1) Integrated SOC Solutions at Cyberstanc

- A Technical Analysis Report

Submitted by,

Ramaa Manish Rahatekar

Intern, Cyberstanc

Date of Submission : June 1, 2025

Prepared for Cyberstanc Organization, Dover, DE, United States

2) Summary

This report is a detailed study of Cyberstanc's advanced security solutions, undertaken during my learning phase as a student. I read all the datasheets available under the resources section and learnt about various products developed and offered by this company. The goal of this report is to present key points that I noticed, highlight my observations and provide you with the content that I have formulated on my own. Since I am a fresher, I thought of analysing these tools in relation to core BTech CSE concepts. I could relate to the theoretical knowledge I learned during my undergrad years and could visibly see the void between bookish knowledge and practical knowledge disappear.

3) Introduction

Cyber threats today are not just more frequent—they're smarter, faster, and more complex. Organizations are constantly seeking proactive and scalable security solutions to stay ahead of malicious actors. Cyberstanc, with its suite of intelligent tools like Vortex and Scrutiny, offers integrated SOC solutions that detect, contain, and respond to threats in real time. Cyberstanc products are developed with care, precision, logic and a lot of forethought by their amazing team. During my learning phase, I had the chance to explore these platforms, understand how they mitigate evolving malware threats, and examine their alignment with computer science fundamentals.This report outlines my learning journey of Cyberstanc's malware detection and response tools, particularly in the context of secure cloud storage, endpoint protection, real-time threat analytics, and signature-less detection.

4) Findings

4.1 Vortex File Malware Detection and Sanitization

4.1.1 Description -

This is a file security solution by Cyberstanc's Vortex platform. It is brought into existence with a unique purpose of providing users with top-notch level product to detect suspicious files by making use of Multi Engine Scanning, Sandboxing, Content Disarm and Reconstruction (CDR) and a software that actively looks out for threats and provides easy integration of SIEM with the existing architecture.

4.1.2 Purpose -

- The main agenda of this platform is to detect and eliminate file-borne malware threats so that the end user remains unaffected.
- To preserve the remaining content of the file while trying to get rid of any potentially malicious code that may disrupt our OS's usual functioning if unidentified.

4.1.3 Motivation behind bringing this solution into existence -
ie. Cons of traditional threat detection

- Threats can be categorised into many kinds in todays day and age and the concept of launching an attack has transformed into singular attacks. They have become specific in nature.
- Hackers are now said to be planning to carry out attacks for months, unlike that of older days when one person bombarded multiple systems in a similar approach.
- Earlier techniques had a trade-off between them due to the unique scenarios they catered to.
- While Network Scanning was scalable, it was not as detail oriented and often resulted in threats that went uncaught and unnoticed when the volume of data increased.
- On the other hand, End-Point Detection was not scalable but supported real-time behaviour with comparatively much better accuracy.

4.1.4 Take Away Pointers -

Sandboxing -

- It is a safe place for opening files that may seem suspicious at the first glance. Sandbox consists of an isolated environment to open those files without making the main architecture susceptible to digital mishaps.
- It mimics a real network system and looks for any code snippet that tries to do extreme level damage like deleting or overwriting documents, attempting to connect to foreign servers etc.

- Traditionally, it makes use of static techniques like equating the file hash against a known database value.
- Vortex plays a pivotal role here as it does not support latency nor usage of a secondary operating system.
- Machine Learning platforms are a clever addition to the existing module. By deploying numerous supervised algorithms, one can train the model for detecting and predicting future activities by using labelled data like good/bad code.
- It can further bifurcate abnormal patterns into ‘malicious’ or ‘benign’ (safe).
- Smart alerts, less delays and fewer false positives can thus be achieved.

  For example :
- A fake user gets phished > His credentials get stolen > Malware moves laterally >
- Sensitive information gets compromised > SOC tools give out an alert

  The role of ML -
- Tracks the activity > Logs the entries > Labels actions > Helps train ML models to spot similar patterns in the future

Content Disarm and Reconstruct (CDR) -

- It is a data sanitization mechanism which assumes that all files contain some segment of harmful codes. Going one step forward, it takes the extra effort of parsing the entire file to look for troublesome content.
- If found, it immediately discards that particular code, and rebuilds the remaining portion such that it is intact for further legitimate use.
- CDR supports over hundred various file types to cater to all sorts of input.

