suspicous mail

field	value
BlindCopyTo	hyunki1984@naver.com
ClientIP	199.66.91.253:40460
CreationTime	2018-08-20T11:21:40
ExternalAccess	false
Id	f131587a-a125-4e87-4421-08d5f268e1ac
Mode	Enforce
Name	SOX
Operation	New-TransportRule
OrganizationId	225e05a1-5914-4688-a404-7030e60f3143
OrganizationName	frothly.onmicrosoft.com
OriginatingServer	CY4PR17MB1398 (15.20.0973.010)
Parameters{}.Name	BlindCopyTo Comments Mode Name RuleErrorAction SenderAddressLocation StopRuleProcessing
Parameters{}.Value	Enforce False Header Ignore SOX hyunki1984@naver.com
Params	[{\
RecordType	1
ResultStatus	True
RuleErrorAction	Ignore
SenderAddressLocation	Header
StopRuleProcessing	False
UserId	fyodor@froth.ly
UserKey	1003BFFDA2E71FF9
UserType	2
Version	1
Workload	Exchange
app	Exchange
authentication_service	Exchange
command	New-TransportRule
date_hour	11
date_mday	20
date_minute	30
date_month	august
date_second	11
date_wday	monday
date_year	2018
date_zone	0
dest	225e05a1-5914-4688-a404-7030e60f3143
dest_name	225e05a1-5914-4688-a404-7030e60f3143
dvc	Exchange
host	splunk.froth.ly
index	botsv3
linecount	1
punct	{\
record_type	ExchangeAdmin

field	value
result	True
signature	New-TransportRule
source	https://manage.office.com/api/v1.0/225e05a1-5914-4688-a404-7030e60f3143/activity/feed/audit/20180725200144261001643$20180725200144261001643$audit_exchange$Audit_Exchange
sourcetype	o365:management:activity
splunk_server	botsv3
src	199.66.91.253:40460
src_ip	199.66.91.253:40460
status	success
tenant_id	225e05a1-5914-4688-a404-7030e60f3143
timeendpos	72
timestartpos	53
user	fyodor@froth.ly
user_id	fyodor@froth.ly
user_type	Admin
vendor_account	225e05a1-5914-4688-a404-7030e60f3143
vendor_product	Microsoft Office 365 Exchange