

This document explains the procedure of how to use the security tools and their implementations in real time. All the commands concepts etc., are implemented by me in real time and got certifications on that.

Please do check my LinkedIn profile: <https://www.linkedin.com/in/vinay-reddy-donda-36b10a20b/>

- This document will cover the different topics of Symantec DLP.
- Identifying and describing the confidential data.
- Create policy groups:
- Configure a policy for PII Detection, PCI compliance.
- Configure a policy to protect the confidential document, protect the source code, form recognition:
- Export policies for use at the Disaster Recovery Site
- Configure the optical character recognition.
- Locating the confidential data stored on the premises and on the cloud.
- Scan endpoint computers for confidential data.
- Scan server for confidential data using EMDI
- Configure a global policy for PII Compliance.
- Understanding how confidential data is being used.
- Use network prevent for email to monitor SMTP Messages.
- Monitor endpoint activity- Email, Monitor Endpoint activity – Third party apps
- Monitor end point activity copy/paste, Educating users to Adopt data Protection practices.
- Configure Email Notifications., Configure the on screen notifications.
- Preventing unauthorized exposure of confidential data.
- Testing Optical character recognition(OCR) and “HIPAA and HITECH (including PHI)” Policy.
- Configure Endpoint blocking, Scan and quarantine files on a server file share target.
- Scan and Quarantine files on a endpoint target.
- Remediating the data loss incidents and tracking risk reduction:

- User reports to track risk Exposure and Reduction.

- Define Incident statuses and incident groups.
- Configure and Use smart responses, Schedule and send reports.
- Enhancing data loss preventions with Integrations.

Lab 1:

Identifying and describing the confidential data.

Exercise 1:

Tour of enforce console.

The screenshot shows the Symantec Data Loss Prevention enforcement console. The title bar reads "Symantec Data Loss Prevention". The address bar shows the URL "https://enforce.symplyfied.com/ProtectManager/enforce/ui/dashboard/endpoint". The navigation menu at the top includes "Home", "Incidents" (which is selected), "Manage", and "System". Below the menu, the breadcrumb navigation shows "Incidents > Endpoint > Exec. Summary - Endpoint". The main content area has a header "Endpoint". It contains two sections: "Policy Summary" and "Top 5 Highest Offenders", both of which display the message "No data available".

Home tab this contains few built-in reports and dashboards.

The screenshot shows the "All Reports" page of the Symantec Data Loss Prevention enforcement console. The title bar reads "Symantec Data Loss Prevention". The address bar shows the URL "https://enforce.symplyfied.com/ProtectManager/ViewAllReports.do". The navigation menu at the top includes "Home", "Incidents" (which is selected), "Manage", and "System". Below the menu, the breadcrumb navigation shows "Incidents > All Reports". There are buttons for "Create Dashboard" and "Edit Preferences". The main content area displays two tables: "Saved Reports - Administrator" and "Network".

Name	Product	Sharing	Description	Schedule
<no reports in this section>				

Name	Product	Description
Exec. Summary - Network	Dashboard	Dashboard overview of Network incidents by Policy, Sender, Protocol, Domain, Status, Lists all Network incidents for the current week, sorted by date.
Incidents - Week, Current	Network	Lists all Network incidents, sorted by date.
Incidents - All	Network	Lists all Network incidents with a status of "New", sorted by date.
Incidents - New	Network	Lists all Network incidents grouped by Policy.
Policy Summary	Network	Lists all Network incidents grouped by Policy, then by Month.
Policy Trend	Network	Lists all Network incidents grouped by Week, then by Status.
Status by Week	Network	Lists all Network incidents grouped by Policy, then by Status.
Status by Policy	Network	Lists all Network incidents grouped by Protocol.
Protocol Summary	Network	Lists all Network incidents grouped by Protocol, then by Month.
Protocol Trend	Network	Lists Network incidents in the OPEN status group by Week, then by Policy; lists oldest.
Aging Unres. Incidents	Network	Lists the top senders over the last 30 days, by descending incident count.
High Risk Senders - Last 30 Days	Network	Lists the top senders by descending high severity incident count.
High Risk Senders - High Severity	Network	Lists the top recipient domains over the last 30 days, by descending incident count.
Top Recipient Domains	Network	

Incident tab this displays the list of reports and incident list for each vector.

The screenshot shows the Symantec Data Loss Prevention interface. At the top, it says "Run time remaining: 1 h : 41 m : 25 s" and "URL expires: Mar. 9, 2021, 1:44 PM - UTC". The title bar is "Symantec Data Loss Prevention". The address bar shows the URL: https://enforce.simplified.com/ProtectManager/enforce/admin/policy/list. The main menu includes File, Edit, View, History, Tools, Help, and various system icons. Below the menu, there's a toolbar with actions like New, Import, Export, Download Details, Activate, Suspend, Delete, Clone, and Assign Group. The navigation bar shows "Manage > Policies > Policy List". A message "No entries available" is displayed above a table header. The table columns are Status, Name, Description, Policy Group, and Last Modified. A note "No data available" is shown below the table.

Manage tab this is where we add the policies and also says about data profiles and discover scanning.

The screenshot shows the Symantec Data Loss Prevention interface on the System tab. The title bar is "Symantec Data Loss Prevention". The address bar shows the URL: https://enforce.simplified.com/ProtectManager/SystemOverview.do. The main menu includes Home, Incidents, Manage, and System. Below the menu, there's a navigation bar: System > Servers and Detectors > Overview. A button "Add Server..." is visible. The main content area has three sections: "Servers and Detectors", "Recent Error and Warning Events", and "License".

Servers and Detectors

Status	Name	Version	Type	Form Factor	Messages (Last 10 sec)	Messages (Today)
Running	Enforce Server	15.5.0.17018	N/A	Software	N/A	N/A
Running	Simplified Detection Server	15.5.0.17018	Network Monitor, Network Prevent for Email, Network Prevent for Web, Endpoint, Network Discover/Cloud Storage Discover	Software	0	0

Recent Error and Warning Events [show all >]

Type	Time	Name	Host	Code
⚠	February 23, 2021 3:11:38 PM PST	Simplified Detection Server	127.0.0.1	1202
✗	February 23, 2021 3:11:21 PM PST	Simplified Detection Server	127.0.0.1	1008
✗	February 23, 2021 3:11:14 PM PST	Simplified Detection Server	127.0.0.1	1302
⚠	February 23, 2021 3:10:44 PM PST	Simplified Detection Server	127.0.0.1	1014
⚠	February 23, 2021 12:54:31 PM PST	Simplified Detection Server	127.0.0.1	1202

License

Network Monitor, Network Discover, Network Protect, Endpoint Prevent, Endpoint Discover, Network Prevent for Email, Network Prevent for Web

System tab it is where system wide configuration is done and we can view the status of the enforce server, detection servers , endpoint agents and so on. It is also where the user roles, and permissions are configured.

Product	Description
Network	Lists all Network incidents grouped by Policy, then by Month.
Network	Lists all Network incidents grouped by Week, then by Status.
Network	Lists all Network incidents grouped by Policy, then by Status.
Network	Lists all Network incidents grouped by Protocol.
Network	Lists all Network incidents grouped by Protocol, then by Month.
Network	Lists Network incidents in the OPEN status group by Week, then by Policy; lists oldest incidents first.
Network	Lists the top senders over the last 30 days, by descending incident count.
Network	Lists the top senders by descending high severity incident count.
Network	Lists the top recipient domains over the last 30 days, by descending incident count.
Network	Lists all Network incidents grouped by Sender IP.
Dashboard	Dashboard overview of Endpoint incidents by Policy, Windows User, Connection Status, Device Type, Workflow Status, and trend over time.
Endpoint	Lists all Endpoint incidents for the current week, sorted by date.
Endpoint	Lists all Endpoint incidents, sorted by date.
Endpoint	Lists all Endpoint incidents with a status of "New", sorted by date.
Endpoint	Lists Endpoint incidents for removable media grouped by Policy.
Endpoint	Lists Endpoint incidents for removable media grouped by Policy, then by Month.
Endpoint	Lists Endpoint incidents for fixed drive transfers grouped by Policy.
Endpoint	Lists Endpoint incidents for fixed drive transfers grouped by Policy, then by Month.
Endpoint	Lists Endpoint incidents grouped by Policy.
Endpoint	Lists Endpoint incidents for downloads grouped by Month, then by Status
Endpoint	Lists Endpoint incidents for downloads grouped by Policy, then by Status

On the top right corner first symbol indicates the help

Second symbol indicates that whenever we click on that button whatever the console we are using at that time it will become the home screen.

Third symbol indicates going to previous console

Fourth symbol indicates Refresh of the console

Exercise 2:

Create policy groups:

Policy groups allows us to group similar policies and allows us to detect whether which policy should be used for better data security and avoiding sensitive data loss.

Adding Symplified PII Policies group.

Name	Description	Available Servers and Detectors
Classification	Adding Classification group	All Servers and Detectors
Default Policy Group	The default protect policy group	All Servers and Detectors
Symplified PCI Policies	Adding Symplified PCI policies	All Servers and Detectors
Symplified PII Policies	Adding Symplified PII policies group	All Servers and Detectors

Similary I added Symplified PCI policies and classification group Default Ploicy group need not be added it comes by default.

Exercise 3:**Configure a policy for PII Detection:****PII – Personally identifiable information.**

We are creating the policy using the described content matching (DCM) to detect where the PII data is used or stored.

Adding the new policy in the list by clicking new in the console.

Rule Type	Product	Technology
Content		
<input type="radio"/> Content Matches Regular Expression <small>Detect incidents using regular expressions.</small>		(DCM)
<input type="radio"/> Content Matches Exact Data From: No Exact Data Profiles Available <small>Detect incidents from exact data profiles. Select the appropriate exact data profile.</small>		(EDM)
<input type="radio"/> Content Matches Keyword <small>Detect incidents containing keywords or keyphrases.</small>		(DCM)
<input type="radio"/> Content Matches Document Signature From: No Document Profiles Available <small>Match content contained in indexed document profile.</small>		(IDM)
<input checked="" type="radio"/> Content Matches Data Identifier: - US Social Security Number (SSN) <small>Detect incidents by searching for data identifiers.</small>		(DCM)
<input type="radio"/> Detect using Vector Machine Learning profile: No Machine Learning Profiles Available <small>Detects incidents by using Vector Machine Learning profile to classify contents.</small>		(VML)
<input type="radio"/> Content Matches Classification <small>Detect incidents by classification.</small>		(ICT)
File Properties		
<input type="radio"/> Message Attachment or File Type Match <small>Use this rule to find specific types of documents, such as Office or PDF files.</small>		(DCM)
<input type="radio"/> Message Attachment or File Size Match <small>Match attachment or files over or under a certain size.</small>		(DCM)
<input type="radio"/> Message Attachment or File Name Match <small>Match attachment filenames by exact name or by pattern.</small>		(DCM)
Protocol		
<input type="radio"/> Protocol or Endpoint Monitoring <small>Detects incidents on the Network, Endpoint, or Mobile. Based on method of detection or communication.</small>		(DCM)
<input type="radio"/> Endpoint Device Class or ID <small>Detect Endpoint incidents depending on device metadata.</small>		(DCM)
<input type="radio"/> Endpoint Location <small>Detect Endpoint incidents depending on the network location of the endpoint.</small>		(DCM)

Manage > Policies > Policy List > Configure Policy - Edit Rule

OK Cancel

General

Rule Name: **US Social Security Numbers**

Severity

Default: **High** Add Severity

Conditions

Content Matches Data Identifier:

Data Identifier: **US Social Security Number (SSN)**

Personal identification number issued by the Social Security Administration of the United States government. Although primarily used for administering the Social Security program, it is widely used as a personal identification number in many purposes. ([More info](#))

Breadth:

- Wide Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, periods, slashes, or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
- Medium Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes, spaces, or periods. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit.
- Narrow Detects 9 digit numbers with the pattern DDD-DD-DDDD separated with dashes or spaces or without separators. Must be in valid assigned number ranges. Eliminates common test numbers, such as 123456789 or all the same digit. Also requires the presence of a Social Security-related keyword.

Optional Validators: [Optional Validators](#)

Match Count: [Check for existence \(don't count multiple matches\)](#)

The screenshot shows the 'Configure Policy' interface for a policy named 'Simplified PII (DCM)'. The 'General' tab is selected, displaying fields for Name, Description, Policy Label, Policy Group (set to 'Simplified PII Policies'), Status (Active), and Last Modified (2/23/21 4:04 PM by Administrator). The 'Detection' tab is also visible. Under 'Rules:', three categories are listed: 'US Social Security Numbers (Data Identifiers)', 'Mexican Unique Population Registry Code Numbers (Data Identifiers)', and 'Canadian Social Insurance Numbers (Data Identifiers)'. Each category has a severity of 'High' and a note about counting unique matches across envelope, subject, body, and attachments. The 'Exceptions:' section indicates no exceptions are present. A link to 'Create a template from this policy' is at the bottom.

In this we added the rules for DCM which identifies the sensitive data by fingerprinting the unstructured data.

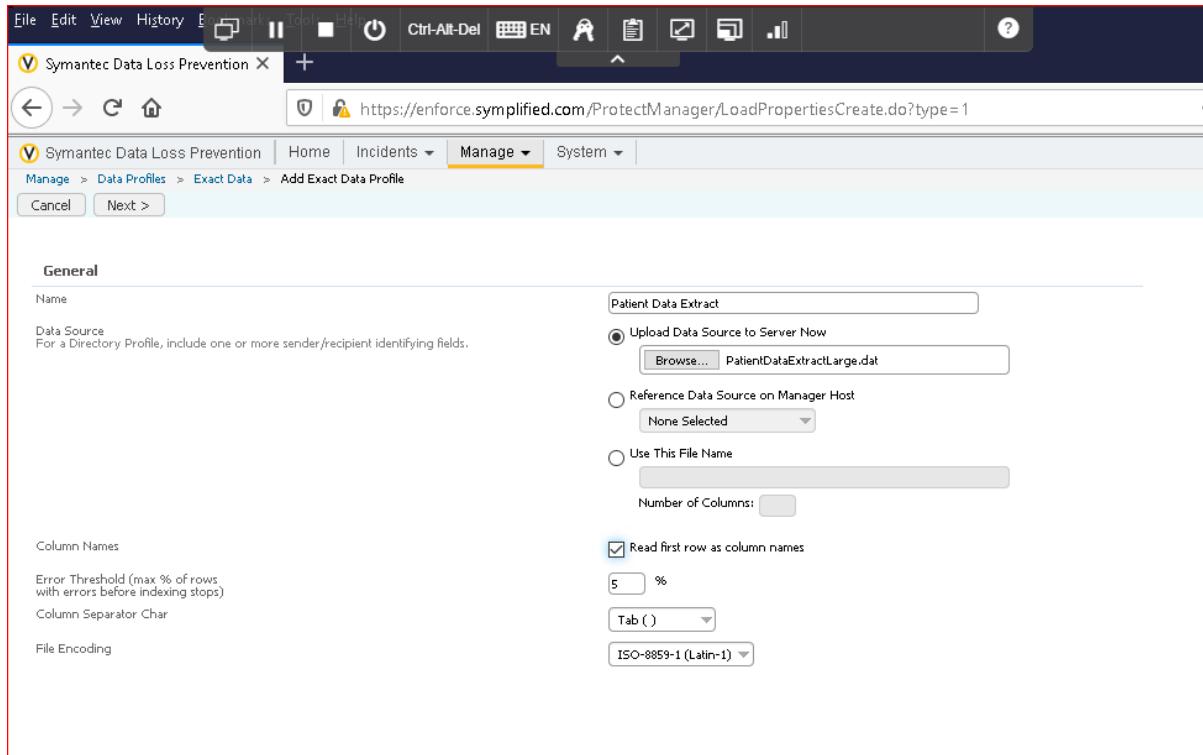
The screenshot shows the 'Policy List' interface. At the top, it displays 'Run time remaining: 0 h : 52 m : 32 s' and 'URL expires: Mar. 9, 2021, 1:44 PM - UTC'. The main area shows a table of policies. A success message at the top of the table states: 'The policy 'Simplified PII (DCM)' was saved successfully.' The table has columns for Status, Name, Description, Policy Group, and Last Modified. One entry is shown: 'Simplified PII (DCM)' with a green status icon, 'Simplified PII Policies' in the Policy Group column, and 'February 23, 2021 4:04' in the Last Modified column.

Below the status indicates that the policy is in active state and running

Exercise 4:

Configuring the policy for PCI compliance.

Sensitive data like credit card information will be stored in the database however it is encrypted but some of the inside employees can see the unencrypted data so they can leak the information as well. The main precaution we should take is we should use the exact data match (EDM) which is done by fingerprinting the structured data. So, whenever the data is transmitted over the network EDM should identify that and for information not getting leaked we add the policies.



The screenshot shows the Symantec Data Loss Prevention interface. The title bar says "Symantec Data Loss Prevention". The URL in the address bar is "https://enforce.symplified.com/ProtectManager/LoadPropertiesCreate.do?type=1". The navigation menu includes "File", "Edit", "View", "History", "Engage", "Tool", "Help", "Ctrl-Alt-Del", "EN", and "System". The main menu bar has "Manage" selected. Below it, the breadcrumb navigation shows "Manage > Data Profiles > Exact Data > Add Exact Data Profile". There are "Cancel" and "Next >" buttons.

General

Name: Patient Data Extract

Data Source: For a Directory Profile, include one or more sender/recipient identifying fields.

Upload Data Source to Server Now (radio button selected):
 PatientDataExtractLarge.dat

Reference Data Source on Manager Host:
 None Selected

Use This File Name:

Number of Columns:

Column Names:
 Read first row as column names
 5 %

Error Threshold (max % of rows with errors before indexing stops):

Column Separator Char:

File Encoding: ISO-8859-1 (Latin-1)

Field Mappings

(For a Directory Profile, include one or more of: Email Address, IP Address, AOL IM Name, Yahoo IM Name, MSN IM Name)

Data Source Field	System Field
SOCIAL_SECURITY_NUMBER	Social Security Number
ACCOUNT_ID	Account Number
FIRST_NAME	First Name
LAST_NAME	Last Name
DRIVERS_LICENSE	Driver License Number
EMAIL_ADDRESS	Email
PASSWORD	Password

All the required fields are mapped for the specified policy template

< Previous | Finish | Cancel

Data Source Field	System Field
SOCIAL_SECURITY_NUMBER	Social Security Number
ACCOUNT_ID	Account Number
FIRST_NAME	First Name
LAST_NAME	Last Name
DRIVERS_LICENSE	Driver License Number
EMAIL_ADDRESS	Email
PASSWORD	Password
PHONE_NUMBER	Phone Number
POSTAL_CODE	Zip Code
CREDIT_CARD	Bank Card Number

Check mappings against policy template

Indexing

Submit Indexing Job on Save
 Submit Indexing Job on Schedule

Indexing Schedule

 It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Rule Name: Credit card Detection

Severity

Default: High

Set Severity to: Medium when match count Is Between from 10 to 25 matches. X

Set Severity to: Low when match count Is Less Than 10 matches. X

Conditions

Content Matches Exact Data From Patient Data Extract.

Match Data Rows when All of these match

2 of the selected fields

Social Security Number Account Number First Name
 Last Name Driver License Number Email
 Password Phone Number Zip Code
 Bank Card Number

WHERE Social Security Number IS ANY OF

Ignore Data Rows when ANY of these match

Sender matches

Content Matches Exact Data From Patient Data Extract.

Match Data Rows when All of these match
 2 of the selected fields
 [select all] [deselect all]

<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Account Number	<input checked="" type="checkbox"/> First Name
<input checked="" type="checkbox"/> Last Name	<input type="checkbox"/> Driver License Number	<input type="checkbox"/> Email
<input type="checkbox"/> Password	<input type="checkbox"/> Phone Number	<input type="checkbox"/> Zip Code
<input type="checkbox"/> Bank Card Number		

WHERE Social Security Number IS ANY OF

Ignore Data Rows when ANY of these match
 Sender matches Email
 Any Recipient matches Email

Field 1 Field 2 Field 3 Excluded Combinations

<input type="checkbox"/> First Name	<input type="checkbox"/> First Name	<input type="checkbox"/> >	<input type="checkbox"/> First Name,Last Name
Last Name	Last Name	<input type="checkbox"/> <	
Bank Card Number	Bank Card Number		

Incident minimum: Only report incidents with at least matches

Match On: Envelope
 Subject
 Body
 Attachments

Run time remaining: 011.20 m. 59 s URL Expires: Mar. 5, 2021, 1:44 PM - UTC

Symantec Data Loss Prevention X +

Manage Policies Policy List Configure Policy Save Cancel

General

Name:	Simplified PCI (EDM/DCM)
Description:	
Policy Label:	
Policy Group:	Simplified PCI Policies
Status:	Active [suspend]
Last Modified:	2/23/21 4:32 PM by Administrator

Detection Groups Response

Add Rule Add Exception

Rules:

- **Credit card Detection (EDM):** Match 2 of (First Name, Last Name, Bank Card Number) from Patient Data Extract.
Severity: High,Low,Medium. Look in envelope, body, attachments.

or

- **Credit Card Catchall (Data Identifiers):** Credit Card Number
Severity: High. Count all unique matches. Look in envelope, subject, body, attachments.

Exceptions:

This policy contains no exceptions.

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes 'Manage' (selected), 'Home', 'Incidents', 'Manage', 'System', and a dropdown menu. The main content area is titled 'Policy List' under 'Manage > Policies'. A success message states 'The policy 'Simplified PCI (EDM/DCM)' was saved successfully.' Below this, there are buttons for 'New', 'Import', 'Export', 'Download Details', and 'Activate'. A table lists two entries:

	Status	Name	Description
<input type="checkbox"/>	Green	Simplified PCI (EDM/DCM)	
<input type="checkbox"/>	Green	Simplified PII (DCM)	

Below the table, it says 'Showing 1 to 2 of 2 entries'. To the right, a sidebar titled 'System' lists various management options like 'Servers and Detectors', 'Agents', 'System Reports', etc., each with a 'Clone' and 'Assign Group' button.

Exercise 5:

Configure and alternate policy for PII Compliance.

The screenshot shows the Symantec Data Loss Prevention interface with a red border around the main configuration area. The URL in the browser is <https://enforce.simplified.com/ProtectManager/LoadEMDIPropertiesCreate.do>. The page title is "Add Exact Match Data Identifier Profile".

General

Name: Patient Data Extract EMDI

Data Source: For Exact Match Data Identifier, map one or more fields

Upload Data Source to Server Now:
 Browse... PatientsForProcessing.dat

Reference Data Source on Manager Host: None Selected

Use This File Name:

Number of Columns:

Column Names: Read first row as column names

Error Threshold (max % of rows with errors before indexing stops): 5 %

Column Separator Char: Comma (,)

File Encoding: ISO-8859-1 (Latin-1)

The screenshot shows the Symantec Data Loss Prevention interface with a red border around the configuration area. The URL in the browser is <https://enforce.simplified.com/ProtectManager/UploadEMDIDataSource.do?by>.

Data Classifier

Valid Source Field	Ignore	Optional	Required	Data Classifier
SSN				- US Social Security Number (SSN) medium
ACCOUNT ID				
FIRST				
LAST				
ACCOUNT NUMBER				
DRIVERS LICENSE				
EMAIL_ADDRESS				
PHONE_NUMBER				
POSTAL_CODE				
PASSWORD				

Indexing

Submit Indexing Job on Save

Run time remaining: 2 h : 08 m : 45 s URL expires: Mar. 9, 2021, 1:44 PM - UTC

File Edit View History Bc Ctrl-Alt-Del EN

Symantec Data Loss Prevention + https://enforce.simplified.com/ProtectManager/UploadEMDIDataSource.do?by=

No trackers known to Firefox were detected on this page.

Data File PatientsForProcessing.dat

At least one field must be selected as Required and mapped to a Data Identifier. At least one field must be Optional.

Data Source Field	Ignore	Optional	Required	Data Identifier
SSN			▼	- US Social Security Number (SSN) medium
ACCOUNT ID	▼			
FIRST		▼		
LAST		▼		
ACCOUNT NUMBER	▼			
DRIVERS LICENSE	▼			
EMAIL_ADDRESS	▼			
PHONE_NUMBER	▼			
POSTAL_CODE	▼			
PASSWORD	▼			

File Edit View History Bc Ctrl-Alt-Del EN

Symantec Data Loss Prevention + https://enforce.simplified.com/ProtectManager/DataSources.do

Manage > Data Profiles > Exact Data

A new registered content 'Patient Data Extract EMDI' was saved successfully. You can now create new policies against this registered content. Those policies will not take effect until the registered content has been successfully indexed.

Add Exact Data Profile	Add Exact Match Data Identifier Profile	Profile Type	Profile Size	Latest Active Version	Status
Patient Data Extract	EDM	0.0 MB			Next Scheduled: None [download profile]
Patient Data Extract EMDI	EMDI	0 MB			Next Scheduled: None [download profile]

The screenshot shows the Symantec Data Loss Prevention Policy List interface. The URL is https://enforce.simplified.com/ProtectManager/enforce/admin/policy/list. The interface includes a toolbar with various icons, a navigation bar with Home, Incidents, Manage, and System, and a breadcrumb trail showing Manage > Policies > Policy List. A success message at the top states "The policy 'Simplified PII (EMDI)' was saved successfully." Below this, there is a table listing three policies:

	Name	Description	Policy Group	Last Modified	Action
<input type="checkbox"/>	Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 23, 2021 4:34:16 PM PST	
<input type="checkbox"/>	Simplified PII (DCM)		Simplified PII Policies	February 23, 2021 4:05:36 PM PST	
<input type="checkbox"/>	Simplified PII (EMDI)		Simplified PII Policies	February 23, 2021 4:48:50 PM PST	

Showing 1 to 3 of 3 entries

This indicates that added policy is not active.

Exercise 6:

Configure a policy to protect the confidential document.

It used the INDEXED DOCUMENT MATCHING.

For instance, a medical company discovered the new drug and whole details were there in the pdf and the pdf should not be leaked outside especially into the competitors. For this we use the INDEXED DOCUMENT MATCHING.

General

Name: Drug Process Documents

Document Source:

- Upload Document Archive to Server Now **Do not use for archives containing Non-ASCII filenames**
 NewPharmaProcess.zip
- Reference Archive on Enforce Server
- Use Local Path on Enforce Server
- Use Remote SMB Share

User:

- Use Saved Credentials: -- None --
- Use These Credentials:

Username:

Password:

Re-enter Password:

ProtectManager/PreDocumentSourceCreate.do

Password to Decrypt Remote IDM Profile:

Re-enter Password:

Filters

File Name Include Filters:

File Name Exclude Filters:

Size Filters:

- Ignore Files Smaller Than: Bytes
- Ignore Files Larger Than: Bytes

Indexing

Submit Indexing Job on Save

Submit Indexing Job on Schedule

Indexing Schedule:

Symantec Data Loss Prevention | Home | Incidents | Manage | System | Page > Policies > Policy List > Configure Policy - Edit Rule | Administrator

General

Rule Name: Drug Process Detection

Severity

Default: High

Set Severity to: Medium when match count Is Between from 10 to 25 matches. X

Set Severity to: Low when match count Is Less Than 10 matches. X

Conditions

Content Matches Document Signature From Drug Process Documents.

Minimum Document Exposure: 30

Match Counting: Check for existence (don't count multiple matches) Count all matches

Match On: Envelope Subject Body

Symantec Data Loss Prevention | Home | /SaveDocumentProfileCondition.do?isException=false&isIdentity=false | Admin

General

Name: Simplified Drug Process Detection (IDM)

Description:

Policy Label:

Policy Group: Default Policy Group

Status: Active [suspend]

Last Modified

Detection **Groups** **Response**

Rules:

- Drug Process Detection (IDM):** Detect documents in Drug Process Documents index with at least 30% match. Severity: High,Low,Medium. Check for existence. Look in body, attachments. X

Exceptions:

This policy contains no exceptions.

[Create a template from this policy](#)

The policy 'Simplified Drug Process Detection (IDM)' was saved successfully.

<input type="checkbox"/>	Status	Name	Description	Policy Group	Last Modified	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Clone"/>	<input type="button" value="Assign Group"/>	<input type="button" value="Filter"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	●	Simplified Drug Process Detection (IDM)		Default Policy Group	February 23, 2021 4:58:31 PM PST	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Clone"/>	<input type="button" value="Assign Group"/>	<input type="button" value="Filter"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	●	Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 23, 2021 4:34:16 PM PST	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Clone"/>	<input type="button" value="Assign Group"/>	<input type="button" value="Filter"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	●	Simplified PII (DCM)		Simplified PII Policies	February 23, 2021 4:05:36 PM PST	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Clone"/>	<input type="button" value="Assign Group"/>	<input type="button" value="Filter"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	●	Simplified PII (EMDI)		Simplified PII Policies	February 23, 2021 4:48:50 PM PST	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Clone"/>	<input type="button" value="Assign Group"/>	<input type="button" value="Filter"/>	<input type="button" value="Clear"/>

Showing 1 to 4 of 4 entries

Exercise 7:

Configure the policy to protect the source code:

In an organization source code plays a vital and it should not be leaked as well for this we use the vector machine learning(VML) is best for finding the matches in the source code.

The screenshot shows the Symantec Data Loss Prevention interface. At the top, there's a navigation bar with 'Manage' selected. Below it, a sub-menu shows 'Data Profiles > Vector Machine Learning'. A 'New Profile...' button is visible. The main area displays a table with columns: 'Profile Name' (sorted), 'Memory Required (KB)', 'Status', and 'Deployment Status'. A modal window titled 'Create New Profile' is open, showing fields for 'Name' (set to 'Source Code Profile') and 'Description'. Below the table, another modal window titled 'Vector Machine Learning Profile' is open, showing a summary of the profile settings: Name (Source Code Profile), Description ([Edit]), Similarity Threshold (10 [Edit]), and Memory Allocation (High). It also lists 'Example' and 'New Document' sections. A third modal window titled 'Upload Contents' is overlaid on the main interface, asking 'Is this a positive or negative document?' with radio buttons for 'Positive' and 'Negative'. It includes a 'Browse...' button to select a file named 'VML_Positive.zip'. To the right of these modals, there are 'Uploaded' and 'Removed' sections with their respective lists and actions.

The screenshot shows the Symantec Data Loss Prevention interface. A green checkmark icon indicates "TRAINING SUCCESSFUL". The "Trained Example Documents" section shows:

	Current Profile	New Profile
Positive Example Documents	0	196
Negative Example Documents	0	198
Total Documents	0	394

The "Accuracy Rate from Training" section shows:

	Current Profile	New Profile
Base False Positive Rate (%)	0	0
Base False Negative Rate (%)	0	0

The "Memory" section shows:

	Current Profile	New Profile
Memory Required (KB)	0	2,883

Buttons for "Accept" and "Reject" are present.

Memory Allocation section: Memory Setting is set to High.

Example Documents section: Contents in positive example documents are matched, contents in negative documents are ignored. A table lists "New Documents":

Document Type	Document Name	Size (KB)	Uploaded	By	Remove
Positive	VML_Positive.zip	824	2/23/21 5:03 PM	Administrator	X
Negative	VML_Negative.zip	1533	2/23/21 5:05 PM	Administrator	X

Upload Contents... button is available.

The screenshot shows the Symantec Data Loss Prevention interface under "Vector Machine Learning Profile". A "Similarity Threshold" dialog box is open, showing a slider from "More Incidents" to "Fewer Incidents" with a current value of 3.5. The "Current Value: 3.5" label is below the slider. The "Save", "Cancel", and "Help" buttons are at the bottom of the dialog.

The main interface shows:

- Name:** Source Code Profile [Edit]
- Description:** [Edit]
- Similarity Threshold:** 10 [Edit]
- Current Profile** section: Trained Example Documents (Positive: 196, Negative: 198, Total: 394), Accuracy Rate from Training (Both 0%), and Memory (2,883 KB).
- Example Documents** section: Shows the same table as the first screenshot, with "Upload Contents..." available.
- Similarity Threshold** dialog box: Shows the current value of 3.5 and a slider for adjustment.

The screenshot shows the Symantec Data Loss Prevention Policy List interface. The top navigation bar includes File, Edit, View, History, Back, Forward, Ctrl-Alt-Del, and System. The main title is "Symantec Data Loss Prevention". The URL in the address bar is https://enforce.symplified.com/ProtectManager/enforce/admin/policy/list. The current page is "Manage > Policies > Policy List". A success message at the top states "The policy 'Simplified Source Code Detection (VML)' was saved successfully." Below this is a toolbar with New, Import, Export, Download Details, Activate, Suspend, Delete, Clone, Assign Group, Filter, and Clear buttons. A table lists five entries:

	Status	Name	Description	Policy Group	Last Modified	Action
<input type="checkbox"/>	●	Simplified Drug Process Detection (IDM)		Default Policy Group	February 23, 2021 4:58:31 PM PST	
<input type="checkbox"/>	●	Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 23, 2021 4:34:16 PM PST	
<input type="checkbox"/>	●	Simplified PII (DCM)		Simplified PII Policies	February 23, 2021 4:05:36 PM PST	
<input type="checkbox"/>	🚫	Simplified PII (EMDI)		Simplified PII Policies	February 23, 2021 4:48:50 PM PST	
<input type="checkbox"/>	●	Simplified Source Code Detection (VML)		Default Policy Group	February 23, 2021 5:08:26 PM PST	

Showing 1 to 5 of 5 entries

Exercise 8:

Configure a policy form recognition:

Basically an organization receives or stores many forms it is not a problem if a form is empty but if there are any details in it it can cause the problem so we need to protect the data.

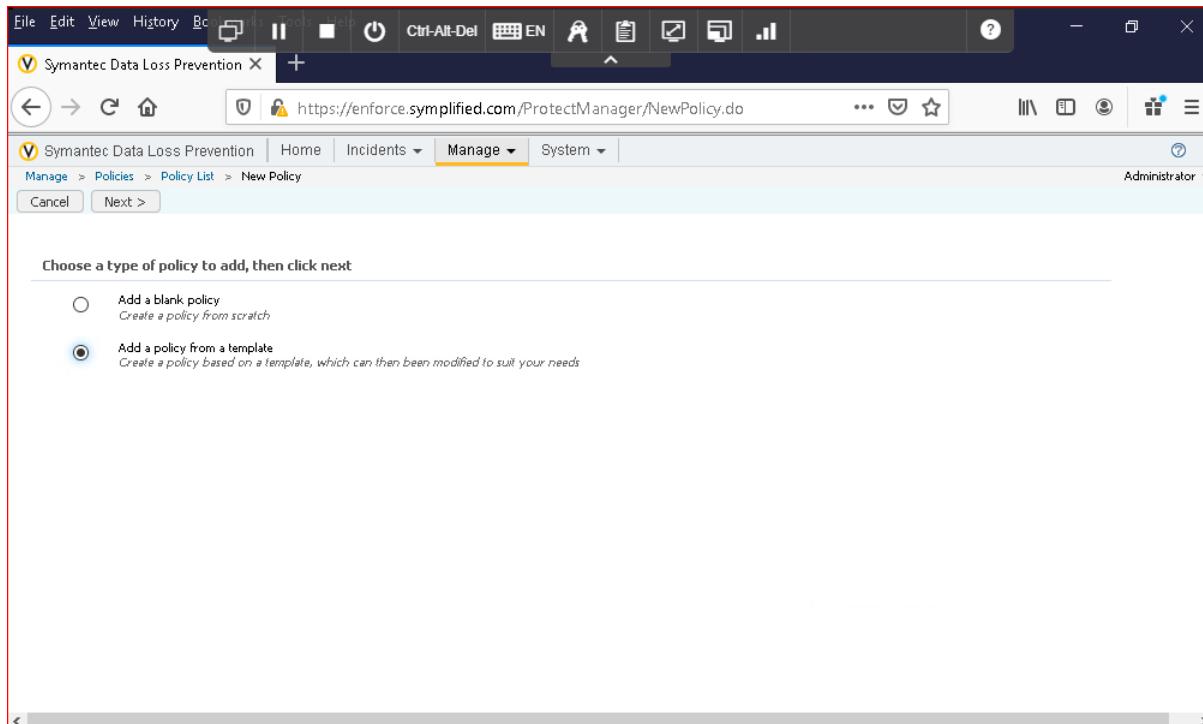
Since there is no form recognition tab in the data profiles I am skipping the exercise 8.

Exercise 9:

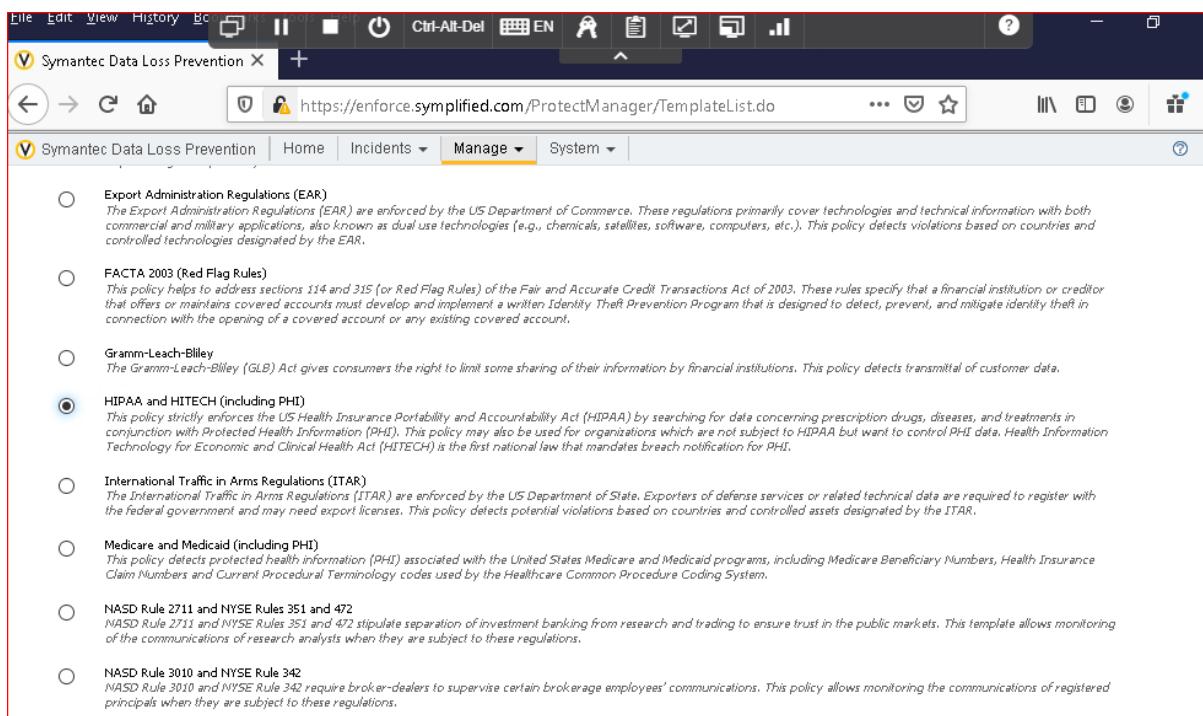
Use a template to add the DLP policy.

