



CYBERSTANC

*Pioneer in Malware Detection,
Sanitization and Mitigation
Strategies*

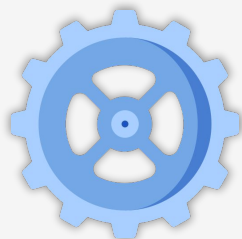


www.cyberstanc.com





Company Verticals



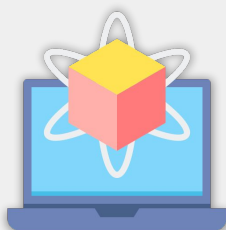
Anti-malware Engine

No Signature Dependency
Environment learning



Threat Integrations

75+ Alliance Partners
60+ Research Projects



Ransomware Study

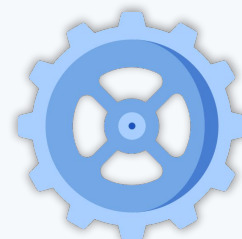
100+ Ransomware
Responders Taskforce



R&D Center

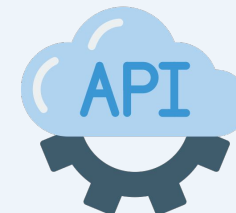
Simulation Learning

Products & Services



Scrutiny

Highest ZERO Day detections



Swatbox

Intelligent Real-time
Sandbox Detection



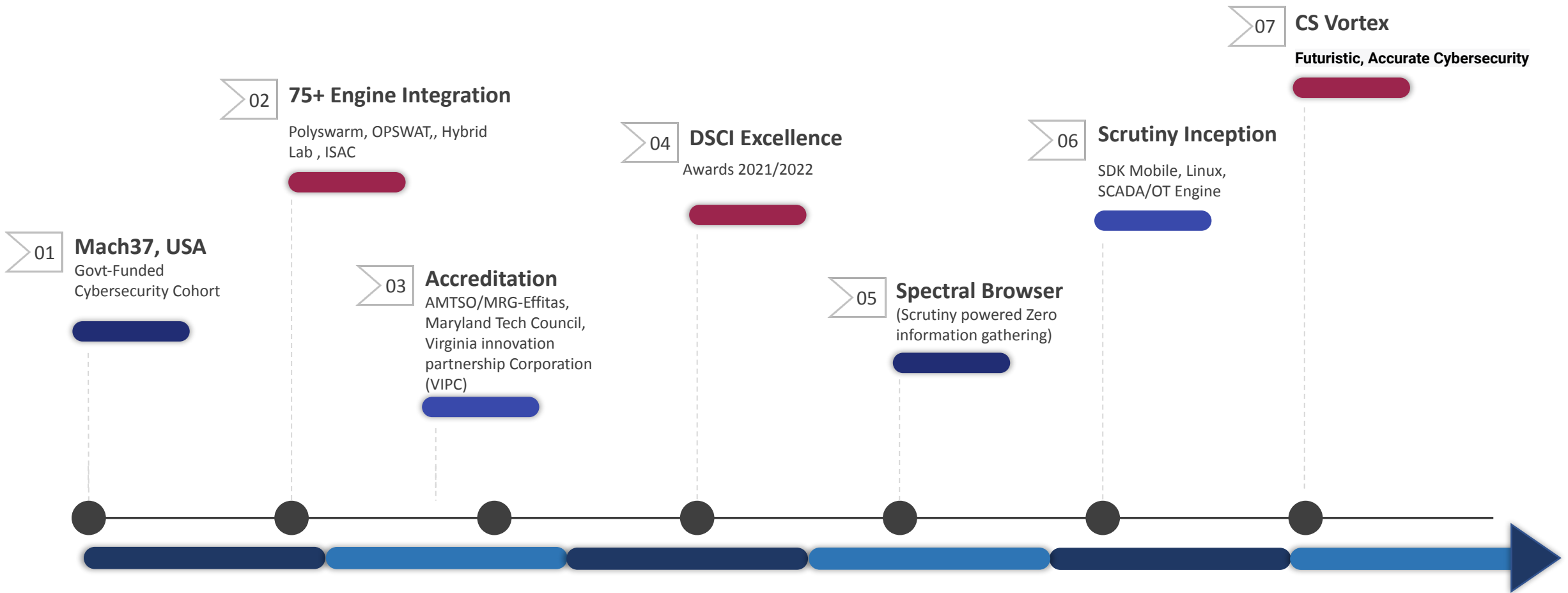
Vortex

Attack Mitigation and
Sanitization



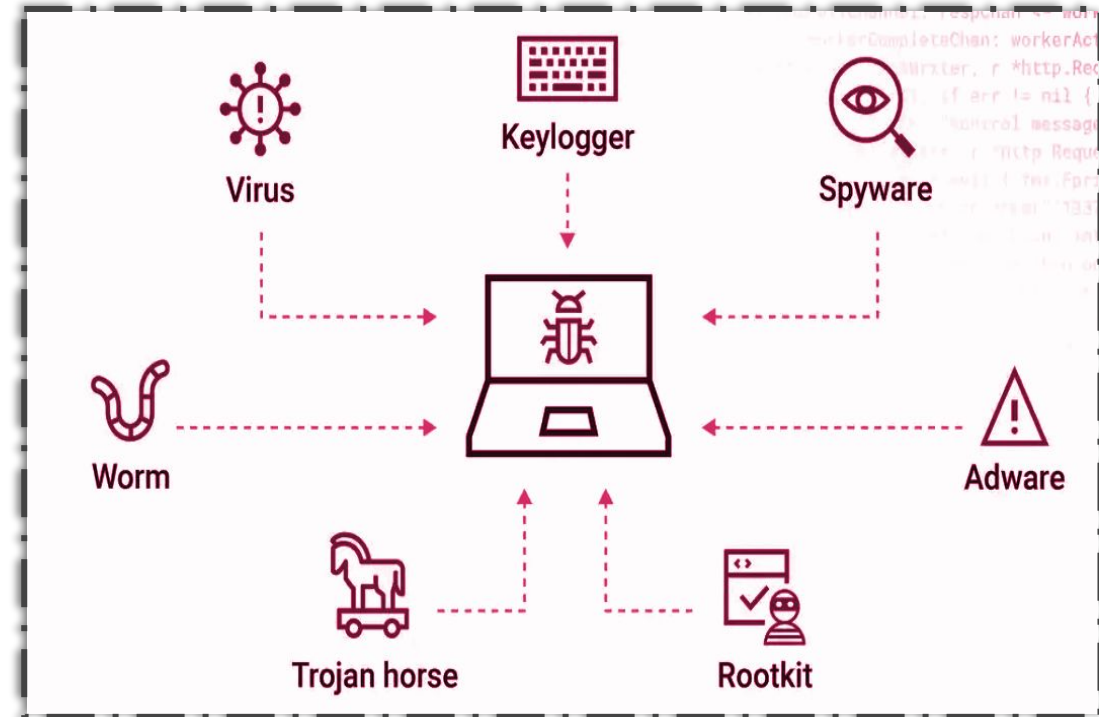
Spectral Browser

A Non-Chromium browser
enabled with Scrutiny Engine



Sophisticated Malware and Vulnerability Infections

1. Lack of Effective Security Management in Organizations.
2. **Lateral Movement** Mitigations during Endpoint and Network Data Transfer.
3. Insufficient Protection for **Sensitive Data Transfer** in Remote and Multi-Network Environments.
4. The Importance of **Data Sanitization** in Preventing Security Breaches and Leaks.
5. The Need for a Standard Framework for Sanitization and Advanced Malware detection.



A Futuristic Cybersecurity with Unmatched Threat Detection and Sanitization


- Advanced protection is essential for corporated against **cyber and supply-chain attacks**.
- **Proprietary engines** extract IOCs and threat information from files, documents, images, and unknown file types at scale and speed.
- Inspired by the peacock's natural abilities, Cyberstanc Vortex excels at catching all kinds of cyber threats and provides actionable intelligence, reducing the need for **time-consuming sandboxing**.
- **Simulation Intelligence** and **Signature-less** detection capabilities for better protection against cyber threats.

