COHESITY REDLab

NEWSLETTER | JANUARY 2026

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 REDLab Advisories - https://www.cohesity.com/trust/redlab/advisories/

Critical Threat Updates – January 2026

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.

Cohesity Trust Center: Learn more about Cohesity REDLab

Threat Focus for January: Luxshare Ransomware Attack (RansomHub) and Osiris Ransomware (POORTRY Driver - BYOVD Attack)

A significant ransomware incident targeted Luxshare, a key manufacturing partner for global technology leaders including **Apple, Nvidia and Tesla**. The ransomware group RansomHub claimed responsibility for the attack, which initially occurred in mid-December 2025 and continued to escalate with public data leaks throughout January 2026.

- **Attack Vector:** Threat actors gained unauthorized access to Luxshare's internal engineering and manufacturing data repositories. While the precise entry method has not been publicly disclosed, security analysts attribute the compromise to a combination of credential abuse and exploitation of exposed systems within the engineering environment.

- **Methodology:** After gaining persistent access, the attackers exfiltrated a large volume of sensitive intellectual property, including 3D CAD models, circuit board schematics, manufacturing documents and engineering PDFs spanning several years.

- **Impact:** Leakage of proprietary Apple and Tesla component designs could enable counterfeiting, competitive replication and long-term erosion of trade-secret protections.

- **The Kill Chain:** Following initial compromise, threat actors harvested and staged internal engineering files before exfiltrating them to external infrastructure. They then encrypted local systems and issued extortion demands. Over the following weeks, the group began selectively publishing Luxshare's proprietary design documents on leak sites as pressure escalated.

A newly identified ransomware strain, Osiris was used in attacks against a major Southeast Asian food service franchise in late 2025. Researchers confirm Osiris is a distinct family with no relation to the older 2016 Locky-derived variant. The operation demonstrates a highly engineered evasion capability centered around kernel-level driver abuse.

- **Attack Vector:** Initial access involved the use of dual-use administration tools and a modified RustDesk remote-access binary disguised as “WinZip Remote Desktop”, enabling persistent connection and network reconnaissance prior to payload deployment.

- **Methodology:** The attackers leveraged a Bring-Your-Own-Vulnerable-Driver (BYOVD) technique using a malicious custom driver named POORTRY. Unlike typical BYOVD attacks that abuse legitimate outdated drivers, POORTRY is purpose-built to grant kernel privileges and kill EDR/AV processes.

- **Impact:** Enables rapid privilege escalation and full EDR bypass, allowing operators to perform pre-encryption data theft, credential harvesting and remote command execution.

- **The Kill Chain:** The attack progresses through reconnaissance using modified remote-access tooling, deployment of the POORTRY driver to dismantle endpoint defenses, staged data exfiltration to cloud storage and final execution of the Osiris encryptor with targeted process termination and per-file encryption.

REDLab recommendations:

- **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.
- Schedule regular threat scans using updated threat libraries

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

Name	Ransomware family	Behavioral pattern
BackLock	BackLock ransomware family	Command and Scripting Interpreter, Windows Management Instrumentation, Process Injection, Obfuscated Files or Information, Masquerading, Modify Registry, Boot or Logon Autostart Execution, Hijack Execution Flow, Access Token Manipulation, OS Credential Dumping, File and Directory Discovery
Deep	Phobos ransomware family	Scheduled Task/Job, Command and Scripting Interpreter, Hidden Files and Directories, Boot or Logon Autostart Execution, Access Token Manipulation, Obfuscated Files or Information, Masquerading, Indicator Removal, Disabling Security Tools, File and Directory Permissions Modification
WarLock	WarLock Group	Obfuscated Files or Information, Masquerading, Software Packing, NTFS File Attribute Abuse, Impair Defenses, Credential Dumping, Unsecured Credentials, System Service Discovery, Network Share Discovery, File and Directory Discovery, Peripheral Device Discovery, Data Encrypted for Impact, Service Stop
LeakDB	LeakDB Variant	Boot or Logon Autostart Execution, Access Token Manipulation, Obfuscated Files or Information, Masquerading, Indicator Removal, File and Directory Permissions Modification, Virtualization/Sandbox Evasion, Impair Defenses, Credential Dumping, File and Directory Discovery, Network Share Discovery, Application Layer Protocol, Inhibit System Recovery

REDLab findings:

- **BackLock (attack on NetBackup and Data Protect client):**
    - **Family**: BackLock ransomware family | **Behavior pattern**: Command and Scripting Interpreter, Windows Management Instrumentation, Process Injection, Obfuscated Files or Information, Masquerading, Modify Registry, Boot or Logon Autostart Execution, Hijack Execution Flow, Access Token Manipulation, OS Credential Dumping, File and Directory Discovery.
    - **Know Me**: BackLock encrypts user and system data, renaming each file with a unique victim ID and ".backlock" extension. It drops README.TXT as its ransom note and actively kills processes holding open database, document and productivity files to maximize encryption coverage. BackLock is commonly delivered through phishing, drive-by downloads and RDP brute-force attacks. It has also been observed in campaigns abusing vulnerabilities in MOVEit Transfer and Citrix NetScaler environments.
    - **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.