The templated implied that there is a policy which is already there and we just use that template and later we can modify that particular template.

Symantec DLP ships with HIPAA template and we can use this template in order to define the policy.



Click next



After selecting this click next

The "HIPAA and HITECH (including PHI)" template works best with an exact data profile that contains the following columns: Account Number, Email, ID Card Number, Last Name, Phone Number, Social Security Number.

If the chosen exact data profile does not have all recommended columns, the new policy will only depend on the columns that are present.

Do Not Use Exact Data Matching
Using this option will still create a policy from the template, but any Exact Data Matching rules contained in the template will not be created.

Patient Data Extract
Some recommended columns are not present. Those columns are : ID Card Number

After selecting this click next

Run time remaining: 1 h : 24 m : 12 s URL expires: Mar. 9, 2021, 1:44 PM - UTC

Manage > Policies > Policy List > Configure Policy Administrator

General

Name	HIPAA and HITECH (including PHI)
Description	This policy strictly enforces the US Health Insurance Portability and
Policy Label	
Policy Group	Simplified PII Policies
Status	Active [suspend]
Last Modified	

Detection

Add Rule Add Exception

Rules:

- **SSN and Drug Keywords (Data Identifiers):** Randomized US Social Security Number (SSN)
Severity: High. Count all matches. Look in envelope, subject, body, attachments.

and
- **SSN and Drug Keywords (Keyword Match):** Match "a.t.o. epinephrine", "a+typhoid", "a+vitamin", "a-25 pill", "aa comb.no3",
Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

or

- **SSN and Treatment Keywords (Data Identifiers):** Randomized US Social Security Number (SSN)

Click on save

Rules:

- **SSN and Drug Keywords (Data Identifiers):** Randomized US Social Security Number (SSN)
Severity: High. Count all matches. Look in envelope, subject, body, attachments.
and
- **SSN and Drug Keywords (Keyword Match):** Match "a.t.o. epinephrine", "a+typhoid", "a+vitamin", "a-25 pill", "aa comb.no3",
Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

- **SSN and Treatment Keywords (Data Identifiers):** Randomized US Social Security Number (SSN)
Severity: High. Count all matches. Look in envelope, subject, body, attachments.
and
- **SSN and Treatment Keywords (Keyword Match):** Match "abximab", "abdomen", "abdomen and chest", "abdomen and pelvis", "abdominal",
Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.

- **SSN and Disease Keywords (Keyword Match):** Match "a2 anemia", "aarskog's", "aarskog's syndrome", "aat deficiency", "ab igne",
Severity: High. Check for existence. Look in envelope, subject, body, attachments. Case insensitive. Match on whole words only.
and
- **SSN and Disease Keywords (Data Identifiers):** Randomized US Social Security Number (SSN)
Severity: High. Count all matches. Look in envelope, subject, body, attachments.

- **SSN and Drug Codes (Data Identifiers):** National Drug Code (NDC)
Severity: High. Count all matches. Look in envelope, subject, body, attachments.

These are the rules which are there in the template we didn't add any rules

Exceptions:

- **TPO Exception (Recipient):** Match e-mail [Recipient@TPOpartner.com].
At least 1 recipient(s) must match.

Create a template from this policy

Rules and exceptions

Manage > Policies > Policy List						
		Status		Name	Description	Policy Group
		Last Modified				
<input type="checkbox"/>		HIPAA and HITECH (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.	Simplified PII Policies	February 24, 2021 4:56:33 AM PST	
<input type="checkbox"/>		Simplified Drug Process Detection (IDM)		Default Policy Group	February 23, 2021 4:58:31 PM PST	
<input type="checkbox"/>		Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 23, 2021 4:34:16 PM PST	
<input type="checkbox"/>		Simplified PII (DCM)		Simplified PII Policies	February 23, 2021 4:05:36 PM PST	
<input type="checkbox"/>		Simplified PII (EMDI)		Simplified PII Policies	February 23, 2021 4:48:50 PM PST	

Since the it is not quite ready to detect the HIPAA template data we need to suspend that.

NOTE:

IN the above labs we added the rules manually but we can simply use the templates and we can modify them .

Exercise 10:

Export policies for use at the DR Site

DR – Disaster Recovery.

If anything goes wrong there will be huge loss to the data and the policies as well. So we need to export the existing policies just in case if the recovery of the existing policies is needed.

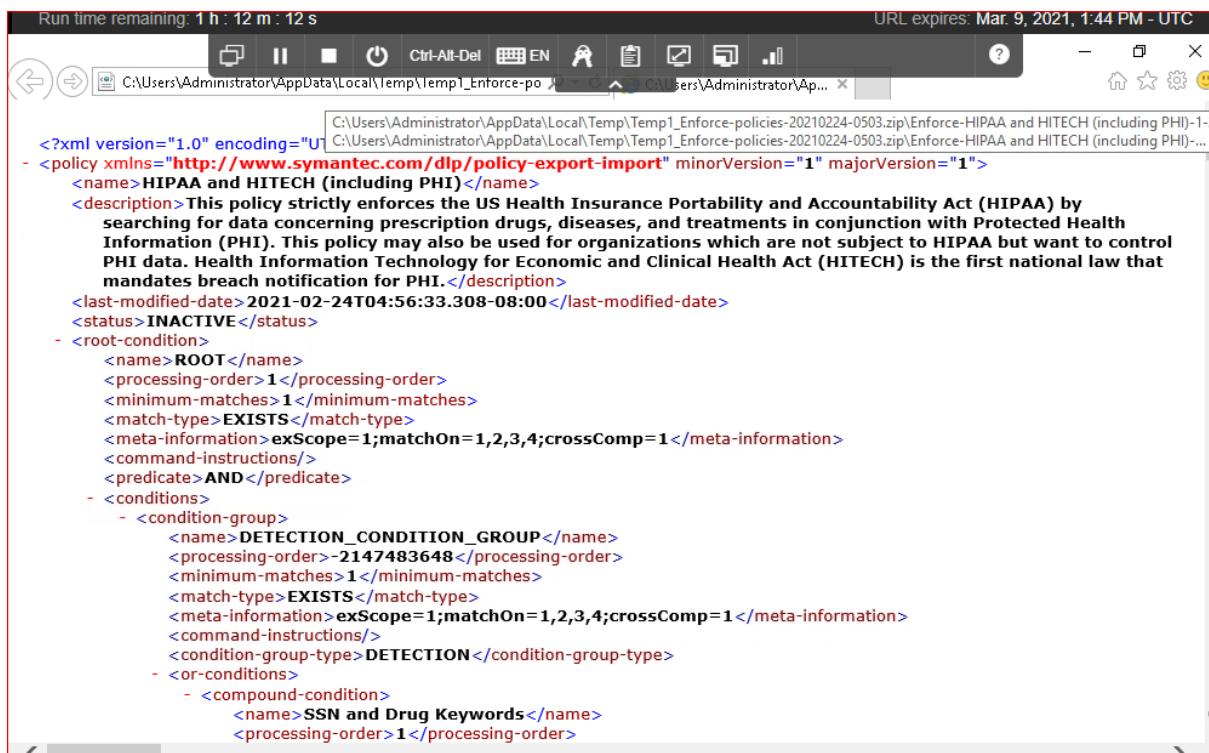
Showing 1 to 6 of 6 entries					
	Status	Name	Description	Policy Group	Last Modified
<input checked="" type="checkbox"/>	*	HIPAA and HITECH (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.	Simplified PII Policies	February 24, 2021 4:56:33 AM PST
<input checked="" type="checkbox"/>	●	Simplified Drug Process Detection (IDM)		Default Policy Group	February 23, 2021 4:58:31 PM PST
<input checked="" type="checkbox"/>	●	Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 23, 2021 4:34:16 PM PST
<input checked="" type="checkbox"/>	●	Simplified PII (DCM)		Simplified PII Policies	February 23, 2021 4:05:36 PM PST
<input checked="" type="checkbox"/>	*	Simplified PII (EMDI)		Simplified PII Policies	February 23, 2021 4:48:50 PM PST

Exporting all existing policies first we need to select all and should export that I mean click on export next to import on the console.

We get a pop up window and should select for save option.

Name	Type	Compressed size	Password ...	Size
Enforce-HIPAA and HITECH (includ...	XML Document	249 KB	No	
Enforce-Simplified Drug Process D...	XML Document	2 KB	No	
Enforce-Simplified PCI (EDM-DC...	XML Document	6 KB	No	
Enforce-Simplified PII (DCM)-4-20...	XML Document	4 KB	No	
Enforce-Simplified PII (EMDI)-5-20...	XML Document	4 KB	No	
Enforce-Simplified Source Code D...	XML Document	2 KB	No	

Should follow the above path for exported documents.



```
<?xml version="1.0" encoding="U
<policy xmlns="http://www.symantec.com/dlp/policy-export-import" minorVersion="1" majorVersion="1">
  <name>HIPAA and HITECH (including PHI)</name>
  <description>This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.</description>
  <last-modified-date>2021-02-24T04:56:33.308-08:00</last-modified-date>
  <status>INACTIVE</status>
  - <root-condition>
    <name>ROOT</name>
    <processing-order>1</processing-order>
    <minimum-matches>1</minimum-matches>
    <match-type>EXISTS</match-type>
    <meta-information>exScope=1;matchOn=1,2,3,4;crossComp=1</meta-information>
    <command-instructions/>
    <predicate>AND</predicate>
    - <conditions>
      - <condition-group>
        <name>DETECTION_CONDITION_GROUP</name>
        <processing-order>-2147483648</processing-order>
        <minimum-matches>1</minimum-matches>
        <match-type>EXISTS</match-type>
        <meta-information>exScope=1;matchOn=1,2,3,4;crossComp=1</meta-information>
        <command-instructions/>
        <condition-group-type>DETECTION</condition-group-type>
      - <or-conditions>
        - <compound-condition>
          <name>SSN and Drug Keywords</name>
          <processing-order>1</processing-order>
```

Here is the xml document.

Exercise 11:

Configure the optical character reconigantion.

OCR basically extracts the text from the supported image file and send this for the analysis whether if there any policy violations.

Since there is no OCR engine configuration option iam skipping this exercise.

Lab 2:

Locating the confidential data stored on the premises and on the cloud.

Exercise 1:

Run a Content Enumeration scan:

In an organization there will be many huge data sharing within the internal network and most of the times the data wont be well documented and it is difficult to know where this shares reside so this scan can possibly locate the shares on the network.

The screenshot shows the 'Configure Directory Connection' page for 'Simplified Active Directory'. The 'General' tab is selected. The 'Name' field contains 'Simplified Active Directory'. Under 'Network Parameters', the 'Hostname' is set to 'localhost' and the 'Port' is set to '389'. The 'Base DN' field contains 'DC=simplified,DC=com'. The 'Authentication' section has a checked checkbox for 'Connect with Credentials'.

Configuring the connection to simplified active directory. Before doing enumerated scan we need to do this steps

The screenshot shows the 'Configure Directory Connection' page for 'Simplified Active Directory'. The 'Port' is set to '389' and the 'Base DN' is set to 'DC=simplified,DC=com'. The 'Authentication' section has a checked checkbox for 'Connect with Credentials'. Below it, the 'Username' field is filled with 'simplified\dlpldap' and the 'Password' field contains a masked password. A 'Test Connection' button is visible at the bottom.

Configuring the connection to simplified active directory.

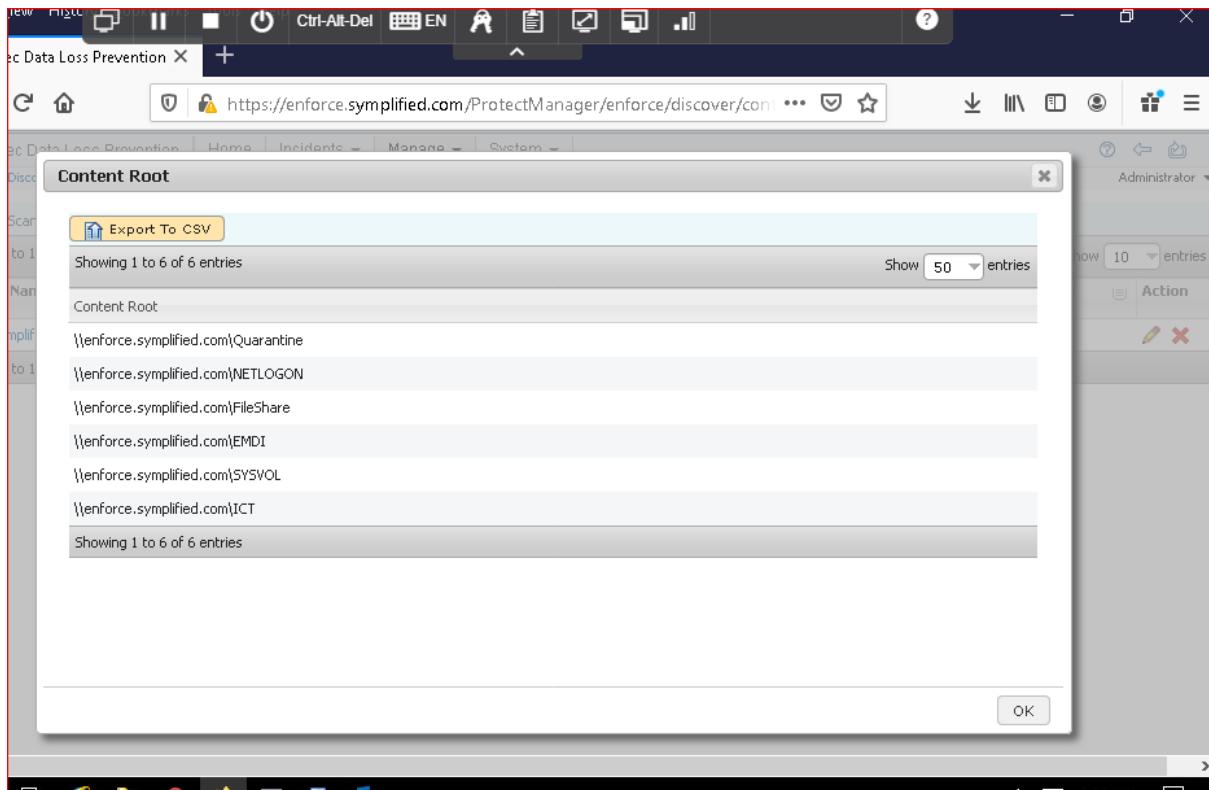
Training! Is the password

The screenshot shows the Symantec Data Loss Prevention web interface. The URL is https://enforce.simplified.com/ProtectManager/enforce/admin/directories. The page title is "Configure Directory Connection". A green success message at the top says "Directory Connection tested successfully.". Below it are "Save" and "Cancel" buttons. There are two tabs: "General" and "Index Settings", with "Index Settings" selected. The "Index Settings" section has a sub-section titled "Indexing Schedule". It contains a legend: "No Regular Schedule" (radio button), "Once" (radio button), "Daily" (radio button), "Weekly" (radio button, highlighted with a yellow background), and "Monthly" (radio button). To the right of the legend are checkboxes for days of the week: Sunday (checked), Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.

Configuring the connection to simplified active directory.s

The screenshot shows the "Content Root Enumeration Scan Configuration" screen. At the top are "Save" and "Cancel" buttons. The title is "Content Root Enumeration Scan Configuration". A note says "* Required Fields". The "General" section includes fields for "Name" (set to "Simplified File Share Scan") and "Directory Connection" (set to "Simplified Active Directory"). Under "Enumerate shares?", the "Yes" radio button is selected. The "Filters" section includes an IP Range field ("From . . . To . . .") and a "Server Names" field where "does contain" is selected and the value "enforce" is entered. There is also a link "Add Server Name Filter".

Configuring the content root enumeration scan.



Results of the scan.

Exercise 2:

Scan a windows target

Whatever the data which is flowing through the network it should not be unencrypted and this scan analyses the data which is in the openshare.

Symantec Data Loss Prevention > Settings > Credentials > New Credential

Administrator

General

Credential Name * dlpscan

Access Username * sympified\dlpscan

Access Password *****

Re-enter Access Password *****

Usage Permission

Only on Servers (Indexed Documents, Discover Targets, Manual Proxy)

Servers and Endpoint agents (Indexed Documents, Discover Targets, Endpoint Response Rules, Manual Proxy)

Save Cancel

Adding credentials.

Symantec Data Loss Prevention > Manage > Discover Scanning > Discover Targets > Add File System Target

Administrator

General Targeting Scanned Content Filters Advanced Protect

General

Name * Windows File Share Scan

Policy Groups *

Classification

Default Policy Group

Sympified PCI Policies

Sympified PII Policies

Scan Execution

Scan only new or modified items (incremental scan)

Scan all items for next scan. Subsequent scans will be incremental

Always scan all items (full scan)

Use Incremental indexes from (Please select one or more)

Available Discover Targets Selected Discover Targets

Save Cancel

Adding details in the general tab.

The screenshot shows the Symantec Data Loss Prevention management interface. At the top, it displays "Run time remaining: 0 h : 30 m : 47 s" and "URL expires: Mar. 9, 2021, 1:44 PM - UTC". The main window has tabs for "Manage" and "System". Under "Manage", the "Discover Scanning" tab is selected. In the "Discover Targets" section, there is a table with one entry:

Action	Target Name	Target Type	Policy Groups	Servers or Detectors	Last Modified	Scan Status	Next Scan	Action
<input checked="" type="checkbox"/>	Windows File Share Scan	File System	Simplified PCI Policies	Simplified Detection Server	2/24/21 5:45 AM	Ready		

Below the table, it says "Showing 1 to 1 of 1 entries".

Adding the details in the scanned content tab.

The screenshot shows the Symantec Data Loss Prevention management interface. At the top, it displays "Run time remaining: 0 h : 30 m : 47 s" and "URL expires: Mar. 9, 2021, 1:44 PM - UTC". The main window has tabs for "Manage" and "System". Under "Manage", the "Discover Scanning" tab is selected. In the "Discover Targets" section, there is a table with one entry:

Action	Target Name	Target Type	Policy Groups	Servers or Detectors	Last Modified	Scan Status	Next Scan	Action
<input checked="" type="checkbox"/>	Windows File Share Scan	File System	Simplified PCI Policies	Simplified Detection Server	2/24/21 5:45 AM	Ready		

Below the table, it says "Showing 1 to 1 of 1 entries".

Added target and need to scan this.

The screenshot shows the Symantec Data Loss Prevention interface. The main title bar says "Symantec Data Loss Prevention". The URL in the address bar is "https://enforce.simplified.com/ProtectManager/DiscoverIncidentSummary". The top navigation bar includes "Home", "Incidents" (which is selected), "Manage", and "System". On the left, there's a sidebar with "Saved Reports" (No Saved Reports Available) and "Discover Reports" (Exec. Summary - Discover, Incidents - All Scans, Incidents - New, Target Summary, Policy by Target, Status by Target, Content Roots at Risk). The main content area has a "Filter" section with dropdowns for Status (Equals All), Scan (Custom, set to "Windows File Share Scan 2/24/21 5:46 AM"), Target ID (All Targets), and Detection Date (All Dates). Below this is an "Advanced Filters & Summarization" section with "Applied Filters" (Status Equals All, Target ID All Targets) and "Summarized by Policy" (Scan Custom 2/24/21 5:46 AM, Severity Is Any Of High 7, Medium 0, Low 0, Info 0). A table titled "Policy" shows totals for each severity level: Total 7, High 7, Med 0, Low 0, Info 0. The "Totals" row shows 332 matches for the Simplified PCI (EDM/DCM) policy. At the bottom right, there are "Show" and "Matches" buttons.

Result after the scan.

The screenshot shows the Symantec Data Loss Prevention interface. The main title bar says "Symantec Data Loss Prevention". The URL in the address bar is "https://enforce.simplified.com/ProtectManager/DarIncidentDetails". The top navigation bar includes "Home", "Incidents" (selected), "Manage", and "System". On the left, there's a sidebar with "Discover Reports" (Incidents - All Scans, Discover Incident Snapshot). The main content area shows an "Incident 00000387" page. It has sections for "File System" (Status: New, Severity: High), "Policy Matches" (Simplified PCI (EDM/DCM) [view policy] with 179 matches, Credit card Detection (EDM) with 100 matches, Credit Card Catchall (Data Identifiers) with 79 matches), and "Incident Details" (Server or Detector: Simplified Detection Server, Target: Windows File Share Scan, Scan: 2/24/21 5:46 AM, Detection Date: 2/24/21 5:46 AM, Seen Before: No, Is Hidden: No [Do Not Hide], URL: //enforce.simplified.com/FileShare). To the right, there's a "Matches" section titled "Matches (matches found in 1 component)" which lists several names and their associated IDs: MARTHA CAHILL 4830782323949940, JOSEPH NICHOLS 4468381105299690, PETER CLARK 4608121971967830, CATHERINE WISCH 4522434791230970, JONATHAN SIEGEL 4588441012817760, and KATHRYN ALFARO 4316025757703390. There's also an "Attributes" section stating "No custom attributes defined".

Incident page.

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes Home, Incidents (selected), Manage, and System. Below the navigation is a breadcrumb trail: Incidents > Discover > Incidents - All Scans > Discover Incident Snapshot. The main content area displays an incident titled "Incident 00000387". On the left, there's a "File System" section with tabs for Key Info, History (selected), Notes, and Correlations. The History tab shows the following log entries:

Date	Submitted By	Summary
2/24/21 5:46 AM	Administrator	Status Changed New
2/24/21 5:46 AM	Simplified Detection Server	Incident data discarded based on response rule Discarded original message. Discard all attachments.
2/24/21 5:46 AM	Administrator	Severity Changed High
2/24/21 5:46 AM	Simplified Detection Server	Detected

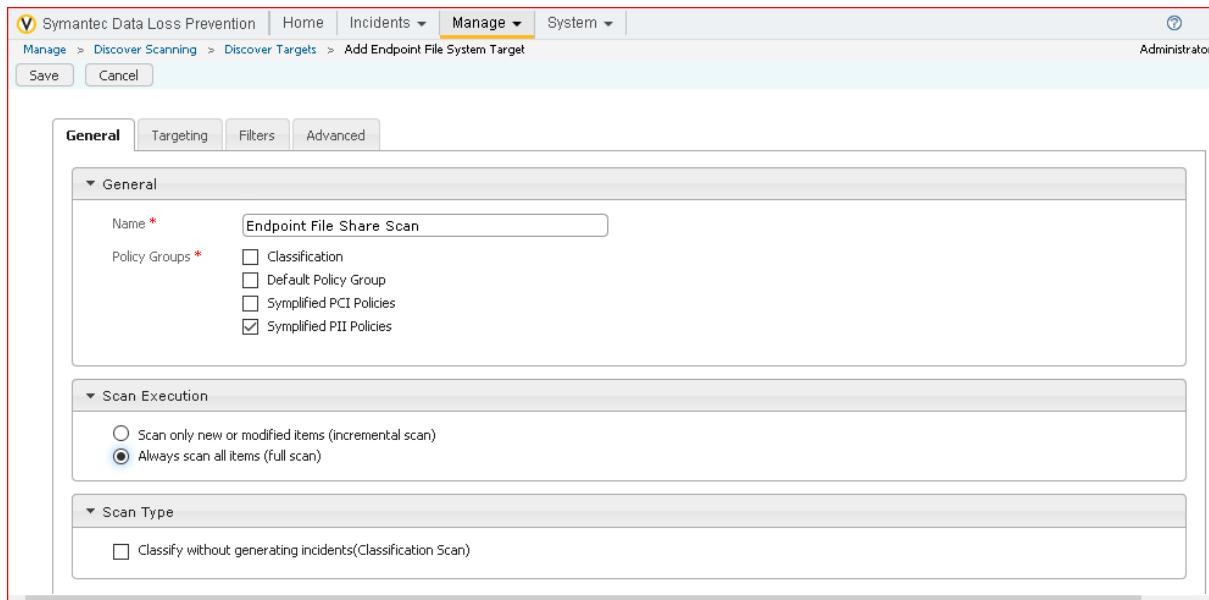
To the right of the history is a "Matches" section listing findings from one component, specifically "PatientsForProcessing.xlsx (179 Matches)". It includes entries for Martha Cahill, Joseph Nichols, Peter Clark, Catherine Wisch, and Jonathan Siegel, each with their respective IDs. The final section on the right is titled "Attributes" with the note "No custom attributes defined".

Seeing the history tab whether any actions taken on the incident.

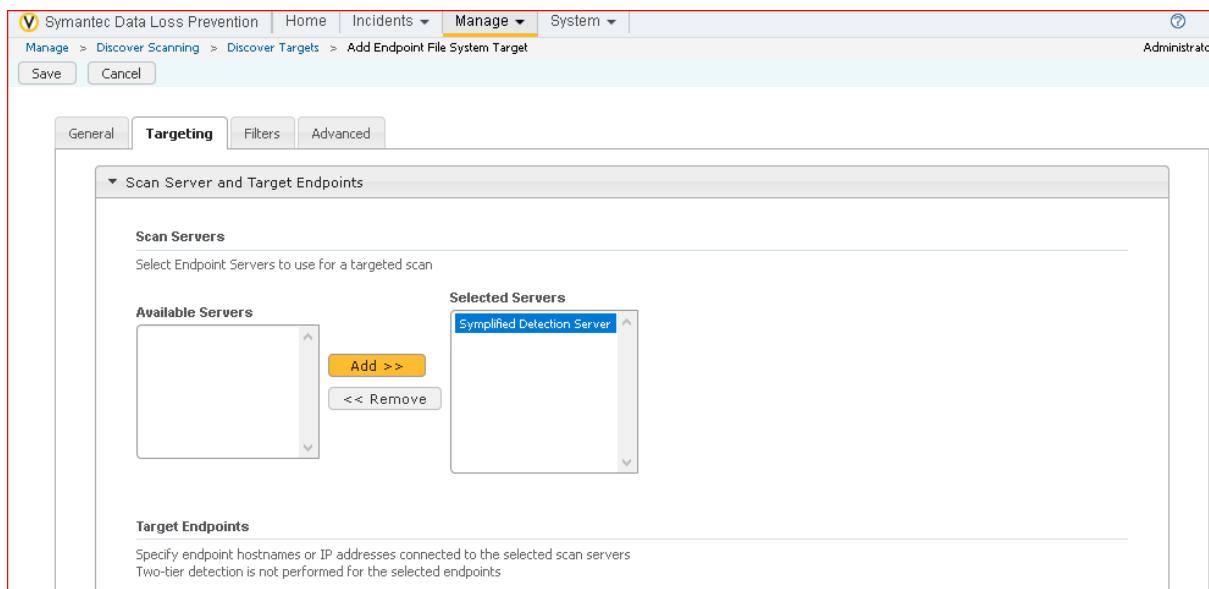
Exercise 3:

Scan endpoint computers for confidential data.

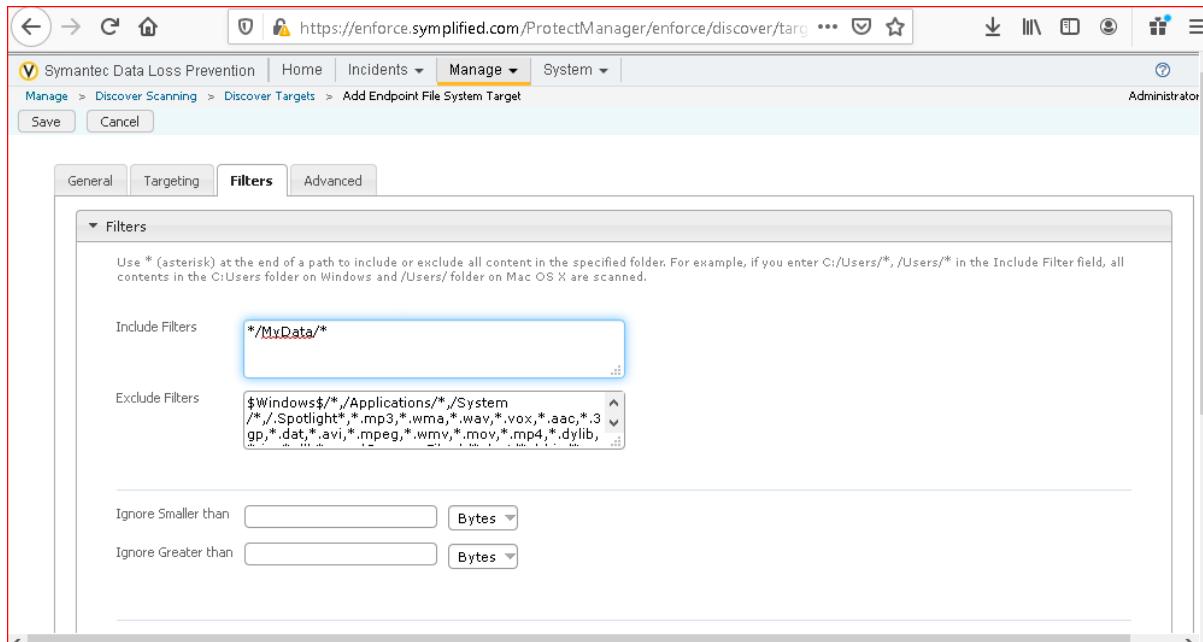
In a organization there will be many endpoints I mean there are many departments which uses the computer for their daily work for an IT guy it is difficult to manage all those so what we need to do is create and perform the DLP scan so that we can see the what confidential data is being stored in the respective endpoints.



Setting rules in the general tab.



Setting rules in targeting tab



Setting rules in filters.

Scan History for Endpoint File Share Scan										
<input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Filters"/> Show 25 entries										
	Target Name	Target Type	Scan Started	Scan Status	Number Of Servers In Grid	Scan Type	Incidents Generated	Run Time	Bytes / Items Scanned	Actions
<input type="checkbox"/>	Endpoint File Share Scan	File System Endpoint	2/24/21 5:54 AM	Starting	N/A	Full	0	00:00:00:09	0 MB / 0	

Scanning the Endpoint File share.

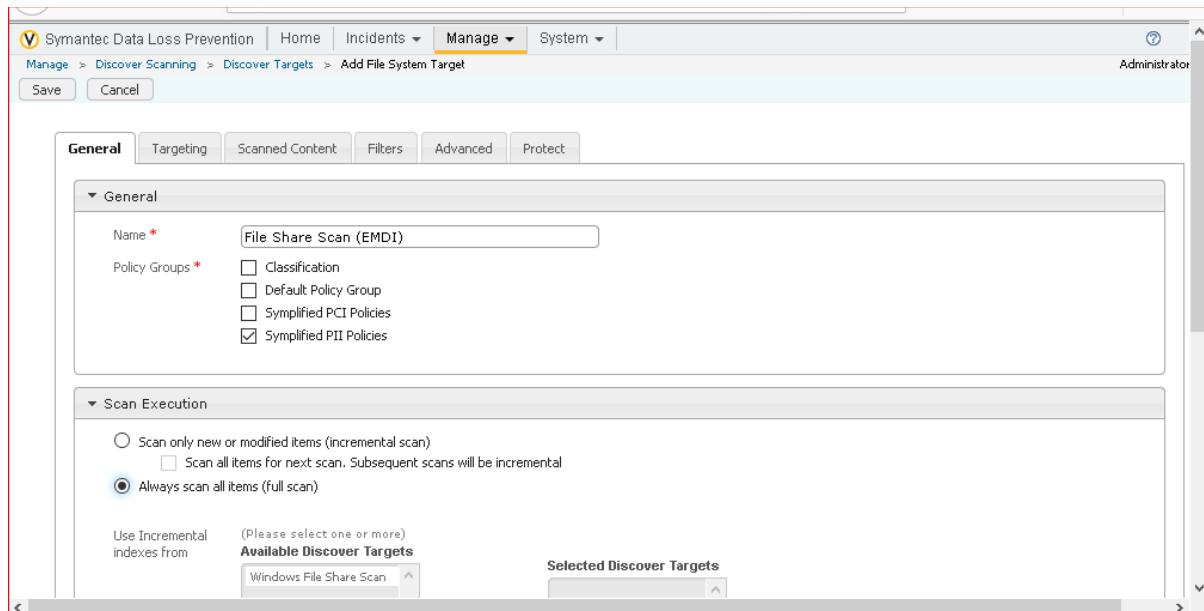
Exercise 4:

Scan server for confidential data using EMDI

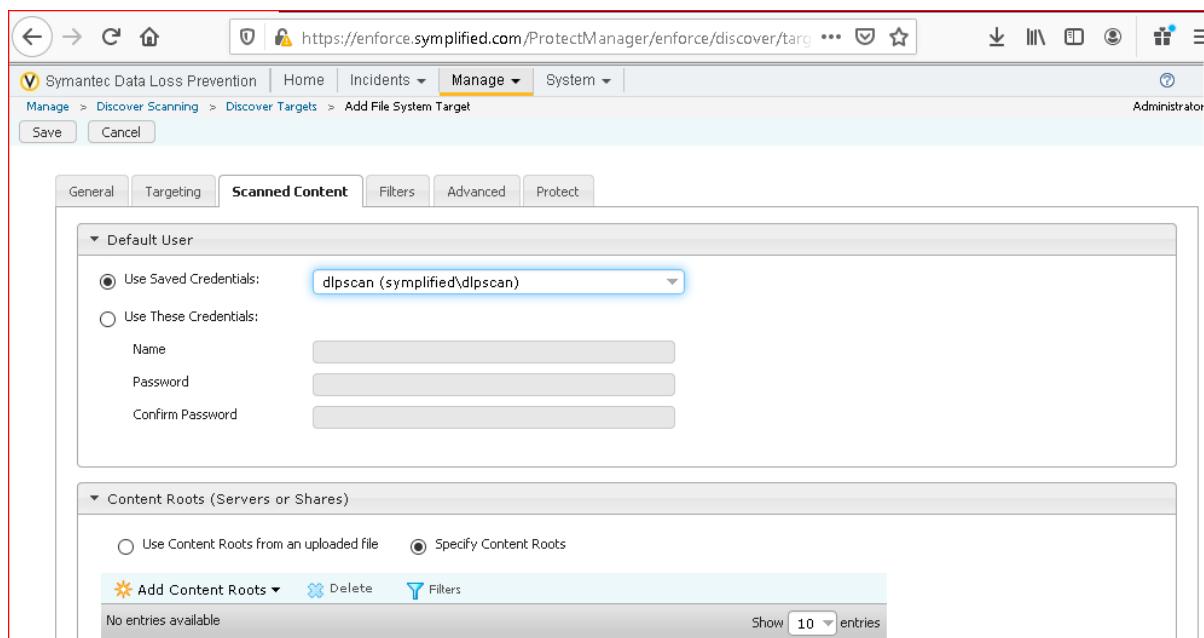
EMDI- Exact data matching.

This exercise is same as the exercise 3 of what we did the scan of the sensitive data but in this lab there is additional concept we are using and that is EMDI and purpose of this to uncut the unimportant incidents when scanning the files on the endpoint computers.

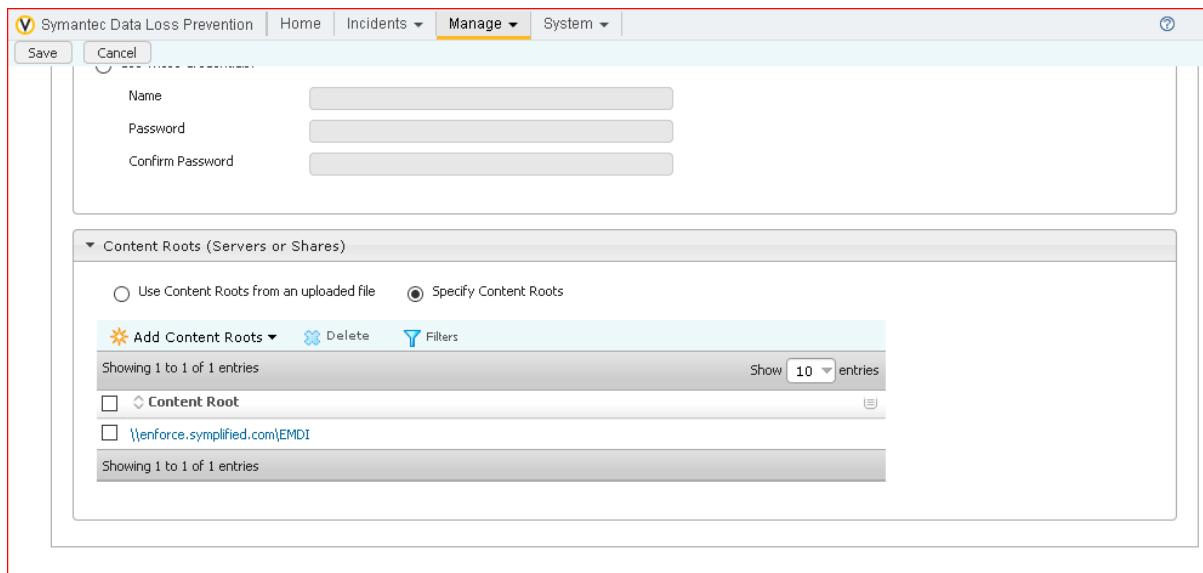
EMDI basically utilises the data set which is there in the exercise 3 in order to validate the potential data breaches even before triggering the incident.



Adding the data in the general tab.



Adding data in the scanned content



Adding the data in the scanned content.

Date	Path	Error
2/24/21 6:06:47 AM		

Date/Time	Level	Message
2/24/21 6:06:47 AM	INFO	Scan started
2/24/21 6:06:47 AM	INFO	Started scanning Share: //enforce.simplified.com/EMDI
2/24/21 6:06:47 AM	INFO	Finished 2 items, 109,474 bytes; filtered 0 items
2/24/21 6:06:47 AM	INFO	Finished scanning Share: //enforce.simplified.com/EMDI
2/24/21 6:06:47 AM	INFO	Scan finished

Reviewing the scan statistics.

