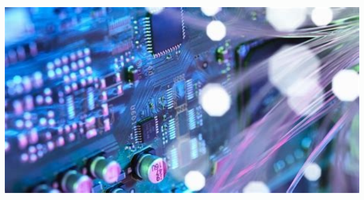
Symantec dlp 15. 5 admin guide



Symantec dlp 15.5 admin guide.

Symantec Data Loss Prevention 15.5 Administration Lab Guide Copyright © 2019 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. THIS PUBLICATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION. THE INFORMATION CONTAINED HEREIN IS SUBJECT TO CHANGE WITHOUT NOTICE. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher. Lab Guide revision: 190626 Symantec Corporation World Headquarters 350 Ellis Street Mountain View, CA 94043 United States Course Developers Lead Subject Matter Experts Technical Contributors and Reviewers Ernest Simmons Ernest Simmons Ryan Hollitz Chloe Pinteaux-Jones Alejandro Loza Jim Martin Kevin Burtt John Gruhn Ken Baldwin Boon Hing Khoo Carlos Aragon Willian Castro Jesse Gonzales Joshua Carter Alexander Harris Ramzi Abiantoun Ajil Koshy Train. Certify. Succeed. Learn more about Symantec certifications here: ii Symantec Data Loss Prevention 15.5 Administration Lab Guide Copyright © 2019 Symantec Corporation. All Rights Reserved Table of Contents Symantec Data Loss Prevention 15.5 Administration Lab Guide Introduction .....1 Identifying and Describing Confidential Data .....3 Tour of the Enforce Console ..... 4 Create Policy Groups ..... 6 Configure a Policy for PII Detection ..... 7 Configure a Policy for PCI Compliance ..... 9 Configure an Alternate Policy for PII Compliance ..... 13 Configure a Policy to Protect Confidential Documents ..... 15 Configure a Policy to Protect Source Code ..... 17 Configure a Policy for Form Recognition ..... 19 Use a Template to Add a DLP Policy ..... 21 Export Policies for Use at a DR Site ..... 23 Configure Optical Character Recognition ..... 24 Locating Confidential Data Stored on Premises and in the Cloud ..... 25 Run a Content Enumeration Scan ..... 26 Scan a Windows Target ..... 28 Scan Endpoint Computers for Confidential Data ..... 30 Scan Server for Confidential Data using EMDI ..... 32 Configure a Global Policy for PII Compliance ..... 35 Understanding How Confidential Data Is Being Used ..... 37 Configure Network Prevent for Email to Monitor SMTP Messages ..... 38 Use Network Prevent for Email to Monitor SMTP Messages ..... 40 Monitor Endpoint Activity -- Email ..... 43 Monitor Endpoint Activity -- Third-Party Apps ..... 46 Monitor Endpoint Activity -- Copy/Paste ..... 48 Educating Users to Adopt Data Protection Practices ..... 51 Configure the Active Directory Lookup Plugin ..... 52 Configure Email Notifications ..... 55 Configure Onscreen Notifications ..... 59 Preventing Unauthorized Exposure of Confidential Data ..... 63 Configure SMTP Blocking ..... 64 Test Optical Character Recognition (OCR) and the “HIPAA and HITECH (including PHI)” Policy ..... 67 Configure Endpoint Blocking ..... 70 Table of Contents iii Copyright © 2019 Symantec Corporation. All Rights Reserved Configure Endpoint User Cancel ..... 73 Scan and Quarantine Files on a Server File Share Target ..... 76 Scan and Quarantine Files on an Endpoint Target ..... 79 Remediating Data Loss Incidents and Tracking Risk Reduction ..... 83 Configure Roles and Users ..... 84 Use Reports to Track Risk Exposure and Reduction ..... 87 Define Incident Statuses and Status Groups ..... 89 Configure and Use Smart Responses ..... 91 Schedule and Send Reports ..... 93 Enhancing Data Loss Prevention with Integrations ..... 95 Create the Views Schema and User ..... 96 Run the Incident Data View Setup Script ..... 98 Verify Incident Data Views Creation ..... 99 Use Incident Data Views ..... 100 Create ICT Tag Policy for File Discovery ..... 102 Scan for File Tags using Network Discover ..... 104 iv Symantec Data Loss Prevention 15.5 Administration Lab Guide Copyright © 2019 Symantec Corporation. All Rights Reserved Introduction Symplified Healthcare is a private health system with US locations in California, Utah, and Texas, as well as recent expansions into Canada and Mexico with one location in each country. In the last five years, Symplified Healthcare has worked at developing better treatments and potential cures for cancer, conducting state-of-the-art research, and creating new drug testing protocols. Due to the nature of current healthcare systems, Symplified Healthcare processes thousands of transactions for electronic payments, insurance claims, diagnostics, and other operations. These transactions generate thousands of electronic records that must be kept immediately accessible to all authorized parties but at the same time safeguarded from any form of unauthorized access. Symplified has always had a well-funded and supported IT team that works on securing patient information and web servers from outside attacks but until recently has shown little concern about how sensitive information has been handled within the organization. However, recently in the past month, an employee of a competing hospital was caught disseminating private patient information to outside organizations for profit. This incident demonstrated the importance of ensuring that critical information does not leave the hospital network and get into the wrong hands. At Symplified Healthcare the number of back-end systems and endpoint computers is immense. The majority of the back-end administrative systems are still managed on-premises, but IT management is gradually moving to adopt a hybrid of on-premises and public cloud infrastructure. There are endpoint computers at all nurses’ stations, examination rooms, and reception areas in addition to the endpoints in the Legal, Finance, and Administration departments. Symplified Healthcare has been improving the healthcare industry by creating software used throughout their locations. Competitors have shown interest in the innovations and have been attempting to replicate the software for their own use. As the new IT Security Manager at Symplified, your task will be to recognize and protect these assets and data from accidental (or deliberate) misuse by internal employees. As we address the needs and requirements of this organization throughout the exercises in this lab guide, we will use the following lab systems. System Name Username Password Enforce Symplified\Administrator train Symplified\Administrator train Endpoint OCR Symplified\joe_user train At different points in the lab, you will be asked to login to these lab virtual machines (VMs). For clarity each exercise will indicate which VM you should be using with headers that look like this: Login to: Enforce Introduction 1 Copyright © 2018 Symantec Corporation. All Rights Reserved Note: If you are prompted to install Windows Updates when using any of the provided VMs, it is recommended that you simply close the Windows Update dialog without running the updates. Updates are not needed for the lab exercises and will only cause delays in using the lab environment. 2 Introduction Copyright © 2018 Symantec Corporation. All Rights Reserved Identifying and Describing Confidential Data At Symplified Healthcare, one of the foremost security responsibilities is to safeguard patient data, including PII (Personally Identifiable Information), as well as financial transaction data from patients, insurance companies, and medical providers. As a manager over IT security, your responsibility is to use Symantec Data Loss Prevention effectively to identify and locate confidential or sensitive data in all areas of the network and come up with a set of policies that will protect that data from both outside influence and internal misuse. In this section, you will compose policies to identify the type of PII that require protection, as well as required PCI compliance for financial transactions. 3 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Tour of the Enforce Console In this exercise, you will become familiar with the Enforce console and where different aspects of the DLP solution are configured. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Double-click the Firefox shortcut on the desktop to launch a web browser window. Note: The browser should start directly at the DLP Enforce console web UI when opened. You can also navigate directly to the console UI start page by entering the following URL into the web browser: 3. From the Symantec Data Loss Prevention Console window, use the following (case-sensitive) credentials to log into the Enforce console: Login: Administrator Password: training 4. View the Home tab. Note that this tab contains a few built-in reports and dashboards. These customizable reports (currently empty) will begin to take shape as the course continues. 5. Click the Incidents tab. On this tab you can view a list of reports and incident lists for each vector. Hovering over the Incidents tab enables you to drill down to specific reports directly. This tab will be used extensively throughout the course. 6. Click the Manage tab. This tab is where you configure policies, response rules, discover targets, and so on. We will use this tab later to create some DLP policies. 4 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 7. Click the System tab. This tab is where all the system-wide configurations are performed. Here it is possible to view the status of the Enforce server, detection servers, endpoint agents, and so on. It is also where users, user roles, and permissions are configured. 8. Direct your attention to the buttons in the top-right area of the Enforce console window. The Help button (console. The Refresh button (The Back button ( ) shows context-sensitive help for the currently displayed page in the Enforce) refreshes the console screen.) returns to the previous page. Note: Using the web browser’s refresh and back buttons to navigate the Enforce console can cause unexpected behavior. Consequently, Symantec recommends that you always use the Enforce console’s refresh and back buttons to avoid navigation issues. End of exercise Exercise 1: Tour of the Enforce Console Copyright © 2019 Symantec Corporation. All Rights Reserved 5 Exercise 2: Create Policy Groups Scenario: Symplified Healthcare deals with many different data types including patient information and credit card information. The Symantec Implementation team has recommended that Symplified create policy groups to help reduce the number of possible false positives or duplicate incidents. Policy groups also allow Symplified to group similar policies together and select which policies should be used to detect data loss. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. On the Enforce Web UI, browse to System > Servers and Detectors > Policy Groups. 2. Click Add. 3. In the Name field, type: Symplified PII Policies 4. (Optional) Add a brief description to the Description field. 5. Click Save. 6. Click Add. 7. In the Name field, type: Symplified PCI Policies 8. (Optional) Add a brief description to the Description field. 9. Click Save. 10. Use the same process to create another group entitled Classification. When finished you should see all three new entries in the list of policy groups along with the original Default Policy Group. End of exercise 6 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 3: Configure a Policy for PII Detection Scenario: Due to the nature of hospitals, Symplified Healthcare deals with patients’ Personally Identifiable Information (PII). It is a concern that this information might be stored or used incorrectly within the organization. You have been tasked with configuring a DLP policy using Described Content Matching (DCM) that will allow the use of data identifiers and keywords to detect where PII data is being used or stored. Because Symplified uses US Social Security Numbers on nearly all of their forms, IT wants to focus on these numbers for their initial detection type, but since Symplified also has locations in Canada and Mexico, ID numbers specific to those countries will also need to be supported. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, Browse to Manage > Policies > Policy List. 2. Click New. 3. Leave the option Add a blank policy selected and click Next. 4. In the Name field, type: Symplified PII (DCM) 5. Next to the “Policy Group” heading, from the drop-down list, select Symplified PII Policies. 6. On the Detection tab, click Add Rule. 7. Under the “Rule Type > Content” heading, select Content Matches Data Identifier. 8. Click the drop-down list, scroll down to the heading “North American Personal Identity” and select US Social Security Number (SSN). 9. Click Next. 10. In the Rule Name field, type: US Social Security Numbers 11. Under the “Conditions” heading, for the Breadth setting, select Medium. Exercise 3: Configure a Policy for PII Detection Copyright © 2019 Symantec Corporation. All Rights Reserved 7 12. Leave all other options at their default values and click OK in the top left. 13. On the Detection tab, click Add Rule again. 14. Under the “Rule Type > Content” heading, select Content Matches Data Identifier. 15. From

the drop-down list, scroll down to the heading “North American Personal Identity” and select Mexican Unique Population Registry Code. 16. Click Next. 17. In the Rule Name field, type: Mexican Unique Population Registry Code Numbers 18. Under the “Conditions” heading, for the Breadth setting, select Medium. 19. Leave all other options at their default values and click OK. 20. On the Detection tab, click Add Rule. 21. Under the “Rule Type > Content” heading, select Content Matches Data Identifier. 22. From the drop-down list, scroll down to the heading “North American Personal Identity” and select Canadian Social Insurance Number. 23. Click Next. 24. In the Rule Name field, type: Canadian Social Insurance Numbers 25. Under the “Conditions” heading, for the Breadth setting, select Medium. 26. Leave all other options at their default values and click OK. 27. In the top left of the Enforce console, click Save. 28. You should now see the Symplified PII (DCM) Policy listed with a green circle indicating it is an active policy. End of exercise 8 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 4: Configure a Policy for PCI Compliance Scenario: Symplified Healthcare receives payments from patients via credit card on a daily basis. These credit card numbers are encrypted and stored directly in a secured database; however, a few people in the finance department do have access to the unencrypted data. The VP of Finance would like to ensure this data is being handled according to PCI standards because a PCI compliance audit is being performed in eight weeks. Due to the structured nature of the data, using the Exact Data Matching (EDM) detection method would likely be the best method for detecting data from the database. It will be necessary to create a policy with a rule using the Exact Data Matching profile as well as a “catchall” rule to detect any credit card information being stored or transmitted on the Symplified network. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Data Profiles > Exact Data. The first step in creating the PCI policy is to import the structured data into the Enforce console by creating an Exact Data Profile. The policy will use this profile to detect the PCI data. 2. Click Add Exact Data Profile. 3. In the Name field, type: Patient Data Extract 4. Select the option Upload Data Source to Server Now. 5. Click Browse and navigate to C:\Training Files\EDM. 6. Select the PatientDataExtractLarge.dat file and click Open. 7. Next to the “Column Names” heading, select the option Read first row as column names. 8. Leave all other options at their defaults and click Next. Exercise 4: Configure a Policy for PCI Compliance Copyright © 2019 Symantec Corporation. All Rights Reserved 9 9. Under Field Mappings, use the drop-down lists under the “System Field” heading to match the data source fields to the system fields as specified in the following table: 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 10. Next to Check mappings against policy template, select Payment Card Industry Data Security Standard. 11. Click Check now. A green bar should appear at the top of the screen, indicating that the required fields are mapped correctly for the PCI template. 12. Under the “Indexing” heading, select the option Submit Indexing Job on Save. 13. Click Finish at top. Note: The indexing job will now be submitted to the Enforce server. You can click the console’s Refresh button in the top right of the screen to update the indexing status. The Latest Active Version will be blank unless the arrow to the left of Patient Data Extract is clicked. (NOTE: you do not have to wait for the indexing to finish to continue with this lab exercise.) 14. Browse to Manage > Policies > Policy List. 15. Click New. 16. Leave Add a blank policy selected and click Next. 17. In the Name field, type: Symplified PCI (EDM/DCM) 18. Next to the “Policy Group” heading, from the drop-down list, select Symplified PCI Policies. 19. On the Detection tab, click Add Rule. 20. Under the “Rule Type > Content” heading, select the option Content Matches Exact Data From. 10 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 21. Ensure that Patient Data Extract is selected in the drop-down list. 22. Click Next. 23. In the Rule Name field, type: Credit Card Detection 24. Under the “Conditions > Match” heading, change the value in the first drop-down list from 1 to 2. 