- **Deep (attack on NetBackup and Data Protect client):**
    - **Family**: Phobos ransomware family | **Behavior pattern**: Scheduled Task/Job, Command and Scripting Interpreter, Hidden Files and Directories, Boot or Logon Autostart Execution, Access Token Manipulation, Obfuscated Files or Information, Masquerading, Indicator Removal, Disabling Security Tools, File and Directory Permissions Modification.
    - **Know Me**: Deep (Phobos) appends a victim ID and attacker email to filenames followed by the ".deep" extension. It drops info.hta and info.txt as ransom notes. This strain is known for terminating database, Office and mail client processes to unlock files for encryption. It is typically deployed via RDP intrusion, SmokeLoader-based loaders, phishing attachments and brute-force credential attacks.
    - **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:

- **WarLock (attack on NetBackup and Data Protect client):**
    - **Family**: WarLock Group | **Behavior pattern**: Obfuscated Files or Information, Masquerading, Software Packing, NTFS File Attribute Abuse, Impair Defenses, Credential Dumping, Unsecured Credentials, System Service Discovery, Network Share Discovery, File and Directory Discovery, Peripheral Device Discovery, Data Encrypted for Impact, Service Stop.
    - **Know Me**: WarLock is a modern double-extortion ransomware used by the group tracked as GOLD SALEM / Storm-2603. It commonly exploits Microsoft SharePoint zero-day vulnerabilities (ToolShell chain: CVE-2025-49704, -49706, -53770/71) to gain initial access. Attackers deploy ASPX web shells (spinstall0.aspx), extract ASP.NET MachineKeys, harvest credentials via Mimikatz and move laterally using PsExec and WMI. The payload encrypts files with ".x2anylock" and drops How to decrypt my data.txt.
    - **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.

- **LeakDB (attack on NetBackup and Data Protect client):**
    - **Family**: LeakDB Variant | **Behaviour pattern**: Boot or Logon Autostart Execution, Access Token Manipulation, Obfuscated Files or Information, Masquerading, Indicator Removal, File and Directory Permissions Modification, Virtualization/Sandbox Evasion, Impair Defenses, Credential Dumping, File and Directory Discovery, Network Share Discovery, Application Layer Protocol, Inhibit System Recovery.
    - **Know Me**: LeakDB is an enterprise-targeted Phobos variant that appends victim ID + attacker email + ".LEAKDB". It terminates processes using open database, document and mail files to accelerate encryption. It drops info.hta and info.txt in all affected directories. LeakDB also deletes Volume Shadow Copies to prevent local recovery and maintains persistence via %LOCALAPPDATA% copies and registry Run keys.
    - **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 BackLock, Deep, WarLock and LeakDB ransomware strains, 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.

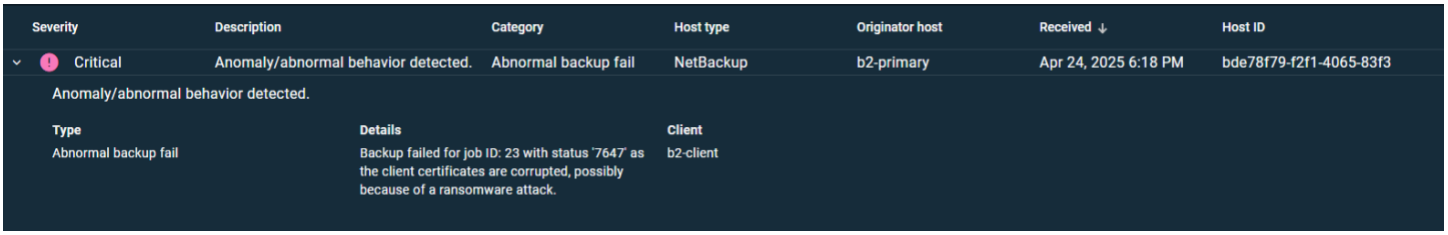
- For all the ransomware strains described earlier, in the case of the Data Protect, Client backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully, demonstrating the platform's resilience and ability to maintain data protection under adverse conditions.

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:



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

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

Data Classification

To improve detection and cover more potential cyber threats, Data Classification is a powerful capability designed to help you discover, categorise and protect sensitive information across your environment.

What is Data Classification?

Data Classification automatically scans your backup and production data, identifying sensitive information such as personal, financial, or health records. Using a library of over 300 built-in patterns and support for custom rules, it enables you to map your data landscape and understand where your most critical assets reside. The feature leverages AI/ML-powered engines for high accuracy and can be triggered on-demand, scheduled, or automatically in response to anomaly alerts.

Classification Methods

Data Classification uses the following classification methods to scan data and discover significant and sensitive information in the data pool:

- **Regex**

  Regular Expressions (regex) detect and classify data by recognizing the syntax pattern of the data's characters. For example, a data string of the form abcxyz@example.com would be recognized and classified as an email address. Cohesity provides out-of-the-box regex patterns you can use or create custom patterns with your own regexes.

- **NER**

  Named Entity Recognition (NER) is an advanced neural network-based technique that analyzes entities in unstructured data sources, identifying hidden personal data and categorizing content type.

Classification Scans

You can perform on-demand or schedule classification scans to classify objects besides the compromised objects alerted by Cohesity Ransomware Detection. You can manually run classification on objects snapshot to scan data and discover significant and sensitive information in the objects snapshot.

From the **Security Center**, you can:

- Start a classification scan on the object snapshots.
- Analyze the number of objects scanned on the object snapshots as part of the classification scan.
- View the files in the object that matched the patterns.
- Download the sensitivity report.

Classification Scan Methods

Data Classification provides the following classification scan methods to perform classification scans to classify objects besides the compromised objects alerted by Cohesity Ransomware Detection:

- Full Scan
- Incremental Scan

Full Scan - Full Scan enables you to classification scans on objects snapshot data and discover significant and sensitive information in the objects snapshot.

Incremental Scan - Incremental Scan enables you to scan only modified or newly added files between object snapshots, improving efficiency while still allowing you to identify significant and sensitive information in the data.