The screenshot shows the Symantec Data Loss Prevention interface. In the top navigation bar, the URL is https://enforce.simplified.com/ProtectManager/DarIncidentReport.do. The main area displays a list of incidents under 'Discover Reports' > 'Incidents - All Scans'. There are two incidents listed:

- Endpoint File Share Scan**: Scan 2/24/21 5:54 AM, File Share Scan (EMDI) 2/24/21 6:06 AM.
- Windows File Share Scan**: Scan 2/24/21 5:46 AM.

On the right side, there are severity filters: High (checked), Low (unchecked), Medium (checked), and Info (unchecked). Below the incidents, there is a table titled 'Applied Filters' with columns for Status, Scan, Severity, Type, Location / Target / Scan, File Owner, ID / Policy, Matches, Severity, and Status.

Status	Scan	Severity	Type	Location / Target / Scan	File Owner	ID / Policy	Matches	Severity	Status
Equals All	Custom 2/24/21 6:06 AM	Is Any Of High 2, Medium 0, Low 0, Info 0		Location //enforce.simplified.com/EMDI/Sample EMDI Invoice.pdf	BUILTIN\Administrators	00000389 Simplified PII (DCM)	2	High	Ne
				Target Scan					

Here there are two incidents

The screenshot shows the Symantec Data Loss Prevention interface under the 'Manage' tab. It lists various policies:

Status	Name	Description	Policy Group	Last Modified	Action Buttons
<input type="checkbox"/>	HIPAA and HITECH (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.	Simplified PII Policies	February 24, 2021 4:56:33 AM PST	
<input type="checkbox"/>	Simplified Drug Process Detection (IDM)		Default Policy Group	February 23, 2021 4:58:31 PM PST	
<input type="checkbox"/>	Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 23, 2021 4:34:16 PM PST	
<input type="checkbox"/>	Simplified PII (DCM)		Simplified PII Policies	February 24, 2021 6:09:15 AM PST	
<input type="checkbox"/>	Simplified PII (EMDI)		Simplified PII Policies	February 24, 2021 6:09:23 AM PST	
<input type="checkbox"/>	Simplified Source Code Detection (VML)		Default Policy Group	February 23, 2021 5:08:26 PM PST	

Activation and deactivation is done.

General

Target Type	File System
Target Name	File Share Scan (EMDI)
Status	Completed
Scan Type	Full
Start Time	2/24/21 6:10 AM
End Time	2/24/21 6:10 AM

Scan Statistics

Processed	Share: 1 of 1
Run Time (Days:Hours:Minutes:Seconds)	00:00:00:00
Items Scanned	2
Bytes Scanned	106.81 KB (109,474 Bytes)
Errors	0
Current Incident Count	1

Recent Scan Errors

Date	Path	Error
2/24/21 6:10:05 AM	/enforce.symplified.com/EMDI	INFO
2/24/21 6:10:05 AM	/enforce.symplified.com/EMDI	INFO
2/24/21 6:10:05 AM	/enforce.symplified.com/EMDI	INFO
2/24/21 6:10:05 AM	/enforce.symplified.com/EMDI	INFO
2/24/21 6:10:06 AM	/enforce.symplified.com/EMDI	INFO

Recent Scan Activity

Date/Time	Level	Message
2/24/21 6:10:05 AM	INFO	Scan started
2/24/21 6:10:05 AM	INFO	Started scanning Share: //enforce.symplified.com/EMDI
2/24/21 6:10:05 AM	INFO	Finished 2 items, 109,474 bytes; filtered 0 items
2/24/21 6:10:05 AM	INFO	Finished scanning Share: //enforce.symplified.com/EMDI
2/24/21 6:10:06 AM	INFO	Scan finished

Only one incident is discovered after activation and deactivation of rules

Symplified

Incidents - All Scans

2/24/21 6:06 AM
Windows File Share Scan
2/24/21 5:46 AM

Applied Filters

Status	Scan	Severity
Equals All	Custom 2/24/21 6:10 AM	Is Any Of High 1, Medium 0, Low 0, Info 0
Target ID All Targets	Detection Date All Dates	

Type	Location / Target / Scan	File Owner	ID / Policy	Matches	Severity
Location	//enforce.symplified.com/EMDI/Patient Extract (EMDI).xlsx	BUILTIN\Administrators	00000390 Symplified PII (EMDI)	35	High 1
Target	File Share Scan (EMDI)				
Scan	2/24/21 6:10 AM				

Displaying that one incident

Exercise 5:

Configure a global policy for PII Compliance.

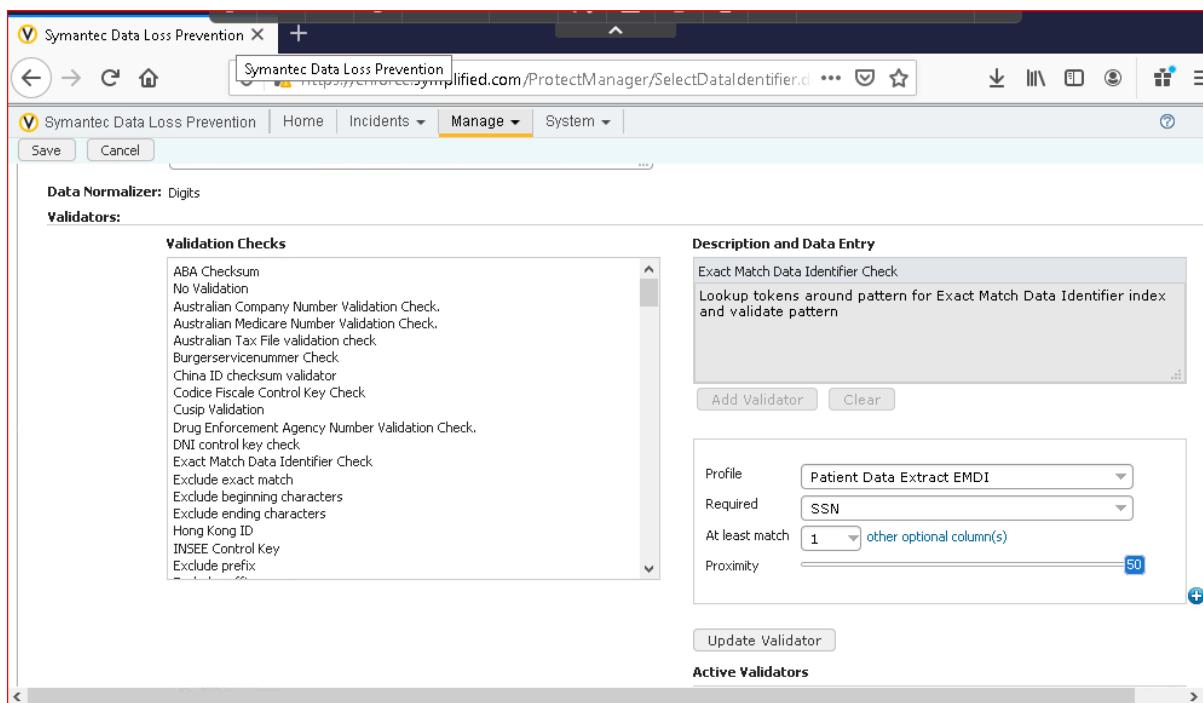
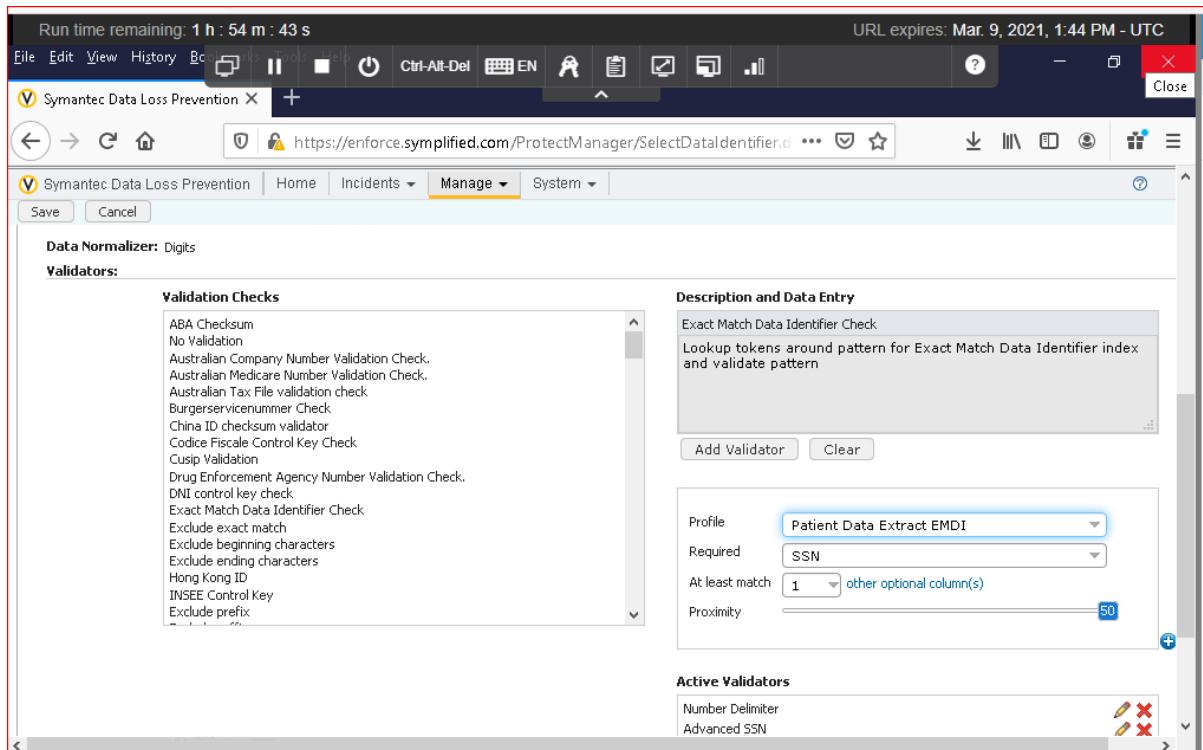
After using the Exact data match in the above exercise we understood how useful the Exact data match is. Since we add many policies in day – to- day life we use SSN numbers and EMDI would be very useful in additional validation check. Rather than adding this everytime I mean for each policy we need to create a global addition across the system so that a new policy can use the established data source.

The screenshot shows the Symantec Data Loss Prevention interface. The URL is https://enforce.simplified.com/ProtectManager>SelectDataIdentifier.c. The page title is "Manage > Policies > Data Identifiers". The user is logged in as "Administrator". The main content area displays the details for a data identifier named "US Social Security Number (SSN)". The details include:

Name:	US Social Security Number (SSN)
Description:	Personal identification number issued by the Social Security Administration of the United States government. Although primarily used for administering the Social Security program, it is widely used as a personal identification number in many purposes.
Category:	North American Personal Identity

Below the details, there is a section titled "Rule Breadth" with three options: "Wide", "Medium", and "Narrow".

US Social Security Number.



Section 3:

Understanding how confidential data is being used.

In this lab we use network prevent for email to monitor outgoing smtp messages looking for important or confidential data that needs to be blocked or encrypted and we also monitor the user activity at the endpoints as well.

Exercise 1:

Configure Network prevent for email to monitor SMTP messages.s

The purpose of this lab is that no sensitive data should be leaked from the organization.

Any emails which contains the sensitive information leaving the organization unencrypted will be logged rather than blocked or rerouted.

It department will configure the DLP such that any emails containing the sensitive information should be re routed to the Symantec Encryption management server before sending to the recipient.

Servers and Detectors					
Status	Name	Version	Type	Form Factor	Messages (Last 10 sec)
Running	Enforce Server	15.5.0.17018	N/A	Software	N/A
Running	Simplified Detection Server	15.5.0.17018	Network Monitor, Network Prevent for Email, Network Prevent for Web, Endpoint, Network Discover/Cloud Storage Discover	Software	0
					21

Recent Error and Warning Events show all »				
Type	Time	Name	Host	Code
⚠️	February 24, 2021 9:45:23 AM PST	Simplified Detection Server	127.0.0.1	1011
⚠️	February 24, 2021 7:40:06 AM PST	Simplified Detection Server	127.0.0.1	1011
⚠️	February 24, 2021 4:43:05 AM PST	Simplified Detection Server	127.0.0.1	1014
⚠️	February 23, 2021 3:11:38 PM PST	Simplified Detection Server	127.0.0.1	1202
✖️	February 23, 2021 3:11:21 PM PST	Simplified Detection Server	127.0.0.1	1008

Now click on the simplified detection server

General

Name	Simplified Detection Server
Host	127.0.0.1
Port	8100
Version	15.5.0.17018
Status	Running [stop] [recycle]
CPU Usage	16%
Physical Memory	72%
Disk Usage	84%
Message Processing Wait Time (HH:MM:SS)	N/A
Number of Stream Directories on Disk	0

All Agents

Registered	1 agents
Reporting/Connected	0 agents
Not Reporting/Disconnected	1 agents
OK/Healthy	0 agents
Warning	0 agents
Critical/Down	1 agents
Disabled	N/A
Shutdown	N/A

Recent Error and Warning Events | show all >

Type	Time	Code	Message
!	2/24/21 9:45 AM	1011	Restarted PacketCapture
!	2/24/21 7:40 AM	1011	Restarted PacketCapture
!	2/24/21 4:43 AM	1014	Low disk space
!	2/23/21 3:11 PM	1202	No policies loaded

Simplified detection server details.

Process Control

Advanced Process Control

Agent Connection Status Configuration

Show Agent as "Not Reporting" after hours minutes

DLP User Authentication

Users are authenticated Forms based using

For all users:

Require Strong Password

Password Rotation Period days (0 means no rotation)

Selecting the advanced process control and click save

The screenshot shows the 'Inline SMTP' configuration page. In the 'Security Configuration' section, there is a checkbox for 'Trial Mode (Do not block violating messages)' which is unchecked. Below it, 'Maximum number of connections *' is set to 12. In the 'Next Hop Configuration' section, the 'Forward' option is selected. Under 'Forward', 'Enable MX lookup (Specify Domains)' and 'Disable MX lookup (Specify Host Names/IP Addresses)' are listed; the latter is selected. A text input field contains 'enforce.simplified.com'. A note at the bottom says '(newline separated, priority ordered list)'.

Rules in inline smtp

The screenshot shows the 'Server Settings' page. A yellow banner at the top says 'You must recycle the server for the new values to take effect.' Below are three tabs: 'Done', 'Configure', and 'Server Settings', with 'Server Settings' being active. The 'General' section displays various server statistics:

Name	Simplified Detection Server
Host	127.0.0.1
Port	8100
Version	15.5.0.17018
Status	Running [stop] [recycle]
DetectionServerDatabase Status	Running [stop]
EndpointServer Status	Running [stop]
FileReader Status	Running [stop]
PacketCapture Status	Running [stop]
RequestProcessor Status	Running [stop]
CPU Usage	17%
Physical Memory	73%
Disk Usage	84%
Message Processing Wait Time (HH:MM:SS)	N/A
Number of Stream Directories on Disk	0

To the right, the 'All Agents' section shows agent status counts:

Registered	1 agents
Reporting/Connected	0 agents
Not Reporting/Disconnected	1 agents
OK/Healthy	0 agents
Warning	0 agents
Critical/Down	1 agents
Disabled	N/A
Shutdown	N/A

At the bottom, the 'Recent Error and Warning Events' section lists two entries:

Type	Time	Code	Message
Warning	2/24/21 9:45 AM	1011	Restarted PacketCapture
Warning	2/24/21 7:40 AM	1011	Restarted PacketCapture

We need to recycle the server in order to apply the new rules.

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes Home, Incidents, Manage, System, and a URL bar pointing to https://enforce.symplified.com/ProtectManager/MonitorDetail.do?value(monitorID)=1. Below the navigation is a breadcrumb trail: System > Servers and Detectors > Overview > Server / Detector Detail. Action buttons Done, Configure, and Server Settings are available.

General

Name	Symplified Detection Server
Host	127.0.0.1
Port	8100
Version	15.5.0.17018
Status	Running [stop] [recycle]
DetectionServerDatabase Status	Running [stop]
EndpointServer Status	Running [stop]
FileReader Status	Running [stop]
PacketCapture Status	Running [stop]
RequestProcessor Status	Running [stop]
CPU Usage	20%
Physical Memory	71%
Disk Usage	84%
Message Processing Wait Time (HH:MM:SS)	N/A
Number of Stream Directories on Disk	0

All Agents

Registered	1 agents
Reporting/Connected	0 agents
Not Reporting/Disconnected	1 agents
OK/Healthy	0 agents
Warning	0 agents
Critical/Down	1 agents
Disabled	N/A
Shutdown	N/A

Recent Error and Warning Events | show all »

Type	Time	Code	Message
!	2/24/21 9:52 AM	1014	Low disk space
!	2/24/21 9:45 AM	1011	Restarted PacketCapture
!	2/24/21 7:40 AM	1011	Restarted PacketCapture
!	2/24/21 4:43 AM	1014	Low disk space

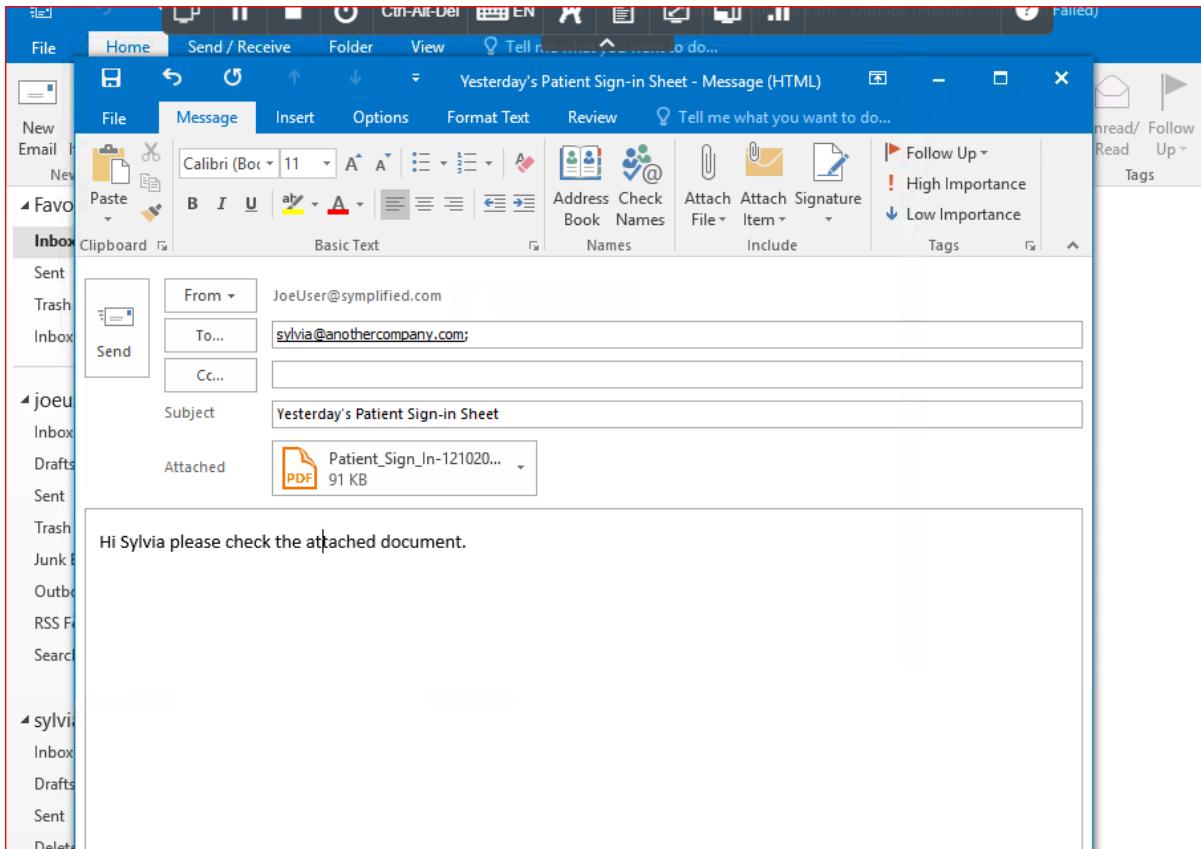
After recycling all the status in general should be running and we can see that in above screenshot.

Exercise 2:

Use network prevent for email to monitor SMTP Messages.

In this lab user1 sends the email to the user2 first he sends the unsensitive data and next he sends the sensitive data so, in both the cases lets see for which incidents will be rised and how enforce server is gonna detect that.

This incident is raised when the sensitive data is transferring through the network.



Logged in as user joe and sending the mail to the sylvia which is not sensitive data.

The screenshot shows the Symantec Data Loss Prevention interface. The left sidebar has sections for 'Saved Reports' (No Saved Reports Available) and 'Network Reports' (Incidents - All, Incidents - New, Policy Summary, Status by Policy, High Risk Senders - Last 30 Days). The main area is titled 'Incidents' and shows a table of incidents. The filters applied are: Status Equals New, Date Last 30 Days, and Severity Is Any Of High (2), Medium (1), Low (0), Info (0). The table has columns for Type (Email), Subject / Sender / Recipient(s), Sent (2/24/21 10:37 PM), ID / Policy (00000403, Symplyfied PCI (EDM/DCM)), Matches (179), and Severity (High). There are two rows of data.

Type	Subject / Sender / Recipient(s)	Sent	ID / Policy	Matches	Severity
Email	Patents Data for Processing JoeUser@symplyfied.com sylvia@anothercompany.com	2/24/21 10:37 PM	00000403 Symplyfied PCI (EDM/DCM)	179	High
Email	Patents Data for Processing JoeUser@symplyfied.com sylvia@anothercompany.com	2/24/21 10:37 PM	00000402 Symplyfied PII (DCM)	100	Medium

While sending the insensitive data no incident is rised but while sending the sensitive data over the email incident is rising.

This incidents is raised in the networks not at the endpoint

Incidents at the network.

Exercise 3:**Monitor endpoint activity- Email**

Network prevent for email has previously only used to monitor the emails at the networks but now monitoring at the end point is very much essential.

First point of security should be there at the endpoint and second point should be at the network. So always protect the data at the endpoints and next at the network.

In this exercise we use email monitoring to check email contents and attachments similarly how the network monitoring analyzed the email in the previous exercise.

The screenshot shows the Symantec Data Loss Prevention interface. The URL is https://enforce.simplified.com/ProtectManager/NewAgentConfiguration. The navigation bar includes Home, Incidents, Manage, and System. The current page is System > Agents > Agent Configuration. A red box highlights the 'Name' field, which contains 'Simplifed Agent Configuration'. Below it is a 'Description' field with a placeholder. The 'Channels' tab is selected, indicated by a yellow background. Under 'Enable Monitoring', there's a checkbox for 'Enable different monitoring settings for endpoints located on and off the corporate network.' The 'Destinations' section lists Removable Storage, CD/DVD, Local drive, and Printer/Fax, with Removable Storage checked. The 'Clipboard' section has 'Copy' checked. The 'Email' section has 'Outlook' checked. The 'Web' section lists IE (HTTPS), Edge (HTTPS), Firefox (HTTPS), Chrome (HTTPS), Safari (HTTPS), HTTP, and FTP, all of which are unchecked.

Giving name and selecting outlook in channels tab

Setting	Value
Discover.SCAN_ONLY_WHEN_IDLE.int	2
Discover.SECONDS_UNTIL_IDLE.int	120
Discover.STANDARD_REPORT_INTERVAL.int	900000
EncryptionDriver.FORCE_UNLOAD_TIMEOUT.int	10
EncryptionDriver.LISTENER_THREADS_COUNT.int	1
EncryptionDriver.MESSAGE_HANDLER_THREADS_COUNT.int	10
EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int *	10
EndpointCommunications.IDLE_TIMEOUT_IN_SECONDS.int *	0
EndpointLocation.MATCHES_ALL_INTERFACES_FOR_MANUAL_SETTING.int *	1
ExtensionEnablement.DISPLAY_BROWSER_EXTENSION_NOTIFICATION.int	1
ExtensionEnablement.DISPLAY_SAFARI_EXTENSION_NOTIFICATION.int	1
FileService.MAX_CACHE_SIZE.int	250
FileSystem.APPS_LISTUSES_TRUNCATE_FILE_FOR_BLOCK_RULE.str	TextEdit;Microsoft PowerPoint
FileSystem.DRIVER_FILE_OPEN_REQUEST_TIMEOUT.int	10
FileSystem.ENABLE_FILE_RESTORATION.int	1
FileSystem.ENABLE_VEP_FILE_ELIMINATION.int	3

Changing the time in seconds for

EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int SECONDS TO 10

EndpointCommunications.IDLE_TIMEOUT_IN_SECONDS TO 0

Endpoint

Setting	Value
ResponseCache.MAX_SIZE.int	60000
ServerCommunicator.CONNECT_BACKOFF_DURATION_MULTIPLIER.int *	100
ServerCommunicator.CONNECT_DELAY_POST_WAKEUP_OR_POST_VPN_SECONDS.int *	2
ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int *	60
ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int *	10
ServerCommunicator.INITIAL_CONNECT_BACKOFF_DURATION_SECONDS.int *	30
ServerCommunicator.MAX_CONNECT_BACKOFF_DURATION_SECONDS.int *	1800
Transport.ALLOW_EXPIRED_CERTIFICATES.int *	1
Transport.AUTO_FLUSH_LIMIT_KILOBYTES.int *	16
Transport.DNS_HOST_CACHE_TIMEOUT_SECONDS.int *	86400
Transport.MAX_CONNECT_WAIT_SECONDS.int *	30
Transport.MAX_INBOUND_KILOBYTES_TO_BUFFER.int *	100
Transport.MAX_OUTBOUND_KILOBYTES_TO_BUFFER.int *	100
Transport.MAX_SSL_SESSION_LIFETIME_SECONDS.int *	86400
Transport.VERIFY_SERVER_HOSTNAME.int *	0
UI.BUTTON_ENCRYPT_ALLOW.str	

Configuring the setting

Setting server communicator.CONNECT_POLLING_INTERVAL_SECONDS.int to 10

The screenshot shows the Symantec Data Loss Prevention ProtectManager interface. The URL is https://enforce.simplified.com/ProtectManager/enforce/admin/endpoint/agentgroups/list. The 'System' tab is selected. In the center, there's a modal dialog titled 'Assign Configuration'. It says 'Select configuration to assign it to the Agent group(s). The configuration will be deployed for enabled Agent group(s.)'. Under 'For agent groups:', 'Default Group' is selected. Under 'Assign configuration:', 'Simplified Agent Configuration' is selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The background shows a table of 'Agent Groups' with one entry: 'Default Group' (Status: Enabled, Last Deployment Date: 5/7/19 12:41 PM, Modified By: Administrator).

Updating the simplified agent configuration.

The screenshot shows the Symantec Data Loss Prevention ProtectManager interface. The URL is https://enforce.simplified.com/ProtectManager/enforce/admin/endpoint/agentgroups/list. The 'System' tab is selected. A green success message at the top says 'Agent configuration assigned successfully to agent group(s.)'. Below it, the 'Agent Groups' section shows a table with one entry: 'Default Group' (Status: Enabled, Agent Configuration: Simplified Agent Configuration, Last Deployment Date: 2/24/21 9:47 PM, Modified By: Administrator).

Since it is advanced setting we need to restart the device.

Vinay Kumar Reddy Donda

dondavinayreddy@gmail.com

Sent - JoeUser@sympified.com - Outlook (Product Activation Failed)

Home Send / Receive Folder View Tell me what you want to do...

New New Email Items New Delete Reply Reply All Forward Respond

Move to: ? To Manager Team Email Rules Follow Up Tags Find Send/Receive All Folders Send/Receive

Favorites

- Inbox - JoeUser@sympified.com
- Sent
- Trash
- Inbox 6 - sylvia@anothercompany.com

joeuser@sympified.com

- Inbox
- Drafts
- Sent**
- Trash
- Junk E-mail
- Outbox [3]
- RSS Feeds
- Search Folders

File Home Send / Receive Folder View Tell me what you want to do...

Move to: ? To Manager Team Email Rules Follow Up Tags Find Send/Receive All Folders Send/Receive

Tell Me (Alt+Q)
Just start typing here to bring features to your fingertips and get help.

All Unread
Today

'sylvia@anothercom... Patents Data for Processing 11:18 PM
Hi Sylvia, Please find the

'sylvia@anothercom... Patents Data for Processing 11:08 PM
Hi Sylvia, Please find the

'sylvia@anothercom... Patents Data for Processing 11:00 PM
Hi Sylvia, Please find the

'sylvia@anothercom... Yesterday's Patient Sign-in ... 10:57 PM
Hi Sylvia please check the

'sylvia@anothercom... Patents Data for Processing 10:37 PM
Hi Sylvia, Please find the

'Joe User'

To 'sylvia@anothercompany.com'

PatientsForProcessing.... 102 KB

Hi Sylvia,

Please find the attachment.

Best Reagrds,
JOe

Sent message from joe to syvliva

Sent - JoeUser@sympified.com - Outlook (Product Activation Failed)

Home Send / Receive Folder View Tell me what you want to do...

New New Email Items New Delete Reply Reply All Forward Respond

Move to: ? To Manager Team Email Rules Follow Up Tags Find Send/Receive All Folders Send/Receive

Favorites

- Inbox - JoeUser@sympified.com
- Sent
- Trash
- Inbox 6 - sylvia@anothercompany.com

sylvia@anothercompany.c...

- Inbox 6
- Drafts
- Sent
- Deleted Items
- Junk E-mail
- Outbox
- Search Folders

File Home Send / Receive Folder View Tell me what you want to do...

Move to: ? To Manager Team Email Rules Follow Up Tags Find Send/Receive All Folders Send/Receive

Tell Me (Alt+Q)
Just start typing here to bring features to your fingertips and get help.

All Unread
Today

Joe User Patents Data for Processing 11:18 PM
Hi Sylvia, Please find the

Joe User Patents Data for Processing 11:08 PM
Hi Sylvia, Please find the

Joe User Patents Data for Processing 11:00 PM
Hi Sylvia, Please find the

Joe User Yesterday's Patient Sign-in ... 10:57 PM
Hi Sylvia please check the

Joe User Patents Data for Processing 10:37 PM
Hi Sylvia, Please find the

Joe User

To sylvia@anothercompany.com

PatientsForProcessing.... 98 KB

Hi Sylvia,

Please find the attachment.

Best Reagrds,
JOe

inbox in sylvia

Applied Filters:

- Status Equals New
- Date Last 30 Days
- Severity Is Any Of High (8), Medium (0), Low (0), Info (0)

Type	Subject / Sender / Recipient(s)	Sent	ID / Policy	Matches	Severity	Status
✉	Patents Data for Processing JoeUser@sympified.com sylvia@anothercompany.com	2/24/21 11:17 PM	00000409 Sympified PCI (EDM/DCM)	179	High	New
✉	Patents Data for Processing JoeUser@sympified.com sylvia@anothercompany.com	2/24/21 11:17 PM	00000408 Sympified PII (DCM)	100	High	New
✉	Patents Data for Processing JoeUser@sympified.com sylvia@anothercompany.com	2/24/21 11:07 PM	00000407 Sympified PCI (EDM/DCM)	179	High	New
✉	Patents Data for Processing JoeUser@sympified.com sylvia@anothercompany.com	2/24/21 11:07 PM	00000406 Sympified PII (DCM)	100	High	New

Incident is raised at the endpoint.

Applied Filters:

- Status Equals New
- Date Last 30 Days
- Severity Is Any Of High (3), Medium (0), Low (0), Info (0)

Type	Destination / Machine / User	Occurred On	ID / Policy	Matches	Severity	Status
✉	ENDPOINT SYMPLIFIED\joe_user Patents Data for Processing sylvia@anothercompany.com	2/24/21 11:17 PM	00000412 Sympified PCI (EDM/DCM)	100	High	New
✉	ENDPOINT SYMPLIFIED\joe_user Patents Data for Processing sylvia@anothercompany.com	2/24/21 11:17 PM	00000411 Sympified PII (DCM)	300	High	New
✉	ENDPOINT SYMPLIFIED\joe_user Patents Data for Processing sylvia@anothercompany.com	2/24/21 11:17 PM	00000410 Sympified PCI (EDM/DCM)	79	High	New

Incident is raised at the endpoint.

Exercise 4:

Monitor Endpoint activity – Third party apps

We know how important the sensitive data at the endpoints the best and easy solution is to use the Symantec DLP to monitor endpoints.

In this lab Application file Access control enables administrators to configure applications that are not pre-configured in Symantec dlp to be monitored the sensitive data usage. For suppose user joe want to encrypt the company's data with another application named AxCrypt but this application was not listed in Symantec DLP and its un authorized app which can steal the company's sensitive data. So company observed this thing and used the Symantec DLP such that no data is encrypted is using the other applications apart from which is listed in the Symantec DLP.

Application Information

Operating System Windows
Name * AxCrypt
Binary Name (*) AxCrypt.exe
Internal Name (*)
Original Filename (*)
Publisher Name
 Verify publisher name
(*) You must provide at least one of these names.

Application Type

Select application type.

Adding the application in order to block that.

Application Monitoring Configuration

Select the channels to monitor:
For 14.5.x and earlier agents, selecting any of Removable Storage, Local Drive, Copy to Network Share, or Application File Access enables monitoring for all of the following channels.
Likewise, for 14.5.x and earlier agents, selecting either HTTP or FTP enables monitoring for both HTTP and FTP channels.

Destinations

Removable Storage
 Printer/Fax
 Local Drive

Clipboard

Clipboard
 Copy
 Paste

Web

HTTP
 FTP

Application File Access

Application File Access
 Open
 Read

Network Shares

Copy to Network Share

Setting the rules need to deselect everything and select application file access and select read option.

The screenshot shows the 'Enable Monitoring' section of the Symantec Data Loss Prevention configuration. It includes sections for Destinations (Removable Storage, CD/DVD, Local drive, Printer/Fax), Clipboard (Copy, Paste), Email (Outlook, Lotus Notes), Web (IE (HTTPS), Edge (HTTPS), Firefox (HTTPS), Chrome (HTTPS), Safari (HTTPS), HTTP, FTP), Configured Applications (Application File Access, Cloud Storage), Network Shares (Copy to Local Drive, Copy to Share), and SEP Integration (SEP Intensive Protection).

Adding the rules.

The screenshot shows a Windows File Explorer window displaying files in the 'Misc' folder. One file, 'Patients Credit Card Info.xlsx', is selected and highlighted with a blue border. The status bar at the bottom indicates it is an AxCrypt file (16 KB). Other files listed include 'Email Block', 'Email Notification', 'email_banner', 'JamesGuerra_Lab_Test_Order_Form', 'lookupstrings', 'NatalieWaldman-PIF', 'NewPharmaProcess', 'Patient_Sign_In-12102016', 'Patients Credit Card Info CSV', 'PatientsForProcessing', 'Quarantine Text', 'reboot', and 'Sample EMDI Invoice'.

Displaying that patient credit card info is encrypted with ACRYPT app.

Symantec Data Loss Prevention

Incidents > Endpoint > Incidents - New

Filter

Status: Equals New Date: Last 30 Days Severity: High, Medium, Low, Info

Applied Filters

Status Equals New Date Last 30 Days Severity Is Any Of High 4, Medium 0, Low 0, Info 0

Type	Destination / Machine / User	Occurred On	ID / Policy	Matches	Severity
File Name	Patients Credit Card Info.xlsx ENDPOINT SYMPILIFIED\joe_user	2/25/21 12:27 AM	00000413 Symplified PCI (EDM/DCM)	40	High
Machine User	ENDPOINT SYMPILIFIED\joe_user	2/24/21 11:17 PM	00000412 Symplified PCI (EDM/DCM)	100	High
Subject Recipient	Patents Data for Processing sylvia@anothercompany.com	2/24/21 11:17 PM	00000411 Symplified PII (DCM)	300	High
Machine User	ENDPOINT SYMPILIFIED\joe_user	2/24/21 11:17 PM	00000410 Symplified PCI (EDM/DCM)	79	High
Subject Recipient	Patents Data for Processing sylvia@anothercompany.com	2/24/21 11:17 PM	00000410 Symplified PCI (EDM/DCM)	79	High

When encrypted an incident is raised at the endpoint

Incident 00000413

Status: New Severity: High

Endpoint Application File Access

Policy Matches

Symplified PCI (EDM/DCM) [view policy] Matches 40

Credit Card Catchall (Data Identifiers) Matches 40

Incident Details

Server or Detector	Symplified Detection Server
Occurred On	2/25/21 12:27 AM
Reported On	2/25/21 12:27 AM
Is Hidden	No [Do Not Hide]
User	SYMPILIFIED\joe_user
Machine Name	ENDPOINT
Machine IP (Corporate)	10.10.2.20
Environment	

Matches (matches found in 1 component)

C:\Training Files\Misc\Patients Credit Card Info.xlsx (40 Matches):

- ... TALIE WALDMAN AMEX: **342955624318368** Apr-10 (592)
- 427-8964 89427-8964 30001 DAMION GWEN Discover: **6011624665174125** Oct-09 (489) 687-4819 73187-4819
- 30002 AGNES QUITIN MasterCard: **5120939736834980** Jan-09 (644)
- 870-9142 41870-9142 30003 JAMES, CHARTIER Visa: **4116509050569147** Apr-09 (515) 743-8908 02043-8908
- 30006 JEFF BURNS AMEX: **344058488426266** Oct-09 (337)
- 288-6963 82288-6963 30008 JACQUELINE MCMILLAN Discover: **6011976857117225** Jun-11 (781)
- 312-7066 03312-7066 30010 HAROLD HALL MasterCard: **5123695007103193** Jul-11 (839)
- 241-5325 25241-5325 30011 MIKE LEPERBRE Visa: **4116480559370132** Jul-11 (506) 755-7405 36055-7405
- 30014 TRACIE BROWN AMEX: **345672983453416** Jul-11 (830)
- 831-3083 80831-3083 30016 JOHN HOOVER Discover: **6011750048255222** Jul-12 (671)

Attributes

No custom attributes defined

Incident is defined as the Endpoint Application file Access.

Exercise 5:**Monitor end point activity copy/paste**

Malicious intruders inside the organization can leak the information and they try to copy/paste the information. We will now see how this endpoint detects the copy paste operation.