Vortex File Submission

Vortex's AI-driven data analysis and selective sanitization service sets a new industry standard with its innovative approach, delivering unparalleled accuracy and security to the next-gen malware detection landscape.

Report. Remove. Sanitise!

Vortex utilizes advanced AI simulations to thoroughly sanitize files, ensuring that all potentially harmful elements are detected and eliminated, giving you the confidence to securely share your files.

 Upload Files

Password (Optional)



Unlocking the Power of Cross-Simulation

Threat Detection and Mitigation with Vortex

- Easy **API** integration and agent-based use cases for endpoint, network, email, DMZ and storage protection.
- Covers most grey areas that attackers target or plan to exploit in the future.
- Highly obfuscated and real-world malware techniques, including **macro malware, VBA, VBS, PowerShell, DOCx, Calendar files**.
- Emphasizes transparency, interpretability, and accuracy in its approach to detection.
- Advanced malware simulation and evidence-based detection platform.



Upload Your File

Upload your file to the Vortex platform. Our sophisticated algorithms will then determine whether your file contains any malware, viruses, or harmful code.



Select Scanning Options

Choose the scanning options you want to run on your file. Vortex leverages advanced AI simulations to thoroughly sanitize files, ensuring that all potentially harmful elements are detected and eliminated.



Scan and Sanitize Your File

Vortex runs lightning-fast analysis of your file, providing a selection of data points and reports. The selective sanitization service then separates any harmful code from the projected results.



Review Your Results

After your file has been scanned and sanitized, you will receive a comprehensive report outlining the results of the analysis. You can view the sanitized version of your file and safely share it with confidence.



High-volume scanning

Fast and accurate threat detection

- File upload size upto **1GB**.
- **50,000 scans/Day**
- MIME type detection regardless of file suffix.
- Common archive and media file formats 7Z, ACE, GZIP, LZIP, ISO, RAR, TAR, ZIP
- **Microsoft Office Files:** DOC, DOCM, DOCX, DOT, DOTM, DOTX, PPSX, PPT, PPTM, PPTX, XLS, XLSM, XLSX
- Email Files: EML, MBOX
- **Malware Installation File Types:** .exe, .dll, .bat, .cmd, .js, .vbs, .jar, .py, .scr, .reg, .ps1, .hta, .chm, .lnk, .msi

Supported File Types

A collection of icons representing various file types: Word (document with 'W'), Excel (spreadsheet with 'X'), PowerPoint (slide with 'P'), RTF (document with checkmark), Archives (folder), PDF (document with 'P'), Email (envelope), Images (picture), and Portable Executable (document with 'EXE').

Submissions

Name:
bank-invoice-202376.ppsx

Type:
Microsoft PowerPoint 2007+

Size:
5.33 MB

TLSH Hash:
T12D46338E5F53DB64EFE3A7BC195A899B0542CC360A279A41D3805C40FD713CA1AADC9F

MD5 Hash:
72fe4dbbc93c2959ef962aced683282a

SHA-256 Hash:
cac494786970961b0bd648f430892b00e014164088a49e16c5d9026b229ac852

Scrutiny Verdict:
Malicious



Cyberstanc Vortex vs. VirusTotal

Cyberstanc Vortex's detection accuracy is much faster than traditional anti-virus solutions, as it reduces the number of artifacts that need to be sandboxed, saving time and resources. Reduce the risk of **false positives**.

Examining metadata, file structure, and relationships between files to identify threats with simulation intelligence.

Actionable intelligence to security teams, which includes detailed information on the nature of the threat, including the type of malware and its behavior. In contrast, **VirusTotal only flag a file as suspicious**.

Vortex places great emphasis on **transparency and accountability** in its detection designed and built.

