

What's new?

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 Trust Center: Learn more about Cohesity REDLab](#)

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.

For IT and security leaders, this means confidence that your backup and recovery solutions have been tested to deliver the highest levels of data security. They're hardened and tested components of your cybersecurity strategy.

Since REDLab was built in early 2023, the focus has been on validating [Cohesity NetBackup software](#) and [NetBackup appliances](#). With the addition of DataProtect, we're raising the bar, ensuring that more of [our platform](#) is hardened against advanced threats before they reach your environment.

We now continuously validate DataProtect's 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.

Critical Threat Updates – November 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. In November, support for several notable threats was added as noted below and more details are available at: <https://www.cohesity.com/trust/redlab/advisories/>

- Agent Tesla Returns “The Old RAT with New Tricks”: Agent Tesla, a .NET-based RAT and credential-stealer, is back with multi-stage delivery via phishing emails containing obfuscated scripts and PowerShell loaders. It executes in memory to evade detection, steals credentials from browsers, email clients, VPN/FTP tools, and Windows stores, captures keystrokes and screenshots, and exfiltrates data through multiple channels. Action Required: Monitor PowerShell and process injection activity, and run threat scans with updated libraries or custom YARA rules.
- SharePoint to Ransomware “ToolShell & AK47C2”: Attackers exploit SharePoint Server vulnerabilities (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770) to deploy web shells and the AK47C2 backdoor. The malware harvests credentials, machine keys, and configuration data, moves laterally, exfiltrates data, and deploys ransomware. Immediate Response: Patch SharePoint servers, rotate IIS/ASP.NET keys, and scan backup snapshots for malicious artifacts before restoration.

REDLab recommendations:

- Enable continuous anti-ransomware monitoring in Security Center
- Schedule regular threat scans using updated threat libraries
- Implement periodic file-hash scanning for dormant malware detection
- Review and quarantine suspicious backup snapshots before recovery
- 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.

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

Name	Ransomware family	Behavioral pattern
CS173	CS137 Ransomware group	Execution, Defense evasion, Anti Debugging, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies, Double-extortion.
MedusaLocker v3	Medusalocker Ransomware group	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.
Nuclear Ransomware	BTCWare ransomware family	Command and Scripting Interpreter, Data Encrypted for Impact, File and Directory Discovery, Inhibit System Recovery, File/Extension Modification, Defense Evasion, User Impact Message Delivery
SafePay Ransomware	Phobos ransomware family	Command & Scripting Interpreter, Disable Security Tools, Kill Backup Processes, Delete Shadow Copies, Inhibit System Recovery, Data Encrypted for Impact, Network Share Encryption, File Renaming (.safepay), Data Exfiltration, Persistence via Registry & Scheduled Tasks

REDLab findings:

- **CS137 (attack on NetBackup and Data Protect client):**

- **Family:** CS137 Ransomware group | **Behavior pattern:** Execution, Defense evasion, Anti Debugging, File and Directory discovery, Process Discovery, Data encrypted for impact, Delete shadow copies, Double-extortion
- **Know Me:** CS137 is a recently identified and emerging ransomware strain, first observed in early 2025 and believed to be in its initial testing or development phase. The name is derived from the radioactive isotope Cesium-137. The malware uses the strong ChaCha20 symmetric encryption algorithm to encrypt files, making them inaccessible without the specific decryption key. The attackers employ a traditional encryption-based extortion model, leaving behind a basic text ransom note and changing the victim's desktop background. Encrypted files are renamed with a random 10-alphanumeric character sequence while keeping the original extension.
- **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 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.

- **MedusaLocker v3 (attack on NetBackup and Data Protect client):**

- **Family:** Medusalocker Ransomware group | **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:** MedusaLocker v3 is an evolved ransomware strain designed for rapid, wide-scale encryption across enterprise environments. Distributed through a RaaS model, it spreads via compromised RDP, phishing, or exploited vulnerabilities. The v3 variant uses multi-threaded encryption, targets entire subnets, and can encrypt hidden or unmounted volumes, enabling maximum data impact. It disables recovery mechanisms, security tools, and backups before encrypting files using AES-256 with RSA key protection. Its strong defense-evasion techniques make it harder to detect and contain during execution.
- **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.

REDLab findings:

- **Nuclear Ransomware (attack on NetBackup and Data Protect client):**
 - **Family:** BTCWare ransomware family | **Behavior pattern:** Command and Scripting Interpreter, Data Encrypted for Impact, File and Directory Discovery, Inhibit System Recovery, File/Extension Modification, Defense Evasion, User Impact Message Delivery
 - **Know Me:** Nuclear is a ransomware variant within the BTCWare family, known for encrypting user files using AES encryption with the AES key protected via RSA, making unauthorized decryption nearly impossible. After encrypting files, it renames them using the format “[attacker-email].nuclear”, such as file.txt.black.world@tuta.io.nuclear. The ransomware displays its ransom note through a HELP.hta window, instructing victims to contact the attacker via email for payment details. Nuclear focuses on quickly encrypting common user directories, disabling recovery options, and evading basic detection tools.
 - **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.