The screenshot shows the Symantec Data Loss Prevention Agent Configuration page. Under the 'Channels' tab, there are sections for 'Clipboard', 'Email', and 'Web'. In the 'Clipboard' section, 'Copy' and 'Paste' are selected. In the 'Email' section, 'Outlook' is selected. In the 'Web' section, several browser options like IE (HTTPS), Edge (HTTPS), Firefox (HTTPS), Chrome (HTTPS), and Safari (HTTPS) are listed. A note at the top says 'Enable different monitoring settings for endpoints located on and off the corporate network.'

Adding the rule for copy and paste.

The screenshot shows an Excel spreadsheet titled 'CustomerDataExtract'. The table has columns: SSN, ACCOUNT ID, FIRST, LAST, and ACCOUNT NUM. The Conditional Formatting ribbon tab is open, showing a preview of color-coded rows based on values 6, 4, 9, 7, and 3. The formula used is =MOD(ROW(),5)=1. The preview shows rows 1, 6, and 11 are green, while rows 2, 4, 5, 7, and 9 are red.

Copying the data

Symantec Data Loss Prevention - Incidents

Filter

Status: Equals New
Date: Last 30 Days

Severity: High (5), Medium (0), Low (0), Info (0)

Applied Filters

Type	Destination / Machine / User	Occurred On	ID / Policy	Matches	Severity	Status
Machine User	ENDPOINT SYMLIFIED\joe_user	2/25/21 12:45 AM	00000415 Sympified PII (DCM)	5	High	New
Machine User	ENDPOINT SYMLIFIED\joe_user	2/25/21 12:45 AM	00000414 Sympified PCI (EDM/DCM)	6	Medium	New
File Name	Patients Credit Card Info.xlsx	2/25/21 12:27 AM	00000413 Sympified PCI (EDM/DCM)	40	High	New
Machine User	ENDPOINT SYMLIFIED\joe_user	2/24/21 11:17 PM	00000412 Sympified PCI (EDM/DCM)	100	High	New
Machine User	ENDPOINT SYMLIFIED\joe_user	2/24/21 11:17 PM	00000411 Sympified PII (DCM)	300	High	New

I tried copying the data twice so two incidents raised at the endpoint

Run time remaining: 5 h : 01 m : 44 s

URL expires: Mar. 9, 2021, 1:44 PM - UTC

Incident 00000415

Status: New
Severity: High

Endpoint Clipboard

Key Info	History	Notes	Correlations
Policy Matches			
Sympified PII (DCM) [view policy] 5 US Social Security Numbers (Data Identifiers) 5			
Incident Details			
Server or Detector	Sympified Detection Server		
Occurred On	2/25/21 12:45 AM		
Reported On	2/25/21 12:45 AM		
Is Hidden	No [Do Not Hide]		
User	SYMLIFIED\joe_user		
Machine Name	ENDPOINT		
Machine IP (Corporate)	10.10.2.20		

Matches (matches found in 1 component)

- Body (5 Matches):
 - ... 420-08-3530 30809 RAUL PASHAL 4684451986499930 B00089620 pashal_63588...om (930)750-0791 53395-9820 d0IeNxBJcB 650-22-0893 30811 ORA LEISURE 4132673384929420 G00698233 leisure_1100...om (293)561-7807 29795-8233 ZEUDkPNK 561-97-2514
 - 30812 JAMES HINTZ 480331697819540 D00451340 hintz_668208...om (714)803-9738 03706-1340 keLoCstt 203-36-9293
 - 30813 GOLDIE PURVIS 4409094843938080 E00907590 purvis_14463...om (693)473-0722 15222-7590 HwbwUgKqD 373-18-2660 30814 SUSAN WILLIAMS 4083121379497770 E0...

Attributes

No custom attributes defined

The raised incident is described as the endpoint clipboard.

Section 4 or lab 4:

Educating users to Adopt data Protection practices.

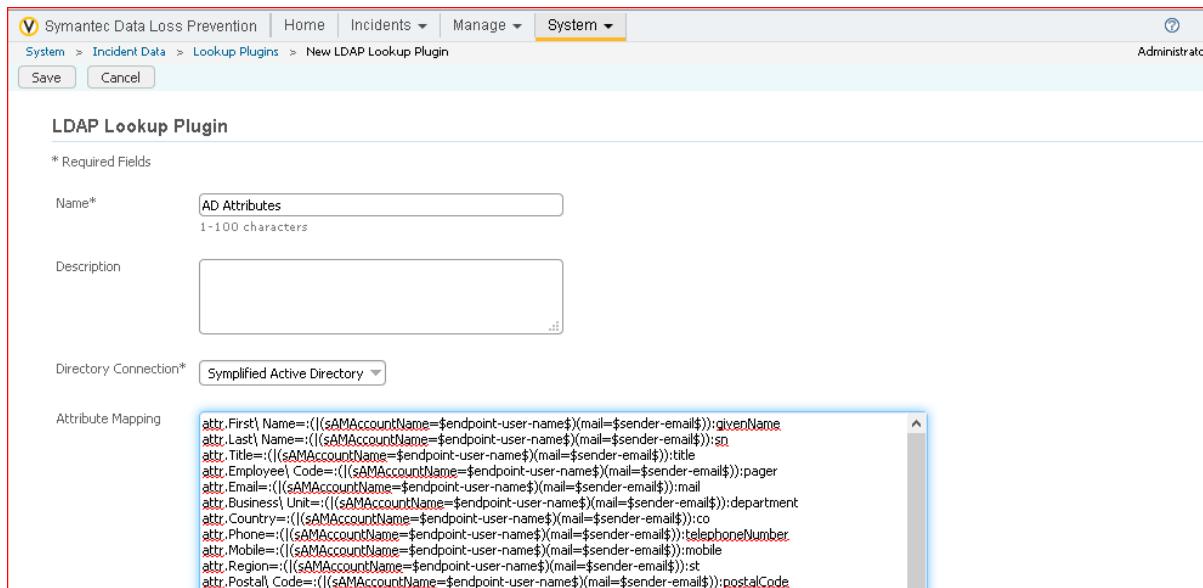
Not all the time data loss can be intentional sometimes it can be due to lack of awareness or carelessness so they should be educated for stopping the sensitive data loss. It basically describes about what actions are allowed and disallowed.

In this lab we will be configuring the policies such that notifications will be raised like you violated this policy. It basically gives us the policy and we

Exercise 1:

Configure the Active directory look up plugin:

Lookup plugins enable the DLP to import the data from the external sources and import into the incidents. Symplified would like to import the additional contextual data from the active directory into the new incidents that are created. This will allow the Enforce server to send notifications to the user and their manager automatically.



Adding the plugin

Modify Lookup Plugin Chain

If you change the sequence or on/off state of a plugin, the plugin chain will reload when you click save on this page.

Execution Sequence	Name	Type	Status	Dedicated Actions
1	AD Attributes	LDAP	Off	<input checked="" type="checkbox"/> On

We need to on the dedication actions.

Lookup Parameter Keys

<input type="checkbox"/> Attachment	View Properties
<input checked="" type="checkbox"/> Incident	View Properties
<input checked="" type="checkbox"/> Message	View Properties
<input type="checkbox"/> Policy	View Properties
<input type="checkbox"/> Recipient	View Properties
<input checked="" type="checkbox"/> Sender	View Properties
<input type="checkbox"/> Server or Detector	View Properties
<input type="checkbox"/> Monitor	View Properties
<input type="checkbox"/> Status	View Properties
<input type="checkbox"/> ACL	View Properties
<input type="checkbox"/> Cloud Applications and API Appliance	View Properties

We need to enable the incident,message and sender.

The Custom Attribute 'Phone' was saved successfully.

Name	Email Address	Display Order
First Name		[Down]
Last Name		[Up] [Down]
Email	Yes	[Up] [Down]
Phone		[Up]

Added the custom attributes.

The Custom Attribute 'Manager Phone' was saved successfully.

Name	Email Address	Display Order
First Name		[Down]
Last Name		[Up] [Down]
Email	Yes	[Up] [Down]
Phone		[Up]
Manager Info		
Manager First Name		[Down]
Manager Last Name		[Up] [Down]
Manager Email	Yes	[Up] [Down]
Manager Phone		[Up]

All the custom attributes were added.

Exercise 2:

Configure Email Notifications.

The name itself saying that when a user is violating the policy while using the outlook the user will get the notification to the email about the violation and also along with the user, the manager , and the infosec team will be receiving the notifications. In this lab we will discuss about how it is going to work.

Note: This is not the on screen notification or pop up notification. It sends the notification to the email.

This screenshot shows the 'Edit General Settings' page in the Symantec Data Loss Prevention interface. The 'System' tab is selected. The 'Reports and Alerts' section contains settings for distribution (radio buttons for 'Do not allow sending of reports and alerts', 'Send reports as links, login required to view', and 'Send report data with emails'), a 'Fully Qualified Manager Name' field set to 'Enforce.simplified.com' with a note about the format, and a checked 'Correlations' checkbox. The 'SMTP' section includes fields for 'Server' (enforce.simplified.com), 'System Email' (itsecurity@simplified.com), 'User ID' (itsecurity@simplified.com), and 'Password' (*****). A 'License' section is also present at the bottom.

Setting the smtp rules.

This screenshot shows the 'Configure Response Rule' page under 'Policies > Response Rules'. The 'General' section includes a 'Rule Name' field set to 'SMTP Notification' and a 'Description' field. A note states 'Used in no active policies.' The 'Conditions' section allows defining rules based on 'Incident Type' (Discover, Endpoint, Network) and 'Severity' (High, Medium, Low, Info). The 'Actions' section is currently empty, showing '<choose action type>'.

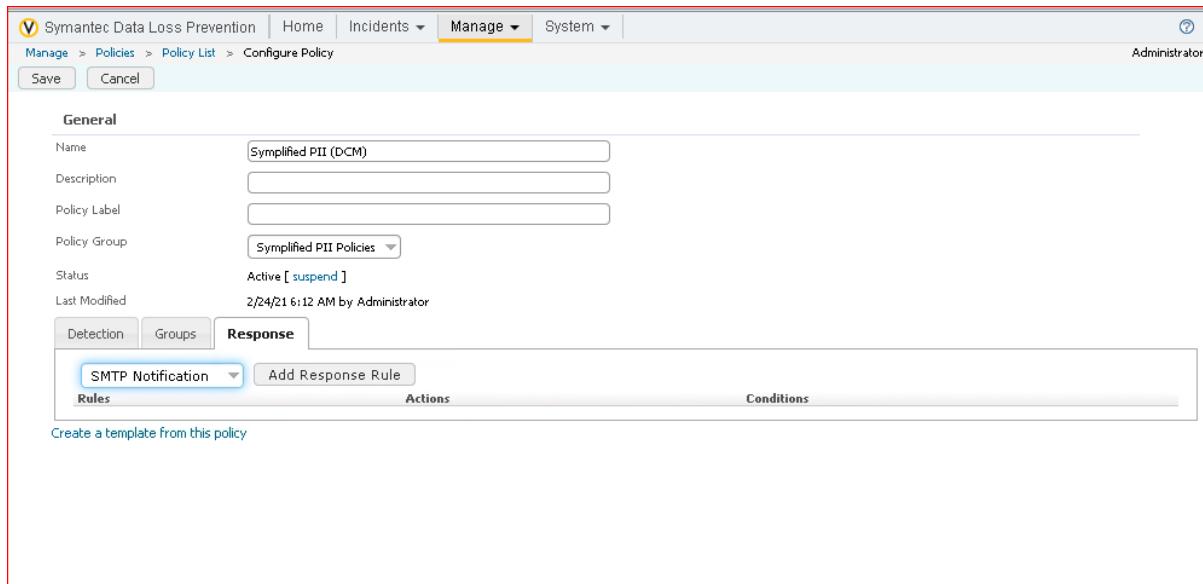
Creating the response rules.

The screenshot shows the Symantec Data Loss Prevention interface with the 'Manage' tab selected. Under 'Actions', 'Send Email Notification' is chosen. The configuration window for 'All: Send Email Notification' is displayed. It includes fields for 'To', 'Custom To', 'CC', 'Custom From', 'Notification Format' (HTML selected), 'Include Original Message' (unchecked), and 'Max Per Day'. Below this is the 'Notification Content' section, which shows the language set to 'English (India)' and the subject line 'email to \$RECIPIENTS\$ was monitored by Symplified IT Security'. The body of the email contains HTML code with placeholders like \$RECIPIENTS\$, \$SENDER\$, \$POLICY\$, etc. A tooltip for 'Insert Variable' lists various incident-related variables such as Application Name, Data Owner, and Incident ID.

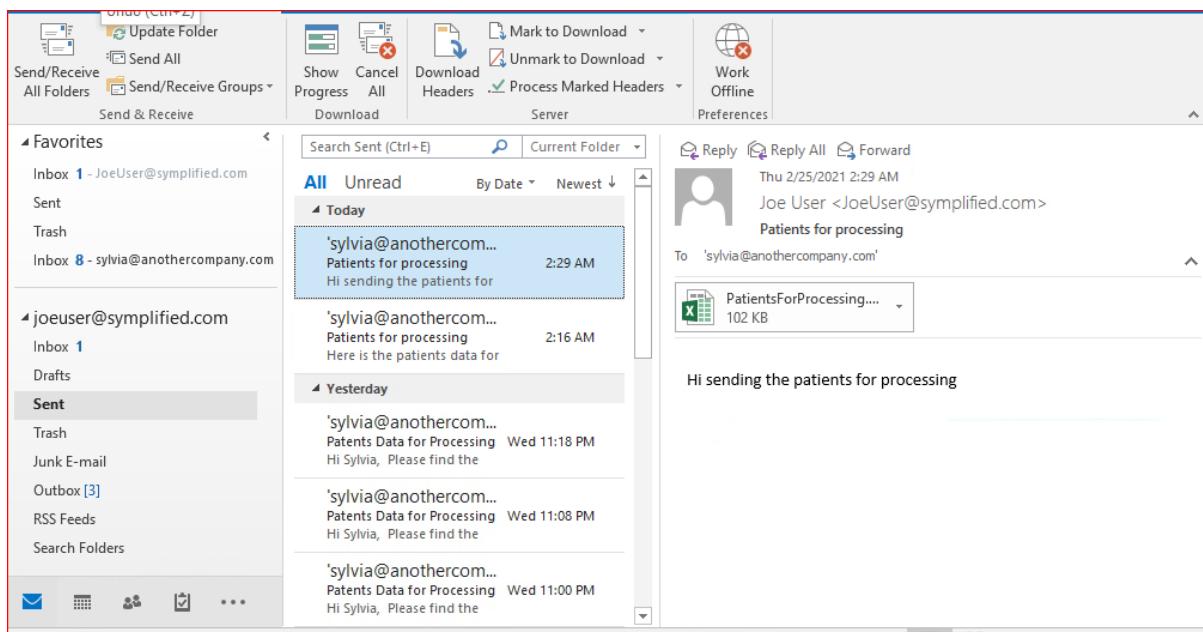
Adding the actions

This screenshot shows the same interface as above, but the 'Body' field of the 'Notification Content' section is expanded to show the full HTML message. The message includes a subject line and a detailed body paragraph explaining a violation, providing links for more details and contact information. The 'Insert Variable' tooltip is still visible on the right side of the screen.

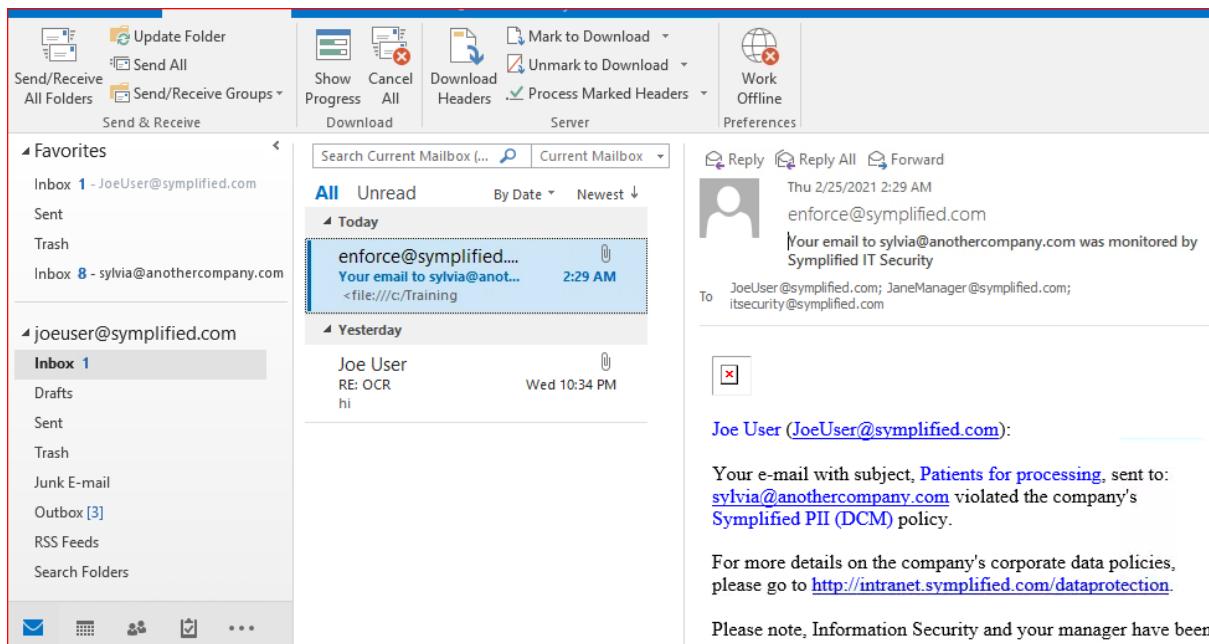
Adding the actions



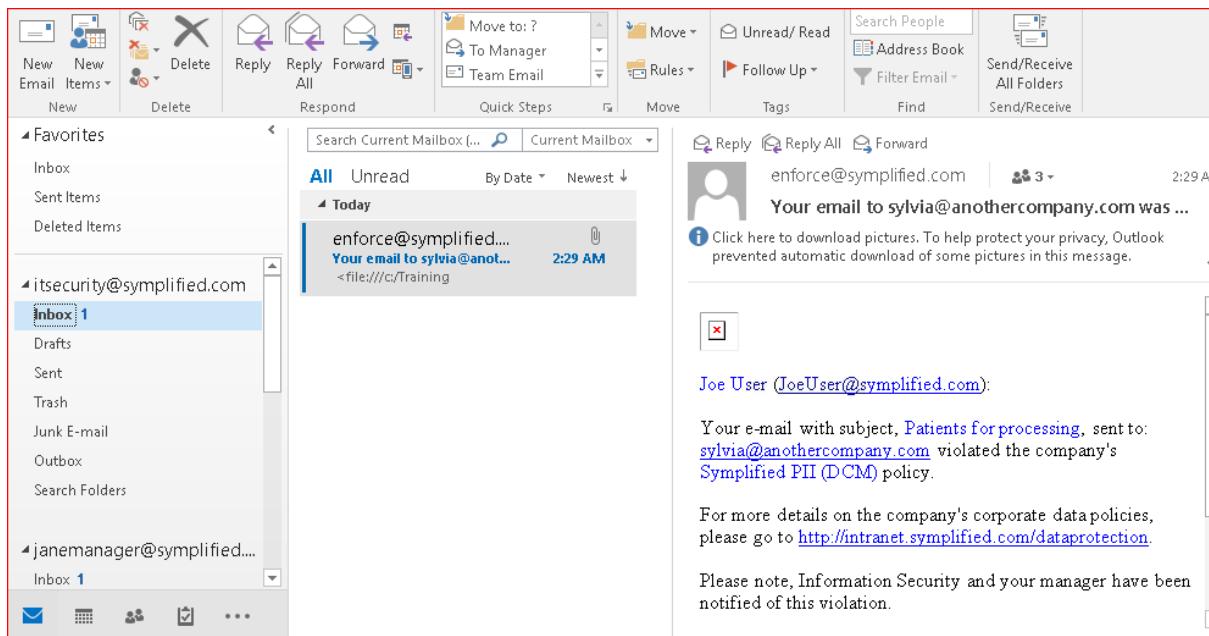
Adding the notification



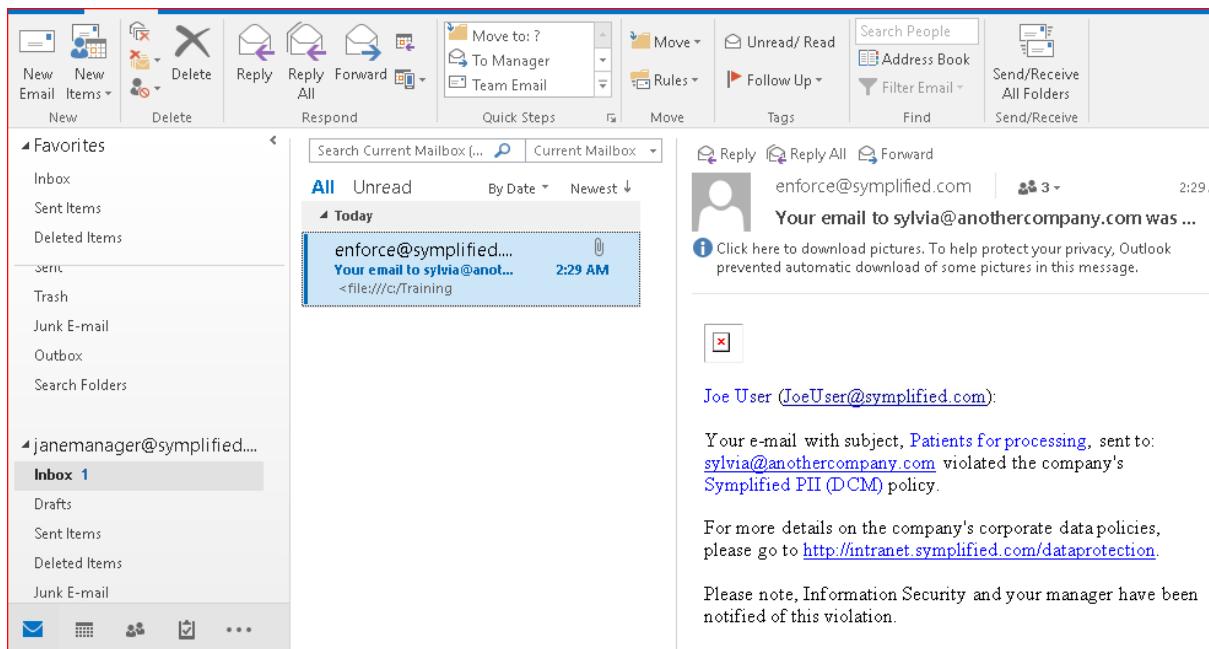
Email from joe is sent to the sylvia



This telling that joe got a mail like he violated the companies policy.



This describes that itsecurity department also got notification about joe violated the policy.



This described that jane who is manager also received about joe violated the policy.

In this way email notifications will be sent if the policy is violated.

Exercise 3:

Configure the on screen notifications.

This basically notifies about the sensitive data mis usage through direct pop up notifications.

The screenshot shows the 'Configure Response Rule' page under 'Manage > Policies > Response Rules'. The 'Rule Name' is set to 'Onscreen Notification'. Under 'Conditions', there are two dropdown menus: 'Incident Type' (set to 'Is Any Of' with 'Discover', 'Endpoint', and 'Network' selected) and 'Severity' (set to 'Is Any Of' with 'High', 'Medium', 'Low', and 'Info' selected). An 'Actions' section at the bottom is currently empty. A red border highlights the entire configuration area.

Configuring the response rules.

The screenshot shows the 'Endpoint Prevent: Notify' configuration dialog. It includes a 'Language' dropdown set to 'English (United States)', a message box containing a template for alert content, and several checkboxes for user interaction. On the right, there's an 'Insert Variable' panel listing items like Application, Content Name, Content Type, etc. A red border highlights the main configuration area.

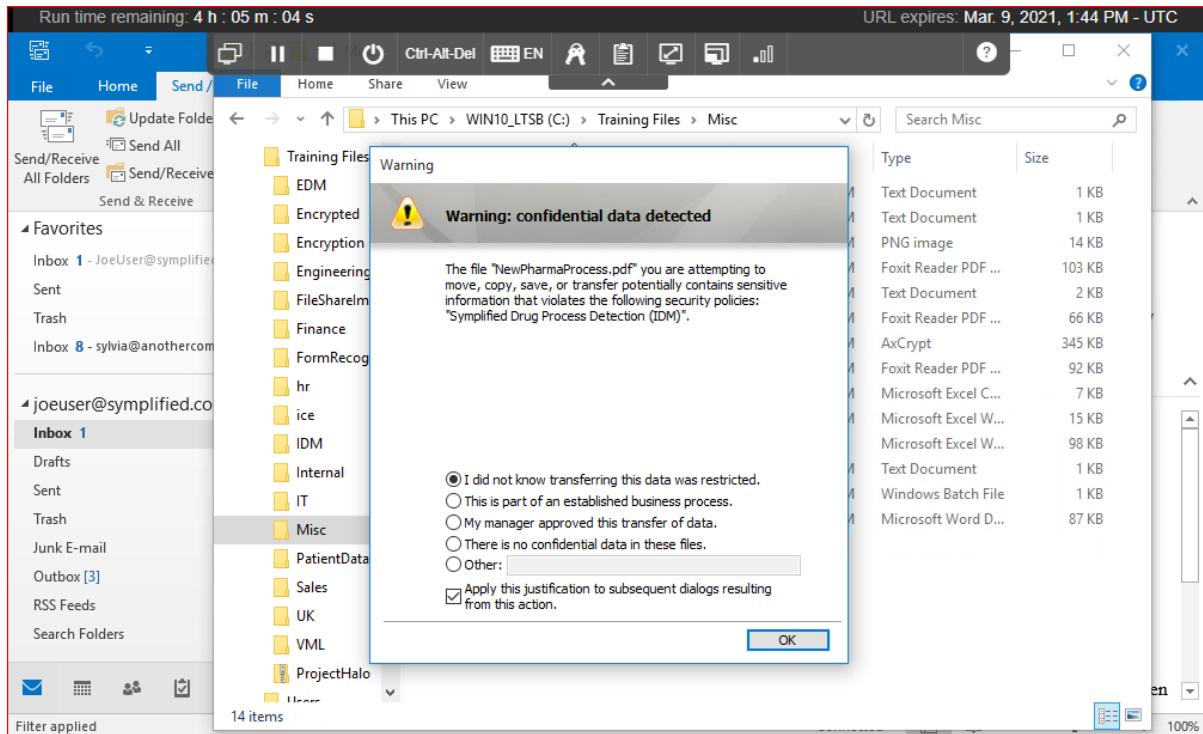
What should be notified is added here.

Order	Rule	Actions	Conditions
1	SMTP Notification	All: Send Email Notification	when Incident Type Is Any Of Network and Severity Is Any Of High, Medium, Low
2	Onscreen Notification	Endpoint Prevent: Notify	when Severity Is Any Of High, Medium, Low and Incident Type Is Any Of Endpoint

Overview of the response rules.

Rules	Actions	Conditions
Onscreen Notification	Endpoint Prevent: Notify	when Severity Is Any Of High, Medium, Low and Incident Type Is Any Of Endpoint

Added the onscreen notification.



When iam trying to encrypt the data its giving the notification.

Symantec Data Loss Prevention | Home | Incidents | Manage | System | Administrator

Incidents > Endpoint > Incidents - New

Close Save Send Export Delete Report

Filter

Status: Equals New
Date: Last 30 Days

Severity:
 High Low
 Medium Info

Advanced Filters & Summarization

Applied Filters

Status Equals New	Date Last 30 Days	Severity Is Any Of High (12), Medium (0), Low (1), Info (0)			
[Show / hide filters] 1-13 of 13					
Type	Destination / Machine / User	Occurred On	ID / Policy	Matches	Severity
<input type="checkbox"/>	File Name Machine User	2/25/21 2:45 AM	00000426 Simplified Drug Process Detection (IDM)	1	High
<input type="checkbox"/>	Machine User Subject Recipient	2/25/21 2:28 AM	00000425 Simplified PII (DCM)	300	Medium
<input type="checkbox"/>	Machine User Subject Recipient	2/25/21 2:28 AM	00000422 Simplified PCI (EDM/DCM)	100	Low
<input type="checkbox"/>	Machine User	2/25/21 2:28 AM	00000421 Simplified PCI (EDM/DCM)	79	Info

Endpoint Reports

- Exec. Summary - Endpoint
- Incidents - All
- Incidents - New**
- Policy Summary
- Incident Status Summary
- Highest Offenders
- Endpoint Location Summary

We can clearly see that incident at the endpoint is captured.

The screenshot shows a Symplified platform interface for managing incidents. On the left, the 'Incident Details' panel displays information about 'Incident 00000426'. It includes fields for 'Status' (New), 'Severity' (High), and 'Endpoint Application File Access' (Key Info, History, Notes, Correlations). The 'Policy Matches' section shows a single match for 'Simplifed Drug Process Detection (IDM)'. In the 'Matches' column, it lists 'Simplifed Drug Process Detection (IDM)' with 1 match and 'Drug Process Detection (IDM)' with 1 match. The 'Incident Details' section shows the following data:

Server or Detector	Simplifed Detection Server
Agent Response	User Notified
Occurred On	2/25/21 2:45 AM
Reported On	2/25/21 2:46 AM
Is Hidden	No [Do Not Hide]
User	SYMPPLIED\joe_user
User Justification	User Education : "I did not know transferring this data was restricted."

The right side of the interface shows the 'Matches (matches found in 1 component)' and 'Attributes' sections. The 'Matches' section lists a single match for 'C:\ProgramData\Symantec\...\\NewPharmaProcess.pdf' from 'Drug Process Documents matched exactly'. The 'Attributes' section contains two groups: 'Employee Info' and 'Manager Info', with the following data:

Employee Info	First Name: Joe Last Name: User Email: JoeUser@sympified.com Phone: 123-456-7890
Manager Info	Manager First Name: Jane Manager Last Name: Manager Manager Email: JaneManager@sympified.com Manager Phone: 1235551234

We can clearly see that in the incident details its showing the user was notified while encrypting the data and along with that its saying that user was responded like “I did not know tranfering this data was restricted”

Lab 5:

Preventing unauthorized exposure of confidential data.

There are no of tools In order to prevent the sensitive data to be leaked.

In this lab we will configure the appropriate responses to policies violations, including blocking , quarantaine and user notification. Also we gonna detect some of the advanced detection techniques like OCR that can find the sensitive data that has been converted to an image. Main concentration in on the data at rest even before becoming into data in motion.

Exercise 1:

Configure SMTP blocking.

Till now we seen notifications to the email, pop-up notifications when the policy is violated but in this we will try to block the data from being sending if there is any policy violated immediately the data will be blocked and it won't send to the recipient.

In this lab we will configure the smtp blocking i.e., when an sensitive data is sending through the mail it will be blocked before sending to the recipient.

The screenshot shows the Symantec Data Loss Prevention interface under the 'Manage' tab. The current page is 'Configure Response Rule'. The rule is named 'SMTP Block & Notify'. It is set to use in the 'Simplified PII (DCM)' active policy. The 'Conditions' section contains two conditions: 'Severity' set to 'Is Any Of' with options 'High', 'Medium', 'Low', and 'Info' (with 'High' selected); and 'Incident Type' set to 'Is Any Of' with options 'Discover', 'Endpoint', and 'Network' (with 'Network' selected). The 'Actions' section is currently empty, showing '<choose action type>' and an 'Add Action' button.

Configuring the response rules

The screenshot shows two windows from the Symantec Data Loss Prevention interface.

Network Prevent: Block SMTP Message

- Bounce Message to Sender: (Leave blank to not bounce message to Sender)
- Redirect Message to this Address: itsecurity@sympified.com

All: Send Email Notification

- To: Data Owner (email address) Sender (SMTP Incidents Only) Manager Email Email
- Custom To: itsecurity@sympified.com
- CC:
- Custom From: enforce@sympified.com
- Notification Format: HTML Plain Text

Configuring the response rules

The screenshot shows the 'Notification Content' configuration window.

Notification Content

Language: English (India)

Subject: Your email to \$RECIPIENTS\$ was blocked by Sympified IT Secu

Body:

```
<html>
<body>

<br>
<br>
<font color="blue">$First Name$ $Last Name$</font>
(<font color="blue">$SENDER$</font>);
<br>
<br>
Your e-mail with subject, <font
color="blue">$SUBJECT$</font>, was blocked from going
to <font color="blue">$RECIPIENTS$</font> because it
violated the company's <font color="blue">$POLICY$</font>
policy.
<br>
<br>
For more details on the company's corporate data policies,
please go to <a href="http://intranet.sympified.com
/dataprotection">http://intranet.sympified.com
/dataprotection</a>.
<br>
<br>
Please note, Information Security will be sent a notification
that this e-mail was sent, and the incident will be reviewed.
<br>
<br>
Please feel free to contact Information Security at
```

Add Language

Insert Variable

- Application Name
- Application User
- Attachment File Name
- Blocked
- Data Owner
- Data Owner Email
- Destination IP
- Device Instance ID
- Endpoint Location
- Endpoint Machine
- Endpoint Username
- File Full Path
- File Name
- File Parent Directory Path
- Incident ID
- Incident Snapshot
- Machine IP
- Match Count
- Occurred On
- Policy Name
- Policy Rules
- Protocol / Device Type / Target Type
- Quarantine Parent Directory Path
- Recipients
- Reported On
- Scan Date
- Sender
- Server or Detector
- Severity
- Status

Configuring the response rules.

The screenshot shows the Symantec Data Loss Prevention web interface. In the top navigation bar, the URL is https://enforce.symplified.com/ProtectManager/UpdateSaveResponseRule. The main content area displays a success message: "The response rule 'SMTP Block & Notify' was saved successfully." Below this, there is a table listing two response rules:

Order	Rule	Actions	Conditions
1	SMTP Block & Notify	Network Prevent: Block SMTP Message All: Send Email Notification	when Incident Type Is Any Of Network and Severity Is Any Of High, Medium, Low
2	Onscreen Notification	Endpoint Prevent: Notify	when Severity Is Any Of High, Medium, Low and Incident Type Is Any Of Endpoint

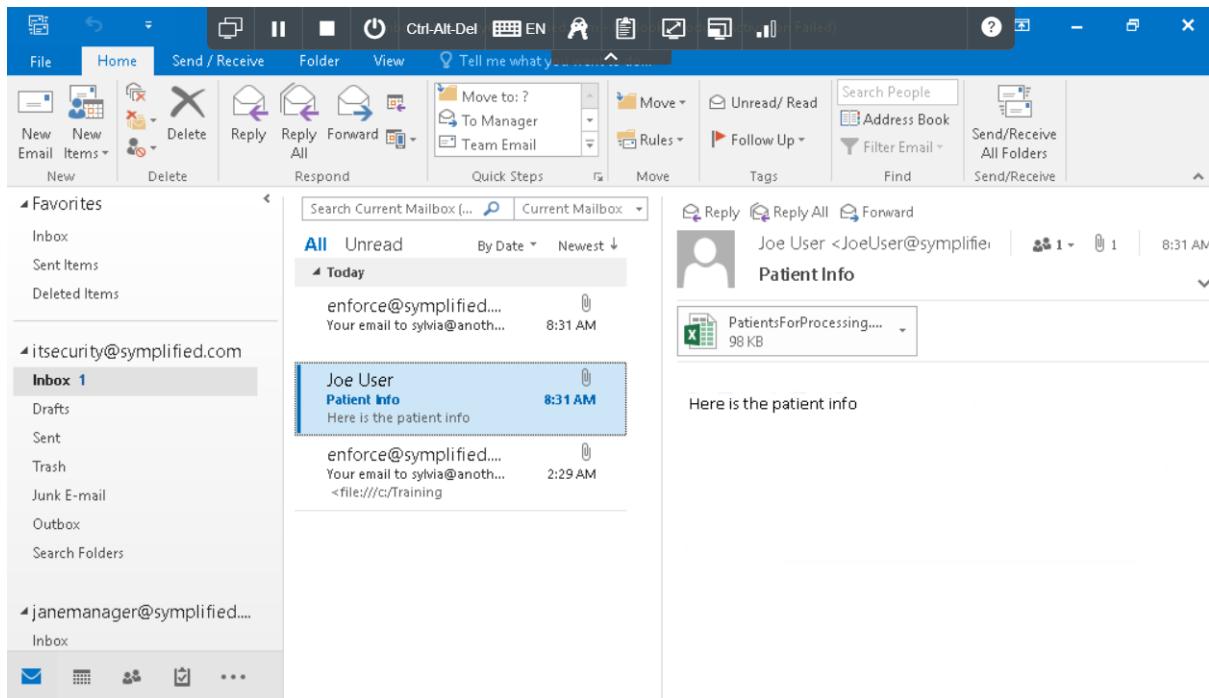
Proof that response rule is added.

The screenshot shows the Microsoft Outlook inbox for the user JoeUser@symplified.com. The subject of the highlighted email is "Your email to sylvia@anothercompany.com". The email body contains the message: "Your email to sylvia@anothercompany.com was blocked by Symplified IT Security". The "From" field is enfore@symplified.com. The "To" field lists JoeUser@symplified.com, JaneManager@symplified.com, and itsecurity@symplified.com. A note at the bottom of the email states: "Joe User (JoeUser@symplified.com): Your e-mail with subject, Patient Info, was blocked from going to [sylvia@anothercompany.com](#) because it violated the company's Symplified PII (DCM) policy. For more details on the company's corporate data policies, please go to <http://intranet.symplified.com/dataprotection>. Please note, Information Security will be sent a notification that this e-mail was sent, and the incident will be reviewed. Please feel free to contact Information Security at 212-555-".

