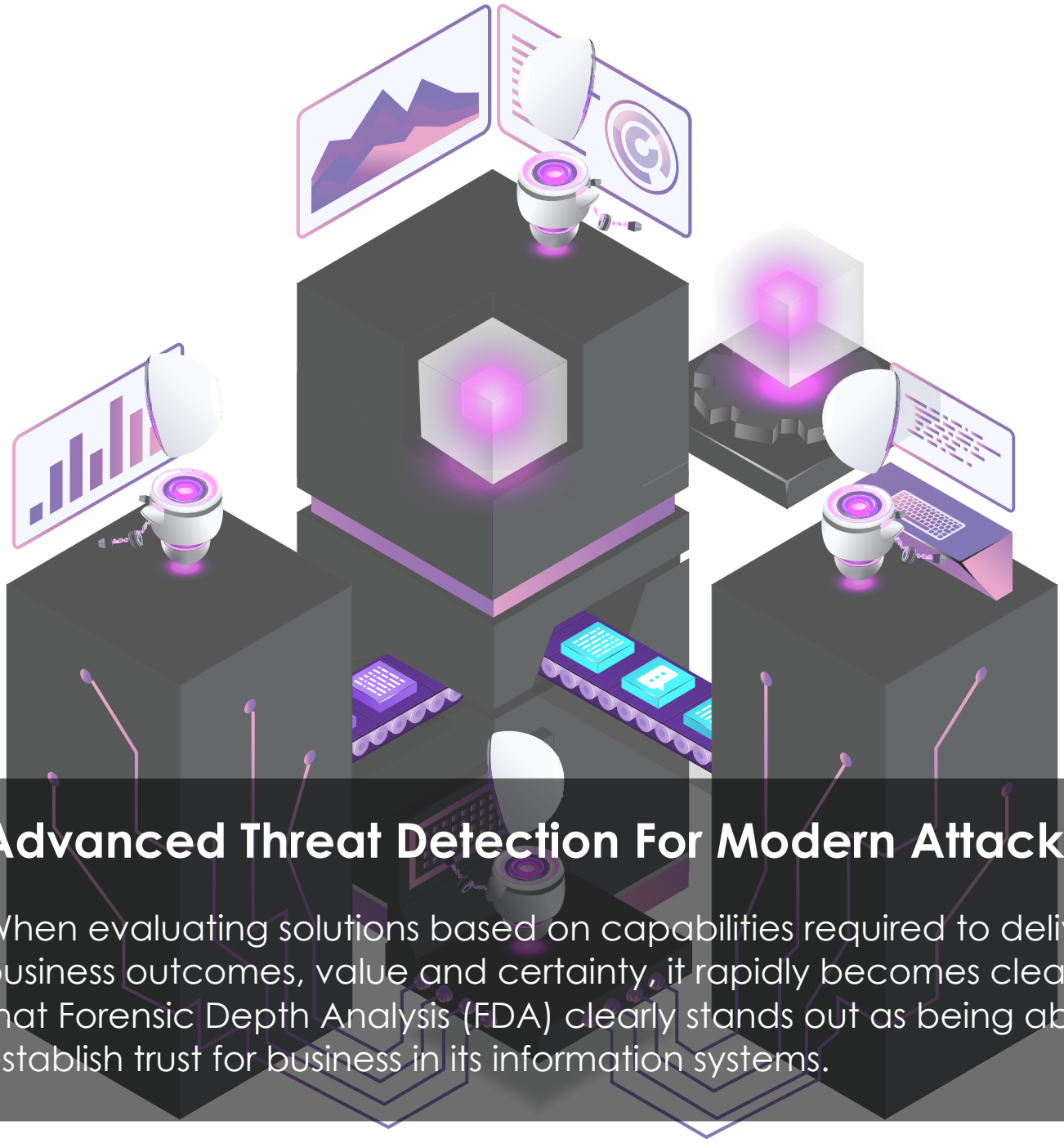
CYBER STASH

Establishing Trust For Business In Its Information Systems

Discovering Compromise to Avoid Business Impact



Advanced Threat Detection For Modern Attacks

When evaluating solutions based on capabilities required to deliver business outcomes, value and certainty, it rapidly becomes clear that Forensic Depth Analysis (FDA) clearly stands out as being able establish trust for business in its information systems.