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	102400	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	106496	118784	116736	7.95	c03cb928bd408ac55ecbbd3d66003a99	9488.98
.rsrc	225280	4096	1536	2.93	6c27246949820751aefd934ac0629ab2	168053.41

Imports

- KERNEL32.DLL
 - ExitProcess
 - GetProcAddress
 - LoadLibraryA
 - VirtualAlloc
 - VirtualFree
 - VirtualProtect
- USER32.DLL
 - GetFocus

Sections

SECTION	VSIZE	VSIZEL	VSIZEH	VSIZELH	VSIZELH2	VSIZELH3	VSIZELH4	VSIZELH5
UPX0	0x19000							
UPX1	0x1d000							
.rsrc	0x1000	0x37000	0x600	0x1cc00	0xc0000040	2.93		6c27246949820751aefd934ac0629ab2

Imports

- USER32.DLL
 - GetFocus
- KERNEL32.DLL
 - LoadLibraryA
 - GetProcAddress
 - VirtualProtect
 - VirtualAlloc
 - VirtualFree
 - ExitProcess

IOC

IOC	NAMESPACE	SCOPE
packed with UPX	anti-analysis/packer/upx	file
(internal) packer file limitation	internal/limitation/file	file
contain a resource (.rsrc) section	executable/pe/section/rsrc	file

Endermanch@Birele.exe
b2dcdf9e7b09f2aa5004668370e77982963ace820e7285b2e264a294441da23



Flexible Options for Vortex

Cloud and On-Premises

- Cloud deployment options include **AWS, Azure, or Private Cloud** for scalability and flexibility.
- On-premises deployment requires installation on own servers or hardware.
- Average processing time per scan is around 3-5 seconds, varies based on input mix.
- The Advantages of **Pay-as-You-Go** for Disaster Recovery and Sanitization Services.



Window/Ubuntu
8 vCPUs,
16GB RAM,
32GB SSD

Private Cloud
Azure/AWS
10,000
scans/Day



Scrutinize Files in early stage

A lightweight agent compatible with all endpoint security control and empower detection by adding advanced and effective anti-bypass and exploits detection.

Features

- Scrutiny avg. scan time (0.8secs)
- Multi-tier Detection Approach for complex and sophisticated malware
- Pre-attack Scenario detection, Before any damage
- Cross-platform support Windows/Linux/IoT devices
- Ease of deployment with SDK, Cloud & Hybrid networks with internal Apps and Secure zone.





Critical Infrastructure Protection

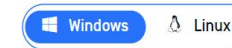
Competing with World-Top class Anti-malware vendor

Partnership Highlights

- Research upgrades: **Achieved 80% detection rate**, surpassing 30-70% by other Anti-virus.
- Critical infrastructure scanner: Designed for Scada/OT networks.
- Scrutiny Engine: Operates in Hybrid-Analysis Lab for comprehensive threat examination.
- Effective protection: Guards against state-sponsored APTs.
- **Signature-less** pattern matching: Enhances accuracy and efficiency in threat detection.

Metascan

Multiscanning is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues. OPSWAT pioneered the concept of multiscanning files with over 35+ anti-malware engines available to deliver enhanced protection from a variety of cyber threats.



Packages	Detection
Public Sector Select	>
Max Engines	99.39%
20 Engines	98.51%
16 Engines	97.32%
12 Engines	91.89%
8 Engines	83.42%

Custom Engines

Highlighted anti-malware engines can be added to this package for a customized threat detection solution. Additional engines can further increase your security profile and provides flexibility to match the requirements of your deployments.