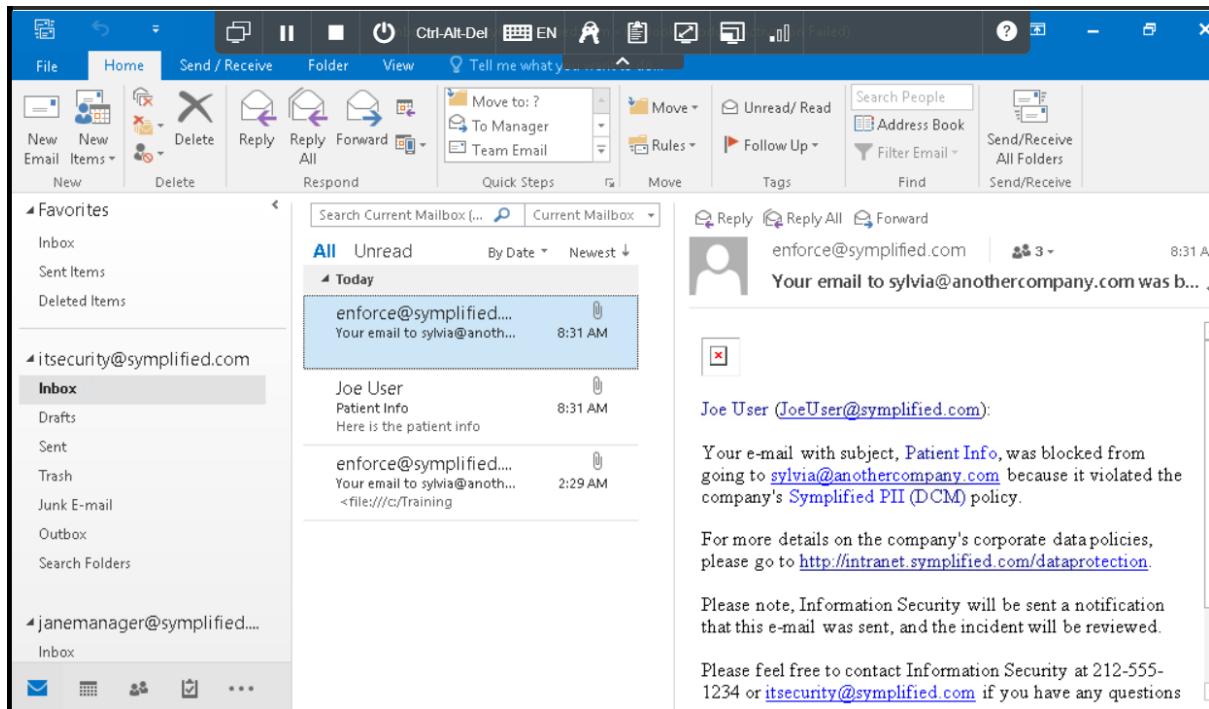
When iam trying to send the mail from joe to sylvia its clearly saying that it was blocked.

Vinay Kumar Reddy Donda

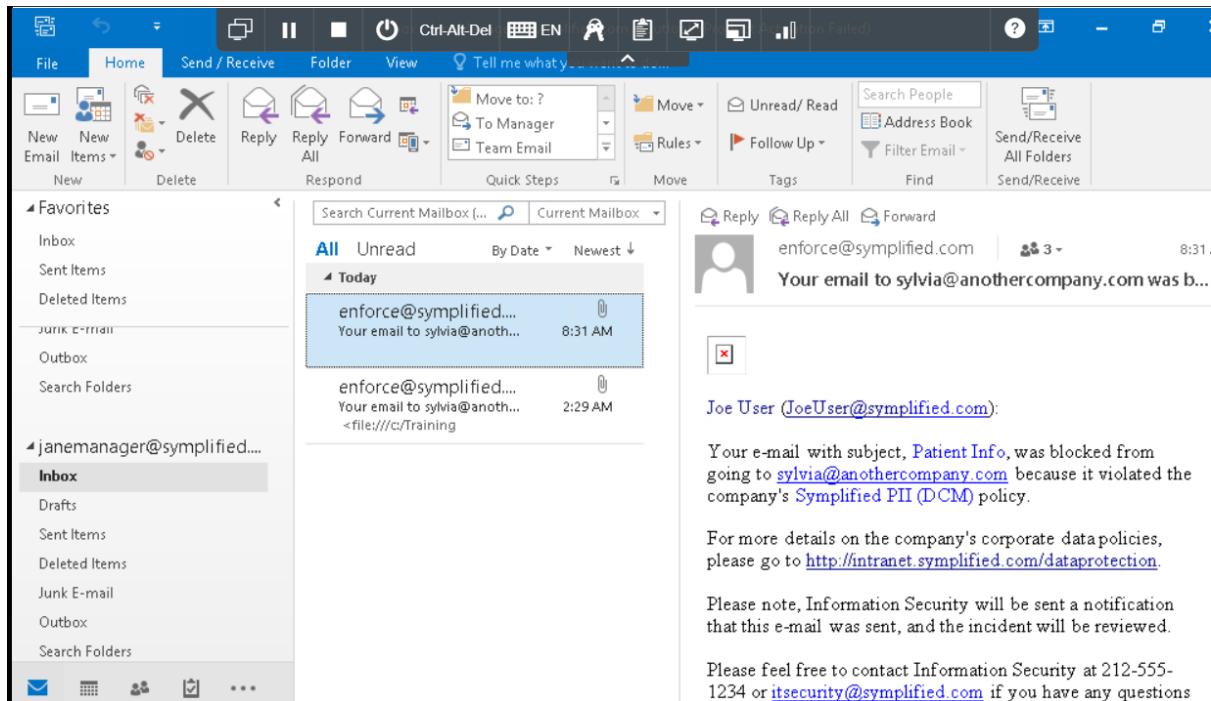
dondavinayreddy@gmail.com



Here is the proof like it security department received the blocked mail



Here is the proof that itsecurity team also received the notification.



Here is the proof that jane manager also received the notification mail.

The screenshot shows the Symantec Data Loss Prevention 'Incidents' screen. An incident titled 'Incident 00000427' is displayed. Under 'Policy Matches', it shows a 'Symplified PII (DCM)' policy violation for 'US Social Security Numbers (Data Identifiers)'. The 'Matches' section lists several names and their associated PII numbers. On the right, 'Attributes' for 'Employee Info' and 'Manager Info' are shown, both belonging to 'Joe' and 'Jane' respectively. A watermark for 'Snipping Tool' is visible at the bottom.

Here is the proof that the incident is raised in the network and red mark indicating that message is blocked.

The screenshot shows the Symantec Data Loss Prevention interface. The main title bar says "Symantec Data Loss Prevention". Below it, the navigation path is "Incidents > Network > Incidents - New > Network Incident Snapshot". The top right has "Administrator" and "Customize Layout" buttons.

The main content area shows an "Incident 00000427" with a red error icon. The status is "New" and the severity is "High". There are tabs for "Key Info", "History", "Notes", and "Correlations". The "History" tab is selected, showing three entries:

- 2/25/21 8:30 Administrator AM: **Notification Sent**. Incident notification sent to JoeUser@symplyfied.com, JaneManager@symplyfied.com, itssecurity@symplyfied.com.
- 2/25/21 8:30 Administrator AM: **Attribute Lookup Completed**. First Name=Joe Manager First Name=Jane Last Name=User Manager Last Name=Manager Manager Email=JaneManager@symplyfied.com Email=JoeUser@symplyfied.com Phone=123-456-7890 Manager Phone=1235551234
- 2/25/21 8:30 Administrator AM: **Attribute Lookup Requested**

To the right, there's a sidebar titled "Matches (matches found in 1 component)" which lists several entries from a file named "PatientsForProcessing.xlsx". The sidebar also contains sections for "Employee Info" and "Manager Info" with their respective details.

History tab shows us the incident related to that which occurred earlier.

Exercise 2:

Testing Optical character recognition(OCR) and “HIPAA and HITECH (including PHI)” Policy.

Symplified is testing a new policy for its US offices along with an additional Symantec DLP feature. They have created a test policy called “HIPAA and HITECH(including PHI),” based on Symantec DLP policy template, that looks for combinations of medical keywords and USsocial security numbers. The simplified DLp administrators have also installed a Symantec DLP OCR server for testing and have configured one of their detection servers to send OCR-amenable iamges to the OCR server for text extraction. They are noew going to run a tes of this setup.

Note: Since this lab is associated with the OCR configuration as we are unable to create the OCR policy we cannot proceed with this exercise so iam skipping this part.

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes 'Symantec Data Loss Prevention' logo, 'Home', 'Incidents', 'Manage', and 'System' (which is selected). Below the navigation is a 'General' configuration section with fields for 'Name' (set to 'Symplified Detection Server'), 'Host' (set to '127.0.0.1'), and 'Port' (set to '8100'). A 'Save' and 'Cancel' button are at the bottom of this section. Below this is a header 'Symantec Encryption Server Administration'. Underneath are tabs: 'Discover' (selected), 'ICAP', 'Inline SMTP', 'Packet Capture', 'SMTP Copy Rule', 'Agent', and 'Detection'. The 'Discover' tab has a 'Maximum Parallel Scans' field set to '1'. Under 'ICE Proxy Settings', it says 'Detection server needs to be recycled for the changes to take effect' and shows two radio buttons: 'No Proxy or Transparent Proxy' (selected) and 'Manual Proxy'.

Since there is no OCR engine

Exercise 3:

Configure Endpoint blocking.

Blocking the sensitive data at the end is the best option if an endpoint user is unable to handle the sensitive data properly we need to block the data at the endpoint.

The screenshot shows the Symantec Data Loss Prevention Agent Configuration interface. The 'Name' field is set to 'Simplified Agent Configuration'. The 'Description' field is empty. The 'Channels' tab is selected. In the 'Enable Monitoring' section, the 'HTTP' checkbox under the 'Web' section is checked. Other checkboxes for various monitoring channels like 'Clipboard', 'Email', and 'Network Shares' are also present but not checked.

Http is checked in the web.

The screenshot shows the Symantec ProtectManager interface for configuring response rules. The 'Rule Name' is 'Block User Action'. The 'Conditions' section shows two conditions: 'Incident Type' set to 'Discover Endpoint Network' and 'Severity' set to 'High'. The 'Actions' section is currently empty, with a placeholder 'choose action type'.

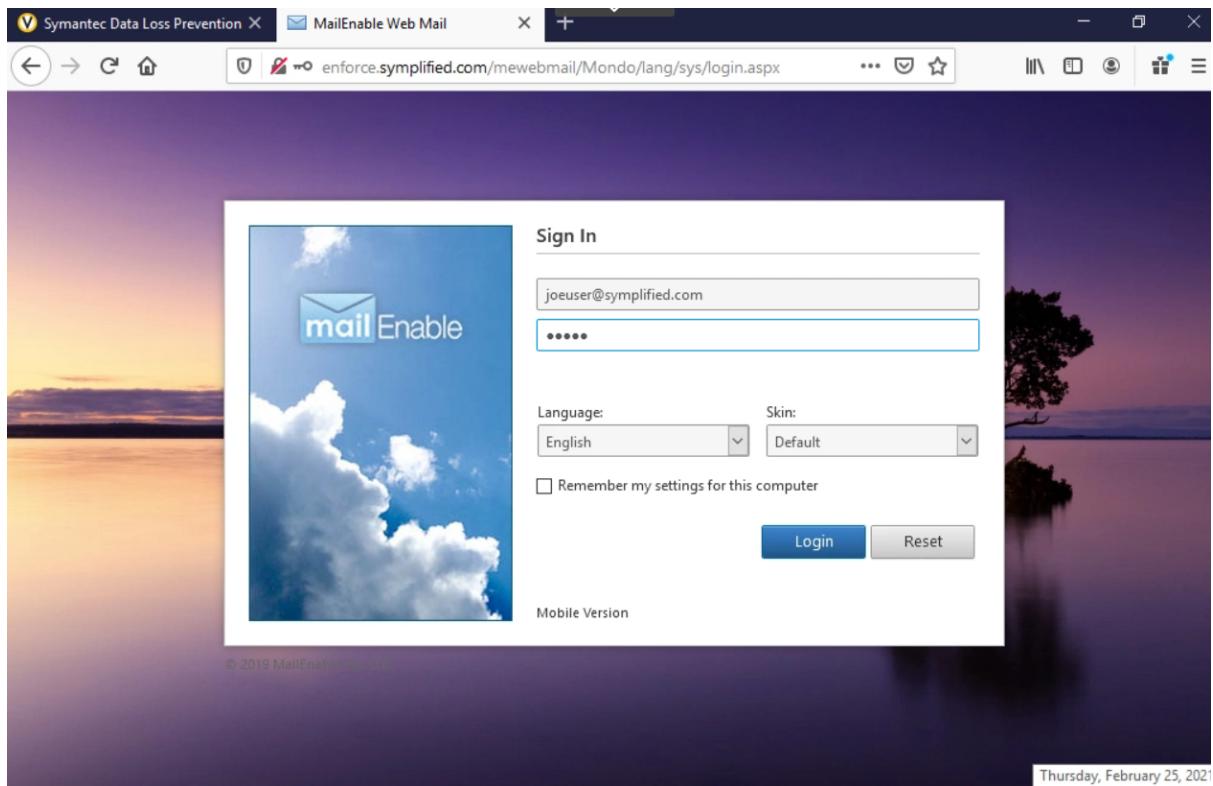
Configuring the response rules

The screenshot shows the Symantec Data Loss Prevention interface under the 'Manage' tab. A modal window titled 'Endpoint Prevent: Block' is open. It contains settings for 'Endpoint Notification Content' in English (United States). It includes a message box for alerting users about policy violations, a section for user explanations with four options ('User Education', 'Broken Business Process', 'Manager Approved', 'False Positive'), and a checkbox for allowing users to enter their own text explanations. An 'Insert Variable' dropdown menu is visible on the right.

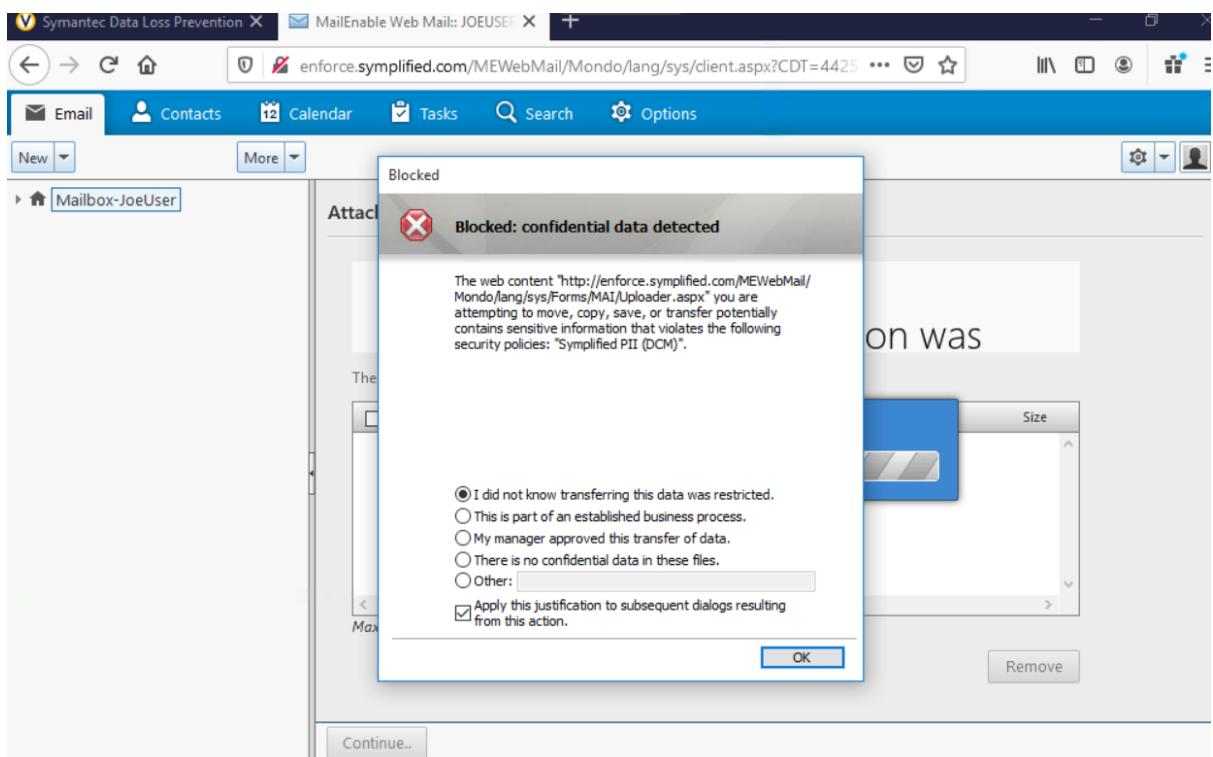
Configuring the action upon the policy violation

The screenshot shows the 'Configure Policy' screen for a policy named 'Simplified PII (DCM)'. The 'Response' tab is selected. Under the 'Rules' section, there are two entries: 'SMTP Block & Notify' (Action: 'Network Prevent: Block SMTP Message All: Send Email Notification') and 'Block User Action' (Action: 'Endpoint Prevent: Block'). The 'Conditions' column specifies conditions for each rule. Below the rules, there is a link to 'Create a template from this policy'.

Blocking the user action by changing it in the response tab.



Accessing the web mail.



We can clearly see that it is blocking the sensitive data from sending.

Symantec Data Loss Prevention - Incident Reports

Applied Filters:

- Status: Equals New
- Date: Last 30 Days
- Severity: Is Any Of High (19), Medium (0), Low (1), Info (0)

Type	Destination / Machine / User	Occurred On	ID / Policy	Matches	Severity
Machine User Recipient	ENDPOINT SYMLIFIED\joe_user http://enforce.simplified.com/MEWebMail/Mondo/lang/sys/Forms/MAI/Uploader.aspx	2/25/21 9:40 AM	00000435 Simplified PII (DCM)	300	High
Machine User Recipient	ENDPOINT SYMLIFIED\joe_user http://enforce.simplified.com/MEWebMail/Mondo/lang/sys/Forms/MAI/Uploader.aspx	2/25/21 9:40 AM	00000434 Simplified PCI (EDM/DCM)	79	Medium
Machine User Recipient	ENDPOINT SYMLIFIED\joe_user http://enforce.simplified.com/MEWebMail/Mondo/lang/sys/Forms/MAI/Uploader.aspx	2/25/21 9:40 AM	00000433 Simplified PCI (EDM/DCM)	100	High
Machine User Recipient	ENDPOINT SYMLIFIED\joe_user http://enforce.simplified.com/mewebmail/Mondo/lang/sys/login.aspx	2/25/21 9:38 AM	00000432 Simplified Source Code Detection (VML)	1	Medium
Machine	ENDPOINT	2/25/21 8:30 AM	00000431	300	High

Incident raised at the endpoint.

Incident 00000435

Endpoint HTTP

Policy Matches

- Simplified PII (DCM) [view policy]: 300 matches
- US Social Security Numbers (Data Identifiers): 300 matches

Incident Details

Server or Detector	Simplified Detection Server
Agent Response	Action Blocked
Occurred On	2/25/21 9:40 AM
Reported On	2/25/21 9:40 AM
Is Hidden	No [Do Not Hide]
User	SYMLIFIED\joe_user
User Justification	User Education : "I did not know transferring this data was restricted."
Machine Name	FNPOINT

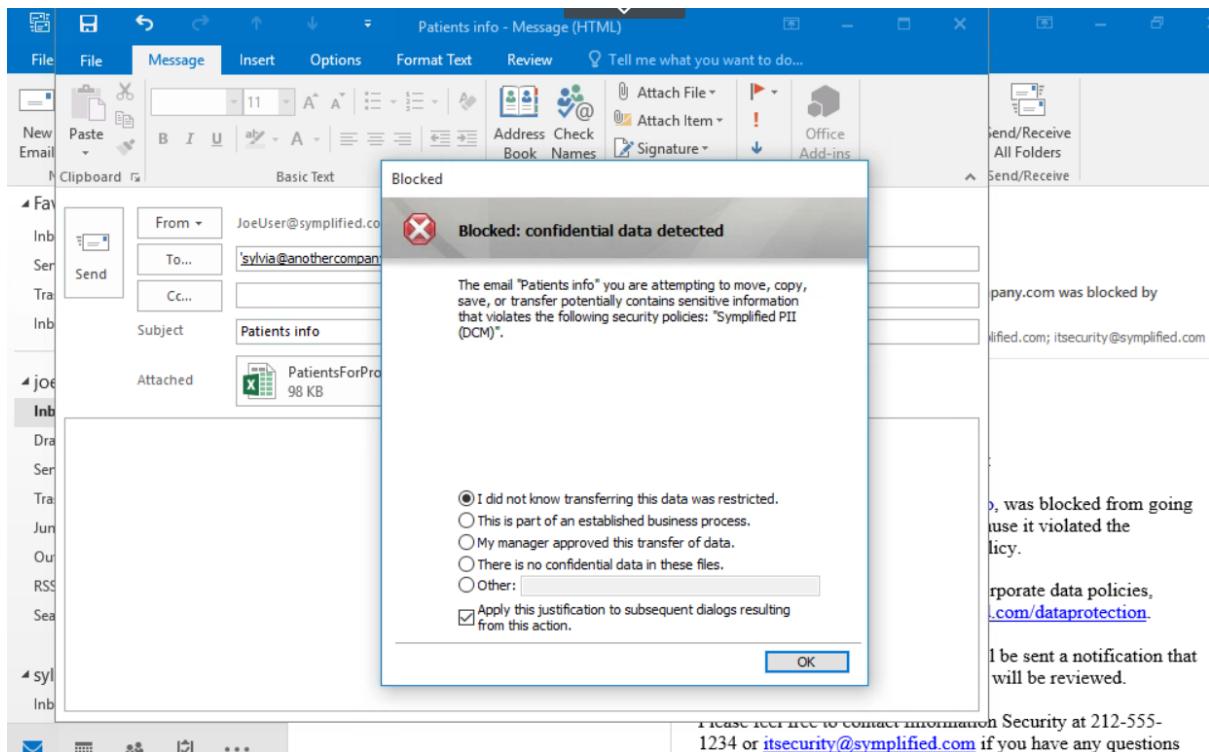
Matches (matches found in 1 component)

- PatientsForProcessing.xlsx (300 Matches):
 - ... 420-08-3530 30809 RAUL PASHAL 4684451986499930 8000898233 pashal_63588...om (930)750-0791 53395-9820 d0TeNx8jCB 650-22-0893 30811 ORA LEISURE 4132673384929420 G00698233 leisure_1100...om (293)561-7807 29795-8233 ZEUDkPkn 561-97-2514 30812 JAMES HINTZ 4803331697819540 D00451340 hintz_668208...om (714)803-9738 03706-1340 keLcStti 203-36-9293 30813 GOLDIE PURVIS 4409094843938080 E00907590 purvis_14463...om (693)473-0722 15222-7590 HwbwUgKqD 373-18-2660 30814 SUSAN WILLIAMS 4083121379497770 E00623438 williams_841...rg (503)627-1556 54724-8334 klsvmSnob 627-12-9288 30817 DANIEL SMITH 4718214769659850 F00557274 smith_491395...om (288)878-2616 52330-7274 vjhgstGean 178-52-6151 30818 HAZEL HANSEN 483619583600...

Attributes

Employee Info	First Name: Joe Last Name: User Email: JoeUser@simplified.com Phone: 123-456-7890
Manager Info	Manager First Name: Jane Manager Last Name: Manager Manager Email: JaneManager@simplified.com Manager Phone: 1235551234

In detail info about the incident red dot indicates that mail was not sent.



I tried sending the mail from outlook app as well the same error has occurred and its blocking the sensitive data from sending to the recipient.

Exercise 4:

Configure end point user cancel

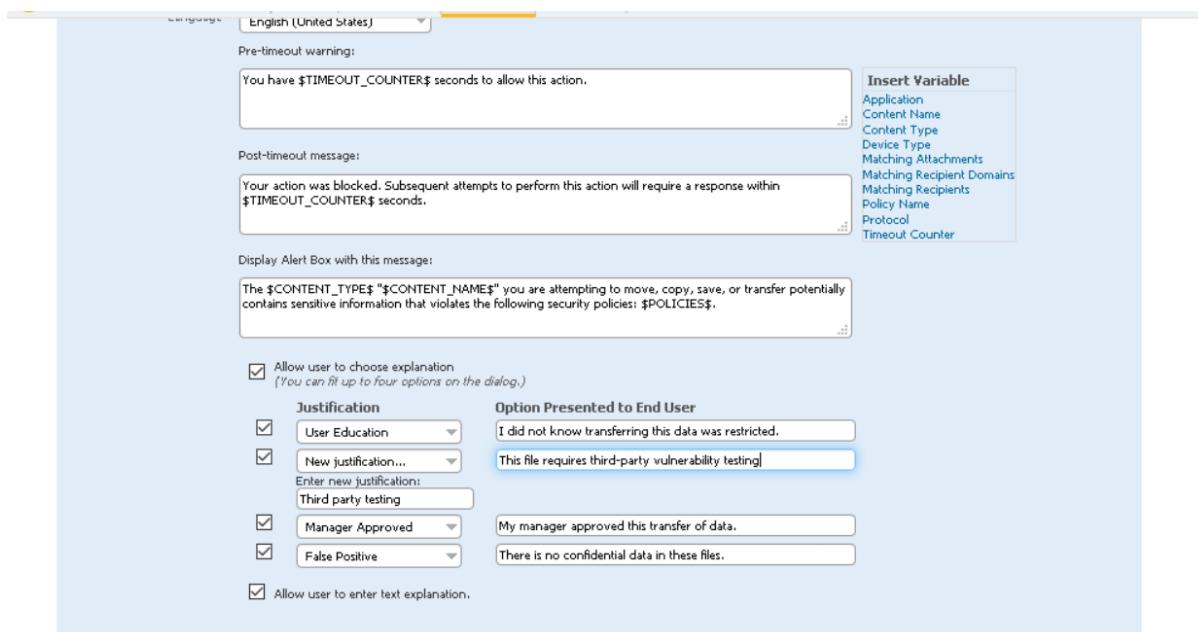
Simplified employees working on new project and they are supposed to check in all code to the git repository. Actually the rules are like no source code should be stored on network drive but there are some instances when a file needs to be stored on a network share for vulnerability testing by a third party. In that case before allowing a file to be copied to the network share, simplified has chosen to block any project halo files but allow the user to consciously decide if the copying is the right action.

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes links for Home, Incidents, Manage, and System. The 'System' tab is currently selected. Below the navigation is a toolbar with Save and Cancel buttons. A search bar is present, followed by a 'Description' input field. The main content area has tabs for Channels, Channel Filters, Application Monitoring, Device Control, Settings, and Advanced Settings. The 'Channels' tab is active. Under 'Enable Monitoring', there is a checkbox for 'Enable different monitoring settings for endpoints located on and off the corporate network'. The 'Destinations' section lists Removable Storage, CD/DVD, Local drive, and Printer/Fax. The 'Clipboard' section has checkboxes for Copy and Paste. The 'Email' section includes Outlook and Lotus Notes. The 'Web' section lists IE (HTTPS), Edge (HTTPS), Firefox (HTTPS), Chrome (HTTPS), Safari (HTTPS), HTTP, and FTP. The 'Configured Applications' section includes Application File Access and Cloud Storage. The 'Network Shares' section has checkboxes for Copy to Local Drive and Copy to Share. The 'SEP Integration' section has a checkbox for SEP Intensive Protection.

Enabled copy to share in network shares.

The screenshot shows the Symantec Data Loss Prevention interface under the 'Manage' tab. The path 'Manage > Policies > Response Rules > Configure Response Rule' is visible. The 'User Cancel' rule is selected. The 'General' tab shows the rule name 'User Cancel' and a note that it is not used in any active policies. The 'Conditions' tab is active, showing a dropdown menu for 'Protocol or Endpoint Monitoring' set to 'Is Any Of'. The dropdown list contains several options: Endpoint Application File Access, Endpoint CD/DVD, Endpoint Clipboard, Endpoint Cloud Storage, Endpoint Copy to Network Share (which is highlighted in blue), and Endpoint Local Drive. The 'Actions' tab shows a dropdown menu set to '<choose action type>' and an 'Add Action' button. A note at the bottom states: 'Response actions will be executed in order they appear below. Please choose one or more actions for this rule.'

Configuring the response rules



Configuring the rules

The screenshot shows the "Configure Policy" screen for a policy named "Simplified Source Code Detection (VML)".

General tab settings:

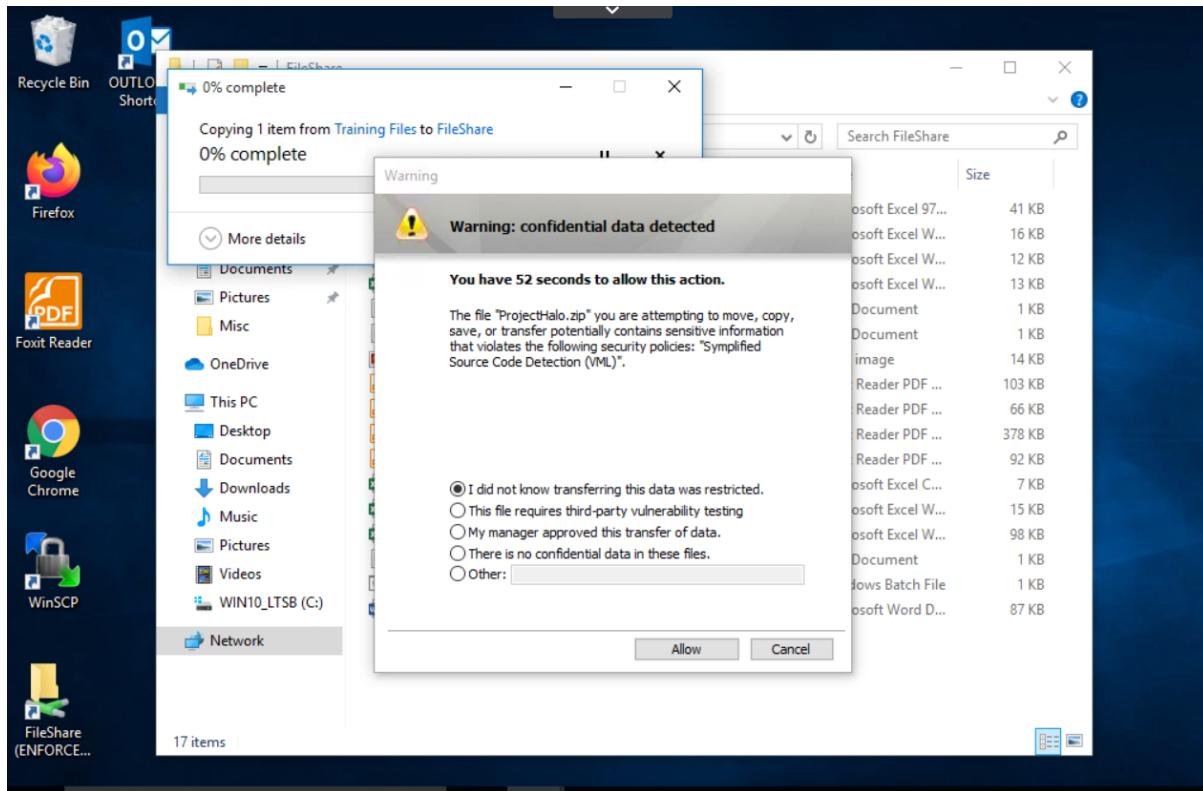
- Name: Simplified Source Code Detection (VML)
- Description: (empty)
- Policy Label: (empty)
- Policy Group: Default Policy Group
- Status: Active [suspend]
- Last Modified: 2/23/21 5:08 PM by Administrator

Response tab settings:

Rules	Actions	Conditions
User Cancel	Endpoint Prevent: User Cancel	when Protocol or Endpoint Monitoring Is Any Of Endpoint Copy to Network Share

Note: Create a template from this policy.

Configuring the policy



A warning is getting while copying the data and after selecting the appropriate reason it will copy

Type	Destination / Machine / User	Occurred On	ID / Policy	Matches	Severity Stat
File Name	ProjectHalo.zip Machine User SYMLIFIED\joe_user	2/25/21 10:12 AM	00000442 Simplified Source Code Detection (VML)	8	High
Machine	ENDPOINT SYMLIFIED\joe_user Patients info sylvia@anothercompany.com	2/25/21 9:44 AM	00000441 Simplified PCI (EDM/DCM)	100	Medium
Machine	ENDPOINT SYMLIFIED\joe_user Patients info sylvia@anothercompany.com	2/25/21 9:44 AM	00000440 Simplified PII (DCM)	300	Medium
Machine	ENDPOINT SYMLIFIED\joe_user Patients info sylvia@anothercompany.com	2/25/21 9:44 AM	00000439 Simplified PCI (EDM/DCM)	79	Medium

Incident is risen at the endpoint

The screenshot shows the Symantec Data Loss Prevention interface. The top navigation bar includes Home, Incidents (selected), Manage, and System. Below the navigation is a breadcrumb trail: Incidents > Endpoint > Incidents - New > Endpoint Incident Snapshot. The main content area displays an incident titled "Incident 00000442". The incident status is "New" and severity is "High". A section titled "Endpoint Copy to Network Share" is shown. The "Policy Matches" section lists "Simplified Source Code Detection (VML)" with 8 matches and "Source Code Detection (Vector Machine Learning)" with 8 matches. The "Incident Details" section provides information such as the server or detector ("Simplified Detection Server"), agent response ("User Notified, User: Allowed"), occurrence time ("2/25/21 10:12 AM"), reporting time ("2/25/21 10:12 AM"), and visibility ("No [Do Not Hide]"). A note from a user ("SYMPIFIED\\joe_user") states: "Third Party Testing : This file requires third-party classification vulnerability testing". The right side of the screen shows "Matches (matches found in 8 components)" and "Attributes" sections, which include employee and manager information.

Employee Info	Attributes
First Name	Joe
Last Name	User
Email	JoeUser@s...
Phone	123-456-78
Manager Info	
Manager First Name	Jane
Manager Last Name	Manager
Manager Email	JaneManag...
Manager Phone	123555123

Detailed view of the incident.

Exercise 5:

Scan and quarantine files on a server file share target.

Earlier, Symplified scanned and found all open shares and configured a windows file share scan to scan the shares. They have now decided it is time to begin quarantining the files found in these shares to a secure file share on the network.

In addition to quarantining the files, a marker file will be left in the place of the original file. This marker file will indicate where the user can find the original file and how to access to it.

The screenshot shows the 'Configure Response Rule' page. At the top, there are 'Save' and 'Cancel' buttons. On the right, it says 'Administrator'. Below that is the 'General' section with fields for 'Rule Name' (set to 'Discover: Quarantine & Leave Marker') and 'Description'. A note says 'Used in no active policies.' Under the 'Conditions' section, there are two dropdown menus: 'Severity' (set to 'Is Any Of' with 'High', 'Medium', 'Low', and 'Info' options) and 'Incident Type' (set to 'Is Any Of' with 'Discover', 'Endpoint', and 'Network' options). An 'Add Condition' button is available. Below the conditions is an 'Actions' section with a dropdown menu set to '<choose action type>' and an 'Add Action' button. A specific action is highlighted: 'Network Protect: Quarantine File'.

Configuring the response rules

This screenshot shows the 'Network Protect: Quarantine File' action configuration. It includes a 'Severity' dropdown ('Is Any Of' with 'High', 'Medium', 'Low', and 'Info') and an 'Incident Type' dropdown ('Is Any Of' with 'Discover', 'Endpoint', and 'Network'). Below these are 'Actions' and 'Add Action' buttons. The main area shows the 'Marker File' checkbox is checked, and the 'Marker Text' field contains the URL 'http://intranet.symplified.com/dataprotection'. A tooltip for the marker text says: 'Please contact IT Security at ITSecurity@symplified.com if you need access to this file.' To the right, an 'Insert Variable' dropdown menu is open, listing options like 'File Full Path', 'File Name', 'File Parent Directory Path', 'Match Count', 'Policy Name', 'Policy Rules', 'Quarantine Parent Directory Path', 'Scan Date', 'Severity', and 'Target'.

Configuring the response rules

Symantec Data Loss Prevention | Home | Incidents | Manage | System | Administrator

General

- Name: Simplified PCI (EDM/DCM)
- Description: (empty)
- Policy Label: (empty)
- Policy Group: Simplified PCI Policies
- Status: Active [suspend]
- Last Modified: 2/23/21 4:34 PM by Administrator

Response

Rules	Actions	Conditions
Discover: Quarantine & Leave Marker	Network Protect: Quarantine File	when Incident Type Is Any Of Discover and Severity Is Any Of High, Medium, Low

Create a template from this policy

Configuring the policy and response to it.

