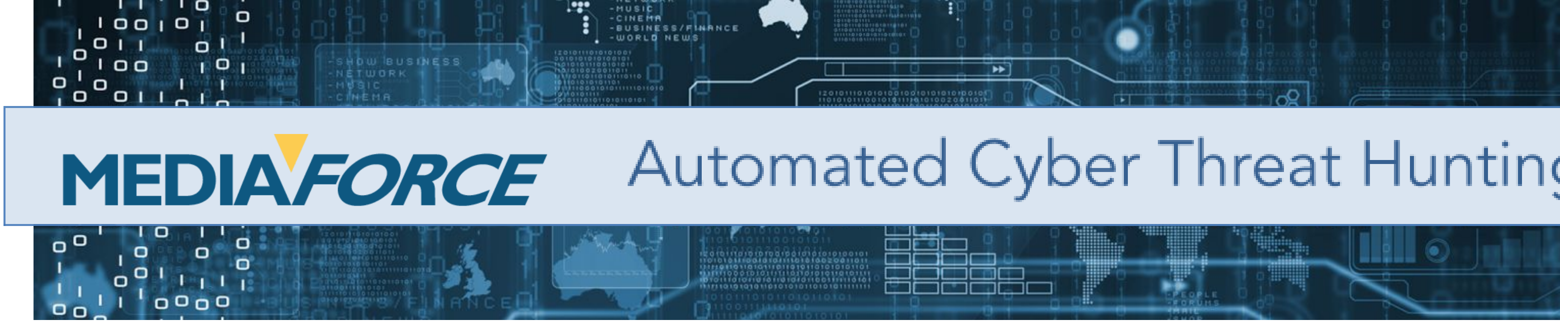


MEDIAFORCE

Automated Cyber Threat Huntin

The breach detection gap (between infection and discovery) currently sits at a global average of 146 days. Furthermore, 81% of these discoveries come from outsiders, and not your security team.

Cyber Threat Hunting starts with the idea that your network is ALREADY compromised. Taking this proactive approach, each endpoint is assessed in a matter of seconds: CLEAN or COMPROMISED.

Automate the process and let the machines do the hard part.

DETECTION: Use any security observation technology as a trigger (e.g. SIEM, NTA, EDR, NGFW).

VALIDATION: Trigger an FSA of the endpoint based on suspicion.

REMEDIATION: If the endpoint is compromised, take it offline immediately and automatically.

Reduce the Breach Detection Gap to Minutes

Whether cloud-hosted or situated on premise, Cyber Threat Hunting as a Service is an essential and complimentary addition to any organization serious about security. Armed with Forensic State Analysis, organizations can now find APTs before they morph into active threats. Reduce the gap from months to minutes, before you become the next headline.

What is Forensic State Analysis (FSA)?

FSA is an essential component of Cyber Threat Hunting that is used to discover hidden threats and compromises within a network. This agentless technology sweeps thousands of endpoints, spending approximately 90 seconds on each host, and conclusively validates their state as: "Clean" or " Compromised".

At the highest level, FSA digs deep into an endpoint to validate
what is actively running, and what is triggered to run through a persistence mechanism. Next, it works 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.

This is starkly different from behavior analysis techniques used by 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 Mediaforce 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, but it CAN leverage IOC detection solutions and automatically validate their observations. 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.

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 (Reactive)

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 (Proactive)

In contrast, FSA does not rely on logs or monitoring events/ changes to a system. Instead, FSA assumes the device is already compromised and validates every aspect of the system, including:

- Evaluating All Active Process, Loaded Modules and Drivers
- Identifying and Evaluating Memory Injected Modules
- 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 inter-process and redirects)
- Auditing all privileged User Accounts (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 the Cyber Threat Hunting Service does.

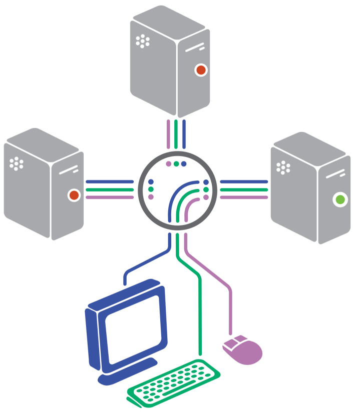
Why you need to be proactive

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, Mediaforce 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

There are a multitude of reasons to incorporate Cyber Threat Hunting services into into your security operations process. Ready to see for yourself? Contact us.



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, but it CAN leverage IOC detection solutions and automatically validate their observations.

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.

MEDIAFORCE

Mediaforce
1333 Michael Street,
Ottawa, ON K1B 3M9
info@mediaforce.ca
www.mediaforce.ca