036c6f7030c4f73ecf2cd1182c7b65357023f8c91

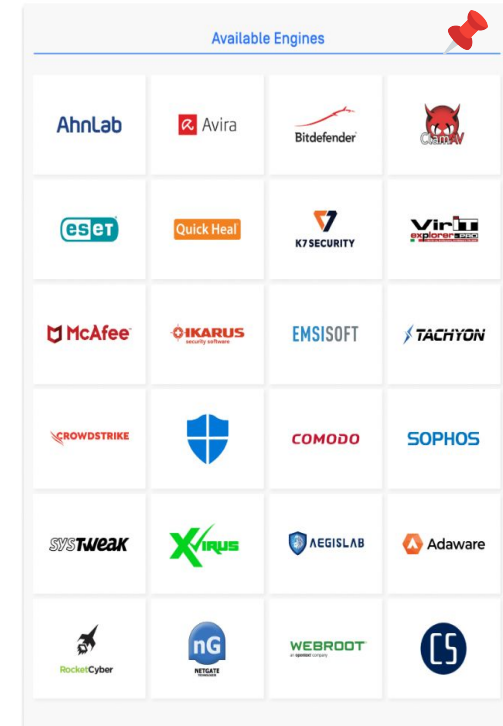
Threat name: Virus/Malware/756TFR

Cast your vote on this file: 0

Metascan Multiscan	Result	Engine	Last Update
Threats detected	✗ Malware	Scrutiny	Apr 5, 2022
01 / 35 ENGINES	✓ No Threat Detected	AegisLab	Apr 5, 2022
	✓ No Threat Detected	Antiy	Apr 5, 2022
	✓ No Threat Detected	Avira	Apr 5, 2022
	✓ No Threat Detected	Bitdefender	Apr 5, 2022
	✓ No Threat Detected	Comodo	Apr 5, 2022
	✓ No Threat Detected	CrowdStrike Falcon ML	Apr 5, 2022
	✓ No Threat Detected	Cyren	Apr 5, 2022

Multiscanning is an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues.

OPSWAT pioneered the concept of multi-scanning files with over 30 anti-malware engines available to deliver enhanced protection from a variety of cyber threats.





Crowdsourced Threat Detection

Secured one of the top engines and Arbiter role in detection

Partnership Highlights

- Effective anti-bypass and exploit detection capabilities.
- True signature-less detection for identifying first-seen malware.
- Top-list engine selected through rigorous testing on Testnet.
- Only 14 engines remain out of the initial 60+.
- Scrutiny engine delivers over **100,000+ unique detections every day.**
- Promoted to "**CS Arbiter**" role for groundbreaking detection.



```
Created at: 2022-05-21 19:03:11.459905
Start date: 2022-05-16 00:00:00
End date: 2022-05-22 00:00:00
Download: https://...
b7eee707036de4bae340198532ab44ef90a?response-content-disp
6&X-Amz-Credential=AKIARD7S6WCVBXF6ZS05%2F20220521%2Fus-e
7c62f1bae52243dc709954dbae8adda9e11b953cb80eccdc9eee
True Positive: 119524
True Negative: 8844
False Positive: 3430
False Negative: 6051
Suspicious: 0
Unknown: 559
Total: 138408
```

Hash	Malware Family	First Seen	Last Seen	PolyScore™	Detections	File Size	File Type	Actions
4cb9e92ee4535aa9b51f...	None	2022-12-12 19:59:59	2022-12-12 19:59:59	0.23	1/14	937 KiB	Win32 EXE	🔗 🗑️
6fbf2d4be31d6530a171...	None	2022-12-12 19:57:45	2022-12-12 19:57:45	0.23	1/13	3.0 MiB	Win32 EXE	🔗 🗑️
c0bba96c884328d5c2cc...	None	2022-12-12 19:52:07	2022-12-12 19:52:07	0.23	1/14	90 KiB	Win32 EXE	🔗 🗑️
892e25f5e58e603d0df6d...	None	2022-12-12 19:49:35	2022-12-12 19:49:35	0.23	1/13	3.8 MiB	Win32 EXE	🔗 🗑️
a31ae3b6842be5a4faad...	None	2022-12-12 19:43:23	2022-12-12 19:43:23	0.23	1/13	14 MiB	Win32 EXE	🔗 🗑️
3cb5bbafeac8a865d44...	None	2022-12-12 19:29:14	2022-12-12 19:29:14	0.23	1/13	313 KiB	Win32 EXE	🔗 🗑️
5cc9dfccc9626148275f...	None	2022-12-12 19:28:34	2022-12-12 19:28:34	0.23	1/14	21 KiB	Win32 DLL	🔗 🗑️
dd7e32f5b5f01e59e908...	None	2022-12-12 19:26:51	2022-12-12 19:26:51	0.23	1/13	23 KiB	Win32 EXE	🔗 🗑️



