ByStorm Software

www.bystorm.com

877-BYSTORM

How to get an e-mail alert when someone sends sensitive files with Webmail.

1. First we need to define what files are sensitive, for my example I'm going to use the trial rule: Audit Access to Microsoft Office Files.

Common tasks	Rule management	Analysis, Reports and Alerts		
Local rules	Master rules (read-only)			
Auditing Re	ile - Monitor AutoCAD file	·		
🖌 🖌 Auditing Ru	ile - Trial Rule for Local N	Machine - Audit Access to Microsoft Office Files		
Auditing Bu	ile . Watch a file			
📃 🗌 Auditing Ru	Auditing Rule - watch exe writes and deletes			
🔲 Auditing Rule - Watch File Accesses				
Auditing Rule - Watch Folder Moves				
📃 🗌 Auditing Ru	Auditing Rule - Watch temp			
📃 🗋 Deny Rule	Deny Rule - Block CD writes			
🖌 🖌 Deny Rule	- Block malware			
📃 🗌 Deny Rule 🛛	- Block Switchblade			
ByStorn	n Software			

2. If we click the 'Edit rule' button, we can see some more information about what exactly this rule will monitor.

わ FileSure - Auditing Rule	×
Rule name: Trial Rule for Local Machine - Audit Access to Microsoft Office Files	Operations to Audit Deselect All
File name filters Include: *.xls; *.doc; *.ppt; *.vsd; *.xlsx; *.dc User name filters Include: * Include: * <td>Access checks ✓ Read access ✓ Write access ✓ Delete access Status changes ✓ Create ✓ Delete ✓ Rename ✓ Security Changes Content operations ✓ File read ✓ He write</td>	Access checks ✓ Read access ✓ Write access ✓ Delete access Status changes ✓ Create ✓ Delete ✓ Rename ✓ Security Changes Content operations ✓ File read ✓ He write
File size filters Other Options Program name filters Group name filters Machine name filters Time slot	filters Signature filters
Bule applies to Image: Send e-mail on rule match Image: Hard drives Image: Files Image: Network drives Image: Folders Image: Network drives	reached.
CD/DVD drives Vorkstations Activate rule when the threshold of 20 matches within 60	minutes is reached.
Comment:	🗸 OK 🛛 🛛 Cancel

I've made a couple of changes and highlighted some interesting things.

- First I checked the Network drives since we want to monitor people sending network files and local drives.
- I also made sure that both servers and workstations were checked as well as 'File reads.' So, this rule now says, 'Record all activity on Microsoft Office files for any user, when the file is on a network, or locally (including removable drives and CDs) and when that file is accessed from either a workstation or a server.'
- 3. Now that we've set up our auditing rule, we need to set up the e-mail alert. On the Common Tasks tab, select the 'Set up an e-mail alert' task.



[Note: if you are prompted to set up your SMTP settings, select 'Yes' and enter them]

4. This will bring up the 'Define alert' screen, click the 'Manage Summaries' button in the upper right:

💦 Define Ale	ert		_	_	
Summary:	Extension Summary by User		<u> </u>) Manage Summaries	2
				Sample Summary	Data
	Count	userName	extension		-
	▶ 29	BYSTORMSOFTWARE\allengh	vic		

5. On the Manage Summaries screen, click 'New...' at the bottom, since we need to set up a new summary for what we want to be alerted on:

Summaries: Drag a column header here to group by that column.			
nabled	Record Age	Summary Name	
V	1 days 0 hours 0 minutes	Extension Summary by User	
	1 days 0 hours 0 minutes	Drive type usage by user	
	1 days 0 hours 0 minutes	Program summary	
	1 days 0 hours 0 minutes	Root Folder Moves	
V	0 days 0 hours 5 minutes	Auto-generated summary for alert: 214,335,828	
V	0 days 1 hours 0 minutes	Possible AutoCAD theft	
	0 days 0 hours 10 minutes	Hidden File Access	
~	0 days 1 hours 0 minutes	Summary for rule: watch exe writes and deletes	
	0 days 0 hours 5 minutes	Auto-generated summary for alert: 43,349,093	
	0 days 1 hours 0 minutes	Test summary	