eclipse

Context - Advanced Detection

Forensic Depth Analysis (FDA) and Endpoint Detection and Response (EDR) platforms are highly effective in detecting modern attacks. Historically, protection and defence have gone hand in hand - from first generation firewalls which were built for enterprise networks to the current EDR solutions that operate on endpoints. The array of endpoint solutions in the market testify to the accepted reality that endpoints are usually the access point for malicious software which then spreads and infects entire networks. As such they must be defended.

EDR solutions are predicated on the idea that a defensive tool can monitor a series of events along the kill chain and capture enough event information that the likelihood of something getting by undetected is significantly reduced. A fundamental underlying assumption to this approach is that there is no way to evade all of the different events along the kill chain that are being monitored. In fact, EDR vendors openly acknowledge that they sometimes miss the primary events associated with malware. Forensic Depth Analysis solutions on the other hand, while they don't prevent system compromise, provide the most complete post-breach detection capability.

Both FDA and EDR remain the most effective solutions available to enterprises however defence alone does not equal protection. In order for enterprises to adopt and maintain a low risk security posture, it is important to recognise where limitations exist and understand what value each solution provides.

Foundation Of EDR

Origins Of EDR

To fully understand today's cyber market, it's important to understand where EDR comes from. Effectively, EDR solutions arise from and are the evolution of whitelisting technologies. Whitelisting technologies monitor and prevent execution events. In doing so, whitelisting solutions were able to prevent the execution of software that was unrecognised or untrusted. Its strength was based on the fact that there were no known ways to evade execution events fired by the OS.

Floodgates Of Fileless Malware

Several years ago, security researchers disclosed findings that showed how to execute software on Windows OS without triggering any events; this discovery, and the widespread sharing of it, triggered the wave of fileless malware we experience today. This single event can be pointed to as the reason whitelisting was significantly weakened as an effective defence.
EDR solutions evolved whitelisting by adding more events and applying analytics engines to the data to uncover instances of things that don't belong and enrich the discoveries with intelligence gathered and maintained about files and events. As it stands with security technologies, early adopters reaped the greatest rewards. Today, the limits of EDR solutions are becoming well understood as vulnerabilities are exploited and attack methodologies multiply.

EDR Detection Dependencies

Event Driven Programming

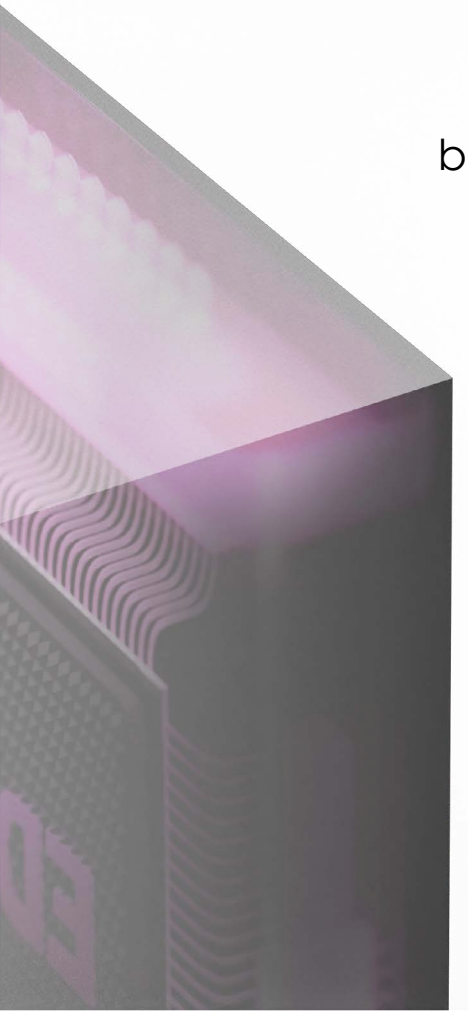
- Real time applications, such as EDR solutions, use what is called event-driven programming.
- Such programs 'listen' for events from the OS and other applications, and, are reliant on the data from these applications provided to function.
- When these programs receive notification of an event they are registered to receive, their work can begin.
- In simple terms, this is how EDR solutions collect their most critical data; the operating system raises an event and the EDR product logs the details of the event.
- Modern event driven defences will block most, but not all, threats from breaching.