Pdf and Excel file analysis by REST API -

- All software systems expose REST APIs so that any script/CICD pipeline/e-mail gateway can make use of it without having complex queries or procedures involved.
- Using the ‘as code’ version, one can directly upload this to batch jobs, SaaS portals, without needing another interface.
- The outcome contains primary key, lifecycle of objects, hashes, list of JavaScript codes, URLs. Hashes make the code forensically traceable i.e., one can still get hold of the event logs when deleted from the client side.
- The parameters are as follows - Name , Type, Size of file, TLSH, MD5, SHA-256, Static analysis, Scrutiny Verdict, File metadata, File properties, Indicator of Compromise (IOC) & Macro analysis.
- These statistics prove to be insightful and crucial for data visualization KPIs (Key Performance Indicator)
- It acts as an amazing resource to the security team.
- Scrutiny engine makes integration into the current system a cake walk.

4.1.5 Lesser Known Facts - Trivia

- CDR was invented in Israel defence units to move files safely between classified networks.
- Sanitization of a file does not imply deletion of the contents. It simply refers to cooking the same dish but without poison in it.
- Vortex doesn't just flag malicious code. It gets rid of the entire suspicious part and reconstructs the original file.

4.1.6 Parallels drawn to CS fundamentals -

- Vortex operates at the Application Layer 7 of the OSI/ISO model not just at the TCP/IP level.
- It detects hidden attachments with 99% accuracy.
- Deep CDR uses hashes, tries, trees as internal data structures.
- REST API based file analysis is a part of a broader scope in microservices under the domain of web services.

4.2 Scrutiny EDR - Cyberstanc's End Point Detection and Response platform

4.2.1 Description-

Scrutiny EDR is a software agent that is installed on devices like computers or laptops, it watches the usual internal working of the system, memory management, has a keen eye on file changes, different user behaviours.
An EDR is on the lookout for any unusual activity that might stand out as a threat.

4.2.2 Purpose -

Scrutiny EDR platform runs a multi engine scanner directly on the end points. It uses machine learning algorithms to gather results with valid proofs and make strong choices as to accept the file or not.
Multiple engines implies multiple results, multiple results means many outcomes for analysts to weigh and come to a most probable accurate conclusion regarding the file contents.

4.2.3 For Example -

In a house- a simple Anti Virus solution is like a watchdog, it barks only when it sees an unknown person, whereas EDR is like a trained security professional who closely watches people against numerous parameters like behaviour, expressions and takes appropriate actions like calling the police, locking the door etc.

EDR is similar to the S-400 Military defence system that has been gathering worldwide attention in recent times. While radar continuously scans for incoming objects, EDR scans for any patterns that may previously have been used.

4.2.4 Motivation to bring this solution into existence -

I.e. Cons of traditional system

In the early days, end point security used single AV engines. Many malicious files were thus missed due to less surety.
Traditional AV's were enough to recognise and reject known threats but as technological advancement occurred, hackers made use of new techniques where firewalls proved to be worthless.
Fileless malware, lateral movement inside networks, Zero Day attacks became more common.
It did not allow multi core processing and had a long waiting time between threat being detected in the vicinity and remedial actions initiated to combat the issue.
This is what they call 'outbreak exposure'.

This reminded me of the incident when my father's Hyderabad based credit card details got hacked via netbanking and a hefty amount of cash was withdrawn in Germany.
Had EDR been installed in his laptop, this situation would have never occurred.

4.2.5 Advantages of advanced EDR platform -

After reading about how EDR works, I learned that it often makes use of distributed computing to improve performance and scalability. Instead of relying on a single endpoint to process and analyze all threat data, EDR solutions can distribute tasks across multiple systems or use cloud infrastructure.
This helps reduce the computational burden on individual devices, enabling faster detection and response without overloading any single machine.

It combines Simulated Intelligence and Signature less detection. Since we are dealing with an ever-evolving landscape, rule-based detection system and AVs do not work as effectively.
Every domain is witnessing rapid growth by integrating Artificial Intelligence to their existing solutions. Microsoft Excel worksheets too have an AI Chatbot integrated. It is only valid to combine this innovation to take our solutions to the next level and solve even more complex problems.

