



Investigating Email Forwarding rules in the Unified Audit Log (UAL)





@InvictusIR

Copyright: Invictus Incident Response B.V.

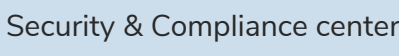
Scenario 3: New transport rule

	Operation	Investigation note
 Microsoft 365 Portal	New-TransportRule	Rule details in the 'Parameters' field
 PowerShell/API	New-TransportRule	Rule details in the 'Parameters' field

Scenario 4: Modified or Deleted transport rule




	Operation	Investigation note
 Microsoft 365 Portal	Set-TransportRule	Rule details are in the 'Parameters' field
	Remove-TransportRule	
 PowerShell/API	Set-TransportRule	Rule details are in the 'Parameters' field
	Remove-TransportRule	

Alternative scenario : Security Alerts created due to email forwarding rules




	Operation	Investigation note
 Security & Compliance center	AlertTriggered	Alert details in the 'Details' field
	AlertEntityGenerated	

Email Forwarding Rules

Scenario 1: New email box rule

	Operation	Investigation note
 Microsoft 365 Portal	Operation = New-InboxRule	Rule details in the 'Parameters' field
	Operation = Set-Mailbox & ForwardingSmtpAddress OR DeliverToMailboxAndForward OR ForwardingAddress	
 PowerShell/API	Operation = New-InboxRule	Rule details in the 'Parameters' field
 Outlook client	Operation = UpdateInboxRules & RuleOperation = AddMailboxRule	Rule details in the 'OperationProperties' field

Scenario 2: Modified or Deleted email box rule

	Operation	Investigation note
 Microsoft 365 Portal	Operation = Set-InboxRule	Rule details in the 'Parameters' field
	Operation = Remove-InboxRule	
 PowerShell/API	Operation = Set-InboxRule	Rule details in the 'Parameters' field
	Operation = Remove-InboxRule	
 Outlook client	Operation = UpdateInboxRules & RuleOperation = ModifyMailboxRule OR RuleOperation = RemoveMailboxRule	Rule details in the 'OperationProperties' field