COHESITY REDLab

NEWSLETTER | DECEMBER 2025

About REDLab Newsletter

Welcome to the REDLab newsletter that provides you with monthly updates on the Cohesity REDLab initiative.

REDLab is a fully isolated security testing facility, hosted and managed by Cohesity, to research and study ransomware and malware. The Cohesity REDLab stress tests our solutions to ensure that our products are hardened against attacks, protecting both the backup data and administrative interfaces. This helps drive a deeper understanding of how to secure your data protection processes and data. It provides meaningful and actionable insights to both security teams and data protection teams when anomalies are detected. This ensures that the data is safe, protected, and that you can be confident in the cyber resilience that Cohesity solutions offer.

Video: Cohesity REDLab helps build stronger defenses against ransomware

Cohesity DataProtect in REDLab

Cohesity REDLab hosts both Cohesity DataProtect and Cohesity NetBackup for comprehensive testing against malware and cyberattacks. REDLab is where we rigorously test the real-world resilience of our products using live malware, advanced exploits, and modern attack techniques. Our REDLab is an air-gapped environment designed to allow full-spectrum threat testing while protecting Cohesity infrastructure.

The Strategic Value for IT Leaders:

- **Proven Confidence:** Your backup and recovery solutions are not just theorized to work; they are tested against the highest levels of active threats.
- **Hardened Defense:** We verify that DataProtect and NetBackup delivers robust security, moving beyond simple recovery to become an active line of defense.
- **Future-Ready:** We are actively expanding our testing scope to include advanced threat detection and threat hunting validation, ensuring your resilience evolves alongside modern attack vectors.

We now continuously validate DataProtect and NetBackup security posture and will expand to include threat detection and threat hunting in the future, all under real-world and fully isolated conditions.

Cohesity Trust Center: Learn more about Cohesity REDLab

Critical Threat Updates – December 2025

The Cohesity Threat Library is updated daily to enhance detection of active attacks. REDLab conducts deeper investigations into high-profile threats and contributes additional detection capabilities to the library.

https://www.cohesity.com/trust/redlab/advisories/

Threat Focus for December: Lumma Stealer (LummaC2) and React2Shell (CVE-2025-55182)

Lumma Stealer is a sophisticated malware family acting as a reconnaissance-and-access broker rather than a simple info-stealer. It serves as a primary entry point for major ransomware operations.

- **Attack Vector:** Enters systems via malvertising or fake installers, executing evasive loaders to avoid detection while establishing persistence.
- **Methodology:** Rather than using OS exploits, it escalates privileges by harvesting browser credentials, crypto wallets, and session tokens to impersonate users.
- **Impact:** Stolen identity data facilitates lateral movement into cloud accounts and SaaS consoles without triggering traditional network alarms.
- **The Kill Chain:** Once data is staged and exfiltrated to a C2 panel, the kill chain often converges with ransomware operations. Lumma hands off compromised access to downstream threat actors like LockBit or Akira.

React2Shell is a maximum-severity (CVSS 10.0) unauthenticated Remote Code Execution (RCE) vulnerability within React Server Components (RSC). It affects major frameworks like Next.js and has become the primary infrastructure target for December.

- **Attack Vector:** Exploits the Flight protocol used for client-server communication. Attackers send a single, malicious HTTP POST request to bypass security boundaries via unsafe deserialization.
- **Methodology:** Targets the server-side decoding logic to "pollute" the prototype of JavaScript objects. This allows attackers to execute arbitrary shell commands (via child_process) with the privileges of the web server.
- **Impact:** Provides an immediate foothold for nation-state espionage (China/North Korea-linked) and financial actors. It is used to drop cryptominers (XMRig) and advanced backdoors (EtherRAT, Sliver).
- **The Kill Chain:** Starts with automated scanning of internet-facing apps. Once access is gained, actors pivot laterally to harvest cloud secrets (AWS/OpenAI keys), modify SSH keys for persistence, and deploy ransomware (Weaxor).

REDLab recommendations:

- Patch React immediately: Upgrade to React 19.0.1, 19.1.2, or 19.2.1.
- Identify any frameworks that bundle React Server Components: Especially Next.js and other ecosystem tools.
- **Continuous Monitoring:** Enable continuous anti-ransomware monitoring in the Security Center. Implement periodic file-hash scanning for dormant malware detection
- Use the Cohesity Anti-Ransomware module to deploy inline ML-based techniques to identify new and unknown threats within your backup data.
- Activate the Threat Detection feature to scan backups for known malware signatures and Indicators of Compromise (IOCs) using built-in threat feeds and custom YARA rules.
- **Rapid Threat Hunt:** Conduct hunts using Cohesity Rapid Threat Hunts, leveraging daily updated intelligence feeds from sources like Google Threat Intelligence, CISA, and Cohesity REDLab.

Here are few of the latest ransomware families and their behavioral patterns that were studied in the REDLab:

Name	Ransomware family	Behavioral pattern
NightSpire	NightSpire Ransomware group	Exploit Public-Facing Application, Command and Scripting Interpreter, Inhibit System Recovery, Defense Evasion, Data Encrypted for Impact, File/Extension Modification, User Impact Message Delivery, Double-extortion, Lateral movement using WMI, PsExec and PowerShell, Maps Active Directory, Credential Theft using Mimikatz
Sinobi	Lynx and INC Ransom families	Brute force attack against open or exposed RDP, CIDR parsing for subnet-wide impact, Anti Debugging, File, Directory and Network share discovery, Local and Network data encrypted for impact, Delete shadow copies, Double-extortion, Mount volumes that are hidden or unmounted.
Devman	DragonForce family	User Execution, Obfuscated Files or Information, Indicator Removal on Host, File Lock Evasion via Restart Manager, Network Share Discovery, Scanning of SMB/Windows Admin Shares, Data Encrypted for Impact, Inhibit System Recovery
Nitrogen	Nitrogen family	Use execution, Obfuscated Files,Defense evasion, Process and file discovery, Command and Control, Exfiltration, Data encrypted for Impact, Inhibit System Recovery

REDLab findings:

- **NightSpire (attack on NetBackup and Data Protect client):**
  - **Family**: NightSpire Ransomware group | **Behavior pattern**: Exploit Public-Facing Application, Command and Scripting Interpreter, Inhibit System Recovery, Defense Evasion, Data Encrypted for Impact, File/Extension Modification, User Impact Message Delivery, Double-extortion, Lateral movement using WMI, PsExec and PowerShell, Maps Active Directory, Credential Theft using Mimikatz
  - **Know Me**: NightSpire is a sophisticated ransomware strain that emerged in early 2025, operating primarily as a private syndicate rather than a broad RaaS. The malware uses a hybrid encryption model (AES-256 for file content and RSA-2048/4096 for key protection) to lock victim data, appending the distinct '.nspire' extension to filenames. Uniquely, NightSpire is known to aggressively target locally synced cloud directories, specifically encrypting OneDrive content to cut off cloud-based recovery options.
  - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.

- **Sinobi (attack on NetBackup and Data Protect client):**
  - **Family**: Lynx and INC Ransom families | **Behavior pattern**: Brute force attack against open or exposed RDP, CIDR parsing for subnet-wide impact, Anti Debugging, File, Directory and Network share discovery, Local and Network data encrypted for impact, Delete shadow copies, Double-extortion, Mount volumes that are hidden or unmounted.
  - **Know Me**: Sinobi is a sophisticated ransomware strain that surfaced in mid-2025 (around June/July), quickly establishing itself as a credible threat to the manufacturing and financial sectors. Sinobi is widely considered a rebrand or direct successor to the Lynx ransomware group, sharing significant code and infrastructure overlaps. The malware uses a high-speed hybrid encryption scheme (Curve25519 + AES-128-CTR) and appends the capitalized '.SINOBI' extension to files. It operates on a double-extortion model, maintaining a Tor-based data leak site to shame victims who fail to pay the ransom.
  - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.

REDLab findings:

- **Devman (attack on NetBackup and Data Protect client):**
  - **Family**: DragonForce family | **Behavior pattern**: User Execution, Obfuscated Files or Information, Indicator Removal on Host, File Lock Evasion via Restart Manager, Network Share Discovery, Scanning of SMB/Windows Admin Shares, Data Encrypted for Impact, Inhibit System Recovery
  - **Know Me**: Devman is a specialized ransomware variant utilized by the DragonForce group, which gained notoriety in late 2023 and throughout 2024 for its aggressive double-extortion tactics. DragonForce typically targets large enterprises by exfiltrating sensitive data before deploying the Devman encryptor. The malware is known for its speed and its "clean" coding style, often avoiding complex obfuscation in favor of high-performance encryption. It typically appends extensions like .devman or randomly generated strings to encrypted files.
  - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.