What happens to the threats that successfully get past these defences?

Limitations Of EDR

There is no dispute that EDR solutions are highly effective, strong endpoint defences. However the market positioning and vendor claims made have led many enterprises to labor under false impressions. Let's examine the market claims and contrast them with the realities:

CLAIM	REALITY
All events along the kill chain are collected, nothing gets missed.	**Limited Event Collection** OS's fire tens of thousands of events per minute. EDR solutions can't collect everything without hampering the performance of the endpoint they are monitoring. Also, EDR solutions do not collect alternate channel events.
Rapid efficacy and low maintenance.	**Time and Tuning** EDR solutions require 30-90 days of endpoint data before they reach peak efficiency, and then require ongoing tuning.
You can effectively hunt for malware with the data set provided by EDR.	**Data Overload** EDR solutions produce tens or hundreds of thousands to millions of event data points per day; being able to comb this data for 'things' EDR missed is both a time consuming and high skill activity.
EDR can hunt in memory.	**Memory Protections** EDR solutions generally do not go into memory, nor do any of them forensically reconstruct discoveries. They do have SOME memory based defences - however they are focused on monitoring for events and protecting files that can be used in memory-based attacks.



The disparity between the claims being made by EDR vendors and the real-world experiences of customers using the products clearly demonstrates that there are gaps that EDR cannot address. To achieve strong protection, what's required is a solution based on the understanding that it's impossible to defend against all threats, some will bypass even the strongest defences. When threats do evade EDR defences, the EDR solutions deployed are not built to hunt the threats they missed and are residing in the estate.

Forensic Depth Analysis (FDA)

FDA INDEPENDANCE

FDA is an automated approach to post breach detection that assumes devices are already compromised and seeks to thoroughly validate every endpoint. The automation inherent in FDA enables users to deploy rapidly, dynamically, and at scale.

FDA operates independently from the host OS and uses dissolvable endpoint surveys to quickly collect live forensic data from both volatile and non-volatile memory. Non memory-based information is also collected to identify persistence mechanisms.

This data is then analysed using a variety of post-breach analytics techniques and then enriched using multiple reputation and threat intelligence sources. Combining this live host forensic data and these forensic techniques, FDA determines the compromise state of endpoints.

For robust protection, enterprises must have the ability to effectively hunt for malware and APTs that have succeeded in breaching defences, wherever they are and whether they are actively running or sitting idle but scheduled to run.

CYBERSTASH FDA

CyberStash FDA provides an automated forensic tool built to detect malware and APTs whether they are known or unknown, actively running or scheduled to run.

Using a Forensic Depth Analysis methodology and memory un-mapping techniques, CyberStash combines and examines data from multiple sources including both volatile and non-volatile memory, along with non-memory-based information required to identify persistence mechanisms.

CyberStash FDA operates independent from the host OS and collects its own data, helping to ensure unbiased results, and, that's how we're able to reduce dwell-time and provide cyber assurance.

Forensically inventories programs, memory, modules, persistence mechanisms, hooks and more to determine compromise state of endpoints.

Enriches data with intelligence gathered from 3rd parties including AV, file reputation, threat intel, catalogues, and forensic analytics.

Forensic Depth Analysis

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

1. What is actively running on an endpoint
2. What is triggered to run – through a persistence mechanism – on an endpoint
3. 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.

FDA does not rely on logs or monitoring events/changes to a system. FDA assumes the device is already compromised and seeks to validate every aspect of the system as deeply as possible. CyberStash Compromise Assessment Service uses FDA 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, Forensic Depth Analysis takes 13 Steps to definitively establish trust in an endpoint.