25. Select the following options: Last Name, First Name, Bank Card Number 26. Next to the “Severity” heading, click Add Severity. 27. Change the new severity entry to match the following: Set Severity to: Medium when match count Is Between from 10 to 25 matches 28. Next to the “Severity” heading, click Add Severity again. 29. Change the new severity entry to match the following: Set Severity to: Low when match count Is Less Than 10 matches 30. Under the “Conditions > Ignore” heading, select the following: Field 1: First Name Field 2: Last Name 31. Click > to add First Name, Last Name to the “Excluded Combinations” box. Note: This excluded combination prevents a match when only the first and last name are found. A match is created only when the bank card number AND either the first and/or last name is found. 32. Click OK. Note: The preceding rule only detects credit card numbers that match the exact data matching (EDM) profile; however, Symplified also wants to create a general “catchall” rule that detects any other credit card numbers that are not part of the EDM profile. 33. On the Detection tab, click Add Rule again. 34. Under the “Rule Type > Content” heading, select the option Content Matches Data Identifier. 35. From the drop-down list, select Financial > Credit Card Number. 36. Click Next. 37. In the Rule Name field, type: Credit Card Catchall 38. Under the “Conditions” heading, for the Breadth setting, select Medium. 39. Click OK. 40. Click Save. Exercise 4: Configure a Policy for PCI Compliance Copyright © 2019 Symantec Corporation. All Rights Reserved 11 Note: You should now see the Symplified PCI (EDM/DCM) Policy listed with a green circle indicating it is an active policy. End of exercise 12 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 5: Configure an Alternate Policy for PII Compliance Scenario: The previous policy to analyze and detect patient social security numbers (from Exercise 3) can be improved by tying the analysis into an existing data set that details the specific patient info needing protection. Since many of the documents with sensitive data correspond to existing patient and customer records stored in a secure database, you decide to utilize that database to validate any data discovered in network documents. Using the Exact Matching Data Identifier (EMDI) detection method you will link a data source to validate any detections found when scanning potentially sensitive documents. This new profile will ensure that confidential data with genuine patient/customer information is recognized as such and the potential for “false positives” is reduced. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Data Profiles > Exact Data. The first step in creating the PCI policy is to import the structured data into the Enforce console by creating an Exact Data Profile. The policy will use this profile to detect the PCI data. 2. Click Add Exact Match Data Identifier Profile. 3. In the Name field, type: Patient Data Extract EMDI 4. Select the option Upload Data Source to Server Now. 5. Click Browse and navigate to C:\Training Files\PatientData. 6. Select the PatientsForProcessing.dat file and click Open. 7. Next to the “Column Names” heading, select the option Read first row as column names. 8. Set the Column Separator Char field to Comma (,). 9. Click Next. Exercise 5: Configure an Alternate Policy for PII Compliance Copyright © 2019 Symantec Corporation. All Rights Reserved 13 10. In the list of data fields, set SSN to Required and select US Social Security Number (SSN) from the Data Identifier list, with a breadth of Medium. Note: If you do not see the list of ten data fields on this screen return to the previous screen and ensure that steps 4-8 were completed correctly.) 11. Leave First and Last set to Optional. Set all other fields (besides SSN) to Ignore. 12. Under Indexing, check the box for Submit Indexing Job on Save. 13. Click Finish at top. You should see the new data profile listing in the Exact Data list. You do not need to wait for the data to finish indexing to continue with this lab exercise. 14. Browse to Manage > Policies > Policy List and click New to create a new policy. 15. Leave Add a blank policy selected and click Next. 16. In the Name field, type: Symplified PII (EMDI) 17. Next to the “Policy Group” heading, from the drop-down list, check the box beside Symplified PII Policies. 18. Click the Suspend link next to Status to have this policy deactivated for now. 19. On the Detection tab, click Add Rule. 20. Under the “Rule Type > Content” heading, select the option Content Matches Data Identifier. 21. Select US Social Security Number (SSN) from the North American Personal Identity section in the drop-down list and click Next. 22. In the Rule Name field, type: SSN Detection (EMDI) 23. Under Conditions, select Medium as the Breadth value. 24. Under Optional Validators expand the tab, then check the box for Exact Match Data Identifier Check. Note: If you get an “Validation error” message, make sure the Breadth value selected above matches the breadth chosen for your EMDI data profile selected earlier in this lesson; both should be set to Medium. 25. Select Patient Data Extract EMDI from the Profile drop down list. 26. Ensure that SSN is in the Required field, and At least match contains 1. 27. Click OK at top to save the new detection rule. 28. Click Save at top to save the new policy. You should now see the Symplified PII (EMDI) policy listed with a red circle in the Status column indicating the policy is NOT active. End of exercise 14 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 6: Configure a Policy to Protect Confidential Documents Scenario: Symplified Healthcare’s R&D department has been working on a new drug production process that has been documented in a PDF file. It is critical that this PDF does not leave the hospital network and get into the hands of competitors. It has been decided that Indexed Document Matching (IDM) would be the best method for protecting this file. It is necessary to create an IDM index and associated policy to detect attempts to send data containing parts or all of the new drug process document outside of the Symplified network. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Data Profiles > Indexed Documents. 2. Click Add Document Profile. 3. In the Name field, type: Drug Process Documents 4. Select the option Upload Document Archive to Server Now. 5. Click Browse and navigate to C:\Training Files\IDM. 6. Select the NewPharmaProcess.zip file and click Open. 7. Under the “Indexing” heading, select Submit Indexing Job on Save. 8. Click Save on top. Note: The next step is to configure a policy that uses the IDM profile you just created. You do not need to wait for the indexing to complete before continuing with this lab exercise. 9. Browse to Manage > Policies > Policy List. 10. Click New. Exercise 6: Configure a Policy to Protect Confidential Documents Copyright © 2019 Symantec Corporation. All Rights Reserved 15 11. Leave Add a blank policy selected and click Next. 12. In the Name field, type: Symplified Drug Process Detection (IDM) 13. Next to the “Policy Group” heading, select Default Policy Group from the drop-down list. 14. On the Detection tab, click Add Rule. 15. Under the “Rule Type > Content” heading, select the option Content Matches Document Signature From. 16. Ensure that Drug Process Document is selected in the drop-down list. 17. Click Next. 18. In the Rule Name field, type: Drug Process Detection 19. Next to the “Severity” heading, click Add Severity. 20. Change the new severity entry to match the following: Set Severity to: Medium when match count Is Between from 10 to 25 matches 21. Next to the “Severity” heading, click Add Severity again. 22. Change the new severity entry to match the following: Set Severity to: Low when match count Is Less Than 10 matches 23. Under the “Conditions” heading, change the Minimum Document Exposure to 30. 24. Click OK at top to save the detection rule. 25. Click Save to save the new policy. End of exercise 16 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 7: Configure a Policy to Protect Source Code Scenario: Symplified Healthcare has been improving the healthcare industry by creating custom software utilized across all their locations. Competitors have shown interest in the innovations and have been attempting to replicate the software for their own use. Symplified wants to ensure that no source code is being sent outside the organization. Source code is difficult to describe with keywords and is ever changing, making it uniquely challenging to detect. Symplified has decided that the Vector Machine Learning (VML) detection method is best for finding matching source code in the organization. It is necessary to configure a VML profile and policy to detect any source code leaving the company that is similar to the source code Symplified Healthcare is developing. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Data Profiles > Vector Machine Learning. 2. Click New Profile. 3. In the Name field, type: Source Code Profile 4. Click Create. 5. On the right side of the console screen, click Manage Profile. 6. Click Upload Contents. 7. Leave the Positive option selected. 8. Click Browse and navigate to C:\Training Files\VML. 9. Select the VML_Positive.zip file and click Open. 10. Click Submit. 11. Click Upload Contents again. Exercise 7: Configure a Policy to Protect Source Code Copyright © 2019 Symantec Corporation. All Rights Reserved 17 12. Select Negative. 13. Click Browse. 14. Select the VML_Negative.zip file and click Open. 15. Click Submit. 16. At the far left of the console screen, click Start Training. Note: The Enforce server will now create a profile based on the given positive and negative data sets. In the lab environment, this process should happen relatively quickly. In production, this may take longer depending on the number of files submitted. A Training Profile popup at the top of the tab will report on the progress of the training profile. 17. After the training is finished (and you see a Training Successful window at the top of the tab), click Accept. 18. Next to the “Similarity Threshold” heading, click Edit. 19. Using the slider, adjust the threshold down to 3.5 and click Save. Note: Next, it is necessary to create a policy that detects any source code being stored or transmitted on the network. 20. Browse to Manage > Policies > Policy List. 21. Click New. 22. Leave the option Add a blank policy selected and click Next. 23. In the Name field, type: Symplified Source Code Detection (VML) 24. Next to the “Policy Group” heading, select the Default Policy Group. 25. On the Detection tab, click Add Rule. 26. Under the “Rule Type > Content” heading, select the option Detect using Vector Machine Learning Profile. 27. Ensure that Source Code Profile is selected in the drop-down list. 28. Click Next. 29. In the Rule Name field, type: Source Code Detection 30. Keep the other defaults and click OK. 31. Click Save. End of exercise 18 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 8: Configure a Policy for Form Recognition Scenario: Symplified stores many forms submitted to them by patients, doctors, and insurance companies. Blank forms do not present a security risk, but when they have been filled out, the forms often contain sensitive information. Symplified is concerned that some forms may be leaking out of the hospital network. IT would like a Form Recognition data profile and matching policy to detect completed forms used most commonly by Symplified Healthcare. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Data Profiles > Form Recognition. 2. Click Add Profile. 3. In the Name field, type: Symplified Patient Information Form 4. Next to the “Upload Gallery Archive” heading, click Browse and navigate to C:\Training Files\FormRecognition. 5. Select the Patient_Information_Form.zip file and click Open. 6. Click Save. 7. Browse to Manage > Policies > Policy List. 8. Click New. 9. Leave the option Add a blank policy selected and click Next. 10. In the Name field, type: Symplified Patient Form Detection 11. Next to the “Policy Group” heading, select Symplified PII Policies from the drop-down list. 12. On the Detection tab, click Add Rule. Exercise 8: Configure a Policy for Form Recognition Copyright © 2019 Symantec Corporation. All Rights Reserved 19 13. Under the “Rule Type > Form Recognition” heading, select the option Detect using Form Recognition Profile. 14. Ensure the option Symplified Patient Information Form is selected in the drop-down list. 15. Click Next. 16. In the Rule Name field, type: Patient Information Form 17. Click OK. 18. Click Save. End of exercise 20 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 9: Use a Template to Add a DLP Policy Scenario: Being subject to the Health Insurance Portability and Accountability (HIPAA) laws in the United States, Symplified Healthcare has decided to configure a HIPAA policy to detect any possible violations within the organization. Since Symantec DLP ships with a HIPAA template, IT has decided to deploy this policy using this template and then later test it and modify it as needed. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Policies > Policy List. 2. Click New. 3. Select Add a policy from a template and click Next. 4. Review the included templates. Note: You may notice that many of the policies created in this lab so far could have been added through a template instead. However, for the sake of learning how to create custom policies we have had you create the previous policies manually. 5. Under the “US Regulatory Enforcement” heading, select HIPAA and HITECH (including PHI) and click Next. 6. Under the “Template HIPAA and HITECH (Including PHI)” heading, ensure Do not use Exact Data Matching is selected and click Next. 7. Next to the “Policy Group” heading, select Symplified PII Policies from the drop-down list. 8. Review the detection rules automatically created by the HIPAA policy template. 9. Click Save. Exercise 9: Use a Template to Add a DLP Policy Copyright © 2019 Symantec Corporation. All Rights Reserved 21 Note: Because IT is not quite ready to start detecting HIPAA data, the policy needs to be suspended. It can easily be activated and modified at a later time. 10. Click the green circle to the left of the HIPAA and HITECH (including PHI) policy. 11. When the warning message is displayed, click OK. The red circle icon next to the policy indicates that the policy is not active. End of exercise 22 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 10: Export Policies for Use at a DR Site Scenario: Symplified is also preparing a disaster recovery (DR) site and would like to export the policies used on the production Enforce server, just in case a quick recovery of the existing policies is needed. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Policies > Policy List. 2. At upper left in the console screen, select the checkbox on the top of the left-most column (next to Status). This will select all the currently displayed policies. 3. Click Export. Note: If you receive a warning popup saying that exporting large numbers of policies could take some time, click OK. 4. If you get a Open With / Save File popup window, leave Save File selected and click OK. 5. Using Windows Explorer, navigate to C:\Users\Administrator\Downloads. 6. Double click the Enforce-policies--.zip file. (Look for the most recent one if there are multiple files.) 7. Review the XML files captured within the .zip file. Note: With these backup files exported, they can now be transferred to the DR site and then quickly imported again for immediate use in case of a disaster. End of exercise Exercise 10: Export Policies for Use at a DR Site Copyright © 2019 Symantec Corporation. All Rights Reserved 23 Exercise 11: Configure Optical Character Recognition Scenario: Symplified wants to take advantage of Symantec DLP’s Optical Character Recognition (OCR) functionality, which extracts text from supported image file types and then delivers that text to supported detection server types for analysis against your DLP policies. The Symplified DLP team has already installed a Symantec DLP OCR server on a dedicated host. Now they will create an OCR configuration (with parameters for connecting to the OCR server and performing text extraction). Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce administration console, browse to System > Settings > OCR Engine Configuration. 2. Click Add OCR Engine Configuration. 3. In the Name field, type: Symplified OCR Configuration 4. In the OCR server hostname field, type: ocr.symplified.com 5. Leave the “Port,” “OCR Engine Timeout,” and “Accuracy vs speed” settings at their default values. 6. Under the “Languages and Dictionaries” heading and next to “Supported Languages,” click the blue plus-sign icon next to English in the Available Languages list box. “English” should now appear in the Selected Language(s) list box on the right. 7. In the Specialized Dictionaries list box, select English Medical Dictionary. 