Collaborative Intelligence

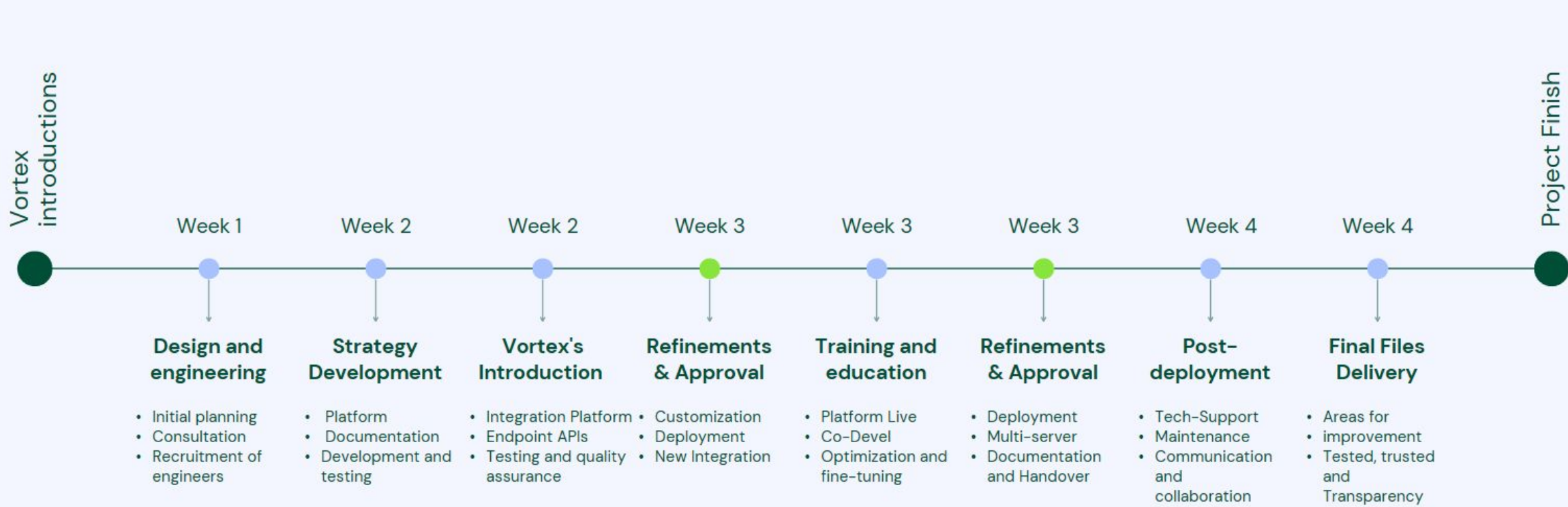
A New Horizon

- Conduct regular **strategic R&D and analysis** to identify potential malware, rootkits vulnerabilities and improve existing systems.
- Investing in **state-of-the-art and sophisticated** approaches to enhance security.
- Team and Infrastructure: **Secure-tech framework** for better support and new pro-type development.
- **No-Data Acquisition Policy:** Designed with **user privacy in mind**, our platform does not collect any data from the user or their system.





Integrating Threat Intelligence Capabilities: Timeline for Vortex Implementation



Legend:

- Cyberstanc R&D Team
- Cyberstanc Product and Testing

Contact Us



[@cyberstanc](https://twitter.com/cyberstanc)

<https://twitter.com/cyberstanc>



[#cyberstanc](https://www.linkedin.com/company/cyberstanc/)

<https://www.linkedin.com/company/cyberstanc/>



www.cyberstanc.com

Scrutinize Files before Malware run !!

Email:- info@cyberstanc.com, sales@cyberstanc.com

More information about the malware and security - including information about our strategy, plans, collaborative partners and achievements - is available at [cyberstanc blog](#)