- **Nitrogen (attack on NetBackup and Data Protect client):**
  - **Family**: Nitrogen family | **Behaviour pattern**: Use execution, Obfuscated Files,Defense evasion, Process and file discovery, Command and Control, Exfiltration, Data encrypted for Impact, Inhibit System Recovery
  - **Know Me**: Nitrogen is a highly active double-extortion group that has intensified its operations over the past four months (late 2024 to early 2025). It primarily targets technical sectors including construction, finance, manufacturing, and technology across the USA, Canada, and the UK. The group is notable for its use of "technical" lures, such as malvertising for IT tools, to gain initial access. Once inside, Nitrogen employs sophisticated anti-analysis techniques like VM detection and stack string obfuscation to hide its activity. It utilizes a coercive, Tor-based double-extortion model, threatening to publish stolen data and legal/GDPR penalties to pressure victims into payment.
  - **Attack Pattern**: After the attack, in the case of the Data Protect Client backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client it encrypted the user data and system files. A backup anomaly that detected unusual behaviour with respect to offline clients was generated.

Impact of attacks by the above ransomware families

- In case of NightSpire, Sinobi and Devman ransomware strains, Job Metadata and Image Entropy anomalies are observed, the backup of application data is successful. In the attack mentioned earlier, user's application files are encrypted but NetBackup configuration files are not compromised.

- While, in case of Nitrogen ransomware, data on NetBackup client is encrypted along with NetBackup configuration files or communication between NetBackup client and primary server is compromised that resulted in failures of backup jobs.

- For all the ransomware strains described earlier, in the case of the Data Protect, Client backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully, demonstrating the platform's resilience and ability to maintain data protection under adverse conditions.

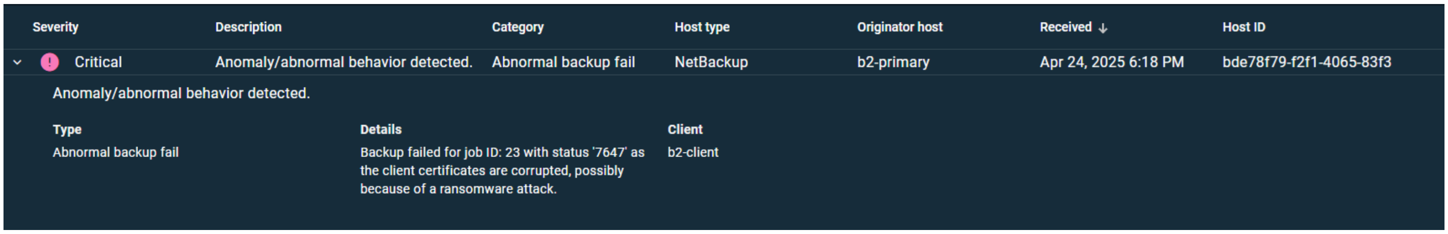
- Ransomware like **Devman** uses Windows Restart Manager to stop processes that lock files, improving encryption success. The **Nitrogen** group exploits truesight.sys, a signed driver from the LOLDrivers catalog, to kill AV and EDR. By abusing trusted Windows components with LOLBin/LOLBAS methods, these attackers hide their activity and evade security measures. **Sinobi** utilizes CIDR parsing to achieve subnet-wide impact and systematically mounts hidden or unmounted volumes to ensure no data escapes discovery. **NightSpire** maps the Active Directory environment to identify high-value targets, using Mimikatz to dump credentials and escalate to domain-level privileges.

Security solutions detail at a glance:

Data on NetBackup client is encrypted along with NetBackup configuration files

- Client Offline backup anomaly detects unusual network communication behaviour between NetBackup primary servers and clients. It checks the health of certificates that are deployed on the NetBackup client and starts the anomaly detection process.
- When the anomaly is detected, the Client Offline anomaly creates a critical audit event that indicates failed communication with the NetBackup client.

The following screenshot shows the data from REDLab:



Severity	Description	Category	Host type	Originator host	Received ↓	Host ID
Critical	Anomaly/abnormal behavior detected.	Abnormal backup fail	NetBackup	b2-primary	Apr 24, 2025 6:18 PM	bde78f79-f2f1-4065-83f3

Anomaly/abnormal behavior detected.

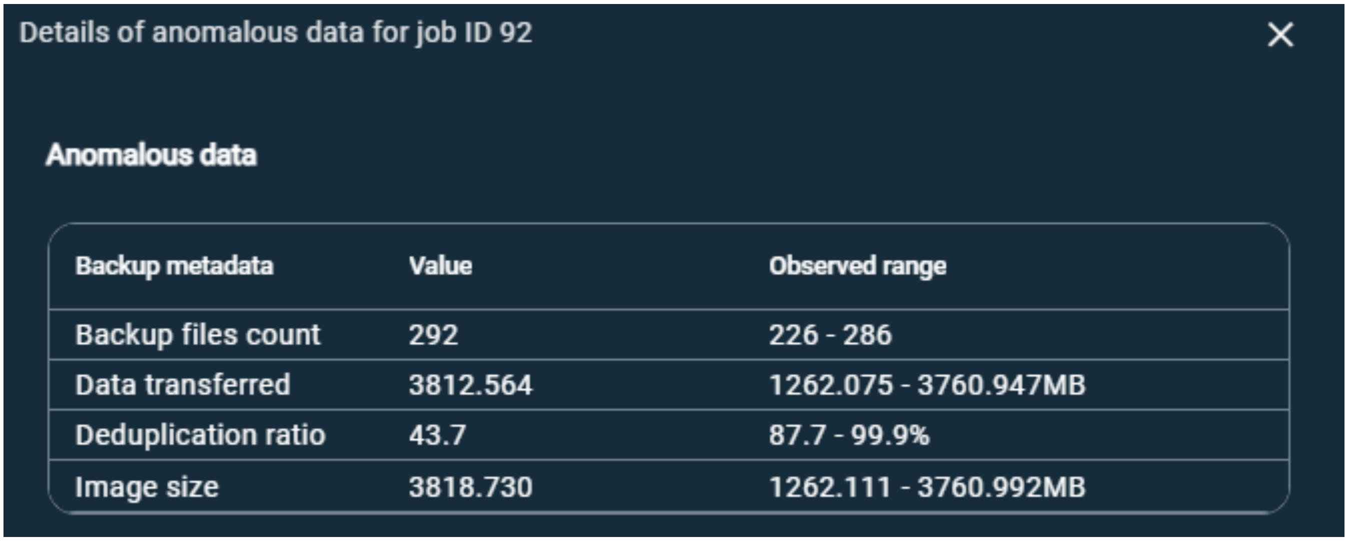
Type	Details	Client
Abnormal backup fail	Backup failed for job ID: 23 with status '7647' as the client certificates are corrupted, possibly because of a ransomware attack.	b2-client

More information around Client Offline Anomaly can be found in the NetBackup™ Security and Encryption Guide.

Data on NetBackup client is encrypted however NetBackup configuration files are intact and backup jobs are successful.

- **Job Metadata Anomaly:**
  - NetBackup uses machine learning (ML)-driven anomaly detection to detect anomalies. In this case, the change of backup file count, data transferred, data deduplication rate, image size and total time are detected by the ML algorithm, and an alert is generated.