6. This will bring up the 'Define Summary' screen and since we're lucky enough that this is a pretty popular request, click on the 'Visit the Summary Section of the ByStorm User Forum' link at the bottom:



7. Clicking on the link will open a browser and navigate to the ByStorm User Forum. The summary you want is:



and it will bring up the following screen:

Protected dat	ta being sent by web mail.		
new topic pos	treply ByStorm Software Forum Index -> Alert summaries		
	View previous topic :: View next topic		
Author	Message		
ByStormAdmin Site Admin	🗅 Posted: 16 Mar 2009 08:34 am 🛛 Post subject: Protected data being sent by web mail. 🔅 🖓 quote 📿 edit 🗶 🕪		
T	This summary will list every instance of a protected file being read by either Internet Explorer or FireFox. Protected data being read by a internet browser typically means that someone is stealing data.		
Joined: 10 Aug 2004 Posts: 43	Select 1, * from AuditRecords where eventTime > OldestRecordAge and ((exeName = 'iexplore.exe' or exeName) = 'firefox.exe') and deniedOp = 0)		
Back to top	🗟 profile) 🗟 pm) (af email)		
	Display posts from previous: All Posts 💌 Oldest First 💌 🛛 Go		
Brautanie Brae	All times are GMT - 6 Hours		

 Cut and paste the 'Summary title' from the web page to the 'Define summary' screen in FileSure. Do the same thing for the SQL query. Leave the OldestRecordAge at 1 hour and when you're done, you should have something looking like this:

わ Defin	e Summary		
Name:	Protected data being sent by w	veb mail.	🔽 Enabled
Oldest	Record Age: 0 🛨 days	1 🛨 hours 0 🛨 minutes	
	Select 1, * from AuditRecords w exeName = 'firefox.exe') and de	where eventTime > OldestRecordAge and ((exeName sniedOp = 0)	= 'iexplore.exe' or
SQL Query:			
	Test Summary Query	🔲 Publish this summary as a deskto	p/screensaver alert
			Sample Summary Data
	Visit the Summary Section of th	ne ByStorm User Forum.	OK 🛛 🛛 Cancel

[Note: You might have a little trouble copying the title from the webpage into the Name field since the copy sometimes picks up a blank line before the title.]

- 9. Click OK to close the Define Summary screen, click 'Close' to close the Manage Summaries screen and click 'Ok' on the message box saying you might need to wait a few minutes for the summary to be published.
- 10. After a couple of minutes, click the 'Summary' drop down at the top and select our new 'Protected data being sent by web mail' option. Fill out the rest of the form per your requirements; if you right click in the Subject and Body sections, you can select values from the summary. Here is how I sent my example:

ろ Define Al	ert _ D >	(
Summa y:	Protected data being sent by web mail.	
C C	Sample Summary Data	
	Count ouser ev exten fil op m re wr de re m de is wa ex dri ex wa re op alert	ID
	Monitor all machines	
ſ	UUAL24	
Machiner		
in doninio .		
L		
	Send e-mail when count exceeds 10 - Do not send e-mails more than every 30 - minutes.	
Mail to:	gene@bystorm.com	
Subject	Possible data theft	
	/ <%userName%> sent <%fileName%> on <%MachineName%> at <%eventTime%>	
Body		
body		
	¹ "Use right-click to enter a variable. [Note]: the body text will repeat once for every item over the threshold.	
	To: gene@bustom.com	
	Subject Bossible data theft	
Proview		
1 1041044		
	M Enabled V OK S Cancel	

Make sure to click enabled, and then click OK.

If you now try to send a file by webmail, you should get an alert.