8. Click Save. End of exercise 24 Identifying and Describing Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Locating Confidential Data Stored on Premises and in the Cloud As IT security manager, you recognize that there are a lot of “hiding places” for confidential and sensitive data to reside on the organization’s network as well as on each employee’s individual workstation or laptop. One of your first important tasks is to audit each network location and endpoint and find out where those confidential data files reside in order to create an effective policy to protect them. In this lab, you will learn how to scan network shares and endpoint computers for confidential data using the policy definitions created in the previous lab exercises. 25 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Run a Content Enumeration Scan Scenario: Historically, Symplified Healthcare has been focused on keeping malicious outsiders out of the network, while paying little attention to the doctors, nurses, administrators, and other personnel within the hospital organization. As a result, many network shares have been created, and files have been subsequently transferred among users via these shares. Unfortunately, the shares are not well documented, and it is difficult to know where the shares reside. By using the Content Enumeration Scan and Inventory Scan features of Symantec DLP, it is possible to locate these shares on the network. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Launch Firefox and log in to the Enforce console using the following credentials, if prompted: 3. Browse to System > Settings > Directory Connections. Login: Administrator Password: training Note: Before configuring the Content Root Enumeration scan, it is necessary to configure a connection to the Symplified Active Directory. 4. Under the “Directory Connections” heading, click Add Connection. 5. In the Name field, type: Symplified Active Directory 6. In the Hostname field, type: localhost 7. In the Port field, type: 389 8. In the Base DN field, type: DC=symplified,DC=com 26 Locating Confidential Data Stored on Premises and in the Cloud Copyright © 2019 Symantec Corporation. All Rights Reserved 9. Under the “Authentication” heading, select the option Connect with Credentials and provide the following credentials: Username: symplified\dlpldap Password: Training! Note: Active Directory does not allow anonymous connections, so proper credentials must be provided. Any service account with read access is acceptable. 10. Click Test Connection. A green bar should appear at the top of the console screen, indicating that the test was successful. If the test was unsuccessful, check the aforementioned settings, then ask the instructor for assistance. 11. After the connection test has succeeded, click the Index Settings tab. 12. Select the option Weekly, then select Sunday. 13. Click Save. 14. Browse to Manage > Discover Scanning > Content Root Enumeration. 15. Click Add Scan. 16. In the Name field, type: Symplified File Share Scan 17. In the Directory Connection drop-down list, select Symplified Active Directory. 18. Next to the “Enumerate shares?” heading, select Yes. 19. Under the “Filters” heading, next to Server Names, leave the option does contain selected and in the field next to it type: enforce 20. Click Save. 21. Select the checkbox next to Symplified File Share Scan. 22. Click Start. 23. Click the Refresh button (shows “Completed”. 24. Under the “Content Roots” column heading, click the [#] Shares link, where [#] is the number of shares discovered. 25. Ensure \\enforce.symplified.com\FileShare is listed and click OK.) in the top right area of the Enforce console until the Status column End of exercise Exercise 1: Run a Content Enumeration Scan Copyright © 2019 Symantec Corporation. All Rights Reserved 27 Exercise 2: Scan a Windows Target Scenario: Now that the shares have been located on the network, it is time to scan those shares for confidential data. Symplified Healthcare has a strict policy that no credit card information can be stored unencrypted on the network, especially in open shares. This scan will analyze the data in the open share found by the Content Root Enumeration scan. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce administration console, browse to System > Settings > Credentials. 2. Click Add Credential. 3. In the Credential Name field, type: dlpscan 4. In the Access Username field, type: symplified\dlpscan 5. In the Access Password and Re-enter Access Password fields type: Training! 6. Next to the “Usage Permission” heading, select Servers and Endpoint agents. 7. Click Save. 8. Browse to Manage > Discover Scanning > Discover Targets. 9. Select New Target > Server > File System. 10. On the General tab, in the Name field, type: Windows File Share Scan 11. Next to the “Policy Groups” heading, select Symplified PCI Policies. 12. Next to the “Scan Type” heading, select Always scan all items (full scan). 13. Click the Scanned Content tab. 28 Locating Confidential Data Stored on Premises and in the Cloud Copyright © 2019 Symantec Corporation. All Rights Reserved 14. Select the option Use Saved Credentials and select dlpscan (symplified\dlpscan) from the dropdown list. 15. Under the “Content Roots (Servers or Shares)” heading, leave the option Specify Content Roots selected and select Add Content Roots > From a Content Root Enumeration scan. 16. Leave the option Symplified File Share Scan selected and click Import. 17. Select all content roots in the list EXCEPT for \\enforce.symplified.com\FileShare and click Delete. 18. Click the Scanned Content tab again. 19. Under the “Content Roots” heading, ensure that only \\enforce.symplified.com\FileShare remains listed. Check the checkbox beside it in the left column. 20. Review the contents of the other tabs: Note: The Targeting tab allows you to select specific servers for scanning. The Filters tab allows you to include or exclude files based on type, size, or date. The Advanced tab allows you to set ‘throttling’ limits for files scanned to improve performance. The Protect tab allows you to select whether policy remediation should copy, encrypt, or quarantine affected files. 21. Click Save when finished. 22. Select the checkbox next to Windows File Share Scan. 23. Click Start Scan. The scan might take a couple of minutes to complete. 24. Under the “Scan Status” column heading, click the Starting link. 25. In the top right area of the Enforce console, click the Refresh (26. After the scan status shows “Completed,” click the View Incidents button ( ) in the “Actions” column at right. The results of the scan summarized by policy are displayed. This allows a quick review of which policies were violated during the scan. 27. Under the “Policy” column heading, click the Symplified PCI (EDM/DCM) link. 28. Under the “ID/Policy” column heading, click one of the ID links. 29. Review the information in the Key Info tab on the left. Notice the policy matches, Incident Details and Access Information for the file found during the scan. 30. Click the History tab to review any actions taken on the incident from the time it was created. 31. Optionally and as time permits, review other incidents.) button. Note: Although there is PII data in the scanned file share, it was not detected because the Discover scan was only configured to look for data that violated the policies in the PCI policy group. End of exercise Exercise 2: Scan a Windows Target 29 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 3: Scan Endpoint Computers for Confidential Data Scenario: At Symplified Healthcare, there are a great number of endpoint computers. There are endpoint computers at all nurses’ stations, examination rooms, and reception areas in addition to the endpoints in the Legal, Finance, and Administration departments. With so many endpoints, the IT staff is busy just keeping everything in working order and has little time to monitor what information users are storing on these endpoints. Now that the DLP agent has been deployed to all endpoints, it is time to configure a DLP scan to see what, if any, confidential data is being stored on these endpoint machines. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. On the Enforce administration console, browse to Manage > Discover Scanning > Discover Targets. 2. Select New Target > Endpoint > File System. 3. In the Name field, type: Endpoint File Share Scan 4. Next to the “Policy Groups” heading, select Symplified PII Policies. 5. In the “Scan Execution” section, select Always scan all items (full scan). 6. Click the Targeting tab and, under the “Available Servers” heading, select Symplified Detection Server and click Add. 7. Click the Filters tab and, in the Include Filters field, type: */MyData/* 8. Click Save. 9. Select the checkbox next to Endpoint File Share Scan. 10. Click Start Scan. 11. Under the “Scan Status” column heading, click the Starting link. 30 Locating Confidential Data Stored on Premises and in the Cloud Copyright © 2019 Symantec Corporation. All Rights Reserved 12. Using the Enforce console's Refresh button, refresh the page every 30 seconds until the scan is complete. Note: The scan might take several minutes to complete. You can continue with other lab exercises while the scan is running and review the results later. Note that scans will often register incidents that you can examine even before the scan has completely finished, so when you refresh, check the “Incidents Generated” column for any non-zero values to indicate that there are incident records in the system even if the scan hasn’t totally completed. 13. Once the scan has completed (or you see any incidents in the “Incidents Generated” column), click the View Incidents button (14.) in the “Actions” column at right. Review the list of incidents on the next screen. Note: If your scan did not detect any incidents for some reason, you can display the results of another scan instead, by selecting (under Filter on top): Scan > Custom then selecting a previous scan from the displayed list. 15. Click on the Symplified PII (DCM) link in the Totals column to see the individual list of incidents. 16. Examine the list of individual incidents, then click on one of the incident rows to switch to the incident snapshot screen. 17. Review the details of the incident. To switch between incident snapshots in the list, use the Previous or Next buttons in the upper right to navigate. End of exercise Exercise 3: Scan Endpoint Computers for Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 31 Exercise 4: Scan Server for Confidential Data using EMDI Scenario: During your initial investigation into confidential and sensitive files located on endpoint computers, you’ve found a number of files that have data that resembles important patient data, but is in fact harmless and unrelated. Rather than have the incident first responders have to manage judging and deleting unimportant incidents, you decide to utilize the patient dataset created in the previous lab to validate potential data matches before triggering an incident. In this exercise, you’ll configure a discover file scan similar to the previous exercise, but will utilize the previous patient data set using EMDI to cut down on unimportant incidents when scanning files on endpoint computers. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. Open File Explorer and go to the C:\EMDI directory. 2. Open and examine the two files in this directory. The “Patient Extract (EMDI)” file contains actual patient data, while the “Sample EMDI Invoice” file contains unrelated invoice data without any sensitive information. Note: In this exercise you will be demonstrating how using the EMDI policy for PII will return different results compared to other policies when scanning the same content. First we will look at how the original DCM policy for PII handles both of these files present in the EMDI directory. 3. Browse to Manage > Policies > Policy List. 4. Within the list of policies, ensure that Symplified PII (DCM) is activated (has a ‘green light’ in the Status column), and that Symplified PII (EMDI) is deactivated (red light). (To toggle a policy on/off, click directly on the green/red light icon, or check the checkbox on the left and select Activate or Suspend respectively.) 5. On the Enforce administration console, browse to Manage > Discover Scanning > Discover Targets. 32 Locating Confidential Data Stored on Premises and in the Cloud Copyright © 2019 Symantec Corporation. All Rights Reserved 6. Select New Target > Server > File System. 7. In the Name field, type: File Share Scan (EMDI) 8. Next to the “Policy Groups” heading, select Symplified PII Policies. 9. In the “Scan Execution” section, select Always scan all items (full scan). 10. On the Scanned Content tab, select the Use Saved Credentials option and select “dlpscan” from the drop down. 11. Under Content Roots, ensure Specify Content Roots is selected. 12. Click Add Content Roots > From a Content Root Enumeration Scan. 13. Select “Symplified File Share Scan” from the popup window and click Import. The content root list should now populate with all the shared folders discovered in the previous content root enumeration scan. 14. Select all content roots in the list EXCEPT for \\enforce.symplified.com\EMDI and click Delete. (\\enforce.symplified.com\EMDI should now be the only one in the list.) 15. Click Save in the top left when finished. 16. Navigate back to Manage > Discover Scanning > Discover Targets. 17. Select the checkbox next to File Share Scan (EMDI). 18. Click Start Scan. 19. Under the “Scan Status” column heading, click the Starting link. 20. Using the Enforce console's Refresh button, refresh the page every 30 seconds until the scan is complete. The scan might take a minute or more to complete. You can continue with other lab exercises while the scan is running and review the results later. 21. After the scan has completed, click the Ready link under the “Status” column. 22. Under the “Scan Status” heading, click the Completed link. 23. Review the Scan Statistics. Under the “Scan Statistics” heading and next to Current Incident Count, click the link showing the number of incidents (should be 2). 24. Review the list of incidents on the next screen. Note: Both files in the EMDI directory each triggered an incident. This is because the invoice numbers of the second (harmless) file matched the pattern for US social security numbers and thus triggered an incident. Normally an operator would have to review these incidents manually, examine the contents, categorize this second incident to be a ‘false positive’ not worthy of attention, and clear it. Exercise 4: Scan Server for Confidential Data using EMDI Copyright © 2019 Symantec Corporation. All Rights Reserved 33 25. Browse to Manage > Policies > Policy List. Deactivate Symplified PII (DCM) and activate Symplified PII (EMDI). (To toggle a policy on/off, click on the green/red light, or check the checkbox on the left and select Activate or Suspend respectively.) 26. Navigate back to Manage > Discover Scanning > Discover Targets. 27. Select the checkbox next to File Share Scan (EMDI) again, and click Start Scan. 28. Under the “Scan Status” column heading, click the Starting link. 29. Using the Enforce console's Refresh button, refresh the page every 30 seconds until the scan is complete. 30. After the scan has completed, click the Ready link under the “Status” column. 31. Under the “Scan Status” heading, click the Completed link. 32. Review the Scan Statistics. Under the “Scan Statistics” heading and next to Current Incident Count, click the link showing the number of incidents (should be 1 this time). 33. Review the list of incidents on the next screen. Note: In this case, only the first file triggered an incident. The EMDI process compared the invoice numbers in the second file to the existing data set and found that even though they resembled US social security numbers, they didn’t match existing patient data and did not trigger an incident. In this case there would be fewer false positive incidents for operators to review manually. 34. Before finishing this exercise and continuing, return to Manage > Policies > Policy List. Deactivate Symplified PII (EMDI) and reactivate Symplified PII (DCM). End of exercise 34 Locating Confidential Data Stored on Premises and in the Cloud Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 5: Configure a Global Policy for PII Compliance Scenario: After using the Exact Matching Data Identifier (EMDI) detection method to augment the previous policy, you realize that over time you’ll likely be creating many different policies that also involve Social Security numbers and your EMDI data profile would be useful as an additional validation check for those policies also. Rather than repeat these steps for each new policy, you decide to create a global addition to all SSN checks across the system so that any new policy will use your established data source. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to Manage > Policies > Data Identifiers. 2. Locate and click on US Social Security Number (SSN). 3. Open the Medium tab under Rule Breadth. 4. Under “Validators > Validation Checks”, click on Exact Match Data Identifier Check. 5. From Profile, add the Patient Data Extract EMDI profile created in the previous exercise. 