Refer to the following screenshot:



Details of anomalous data for job ID 92

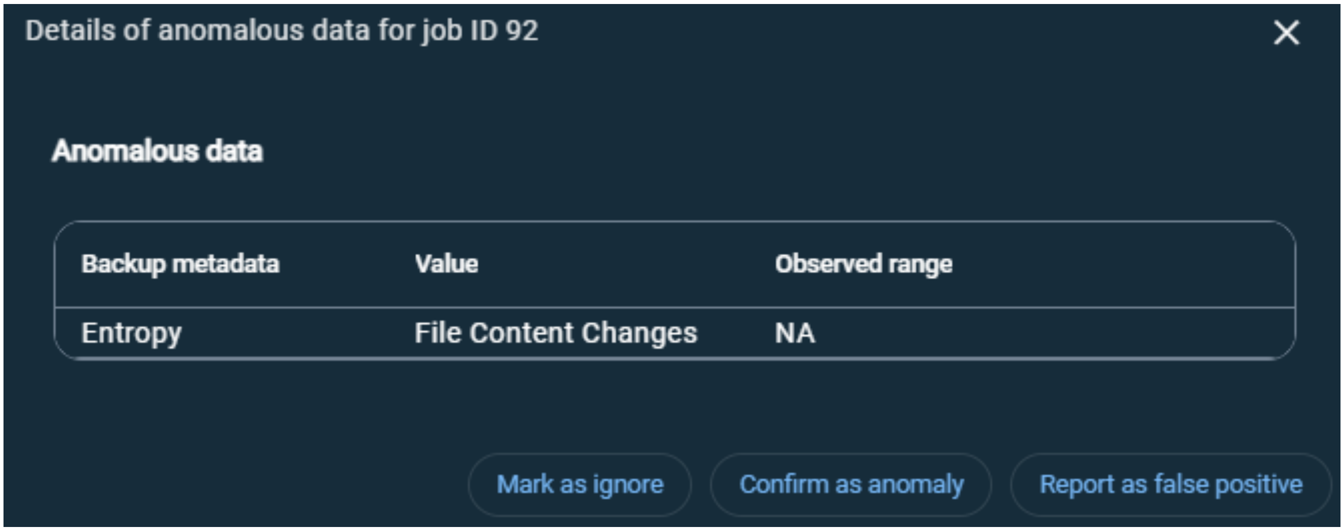
Anomalous data

Backup metadata	Value	Observed range
Backup files count	292	226 - 286
Data transferred	3812.564	1262.075 - 3760.947MB
Deduplication ratio	43.7	87.7 - 99.9%
Image size	3818.730	1262.111 - 3760.992MB

See more information about the Job Metadata anomaly here.

- **Image Entropy Data Anomaly:**
  - NetBackup computes an additional risk signal in-line, called entropy. It improves the quality of detected anomalies. Entropy is a measure of randomness of file contents. Threat vectors that encrypt files tend to abruptly change the entropy.
  - The entropy metric is used with the anomaly detection mechanism to help detect potential malicious activity. When this indicates anomaly activities, it is recommended to check the system for potential malicious actors. If suspicious activities are found, do not use those images as a recovery point.

Refer to the following screenshot:



Details of anomalous data for job ID 92

Anomalous data

Backup metadata	Value	Observed range
Entropy	File Content Changes	NA

See more information about the Image Entropy Data anomaly here.

Cohesity's Security Feature Overview: What's New?

Rapid Threat Hunt

To improve detection and cover more potential cyber threats, Threat Detection uses rapid threat hunting powered by multiple high-quality hash feeds. These feeds help security teams quickly identify suspicious or malicious files in their environment.

Following are the integrated hash feed sources:

- **Custom Hash Feeds**: Organizations can create their own list of malicious hashes based on their investigations. This helps find threats that are specific to their environment.
- **CISA (Cybersecurity and Infrastructure Security Agency):** CISA provides official threat intelligence, including file hashes, domains, and IP addresses linked to known cyber threats. These authoritative feeds are useful for detecting ransomware and other serious attacks.
- **Cohesity REDLab**: Cohesity in-house cybersecurity research lab which analyses malware, ransomware, and other cyber threats in controlled environments. The proprietary intelligence it generates gives unique insights that enhance threat detection.
- **Google Threat Intelligence:** This feed includes file hashes of known malicious files including the latest ones collected from real-world investigations and malware studies. Backed by Google's scale and expertise, it offers up-to-date and highly reliable information.
- **Open Source:** Uses publicly available threat intelligence feeds that share file hashes and indicators of compromise from global security communities. This helps identify new or lesser-known threats discovered by researchers worldwide.

By combining these feeds, Rapid Threat Hunt lets you quickly search using trusted Indicators of Compromise (IOCs), helping you detect, investigate, and respond to threats faster across your environment.

From the Security Center, you can perform the following actions:

- Perform Rapid Threat Hunt: Conduct rapid threat hunting activities using either recent searches or new search criteria to identify potential security threats efficiently.
- View the Search Results: Access and review the results generated from rapid threat hunts.
- Manage the Custom Hash Feeds: Add or delete custom hash feeds to enhance the accuracy and scope of threat detection.
- Manage the Hash Configuration Settings: Configure and maintain hash-related settings to ensure alignment with organizational security policies and operational requirements.

To run Rapid Threat Hunt, ensure your Cohesity cluster is upgraded to version 7.3-p20251104-00-0d574408.

Considerations for Custom Hash Management

Following are the key considerations for managing custom hashes and conducting hash-based scans within Threat Detection:

- **CSV File Upload – Maximum File Size and Count:** This configuration defines the maximum supported size for CSV file uploads containing custom hashes. The maximum file size is 500 KB. This typically supports about 4,000 to 4,500 hashes; the exact count may vary based on attributes such as comments, source, or type.
  For more information, see Add File Hashes.
- **Total custom hash library limit:** This setting defines the recommended and potential capacity for storing custom hashes within a tenant or library.
- **Recommended limit:** For best performance, 4000 to 7000 hashes for the cluster search.
- **Maximum limit:** Upto 10000 hashes including all the provider threat feeds (may affect performance).
- **Manual paste limits for Search:** There is no hard limit on the number of hashes you can paste into the Search field. The input area expands dynamically and is scrollable, with a fixed maximum height, and the latest entries remain visible. For best results, paste 10 to 30 hashes for the search, and use CSV upload or library management for larger sets.

Performance Considerations for Custom Hash Management

Following are the performance considerations for managing custom hashes and conducting hash-based scans within Threat Detection:

- **Scan performance and scaling behavior:** Scan performance may slow down as the number of hashes increases; for best results, keep your library under 10,000 hashes. Regularly remove stale or rarely used custom hashes to maintain an up-to-date and efficient library.
- **Cluster selection behavior:** By default, the scans are triggered across all eligible clusters which are healthy and connected.

Perform Rapid Threat Hunt

Threat Detection allows you to perform a Rapid Threat Hunt using either of these methods:

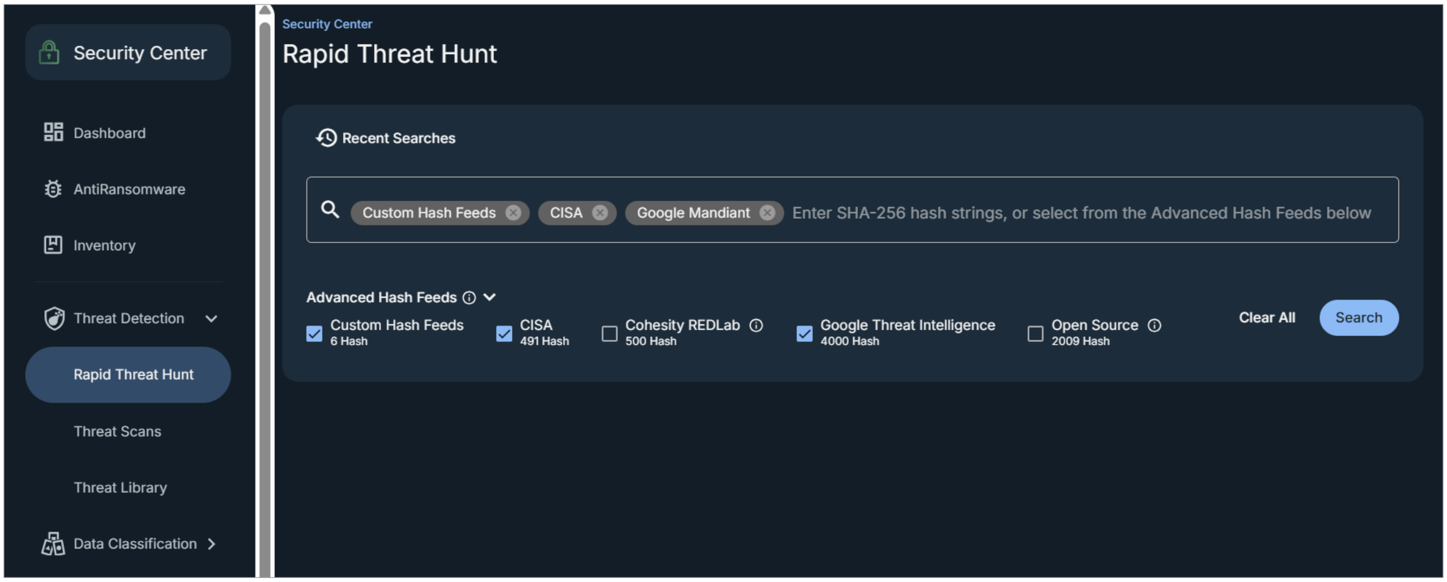
- New Search Criteria – Create fresh search queries to find new potential threats.
- Recent Searches – Quickly revisit past searches to spot threats.