Save | Cancel

Protect

- Allowed Protect Remediation:**
 Copy
 Encrypt
 Quarantine
- Quarantine/Copy Share:**

(Share where files are quarantined/copied, write access credential. A local path will use system credentials)

Path: \\Enforce\Quarantine

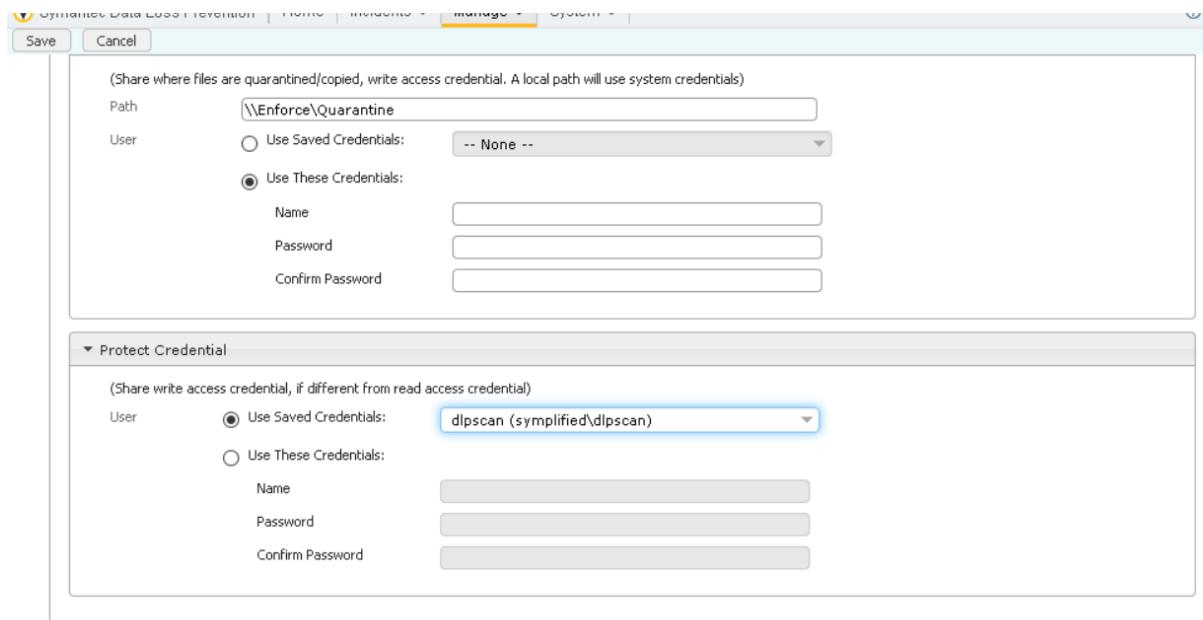
User:
 Use Saved Credentials: -- None --
 Use These Credentials:

Name: (empty)

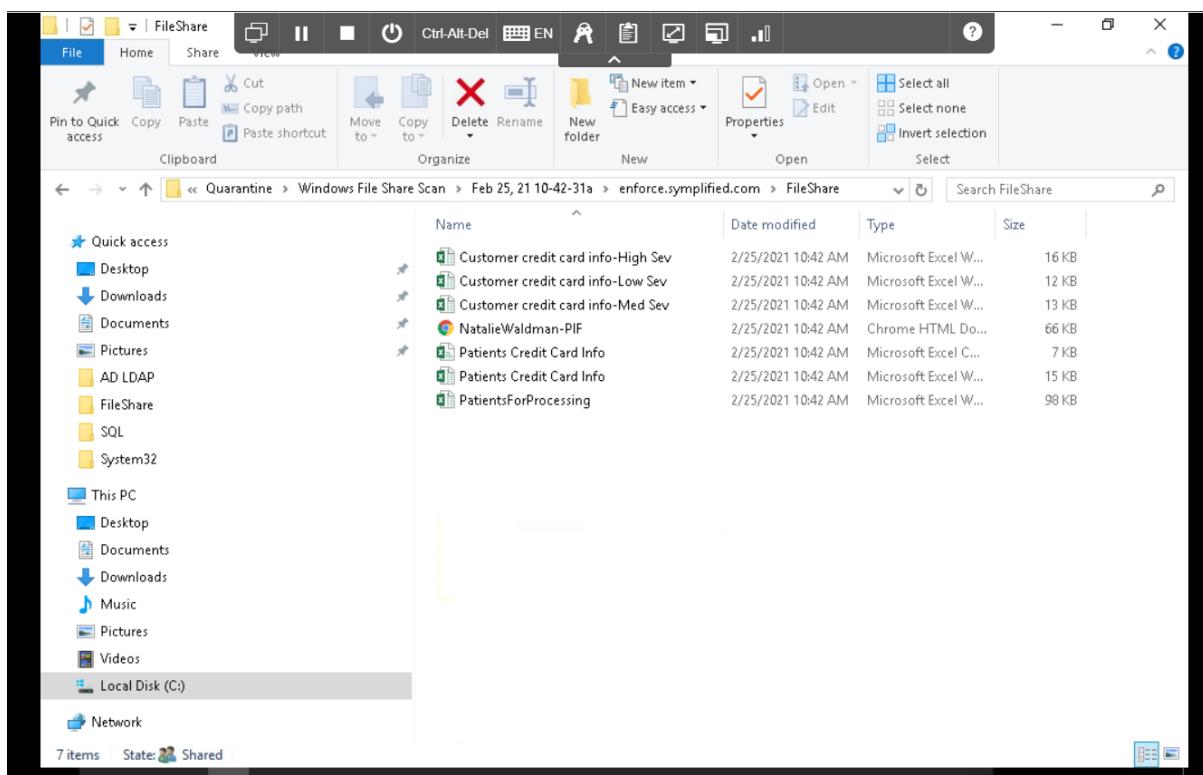
Password: (empty)

Confirm Password: (empty)
- Protect Credential:** (empty)

Editing the protect (File system Target)



Editing the file system target.



Analyzing the file of the located incident.

Exercise 6:

Scan and Quarantine files on a endpoint target.

Till now, we scanned and quarantined the files which are transferring the network but in this lab we are going to scan and quarantine the files even before travelling through the network i.e., at the end point.

The screenshot shows the Symantec Data Loss Prevention interface under the 'Manage' tab. The current page is 'Configure Response Rule'. The 'General' section contains a 'Rule Name' field set to 'Endpoint Discover: Quarantine File' and a 'Description' field which is empty. A note below states 'Used in no active policies.' The 'Conditions' section includes two dropdown menus: 'Incident Type' (set to 'Discover') and 'Severity' (set to 'High'). Both dropdowns have a red 'X' icon next to them, indicating they are currently inactive or being configured. Below these conditions is an 'Actions' section with a dropdown menu set to '<choose action type>' and a 'Add Action' button.

Configuring the response rules.

This screenshot shows the configuration dialog for the 'Endpoint Discover: Quarantine File' rule. It has a header 'Endpoint Network' and an 'Actions' section with a dropdown set to '<choose action type>'. The main configuration area is titled 'Endpoint Discover: Quarantine File' with a sun icon. It includes fields for 'Quarantine Path' (set to '\\Enforce\Quarantine'), 'Anonymous Access' (unchecked), and 'Use Saved Credentials' (checked, set to 'dlpscan (symplified\dlpscan)'). Under the 'Marker File' section, there is a checked checkbox 'Leave marker file in place of remediated file'. In the 'Marker Text' field, the value is '\$PATH\$\$FILE_NAME\$\$POLICIES\$\$QUARANTINE_PARENT_PA TH\$\$QUARANTINE_PATH\$|'. A tooltip 'Insert Variable' is shown over this field, listing options like 'File Full Path', 'File Name', etc. The entire configuration dialog is enclosed in a red border.

Composing the new custom market test using the insert variables

The screenshot shows the 'Configure Policy' screen for a policy named 'Simplified PII (DCM)'. The 'Response' tab is selected. It lists three response rules:

- SMTP Block & Notify**: Action: Network Prevent: Block SMTP Message All: Send Email Notification. Condition: when Incident Type Is Any Of Network and Severity Is Any Of High, Medium, Low.
- Block User Action**: Action: Endpoint Prevent: Block. Condition: when Incident Type Is Any Of Endpoint and Severity Is Any Of High, Medium, Low.
- Endpoint Discover: Quarantine File**: Action: Endpoint Discover: Quarantine File. Condition: when Incident Type Is Any Of Discover and Severity Is Any Of High, Medium, Low.

Below the table, there is a link to 'Create a template from this policy'.

Adding the response rules.

The screenshot shows the 'Incidents - New' screen. The left sidebar shows 'Discover Reports' with 'Incidents - New' selected. The main area displays a table of incidents:

Type	Location / Target / Scan	File Owner	ID / Policy	Matches	Severity	Status
Location	ENDPOINT - c:\MyData\PatientsForProcessing.xlsx	SYMPPLIFIED\joe_user	00000450 Simplified PII (DCM)	300	High	New
Location	//enforce.simplified.com/FileShare/PatientsForProcessing.xlsx	BUILTIN\Administrators	00000449 Simplified PCI (EDM/DCM)	179	High	New
Location	//enforce.simplified.com/FileShare/Patients/Credit Card Info.xlsx	BUILTIN\Administrators	00000448 Simplified PCI (EDM/DCM)	40	High	New

We can clearly see that incident is generated

Symantec Data Loss Prevention | Home | Incidents | Manage | System | bookmark this page (Ctrl+D) | Administration | Customize Layout

Incidents > Discover > Incidents - New > Discover Incident Snapshot

Incident 00000450

Status: New Severity: High

Endpoint File System

Key Info History Notes Correlations

Policy Matches

	Matches
Simplified PII (DCM) [view policy]	300
US Social Security Numbers (Data Identifiers)	300

Incident Details

Server or Detector	Simplified Detection Server
Protect Status	Endpoint File Quarantined
Endpoint Quarantine Location	\Enforce\Quarantine\183\ENDPOINT\c\MyData\PatientsForProcessing.xlsx
Target Scan	Endpoint File Share Scan 2/25/21 9:15 PM
Detection Date	2/25/21 9:15 PM
Seen Before	First seen less than 1 day earlier.
Is Hidden	No [Do Not Hide]
File Location	ENDPOINT - c:\MyData

Matches (matches found in 1 component)

- ▼ c:\MyData\PatientsForProcessing.xlsx (300 Matches):
 - ... 420-08-3530 30809 RAUL PASHAL 4684451986499930 800089820 pashal_63588...om (930)750-0791 53395-9820 d0IeNxBjCB 650-22-0893 30811 DRA LEISURE 4132673384929420 G00698233 leisure_1100...om (293)561-7807 29795-8233 ZEUDPKNN 561-97-2514 30812 JAMES HINTZ 480331197819540 D00451340 hintz_668208...om (714)803-9738 03706-1340 keLCsttij 203-36-9293 30813 GOLDIE PURVIS 4409094843938080 E00907590 purvis_14463...om (693)473-0722 15222-7590 HwbwUgKQqP 373-18-2660 30814 SUSAN WILLIAMS 4083121379497770 E00623438 williams_841...rg (503)627-1556 54724-8334 KlsvsmSnob 627-12-9288 30817 DANIEL SMITH 4718214769659850 F00557274 smith_491395...om (288)878-2616 52330-7274 vjhqgstGeAn 178-52-6151 30818 HAZEL HANSEN 483619563600...
 - ...52-6151 30818 HAZEL HANSEN 483619563600...om

In detail view of the incidents.

Symantec Data Loss Prevention | Home | Incidents | Manage | System | View history, saved bookmarks, and more | Administrator

Incidents > Discover > Incidents - New

Close Save Send Export Delete Report

Saved Reports
No Saved Reports Available

Discover Reports
Exec. Summary - Discover
Incidents - All Scans
Incidents - New
Target Summary
Policy by Target
Status by Target
Content Roots at Risk

Filter

Status: Equals New
Scan: Last Completed Scan
Target ID: Custom Endpoint File Share Scan
Detection Date: Last 30 Days

Severity:
 High Low
 Medium Info

Advanced Filters & Summarization

Applied Filters

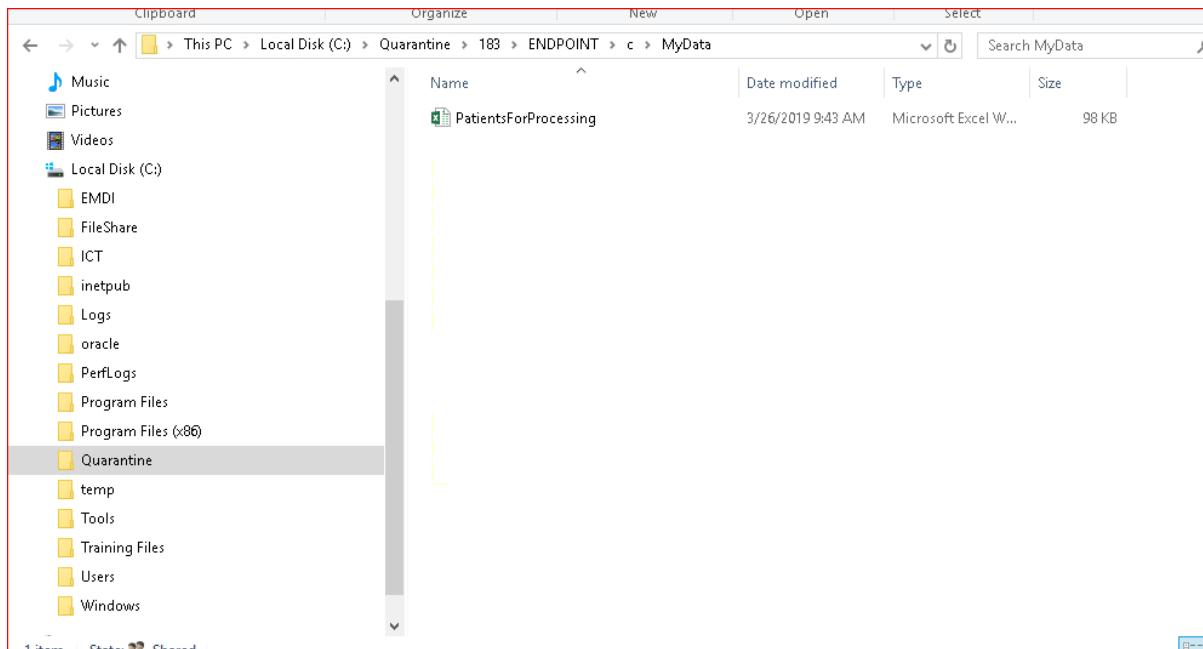
Status Equals New	Scan Last Completed Scan	Severity Is Any Of
High 1	Medium 0	Low 0
Medium 0	Low 0	Info 0

Target ID Custom Endpoint File Share Scan **Detection Date** Last 30 Days

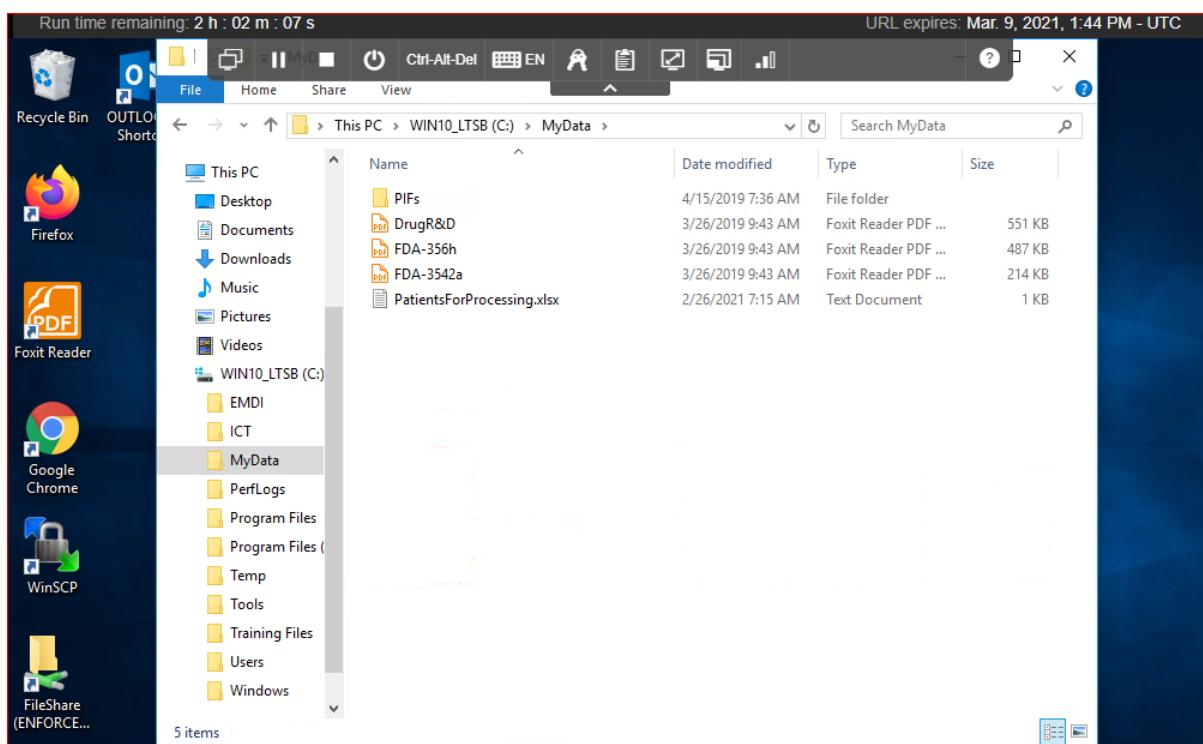
Incident Actions Select All [Show / hide filters] 1 of 1 Show

Type	Location / Target / Scan	File Owner	ID ▾ / Policy	Matches	Severity	St
Location	ENDPOINT - c:\MyData\PatientsForProcessing.xlsx	SYMPIFIED\joe_user	00000401	300	High 1	Ne
Target	Endpoint File Share Scan		Sympified PII (DCM)			
Scan	2/24/21 5:54 AM					

Incident at the endpoint



File is Quarantined.



Even at the endpoint in my data the endpoint as well.

Lab 6:

Remediating the data loss incidents and tracking risk reduction:

This is very important phase because once after implementing the policy violations the steps we have done till now I mean the exercises till now. When a policy is violated how do we identify whether a user is done with carelessness or intentionally i.e., malicious user and how do we track all the incidents over a period of time.

In this lab we will do about how do we assign the user roles and responsibilities and how the genuine user will view, analyze and remediate the incidents after they occurred. We will learn about the reporting capabilities of DLP's enforce server and how to generate the reports and view them by the category. Additionally we will learn how to configure the smart responses as well which generally don't need direct human impact.

Exercise 1:

Configure roles and users.

Generally after incidents are raised we should carefully evaluate the false positives. The Symantec DLP team should have only access to view the incidents but not to make any changes in the enforce console.

In this lab we create roles for the IT team who are responsible for creating and maintaining the DLP policies and response rules. A role should be created for seeing the risk reduction reports that have been created for them.

The screenshot shows the 'Configure a role' page in the Symantec DLP interface. The 'General' tab is active. The 'Name' field contains 'DLP First Responders'. The 'Description' field is empty. In the 'User Privileges' section, under the 'System' heading, there are three checkboxes: 'User Administration (Superuser)', 'Server Administration', and 'Agent Management', none of which are checked. There are also tabs for 'Incident Access', 'Policy Management', and 'Users'.

Adding the rules for DLP First Responders

The screenshot shows the 'Display Attributes' section of the Symantec Data Loss Prevention system. It is divided into three columns: Shared, Endpoint, and Discover.

Shared	Endpoint	Discover
<input checked="" type="checkbox"/> History	<input type="checkbox"/> Username	<input type="checkbox"/> File Owner
<input type="checkbox"/> Body	<input checked="" type="checkbox"/> Machine name	<input type="checkbox"/> File Owner Email
<input type="checkbox"/> Attachments		<input checked="" type="checkbox"/> Location
<input type="checkbox"/> Matches		
<input type="checkbox"/> Sender		
<input type="checkbox"/> Recipients		
<input checked="" type="checkbox"/> Subject		
<input type="checkbox"/> Original Message		

Below this is the 'Custom Attributes' section, which lists attributes with 'View' and 'Edit' checkboxes:

	<input type="checkbox"/> View All	<input type="checkbox"/> Edit All
First Name	<input type="checkbox"/> View	<input type="checkbox"/> Edit
Manager First Name	<input checked="" type="checkbox"/> View	<input type="checkbox"/> Edit

Adding the rules for DLP First Responders

The screenshot shows the 'Custom Attributes' section of the Symantec Data Loss Prevention system. It lists attributes with 'View' and 'Edit' checkboxes:

	<input type="checkbox"/> View All	<input type="checkbox"/> Edit All
First Name	<input type="checkbox"/> View	<input type="checkbox"/> Edit
Manager First Name	<input checked="" type="checkbox"/> View	<input type="checkbox"/> Edit
Manager Last Name	<input checked="" type="checkbox"/> View	<input type="checkbox"/> Edit
Last Name	<input type="checkbox"/> View	<input type="checkbox"/> Edit
Email	<input type="checkbox"/> View	<input type="checkbox"/> Edit
Manager Email	<input checked="" type="checkbox"/> View	<input type="checkbox"/> Edit
Phone	<input type="checkbox"/> View	<input type="checkbox"/> Edit
Manager Phone	<input checked="" type="checkbox"/> View	<input type="checkbox"/> Edit

Adding the rules for DLP First Responders

System > Login Management > Roles > Configure Role

Administrator

Save Cancel

Configure a role

Define the privileges and rights for users with a specific role.

General Incident Access Policy Management Users

Only show incidents meeting the following criteria:

Status Equals New

Adding the rules for DLP First Responders

Save Cancel

General Incident Access Policy Management Users

Name * IT Security

Description

User Privileges

System

User Administration (Superuser)
 Server Administration
 Agent Management

People

User Reporting (Risk Summary, User Snapshot)

Incidents

View

Adding the rules for IT Security team

Privileges

- Import Policies
Policy import can be enabled for all users in this role
- Author Policies
- View Policies
- Discover Scan Control
- Credential Management
- Author Response Rules

Policy Groups

- All Policy Groups
- Default Policy Group
- Simplified PCI Policies
- Simplified PII Policies
- Classification

Adding the rules for IT Security team

General

Name * CISO

Description

User Privileges

System

- User Administration (Superuser)
- Server Administration
- Agent Management

People
Incident access conditions are disabled when the User Reporting option on the General tab is selected.

- User Reporting (Risk Summary, User Snapshot)

Incidents

Adding the rules for CISO team

The role 'CISO' was saved successfully. Affected users will need to re-login to see changes.

Roles

A list of all the roles in the system

Name	Description	Actions
CISO		X
DLP First Responders		X
IT Security		X

Show 10 entries First Previous 1 Next Last

Adding the rules for CISO team

The screenshot shows the 'Configure DLP User' page in the Symantec DLP interface. The user 'FirstResponder' is being created. Under 'Authentication', 'Password Access' is checked, and a new password is entered twice. Under 'General', an email address is listed, and the language is set to English (United States). Buttons for 'Save' and 'Cancel' are at the bottom.

Adding the First Responder to the DLP USER

The screenshot shows the 'Report Preferences' screen. Under 'Roles', the 'DLP First Responders' checkbox is checked. Under 'Default Role', 'DLP First Responders' is selected. Other options like 'CISO' and 'IT Security' are also present but unchecked.

Adding the First Responder to the DLP USER

Report Preferences

Text File Encoding Use browser default encoding
UTF-8

CSV Delimiter Comma [,]

Include Incident Violations in XML Export

Include Incident History in XML Export

Roles

CISO
 DLP First Responders
 IT Securiy

Default Role

IT Securiy

Adding the IT security team to the DLP USER

Report Preferences

Text File Encoding Use browser default encoding
UTF-8

CSV Delimiter Comma [,]

Include Incident Violations in XML Export

Include Incident History in XML Export

Roles

CISO
 DLP First Responders
 IT Securiy

Default Role

CISO

Adding the CISO team to the DLP USER

The user 'CISO' was saved successfully.		
Add DLP User	Email	Access
DLP User Name		
Administrator		All Roles
CISO		CISO
FirstResponder		DLP First Responders
ITSecurity		IT Securiy

Displaying the teams added to the DLP USERS

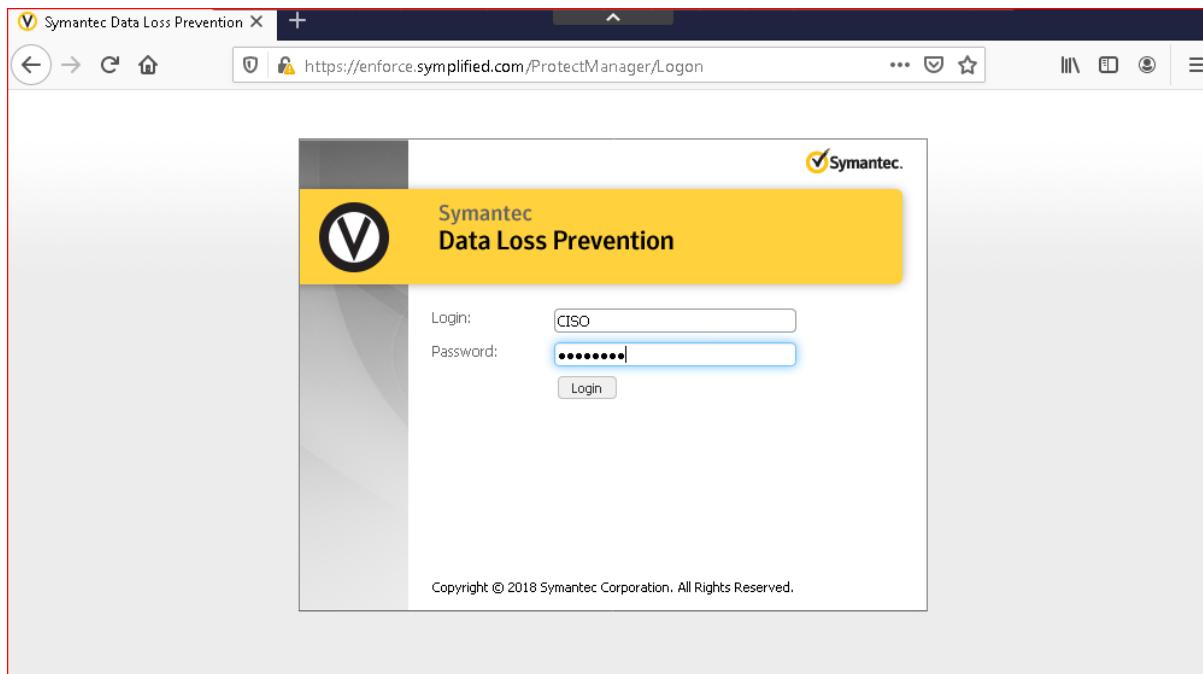
The screenshot shows the 'Edit General Settings' page in the Symantec Data Loss Prevention interface. The 'System' tab is selected. The 'Reports and Alerts' section contains a 'Distribution' configuration where the 'Send reports as links, login required to view' option is selected. It also includes fields for 'Fully Qualified Manager Name' (set to 'EnForce.symplified.com') and 'Correlations'. The 'SMTP' section provides settings for 'Server' ('enforce.symplified.com'), 'System Email' ('itsecurity@symplified.com'), 'User ID' ('itsecurity@symplified.com'), and 'Password' (redacted). The 'License' section is present at the bottom.

At last we are configuring the rules and we selected the option send reports as links, login required to view in Distribution tab.

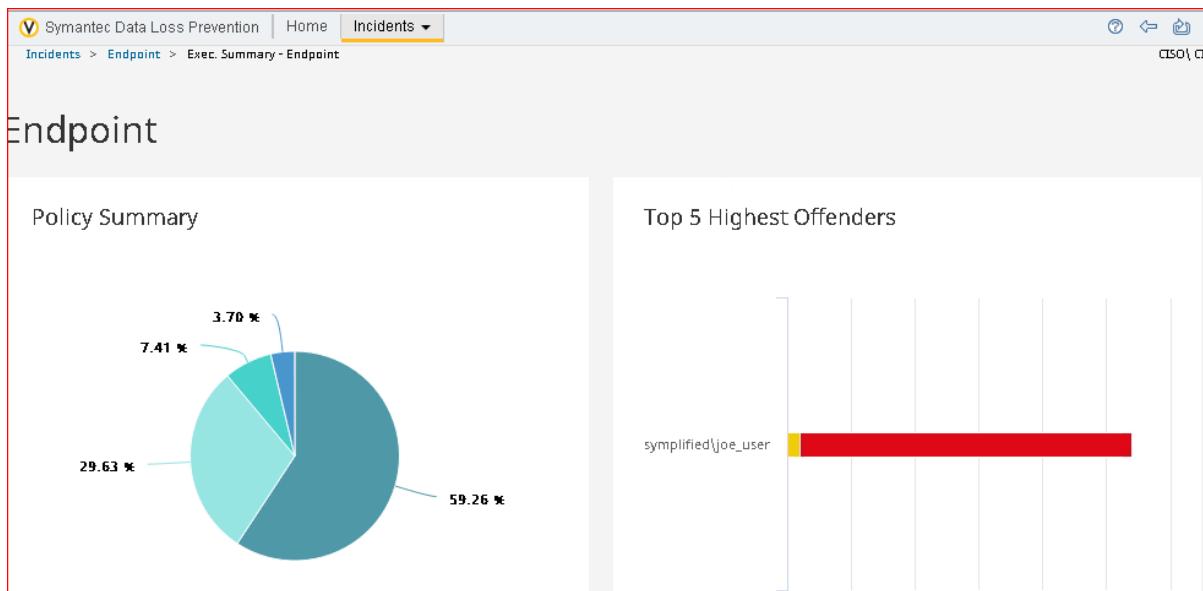
Exercise 2:

User reports to track risk Exposure and Reduction.

Generally the organization want to keep the data very secure and they will ask the proof of incidents to the Symantec DLP team and also asks how the daily implementation is going on. They also want to see that the data loss is reducing and they want that report. In order to provide that custom reports and custom dashboard need to be created in the Enforce Console. This enables the organization to view the real time reporting on data loss reduction.



Login as CISO



We can clearly see that no of options decreased when logging as CISO

Symantec Data Loss Prevention | Home | Incidents ▾

Incidents > All Reports > Configure Dashboard

<https://enforce.symplified.com/ProtectManager/CreateRoleDashboard.d>

CISO\ CISO

Save Cancel

General

Name: Executive Summary Report

Description:

Delivery Schedule

Schedule: No Schedule

Left Column (Chart Only)

- Policy Summary
- Policy Summary
- Target Summary

Right Column (Chart and Table)

- Incidents - New
- Incident Type Summary
- Incidents - All Scans

Generating the new report according to the needs

Network

Policy Summary

Total	High	Med	Low	Info	Matches
14	14	0	0	0	1,953

Incidents - New

Jan 27, 2021 to Today

Date	Total	High	Med	Low	Info	Matches
12/8/21	14	14	0	0	0	1,953

Incident

Category	Date	Count
Patient Info	2/25/21 8:30 AM	179
Patient Info	2/25/21 8:30 AM	100
Patients for processing	2/25/21 2:28 AM	179
Patients for processing	2/25/21 2:28 AM	100
Patients for processing	2/25/21 2:15 AM	179
Patients for processing	2/25/21 2:15 AM	100
Patents Data for Processing	2/24/21 11:17 PM	179
Patents Data for Processing	2/24/21 11:17 PM	100
Patents Data for Processing	2/24/21 11:07 PM	179
Patents Data for Processing	2/24/21 11:07 PM	100

Endpoint

Policy Summary

Total	High	Med	Low	Info	Matches
27	26	0	1	0	3,414

Incident Type Summary

Total	High	Med	Low	Info	Matches
27	26	0	1	0	3,414

Protocol or Endpoint Monitoring

Protocol	All	High	Matches
Application File Access	2	2	
Clipboard	2	1	
Copy to Network Share	1	1	
Email/SMTP	18	18	2
HTTP	4	4	

Displaying the saved reports

Symantec Data Loss Prevention | Home | Incidents ▾

Policy Summary

Total	High	Med	Low	Info	Matches
27	26	0	1	0	3,414

Incident Type Summary

Total	High	Med	Low	Info	Matches
27	26	0	1	0	3,414

Discover

Target Summary

Total	High	Med	Low	Info	Matches
2	2	0	0	0	335

Incidents - All Scans

Incident	Date	Count
ENDPOINT - c:\MyData\PatientsForProcessing.xlsx		300
/enforce.symplified.com/FileShare/PatientsForProcessing.xlsx		179
//enforce.symplified.com/FileShare/Patients Credit Card Info.xlsx		40
//enforce.symplified.com/FileShare/Patients Credit Card Info.csv		40
//enforce.symplified.com/FileShare/Customer credit card info-Low Sev.xlsx		7
//enforce.symplified.com/FileShare/Customer credit card info-High Sev.xlsx		40
//enforce.symplified.com/FileShare/Customer credit card		25

Displaying the saved report

The screenshot shows the Symantec Data Loss Prevention interface. A modal dialog box titled "Save Report As" is open in the center. The "Name:" field contains "Protocol by Policy Summary". The "Sharing:" section has "Shared" selected. On the right side of the dialog, there are severity filters: "High" (unchecked), "Medium" (unchecked), "Low" (checked), and "Info" (checked). Below the dialog, a main report table is visible, showing data categorized by policy. The table includes columns for policy name, count of incidents, and severity distribution (Info, Low, Medium, High). The total count for all policies is 3,412.

Policy	Count	Info	Low	Medium	High
Simplified Drug Process Detection (IDM)	1	1	0	0	0
Application File Access	1	1	0	0	0
Simplified PCI (EDM/DCM)	16	15	0	1	0
Application File Access	1	1	0	0	0
Clipboard	1	0	0	1	0
Email/SMTP	12	12	0	0	0
HTTP	2	2	0	0	0
Simplified PII (DCM)	8	8	0	0	0

Generating the new report as Protocol by Policy Summary.

Exercise 3:

Define Incident statuses and incident groups.

The first responders team within IT department has expressed a need for some new incident statuses to be created. These new statuses will make it easier for the escalation team to focus on the higher priority incidents first and help everyone keep track of which incidents have been already addressed.

The screenshot shows the Symantec Data Loss Prevention Policy List interface. The top navigation bar includes 'Manage' and 'System' dropdowns, and a breadcrumb path 'Manage > Policies > Policy List'. The main area displays a table with columns: Status, Name, Description, Policy Group, and Last Modified. A red box highlights the entire table area.

Status	Name	Description	Policy Group	Last Modified
<input type="checkbox"/>	HIPAA and HITECH (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.	Simplified PII Policies	February 24, 2021 4:56:33 AM PST
<input type="checkbox"/>	Simplified Drug Process Detection (IDM)		Default Policy Group	February 25, 2021 2:43:01 AM PST
<input type="checkbox"/>	Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 25, 2021 10:51:54 AM PST
<input type="checkbox"/>	Simplified PII (DCM)		Simplified PII Policies	February 25, 2021 9:14:32 PM PST
<input type="checkbox"/>	Simplified PII (EMDI)		Simplified PII Policies	February 24, 2021 6:13:07 AM PST

We can see there is no incident tab when we logged in as the IT Security team.

The screenshot shows the Symantec Data Loss Prevention System > Incident Data > Attributes > Configure Status Value interface. The top navigation bar includes 'System' and 'Manage' dropdowns, and a breadcrumb path 'System > Incident Data > Attributes > Configure Status Value'. The main area shows a 'General' section with a 'Name' field containing 'Resolved'. A red box highlights the 'Name' field.

Configuring the status value

Name	New Incident Default	Display Order
New	[set as default]	[Down] [Up] [Delete]
Resolved	[set as default]	[Up] [Down] [Edit] [Delete]
Resolved - Education	[set as default]	[Up] [Down] [Edit] [Delete]
Resolved - HR	[set as default]	[Up] [Down] [Edit] [Delete]
Resolved - False Positive	[set as default]	[Up] [Down] [Edit] [Delete]
Escalated	[set as default]	[Up] [Down] [Edit] [Delete]

Configured the status values

Name	Resolved
Member Status	<input type="checkbox"/> New <input checked="" type="checkbox"/> Resolved <input checked="" type="checkbox"/> Resolved - Education <input checked="" type="checkbox"/> Resolved - HR <input checked="" type="checkbox"/> Resolved - False Positive <input type="checkbox"/> Escalated

Configuring the status group.

The screenshot shows a software interface for managing status groups and values. At the top, a green header bar displays a success message: "The Status Group 'Resolved' was saved successfully." Below this, there are two tabs: "Status" (selected) and "Custom Attributes".

Status Values:

Name	New Incident Default	Display Order
New	DEFAULT	[Down]
Resolved	[set as default]	[Up] [Down]
Resolved - Education	[set as default]	[Up] [Down]
Resolved - HR	[set as default]	[Up] [Down]
Resolved - False Positive	[set as default]	[Up] [Down]
Escalated	[set as default]	[Up]

Status Groups:

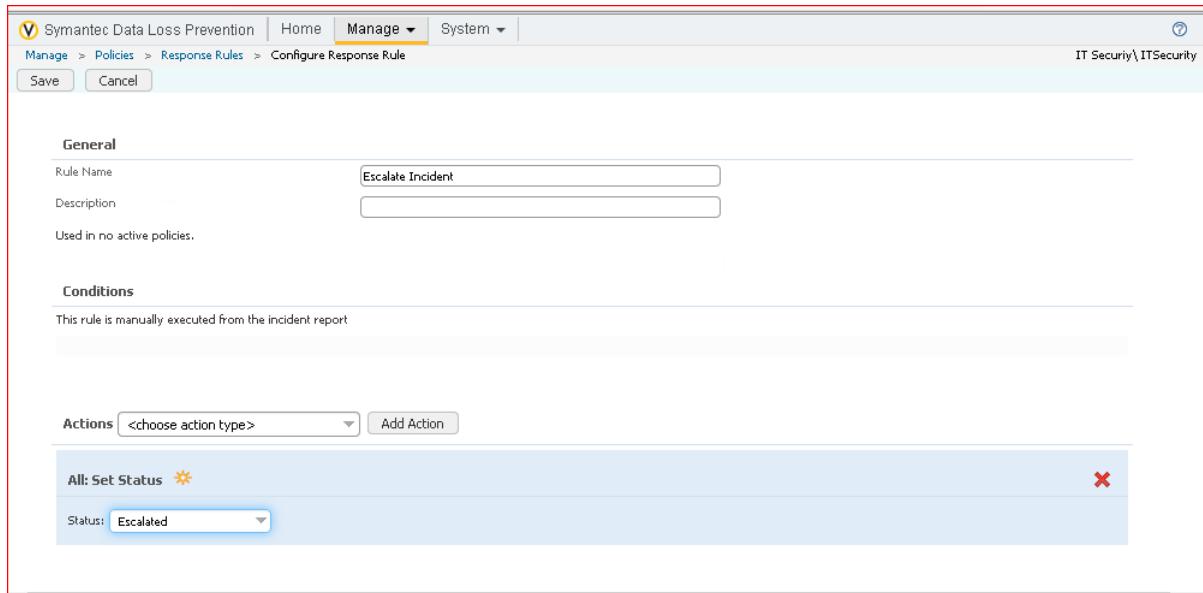
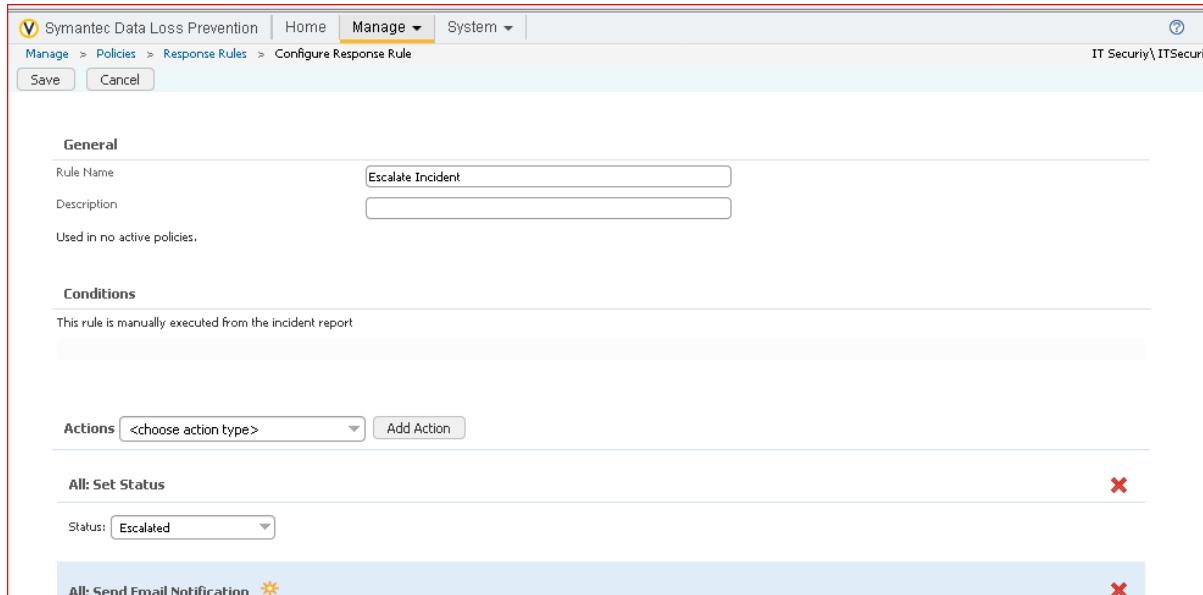
Name	Member Status	Add Status Group	Display Order
Resolved	Resolved Resolved - Education Resolved - HR Resolved - False Positive		

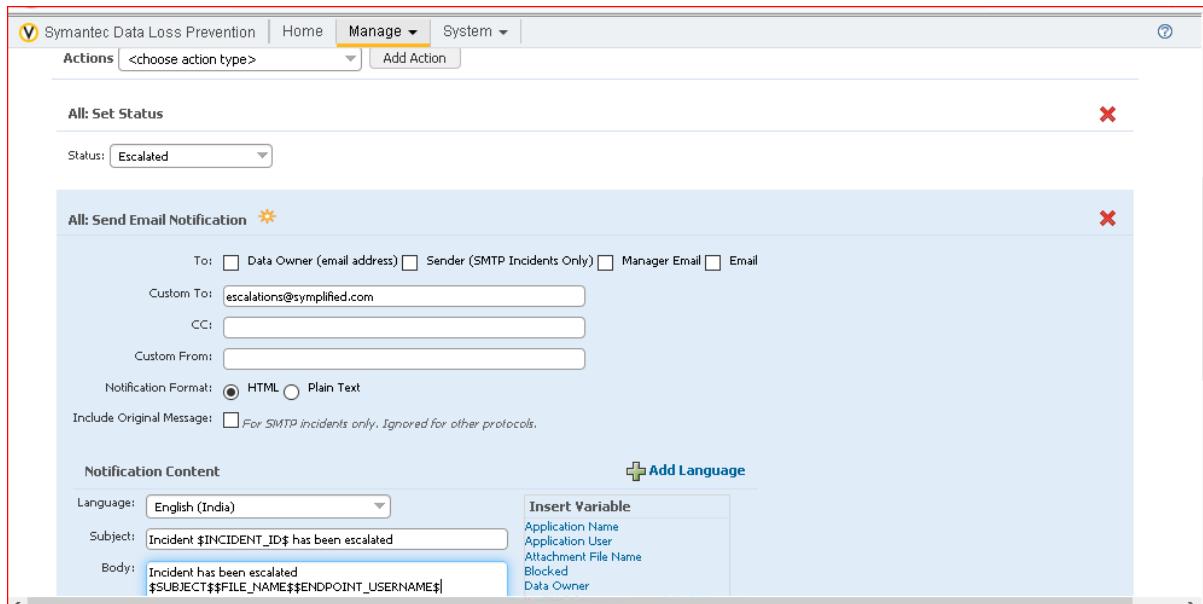
Displaying all the status groups and status values.