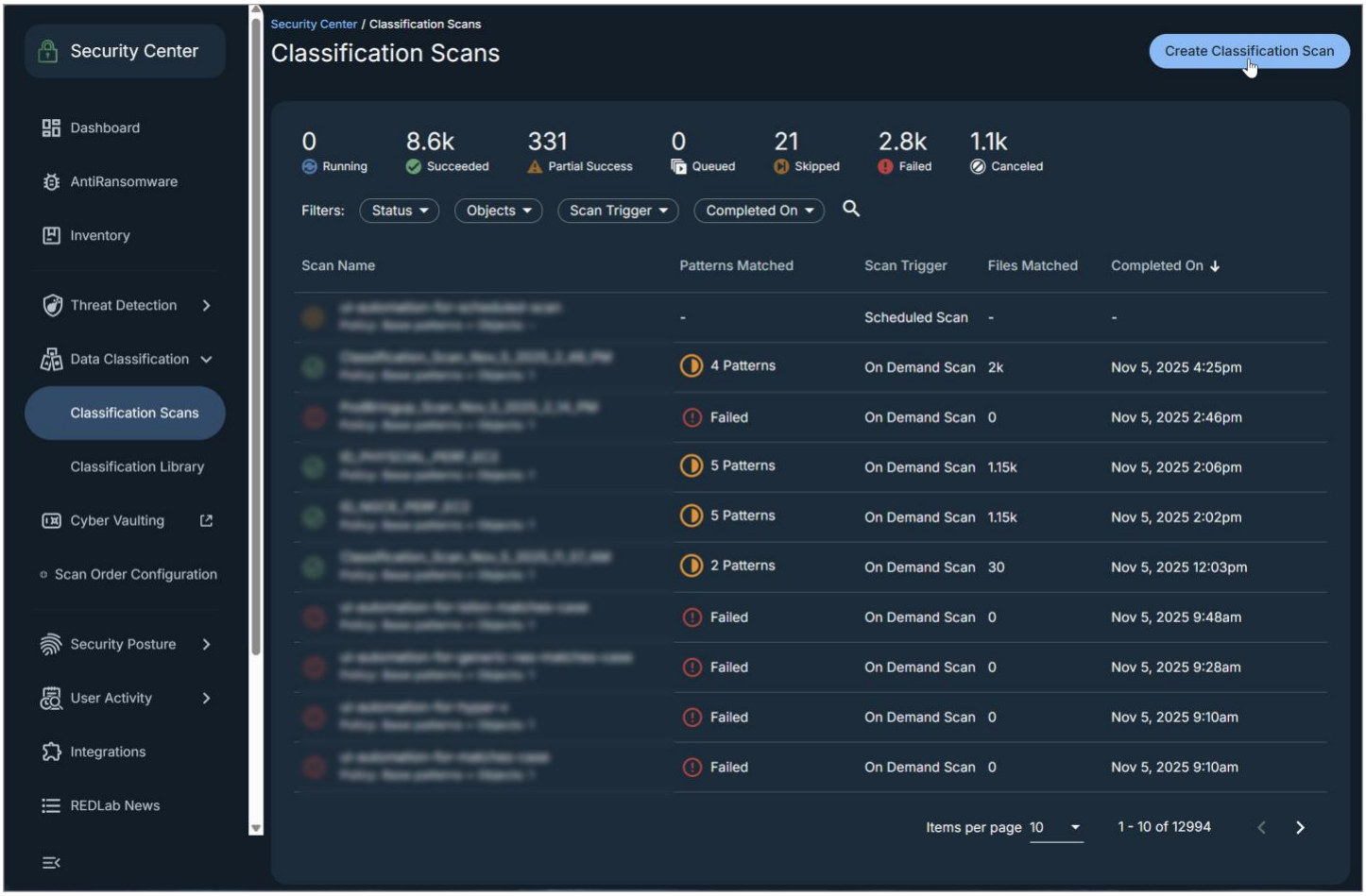
- **On-demand scans** – The most recent snapshot (*n*) and the previous snapshot (*n-1*) in the same protection group are compared to compute file differences , and the scan is performed only on the changed data.
- **Scheduled scans** – The first scheduled scan is a full scan. Subsequent scans process only the changes in object snapshots. If the base snapshot is deleted or has expired, a full scan is performed on the next most recent snapshot.

Start a Classification Scan

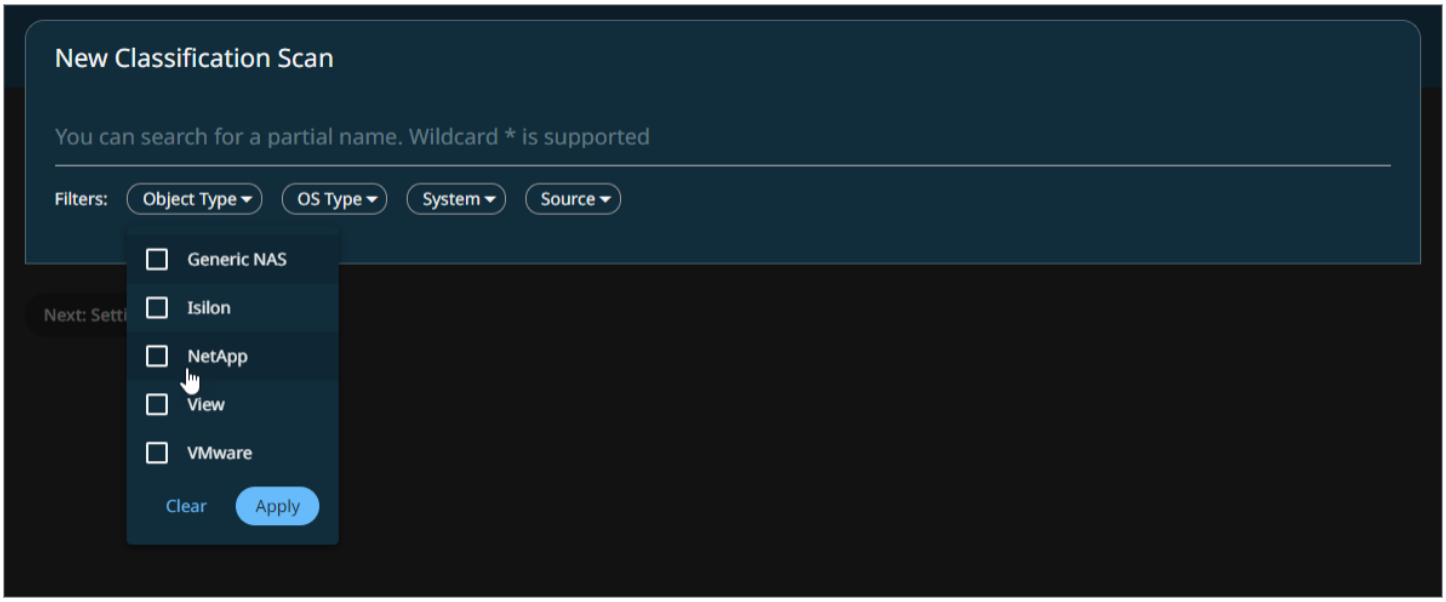
From the **Security Center**, you can start an on-demand classification scan on one or multiple objects snapshot on the Cohesity clusters managed on Helios.