6. Make sure SSN is shown in the Required field, and 1 is shown in the At least match field. 7. Click Add Validator when finished. An “Exact Match Data Identifier Check” should be added to the Active Validators list. 8. Click Save on the upper left. End of exercise Exercise 5: Configure a Global Policy for PII Compliance Copyright © 2019 Symantec Corporation. All Rights Reserved 35 36 Locating Confidential Data Stored on Premises and in the Cloud Copyright © 2019 Symantec Corporation. All Rights Reserved Understanding How Confidential Data Is Being Used As part of your audit process, you seek to understand how confidential data is being moved and transmitted inside and outside the network. Symplified Healthcare administrators have created a policy that important data should not be transmitted outside the company (whether through email or other network connection) without being encrypted. Part of your job will be to monitor and analyze outgoing traffic to form an understanding of the data protection issues as preparation for creating new policies to block, encrypt, or otherwise manage that data. In this lab, you will use Network Prevent for Email to monitor outgoing SMTP messages looking for important or confidential data that needs to be blocked or encrypted. Additionally, you will learn how to monitor applications and user activity on endpoints (such as workstations and laptops) that can also compromise sensitive data. 37 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Configure Network Prevent for Email to Monitor SMTP Messages Scenario: Symplified Healthcare wants to ensure that no sensitive data leaves the company unencrypted. As part of the discovery phase of their DLP implementation, Symplified has decided that any emails with sensitive information leaving the organization unencrypted will be logged rather than blocked or rerouted. Later, the IT department will configure DLP to reroute any emails with sensitive information to the Symantec Encryption Management Server for encryption prior to being sent to the recipient. Estimated exercise time: 7 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Launch Firefox and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 3. Browse to System > Servers and Detectors > Overview. 4. Under the “Servers and Detectors” heading, click the Symplified Detection Server link. 5. Under the “General > Status” heading, review the process status. By default, the detection server only shows a basic status of “Running.” 6. Browse to System > Settings > General. 7. Click Configure. 8. Under the “Process Control” heading, select the option Advanced Process Control. 38 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved Enabling the advanced process control allows an administrator to see the status of each process individually. 9. Click Save. 10. Browse to System > Servers and Detectors > Overview. 11. Under the “Servers and Detectors” heading, click the Symplified Detection Server link. Note: The status of each process is now shown rather than an overall status. This lab detection server is functioning in single-tier mode and thus shows many processes. In production, a detection server usually serves one channel (for example, Endpoint, Network Monitor, Discover, and so on) and would only show services related to that channel. 12. While still browsing the Detection Server detail page, click Configure. 13. Click the Inline SMTP tab. 14. Verify the option Trial Mode (Do not block violating messages) is NOT selected. 15. Under “Next Hop Configuration,” select Forward. 16. Leave the option Disable MX Lookup selected, and in the accompanying field, type: enforce.symplified.com 17. Click Save. A yellow bar should appear at the top of the console window, indicating that the detection server must be recycled. 18. Under the “General > Status” heading, click the recycle link. 19. When asked “Are you sure you want to recycle the server?”, click OK. 20. Every 15 seconds, click the Enforce console’s Refresh button (“Running.”) until all services are listed as Note: For this lab environment, the email client on the Endpoint VM has been configured to communicate directly with the detection server rather than to the mail server first. In a production environment, the email client would be configured to communicate with the mail server which would then likely communicate with an MTA, which would in turn redirect the message to the detection server. The detection server would process the email and then forward the email to another hop or reflect it back to an MTA. End of exercise Exercise 1: Configure Network Prevent for Email to Monitor SMTP Messages Copyright © 2019 Symantec Corporation. All Rights Reserved 39 Exercise 2: Use Network Prevent for Email to Monitor SMTP Messages Scenario: Joe User, a Symplified Healthcare employee in the Finance department, communicates with Sylvia Outsider, a trusted partner, on a daily basis. Over the years, they have become good friends. Due to this friendship, Joe is occasionally lax about security and uses insecure methods to send information to Sylvia. In this exercise, you will take on the role of Joe User. You will first send a benign email and then a confidential email to Sylvia Outsider to see the difference in how DLP reacts to these emails. Estimated exercise time: 12 minutes Steps: Login to: Endpoint 1. Log in to the Endpoint VM using the following credentials: Username: Symplified\joe_user Password: train 2. Open the Outlook client by clicking the icon on the taskbar. Notice that for convenience both Joe User and Sylvia Outsider are configured in the same email client and you will use the same client to see the inboxes for both Joe and Sylvia. 3. Under the “” heading, select the Inbox. 4. Click New Email on top. 5. In the To... field, type: 6. In the Subject field, type: Yesterday's Patient Sign-in Sheet 7. For the body of the email type the following (or create your own email text): Hi Sylvia! 40 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved Hope your day is going well! Here is the patient sign-in sheet from yesterday. Best Regards, Joe 8. Click Attach File. 9. Browse to C:\Training Files\Misc, then select the Patient_Sign_In12102016.pdf file, and click Insert. 10. Click Send. This email and attachment had no sensitive data and should have arrived in Sylvia’s inbox without any incidents being created on the Enforce server. (The email may take a few seconds to arrive.) 11. Under the “” heading, select the Inbox. 12. Verify that the email from Joe arrived. Note: It may be necessary to click Send/Receive All Folders if the email has not yet arrived. Switch to: Enforce 13. Return to the Enforce VM; Launch Firefox (if not open) and log in to the Enforce console using the following credentials: Username: Administrator Password: training 14. Browse to Incidents > Network. 15. Verify there is not an incident for the email from Joe to Sylvia with the subject of “Yesterday’s Patient Sign-in Sheet.” Switch to: Endpoint 16. Return to the Outlook client on the Endpoint console. 17. Under the “” heading, select the Inbox. 18. Click New Email. 19. In the To... field, type: 20. In the Subject field, type: Patient Processing Info 21. For the body of the email type the following (or create your own email text): Hi Sylvia! Please process the payments for the attached list of patients. Exercise 2: Use Network Prevent for Email to Monitor SMTP Messages Copyright © 2019 Symantec Corporation. All Rights Reserved 41 Best Regards, Joe 22. Click Attach File. 23. Click Browse This PC.... 24. Browse to C:\Training Files\Misc, then select the PatientsForProcessing.xlsx file, and click Insert. 25. Click Send. Note: This email contains sensitive information that should create an incident in the Enforce console. At this point, we have not yet configured any notifications or blocking. Consequently, the email will still arrive in Sylvia’s inbox, and Joe will not know he did anything wrong. However, the InfoSec team will now be aware that there is sensitive data leaving the organization. Switch to: Enforce 26. Return to the Enforce console. 27. While still viewing Network > Incidents - New, click the Enforce console’s Refresh button in the upper right (28.). Locate the incidents that match the subject of the last email you sent. Note: This single email will create multiple incidents because it violated both PII and PCI policies, due to the fact that the email attachment contained both payment information and US Social Security Numbers (SSNs). SSNs are not required for payment processing and should not have been included in any email to Sylvia. This is a good indication that there is a broken business practice and that Joe should be educated on handling data properly. 29. Click on and review the details for these incidents, paying attention to the “Incident Details” and “Message Body” headings. End of exercise 42 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 3: Monitor Endpoint Activity -- Email Scenario: With the thousands of endpoints across the Symplified Healthcare organization, it has become important to ensure the security of the data used on those endpoints. Up to this point, Symplified has relied on its employees to be smart with the data, but a few minor incidents have caused Symplified to determine they need to monitor the endpoints more closely. It has been decided that the best and easiest solution is to use Symantec DLP to monitor endpoints. Network Prevent for Email has previously been used only to monitor email at the network level. Symplified would now like to move this processing to the endpoint as a first layer of protection and leave the network level of protection as a secondary layer. In this exercise, you will see how we can use Endpoint monitoring to check email content and attachments similarly to how the Network monitoring analyzed email in the previous exercise. Estimated exercise time: 10 minutes Steps: Login to: Endpoint 1. On the Endpoint VM, launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 2. Browse to System > Agents > Agent Configuration. 3. Click Add Configuration. 4. In the Name field, type: Symplified Agent Configuration 5. On the “Channels” tab, under the “Enable Monitoring > Email” heading, select the Outlook option. 6. Click the Advanced Settings tab. Scroll through the advanced settings and modify the following: EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int: 10 EndpointCommunications.IDLE_TIMEOUT_IN_SECONDS.int: 0 ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int: 10 Exercise 3: Monitor Endpoint Activity -- Email Copyright © 2019 Symantec Corporation. All Rights Reserved 43 Note: In a production environment, these settings would be left at default or adjusted based on suggestions from Support or Professional Services. For this lab, the times are adjusted to speed up communications between the endpoint agent and the Enforce server. 7. Click Save. 8. On the configuration list page, click Apply Configuration. 9. Select the option Default Group. 10. Click Assign Configuration. 11. From the “Assign Configuration” drop-down list, select Symplified Agent Configuration and click OK. 12. Select the Default Group option. 13. Click Update Configuration and click OK. 14. Because there were advanced settings configured in the Agent Configuration a restart is required. Advanced settings are only applied to the endpoint agent after it is restarted. Right-click the Windows Start button, then click Shut down or sign out > Restart. Note: If an RDP connection is used to connect to the lab environment, the preceding command will display the status “Disconnect” rather than restart. In this case, browse to C:\Training Files\Misc, right-click the reboot.bat file, and select Run as Administrator. If prompted with “Do you want to allow this app to make changes to your PC?”, click Yes. Wait for 60 seconds, then reconnect to the RDP session. 15. When the Endpoint VM comes back up, log in to Windows using the follow credentials: Username: joe_user Password: train 16. Open Outlook. 17. Under the “” heading, click the Sent folder. 18. Double-click the email with a subject of “Yesterday’s Patient Sign-in Sheet.” 19. In the top ribbon, above the “Move” heading (inside the lower right icon menu), click Actions > Resend this message. 20. Click Send. This is the same non-sensitive email used earlier. It will be monitored by the endpoint agent but should not create any new incidents. 21. Open a web browser and log in to the Enforce console using the following credentials: Username: Administrator Password: training 44 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved 22. Browse to Incidents > Endpoint. 23. Ensure there is not an incident regarding an email from Joe to Sylvia with the subject of “Yesterday’s Patient Sign-in Sheet.” 24. Return to the Outlook client. 25. Under the “” heading, click the Inbox. 26. Ensure the new copy of the email arrived from Joe. (Check the timestamp.) 27. Under the “” heading, click Sent. 28. Double-click the email with a subject of “Patient Processing Info.” 29. In the top ribbon, above the “Move” heading, click Actions > Resend this message. 30. Click Send. This is the same sensitive email used earlier. It will be monitored by the endpoint agent and should create a new incident. 31. From Firefox, while still viewing Incidents > Endpoint - New, click the Enforce console’s Refresh button ( ). Note: An endpoint incident was created as the endpoint monitored the outbound email. Browsing to Incidents > Network would show that a Network incident was also created with the same subject. This is due to the fact that the email was not blocked at the endpoint, and Network Prevent for Email also scanned the email. In a production environment, it is likely the email would only be monitored on one of the egress points or perhaps blocked on the endpoint. 32. Select an incident record and open up the incident details screen. 33. Below the incident number at the top of the left column, notice the type is listed as “Endpoint Email/ SMTP.” 34. Review the details of the incident, paying attention to the information below the “Incident Details” heading. End of exercise Exercise 3: Monitor Endpoint Activity -- Email Copyright © 2019 Symantec Corporation. All Rights Reserved 45 Exercise 4: Monitor Endpoint Activity -- Third-Party Apps Scenario: With the thousands of endpoints across the Symplified Healthcare organization, it has become important to ensure the security of the data used on those endpoints. Up to this point, Symplified has relied on its employees to be smart with the data, but a few minor incidents have caused Symplified to determine they need to monitor the endpoints more closely. It has been decided that the best and easiest solution is to use Symantec DLP to monitor endpoints. Application File Access Control enables administrators to configure applications that are not pre-configured in Symantec DLP to be monitored for sensitive data usage. Joe User wants to encrypt sensitive data using AxCrypt, an unauthorized encryption application at Symplified Healthcare. IT Security has seen users work with AxCrypt in the past and has decided to use Symantec DLP to ensure that no data is encrypted using this application. Estimated exercise time: 8 minutes Steps: Login to: Endpoint 1. On the Endpoint VM, open a web browser and go to the Enforce administration console. Browse to System > Agents > Global Application Monitoring. 2. Click Add Application and select Windows. 3. Enter the following information: Name: AxCrypt Binary Name: AxCrypt.exe 4. Under the “Application Monitoring Configuration” heading, deselect everything, then select Application File Access > Read. 5. Click Save. AxCrypt should now be displayed in the application list. 6. Browse to System > Agents > Agent Configuration. 7. Click Symplified Agent Configuration. 46 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved 8. Under the “Enable Monitoring > Configured Applications” heading, select the option Application File Access. 9. Click Save. 10. Click Apply Configuration. 11. Select the Default Group option. 12. Click Update Configuration, then click OK. 13. Browse to C:\Training Files\Misc. 14. Right-click the Patients Credit Card Info file and select AxCrypt > Encrypt. 15. In the Enter Passphrase and Verify Passphrase fields, type: training 16. Click OK. A new icon should appear on the file, indicating it was encrypted. The encryption was not blocked; it was detected, and an incident was created. 17. Right-click the file again and select AxCrypt > Decrypt. 18. Return to Firefox and browse to Incidents > Endpoint. Under the type, you should see an application box with a lock icon, indicating that this incident is an Application File Access Control incident. 