Rapid Threat Hunt Using New Search Criteria

You can start a Rapid Threat Hunt by choosing custom search settings and advanced hash feeds for deeper, targeted detection.

To perform a Rapid Threat Hunt using the new search criteria:

1. Navigate to Threat Detection > Rapid Threat Hunt.
2. On the Rapid Threat Hunt page, in the Search field, enter one or more SHA-256 hash values, or select options from the Advanced Hash Feeds.

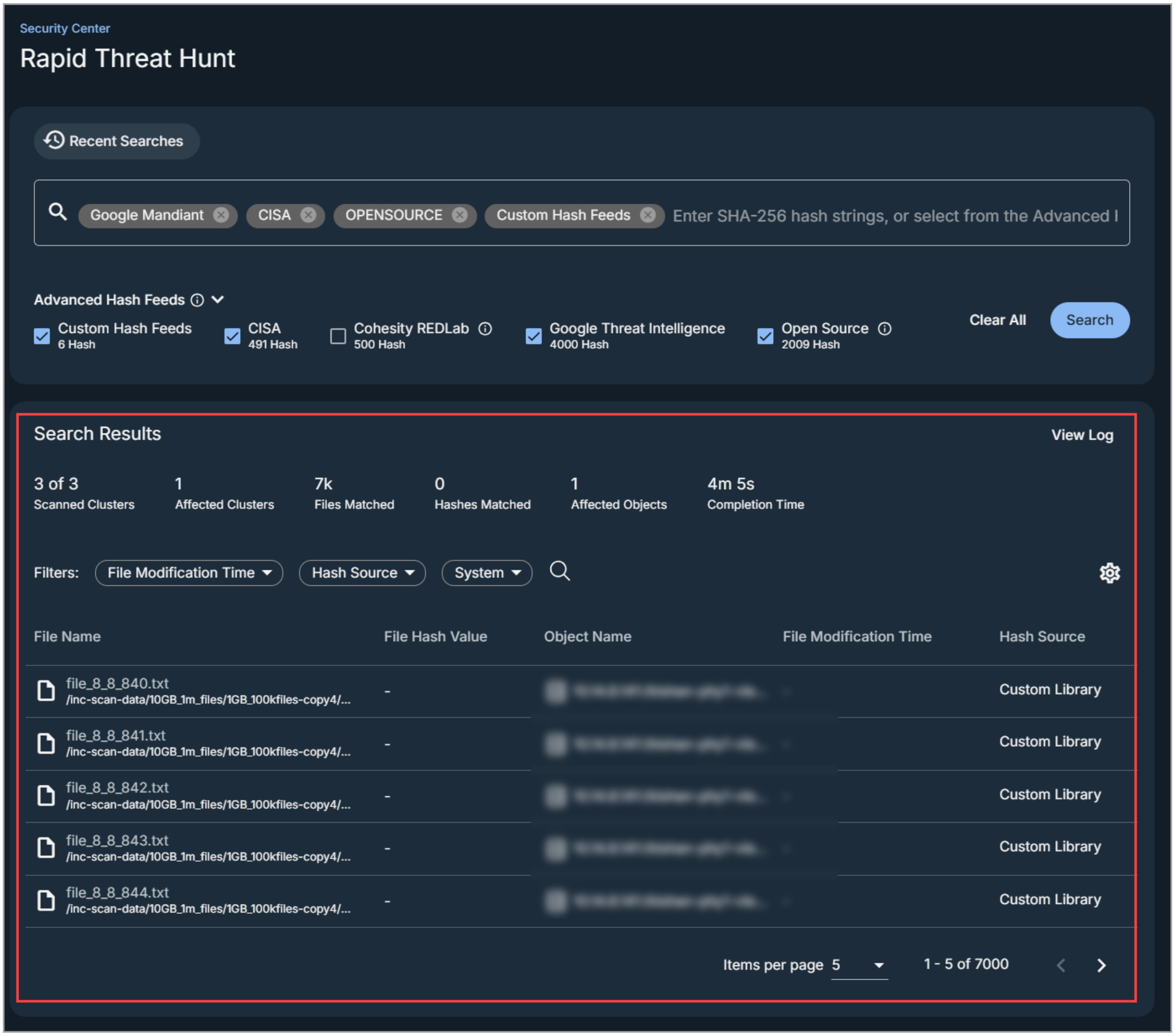


Custom Hash Feeds ⊗ CISA ⊗ Google Mandiant ⊗ Enter SHA-256 hash strings, or select from the Advanced Hash Feeds below

Advanced Hash Feeds

☑ Custom Hash Feeds 6 Hash
☑ CISA 491 Hash
□ Cohesity REDLab 500 Hash
☑ Google Threat Intelligence 4000 Hash
□ Open Source 2009 Hash

3. Click Search.



Security Center

Rapid Threat Hunt

Google Mandiant ⊗ CISA ⊗ OPENSOURCE ⊗ Custom Hash Feeds ⊗ Enter SHA-256 hash strings, or select from the Advanced I

Advanced Hash Feeds ⓘ

☑ Custom Hash Feeds 6 Hash
☑ CISA 491 Hash
☐ Cohesity REDLab ⓘ 500 Hash
☑ Google Threat Intelligence 4000 Hash
☑ Open Source ⓘ 2009 Hash

Search Results

3 of 3	1	7k	0	1	4m 5s
Scanned Clusters	Affected Clusters	Files Matched	Hashes Matched	Affected Objects	Completion Time

Filters: File Modification Time ▾ Hash Source ▾ System ▾

File Name	File Hash Value	Object Name	File Modification Time	Hash Source
file_8_8_840.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	[redacted]	Custom Library
file_8_8_841.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	[redacted]	Custom Library
file_8_8_842.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	[redacted]	Custom Library
file_8_8_843.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	[redacted]	Custom Library
file_8_8_844.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	[redacted]	Custom Library

Items per page 5 ▾ 1 - 5 of 7000

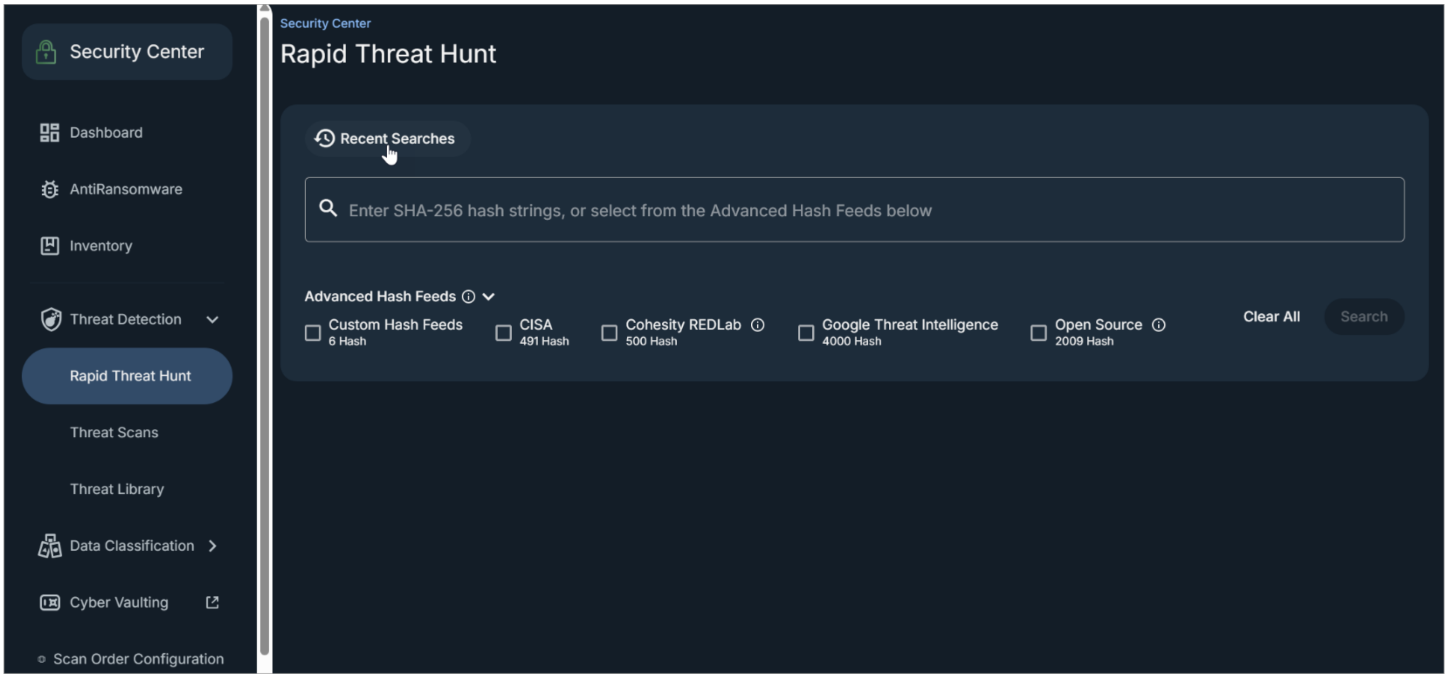
The results of the Rapid Threat Hunt appear in the Search Results section