To start a classification scan:

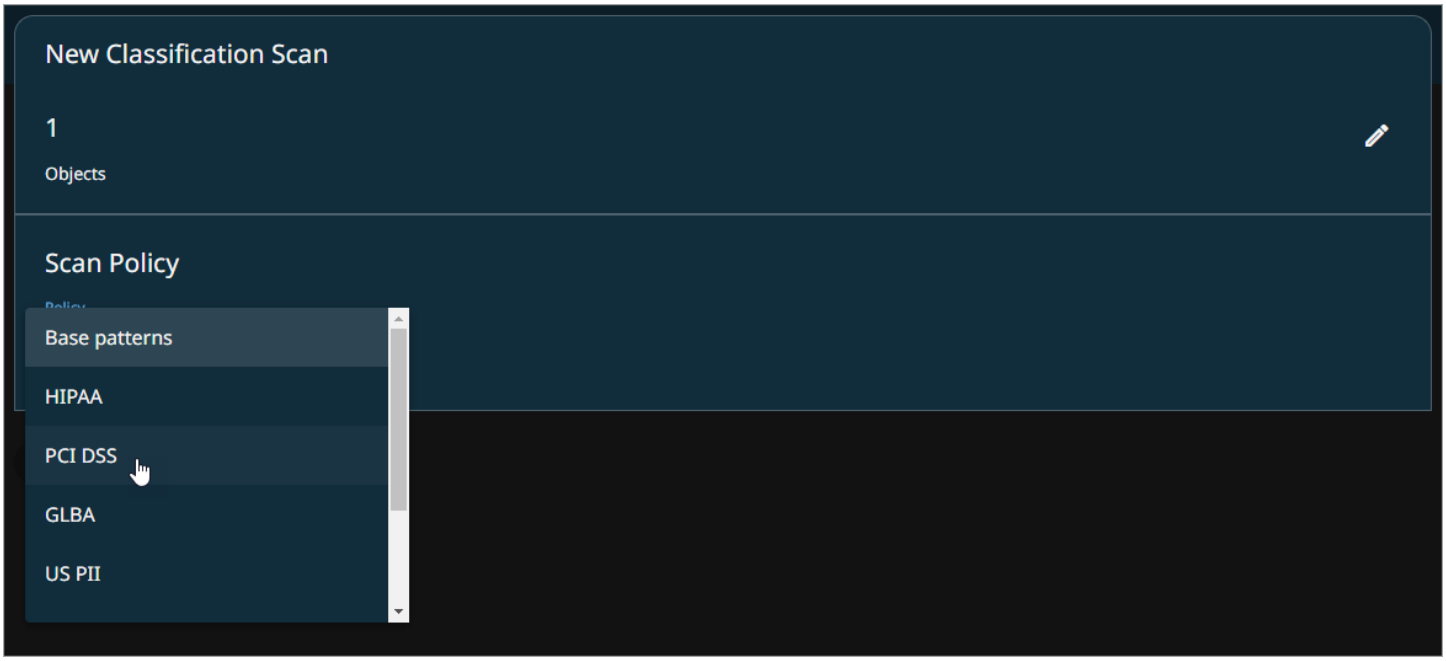
1. Navigate to **Data Classification** > **Classification Scans**.
2. On the **Classification Scans** page, click **Create Classification Scan**.



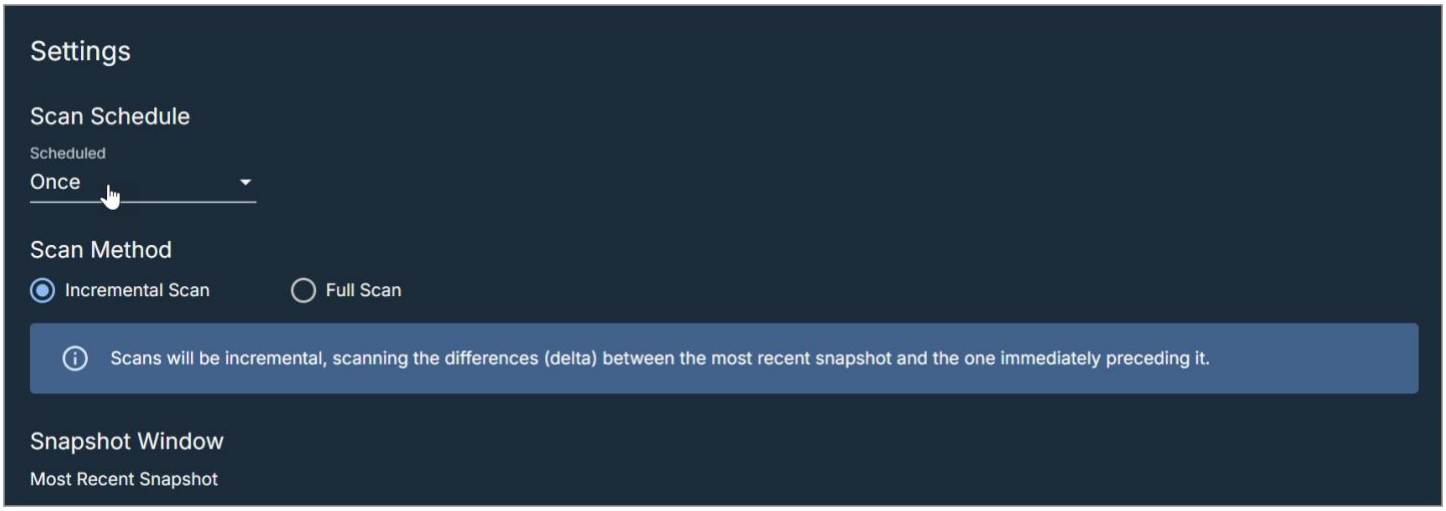
3. Use the search to find and select the object(s) you want to scan for classification. Also, you can use the following filters to narrow down your search and click **Next: Settings**:



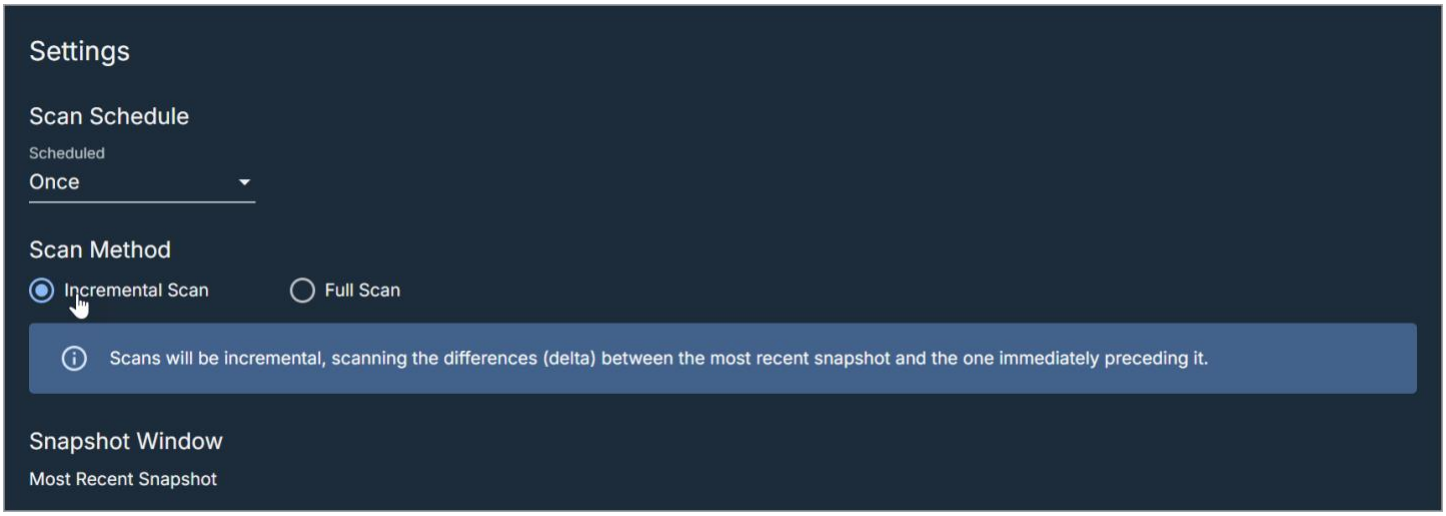
4. In the **Scan Policy** section, select the data classification policy from the **Policy** drop-down.



5. In the **Settings** section, perform the following:
    a. Under **Scan Schedule**, from the **Scheduled** drop-down, select **Once** to perform a classification scan immediately.



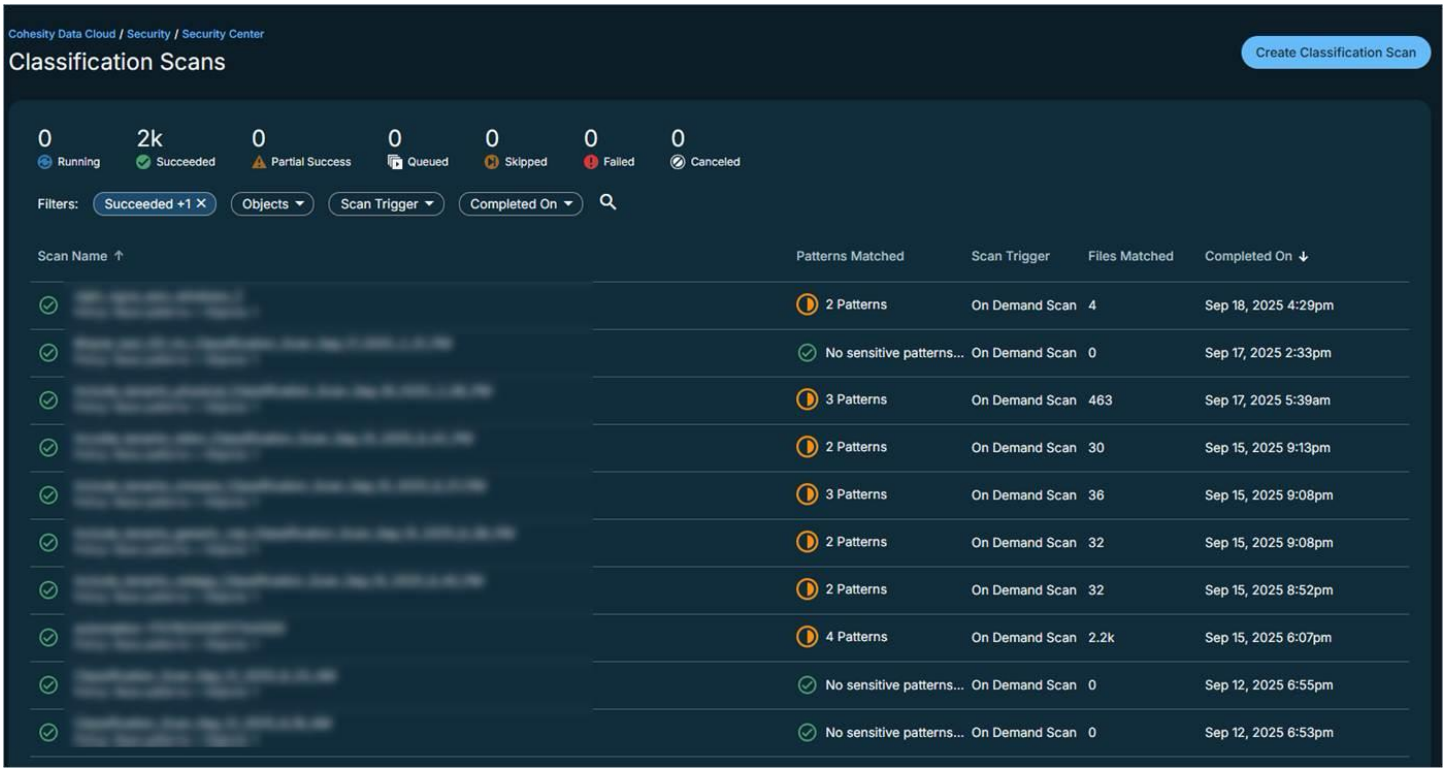
    b. Under **Scan Method**, choose one of the following options:
        - **Incremental Scan** – Runs an Incremental Scan. The most recent two snapshots are compared to compute file differences, and only the changed data is scanned.
        - **Full Scan** – Runs a Full Scan for every classification scan.