- **SafePay Ransomware (attack on NetBackup and Data Protect client):**
 - **Family:** Babuk Ransomware Gang | **Behaviour pattern:** Command & Scripting Interpreter, Disable Security Tools, Kill Backup Processes, Delete Shadow Copies, Inhibit System Recovery, Data Encrypted for Impact, Network Share Encryption, File Renaming (.safepay), Data Exfiltration, Persistence via Registry & Scheduled Tasks
 - **Know Me:** SafePay is a Phobos-lineage ransomware variant delivered through a RaaS model. It uses fast AES-256 + RSA-2048 hybrid encryption to lock files across local systems and network shares, renaming them with the “.safepay” extension. SafePay disables security tools, deletes shadow copies, kills backup-related processes, and exfiltrates sensitive data for double-extortion. A TXT/HTML ransom note directs victims to a Tor-based chat portal for payment instructions.
 - **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 given ransomware families

- In case of CS137 ransomware, 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 MedusaLocker V3, Nuclear and SafePay ransomwares, 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.

Recommended solutions:

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.

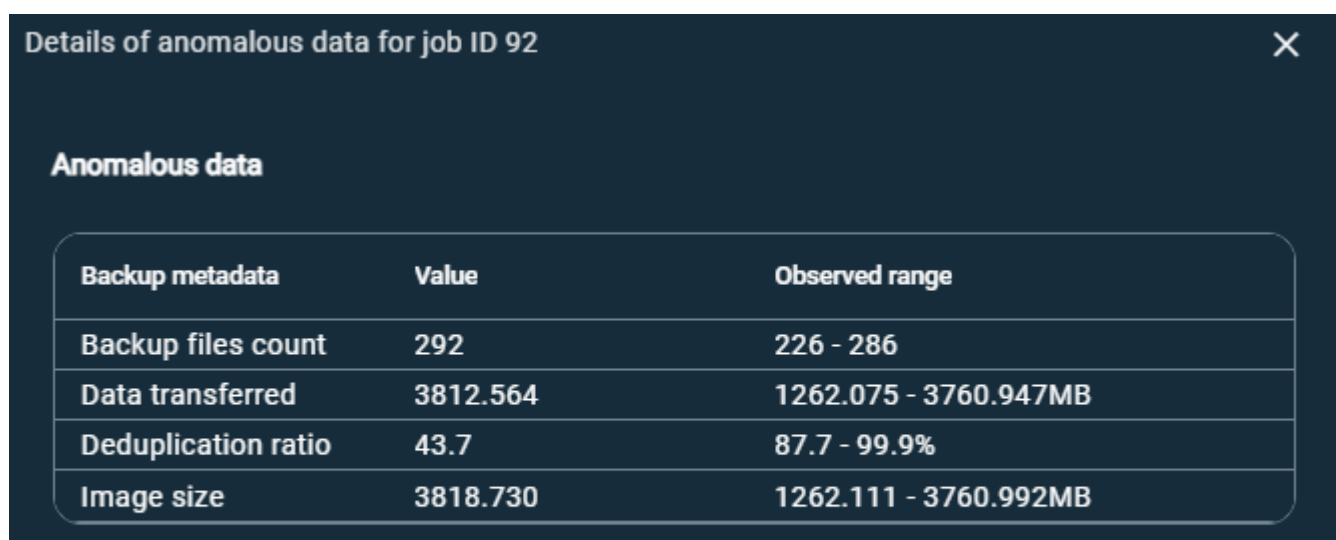
The following screenshot shows the data from REDLab:

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			

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:



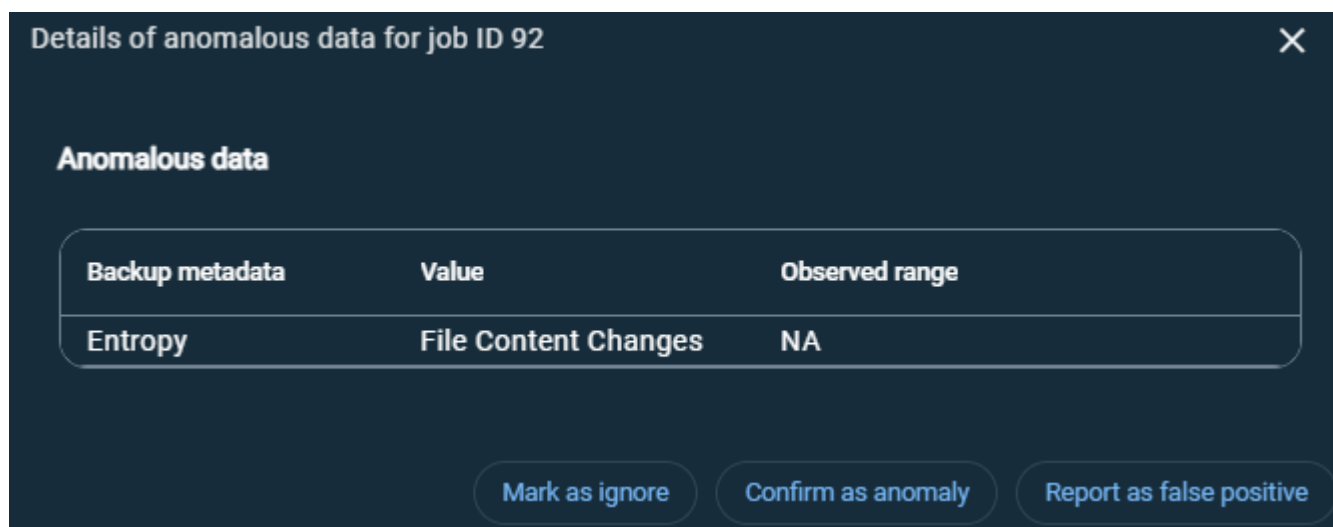
Backup metadata	Value	Observed range
Backup files count	292	226 - 286
Data transferred	3812.564	1262.075 - 3760.947MB
Deduplication ratio	43.7	87.7 - 99.9%
Image size	3818.730	1262.111 - 3760.992MB

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:



See more information about the Image Entropy Data anomaly [here](#).