13 Steps For Conclusive Validation

1. Evaluation of all active processes.
2. Evaluation of all loaded modules and drivers.
3. Identification and evaluation of all memory injected modules.
4. Conduct 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 parocesses, 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.

Bypassing Anti-Forensic Techniques

To establish trust in endpoints, successful state analysis also requires the ability to bypass anti-forensics techniques. CyberStash Compromise Assessment Service accomplishes this by:

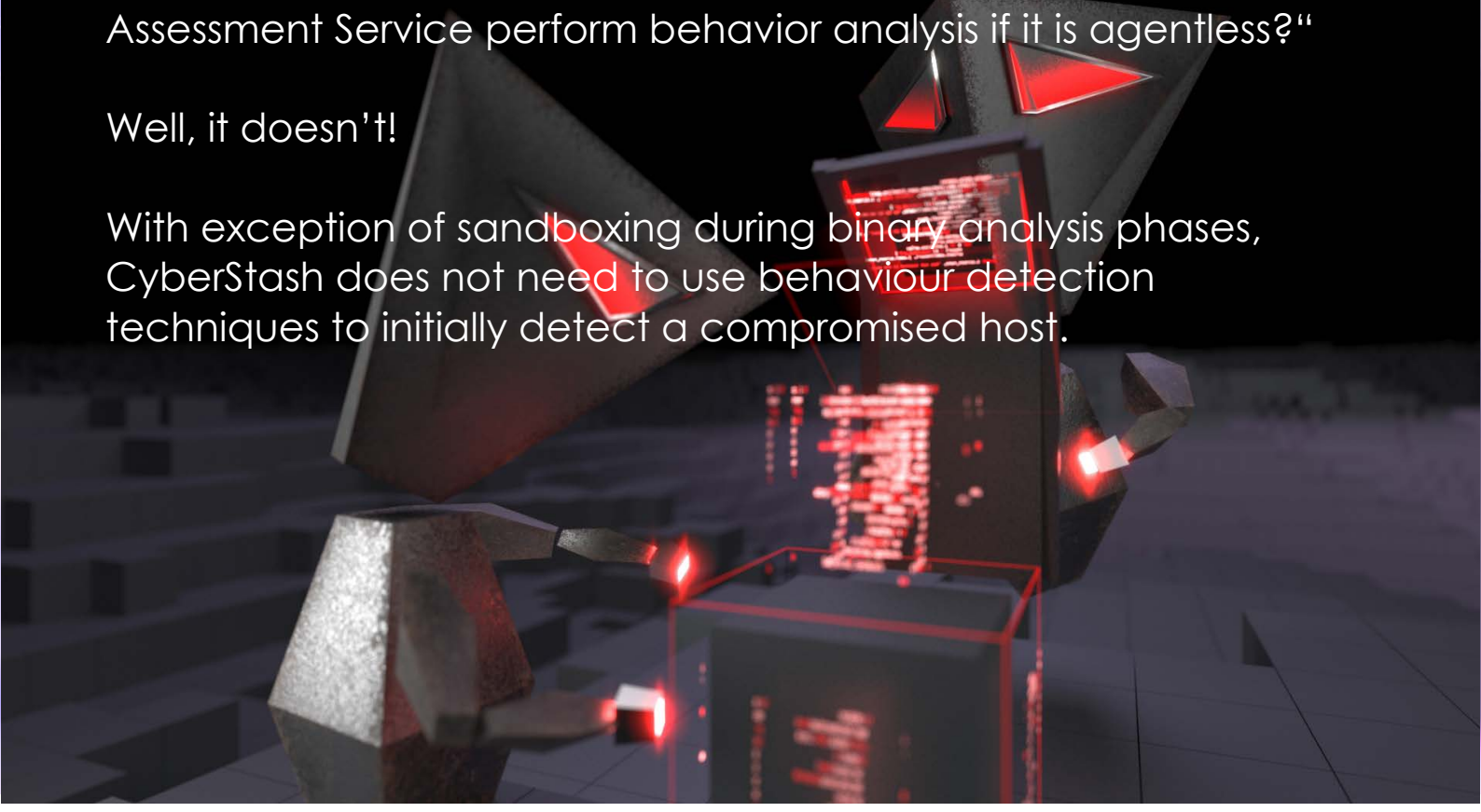
- Going underneath higher-level operating system APIs, and
- Working directly with volatile memory structures using patented memory analysis techniques

So you see, post compromise detection is different from finding an attack in progress as it is completely independent from the Operating System or the method that was able to compromise the system in the first place.