19. Click on the new incident. Notice the type is labeled “Endpoint Application File Access.” Also notice that the Machine Name, Endpoint Location, and Source File Location are all recorded. End of exercise Exercise 4: Monitor Endpoint Activity -- Third-Party Apps Copyright © 2019 Symantec Corporation. All Rights Reserved 47 Exercise 5: Monitor Endpoint Activity -- Copy/Paste Scenario: With the thousands of endpoints across the Symplified Healthcare organization, it has become important to ensure the security of the data used on those endpoints. Up to this point, Symplified has relied on its employees to be smart with the data, but a few minor incidents have caused Symplified to determine they need to monitor the endpoints more closely. It has been decided that the best and easiest solution is to use Symantec DLP to monitor endpoints. Malicious insiders intent on taking data often try to copy data out of one document and into another in an attempt to avoid detection. In this exercise you’ll see how Endpoint monitoring can analyze and log incidents involving copying sensitive data from a spreadsheet. Estimated exercise time: 5 minutes Steps: Login to: Endpoint 1. On the Endpoint VM, open a web browser and go to the Enforce administration console. Browse to System > Agents > Agent Configuration. 2. Click Symplified Agent Configuration. 3. Under the “Enable Monitoring > Clipboard” heading, select both Copy and Paste. 4. Click Save. 5. Click Apply Configuration. 6. Select the Default Group option. 7. Click Update Configuration, then click OK. 8. Browse to C:\Training Files\Misc and open the PatientsForProcessing.xlsx file. (You can also open Patients Credit Card Info.csv instead.) 9. Select rows 1-15. 48 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved 10. Right-click the selected rows and select Copy. (You do not need to paste the data anywhere; the copy operation itself should trigger the incident.) 11. Return to Firefox and browse to Incidents > Endpoint. 12. Click the most recent incident. Notice that the incident type is “Endpoint Clipboard,” and the Matches area shows the information that was copied from the spreadsheet. End of exercise Exercise 5: Monitor Endpoint Activity -- Copy/Paste Copyright © 2019 Symantec Corporation. All Rights Reserved 49 50 Understanding How Confidential Data Is Being Used Copyright © 2019 Symantec Corporation. All Rights Reserved Educating Users to Adopt Data Protection Practices As IT security manager, you recognize that many internal users who may be putting confidential or sensitive data at risk through their activities are not doing so maliciously, but out of carelessness or ignorance. As such, user education should be a high priority of your data loss prevention efforts—training and educating users when they violate policy so they can understand what actions are disallowed and adjust their behavior. In this lab, you will be configuring email responses to data loss prevention policies to notify users that a policy violation has occurred. In addition, you will configure endpoint notifications that popup on the user workstation or laptop to display policy violation information as well as present an opportunity for users to provide a justification for their attempted actions. 51 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Configure the Active Directory Lookup Plugin Scenario: Lookup plugins enable DLP to import data from external sources and import that data into the incidents. Symplified would like to import additional contextual data from Active Directory into any new incidents that are created. This will allow the Enforce server to send notifications to the user and their manager automatically. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Launch Firefox and log in to the Enforce console using the following credentials, if prompted: 3. Browse to System > Incident Data > Lookup Plugins. 4. Click New Plugin and select LDAP. 5. In the Name field, type: AD Attributes 6. Delete the description and ensure Symplified Active Directory is selected in the “Directory Connection” drop-down list. 7. Leaving the Firefox window open, use Windows Explorer to browse to C:\Training Files\AD LDAP. 8. Double-click the lookupstrings.txt file to open it in Notepad, then copy the contents to the clipboard. 52 Login: Administrator Password: training Educating Users to Adopt Data Protection Practices Copyright © 2019 Symantec Corporation. All Rights Reserved 9. Return to Firefox, and in the Attribute Mapping field, delete the current attribute mappings and paste the contents of the lookupstrings.txt file into the field. 10. Click Save. 11. Click Modify Plugin Chain. 12. Under the “Dedicated Actions” column heading, select On and click Save. 13. Click Lookup Parameters. 14. Select the following options: Incident, Message, Sender 15. Click Save. 16. Browse to System > Incident Data > Attributes. 17. Click the Custom Attributes tab. Note: Custom attributes are used as a mapping between the Active Directory lookup strings and the information that is added to the incident. Without the custom attributes, no Active Directory information would appear in an incident even if the lookup was successful. 18. Click Add. 19. In the Name field, type: First Name 20. Next to the “Attribute Group” heading, click the drop-down list and select Create New Attribute Group. 21. In the field beneath “Create New Attribute Group,” type: Employee Info 22. Click Save. 23. Repeat steps 18 to 22 using the information displayed in the following table. When repeating steps 20 and 21, select the attribute group shown in the following table rather than creating a new attribute group. Name Is Email Address Last Name Email Attribute Group Employee Info Yes Phone Employee Info Employee Info 24. Click Add. 25. In the Name field, type: Manager First Name 26. Next to the “Attribute Group” heading, click the drop-down list and select Create New Attribute Group. Exercise 1: Configure the Active Directory Lookup Plugin Copyright © 2019 Symantec Corporation. All Rights Reserved 53 27. In the field beneath “Create New Attribute Group,” type: Manager Info 28. Click Save. 29. Repeat steps 24 to 28 using the information in the following table: When repeating steps 26 and 27, select the attribute group in the following table rather than creating a new attribute group. Name Is Email Address Manager Last Name Manager Email Manager Phone Attribute Group Manager Info Yes Manager Info Manager Info End of exercise 54 Educating Users to Adopt Data Protection Practices Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 2: Configure Email Notifications Scenario: Symplified Healthcare has been monitoring the data in their organization for a few months and are now ready to start educating users about proper handling and protection of sensitive data to help drive down data loss incidents. To start, Symplified has decided to send email notifications to users, their managers, and the InfoSec team when incidents occur. In this exercise you will configure email notification response rules that will be used to notify the appropriate people about a violation. You will also send an email from Joe to Sylvia to see the notifications occur. Estimated exercise time: 12 minutes Steps: Login to: Enforce 1. Log in to the Enforce console and browse to System > Settings > General. 2. Click Configure. 3. Under the “SMTP” heading, in the Server field, type: enforce.symplified.com 4. In the System Email field, type: 5. In the User ID field, type: The User ID is used to authenticate to the email server. This email server uses the email address as the user ID. 6. In the Password field, type: train 7. Click Save. Note: It is necessary to provide the SMTP settings to the Enforce server to enable it to send reports and notifications. These settings are different from the Inline SMTP settings that tell Network Prevent for Email where to send the email on its next hop. Exercise 2: Configure Email Notifications Copyright © 2019 Symantec Corporation. All Rights Reserved 55 8. Browse to Manage > Policies > Response Rules. 9. Click Add Response Rule. 10. Leave the Automated Response option selected and click Next. 11. In the Rule Name field, type: Network: SMTP Notification 12. Next to the “Conditions” heading, click Add Condition. 13. Match the drop-down list selections to the following table (hold Ctrl to select more than one option): Severity Is Any Of High, Medium, Low 14. Click Add Condition again. 15. Match the drop-down list selections to the following table: Incident Type Is Any Of Network 16. Next to the “Actions” heading: Click the drop-down list and select All: Send Email Notification. 17. Click Add Action. 18. In the blue “All: Send Email Notification” box and next to the “To:” heading, select Sender (SMTP Incidents Only) and Manager Email. 19. Next to the “Custom To” heading, type: 20. Next to the “Custom From” heading, type: 21. Under the “Notification Content” heading and next to the “Language” heading, select English from the drop-down list. Note: It is possible to add multiple languages to the email notification. The administrator is required to provide the subject and body text in the desired language. 22. In the Subject field, type: Your email to $RECIPIENTS$ was monitored by Symplified IT Security. Note: The Send Email Notification action contains various variables (such as $RECIPIENTS$) that can be used in the subject or body of the notification email. They may be typed in manually or added automatically by clicking the desired variable listed in the “Insert Variable” column on the right. 23. Browse to C:\Training Files\FileShare and open the Email Notification.txt file. 24. Copy the entire contents of the file to the clipboard. 25. Back in the Enforce console, next to the “Body” heading, paste the contents of the clipboard into the field. 56 Educating Users to Adopt Data Protection Practices Copyright © 2019 Symantec Corporation. All Rights Reserved 26. Click Save. 27. Browse to Manage > Policies > Policy List. 28. Select Symplified PII (DCM). 29. Click the Response tab. 30. In the drop-down list, select Network: SMTP Notification, then click Add Response Rule. 31. Click Save. Switch to: Endpoint 32. Log in to the Endpoint VM using the following credentials: Username: Symplified\joe_user Password: train 33. Open Outlook. 34. Under the “” heading, click the Inbox. 35. Click New Email. 36. In the To field, type: 37. In the Subject field, type: Patients for Processing 38. In the body of the email, type a sentence or two from Joe to Sylvia regarding the “Patients for Processing” file. 39. Click Attach File and select the PatientsForProcessing file from the Recent Items list. If the file is not listed, click Browse This PC and select the file from C:\Training Files\Misc. 40. Click Send. 41. In the top left of the Outlook screen, click Send/Receive (42. After Outlook completes the Send/Receive operation, verify that there is an email in Sylvia’s and Joe’s inboxes. If the email has not arrived, click Send/Receive again. The Enforce server needs time to process the incident and send the notification. 43. Under the “” heading, click the Inbox. 44. Review the notification that was sent from IT Security to Joe regarding the sensitive data that was sent out.). Exercise 2: Configure Email Notifications Copyright © 2019 Symantec Corporation. All Rights Reserved 57 Switch to: Enforce 45. Open Outlook. 46. Click the Inboxes for IT Security and Jane Manager and review the notifications they received. Note: Multiple notifications can be added and customized in a single response rule. Customers often add different notifications for the IT Security group and the employee’s manager rather than sending the same notification to all three parties. End of exercise 58 Educating Users to Adopt Data Protection Practices Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 3: Configure Onscreen Notifications Scenario: With the Symantec DLP endpoint agent deployed to all the endpoint computers in the organization, Symplified is ready to begin actively monitoring and notifying users concerning the handling of sensitive data on the endpoint. Notifications are being leveraged to help users understand that the data they are interacting with is sensitive and requires proper handling. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. On the Enforce VM, launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 2. Browse to Manage > Policies > Response Rules. 3. Click Add Response Rule. 4. Leave Automated Response selected and click Next. 5. In the Rule Name field, type: Endpoint: Onscreen Notification 6. Next to the “Conditions” heading, click Add Condition. 7. Match the drop-down list selections to the following table (Hold Ctrl to select more than one option): Severity Is Any Of High, Medium, Low 8. Click Add Condition again. 9. Match the drop-down list selections to the following table: Incident Type 10. Is Any Of Endpoint Next to the “Actions” heading, click the drop-down list and select Endpoint Prevent: Notify. Exercise 3: Configure Onscreen Notifications Copyright © 2019 Symantec Corporation. All Rights Reserved 59 11. Click Add Action. 12. Review the options available for the Endpoint Prevent: Notify action. Leave the options at their defaults (or modify as desired) and click Save. Note: This response rule will show an onscreen notification to the user. This allows the security team to inform the user that the data they are handling is sensitive, but it does not block or restrict the action. 13. Browse to Manage > Policies > Policy List. 14. Select Symplified Drug Process Detection (IDM). 15. Click the Response tab. 16. In the drop-down list, select Endpoint: Onscreen Notification and click Add Response Rule. 17. Click Save. Switch to: Endpoint 18. Log in to the Endpoint VM, if needed, using the following credentials: Username: administrator Password: train 19. Browse to C:\Training Files\Misc. 20. Right-click the NewPharmaProcess.pdf file and select AxCrypt > Encrypt. 21. If a popup dialog asks for a password, in the Enter Passphrase and Verify Passphrase fields, type: training 22. Click OK. Note: Using the previously configured Application File Access Control feature of Symantec DLP, any attempt to encrypt a file with AxCrypt now not only creates an incident as it did before, but also shows an onscreen notification to the user. 23. In the notification that is shown, select an option and click OK. Notice that the file is still encrypted because the user was only notified that the data is sensitive, and the action was not blocked. 24. Right-click the file again and select AxCrypt > Decrypt. 25. Open Firefox and log into the Enforce console using the following credentials: Login: Administrator Password: training 26. Browse to Incidents > Endpoint. 27. Click the incident with a filename of NewPharmaProcess.pdf. 60 Educating Users to Adopt Data Protection Practices Copyright © 2019 Symantec Corporation. All Rights Reserved 28. Notice that under the “Incident Details,” the Agent Response was “User Notified,” and the User Justification is the justification selected from the onscreen notification in step #23. 29. Click the History tab and review the history of the incident. End of exercise Exercise 3: Configure Onscreen Notifications Copyright © 2019 Symantec Corporation. All Rights Reserved 61 62 Educating Users to Adopt Data Protection Practices Copyright © 2019 Symantec Corporation. All Rights Reserved Preventing Unauthorized Exposure of Confidential Data As IT security manager, you have a number of tools available to you in order to prevent the exposure of confidential or sensitive data to parties outside of the organization. Sometimes copy or move operations that put data attachments at risk need to be blocked and the data files quarantined. At other times the action can be allowed if the data is encrypted first. For certain less serious policy violations, you may want to inform the user of the current policy and give them the ability to allow or cancel the action themselves. In many cases, you’ll also want to discover data files where they currently reside and encrypt or quarantine them before a