Rapid Threat Hunt from Recent Searches

You can easily re-run a Rapid Threat Hunt from your recent search history, allowing you to efficiently repeat previously performed threat checks and investigations.

To perform a Rapid Threat Hunt using the recent searches:

1. Navigate to Threat Detection > Rapid Threat Hunt.
2. On the Rapid Threat Hunt page, click Recent Searches.



The Recent Searches page appears and lists all previously performed rapid threat hunts.

View Rapid Threat Hunt Results

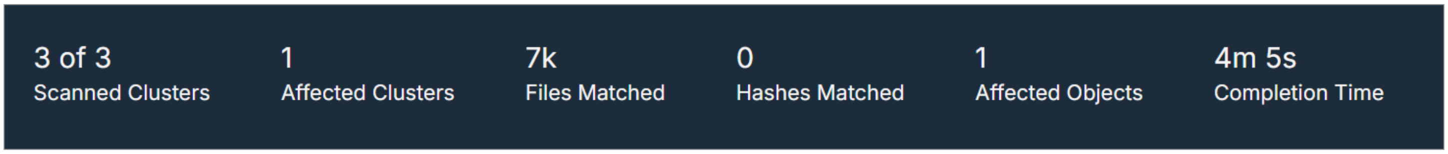
The Search Results section in the Rapid Threat Hunt page provides summary and details of all the files that match the search criteria, displaying the following details:

- Glance Bar
- File Hash Filter Details
- File Hash Search Data
- View the Log Details

Glance Bar

The glance bar summarizes the Rapid Threat Hunt details:

- **Scanned Clusters:** The number of clusters that were included in the Rapid Threat Hunt scan.
- **Affected Clusters:** The number of clusters where suspicious files were found during the Rapid Threat Hunt.
- **Files Matched:** The number of files in the system that match known suspicious file hashes from the Rapid Threat Hunt.
- **Hashes Matched:** The number of suspicious file hashes found in the system during the Rapid Threat Hunt.
- **Affected Objects:** The number of objects (files or devices) that match suspicious hashes found during the Rapid Threat Hunt.
- **Completion Time:** The date and time when the Rapid Threat Hunt scan finished.

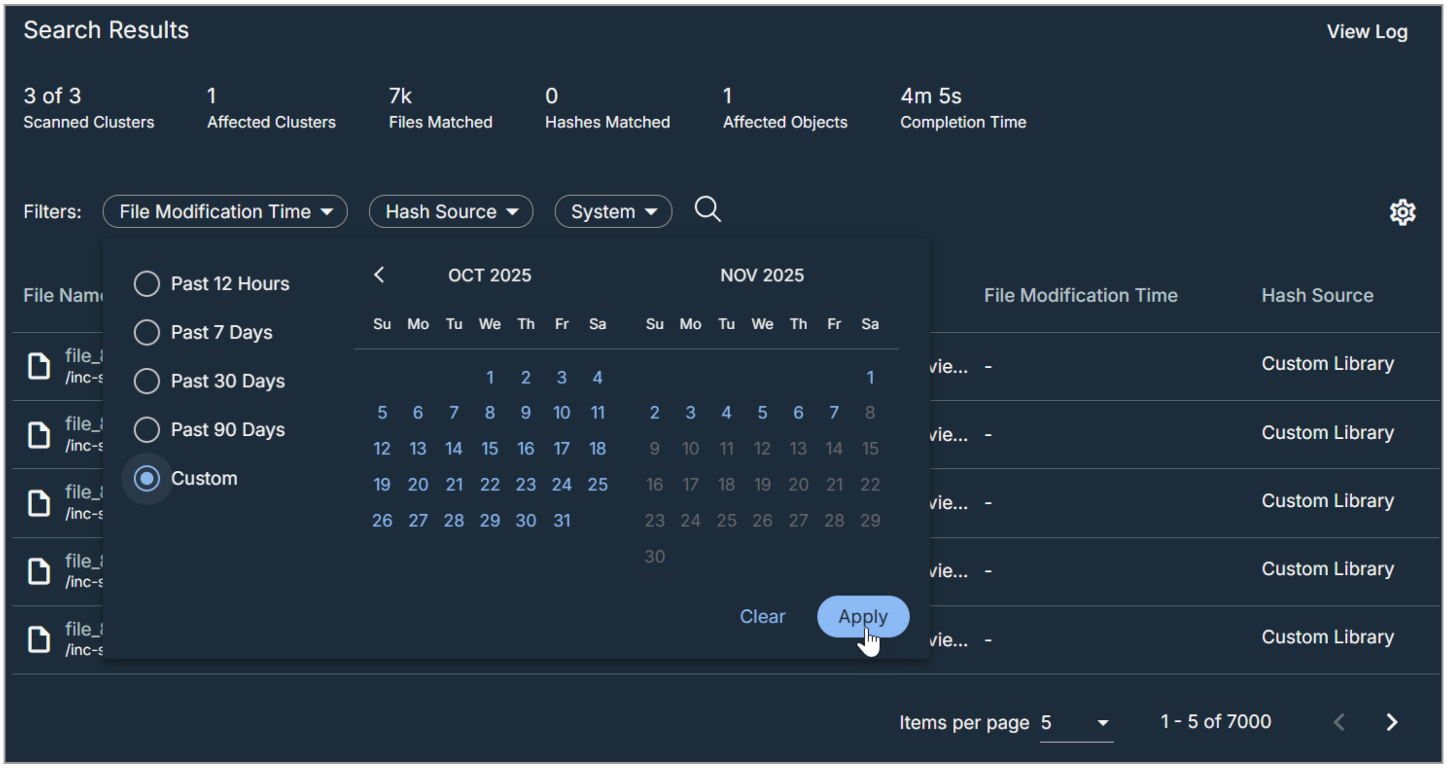


3 of 3	1	7k	0	1	4m 5s
Scanned Clusters	Affected Clusters	Files Matched	Hashes Matched	Affected Objects	Completion Time

File Hash Filter Details: Narrowing Your Search

Use these filters to isolate specific threats or timeframes:

- Modification Time: Narrow results to specific windows (e.g., Past 12 hours or a Custom range).