6. Under **More Options**, review all the settings and edit them based on your preference.
7. Click **Create Scan**.

View Classification Scan Details

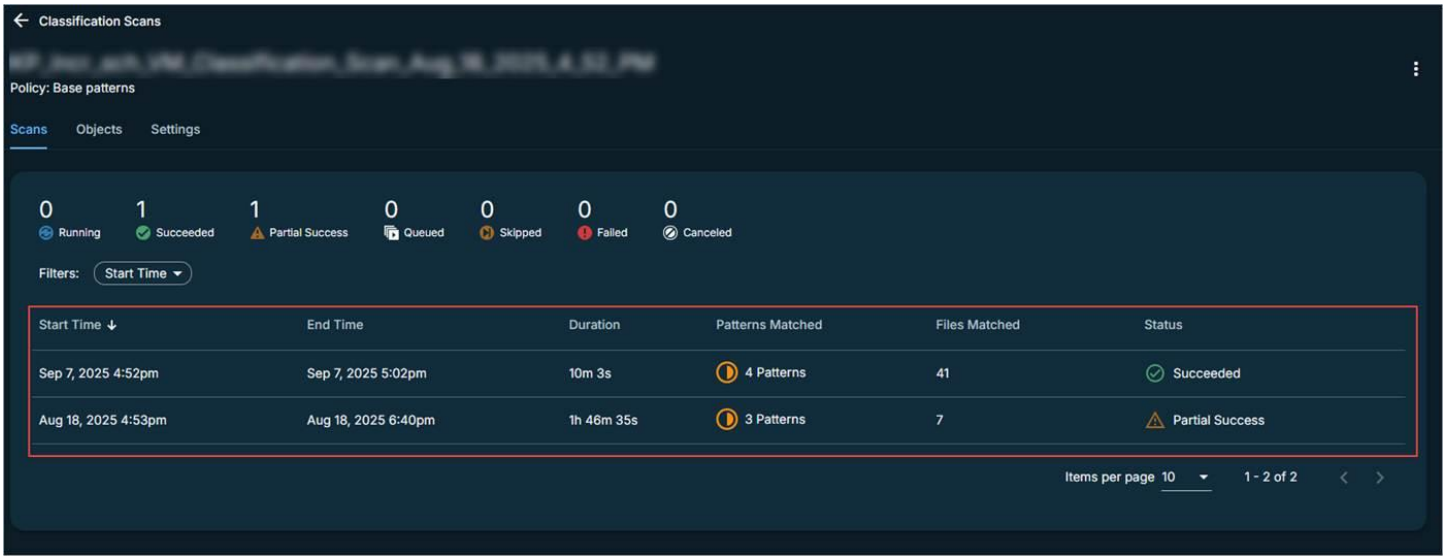
From the **Classification Scan** page, you can view the details of a classification scan. To view the details of a classification scan, navigate to **Data Classification** > **Classification Scans** and click on the classification scan on the **Classification Scan** page.



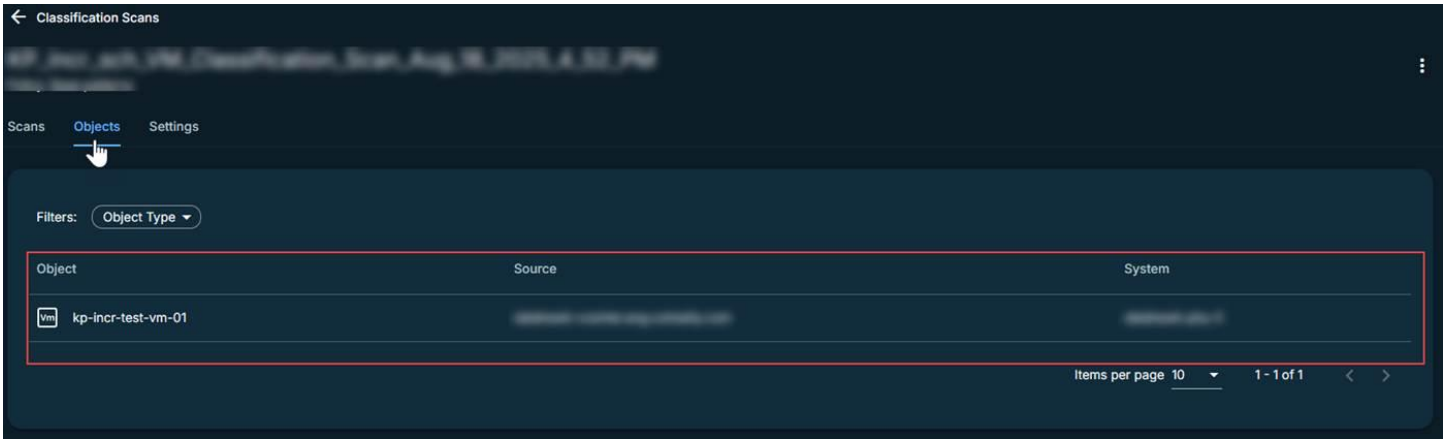
On the **Classification Scans** page, click a **Scan Name** to view the details of the corresponding classification scan.