Security Feature Overview

Threat Library - Custom Hash Feeds

The Threat Library helps you manage threat intelligence in one place, making it easier to detect and respond to cyber threats. In Custom Hash Feeds users can add or remove file hash feeds that are relevant to your organization. These custom feeds allow you to track known malicious or suspicious files and quickly detect them across endpoints.

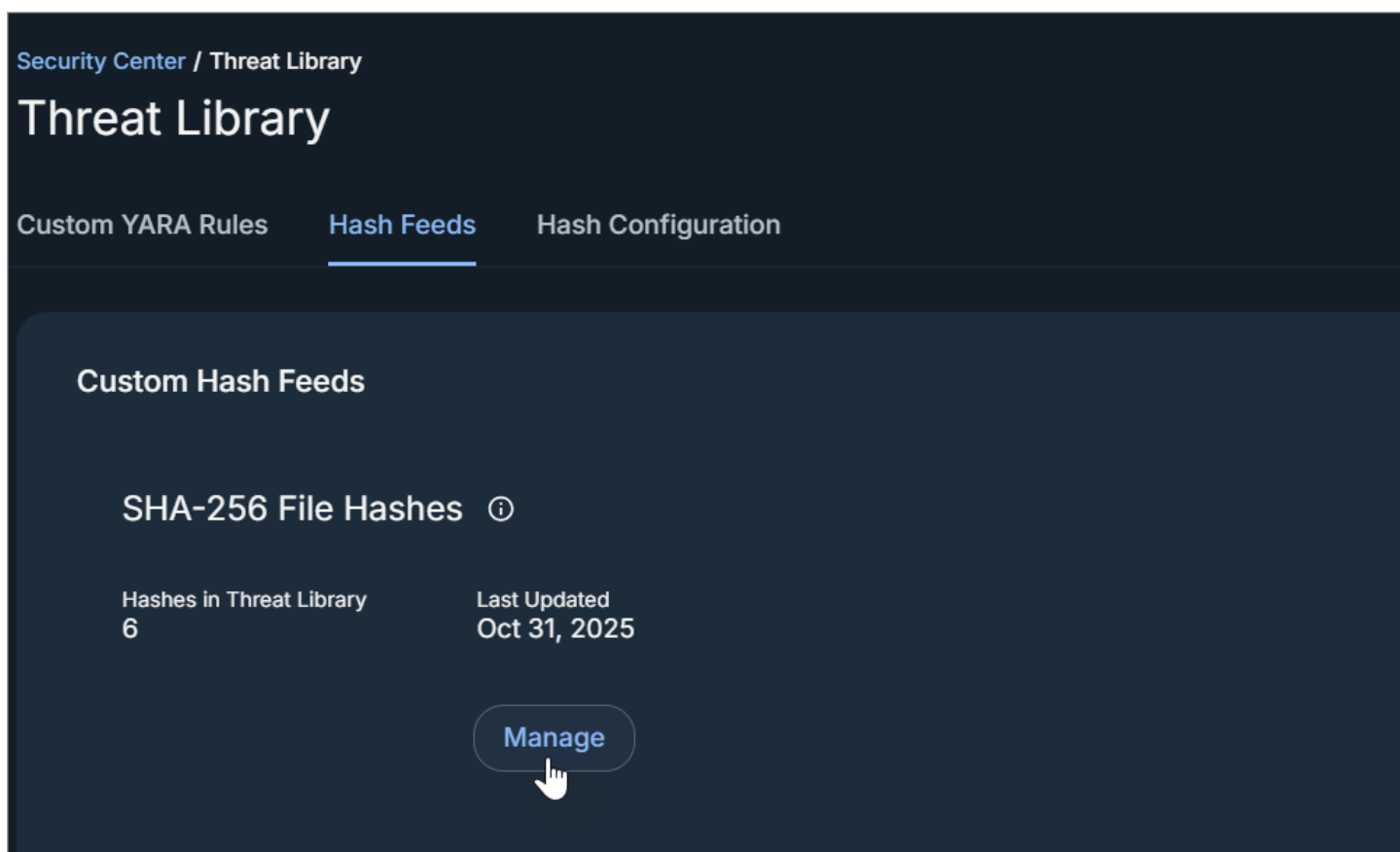
The Hash Feeds tab allows you to add or delete custom hash feeds within the Threat Library. These feeds contain file hashes identified during investigations or sourced from trusted intelligence, helping you detect known malicious or suspicious files specific to your environment.