4.2.6 Take Away Pointers & Workflow -

Pattern recognition plays a crucial role in using AI/ML approaches to handle threats.
Simulated intelligence uses chronological steps to arrive at a final classification.
It includes
Behavioral analysis
Cryptographic caging i.e. uncovering crypto algorithms or hashes

To read about our hypothesis (this is the fact checking stage where we gather insights that support our hypothesis and leave no space for cross questioning)
Drawing logical inferences
Final classification
Sanitization (removal of file)
After deep diving into the architecture I noticed that core engines, database and workflows make up the central part. It separates the client and other engines.

EDR offers 4 key solutions. They are –
Cryptography, Ransomware AI, API Integration, Cost effective alternatives

Scrutiny does not promote tampering of any sort. It reduces false positives.
It backs up data only when a ransomware is found. This reminds me of memory optimization algorithms from the Operating Systems chapter.

4.2.7 Statistical Analysis -

About 57% of organizations are said to be using EDR in some way or another. The percentage has increased by 15 percent in the last 3 years.
Cloud based EDR solutions make up 87% of the market share.

4.3) Vortex's Cloud File Scanning Anti Malware Engine -

4.3.1 Description -

It is a systematic defense software driven with the ideology of being convenient and offering easily integrable solutions across diverse platforms.
It uses ICAP and HTTP; the two pivotal concepts of Computer Networks in order to function.

4.3.2 Take Away Points -

It comprises PDF. scanning, provides an interface to search for files in the cloud architecture, and enables polymorphic scanning too.
A polymorphic virus, as the name suggests, is designed to mutate its appearance multiple times. It is similar to a Chameleon that changes its skin color (appearance) to hide from being caught.

A. AWS S3
It is a simple cloud storage service offered by Amazon.
Amazon's GuardDuty automatically scans newly uploaded objects into buckets.
Buckets are created as per industrial and consumer requirements.
It is a refined version that prefers storing data as objects and not bulky files.
According to me, this is done to add more benefits related to modularity.

It is also super budget friendly for small scale companies as no extra infrastructure is required. This is the crux of the matter.

B. Azure Defender for Storage
Azure is a product of Microsoft.
It is flexible in nature and supports collaboration of various clients.

C. Google Cloud Platform (GCP)
GCP is an event based pipeline.
I remember seeing event based methods in Java programming.

Regulatory compliance (GRC), customization, better integration and hassle free setup is the main goal of each cloud scanning service irrespective of company.
It may differ in use cases, business to business, duration, location of setup, amount of usage and cost of infrastructure.

4.3.3 Operation -

The best part of the Anti malware engine is that it allows bulk file scanning without any bottlenecks.
The phases include Bulk scanning, local analysis, cloud lookup, Simulated intelligence, Final verdict, Sanitization.

4.3.4 Workflow -

SDK bindings form the intermediate layer.
Network layer, File System layer, Execution layer provide supply chain management security & administers open critical server damage.
The client side contains raw data and get/post methods that enable data exchange over the network protocols.

4.3.5 Advantages -

Over 100,000 files can be handled effortlessly.
It successfully cleans buckets and puts them away from the rest.
Has LLM assistance, enables cloud infrastructure, uses REST API making handling very simple.

4.4) Vortex’s E-Mail security -

4.4.1 Description -

Electronic mail, as we all know, has become a part and parcel of our lives.
Vortex’s feature allows this to be done in a seamless manner.

4.4.2 Take Away Points -

This mechanism internally nullifies risky parameters.
Recognises unsigned threats from a mile away (almost instantly).
Any browser is a great starting place as the solution is inclusive.
Anti spam filtering using AI is what makes the difference and sets it apart.
SPF provides additional security wrapper to the DNS (domain name system) to avoid attacks.
DKIM makes sure there are no key alterations in transit. It uses a public key encryption algorithm to check things sent over the network.