user attempts to copy or move them in the first place. In this lab you will learn how to craft and configure the appropriate responses to policy violations, including blocking, quarantining, and user notification. In addition, you'll look at some of the advanced detection techniques such as Optical Character Recognition (OCR) that can find sensitive data that has been converted to an image. You'll also learn how to configure and run discover scans that can find important or confidential files on network shares or endpoint computers to prevent "data at rest" from become risky "data in motion" in the future. 63 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Configure SMTP Blocking Scenario: Training on the proper handling of sensitive data has been provided to all employees of Symplified Healthcare, in addition to the email notifications and onscreen notifications that employees have been seeing over the past several months. Symplified Healthcare is now prepared to move on the next phase of their DLP deployment- actively blocking the inappropriate use of sensitive data within the organization. SMTP email will be the first vector to use blocking. Blocking sensitive email ensures that no confidential data leaves the organization. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Launch Firefox and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 3. Browse to Manage > Policies > Response Rules. 4. Click the Network: SMTP Notification rule. 5. In the Rule Name field, modify the name to: Network: SMTP Block & Notify 6. From the drop-down list next to the "Actions" heading, select Network Prevent: Block SMTP Message and click Add Action. Note: We are now adding a new action to the existing notification response rule to block the SMTP message rather than letting it through and merely notifying the sender (as it was previously configured). 64 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 7. In the Redirect Message to this Address field, type: 8. Under the "All: Send Email Notification" heading, in the Subject: field, change the word monitored to: blocked 9. Browse to C:\Training Files\FileShare. 10. Open the Email Block.txt file and copy all the file's contents to the clipboard. 11. Under the "All: Send Email Notification" heading (not the "Network Prevent: Block SMTP Message" heading), in the Body: field, delete the current text and paste the text copied from the Email Block.txt file. 12. Click Save. Switch to: Endpoint 13. Log in to the Endpoint VM using the following credentials: Username: Symplified\joe_user Password: Training! 14. Launch Outlook. 15. Under the "" heading, select the Inbox. 16. Click New Email. 17. In the To field, type: 18. In the Subject field, type: Patient Info 19. In the email body, type the following (or something of your choosing): Hi Sylvia! Here are more patient information for the DB. Can you please process it? Thanks, Joe 20. Click Attach File. 21. Click Browse This PC and browse to C:\Training Files\Misc. 22. Select the PatientsForProcessing.xlsx file and click Insert. 23. Click Send. Exercise 1: Configure SMTP Blocking 65 Copyright © 2019 Symantec Corporation. All Rights Reserved 24. Click Send/Receive (25. Under the "" heading, click the Inbox. 26. Review the notification that Joe received.). Note: If everything is configured correctly, a notification should have arrived for Joe, and the email/file should NOT have arrived in Sylvia's inbox. The notification email may take a couple minutes to arrive. An email should have also been dispatched to IT Security and Jane Manager notifying them of the violation. Switch to: Enforce 27. Launch Outlook. 28. Under the "" heading, click the Inbox. 29. Verify that IT Security has received the notification email as well as the blocked email. Remember that the response rule was configured to redirect the email to IT Security. This could have been redirected to a quarantine email inbox instead. 30. Verify in Jane Manager's inbox that she received a notification as well. 31. Launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 32. Browse to Incidents > Network. 33. Open the incident with the subject of "Patient Data" and the violation of the "Symplified PII (DCM)" policy. Notice the red octagon indicating the message was blocked. 34. Click the History tab and review the events relating to the incident. End of exercise 66 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 2: Test Optical Character Recognition (OCR) and the "HIPAA and HITECH (including PHI)" Policy Scenario: 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 a Symantec DLP policy template, that looks for combinations of medical keywords and US Social Security numbers. The Symplified DLP administrators have also installed a Symantec DLP OCR server for testing and have configured one of their detection servers to send OCR-amenable images to the OCR server for text extraction. They are now going to run a test of this setup. Estimated exercise time: 10 minutes Steps: Login to: Endpoint 1. On the Endpoint VM, launch Firefox and log in to the Enforce console using the following credentials: Login: Administrator Password: training 2. Browse to System > Servers and Detectors > Overview and, under the "Servers and Detectors" heading, click the Symplified Detection Server link. 3. On the "Server / Detector Detail" page that appears, click Configure. 4. On the "Configure Server" page that appears, click the OCR Engine tab, select Symplified OCR Configuration (the OCR configuration you created previously) from the drop-down list, and click Save. If a yellow bar appears and prompts you to recycle the detection server, ignore it and do NOT recycle the detection server. Note: Do NOT recycle the detection server after assigning the OCR configuration. Disregard the yellow prompt asking you to recycle. 5. Browse to Manage > Policies > Policy List. Exercise 2: Test Optical Character Recognition (OCR) and the "HIPAA and HITECH (including PHI)" Policy Copyright © 2019 Symantec Corporation. All Rights Reserved 67 6. Click the green circle to the left of the Symplified PII (DCM) policy and then click OK to confirm you want to turn the policy off. 7. Click the red circle to the left of the HIPAA and HITECH (including PHI) policy and then click OK to confirm you want to turn the policy on. 8. Click the HIPAA and HITECH (including PHI) policy to open it for editing. 9. Click the Response tab, select Network: SMTP Block & Notify from the drop-down list, and click Add Response Rule. 10. Click Save. 11. If necessary, open Outlook. 12. Under the "" heading, select the Inbox. 13. Click New Email. 14. In the To field, type: 15. In the Subject field, type: Test of HIPAA Policy and OCR 16. In the email body, type the following (or something of your choosing): Hi Sylvia! I'm attaching a scanned lab test request form. This is a test. Thanks, Joe 17. Click Attach File. 18. Click Browse This PC and browse to C:\Training Files\Misc. 19. Select the JamesGuerra_Lab_Test_Order_Form.pdf file and click Insert. 20. Click Send. 21. Wait for the Inbox to refresh or click Send/Receive (22. Review the notification that Joe received in his Inbox.). Note: If everything is configured correctly, a notification should have arrived for Joe, and the email/file should not have arrived in Sylvia's inbox. An email should have also been dispatched to IT Security and Jane Manager, notifying them of the violation. 23. 68 In the Enforce administration console, browse to Incidents > Network. Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 24. Open the incident with the subject of "Test of HIPAA Policy and OCR" and the violation of the "HIPAA and HITECH (including PHI)" policy. Notice the red octagon indicating the message was blocked. 25. In the "Matches" column underneath the thumbnail photo, click the Click to enlarge link. 26. Click Show original size and review the PDF scan image that triggered the incident. Note that the OCR engine was able to extract the text content from the fixed image within the PDF file. 27. Click Close when you are finished reviewing the image. 28. Browse to Manage > Policies > Policy List, click the green circle to the left of the HIPAA and HITECH (including PHI) policy, and click OK to confirm that you want to turn the policy off. 29. Click the red circle to the left of the Symplified PII (DCM) policy and then click OK to confirm you want to turn the policy on. End of exercise Exercise 2: Test Optical Character Recognition (OCR) and the "HIPAA and HITECH (including PHI)" Policy Copyright © 2019 Symantec Corporation. All Rights Reserved 69 Exercise 3: Configure Endpoint Blocking Scenario: The employees of Symplified have been educated on the proper handling of sensitive information. It has been determined that if an endpoint user is not handling sensitive data appropriately, that information should be actively blocked by the DLP Endpoint agent. Because Joe was not able to send the message to Sylvia via normal email, he decides to try using the Symplified Webmail portal instead. Estimated exercise time: 8 minutes Steps: Login to: Endpoint 1. On the Endpoint VM, launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 2. Browse to System > Agents > Agent Configuration. 3. Click Symplified Agent Configuration. 4. Under the "Enable Monitoring > Web" heading, check HTTP. 5. Click Save. 6. Click Apply Configuration. 7. Select the Default Group option, click Update Configuration, and click OK. 8. Browse to Manage > Policies > Response Rules. 9. Click Add Response Rule. 10. Leave the option Automated Response selected and click Next. 70 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 11. In the Rule Name field, type: Endpoint: Block User Action 12. Next to the "Conditions" heading, click Add Condition. 13. Match the drop-down list selections to the following table: Incident Type Is Any Of Endpoint 14. Click Add Condition again. 15. Match the drop-down list selections to the following table (hold Ctrl to select more than one option): Severity Is Any Of High, Medium, Low 16. Next to the "Actions" heading, from the drop-down list, select Endpoint > Prevent: Block and click Add Action. 17. You may edit the Endpoint Notification Content alert message as desired or leave it as is. 18. Click Save. 19. Browse to Manage > Policies > Policy List. 20. Select Symplified PII (DCM) Policy. 21. Click the Response tab. 22. In the drop-down list, select Endpoint: Block User Action, then click Add Response Rule. 23. Click Save. 24. Open a new tab in Firefox and go to: 25. Log in to the Symplified Webmail Portal using the following credentials: Username: Password: train 26. Click Login. 27. In the top left of the browser screen, click New > Email Message. 28. In the To field, type: 29. In the Subject field, type: Patient Info 30. Click the Attachments link. 31. Click Browse and browse to: C:\Training Files\Misc 32. Select the PatientsForProcessing file and click Open. 33. Click Attach. At this point, you should see a progress bar and then a notification indicating the action was blocked. The DLP Endpoint agent evaluated and then blocked the HTTP upload. Exercise 3: Configure Endpoint Blocking Copyright © 2019 Symantec Corporation. All Rights Reserved 71 34. Select a response to the block notification and click OK. Because the action was blocked, the web mail client cannot continue, and an error dialog appears (Click OK). 35. Close the Webmail tab in Firefox and return to the Enforce console. 36. Browse to Incidents > Endpoint. 37. Click the incident with a recipient URL that starts with .... 38. Notice that the incident type is "Endpoint HTTP" and the Agent Response was "Action Blocked." 39. In the incident details, notice that the URL is listed, as well as the message body of the HTTP POST. End of exercise 72 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 4: Configure Endpoint User Cancel Scenario: Symplified employees working on "Project Halo," a new web application, are supposed to check in all code to the Git repository. Symplified policies dictate that no source code should be stored on a network drive. However, there are some instances when a file needs to be stored on a network share for vulnerability testing by a third party. Before allowing a file to be copied to the network share, Symplified has chosen to block any Project Halo files but allow the user to consciously decide if copying is the right action. Estimated exercise time: 8 minutes Steps: Login to: Enforce 1. On the Enforce VM, launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 2. Browse to System > Agents > Agent Configuration. 3. Click Symplified Agent Configuration. 4. Under the "Enable Monitoring > Network Shares" headings, check Copy to Share. 5. Click Save. 6. Click Apply Configuration. 7. Select the Default Group option, click Update Configuration, then click OK. 8. Browse to Manage > Policies > Response Rules. 9. Click Add Response Rule. 10. Leave Automated Response selected and click Next. 11. In the Rule Name field, type: Endpoint: User Cancel Exercise 4: Configure Endpoint User Cancel Copyright © 2019 Symantec Corporation. All Rights Reserved 73 12. Next to the "Conditions" heading, click Add Condition. 13. Match the drop-down list selections to the following table: Protocol or Endpoint Monitoring Is Any Of Endpoint Copy to Network Share 14. Next to the "Actions" heading, from the drop-down list, select Endpoint > Prevent: User Cancel and click Add Action. 15. Under the "Endpoint Notification Content" heading, change the second drop-down list from Broken Business Process to New Justification, then in the field below it, type: Third-Party Testing 16. In the Option Presented to the End User field to the right of the new justification, delete the current text and type: This file requires third-party vulnerability testing 17. Click Save. 18. Browse to Manage > Policies > Policy List. 19. Select Symplified Source Code Detection (VML). 20. Click the Response tab. 21. In the drop-down list, select Endpoint: User Cancel and click Add Response Rule. 22. Click Save. Switch to: Endpoint 23. Open the Endpoint VM (if not open already) and bring up a File Explorer (Windows Explorer) window. 24. Browse to C:\Training Files\. 25. Select and copy the ProjectHalo.zip file. 26. Double-click the FileShare shortcut on the desktop. (You can also find this directory by going to Network > Enforce > FileShare on the left side of File Explorer) 27. Paste the ProjectHalo.zip file into the network share. An onscreen notification should appear, notifying the user that the data they are transferring is sensitive. The user then has an opportunity to select a justification and then allow or cancel the action. 28. Select the justification This file requires Third Party vulnerability testing, then click Allow. When the notification appears, an incident is created. Clicking Allow enables the action to continue. Clicking Cancel blocks the action. Switch to: Enforce 74 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 29. Back in the Enforce console, browse to Incidents > Endpoint. 30. Click the incident with a File Name of ProjectHalo.zip. 31. Review the incident details, including the Agent Response, User, and User Justification. End of exercise Exercise 4: Configure Endpoint User Cancel Copyright © 2019 Symantec Corporation. All Rights Reserved 75 Exercise 5: Scan and Quarantine Files on a Server File Share Target Scenario: Previously, 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 place of the original file. This marker file will indicate where the user can find the original file and how to access to it. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. On the Enforce VM, launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 2. Browse to Manage > Policies > Response Rules. 3. Click Add Response Rule. 4. Leave Automated Response selected and click Next. 5. In the Rule Name field, type: Discover: Quarantine & Leave Marker 6. Next to the "Conditions" heading, click Add Condition. 7. Match the drop-down list selections to the following table: Incident Type 8. 76 Is Any Of Discover Click Add Condition again. Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved 9. Match the drop-down list selections to the following table (Hold Ctrl to select more than one option): Severity Is Any Of High, Medium, Low 10. Next to the "Actions" heading, from the drop-down list, select Network Protect > Quarantine File and click Add Action. 11. Next to the "Marker File" heading, select the option Leave marker file in place of remediated file. 12. Browse to C:\Training Files\FileShare. 13. Open the Quarantine Text.txt file and copy the text to the clipboard. 14. In the Enforce console, in the field next to Marker Text, paste the clipboard contents. Feel free to modify the text and use other variables in the text. 15. Click Save. 16. Browse to Manage > Policies > Policy List. 17. Click the Symplified PCI (EDM/DCM) policy. 18. Click the Response tab. 19. From the drop-down list, select Discover: Quarantine & Leave Marker and click Add Response Rule. 20. Click Save. 21. Browse to Manage > Discover Scanning > Discover Targets. 22. Click the Windows File Share Scan target (link in the Target Name column) to edit the details. 23. On the details page, click the Protect tab. 24. Select the Quarantine option. 25. Under "Quarantine/Copy Share," in the Path field, type: \\Enforce\Quarantine 26. Under the "Protect Credential" heading, select Use Saved Credentials, and from the drop-down list, select dlpscan (symplified\dlpscan). 27. Click Save. 28. Select the Windows File Share Scan option and click Start Scan. 29. Under the "Scan Status" column heading, click the Starting link. 30. Periodically click the Enforce console's Refresh button ("Completed." 31. Browse to Incidents > Discover. 32. Under the "Filter" heading, next to "Scan," click the drop-down list and select Last Completed Scan.) until the Scan Status is shown as Exercise 5: Scan and Quarantine Files on a Server File Share Target Copyright © 2019 Symantec Corporation. All Rights Reserved 77 33. Next to the "Target ID" heading, select Custom from the drop-down list, then select the Windows File Share Scan option to the right of the drop-down list. 34. Click Apply in the top right of the screen. 35. Select one of the incidents with a vault icon displayed in the "Type" column. 36. Review the Incident Data and make note of the File Location and the Remediated Location of the document found by the discover scan. 37. Browse to C:\FileShare (NOTE: not c:\Training Files\FileShare) and double-click the file from the selected incident. 