Search Results

View Log

3 of 3	1	7k	0	1	4m 5s
Scanned Clusters	Affected Clusters	Files Matched	Hashes Matched	Affected Objects	Completion Time

Filters: File Modification Time ▾ Hash Source ▾ System ▾

○ Past 12 Hours
○ Past 7 Days
○ Past 30 Days
○ Past 90 Days
● Custom

OCT 2025

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

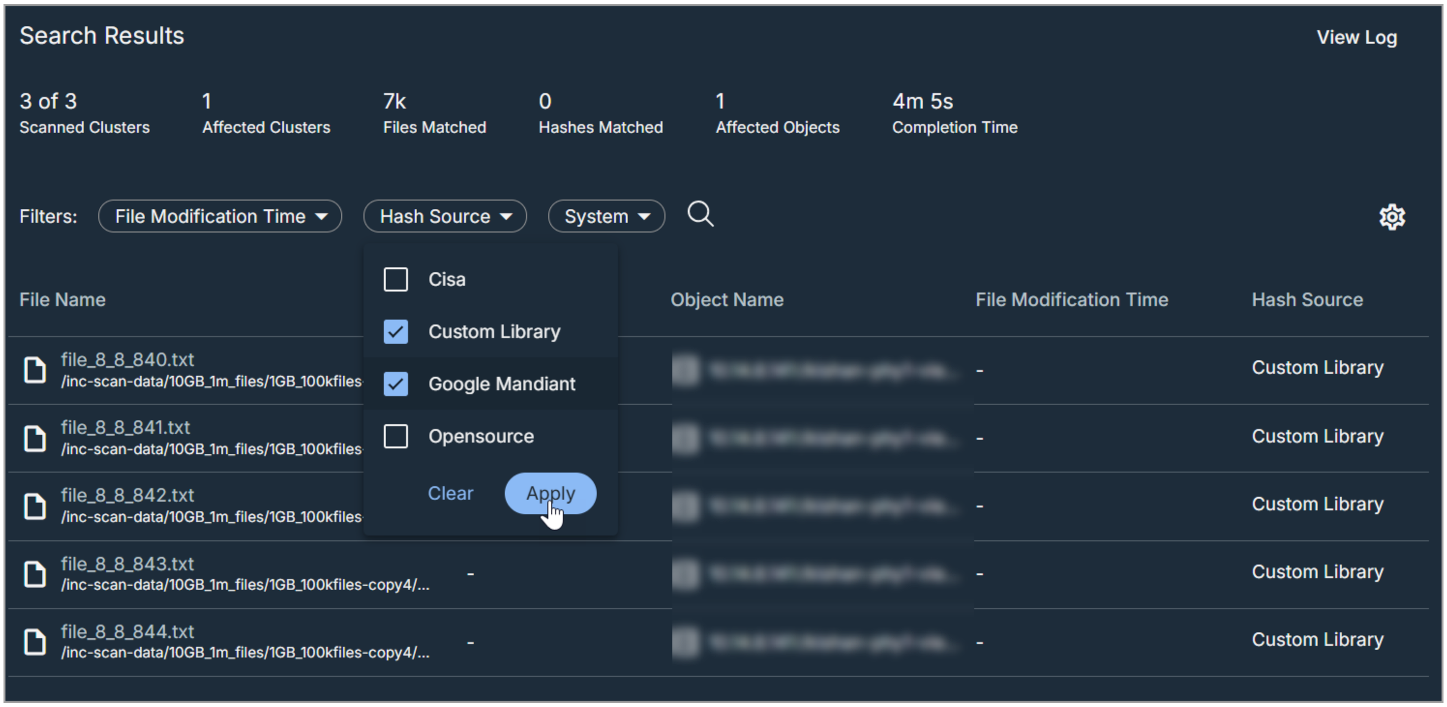
NOV 2025

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

File Nam		File Modification Time	Hash Source
file_ /inc-s	vie...	-	Custom Library
file_ /inc-s	vie...	-	Custom Library
file_ /inc-s	vie...	-	Custom Library
file_ /inc-s	vie...	-	Custom Library
file_ /inc-s	vie...	-	Custom Library

Items per page 5 ▾ 1 - 5 of 7000

- Hash Source: Filter by the intelligence origin, such as CISA, Google Threat Intelligence, or your own Custom Feeds.



Search Results

View Log

3 of 3 Scanned Clusters | 1 Affected Clusters | 7k Files Matched | 0 Hashes Matched | 1 Affected Objects | 4m 5s Completion Time

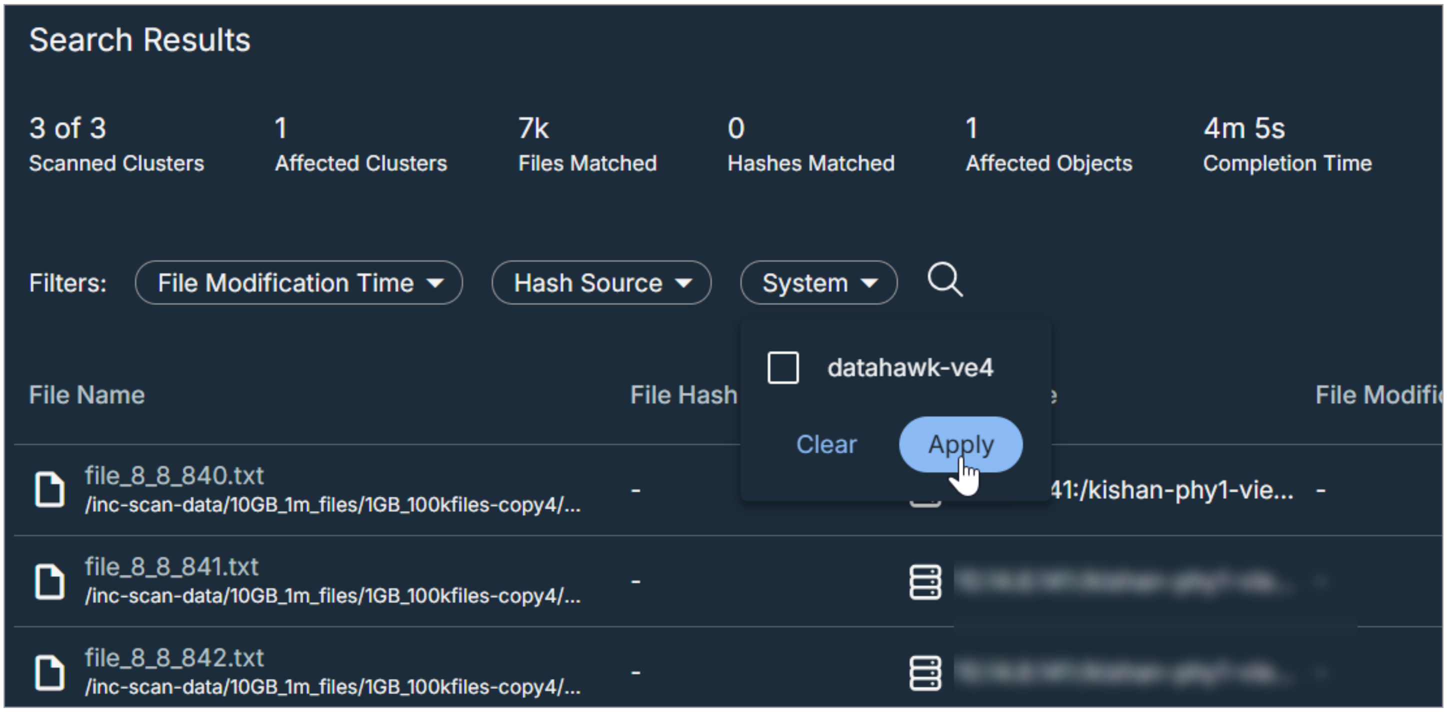
Filters: File Modification Time ▾ | Hash Source ▾ | System ▾

Hash Source:
- ☐ Cisa
- ☑ Custom Library
- ☑ Google Mandiant
- ☐ Opensource

Clear | Apply

File Name		Object Name	File Modification Time	Hash Source
file_8_8_840.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles		[redacted]	-	Custom Library
file_8_8_841.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles		[redacted]	-	Custom Library
file_8_8_842.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles		[redacted]	-	Custom Library
file_8_8_843.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library
file_8_8_844.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library

- System: Focus on specific devices or groups where files were detected.