The screenshot displays the Cohesity Security Center interface, specifically the Threat Library section. The left sidebar contains a navigation menu with options: Security Center, Dashboard, AntiRansomware, Inventory, Threat Detection (with a dropdown arrow), Rapid Threat Hunt, Threat Scans, Threat Library (highlighted), Data Classification (with a right arrow), Cyber Vaulting (with an external link icon), Scan Order Configuration, Security Posture (with a right arrow), Sensitive Data Posture, User Activity (with a right arrow), Integrations, and Alerts. The main content area is titled 'Threat Library' and has three tabs: Custom YARA Rules, Hash Feeds (selected), and Hash Configuration. Under the 'Hash Feeds' tab, there are two sections: 'Custom Hash Feeds' and 'Built-in Hash Feeds'. The 'Custom Hash Feeds' section shows 'SHA-256 File Hashes' with 6 hashes in the library, last updated on Oct 31, 2025, and a 'Manage' button. The 'Built-in Hash Feeds' section lists four feeds: CISA (491 hashes, last updated Nov 7, 2025), Cohesity REDLab (500 hashes, last updated Nov 7, 2025), Google Threat Intelligence (4000 hashes, last updated Nov 7, 2025), and Open Source (2009 hashes, last updated Nov 7, 2025).

Steps to Add File Hashes

To add file hashes:

1. Navigate to **Threat Detection > Threat Library** and select the Hash Feeds tab.
2. Under Custom Hash Feeds tile, click **Manage**.