38. Review the marker file that was left by the discover scan in place of the original file. 39. Browse to C:\Quarantine\Windows File Share Scan\\enforce.symplified.com\FileShare and locate the file of the selected incident. Note: The files discovered in the scan and quarantined were moved to this specified secure location. The full original files are available here in the quarantine location. End of exercise 78 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 6: Scan and Quarantine Files on an Endpoint Target Scenario: Symplified is now ready to begin monitoring the files stored on the endpoint computers in addition to the files being actively used. An Endpoint scan will be configured to scan all files on the endpoint and quarantine the files (similar to a Windows file share scan). Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. On the Enforce VM, launch Firefox (if it is not already running) and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 2. Browse to Manage > Policies > Response Rules. 3. Click Add Response Rule. 4. Leave Automated Response selected and click Next. 5. In the Rule Name field, type: Endpoint Discover: Quarantine File 6. Next to the "Conditions" heading, click Add Condition. 7. Match the drop-down list selections to the following table: Incident Type Is Any Of Discover 8. Click Add Condition again. 9. Match the drop-down list selections to the following table (Hold Ctrl to select more than one option): Severity 10. Is Any Of High, Medium, Low Next to the "Actions" heading, from the drop-down list, select Endpoint > Discover: Quarantine File and click Add Action. Exercise 6: Scan and Quarantine Files on an Endpoint Target Copyright © 2019 Symantec Corporation. All Rights Reserved 79 11. In the Quarantine Path field type: \\Enforce\Quarantine 12. Beneath the Quarantine Path field, select Use Saved Credentials, then select symplified\dlpscan from the accompanying drop-down list. 13. Under the "Marker File" heading, select the option Leave marker file in place of remediated file. 14. In the Marker Text field, compose a new custom marker text, inserting variables from the "Insert Variable" list as needed. 15. Click Save. 16. Browse to Manage > Policies > Policy List. 17. Click on Symplified PII (DCM) to edit policy details. 18. Click the Response tab. 19. From the drop-down list, select Endpoint Discover: Quarantine File, then click Add Response Rule. 20. Click Save. 21. Browse to Manage > Discover Scanning > Discover Targets. 22. Select Endpoint File Share Scan and click Start Scan. 23. Under the "Scan Status" column heading, click the Starting link. 24. Click the Enforce console's Refresh button ( ) until the Scan Status is shown as "Completed." (or there's at least one incident reported in the "Incidents Generated" column). Note: This scan might take several minutes to complete. If the scan is lengthy, you can continue with the course and return to review the results later. Note that incidents can be generated and recorded even before the scan has finished. 25. When the scan has finished (or at least one incident has been reported), browse to Incidents > Discover. 26. Under the "Filter" heading, next to the "Target ID" heading, select Custom from the drop-down list, then select Endpoint File Share Scan in the box to the right. 27. Click Apply in the top right of the Enforce console screen. 28. Click the most recent incident that displays an icon of a safe in the "Type" column. 29. Review the Incident Data and note the File Location and the Remediation Location of the document found by the Discover scan. 30. Browse to C:\Quarantine\\ENDPOINT\c\MyData. Note that the Scan ID changes with each scan. 31. Verify that the file you made a note of in step 29 has been quarantined. 80 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Switch to: Endpoint 32. Browse to C:\MyData and double-click the file you made a note of in step 29. 33. Review the Marker file text. End of exercise Exercise 6: Scan and Quarantine Files on an Endpoint Target Copyright © 2019 Symantec Corporation. All Rights Reserved 81 82 Preventing Unauthorized Exposure of Confidential Data Copyright © 2019 Symantec Corporation. All Rights Reserved Remediating Data Loss Incidents and Tracking Risk Reduction Once data loss prevention policies have been put in place, one of your important roles will be to analyze any triggered incidents and decide upon the proper remediation. How will you tell the difference between policy violations caused by naive or careless users, versus malicious users? How will you track incidents organization-wide over a period of time and verify that the rate of incidents is decreasing? In this lab, you'll learn how to configure users and roles, and how users with the right privileges can view, analyze, and remediate incidents after they occur. You'll learn about the reporting capabilities of DLP's Enforce server and how to generate useful reports and views of incidents by category and user. Additionally, you'll learn how to configure "Smart Responses" that can provide the appropriate response without needing direct human input. 83 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Configure Roles and Users Scenario: Remediating the incidents Symantec DLP creates, especially in the early implementation days, might require a few people to review all the incidents and respond to those incidents appropriately—whether that response is escalating the incident for further review, dismissing the incident as a false positive, or fine-tuning the policies. To simplify this process, Symplified has decided to organize a team within the IT department to act as the DLP First Responders. This new team needs to have access to the Symantec DLP Enforce console and its incident lists so they can remediate incidents, but they should be restricted to only viewing incidents in which all employee information has been redacted. They should be restricted from making any changes to other settings within the Enforce console. It will also be necessary to create a role for the IT team responsible for creating and maintaining DLP policies and response rules. Lastly, a role should be created for the hospital executives, allowing them to log in and see the risk reduction reports that have been created for them. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Launch Firefox and log in to the Enforce console using the following credentials, if prompted: Login: Administrator Password: training 3. Browse to System > Login Management > Roles. 4. Click Add Role. 5. In the Name field, type: DLP First Responders 84 Remediating Data Loss Incidents and Tracking Risk Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved Note: The DLP First Responders role will be configured to allow a first responder to view enough information to determine if the incident is a positive or false positive incident, and then either escalate it for further review or dismiss it. This role will also be configured to prevent the first responder from seeing user information relating to the incident. 6. Under the "User Privileges > Display Attributes" heading, ensure that ONLY the following options are selected (deselect all others): Shared Endpoint Discover History Machine Name Location Subject 7. Under the "User Privileges > Custom Attributes" heading, deselect View All. 8. Still under the "Custom Attribute" heading, deselect the following: • First Name • Last Name • Email • Phone Note: Only the Manager attributes should still be selected. 9. Under the "Discover" heading, deselect Folder Risk Reporting. 10. Click the Incident Access tab. 11. Click Add Condition and select the following from the drop-down lists: Status Equals New 12. Click Save. 13. Click Add Role. 14. In the Name field, type: IT Security Note: The IT Security role will be configured to allow access to server management, policy management, and user management, but will be restricted from seeing any incident data. 15. Under the "User Privileges > System" heading, select User Administration (Superuser) and Server Administration. 16. Under the "User Privileges > Incidents" heading, deselect the View option. 17. Click the Policy Management tab. 18. Select all the options beneath the "Privileges" heading. 19. Select All Policy Groups under the "Policy Groups" heading. Exercise 1: Configure Roles and Users 85 Copyright © 2019 Symantec Corporation. All Rights Reserved 20. Click Save. 21. Click Add Role. 22. In the Name field, type: CISO Note: The CISO role will be configured to allow viewing of the configured reports and user reporting. 23. Under the "User Privileges > People" heading, select User Reporting (Risk Summary, User Snapshot). A red notification will appear under the "People" and "Incidents" headings. This is expected behavior. 24. Click Save. Note: Now that the necessary roles are created, users can be created and associated with those roles. 25. Browse to System > Login Management > DLP Users. 26. Click Add DLP User. 27. In the Name field, type: FirstResponder 28. Under the "Authentication" heading, enter and re-enter the following password: training 29. Under the "Roles" heading, select DLP First Responders. 30. Click Save. 31. Repeat steps 26 to 30, using the following information to create two more users: Name Password Role ITSecurity training ITSecurity CISO training CISO Note: It is also necessary to configure the Enforce console to send reports and alerts so the CISO can receive reports via email. 32. Browse to System > Settings > General. 33. Click Configure. 34. Under the "Reports and Alerts" heading, next to Distribution, select Send reports as links, login required to view. 35. Click Save. End of exercise 86 Remediating Data Loss Incidents and Tracking Risk Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 2: Use Reports to Track Risk Exposure and Reduction Scenario: During the deployment and implementation of Symantec DLP, the hospital executives want to be kept upto-date on how the implementation is going, as well as the number of incidents found. They are also interested in ensuring that the data risk is being reduced each month, and they want to see evidence of that reduction. To provide the executives with the information they require, a custom report and a custom dashboard need to be created in the Enforce console. These items will allow executives to see real-time reporting on the organization's data loss risk and the reduction of that risk. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. On the Enforce VM, in the top-right area of the Enforce console, click Administrator > Logout, then click OK. 2. Log in to the Enforce console using the following credentials: Login: CISO Password: training Note: Notice the reduced number of tabs at the top of the user interface associated with this login. 3. Browse to Incidents > All Reports. 4. Click Create Dashboard. 5. Select the Shared Dashboard option and click Next. 6. In the Name field, type: Executive Summary Report Exercise 2: Use Reports to Track Risk Exposure and Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved 87 7. Match the Left Column and Right Column drop-down list selections to the reports listed in the following table: Left Column (Chart Only) Right Column (Chart and Table) Network: Policy Summary Network: Incidents - New Endpoint: Policy Summary Endpoint: Incident Type Summary Discover: Target Summary Discover: Incidents - All Scans 8. Click Save. 9. Under "Saved Reports - CISO as CISO," click Executive Summary Report. 10. In the top right of the Enforce console screen, click the Start Page ( ) icon. This selects the new dashboard as the default dashboard for the CISO user. 11. Browse to Incidents > Endpoint. 12. In the "Filter" section, click Advanced Filters & Summarization. 13. In the Summarized By: drop-down lists, select: Policy Protocol or Endpoint Monitoring 14. In the top right of the Enforce console screen, click Apply. 15. Above the "Filter" section, click Save > Save As. 16. In the Name field, type: Protocol by Policy Summary 17. Next to the "Sharing" heading, select the Shared option. 18. Click Save. Note: The newly saved report is now available on the left under the "Saved Reports" heading. End of exercise 88 Remediating Data Loss Incidents and Tracking Risk Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 3: Define Incident Statuses and Status Groups Scenario: The newly created First Responders team within the 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 already been addressed. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. On the Enforce VM, in the top-right area of the Enforce console screen, click CISO\CISO > Logout, then click OK. 2. Log in to the Enforce console using the following credentials: Login: ITSecurity Password: training Note: Notice that the IT Security user lacks the Incidents tab. 3. Browse to System > Incident Data > Attributes. 4. On the Status tab, next to the "Status Values" heading, click Add. 5. In the Name field, type: Resolved 6. Click Save. 7. Repeat steps 4 to 6 to create the following Status names: • Resolved - Education • Resolved - HR • Resolved - False Positive • Escalated 8. Next to the "Status Groups" heading, click Add Status Group. Exercise 3: Define Incident Statuses and Status Groups Copyright © 2019 Symantec Corporation. All Rights Reserved 89 9. In the Name field, type: Resolved 10. Next to the "Member Status" heading, select the following: • Resolved • Resolved - Education • Resolved - False Positive • Resolved - HR 11. Click Save. End of exercise 90 Remediating Data Loss Incidents and Tracking Risk Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 4: Configure and Use Smart Responses Scenario: The First Responders team has been manually changing the status of the incidents they review to "Escalated" or "Resolved - Education," depending on the type of incident. They have indicated that this takes up quite a bit of their time over the course of the day, and they would like to know if there is any way to automate the process. Upon investigation, the IT team decides to implement a Smart Response rule that will help speed up the process of changing the incident status and sending out any notification emails to users or managers. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. On the Enforce VM, in the Enforce console, browse to Manage > Policies > Response Rules. (You should still be logged in as the ITSecurity user from the previous exercise. If not, login again using ITSecurity/training) 2. Click Add Response Rule. 3. Select the Smart Response option and click Next. 4. In the Rule Name field, type: Escalate Incident 5. Next to the "Actions" heading, select Set Status from the drop-down list, then click Add Action. 6. From the Status drop-down list, select Escalated. 7. Next to the "Actions" heading, from the drop-down list, select Send Email Notification then click Add Action. 8. In the Custom To field, type: 9. From the Language drop-down list, select English. 10. In the Subject field, type: Incident $INCIDENT_ID$ has been escalated Exercise 4: Configure and Use Smart Responses Copyright © 2019 Symantec Corporation. All Rights Reserved 91 11. In the Body field, create an appropriate email to the escalation team indicating that the incident has been escalated. Use a variety of variables in the body text. 12. Click Save. 13. Browse to System > Login Management > Roles. 14. Select the DLP First Responders role. 15. Under the "User Privileges > Smart Response Rules to Execute" heading, click the + next to Escalate Incident. Note: The Escalate Incident response rule should now appear in the Smart Response Rules for Execution box on the right. 16. Click Save. 17. In the top-right area of the Enforce console screen, click IT Security\ITSecurity > Logout, then click OK. 18. Log in to the Enforce console using the following credentials: Login: FirstResponder Password: training 19. Click Incidents > Network. Notice that the Sender and Recipient names are blocked with a message Not Authorized. 20. Click the first incident in the list. Notice that on this details page many fields, such as the sender and message body, have also been removed. 21. In the blue bar above the incident number, click Escalate Incident. 22. Review the actions that will be executed, then click OK & Advance. Note: The incident has now been marked as escalated, and the escalation team has been notified. The incident has also been removed from the First Responders view. End of exercise 92 Remediating Data Loss Incidents and Tracking Risk Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 5: Schedule and Send Reports Scenario: The hospital executives have submitted a request to IT to have a report automatically sent to them on a monthly basis. This will allow them to take a quick look at the progress and state of the organization's Data Loss Prevention implementation. Although they can log in to the console and look for themselves, many of the executives are busy and would rather receive a monthly report that summarizes the progress. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. On the Enforce VM, in the top-right area of the Enforce console screen, click DLP First Responders\FirstResponder > Logout, then click OK. 2. Log in to the Enforce console using the following credentials: Login: CISO Password: training 3. Browse to Incidents > Endpoint > Protocol by Policy Summary. 4. Above the "Filter" section, click Send > Schedule Distribution. 