

ThreatEye

How-To Guide: Casebook

How do you Create a Casebook or Add a finding to an existing Casebook?

How do you Create a Casebook or Add a finding to an existing Casebook?

● ● ← → ऌ м	● ● ● ▲ Findings Explorer x ▲ Findings Explorer x ▲ + ✓ ← → C a dex.ux-dex.threateye.loftindings ♥ △ ☆ ♣ □ ▲ : ☑ Maps M Gmail △ LiveWire confluen ●												
o»		Sep 15, 2022 14:26 → Se	p 22, 2022 14:26 O 🗸	Ex.: saddr=192.168.1.4		Search					A egraham@	pliveaction.com \sim	
ය ව ව	Findin Findin	gs Over Time gs nærd : Casebook 🖂											
Ì		TIMESTAMP	о тире о	MESSAGE C	HOSTNAME	SOURCE ADDRESS C	DEST ADDRESS C	CATEGORY C	DOMAIN	C FLOW COUNT	≎ tags		
Q													
		2022-09-15T14:33:01.0		threat indicator	141.98.10.90	141.98.10.90	216.197.73.65	Command and Control	none				
		2022-09-15T14:32:48.0_		threat indicator	141.98.11.54	141.98.11.54	216.197.73.76	Command and Control	none				
ŵ		2022-09-15T14:32:45.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.163	Command and Control	none				
~		2022-09-15T14:32:08.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.82	Command and Control	none				
		2022-09-15T14:31:52.0_		threat indicator	92.63.197.131	92.63.197.131	216.197.73.172	Command and Control	dag musictoday.com				
		2022-09-15T14:30:48.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.163	Command and Control	none				
		2022-09-15T14:27:44.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.185	Command and Control	none				
		2022-09-15T14:27:26.0	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.227	Command and Control	none				
		2022-09-15114-27:10.0	KOC	threat indicator	179.43.156.143	179.43.156.143	216.197.73.43	Command and Control	none				
		2022-09-15114:20:34.0	юс	threat indicator	92.03.197.131	92.03.197.131	216.197.73.134	Command and Control	none				
											1 - 10 of 5000		
					The table is limited to a	show 5000 of 392024 total res	ults. Use column filtering to se	e more targeted results.					
											?	:	

You can accomplish this through the findings area

OR you can also go into the analyst dashboard then click into a message of interest. This will take you to findings

o»	□ - Sep 15, 2022 14:26 → Sep 22, 2022	14:26 0 Ex.: saddr=192	.168.1.4	Search			A egraham@liveaction.com \lor
ŵ	Mitre Attack						
	Reconnaissance O Resource Develop	pment 😳 Initial Access	Credential Access	Discovery 🧿 Lateral	Movement OPPort Defense Evasion	Command and Control Collection	Exfitration
-	Number of techniques used: • 1-3 • 4-6 • 7+						
2	Casebooks			То	Findings by Severity		
Q	NAME	Ç FINDINGS	OATE AND TIME		ieverity 🗘 mesi	SAGE CATEGORY	¢ count
-	Adam Test		2022-09-20T15:01:0	11.630Z	Alert		17831
м			2022-09-21T17-33:0	15.927Z	Alert 202	2-09-19 Type: PCR; Score of \-0.0	
ŵ			2022-09-20T14:46:4	2.043Z	Alert 202		
	Hari2		2022-09-21T16:42:4	9.0872	Alert 202	2-09-19 Type: PCR; Score of '-0.0	
			2022-09-20T14:57:	9.403Z	Alert 202		
				8of8 < >			1 ~ 10 of 5461
	Assets by Risk		Assets by Three	t		Community Feed	
	NAME	≎ RISK SCORE	C NAME	C THRE	NT SCORE C		
	cms-proxy04p.mt.local	38100333		8904	36	82.102.16.45	
		23009248		3312		Ilh23.com	
		22958681		in.deliveryagent.com 2424		nvoaeicweston.com	
	cms-proxy06p.mt.local	22958628		36 2339		slalomdrivevrsto.today	
	cms-proxy03p.mt.local	22957814		14 2061		r52yoo.top	
		22942384		99 1936		jib81hdvernon.com	
		14879341		1477		okinawajame0.today	+
							?:

Select a finding that you want to add to a casebook or create a new case book by clicking "Add to existing" OR "Add to new."