4.5) Vortex's SWG (Secure Web Gateway) -

4.5.1 Description -

The Internet, a fairly new edition to the world of technical advancements, has surely made a lot of daily activities & functions convenient.
With ease of working comes a ton of challenges that were never encountered before.
Secure Web Gateway, as the name suggests, is like a checkpoint for users accessing the internet.
It is similar to the policeman stopping our car at the toll-gateway to check all paperwork and licences.
Airport security check is another wonderful example I could think of. Our baggage is promptly checked via screening gate, metal detectors, sensors etc. to throw objectionable goods away.
Anything that seems to be a threat to the airport's integrity is cancelled.
There is no use of an SWG to be limited to only one network.
It needs to be scaled vertically. Global Traffic Manager (GTM) makes this possible by managing entries, balancing loads, reducing latency and being super quick.
GAM uses Secure Socket Layers (SSL) certificate to ensure anti-tampering.
It proves to be a safe layer between internal happenings and external factors that may hinder the regular conduct of a network.

4.5.3 Operation -

- A user tries to access a website
- GTM routes them to the nearest server
- The SWG intercepts and scans traffic (even encrypted with SSL)
- If ads are served via GAM, SWG inspects them too
- The user only gets clean and safe content.

4.6) Ransomware Responder Service -

4.6.1 Description -

This is an incident response team that works day and night to safeguard the integrity of the system.
It assesses damage and co-ordinates with law enforcement as and when needed.

It is a middleman or a mediating service that takes matters to the law.
It is a strong entity to prevent and reduce damage escalation by mediating talks or deals.

4.7) SOCaaS - SIEM

4.7.1 Description -

This is responsible for collecting evidence of event related data like logs and entries to analyse threats.

4.7.2 Take Away Pointers -

- SIEM stands for Security Information and Event Management.
- This is similar to locating other devices that might have had our social media account active and in use, to check which location was the phone last active in.
- This will help us track the location via GPS technology of latitudes and longitudes.
- It acts as a CCTV control room.

4.7.3 Operations -

- It collects data from firewalls, servers, apps, databases, helps in normalization, aggregation, correlates logs and events, generates alerts for dashboards.

4.7.4 Use cases -

- Supports in HIPAA compliance audits.
- HIPAA is a U.S. federal law passed in 1996 that protects sensitive patient health information from being disclosed without the patient’s consent or knowledge.

SOCaaS - SOAR

Description -

This acts like a trained robot.
SOAR stands for Security Orchestration, Automation, and Response.
By orchestration, it refers to the entire framework of our entity and its conduct.
It is loaded with pre-written rules in the form of code as input and works on the lines of ITTH (if this then that method).

Operations -

- It integrates with tools like firewalls, EDRs, antivirus, ticketing systems.
- It executes workflows like “block IP,” “quarantine file,” “create incident”.
- It uses predefined playbooks to respond to known threats.

Use cases -

- Auto-blocks ransomware IPs.
- Automates phishing email response.
- Quarantines infected endpoints in real time.

SOCaaS - UEBA

Take away points -

-
- UEBA stands for User and Entity Behavior Analytics.
- This is an analyst plus cybersecurity professional in disguise.
- It has the capabilities of both domains.
- It acts as an observer, alert system, note-taker all in one.
- It knows the answers to questions like
- What went wrong, why it occurred, what better improvisations can be done, etc.
- While SOAR automates responses, UEBA monitors behavior.
- Each entity is efficient in their own purposes and has their objectives mentioned clearly.

4.8) SDK Malware Solutions -

4.8.1 Description -

SDK stands for software development kit. It comprises tools, libraries, codes, documentation and samples required to build products from scratch.
One can look at it as a software developer’s support kit.
It helps integrate technology into existing solutions and architecture.

4.8.2 Use cases -

- Email Gateway: Scanning email attachments before delivery.
- Cloud Storage: Scan files uploaded to AWS S3, GCP, or Azure.

- Web Apps: Check user-uploaded documents/images for malicious payloads.
- Mobile Apps: Prevent users from opening infected files or links.
- File-Sharing Platforms: Remove malicious content during file uploads.

5) Conclusion

This report has provided me with a comprehensive overview of Cyberstanc's core SOC solutions—Vortex File Malware Detection & Sanitization, Vortex SIEM/SOAR/UEBA, Vortex Cloud File Scanning, and Scrutiny EDR—along with a practical malware analysis of a stealer sample. By mapping each tool to fundamental B.Tech CSE concepts such as operating systems, networking, data structures, and information security, I was able to bridge the gap between textbook theory and real-world practice. I will now be using this to further gain knowledge about malware analysis and its reporting.