Exercise 4:

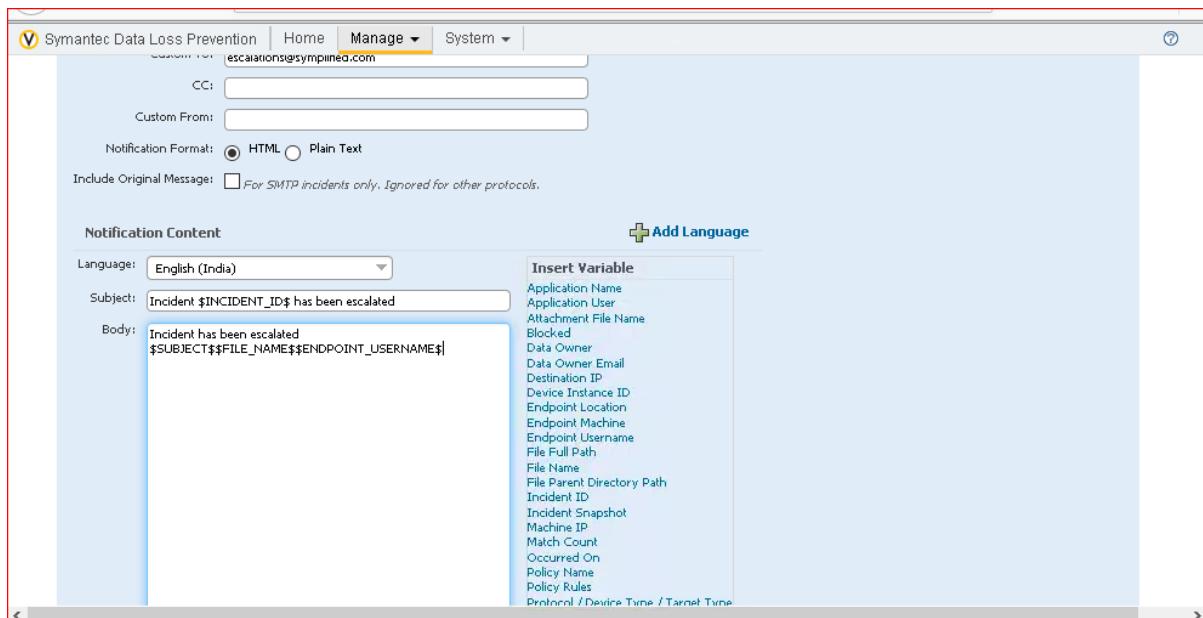
Configure and Use smart responses:

Generally the first responders team has been manually changing the status of the incidents they review to “Escalated” or “Resolved-Education” depending upon the type of the incident but this is taking too much time so upon investigating the it team has come up with the smart responses that will help speed up the process of changing the incident status and sending out any notification emails to users or managers.

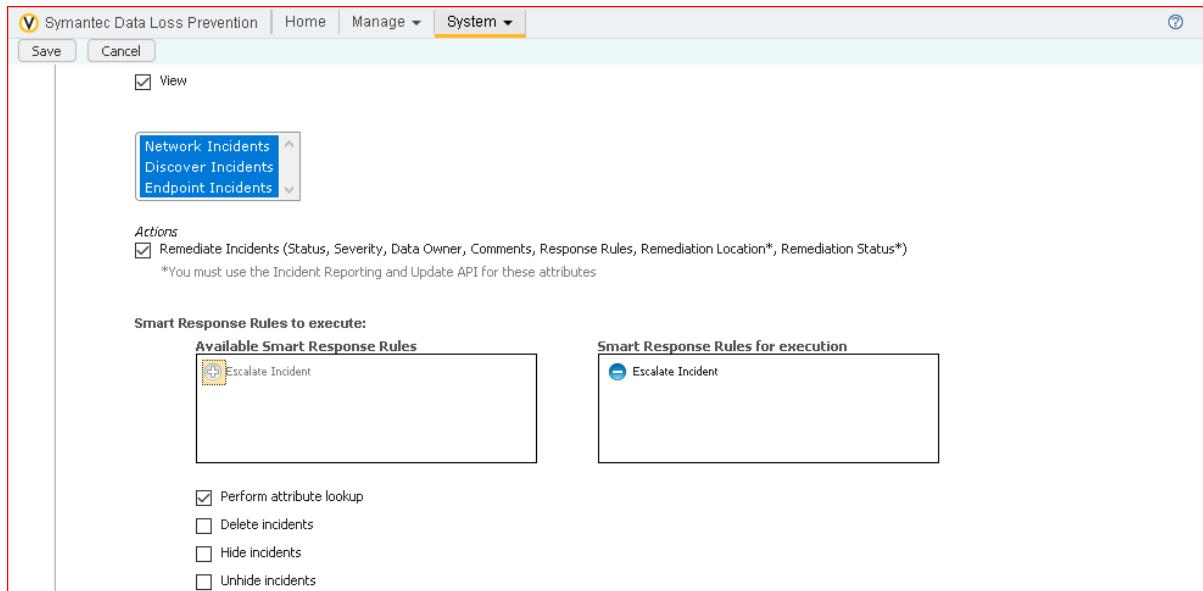
**Adding the response rules****Adding the response rules**



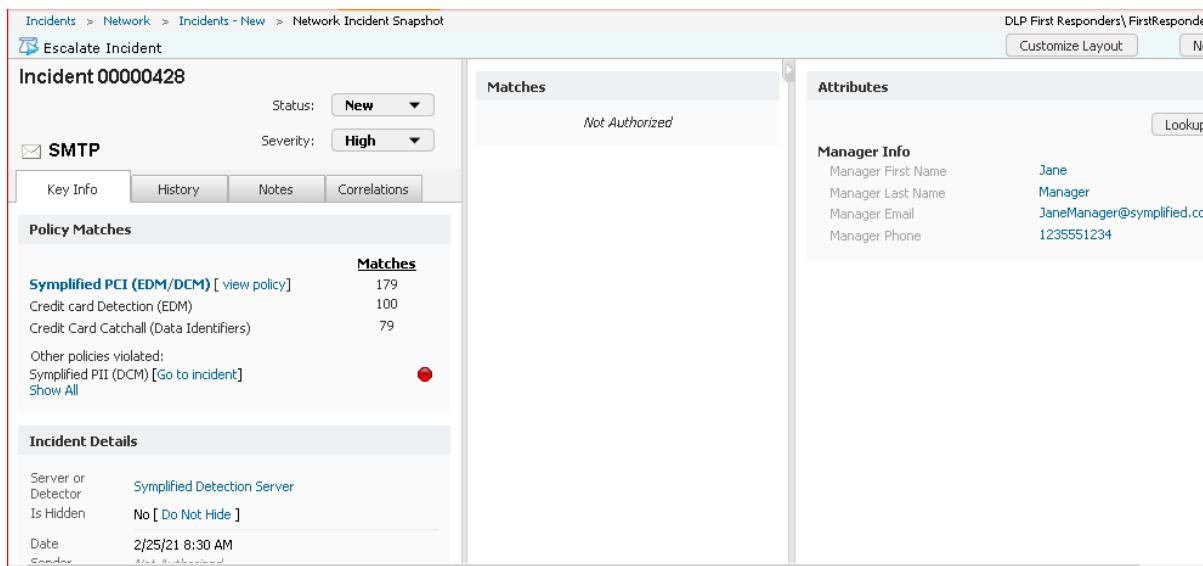
Adding the response rules



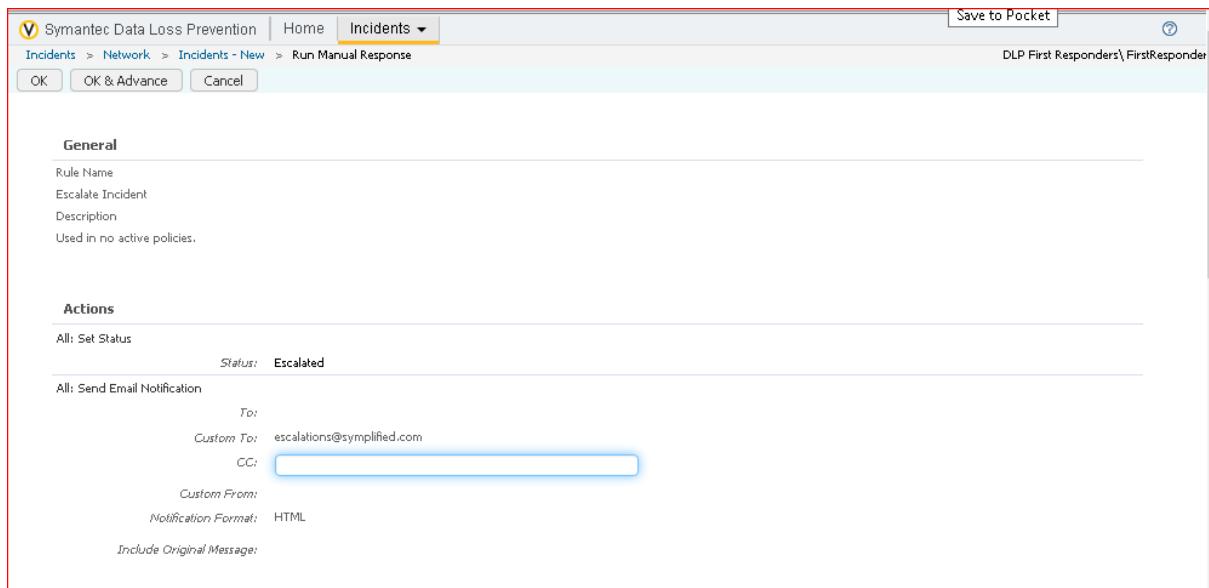
Adding the response rules



Adding the escalate incident option



Processing of escalating



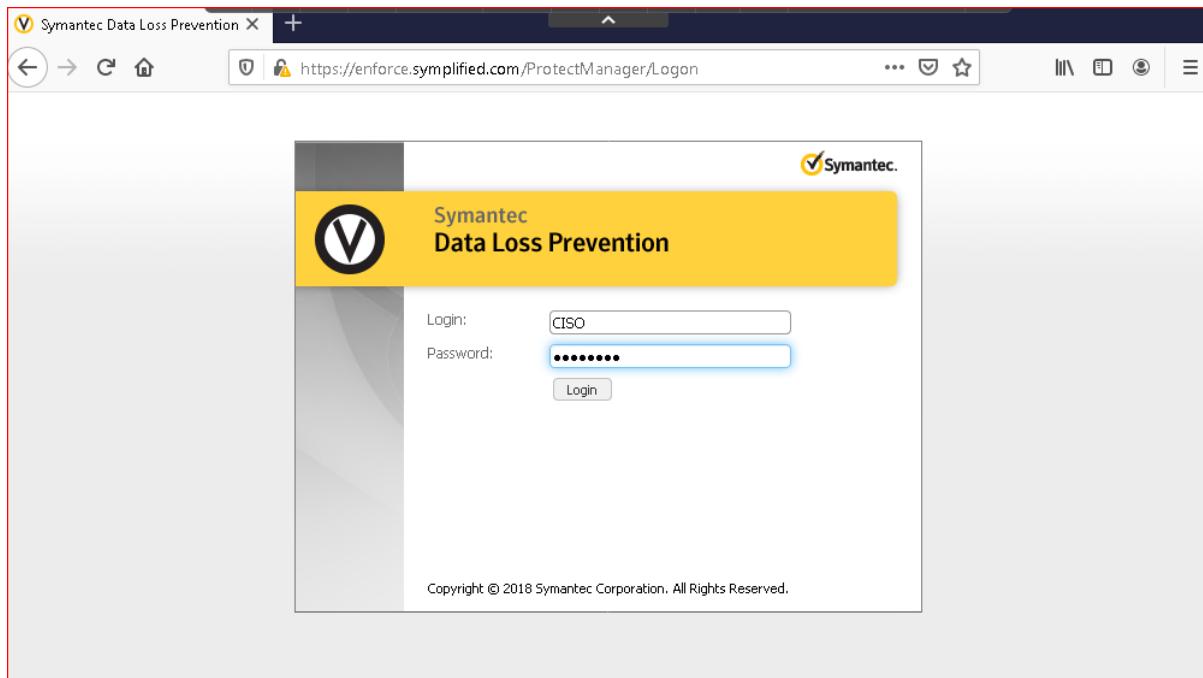
Clicked on OK&Advance and proceed

We can see that incident is escalated.

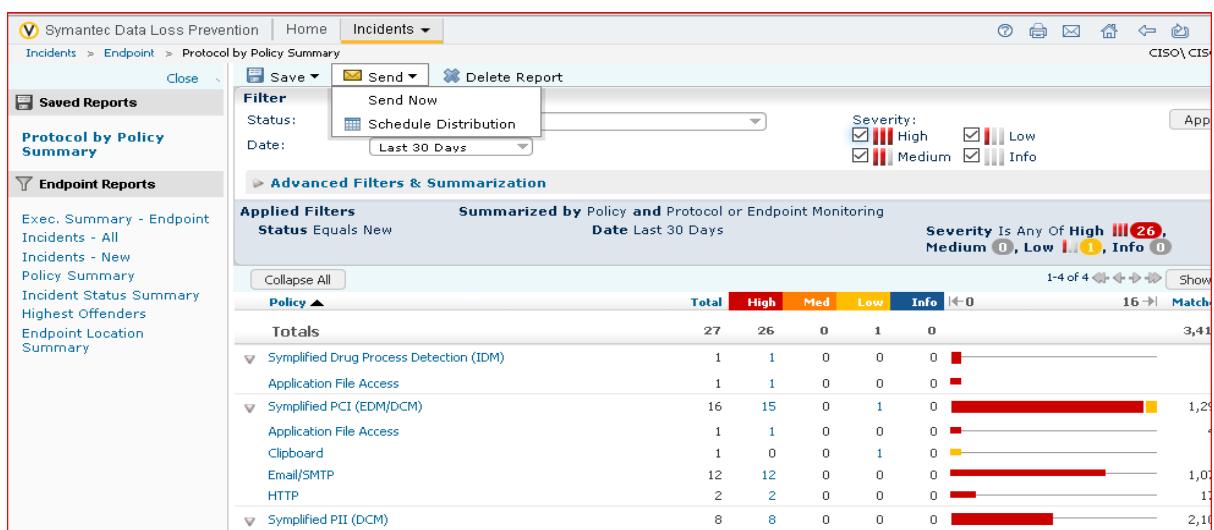
Exercise 5:

Schedule and send reports.

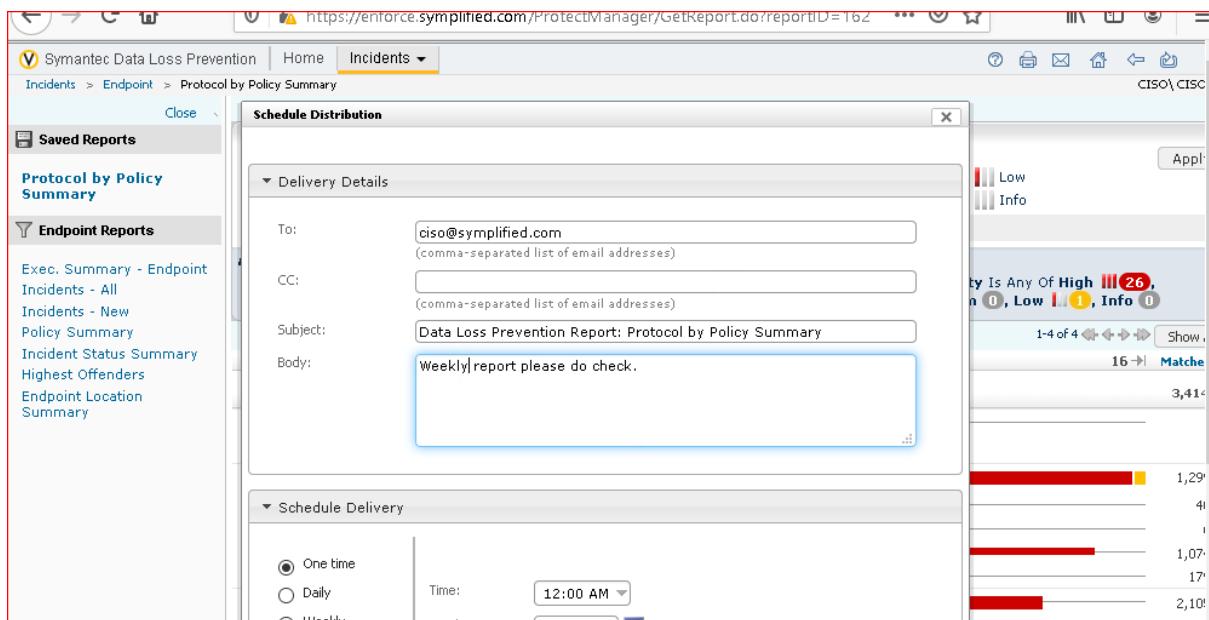
The organizational requested to submit the reports automatically on monthly basis. This makes easy to look after the data although the employees can login and see the reports but since they are busy and the report will be sent to the mails directly.



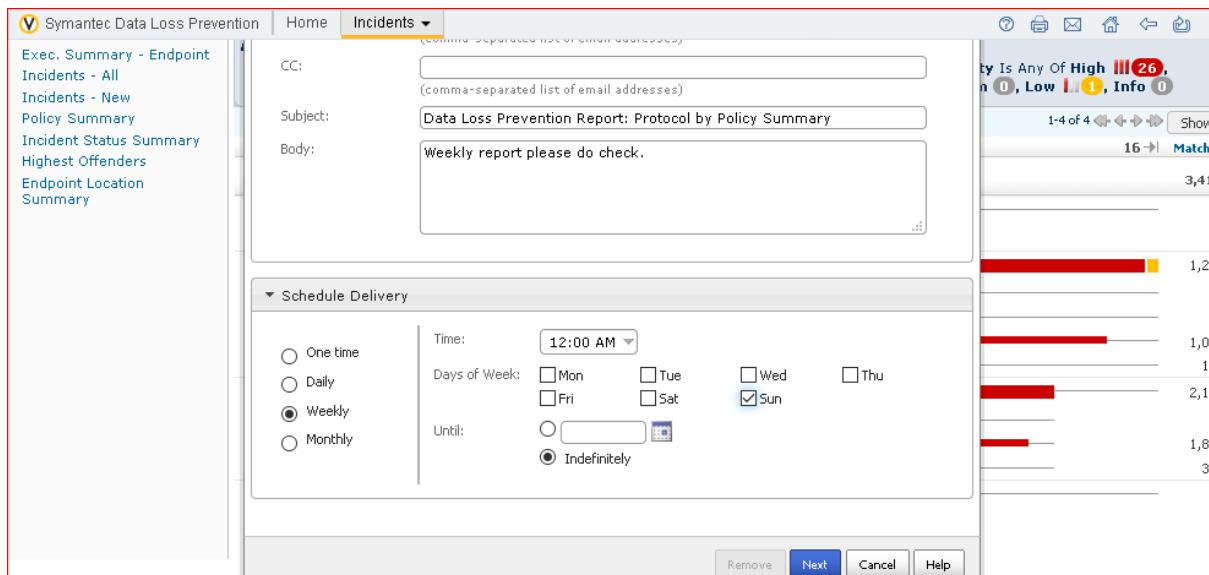
Login through CISO



On the top we can see that We can Schedule the distribution.



We need to add the details



Weekly report and should send on the sunday

The report "Protocol by Policy Summary" was saved successfully.

Saved Reports

Protocol by Policy Summary

Endpoint Reports

Exec. Summary - Endpoint
Incidents - All
Incidents - New
Policy Summary
Incident Status Summary
Highest Offenders
Endpoint Location Summary

Filter

Status: Equals New Date: Last 30 Days Severity: High, Low, Medium, Info

Advanced Filters & Summarization

Applied Filters Status Equals New **Summarized by** Policy and Protocol or Endpoint Monitoring Date Last 30 Days **Severity** Is Any Of High (26), Medium (0), Low (1), Info (0)

Totals

Policy	Total	High	Med	Low	Info
	27	26	0	1	0

Simplified Drug Process Detection (IDM)

Policy	Total	High	Med	Low	Info
Application File Access	1	1	0	0	0

Simplified PCI (EDM/DCM)

Policy	Total	High	Med	Low	Info
Application File Access	16	15	0	1	0
Clipboard	1	1	0	0	0
Email/SMTP	12	12	0	0	0
HTTP	2	2	0	0	0

Confirmation that the report will be sent weekly.

Section 7:

Enhancing data loss preventions with Integrations.

In this labs we will look at the additional products and tools that integrate with the Symantec dlp and how this products and tools assist in the goal of finding and protecting confidential and sensitive data.

Exercise 1:

Create the views schema and user.

Though the reporting features are very useful and powerful, there are times when highly specialized report is required. Using the incident data views, it is possible to use SQL Queries to create the custom report to fit nearly every reporting need.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \Training Files\SQL
C:\Training Files\SQL>sqlplus /nolog

SQL*Plus: Release 12.2.0.1.0 Production on Sat Feb 27 00:36:08 2016

Copyright (c) 1982, 2016, Oracle. All rights reserved.

SQL> @create_incident_access_user.sql
Please enter the password for sys user:
Please enter sid: protect
Please enter required username to be created: INCIDENT_VIEW
Please enter a password for the new username:
Connected.

Profile altered.

User dropped.

User created.

User altered.

User altered.

Grant succeeded.
```

Steps for executing this exercise

```
Administrator: Command Prompt
Profile altered.

User dropped.

User created.

User altered.

User altered.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Disconnected from Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production
C:\Training Files\SQL>
```

Executed successfully and Disconnected from the oracle database.

Exercise 2:

Run the Incident data view steup script.

After the incident data view user is configured, a setup script is run to create the actual incident data views in the oracle database.

```
C:\Training Files\SQL>sqlplus /nolog
SQL*Plus: Release 12.2.0.1.0 Production on Sat Feb 27 01:00:23 2021
Copyright (c) 1982, 2016, Oracle. All rights reserved.

SQL> @setup.sql
Please enter sid: protect
Please enter username for the Enforce schema: protect
Please enter password for the Enforce schema:
Please enter username for the Incident Access schema: INCIDENT_VIEW
Please enter password for the Incident Access schema:
Connected.
old  1: GRANT SELECT ON INCIDENT TO &view_username
new  1: GRANT SELECT ON INCIDENT TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGE TO &view_username
new  1: GRANT SELECT ON MESSAGE TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGECOMPONENT TO &view_username
new  1: GRANT SELECT ON MESSAGECOMPONENT TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGEORIGINATOR TO &view_username
new  1: GRANT SELECT ON MESSAGEORIGINATOR TO INCIDENT_VIEW
```

Process of running the setup script

```
Please enter sid: protect
Please enter username for the Enforce schema: protect
Please enter password for the Enforce schema:
Please enter username for the Incident Access schema: INCIDENT_VIEW
Please enter password for the Incident Access schema:
Connected.
old  1: GRANT SELECT ON INCIDENT TO &view_username
new  1: GRANT SELECT ON INCIDENT TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGE TO &view_username
new  1: GRANT SELECT ON MESSAGE TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGECOMPONENT TO &view_username
new  1: GRANT SELECT ON MESSAGECOMPONENT TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGEORIGINATOR TO &view_username
new  1: GRANT SELECT ON MESSAGEORIGINATOR TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGERECIPIENT TO &view_username
new  1: GRANT SELECT ON MESSAGERECIPIENT TO INCIDENT_VIEW

Grant succeeded.

old  1: GRANT SELECT ON MESSAGEACLENTRY TO &view_username
new  1: GRANT SELECT ON MESSAGEACLENTRY TO INCIDENT_VIEW

Grant succeeded.
```

Result after executing the setup queries

```

old  1: GRANT SELECT ON SCANASSIGNMENT TO &view_username
new  1: GRANT SELECT ON SCANASSIGNMENT TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON INFORMATIONMONITOR TO &view_username
new  1: GRANT SELECT ON INFORMATIONMONITOR TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON POLICY TO &view_username
new  1: GRANT SELECT ON POLICY TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON POLICYGROUP TO &view_username
new  1: GRANT SELECT ON POLICYGROUP TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON DATAOWNER TO &view_username
new  1: GRANT SELECT ON DATAOWNER TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON DATAOWNEREMAIL TO &view_username
new  1: GRANT SELECT ON DATAOWNEREMAIL TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON INCIDENTSTATUS TO &view_username
new  1: GRANT SELECT ON INCIDENTSTATUS TO INCIDENT_VIEW
Grant succeeded.

old  1: GRANT SELECT ON CONDITIONVIEW TO &view_username

```

Result which shows us old and new views

```

Synonym created.

old  1: CREATE OR REPLACE SYNONYM SCANASSIGNMENT FOR &enforce_username..SCANASSIGNMENT
new  1: CREATE OR REPLACE SYNONYM SCANASSIGNMENT FOR protect.SCANASSIGNMENT
Synonym created.

old  1: CREATE OR REPLACE SYNONYM INFORMATIONMONITOR FOR &enforce_username..INFORMATIONMONITOR
new  1: CREATE OR REPLACE SYNONYM INFORMATIONMONITOR FOR protect.INFORMATIONMONITOR
Synonym created.

old  1: CREATE OR REPLACE SYNONYM POLICY FOR &enforce_username..POLICY
new  1: CREATE OR REPLACE SYNONYM POLICY FOR protect.POLICY
Synonym created.

old  1: CREATE OR REPLACE SYNONYM POLICYGROUP FOR &enforce_username..POLICYGROUP
new  1: CREATE OR REPLACE SYNONYM POLICYGROUP FOR protect.POLICYGROUP
Synonym created.

old  1: CREATE OR REPLACE SYNONYM DATAOWNER FOR &enforce_username..DATAOWNER
new  1: CREATE OR REPLACE SYNONYM DATAOWNER FOR protect.DATAOWNER
Synonym created.

old  1: CREATE OR REPLACE SYNONYM DATAOWNEREMAIL FOR &enforce_username..DATAOWNEREMAIL
new  1: CREATE OR REPLACE SYNONYM DATAOWNEREMAIL FOR protect.DATAOWNEREMAIL
Synonym created.

old  1: CREATE OR REPLACE SYNONYM INCIDENTSTATUS FOR &enforce_username..INCIDENTSTATUS
new  1: CREATE OR REPLACE SYNONYM INCIDENTSTATUS FOR protect.INCIDENTSTATUS
Synonym created.

```

Result which shows the old and new views

```
View created.  
Disconnected from Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production  
C:\Training Files\SQL>
```

View created and disconnect from the oracle database

Exercise 3:**Verify Incident Data Views Creation**

After running the user creation setup scripts, it is important to verify that the incident data views were created successfully.

```
View created.  
Disconnected from Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production  
C:\Training Files\SQL>sqlplus INCIDENT_VIEW/INCIDENT_VIEW@PROTECT  
SQL*Plus: Release 12.2.0.1.0 Production on Sat Feb 27 01:10:52 2021  
Copyright (c) 1982, 2016, Oracle. All rights reserved.  
Last Successful login time: Sat Feb 27 2021 01:01:22 -08:00  
Connected to:  
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production
```

Verifying whether the incident data views are created or not

```
SQL*Plus: Release 12.  
Copyright (c) 1982, 2016, Oracle. All rights reserved.  
Last Successful login time: Sat Feb 27 2021 01:01:22 -08:00  
Connected to:  
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production  
SQL> select VIEW_NAME from USER_VIEWS;  
VIEW_NAME  
-----  
CUSTOM_ATTRIBUTES  
CUSTOM_ATTRIBUTE_DEFINITIONS  
DETECTION_SERVERS  
DISCOVER_ACL_ENTRIES  
DISCOVER_CONDITION_VIOLATIONS  
DISCOVER_CONTENTS  
DISCOVER_CONTENT_COMPONENTS  
DISCOVER_CONTENT_ORIGINATORS  
DISCOVER_CONTENT_RECIPIENTS  
DISCOVER_INCIDENTS  
DISCOVER_MSG_ITEM_METADATA  
VIEW_NAME  
-----  
DISCOVER_TARGETS  
DISCOVER_VIOLATIONS  
ENDPOINT_CONDITION_VIOLATIONS  
ENDPOINT_CONTENTS  
ENDPOINT_CONTENT_COMPONENTS  
ENDPOINT_CONTENT_ORIGINATORS  
ENDPOINT_CONTENT_RECIPIENTS  
ENDPOINT INCIDENTS
```

Displaying the different views

```
DETECTION_SERVERS
DISCOVER_ACL_ENTRIES
DISCOVER_CONDITION_VIOLATIONS
DISCOVER_CONTENTS
DISCOVER_CONTENT_COMPONENTS
DISCOVER_CONTENT_ORIGINATORS
DISCOVER_CONTENT_RECIPIENTS
DISCOVER INCIDENTS
DISCOVER_MSG_ITEM_METADATA

VIEW_NAME
-----
DISCOVER_TARGETS
DISCOVER_VIOLATIONS
ENDPOINT_CONDITION_VIOLATIONS
ENDPOINT_CONTENTS
ENDPOINT_CONTENT_COMPONENTS
ENDPOINT_CONTENT_ORIGINATORS
ENDPOINT_CONTENT_RECIPIENTS
ENDPOINT INCIDENTS
EP INCIDENT JUSTIFICATIONS
EP JUSTIFICATION_LABELS
INCIDENT_STATUSES

VIEW_NAME
-----
MOBILE_CONDITION_VIOLATIONS
MOBILE_CONTENTS
MOBILE_CONTENT_COMPONENTS
MOBILE_CONTENT_ORIGINATORS
MOBILE_CONTENT_RECIPIENTS
MOBILE INCIDENTS
NETWORK_CONDITION_VIOLATIONS
NETWORK_CONTENTS
NETWORK_CONTENT_COMPONENTS
NETWORK_CONTENT_ORIGINATORS
```

Displaying the different views

```
ENDPOINT_CONTENTS
ENDPOINT_CONTENT_COMPONENTS
ENDPOINT_CONTENT_ORIGINATORS
ENDPOINT_CONTENT_RECIPIENTS
ENDPOINT INCIDENTS
EP INCIDENT JUSTIFICATIONS
EP JUSTIFICATION_LABELS
INCIDENT_STATUSES

VIEW_NAME
-----
MOBILE_CONDITION_VIOLATIONS
MOBILE_CONTENTS
MOBILE_CONTENT_COMPONENTS
MOBILE_CONTENT_ORIGINATORS
MOBILE_CONTENT_RECIPIENTS
MOBILE INCIDENTS
NETWORK_CONDITION_VIOLATIONS
NETWORK_CONTENTS
NETWORK_CONTENT_COMPONENTS
NETWORK_CONTENT_ORIGINATORS
NETWORK_CONTENT_RECIPIENTS

VIEW_NAME
-----
NETWORK INCIDENTS
POLICIES
POLICY_GROUPS
PROTOCOLS

37 rows selected.