Our prospects often ask, "How does the CyberStash Compromise Assessment Service perform behavior analysis if it is agentless?"

Well, it doesn't!

With exception of sandboxing during binary analysis phases, CyberStash does not need to use behaviour detection techniques to initially detect a compromised host.



Forensic Depth Detection

CyberStash employs a Forensic Depth methodology which is the most effective solution to determine the compromise state of endpoints. CyberStash platform uses agents or dissolvable agents to independently collect, identify and evaluate a variety of data points, then analyses the data using forensic analytics and file intelligence services. Here are some of the functions CyberStash engages in:

Evaluating

- All active processes, loaded modules, scripts and drivers
- All Active Host Connections (including inter-process and redirects)

Identifying Disabled Security Controls

- Disabled AV
- Reduced authentication requirements
- GPO blocking, etc.

Identifying and Evaluating

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

Enumerating and Evaluating Persistence Mechanisms

- Cronjobs
- Registry autostarts/triggers
- DLL hijacking
- WMI Events
- Boot process redirection
- Watchdog processes, etc.

Auditing

- All privileged user accounts (e.g. ID rogue local administrator accounts)
- Legitimate remote administration services such as:
  - Shimcache and Amcache
  - Cmd
  - Powershell
  - NetSH
  - SSH, RDP, VNC
  - PSExec
  - Tunnels
  - WMI

Comparasion Of Functionality

When evaluating FDA and EDR based solutions based on functions and the capabilities delivered, it rapidly becomes clear what the two approaches offer, and one clearly stands out – Forensic Depth Analysis.