3. On the Custom File Hashes page, click Add File Hashes.

Security Center / Custom File Hashes
Add File Hashes

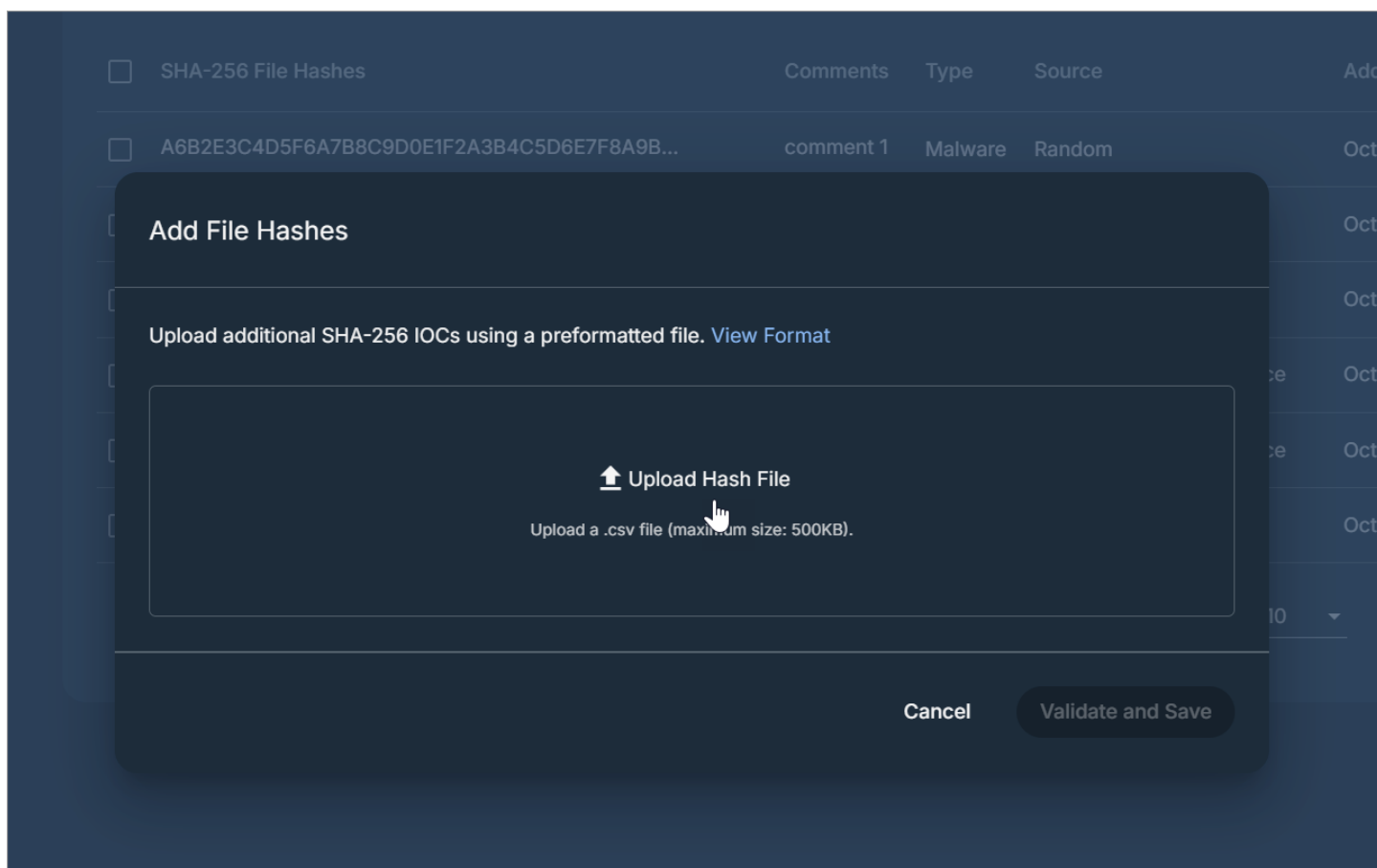
Custom File Hashes

Filters:
Source
Type
Added On

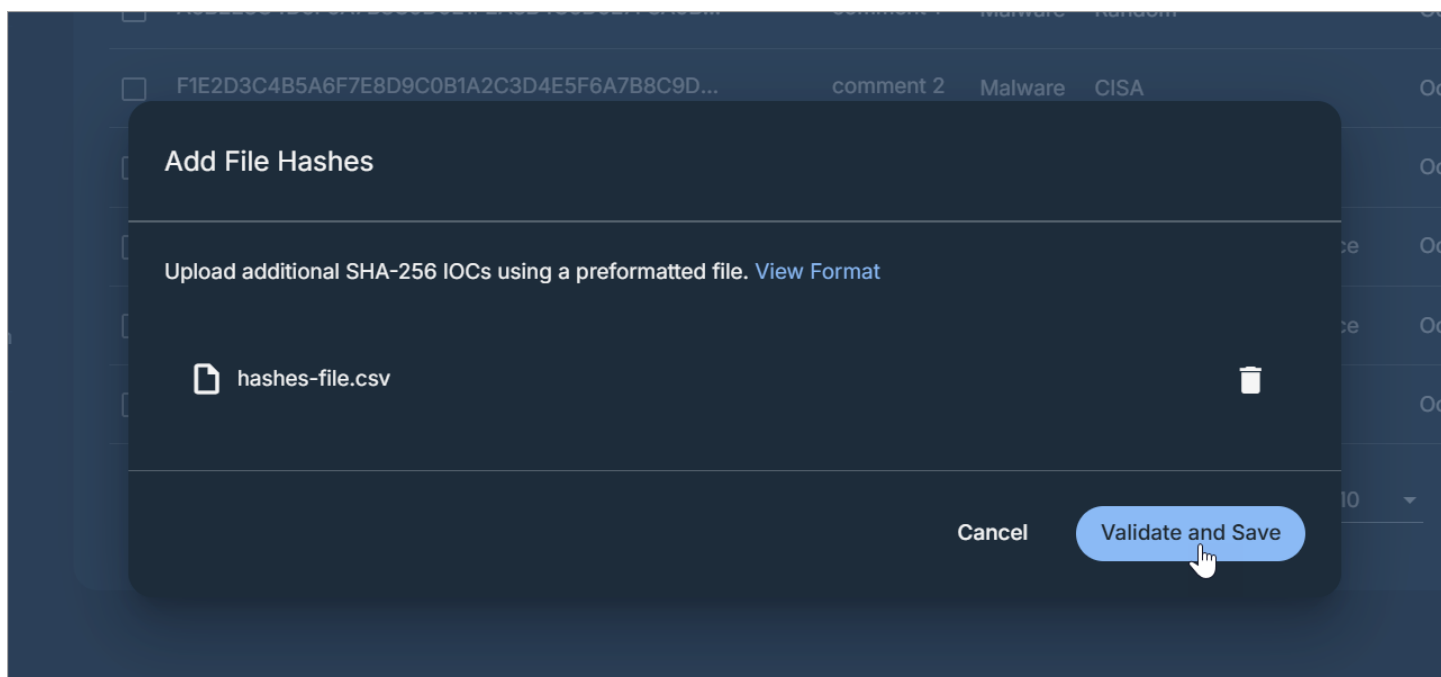
<input type="checkbox"/>	SHA-256 File Hashes	Comments	Type	Source	Added On
<input type="checkbox"/>	A6B2E3C4D5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B...	comment 1	Malware	Random	Oct 31, 2025 3:12pm
<input type="checkbox"/>	F1E2D3C4B5A6F7E8D9C0B1A2C3D4E5F6A7B8C9D...	comment 2	Malware	CISA	Oct 31, 2025 3:12pm
<input type="checkbox"/>	E2F1A0B9C8D7E6F5A4B3C2D1E0F9A8B7C6D5E4F...	comment 6	Malware	Open Source	Oct 31, 2025 3:12pm
<input type="checkbox"/>	B9C8D7E6F5A4B3C2D1E0F9A8B7C6D5E4F3A2B1C...	comment 3	Malware	Google Threat Intelligence	Oct 31, 2025 3:12pm
<input type="checkbox"/>	C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B0C1D...	comment 4	Malware	Google Threat Intelligence	Oct 31, 2025 3:12pm
<input type="checkbox"/>	D8E7F6A5B4C3D2E1F0A9B8C7D6E5F4A3B2C1D0E...	comment 5	Malware	Open Source	Oct 31, 2025 3:12pm