	•	A Findings Explorer	× A Findings Ex	plorer × +									~
$\leftarrow \ \rightarrow $	C	a dev.ux-dev.threatey	ye.io/findings								or 🖞 🟠	* 🗆	1
🛃 Map	M	Gmail A LiveWire confliu	ien										
o»		Sep 15, 2022 14:26 → Sep	22, 2022 14:26 🛛 🗸			Search					୍ର egraha	m@liveactic	on.com 🗸
ώ	Fina	lings Over Time											
	Fine	lings											
•		Add to Casebook ^ 1	Tags 🗸										
٢			TYPE	MESSAGE Ó	HOSTNAME O	SOURCE ADDRESS	DEST ADDRESS	CATEGORY	DOMAIN	C FLOW COUNT	C TAOS		
0		Add to existing casebook											
~		2022-09-15T14:33:01.0		threat indicator	141.98.10.90	141.98.10.90	216.197.73.65	Command and Control	none				
		2022-09-15T14:32:48.0	loc	threat indicator	141.98.11.54	141.98.11.54	216.197.73.76	Command and Control	none				
~		2022-09-15T14:32:45.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.163	Command and Control	none				
रङा		2022-09-15T14:32:08.0	ioc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.82	Command and Control	none				
		2022-09-15T14:31:52.0_		threat indicator	92.63.197.131	92.63.197.131	216.197.73.172	Command and Control	dag.musictoday.com				
		2022-09-15T14:30:48.0	ioc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.163	Command and Control	none				
		2022-09-15T14:27:44.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.185	Command and Control	none				
		2022-09-15T14:27:26.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.227	Command and Control	none				
		2022-09-15T14:27:10.0	loc	threat indicator	179.43.156.143	179.43.156.143	216.197.73.43	Command and Control	none				
		2022-09-15T14:26:34.0		threat indicator	92.63.197.131	92.63.197.131	216.197.73.134	Command and Control	none				
											1 - 10 of 5000		
					The table is limited to s	how 5000 of 392024 total res	sults. Use column filtering to se	e more targeted results.					

If you select "Add to existing" select the casebook you want to add the finding to. A green confirmation box will let you know the finding has been added.

6 1 8 Ma	D No	a dex.	co-direction	eerseye lo	effend inga 71	IndingsSee	ch-maxe	94%3D1202	1-00-19%	807) pa: %339	PCR-9	205core%20o	r76201	127-0.00017171	757388	H54625427 X 23	greater?	20than N30 then	mhold%3	0%27-inf%27.%	30PCS.	. C # 1	A []	* 1
o»	8-	Ny 11, 22		54723	309 H.M	0-	1060.gc 7	C22 69 19 Ty	IC POR 8	oe of 10.007		15758 No r								1 Endings ad	ided to th	n antonio lo cascionis		
슸	Profes	gi Oran Tin																		-				
	Finding																							
Ξ																								
宫		THEFT			1195		winner							CHIT MECHINA		GATTINGTY		-		Name and P		ne:		
D.																								
		2001-04	11125 03.20	1.0082	aroway		1800-08-1	n Types PCB, -				10108.121.13										Resources		
ц (*)	*																							
																				entrate 10	•	1-1611	۰.	>

If you select "Add to new case book," you are prompted to create a name, assign a security analyst, a priority level, and a status. in this example, we are using "Testing_EDG" as the name and giving it the status of "Assigned." This is typically the first status given in a workflow.

	A	Findings Explorer	× A Findings Ex	plorer × -	÷									~
$\leftarrow \rightarrow$	C	a dev.ux-dev.threater	ye.io/findings									아 ① ☆	* 🗆 🕯	1 E
🛃 Map	MG	mail 🙏 LiveWire confliu	uen											
o»	- -	Sep 15, 2022 14:26 → Sep	o 22, 2022 14:26 💿 ~	Ex.: saddr#192.168.1.4		Search				-		ନ egraham	Silveaction.co	om 🗸
ଜ	Finding													
-	Finding	4												
Ξ														
		TIMESTAMP	туре О	MESSAGE O	HOSTNAME	SOURCE ADDRESS	O DEST ADDRESS	C CATE	EGORY C	DOMAIN	C FLOW COUNT	O TAGS		
Q														
				threat indicator	141.98.1				nd and Control					
		2022-09-15T14:32:48.0		threat indicator	141.98.1	Add Casebook			nd and Control					
~		2022-09-15T14:32:45.0		threat indicator	92.63.19	A	• former #11		nd and Control					
562				threat indicator	92.63.15	Casebook Name	Please select user		nd and Control					
				threat indicator	92.63.19	4			nd and Control	dag.musictoday.com				
		2022-09-15T14:30:48.0		threat indicator	92.63.15	Please select priority V	Assigned		nd and Control					
				threat indicator	92.63.15	Description			nd and Control					
		2022-09-15T14:27:26.0		threat indicator	92.63.15	Description			nd and Control					
		2022-09-15T14:27:10.0		threat indicator	179.43.1				nd and Control					
		2022-09-15T14:26:34.0		threat indicator	92.63.19		Cancel	Add	nd and Control					
												1 - 10 of 5000		
						ble is limited to show 5000 of 392024 tota								
												?	1	

Now, in the casebook section my casebook example, "Testing_EDG" is here with the alert.

	• A Carebooks		K 🔥 Findings Dookown	x +						
÷	- C & dev.us-dev	threateyed	a/casebooks						en é é	
	Augo M Canal A Look	the postilization.								
o»	0 - Sep 15, 2022 145	ă → 9ep 22	822 H 26 0 - Go : and - H 20 H		Sec.				A egratum	gilvescion.com
ŵ			Redings By Time							
	Sorthy Sales V		Redegs							
			THEOREM OF THE	O MODINE O HORTHNEE	O WEARSANDAINS (o bian ecoletato o	senseer D course	C REPORT	0 KMR	
٢		1.	202249415T14-22 loc	threat indigence 141.00.10.00	0 141.86.10.80	216.107.20.65	Command and Con., name			
Q	+ tool ngrodg	1.0								
-	- testing	1.								
ы	- test M	-								
\$	- + Adam Text	1.								
	- Had	1.								
	- +Hef	· •								
	- + Chris Canabook	1.								
	-TetC	1.								