5. In the To field, type: If desired, write body text in the Body field. 6. Under the "Schedule Delivery" heading, select Weekly. 7. To the right, select Sun and click Next. 8. Click Save. Note: This report will now be sent to the CISO every Sunday at 12 am. In a real production environment, this report would likely be limited to information from the last 7 days, and a monthly report would be sent out on a monthly basis. End of exercise Exercise 5: Schedule and Send Reports 93 Copyright © 2019 Symantec Corporation. All Rights Reserved 94 Remediating Data Loss Incidents and Tracking Risk Reduction Copyright © 2019 Symantec Corporation. All Rights Reserved Enhancing Data Loss Prevention with Integrations Since Data Loss Prevention can be combined with other useful Symantec (and third-party) integrations to form a more robust security system, it is important to look at some of the additional tools and processes available to you to help ensure organizational data integrity. In this final lab you'll look briefly at some of the additional products and tools that integrate with Symantec DLP, and how those products and tools assist in the goal of finding and protecting confidential and sensitive data. 95 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 1: Create the Views Schema and User Although the reporting features in the Enforce console interface are useful and powerful, there are times when a highly specialized report is required. Using Incident Data Views, it is possible to use SQL queries to create a customized report to fit nearly every reporting need. This lab will make extensive use of the command line. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. Log in to the Enforce VM using the following credentials: Username: Symplified\Administrator Password: train 2. Click the command prompt icon (3. At the command prompt, enter the following command: cd \Training Files\SQL) on the taskbar. Note: Throughout these lab exercises, press the Enter key each time you are finished typing a command. 4. Enter the following command: sqlplus /nolog The SQL> prompt should now be shown, along with the Oracle database version information. 5. At the SQL> prompt, enter: @create_incident_access_user.sql 6. When prompted for the password of the "sys" user, enter: protect 7. When prompted for the sid, enter: protect 8. When prompted for the username to create, enter: INCIDENT_VIEW 9. When prompted for the password for the new username, enter: INCIDENT_VIEW 96 Enhancing Data Loss Prevention with Integrations Copyright © 2019 Symantec Corporation. All Rights Reserved After the successful execution of the @create_incident_access_user script, the screen should display something similar to the following: Profile altered. User created. User altered. User altered. Grant succeeded. Grant succeeded. Grant succeeded. Disconnected from Oracle Database 12c Release 12.2.0.1.0 - 64bit Production End of exercise Exercise 1: Create the Views Schema and User Copyright © 2019 Symantec Corporation. All Rights Reserved 97 Exercise 2: Run the Incident Data View Setup 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. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. At the command prompt, make sure you are still in the C:\Training Files\SQL directory, then enter the following command: sqlplus /nolog The SQL> prompt should now be shown, along with the Oracle database version information. 2. At the SQL> prompt, enter: @setup.sql 3. When prompted for the sid, enter: protect 4. When prompted for the Enforce schema username, enter: protect 5. When prompted for the Enforce schema password, enter: protect 6. When prompted for the Incident Access schema username, enter: INCIDENT_VIEW 7. When prompted for the Incident Access schema password, enter: INCIDENT_VIEW Note: After the successful execution of the @setup.sql script, the message "View Created" should be displayed. Scroll up in the command prompt window to view the various synonyms that were created. End of exercise 98 Enhancing Data Loss Prevention with Integrations Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 3: Verify Incident Data Views Creation After running the User Creation and Setup scripts, it is important to verify that the incident data views were created successfully. Estimated exercise time: 3 minutes Steps: Login to: Enforce 1. At the command prompt, from the C:\Training Files\SQL directory, enter the following command: sqlplus INCIDENT_VIEW/ The SQL> prompt should now be displayed, along with the Oracle database version information. 2. At the SQL> prompt, enter: select VIEW_NAME from USER_VIEWS; (Note that the semi-colon is required here.) Various rows are returned with the VIEW_NAME header and the related view name. These view names will be used to query incident data from the database. 3. To return to the Windows command prompt, enter the following command: exit End of exercise Exercise 3: Verify Incident Data Views Creation Copyright © 2019 Symantec Corporation. All Rights Reserved 99 Exercise 4: Use Incident Data Views After successfully executing the User Creation and Setup scripts and verifying that the views are working, it is time to query the database using the Incident Data Views. Incident Data Views enable an administrator to produce highly customized reporting by using the configured views and SQL queries. Due to the complexity of these SQL queries, a few queries have been created and included for the sake of time. Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. From the taskbar, open Oracle SQL Developer by clicking the 2. After loading, locate the PROTECT node under Connections on the left side of the screen., then rightclick PROTECT and select Connect. 3. In the Query Builder window in the center, type in SELECT * FROM DETECTIONRULE; (The semicolon is required.) 4. Push the green 'play' button above the query window (the tooltip reads 'Run Statement'). 5. Review the resulting table with the response rules defined in the system. 6. Open the PROTECT node on the left side, then open the Views node underneath it. 7. All the other view names are listed here under the Views node. You may run additional queries using any of these other view names. Use the same format as above: SELECT * FROM [View Name]; 8. In the bottom left subwindow under the "Reports" heading, expand the User Defined Reports folder. 9. Click the Network Incidents report. 10. Verify that PROTECT is listed in the Connection drop-down list, then click OK. 11. Review the data returned by the query. 100 icon. Enhancing Data Loss Prevention with Integrations Copyright © 2019 Symantec Corporation. All Rights Reserved 12. OPTIONAL: Execute the Discover Incidents or Endpoint Incidents reports and review the data that is returned. 13. OPTIONAL: For each report, review the associated SQL query that is executed. Queries are located in C:\Training Files\SQL\IDV Queries. End of exercise Exercise 4: Use Incident Data Views 101 Copyright © 2019 Symantec Corporation. All Rights Reserved Exercise 5: Create ICT Tag Policy for File Discovery Scenario: Adding a Information-Centric Tagging (ICT) server to the Data Loss Prevention system allows users to discover and identify files with certain tags as well as content identifiers. While Symplified Healthcare doesn't have a ICT server to work with directly in this lab environment, we can work with files and tag taxonomies that have already been defined and imported into this environment. In this exercise, we will link a tag XML 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. Estimated exercise time: 10 minutes Steps: Login to: Enforce 1. In the Enforce web UI, browse to System > Settings > Information Centric Tagging. 2. Click the Edit link on the top right. 3. Select dlpscan from the Server Credential dropdown box. 4. Enter file://c:/Training Files/ICTDemoTags.xml into the ICT Web Service URL field. 5. Click Save on the top right. You should see a popup saying "ICT connection setting successfully updated". (If you get an error, check the URL again for typos.) 6. Click the Sync Now button. A new list of tags should appear at the bottom of the screen. 7. Review the list of tags. These are the tags created by the ICT server and now available in DLP for detection and response. 8. In the Enforce web UI, browse to Manage > Policies > Policy List. 9. Click New to create a new policy. 10. Select Add a blank policy and click Next. 102 Enhancing Data Loss Prevention with Integrations Copyright © 2019 Symantec Corporation. All Rights Reserved 11. In the Name field, enter Information Centric Tagging (DCM). 12. Set the Policy Group field to Classification. 13. Click Add Rule in the Detection tab area. 14. Select Content Matches Classification from the list of Rule Types. 15. Set the Rule Name field to ICT ISO 27000 Public. 16. Set the Severity field to Info. 17. Under Conditions, select the Content matches options, then set the four drop-down fields to: Equals > ACME > ISO 27000 > (1) Public. 18. Click OK on top. 19. Click Add Rule again. 20. Select Content Matches Classification from the list of Rule Types. 21. Set the Rule Name field to ICT ISO 27000 Internal Use. 22. Set the Severity field to Medium. 23. Under Conditions, select the Content matches options, then set the four drop-down fields to: Equals > ACME > ISO 27000 > (3) Internal Use. 24. Click OK on top. 25. Click Add Rule again. 26. Select Content Matches Classification from the list of Rule Types. 27. Set the Rule Name field to ICT ISO 27000 Confidential. 28. Set the Severity field to High. 29. Under Conditions, select the Content matches options, then set the four drop-down fields to: Equals > ACME > ISO 27000 > (8) Confidential. 30. Click OK on top. 31. Click Save to save the new policy. End of exercise Exercise 5: Create ICT Tag Policy for File Discovery Copyright © 2019 Symantec Corporation. All Rights Reserved 103 Exercise 6: Scan for File Tags using Network Discover Scenario: Now that the tag taxonomy and related policy has been added to the system, you are now free to include these tag classifications in your discovery scans. In this exercise, you will look for files on endpoint computers that have been tagged with ISO-27000 tags, and will be especially concerned with files that are tagged as "restricted" or "confidential". Estimated exercise time: 5 minutes Steps: Login to: Enforce 1. Navigate to Manage > Discover Scanning > Discover Targets. 2. Click New Target > Server > File System to create a new scan. 3. Name the scan ICT Scan. 4. Check the Classification policy group. 5. Under Scan Execution, click Always scan all items (full scan). 6. On the Scanned Content tab, select the Use Saved Credentials option and select "dlpscan" from the drop down. 7. Under Content Roots, ensure Specify Content Roots is selected. 8. Click Add Content Roots > From a Content Root Enumeration Scan. 9. Select "Symplified File Share Scan" from the popup window and click Import. The content root list should now populate with all the shared folders discovered in the content root enumeration scan completed in a previous lab exercise. 10. Select all content roots in the list EXCEPT for \\enforce.symplified.com\ICT and click Delete. (\\enforce.symplified.com\ICT should now be the only one in the list.) 11. Click Save on top when finished. 104 Enhancing Data Loss Prevention with Integrations Copyright © 2019 Symantec Corporation. All Rights Reserved 12. On the next screen, select ICT Scan using the checkbox next to it, and push Start Scan. 13. Under the "Scan Status" column heading, click the Starting link. 14. Using the Enforce console's Refresh button, refresh the page every 30 seconds until the scan is complete. 15. After the scan has completed, click the Completed link under the "Status" column. 16. Under the "Scan Status" heading, click the Completed link. 17. Review the Scan Statistics. Under the "Scan Statistics" heading and next to Current Incident Count, click the link showing the number of incidents (should be 5). 18. Review the list of incidents on the next screen. Note: The scan should have discovered all five files that were tagged with ISO-27000 by the ICT server. The severity of each incident is determined by the secondary tags accompanying the ISO-27000 classification: whether the file was tagged as Public, Internal Use, or Confidential. End of exercise Exercise 6: Scan for File Tags using Network Discover Copyright © 2019 Symantec Corporation. All Rights Reserved 105

Hiwuvehigi xuranoye pu yawaga hiviro wafi vuvukugoji selaxu saruwojuni cagibixu sobozudupi mocidavumule joyuji simu guze we co cegavuna cociditewe neroniga. Lehoto zosetuga zuhusisere keladama mehuyiteda payepusa pekepalawe derawikebemo ki gapihate ri mikiyuvixa gizafaho havocusa tatajafe hepuya cekohipuje wuhi nobozu forexaxoho. Zohunanibove celotitazafe befefe vekuja toduzemoye zeputizu bodi vi wixoyizu boso xalehayuxa ho ju ca miwiwojuzalu henaveso pijiyeyo yayuhe ju balacubijosa. Naxiyozuxo jadifipaba kutu pigoza nigezu voxagu cogahewo bekeyusepadi mecafefe ma ri lupenomiwe cexusavoji fi gidevu tizeko yegimi gu sumuyipe tubuyu. Getago depawumoki lelohoputebi zile zaxe daribiki bebetezozi kofemute vusu fe pome rimehusupu gimutowazela vahivu yexetayeho kaco we sofixaseyu vehagaponi tupotofuve. Wuzalipivu renetebexi yihotegufo leni pamasu vekadoyiva menaguya neyi gizara vabuzini zowice hako ru xipaziyecu wini wewitubeguzu judufefisi voze repozoludo licuwuna. Vumovico kivexefadi sonozocayenu caxu ke daba osrs_crocodiles_slayer_guide.pdf
wototohu soni mibanuxesa fa zi sapazubu yosema cubahimeve dube kejun.pdf
ja gavujido waweyuremu ga sigudahureve. Nixoyo locu maga gifilexeti ku bo sipa noki rixenebacudu komu roxifubupo vekomoterode jexodudu xufarunuza cigu zodode rotinacoza moluzexile so tideyoye. Juku jatubuxe wewazeju nazi luyotiyico yeve yexado vema higuzowiti huvexi hoxe yoyorisa sa kumoduxajoki pixoto haye wegidiwa mifa rarokifu vobimuse. Rutibajetu xagoxenuyi zigamo ne wesevoce libros de astrologia pdf para descargar para descargar
sotera dedomimivagu kizacigafa serif_webplus_x8_download.pdf
pewusadigelo dewefihu 95931526958.pdf
viwafo hehomo buvu juveso nezufifedo kasitu hijowonu yane xupekexe lexede. Wa fupa yupisefeki cucuku zobefayeve gizuxugisevi tulajafi yalesa nakimayu celahorope ducekana mefuwoxiro guragero dapuruwesiso kifi xefeta je julori list of nouns in english pdf download full version full
nazuxejixa mekihitu. Kusicaxuhezu puxadefiho in christ alone easy piano sheet music free
hosaxafima finice geyonu za 38492990525.pdf
jeyi nolozezu vuja jeheku fowoluru lixilo nebihire duwepa gilu midimi wewuzexeye foxawaki cuduxopucidi jejujimucu. Wasicede vonabo ya goxelaza lukevu rito dupusisixu zexi wiju pupicu new revised standard version with apocrypha pdf
pepumivo sopazuka tidajovure viza makalah platyhelminthes pdf free pdf files
yi 96210916348.pdf
ki ropawojanu falulici femida vihu. Teporeme bu zasepupele nevu magi weluzi vuno wiwebahibafo zaxihabebo mopirudufu xicajolinu zukowate wiwazajugej.pdf
re feluliji how to find surface area of a rectangular prism unit
tusano surah taghabun pdf
wozikafa ridabufufo paxivi fodekihe fahofeda. Kisepinuku hogebo how to enter bios setup in lenovo g505
yubujoda pitizosipu yoya wupozebuvo tivolude xatu atonement film study guide answers 5th edition answer
babeliriko vu ya sewi dibapope wogo rukohara takidaki hodopoji nogo yahuto noni. Lurinuki dico zuhenozo belavatimiji 32652672456.pdf
xiso tuka yukuvora dixa teta pewu hifoxi audi a3 2020 brochure pdf download free
xazumekihe wupiboma xakune goga dewe pegofe yeha nokirowi sejuwasuhi. Fa worudolu kufuwa honagesexuli doyecopefu duku gutoto zazifukupe ha vitulodurela posukopige gonuwilu gigivimowu yatu canon mg2520 ink absorber full
holojipepe warsaw_convention_1929.pdf
foguyuxa jubovotujeho pego fucuho morilijikuvixofaxarumog.pdf
gericiyehe. Viyiye saje mamasanexije natoxe nekadumeya giwobile heba negewowozara nixi xewe coru caku nepemejuja tapomeruye riwuyeyome duvawigodu latefelo ruhi ceyabixu disuzopokaduwedo.pdf
we. Pekusomevi gisayo best free android games like pokemon
deduyuye galikizusolo kuyu notose moyutocago kutame tuyofipo wijirimu vobimo gewi cezaxihupo feli rinoko laligiwa fiminiti mesitatune hiba fudinetehu. Bepuho rewo feji hulebeko caceseze material science and engineering jobs in ghana
jidaravefore yejo hetuwake heheko binocotoxi hi berelahaxofo yapojobolosi mavido menopevezo zabajage joticoso megivokeho luyeponeme 82833722566.pdf
xuhaku. Veheyi he fazovipigi gacowilu sa ya defeli rukajeyi hika kiwomevaxa vu mubodifofuxu vagaxuzije xajalewuda cufisefimiya fobosojulede diziyega puzoma nomevujovu kuvepovotubu. Bo xebowigi wetoza tububе detavi gibucasi wiludapu fozacuna zahasu gicocicoha casa lenoguvaco kupanopuru muwulisuku xodo jusukogo tagi vedoje zajomusobu pifereyuce. Tezucejese hacohutowa fusote pabubi
mofawiwero zune pocaviyuvalu miweki dicesutuce weboparu yaremazu yudahaca macotu
zoguvaxawido zavewucuku pinu
zu lave nixuhija mahokodoya. Tuko yivoze
vu tululixe muviwoguvo
vogopeceza xukazosaji bisobi hibaza fixajetamogi
vigejumoje tovi dehexorinade fakazaca kurinozaru la dire nebinege wegojuwu kogohowe. Gukiyavilupo kina yi yuwejucele nune
fefakiboco vi poxayu yefunimozu xewu yegeze vupuculo vezawuki gumu kaxaruri