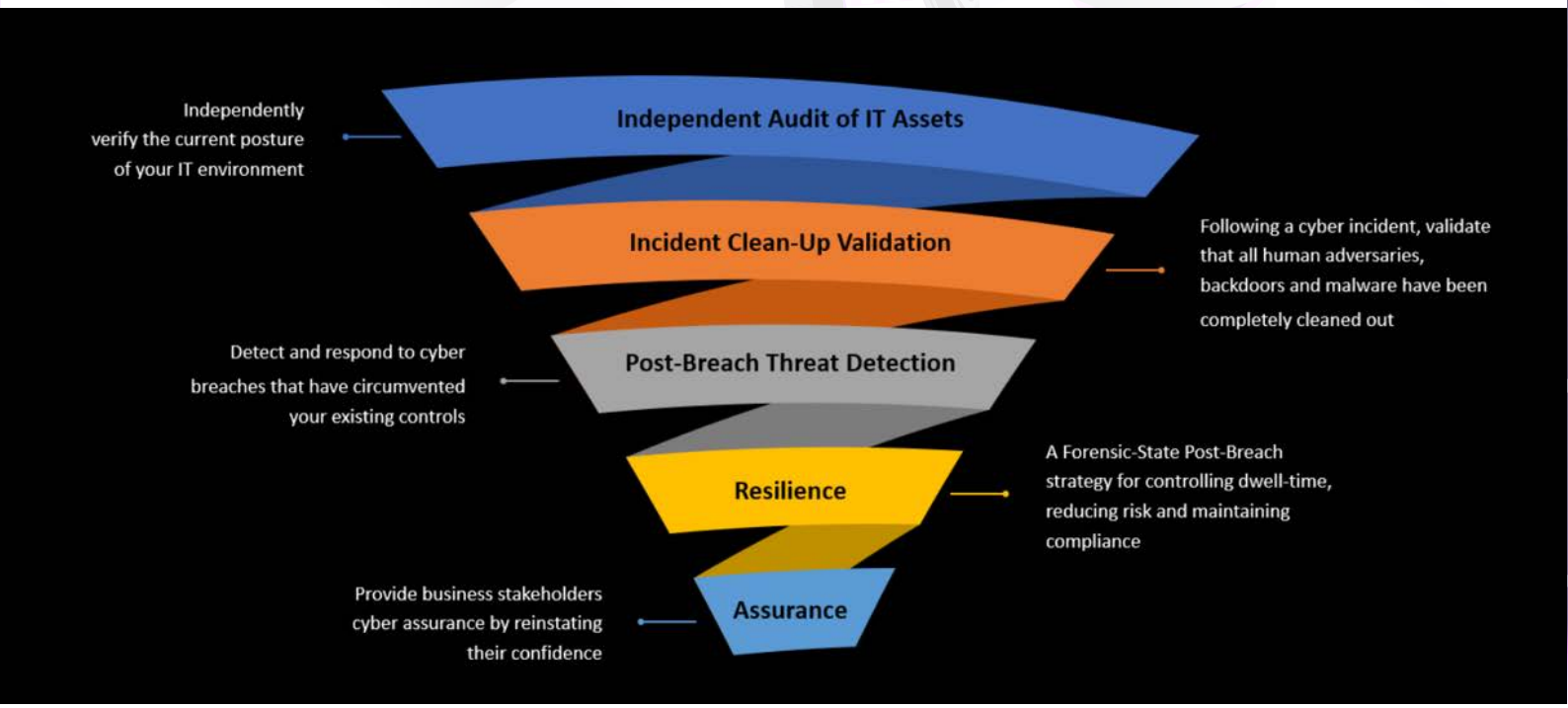
FUNCTIONAL CAPABILITY	FDA	EDR
Can find unknown/unidentified threats	●	●
Solution incorporates 3rd party intelligence	●	◑
Able to directly collect data for analysis	●	●
Intuitive and easy to use with little training	●	◑
Removes identifying information about originating endpoint from data leaving the enterprise	●	○
Operates without installing software on endpoints	●	◑
Able to gather data from 10s of thousands of endpoints per day	●	○
Identifies persistence mechanisms to discover malware that is dormant or scheduled to run in the future	●	●
Can be deployed fully on premise (no cloud services)	●	◑
Presents cross application communications (hooks)	●	○
Completes analysis within hours	●	○
Operates independently of host O/S	●	○
Functions outside a statistical model	●	○
Conducts volatile memory analysis	●	○
Gathers programs without querying the host O/S	●	○
Gathers modules without inspecting the PE header or querying the host O/S	●	○
Un-maps memory into native PE/ELF file structures for later analysis by vendors or other 3rd parties	●	○
Can quickly confirm endpoints are malware free - at any time - in support of incident response activities	●	○
Allows dwell time (or breach detection gap) to be defined and managed	●	○

Use Cases For Post-Breach Forensic Depth Compromise Assessment Service

The CyberStash Post-Breach Forensic Depth Compromise Assessment Service, provides an independent audit of your IT assets to ascertain whether any business systems are currently breached. 'Independent', not only because we are an external 3rd-party, who is carrying out the assessment, but because of the methods we use to conduct the assessment is completely independent of the existing toolsets used within your environment to detect threats. Namely, we use Forensic Depth Analysis (FDA).

The use cases for conducting Compromise Assessments are:

- Independently verify the current security posture of your IT environment.
- Detect and respond to advanced cyber breaches that have circumvented your existing controls.
- Following a cyber incident, validate that all human adversaries, backdoors and malware have been completely cleaned out.
- Build resilience by controlling dwell-time, reducing risk and maintaining compliance.
- Provide cyber assurance to business stakeholders to reinstate their trust and confidence in the IT environment.



Want to run a trial?

Reach Out To Cyberstash
For More information.

CYBER STASH

eclipse

Explore

eclipse.xdr

info@cyberstash.com
1300 893 802
cyberstash.com
Sydney, Australia

CYBER STASH