The **Scan Name** page displays information about the classification scan runs associated with that scan. The page includes the following tabs:

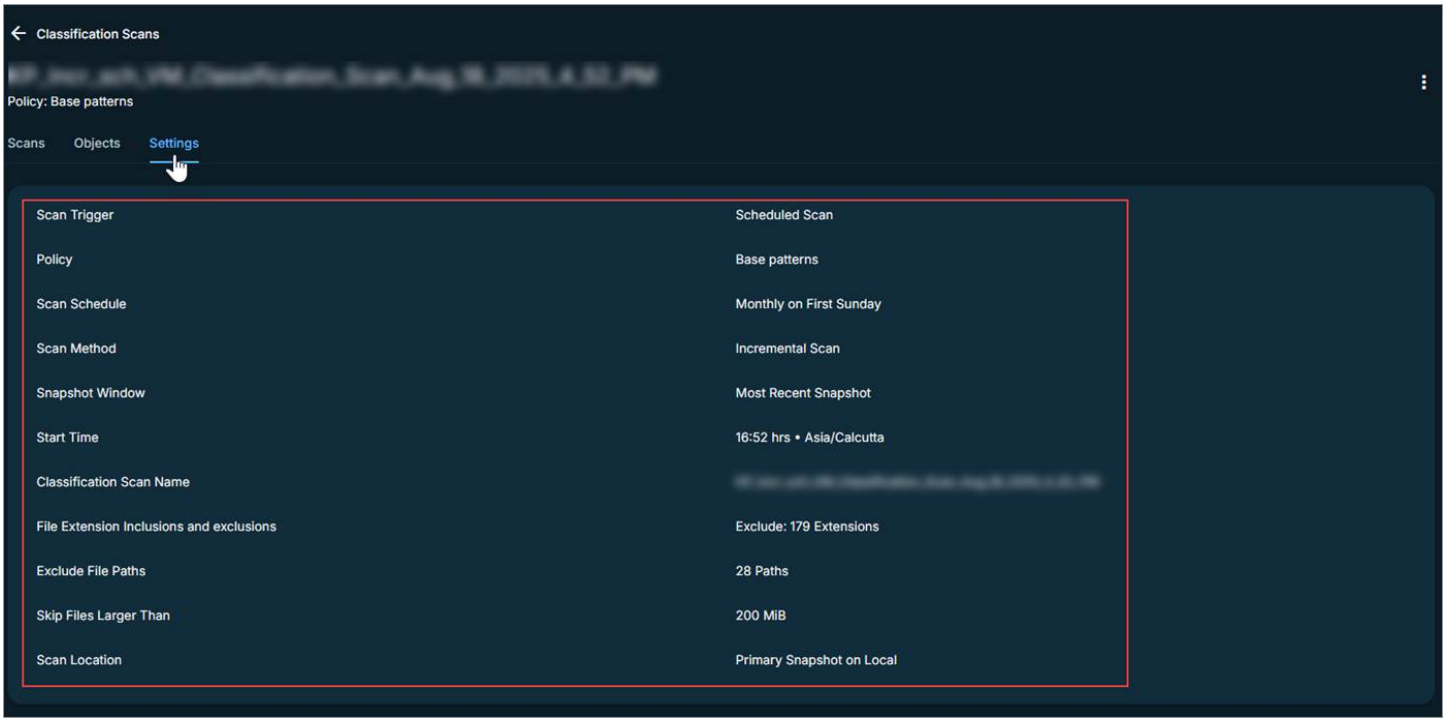
- **Scans**



- **Objects**



- **Settings**



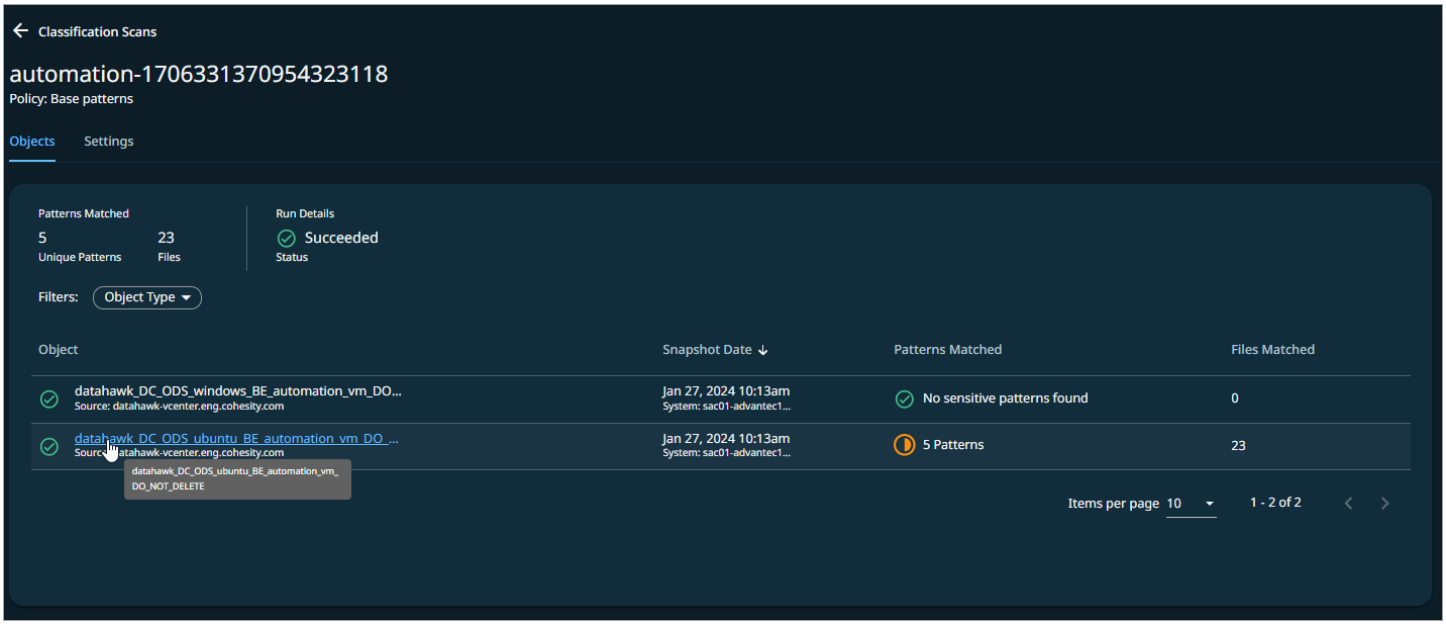
View the Classification Run Details of an Object