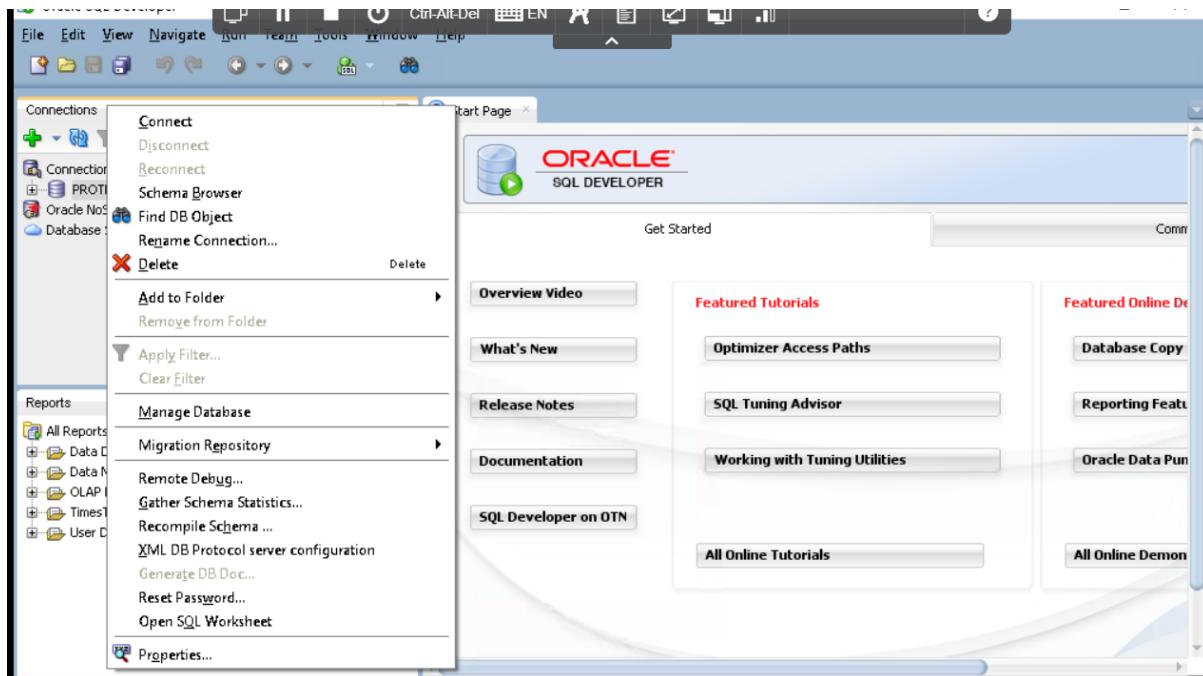
SQL> -
```

Displaying the different views

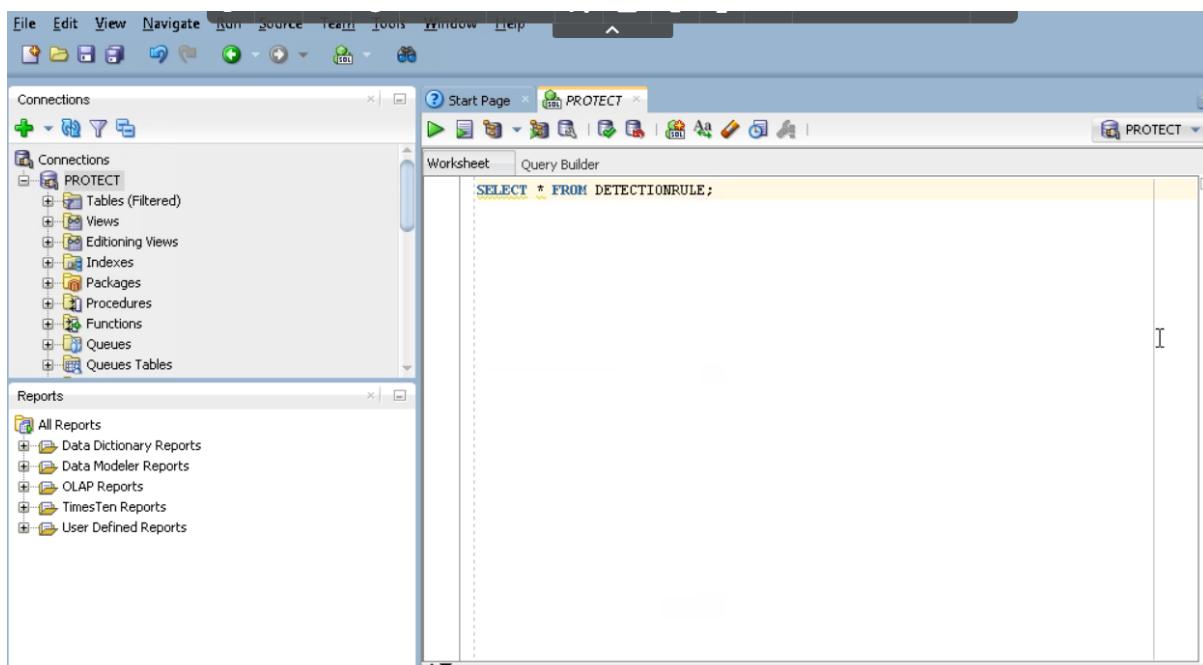
Exercise 4:

After successfully executing the user creation and set up scripts and verifying that the views are working, it is time to query the database using the incident data views.

Incident data views enable the administrator to produce highly customized report by using the configured views and sql queries. Due to the complexity of this query , a few queries have been created which saves the time



Connecting to the protect.



Connected and executing the query

The screenshot shows the Oracle SQL Developer interface. The left sidebar displays connections to 'PROTECT' and various reports. The central workspace contains a 'Worksheet' tab with the SQL query: 'SELECT * FROM DETECTIONRULE;'. Below it is a 'Query Result' tab showing the execution details: 'All Rows Fetched: 64 in 0.125 seconds'. The result set is a table with columns: TOLEVELCONDITIONID, POLICYID, NAME, and ISEXCEPT. The data is as follows:

TOLEVELCONDITIONID	POLICYID	NAME	ISEXCEPT
1	8	Credit Card Detection	
2	188	Credit card Detection	
3	131	Credit Card Detection	
4	68	Credit Card Detection	
5	195	Drug Process Detection	
6	75	Drug Process Detection	
7	15	Drug Process Detection	

Result after executing the query.

The screenshot shows the Oracle SQL Developer interface. The left sidebar displays connections to 'PROTECT' and various reports. The central workspace contains a 'Worksheet' tab with the SQL query: 'SELECT * FROM DETECTIONRULE;'. Below it is a 'Query Result' tab showing the execution details: 'All Rows Fetched: 64 in 0.125 seconds'. The result set is a table with columns: TOLEVELCONDITIONID, POLICYID, NAME, and ISEXCEPT. The data is as follows:

TOLEVELCONDITIONID	POLICYID	NAME	ISEXCEPT
58	146	SSN and Treatment Keywords	
59	147	SSN and Disease Keywords	
60	148	SSN and Drug Codes	
61	203	SSN and Drug Keywords	
62	204	SSN and Treatment Keywords	
63	205	SSN and Disease Keywords	
64	206	SSN and Drug Codes	

Result after executing the query

Worksheet

```
SELECT * FROM ENDPOINT INCIDENTS;
```

Query Result

ENDPOINT INCIDENT ID	ENDPOINT CONTENT ID	INCIDENT STATUS ID	POLICY ID	POLICY VERSION
1	412	347	1	102
2	441	366	1	102
3	415	350	1	101
4	418	352	1	102
5	422	355	1	102
6	421	356	1	102
7	425	356	1	101

Result after executing the query on endpoint.

Worksheet

```
SELECT * FROM ENDPOINT INCIDENTS;
```

Query Result

ENDPOINT INCIDENT ID	ENDPOINT CONTENT ID	INCIDENT STATUS ID	POLICY ID	POLICY VERSION
21	436	364	1	102
22	437	365	1	102
23	438	365	1	101
24	413	348	1	102
25	414	349	1	102
26	429	359	1	102
27	442	368	1	105

Result after executing the query

The screenshot shows the PROTECT software interface. On the left, there are two panes: 'Connections' and 'Reports'. The 'Connections' pane lists various database objects like DISCOVER_TARGETS, DISCOVER_VIOLATIONS, etc. The 'Reports' pane shows 'All Reports' and 'User Defined Reports' sections, with 'Network Incidents' selected. In the center, a 'Worksheet' tab is active with the SQL query `SELECT * FROM ENDPOINT INCIDENTS;`. A 'Select Connection' dialog box is open over the worksheet, showing a dropdown for 'Connection' set to 'PROTECT' and buttons for 'Help', 'OK', and 'Cancel'. Below the worksheet, a results grid displays 27 rows of data from the 'ENDPOINT INCIDENTS' table. The columns are labeled: ENDPOINT INCIDENT_ID, ENDPOINT CONTENT_ID, INCIDENT STATUS_ID, POLICY_ID, and POLICY VERSION.

ENDPOINT INCIDENT_ID	ENDPOINT CONTENT_ID	INCIDENT STATUS_ID	POLICY_ID	POLICY VERSION
21	436	364	1	102
22	437	365	1	102
23	438	365	1	101
24	413	348	1	102
25	414	349	1	102
26	429	359	1	102
27	442	368	1	105

Process in order to display the network incidents.

This screenshot shows the PROTECT software interface again. The 'Connections' and 'Reports' panes are identical to the previous screenshot. The 'Worksheet' tab is now inactive, and the 'Network Incidents' report is active in the center. The results grid displays 20 rows of data from the 'NETWORK INCIDENTS' table. The columns are labeled: EVENT TYPE ID, NETWORK CONTENT ID, EVENT DATE, and POLICY NAME.

EVENT_TYPE_ID	NETWORK_CONTENT_ID	EVENT_DATE	POLICY_NAME
1	2	342 24-FEB-21 10.37.09.000000000 PM	Simplified PCI (EDM/DCM)
2	2	342 24-FEB-21 10.37.09.000000000 PM	Simplified PCI (EDM/DCM)
3	2	342 24-FEB-21 10.37.09.000000000 PM	Simplified PII (DCM)
4	2	351 25-FEB-21 02.15.43.000000000 AM	Simplified PII (DCM)
5	2	351 25-FEB-21 02.15.43.000000000 AM	Simplified PCI (EDM/DCM)
6	2	351 25-FEB-21 02.15.43.000000000 AM	Simplified PCI (EDM/DCM)
7	2	358 25-FEB-21 08.30.31.000000000 AM	Simplified PII (DCM)
8	2	358 25-FEB-21 08.30.31.000000000 AM	Simplified PCI (EDM/DCM)
9	2	358 25-FEB-21 08.30.31.000000000 AM	Simplified PCI (EDM/DCM)
10	2	343 24-FEB-21 11.00.05.000000000 PM	Simplified PCI (EDM/DCM)
11	2	343 24-FEB-21 11.00.05.000000000 PM	Simplified PCI (EDM/DCM)
12	2	343 24-FEB-21 11.00.05.000000000 PM	Simplified PII (DCM)
13	2	344 24-FEB-21 11.07.32.000000000 PM	Simplified PII (DCM)
14	2	344 24-FEB-21 11.07.32.000000000 PM	Simplified PCI (EDM/DCM)
15	2	344 24-FEB-21 11.07.32.000000000 PM	Simplified PCI (EDM/DCM)
16	2	345 24-FEB-21 11.17.53.000000000 PM	Simplified PII (DCM)
17	2	345 24-FEB-21 11.17.53.000000000 PM	Simplified PCI (EDM/DCM)
18	2	345 24-FEB-21 11.17.53.000000000 PM	Simplified PCI (EDM/DCM)
19	2	354 25-FEB-21 02.28.54.000000000 AM	Simplified PII (DCM)
20	2	354 25-FEB-21 02.28.54.000000000 AM	Simplified PCI (EDM/DCM)

Displaying the network incidents.

The screenshot shows the PROTECT software interface with the following details:

- Connections:** A tree view on the left showing various monitoring categories like DISCOVER_TARGETS, DISCOVER_VIOLATIONS, etc.
- Reports:** A list of reports including All Reports, Data Dictionary Reports, Data Modeler Reports, OLAP Reports, TimesTen Reports, User Defined Reports, Discover Incidents, Endpoint Incidents, and Network Incidents. The "Network Incidents" report is selected.
- Network Incidents:** The main pane displays a table of network incidents with the following columns: POLICY_NAME, RESPONSE_ACTION, CONDITION_VIOLATION_COUNT, and INCIDENT_STAT.

POLICY_NAME	RESPONSE_ACTION	CONDITION_VIOLATION_COUNT	INCIDENT_STAT
1:00 PM Simplified PCI (EDM/DCM)	0	100	incident.stat
2:00 PM Simplified PCI (EDM/DCM)	0	79	incident.stat
3:00 PM Simplified PII (DCM)	0	100	incident.stat
4:00 AM Simplified PII (DCM)	0	100	incident.stat
5:00 AM Simplified PCI (EDM/DCM)	0	100	incident.stat
6:00 AM Simplified PCI (EDM/DCM)	0	79	incident.stat
7:00 AM Simplified PII (DCM)	1	100	incident.stat
8:00 AM Simplified PCI (EDM/DCM)	0	100	Escalated
9:00 AM Simplified PCI (EDM/DCM)	0	79	Escalated
10:00 PM Simplified PCI (EDM/DCM)	0	100	incident.stat
11:00 PM Simplified PCI (EDM/DCM)	0	79	incident.stat
12:00 PM Simplified PII (DCM)	0	100	incident.stat
13:00 PM Simplified PII (DCM)	0	100	incident.stat
14:00 PM Simplified PCI (EDM/DCM)	0	100	incident.stat
15:00 PM Simplified PCI (EDM/DCM)	0	79	incident.stat
16:00 PM Simplified PII (DCM)	0	100	incident.stat
17:00 PM Simplified PCI (EDM/DCM)	0	100	incident.stat
18:00 PM Simplified PCI (EDM/DCM)	0	79	incident.stat
19:00 AM Simplified PII (DCM)	0	100	incident.stat
20:00 AM Simplified PCI (EDM/DCM)	0	100	incident.stat

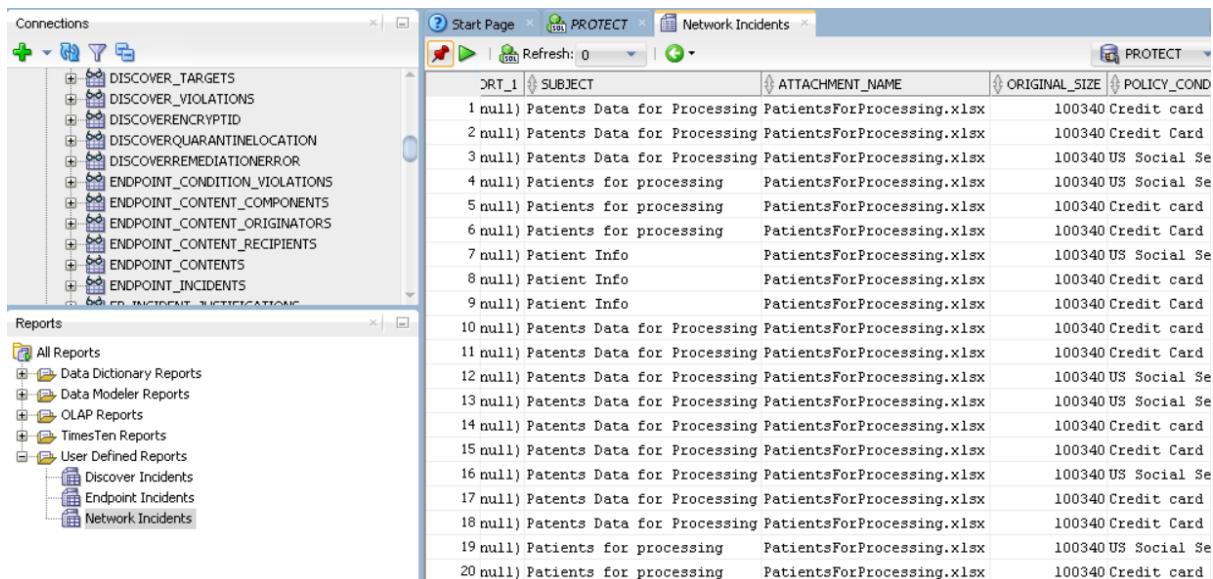
Displaying the network incidents.

The screenshot shows the PROTECT software interface with the following details:

- Connections:** A tree view on the left showing various monitoring categories like DISCOVER_TARGETS, DISCOVER_VIOLATIONS, etc.
- Reports:** A list of reports including All Reports, Data Dictionary Reports, Data Modeler Reports, OLAP Reports, TimesTen Reports, User Defined Reports, Discover Incidents, Endpoint Incidents, and Network Incidents. The "Network Incidents" report is selected.
- Network Incidents:** The main pane displays a table of network incidents with the following columns: INCIDENT_STATUS_NAME, SENDER_IDENTIFIER, IP_ADDRESS, PORT, and RECIPIENT_IDENTIFIER.

INCIDENT_STATUS_NAME	SENDER_IDENTIFIER	IP_ADDRESS	PORT	RECIPIENT_IDENTIFIER
1:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
2:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
3:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
4:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
5:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
6:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
7:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
8:calated	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
9:calated	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
10:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
11:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
12:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
13:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
14:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
15:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
16:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
17:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
18:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
19:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com
20:cident.status.New	JoeUser@symplyfied.com (null)	(null)	(null)	sylvia@anothercompany.com

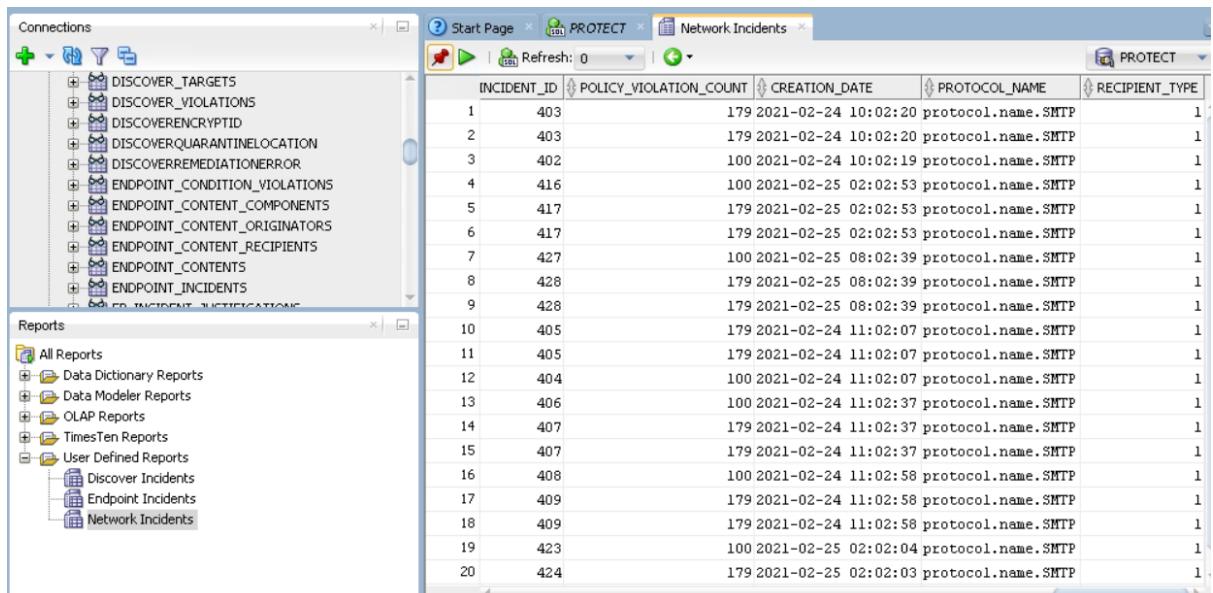
Displaying the network incidents in detail



The screenshot shows the PROTECT tool interface with the 'Network Incidents' tab selected. The left sidebar displays various discovery and reporting options. The main pane shows a table of network incidents with the following columns: SUBJECT, ATTACHMENT_NAME, ORIGINAL_SIZE, and POLICY_COND. The data in the table is as follows:

SUBJECT	ATTACHMENT_NAME	ORIGINAL_SIZE	POLICY_COND
1 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit card
2 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit Card
3 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	US Social Se
4 null) Patients for processing	PatientsForProcessing.xlsx	100340	US Social Se
5 null) Patients for processing	PatientsForProcessing.xlsx	100340	Credit card
6 null) Patients for processing	PatientsForProcessing.xlsx	100340	Credit Card
7 null) Patient Info	PatientsForProcessing.xlsx	100340	US Social Se
8 null) Patient Info	PatientsForProcessing.xlsx	100340	Credit card
9 null) Patient Info	PatientsForProcessing.xlsx	100340	Credit Card
10 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit card
11 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit Card
12 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	US Social Se
13 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	US Social Se
14 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit card
15 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit Card
16 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	US Social Se
17 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit card
18 null) Patents Data for Processing PatientsForProcessing.xlsx	PatientsForProcessing.xlsx	100340	Credit Card
19 null) Patients for processing	PatientsForProcessing.xlsx	100340	US Social Se
20 null) Patients for processing	PatientsForProcessing.xlsx	100340	Credit card

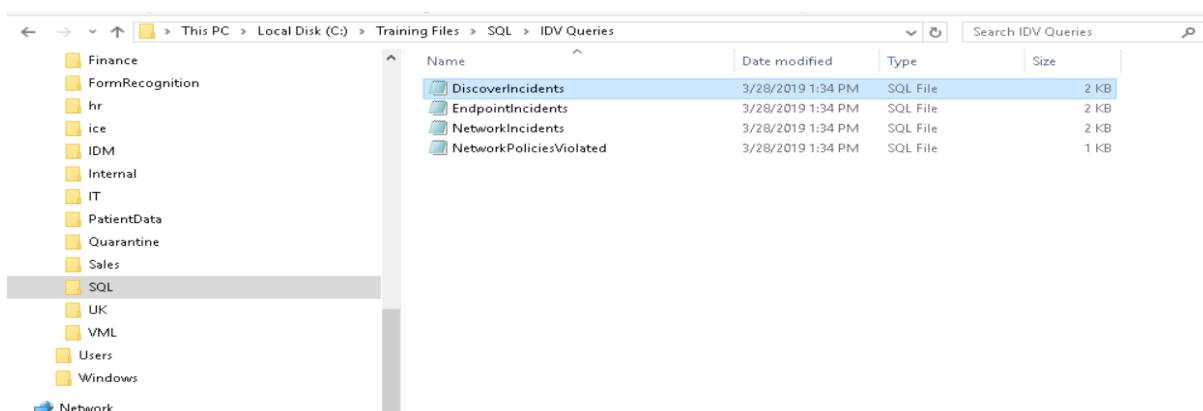
Displaying the network incidents in detail



The screenshot shows the PROTECT tool interface with the 'Network Incidents' tab selected. The left sidebar displays various discovery and reporting options. The main pane shows a table of network incidents with the following columns: INCIDENT_ID, POLICY_VIOLATION_COUNT, CREATION_DATE, PROTOCOL_NAME, and RECIPIENT_TYPE. The data in the table is as follows:

INCIDENT_ID	POLICY_VIOLATION_COUNT	CREATION_DATE	PROTOCOL_NAME	RECIPIENT_TYPE
1	403	179 2021-02-24 10:02:20	protocol.name.SMTP	1
2	403	179 2021-02-24 10:02:20	protocol.name.SMTP	1
3	402	100 2021-02-24 10:02:19	protocol.name.SMTP	1
4	416	100 2021-02-25 02:02:53	protocol.name.SMTP	1
5	417	179 2021-02-25 02:02:53	protocol.name.SMTP	1
6	417	179 2021-02-25 02:02:53	protocol.name.SMTP	1
7	427	100 2021-02-25 08:02:39	protocol.name.SMTP	1
8	428	179 2021-02-25 08:02:39	protocol.name.SMTP	1
9	428	179 2021-02-25 08:02:39	protocol.name.SMTP	1
10	405	179 2021-02-24 11:02:07	protocol.name.SMTP	1
11	405	179 2021-02-24 11:02:07	protocol.name.SMTP	1
12	404	100 2021-02-24 11:02:07	protocol.name.SMTP	1
13	406	100 2021-02-24 11:02:37	protocol.name.SMTP	1
14	407	179 2021-02-24 11:02:37	protocol.name.SMTP	1
15	407	179 2021-02-24 11:02:37	protocol.name.SMTP	1
16	408	100 2021-02-24 11:02:58	protocol.name.SMTP	1
17	409	179 2021-02-24 11:02:58	protocol.name.SMTP	1
18	409	179 2021-02-24 11:02:58	protocol.name.SMTP	1
19	423	100 2021-02-25 02:02:04	protocol.name.SMTP	1
20	424	179 2021-02-25 02:02:03	protocol.name.SMTP	1

Displaying the network incidents in detail



The screenshot shows a Windows File Explorer window displaying files in the 'IDV Queries' folder. The folder contains four SQL files: DiscoverIncidents, EndpointIncidents, NetworkIncidents, and NetworkPoliciesViolated. The details are as follows:

Name	Date modified	Type	Size
DiscoverIncidents	3/28/2019 1:34 PM	SQL File	2 KB
EndpointIncidents	3/28/2019 1:34 PM	SQL File	2 KB
NetworkIncidents	3/28/2019 1:34 PM	SQL File	2 KB
NetworkPoliciesViolated	3/28/2019 1:34 PM	SQL File	1 KB

Sql queries in the IDV queries



The screenshot shows a Windows Notepad window titled "DiscoverIncidents - Notepad". The content of the window is a SQL SELECT statement:

```
SELECT DI.DISCOVER INCIDENT_ID, DI.EVENT_TYPE_ID, DI.DISCOVER_CONTENT_ID, DI.EVENT_DATE, P.POLICY_ID, C.DISCOVER_TARGET_ID AND DI.DISCOVER_CONTENT_ID=DC.DISCOVER_CONTENT_ID AND DI.DISCOVER INCIDENT_DATE >= P.EFFECTIVE_DATE AND DI.DISCOVER INCIDENT_DATE <= P.EXPIRE_DATE
```

To the right of the Notepad window, there is a vertical toolbar labeled "DV Queries" with a dropdown menu. The dropdown menu has a single item "Size" which is currently selected. Below the "Size" item, there are four options: "2 KB", "2 KB", "2 KB", and "1 KB".

Displaying the query.

Exercise 5:

Create the ICT tag policy for File Discovery.

ICT – Information Centric Tagging.

BY adding ICT it allows users to discover and identify files with certain tags as well as content identifiers.

While SYmplified doesn't have ICT to work with files and tag taxonomies that have already been defined and imported into this environment.

In this lab, we will link a tag taxonomy file to the enforce server so it recognizes a defined body of tags which can be used for discovery scans and policy enforcement. Then we will create a policy that looks for those tags.

Information Centric Tagging

Server Credential: Select...

ICT Web Service URL: N/A

Sync daily at: 00:00

Sync Now

Organization	Scope	Sensitivity	Level
--------------	-------	-------------	-------

Setting the new rules on clicking on the edit option

Information Centric Tagging

Server Credential: dlpscan

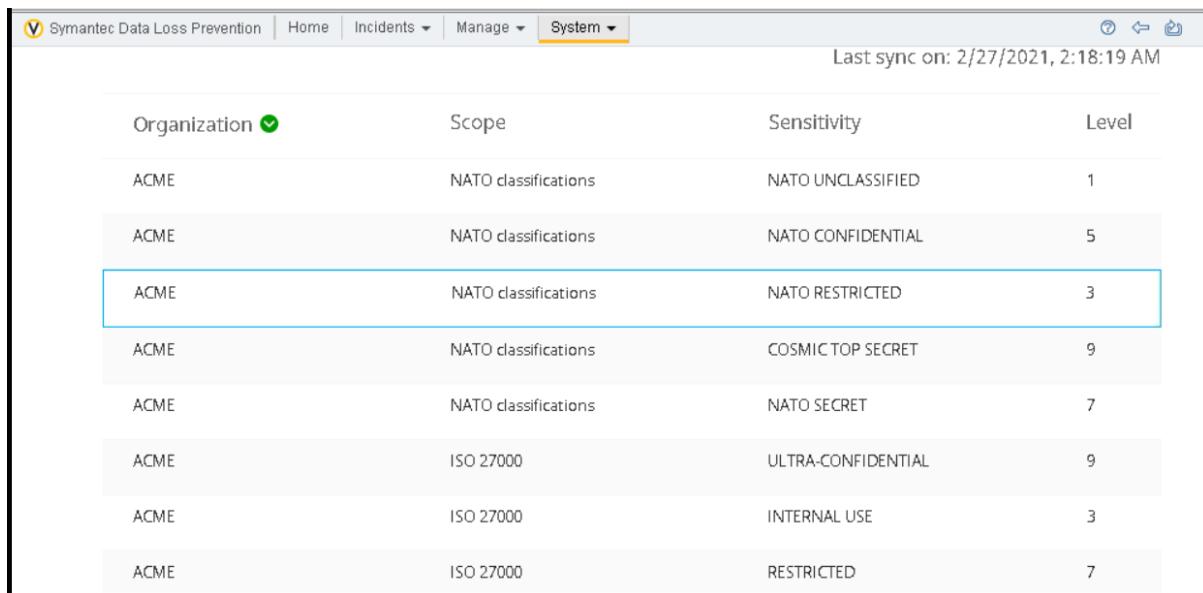
ICT Web Service URL: file:///c:/Training Files/ICTDemoTags.xml

Sync daily at: 00:00

Sync Now

Organization	Scope	Sensitivity	Level
--------------	-------	-------------	-------

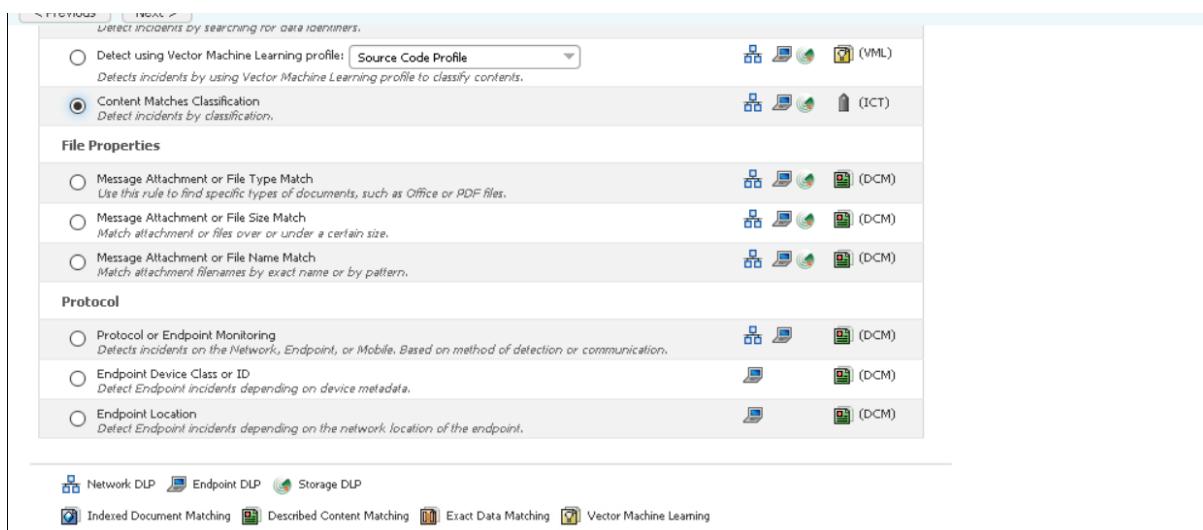
New rules In the Information Centric Tagging



The screenshot shows a table of classification rules under the 'System' tab. The columns are 'Organization', 'Scope', 'Sensitivity', and 'Level'. The rows list various ACME entities and their classification details.

Organization	Scope	Sensitivity	Level
ACME	NATO classifications	NATO UNCLASSIFIED	1
ACME	NATO classifications	NATO CONFIDENTIAL	5
ACME	NATO classifications	NATO RESTRICTED	3
ACME	NATO classifications	COSMIC TOP SECRET	9
ACME	NATO classifications	NATO SECRET	7
ACME	ISO 27000	ULTRA-CONFIDENTIAL	9
ACME	ISO 27000	INTERNAL USE	3
ACME	ISO 27000	RESTRICTED	7

Displaying the list of new tags.



The screenshot shows the configuration interface for incident detection rules. It includes sections for 'File Properties' and 'Protocol'.

- File Properties:**
 - Detect using Vector Machine Learning profile: **Source Code Profile** (VML)
 - Content Matches Classification (ICT)
 - Message Attachment or File Type Match (DCM)
 - Message Attachment or File Size Match (DCM)
 - Message Attachment or File Name Match (DCM)
- Protocol:**
 - Protocol or Endpoint Monitoring (DCM)
 - Endpoint Device Class or ID (DCM)
 - Endpoint Location (DCM)

At the bottom, there are icons for various matching types: Network DLP, Endpoint DLP, Storage DLP, Indexed Document Matching, Described Content Matching, Exact Data Matching, and Vector Machine Learning.

Configuring the new policy

General

Rule Name: ICT ISO 27000 Public

Severity

Default: Info

Conditions

Content Matches Classification

- Content is classified
- Content is not classified
- Content matches

Operator: Equals Company: ACME Scope: ISO 27000 Level: (1) PUBLIC Match On: Envelope

Configuring the new policy.

General

Name: Information Centric Tagging (DCM)

Description:

Policy Label:

Policy Group: Classification

Status: Active [suspend]

Detection

Add Rule Add Exception

Rules:

- **ICT ISO 27000 Public (ICT):** Match Symantec Information Centric Tagging Classification; Operator: "Equals" Company: "ACME" Scope: "ISO 27000" Level: "(1) PUBLIC" Severity: Info. Look in envelope, attachments.

Exceptions:

This policy contains no exceptions.

Adding the rules for the new policy

The screenshot shows the 'Configure Policy - Edit Rule' dialog. At the top, there are 'OK' and 'Cancel' buttons. The main area is divided into sections: 'General', 'Severity', and 'Conditions'. In the 'General' section, the 'Rule Name' is set to 'ICT ISO 27000 Internal Use'. Under 'Severity', the 'Default' is set to 'Medium'. The 'Conditions' section contains a single condition: 'Content Matches Classification'. This condition is set to 'Content matches' (radio button selected). Below this, there are dropdown menus for 'Match On': 'Envelope' (checked), 'Subject', 'Body', and others. To the right of these dropdowns are buttons for 'Equals', 'ACME', 'ISO 27000', and '(3) INTERNAL' (which is highlighted in blue), followed by an 'OR' button.

Ruled for Internal use

The screenshot shows the 'Configure Policy - Edit Rule' dialog for a different rule. The 'Rule Name' is 'ICT ISO 27000 Confidential'. The 'Severity' is set to 'High'. The 'Conditions' section contains a single condition: 'Content Matches Classification'. This condition is set to 'Content matches' (radio button selected). Below this, there are dropdown menus for 'Match On': 'Envelope' (checked), 'Subject', 'Body', and others. To the right of these dropdowns are buttons for 'Equals', 'ACME', 'ISO 27000', and '(8) CONFIDEN' (which is highlighted in blue), followed by an 'OR' button.

Rules for confidential

The policy 'Information Centric Tagging (DCM)' was saved successfully.						
New Import Export Download Details Activate Suspend Delete Clone Assign Group Filter Clear						
Showing 1 to 7 of 7 entries						
	Status	Name	Description	Policy Group	Last Modified	
<input type="checkbox"/>		HIPAA and HITECH (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy may also be used for organizations which are not subject to HIPAA but want to control PHI data. Health Information Technology for Economic and Clinical Health Act (HITECH) is the first national law that mandates breach notification for PHI.	Simplified PII Policies	February 24, 2021 4:56:33 AM PST	
<input type="checkbox"/>		Information Centric Tagging (DCM)		Classification	February 27, 2021 2:26:28 AM PST	
<input type="checkbox"/>		Simplified Drug Process Detection (IDM)		Default Policy Group	February 25, 2021 2:43:01 AM PST	
<input type="checkbox"/>		Simplified PCI (EDM/DCM)		Simplified PCI Policies	February 25, 2021 10:51:54 AM PST	

Indicates that the new policy is added

Exercise 6:

Now that the tag taxonomy and related policy has been added we can include these tag classifications in your discovery scans. In this exercise you will look for files on the endpoint computers that have been tagged with ISO-27000 tags , and will be very cautious about the files which are tagged as restricted or confidential.

Symantec Data Loss Prevention | Home | Incidents | Manage | System | Administrator

Manage > Discover Scanning > Discover Targets > Add File System Target

Save Cancel

General Targeting Scanned Content Filters Advanced Protect

General

Name * ICT Scan

Policy Groups *

- Classification
- Default Policy Group
- Simplified PCI Policies
- Simplified PII Policies

Scan Execution

Scan only new or modified items (incremental scan)

- Scan all items for next scan. Subsequent scans will be incremental

 Always scan all items (full scan)

Use Incremental indexes from

(Please select one or more)

Available Discover Targets

- Windows File Share Scan
- File Share Scan (FMDT)

Selected Discover Targets

Adding the file system target

Symantec Data Loss Prevention | Home | Incidents | Manage | System | Administrator

Manage > Discover Scanning > Discover Targets > Add File System Target

Save Cancel

General Targeting **Scanned Content** Filters Advanced Protect

Default User

Use Saved Credentials: dlpscan (simplified\dlpscan)

Use These Credentials:

Name	
Password	
Confirm Password	

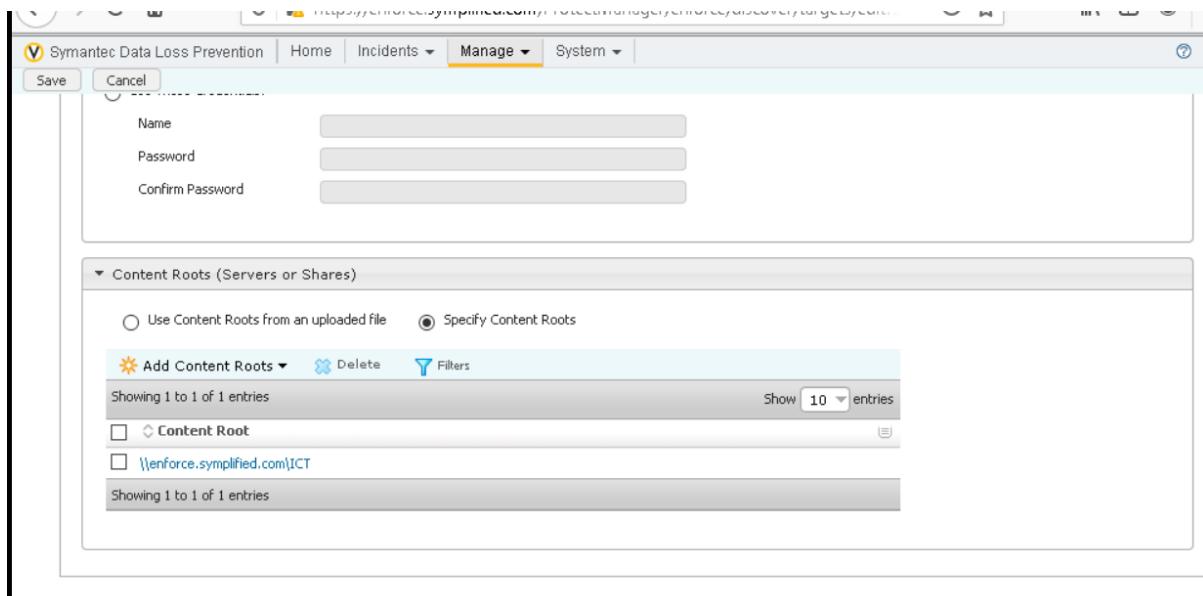
Content Roots (Servers or Shares)

Use Content Roots from an uploaded file Specify Content Roots

Add Content Roots Delete Filters

Showing 1 to 1 of 1 entries Show 10 entries

Setting the rules in Scanned Content



Rules added and need to save on this step

The screenshot shows the 'Scan Detail' page under 'Discover Scanning > Discover Targets'. The 'General' section includes fields for Target Type (File System), Target Name (ICT Scan), Status (Completed), Scan Type (Full), Start Time (2/27/21 2:31 AM), and End Time (2/27/21 2:31 AM). The 'Scan Statistics' section shows Processed (Share: 1 of 1), Run Time (00:00:00), Items Scanned (6), Bytes Scanned (871.46 KB (892,373 Bytes)), Errors (0), and Current Incident Count (5). The 'Recent Scan Errors' section has a 'Download Full Error Report' button. The 'Recent Scan Activity' section shows log entries for the scan process, with a 'Download Full Activity Report' button. The log entries are:

Date/Time	Level	Message
2/27/21 2:31:08 AM	INFO	Scan started
2/27/21 2:31:08 AM	INFO	Started scanning Share: //enforce.simplified.com/ICT
2/27/21 2:31:09 AM	INFO	Finished 6 items, 892,373 bytes; filtered 0 items
2/27/21 2:31:09 AM	INFO	Finished scanning Share: //enforce.simplified.com/ICT
2/27/21 2:31:09 AM	INFO	Scan finished

We can clearly see that incident count was 5.

Incident Roots at Risk		Applied Filters	Scan	Severity	Matches	Severity	Status
Type	Location / Target / Scan	File Owner	ID / Policy				
<input type="checkbox"/>	Location //enforce.simplified.com/ICT/Merger_Contract.doc Target Scan ICT Scan 2/27/21 2:31 AM	BUILTIN\Administrators	00000465 Information Centric Tagging (DCM)	1		New	
<input type="checkbox"/>	Location //enforce.simplified.com/ICT/Federal NRC license.pdf Target Scan ICT Scan 2/27/21 2:31 AM	BUILTIN\Administrators	00000464 Information Centric Tagging (DCM)	1		New	
<input type="checkbox"/>	Location //enforce.simplified.com/ICT/Customer credit card info-High Sev.xlsx Target Scan ICT Scan 2/27/21 2:31 AM	BUILTIN\Administrators	00000463 Information Centric Tagging (DCM)	1		New	
<input type="checkbox"/>	Location //enforce.simplified.com/ICT/Hardware price list.xls Target Scan ICT Scan 2/27/21 2:31 AM	BUILTIN\Administrators	00000462 Information Centric Tagging (DCM)	1		New	
<input type="checkbox"/>	Location //enforce.simplified.com/ICT/BingoWinners.docx Target Scan ICT Scan 2/27/21 2:31 AM	BUILTIN\Administrators	00000461 Information Centric Tagging (DCM)	1		New	

We can clearly see the 5 incidents.