Search Results

3 of 3 Scanned Clusters
1 Affected Clusters
7k Files Matched
0 Hashes Matched
1 Affected Objects
4m 5s Completion Time

Filters: File Modification Time ▾ Hash Source ▾ System ▾

□ datahawk-ve4

Clear Apply

File Name | File Hash | …e | File Modifi

file_8_8_840.txt
/inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/... - 41:/kishan-phy1-vie... -

file_8_8_841.txt
/inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/... - [redacted]

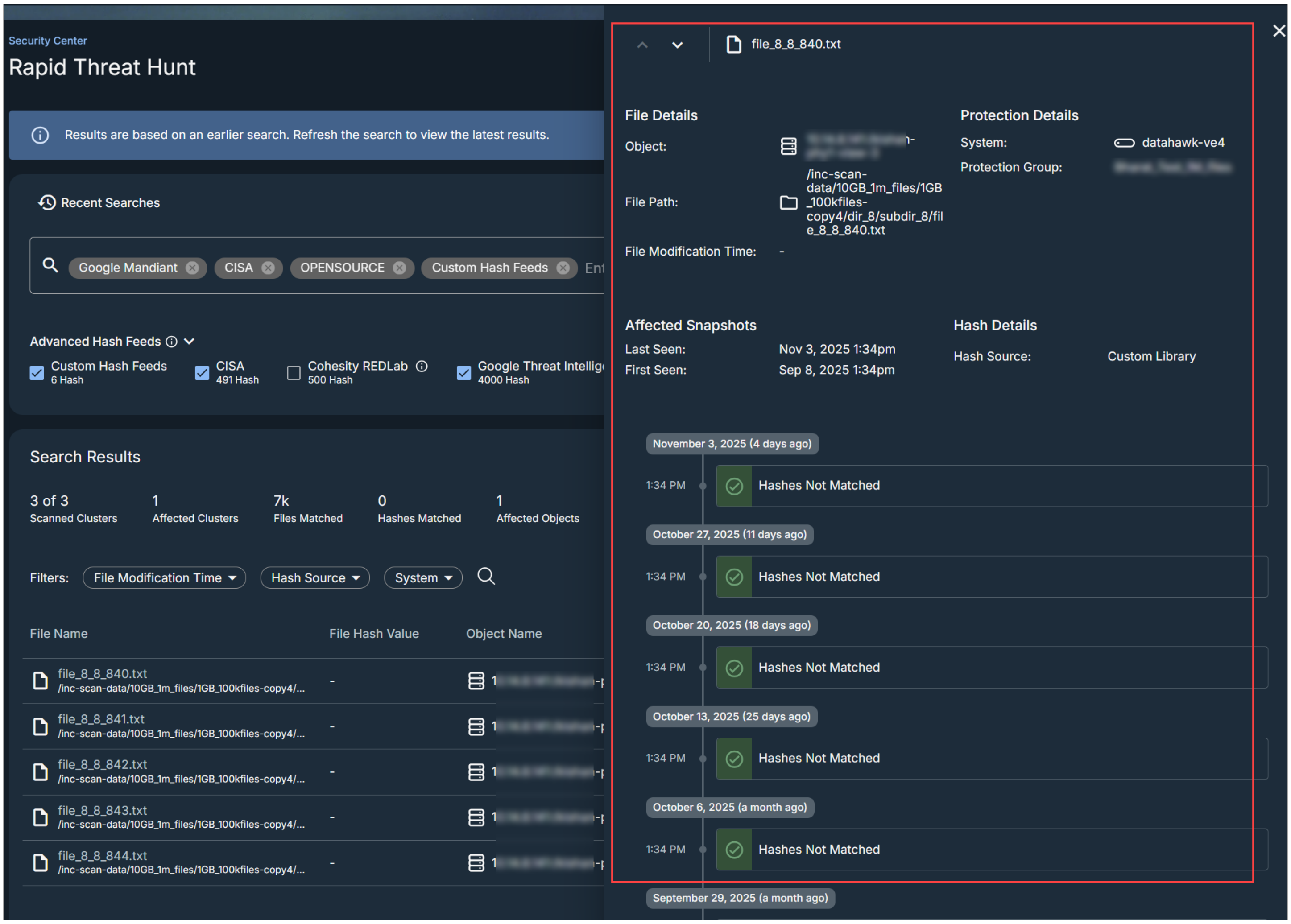
file_8_8_842.txt
/inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/... - [redacted]

File Hash Search Data

The Search Data Table lists every match found, including the File Name, SHA-256 Hash, Object Name, and Hash Source.

Clicking a File Name opens a granular view:

- File/Protection Details: Shows the VM path and the associated protection group.
- Affected Snapshots: Identifies the "First Seen" and "Last Seen" instances in your backups.
- Hash Details: Confirms which threat feed triggered the alert.



Results are based on an earlier search. Refresh the search to view the latest results.

Advanced Hash Feeds

☑ Custom Hash Feeds 6 Hash
☑ CISA 491 Hash
□ Cohesity REDLab 500 Hash
☑ Google Threat Intellig 4000 Hash

Search Results

3 of 3	1	7k	0	1
Scanned Clusters	Affected Clusters	Files Matched	Hashes Matched	Affected Objects

File Name	File Hash Value	Object Name
file_8_8_840.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	1[redacted]-ǀ
file_8_8_841.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	1[redacted]-ǀ
file_8_8_842.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	1[redacted]-ǀ
file_8_8_843.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	1[redacted]-ǀ
file_8_8_844.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	1[redacted]-ǀ

file_8_8_840.txt

File Details

Object: [redacted]n-

File Path: /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/dir_8/subdir_8/file_8_8_840.txt

File Modification Time: -

Protection Details

System: datahawk-ve4

Protection Group: [redacted]

Affected Snapshots

Last Seen: Nov 3, 2025 1:34pm

First Seen: Sep 8, 2025 1:34pm

Hash Details

Hash Source: Custom Library

November 3, 2025 (4 days ago)
1:34 PM ✓ Hashes Not Matched

October 27, 2025 (11 days ago)
1:34 PM ✓ Hashes Not Matched

October 20, 2025 (18 days ago)
1:34 PM ✓ Hashes Not Matched

October 13, 2025 (25 days ago)
1:34 PM ✓ Hashes Not Matched

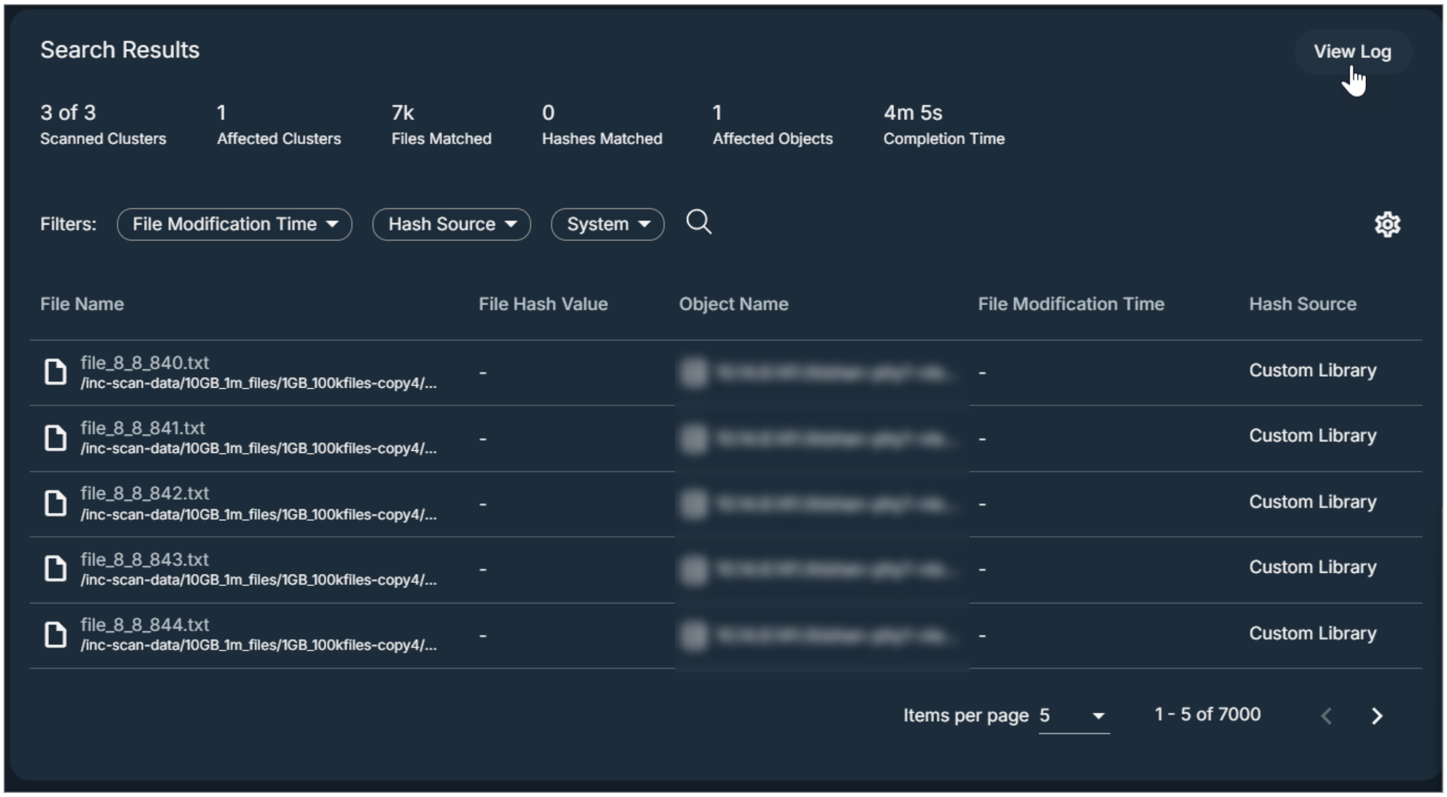
October 6, 2025 (a month ago)
1:34 PM ✓ Hashes Not Matched

September 29, 2025 (a month ago)

View the Log Details

Click View Log on the Search Results page to move from "what was found" to "how it was found."

