Threat Mitigation

The threat mitigation allows a LUCY admin to report reported phishing mails to according abuse contact of the provider's originating IP address taken from the message header. You can click on the mail symbol within the incident center to initiate the sending of the report:

Statis	Statistics +							
0	Time 0	Email 0	Client 0	Campaign 0	Score ()	Status 0		
	08/17/2020 15:17	ter propost of	A	5522 (1)	0.00	Simulation	⊠∎t⊛ ×	
	08/17/2020 14:08	ter propost or	N/A	N/A	10.00	Open	∆ ≊0 ×	
	08/17/2020 14:08	ter proposition of	N/A	N/A	10.00	Open	∆ ⊠ ¤⊙ ×	
	08/17/2020 14:07	ter proposition of	N/A	N/A	10.00	Open	20×	

The email send to the abuse contact of the provider can be edited within the incident settings:

Abuse			O Liphcal Meanage Technick	Rome	Controp + C Described	-
Quella Tiga O Aluse Coul Venime	Subject Desider Rome Resider E-mail	Alsum nobliation Benadig Chian sekan@phiamog.server.cent			Custom Rules Score Factors Algune Achteringon/Car	- august
	Camer	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		Pres Su 22012917 Dr. Dave 22012919 Automates		9004
		For none information, please and the atlanted message.		Unary 12	portud a new photong mail portud a printing site-defice mail reappears from (days).	12 10 4

The abuse report can contain the following variables:

- %domain% Domain or IP
- %email% actual Email
- %time% Tim

Default abuse template

LUCY comes with a default abuse template, which should be customized by the admin:

Last update: 2019/07/25 12:51

threat_mitigation https://wiki.lucysecurity.com/doku.php?id=threat_mitigation&rev=1542288653

Quick Tips Quick Tips	Subject Sender Name Sender E-mail	
You may use the following variables in the template: • NotemathS — Demain or IP • NotmatS — Email: • NotmatS — Time	Content	83mm 80 8 6 8 × 5 8 8 8 + + 4 5 8 5- 8 mm 8 0 8 6 8 × 5 8 8 8 + + 4 5 8 5-
		B J U S x, x ² x ² L = 12 + 0 11 + 0
		This is an exall abuse report for an exall nessage receives from Memolik on Mtimes.

From: https://wiki.lucysecurity.com/ - **LUCY**

Permanent link: https://wiki.lucysecurity.com/doku.php?id=threat_mitigation&rev=1542288653



Last update: 2019/07/25 12:51