After the classification scan is in progress or completed on the snapshot, you can view the details of the classification scan performed on a object snapshot. You can view the following details:

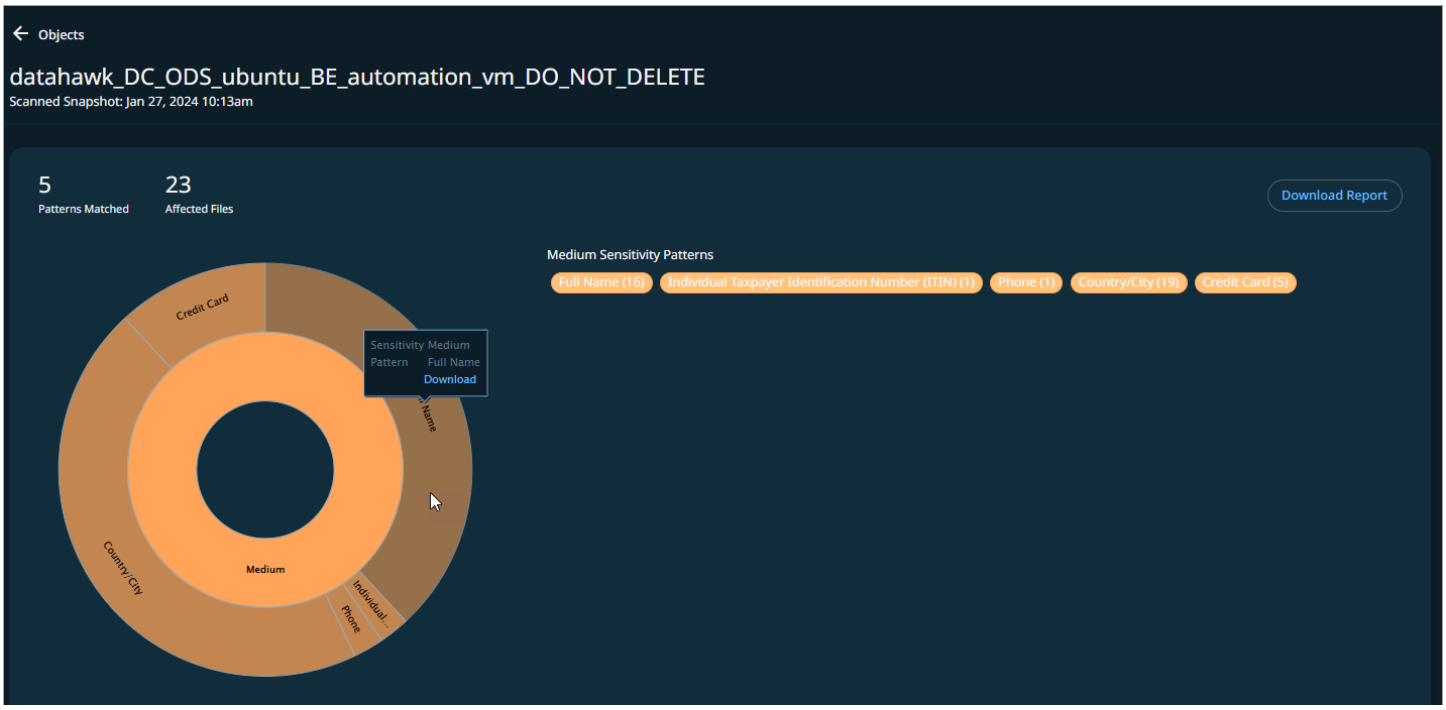
- The number of unique patterns matched from the in-built patterns or your custom patterns applied on the snapshots.
- Number of files with the matched patterns.
- The files in the object matched the pattern.
- The sensitivity of the patterns in the files.

To view details of the patterns and files, navigate to **Data Classification** > **Classification Scans** and click on the completed classification scan on the **Classification Scan** page.

From the <SCAN_NAME> page, click on the object that has completed the scan.



On the <Object> page, hover over the chart for sensitivity and matched pattern details. Also, you can click on the shown sensitivity patterns to view the files with the patterns.



Download the Sensitivity Report of the Object

You can download a sensitivity report that details the sensitivity pattern classified on the object.

To download the report:

1. Navigate to **Data Classification** > **Classification Scans**.
2. Click on the completed classification scan on the **Classification Scan** page.
3. From the ***<SCAN_NAME>*** page, click on the object that has completed the scan.
4. Click **Download Report**.

A report in CSV format is downloaded to your browser which contains the following details:

Parameter	Description
file-path	Path of the file containing the matched patterns.
matches	The matched patterns
sensitivity	The sensitivity of the matched patterns.

Call to Action

Enable Data Classification today to gain visibility into your most sensitive assets, reduce your risk footprint, and demonstrate compliance with confidence. For more information, consult the Cohesity Data Classification 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 pattens for each ransomware family
- https://decoded.avast.io/ - Latest threat research, ransomware analysis and IOC’s