Items per page 10
1 - 6 of 6

4. On the Add File Hashes page, click Upload Hash File to upload a preformatted file containing additional SHA-256 IOCs.



5. Click Validate and Save.



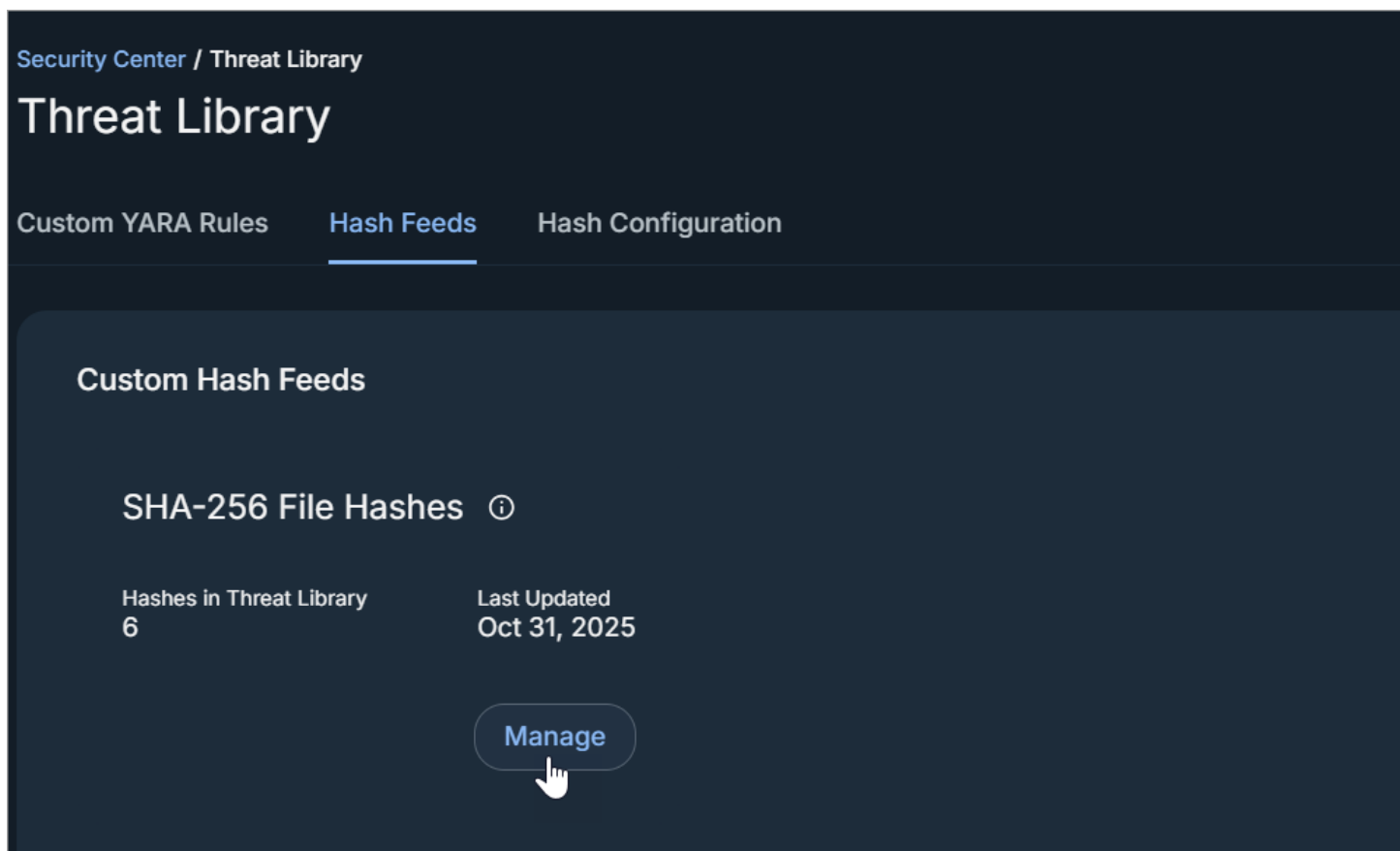
Note: The maximum CSV upload size is 500 KB, which typically supports about 4,000 to 4,500 hashes; the exact count may vary based on attributes such as comments, source, or type.

Delete File Hashes

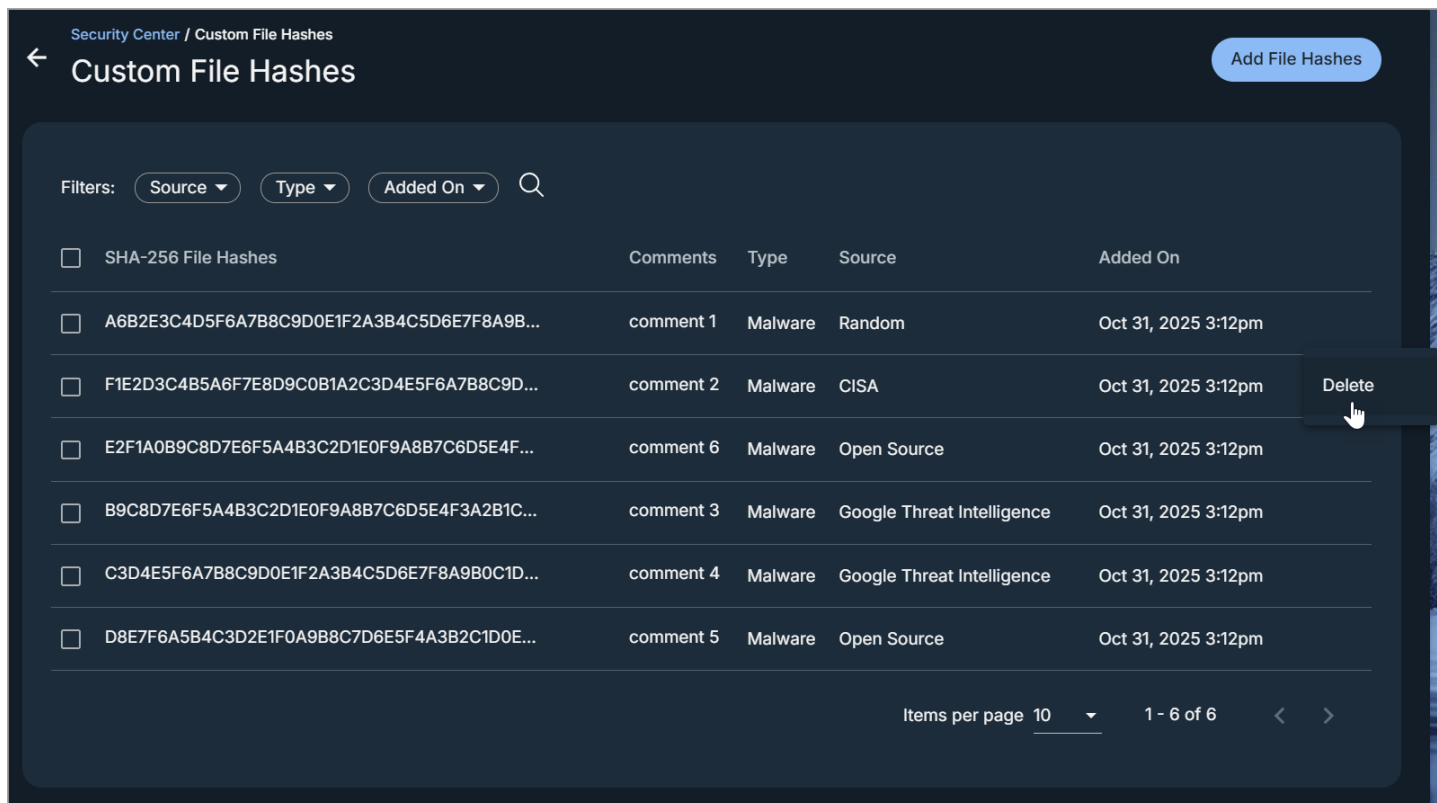
To delete file hashes:

1. Navigate to Threat Detection > Threat Library and select the Hash Feeds tab.

2. Under Custom Hash Feeds tile, click Manage.



3. On the Custom File Hashes page, select the action menu next to the file hash and click Delete.

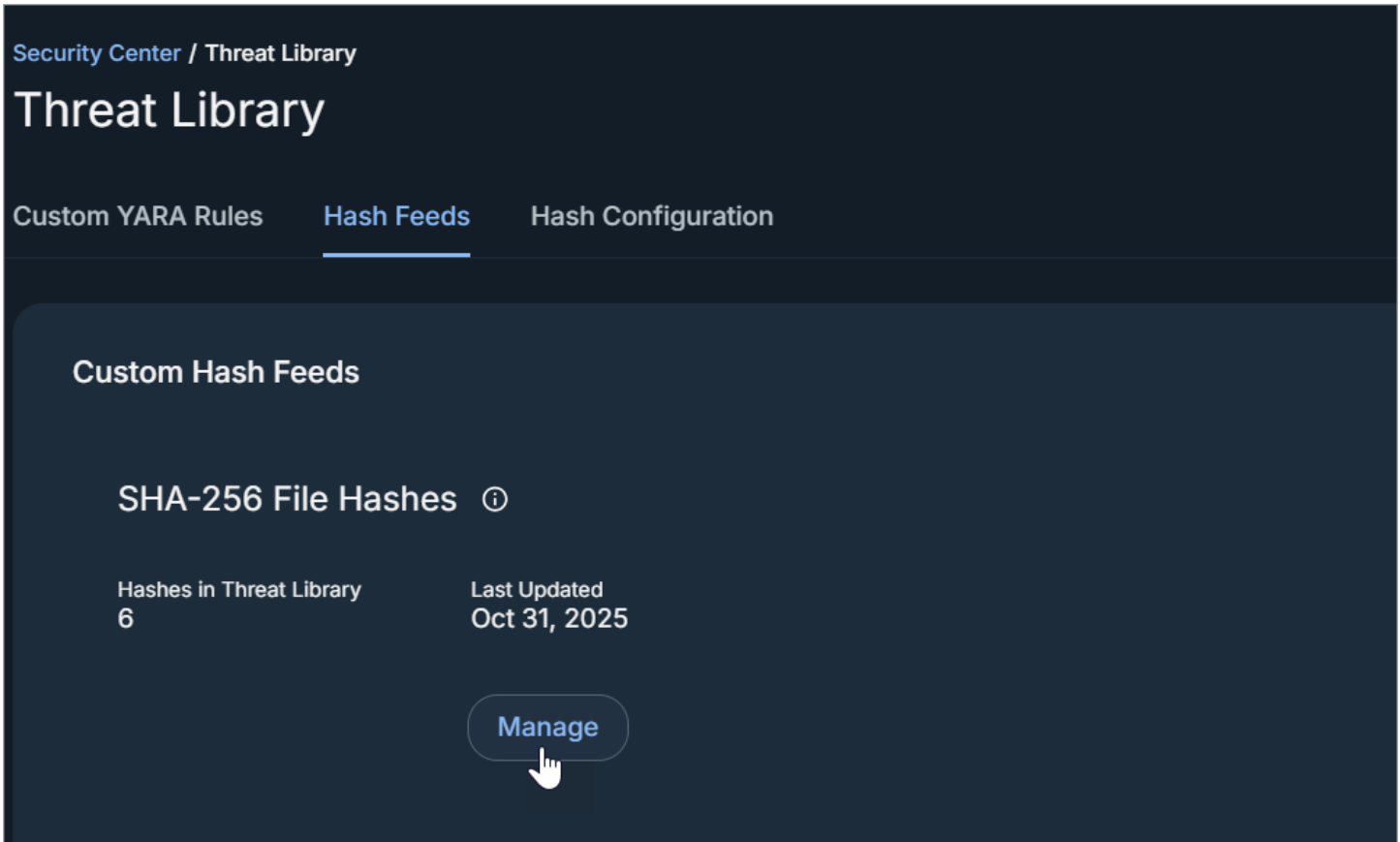


Bulk Delete File Hashes

The bulk delete functionality allows you to remove multiple custom hashes at once. This helps maintain a clean and optimized hash library by removing outdated or unnecessary entries.