In the Search Results page, click View Log:



Search Results

3 of 3 Scanned Clusters

1 Affected Clusters

7k Files Matched

0 Hashes Matched

1 Affected Objects

4m 5s Completion Time

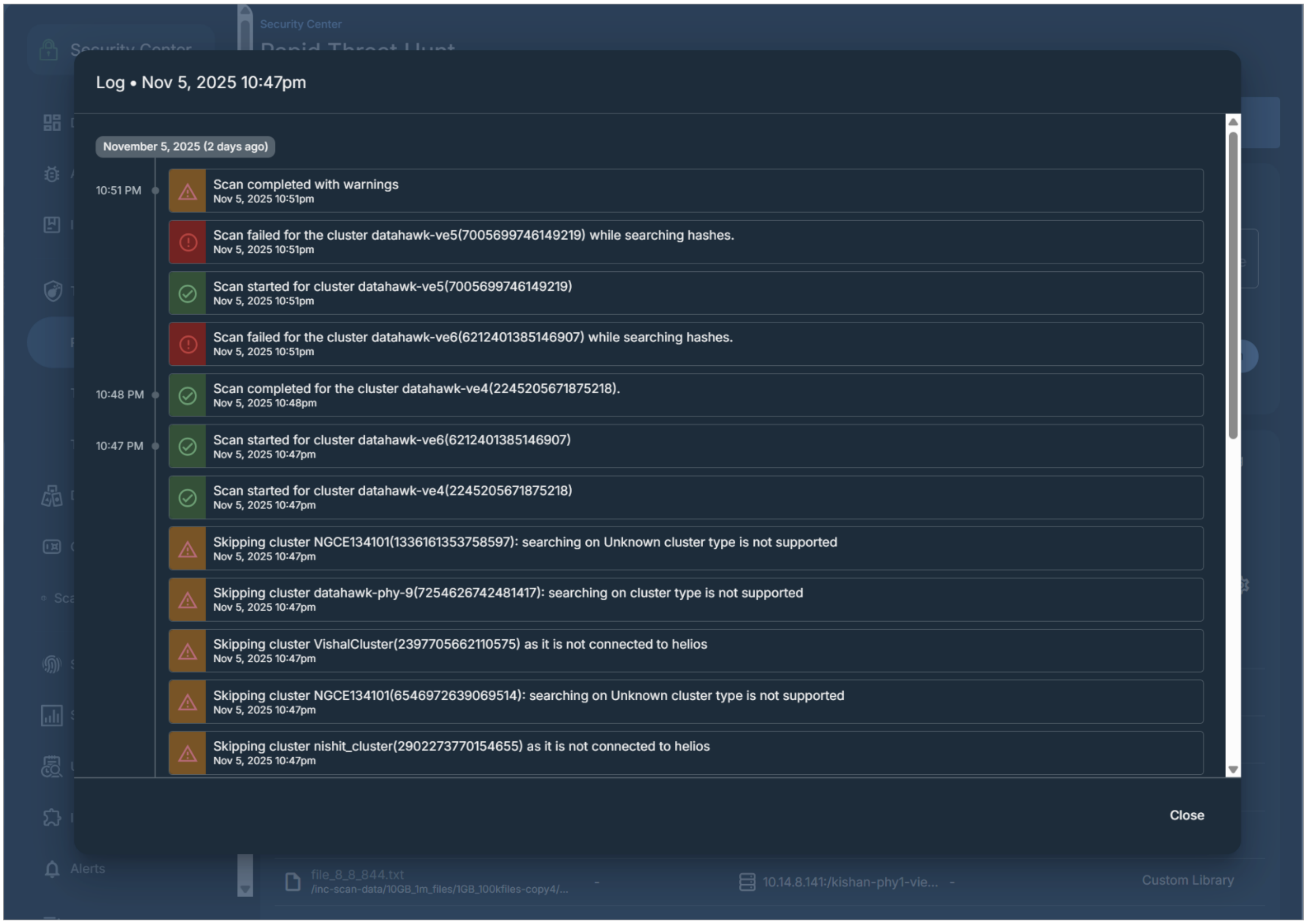
Filters: File Modification Time ▾ Hash Source ▾ System ▾

File Name	File Hash Value	Object Name	File Modification Time	Hash Source
file_8_8_840.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library
file_8_8_841.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library
file_8_8_842.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library
file_8_8_843.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library
file_8_8_844.txt /inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...	-	[redacted]	-	Custom Library

Items per page 5 ▾ 1 - 5 of 7000

The **View Log** option allows you to view detailed information about the Rapid Threat Hunt process, including scan progress, status updates, and any errors or actions taken during the hunt. It helps you review activity and troubleshoot issues if needed.

The following page displays the log details:



Log • Nov 5, 2025 10:47pm

November 5, 2025 (2 days ago)

```
10:51 PM  Scan completed with warnings
          Nov 5, 2025 10:51pm
          Scan failed for the cluster datahawk-ve5(7005699746149219) while searching hashes.
          Nov 5, 2025 10:51pm
          Scan started for cluster datahawk-ve5(7005699746149219)
          Nov 5, 2025 10:51pm
          Scan failed for the cluster datahawk-ve6(6212401385146907) while searching hashes.
          Nov 5, 2025 10:51pm
10:48 PM  Scan completed for the cluster datahawk-ve4(2245205671875218).
          Nov 5, 2025 10:48pm
10:47 PM  Scan started for cluster datahawk-ve6(6212401385146907)
          Nov 5, 2025 10:47pm
          Scan started for cluster datahawk-ve4(2245205671875218)
          Nov 5, 2025 10:47pm
          Skipping cluster NGCE134101(1336161353758597): searching on Unknown cluster type is not supported
          Nov 5, 2025 10:47pm
          Skipping cluster datahawk-phy-9(7254626742481417): searching on cluster type is not supported
          Nov 5, 2025 10:47pm
          Skipping cluster VishalCluster(2397705662110575) as it is not connected to helios
          Nov 5, 2025 10:47pm
          Skipping cluster NGCE134101(6546972639069514): searching on Unknown cluster type is not supported
          Nov 5, 2025 10:47pm
          Skipping cluster nishit_cluster(2902273770154655) as it is not connected to helios
          Nov 5, 2025 10:47pm
```

Close
Security Center
Rapid Threat Hunt
Alerts
file_8_8_844.txt
/inc-scan-data/10GB_1m_files/1GB_100kfiles-copy4/...
10.14.8.141:/kishan-phy1-vie...
Custom Library

Research references:

- https://www.cisa.gov – Threat intelligence data and most pressing issues that CISA tracks, and notifications issued by government organizations.
- https://www.virustotal.com – Intelligence data, ransomware, or malware samples, discover threat commonalities and track new variants of surveilled malware families.
- https://www.hybrid-analysis.com – Malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.
- https://www.enigmasoftware.com/ - PC security alerts & news and Advanced Analytics
- https://www.cyborgsecurity.com/ - Provides a library of expertly crafted constantly updated threat hunting news and content.
- https://www.avertium.com/ - Threat Summary and Blogs
- https://unit42.paloaltonetworks.com/ - Research blogs and Analysis of strains
- https://www.cert-in.org.in/ - Collection, forecast, and alerts of cyber security incidents.
- https://www.pcrisk.com/ - Latest digital threats and malware infections
- https://thecyberexpress.com/ - Intelligence data and news around latest ransomware attacks
- https://www.blackfog.com – Get monthly news around attacks and details of impacted organizations.
- https://www.bleepingcomputer.com – Daily news of recent activities carried out by ransomware gangs and methods used to infiltrate enterprises.
- https://www.truesec.com/ - Blogs and IOC’s
- https://www.csk.gov.in/ - Threat Alerts and Security Announcements
- https://www.sentinelone.com – Analytics data from various security vendors and insights around behavior pattens for each ransomware family
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC’s