1. To delete multiple or all file hashes:
Navigate to Threat Detection > Threat Library and select the Hash Feeds tab.

2. Under Custom Hash Feeds tile, click Manage.



3. On the Custom File Hashes page,
 - a. Deleting multiple file hashes: Select the checkboxes next to the file hashes you want to delete, and then click Delete.

The screenshot shows the 'Custom File Hashes' page in the Security Center. At the top, there's a breadcrumb 'Security Center / Custom File Hashes' and a back arrow. A blue button 'Add File Hashes' is in the top right. Below the header, there are filters: 'Source', 'Type', and 'Added On', along with a search icon. A selection bar shows 'Delete' (highlighted with a red box), 'Delete All Hashes', 'Total 3 Hashes selected', and a link 'Select all 10 Hashes displayed on this page'. The main table lists 6 file hashes, each with a checkbox, a truncated hash, a comment, a category, a source, and a timestamp. The first three rows have their checkboxes checked. The bottom right shows 'Items per page 10' and '1 - 6 of 6'.

Checkbox	File Hash	Comment	Category	Source	Timestamp
<input checked="" type="checkbox"/>	A6B2E3C4D5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B...	comment 1	Malware	Random	Oct 31, 2025 3:12pm
<input checked="" type="checkbox"/>	F1E2D3C4B5A6F7E8D9C0B1A2C3D4E5F6A7B8C9D...	comment 2	Malware	CISA	Oct 31, 2025 3:12pm
<input checked="" type="checkbox"/>	E2F1A0B9C8D7E6F5A4B3C2D1E0F9A8B7C6D5E4F...	comment 6	Malware	Open Source	Oct 31, 2025 3:12pm
<input type="checkbox"/>	B9C8D7E6F5A4B3C2D1E0F9A8B7C6D5E4F3A2B1C...	comment 3	Malware	Google Threat Intelligence	Oct 31, 2025 3:12pm
<input type="checkbox"/>	C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B0C1D...	comment 4	Malware	Google Threat Intelligence	Oct 31, 2025 3:12pm
<input type="checkbox"/>	D8E7F6A5B4C3D2E1F0A9B8C7D6E5F4A3B2C1D0E...	comment 5	Malware	Open Source	Oct 31, 2025 3:12pm

- b. Deleting all file hashes: To delete all hashes at once, either select the checkboxes for each hash or use the Select all <n> hashes displayed on this page option, and then click Delete All Hashes.

The screenshot shows the 'Custom File Hashes' page in the Security Center. At the top, there's a breadcrumb 'Security Center / Custom File Hashes' and a back arrow. A blue button 'Add File Hashes' is in the top right. Below the header, there are filters for 'Source', 'Type', and 'Added On', along with a search icon. A table of file hashes is displayed with columns for selection, hash ID, comment, type, source, and date. Three hashes are selected, and a red box highlights the 'Delete All Hashes' button. Another red box highlights the 'Select all 10 Hashes displayed on this page' link. The bottom of the page shows 'Items per page 10' and '1 - 6 of 6'.

	Hash ID	Comment	Type	Source	Date
<input checked="" type="checkbox"/>	A6B2E3C4D5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B...	comment 1	Malware	Random	Oct 31, 2025 3:12pm
<input checked="" type="checkbox"/>	F1E2D3C4B5A6F7E8D9C0B1A2C3D4E5F6A7B8C9D...	comment 2	Malware	CISA	Oct 31, 2025 3:12pm
<input checked="" type="checkbox"/>	E2F1A0B9C8D7E6F5A4B3C2D1E0F9A8B7C6D5E4F...	comment 6	Malware	Open Source	Oct 31, 2025 3:12pm
<input type="checkbox"/>	B9C8D7E6F5A4B3C2D1E0F9A8B7C6D5E4F3A2B1C...	comment 3	Malware	Google Threat Intelligence	Oct 31, 2025 3:12pm
<input type="checkbox"/>	C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B0C1D...	comment 4	Malware	Google Threat Intelligence	Oct 31, 2025 3:12pm
<input type="checkbox"/>	D8E7F6A5B4C3D2E1F0A9B8C7D6E5F4A3B2C1D0E...	comment 5	Malware	Open Source	Oct 31, 2025 3:12pm

4. Confirm the deletion by typing Yes in the confirmation field, and then click **Delete**.

For more information around support for Custom Hash Feeds in DataProtect, refer to the [Cohesity Documentation](#).

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 patterns for each ransomware family
- <https://decoded.avast.io/> - Latest threat research, ransomware analysis and IOC's