

LiveAction®

ThreatEye

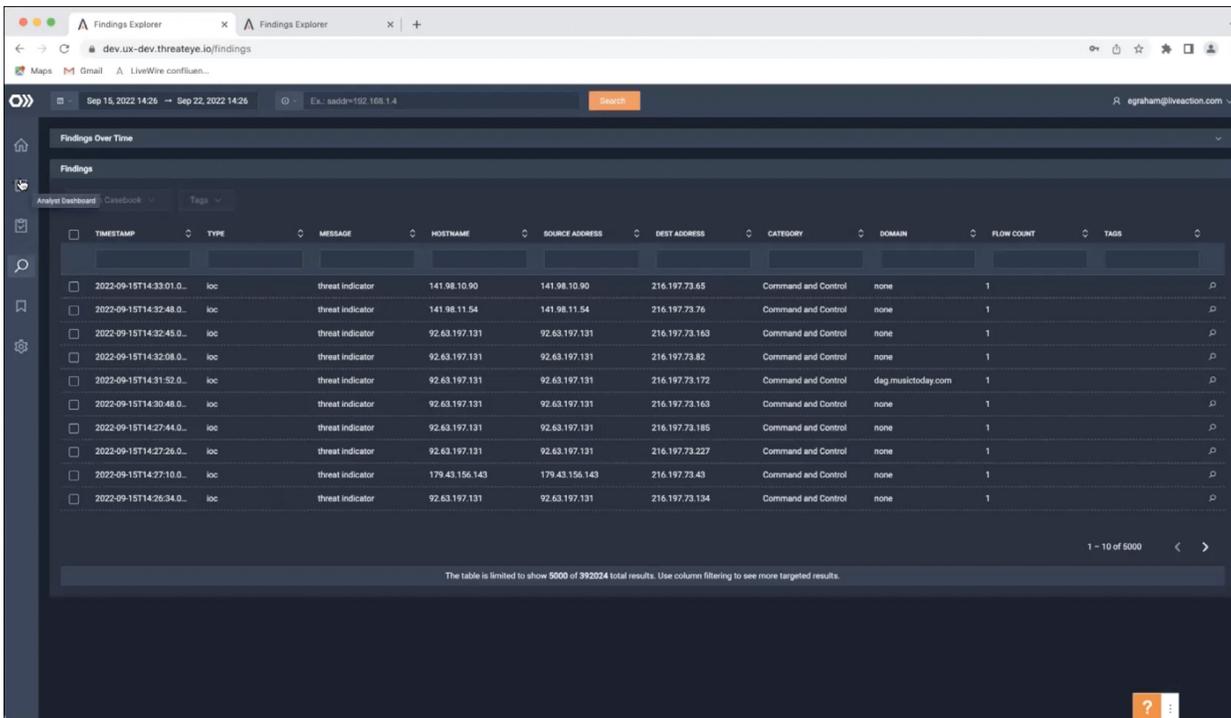
How-To Guide: Casebook

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?

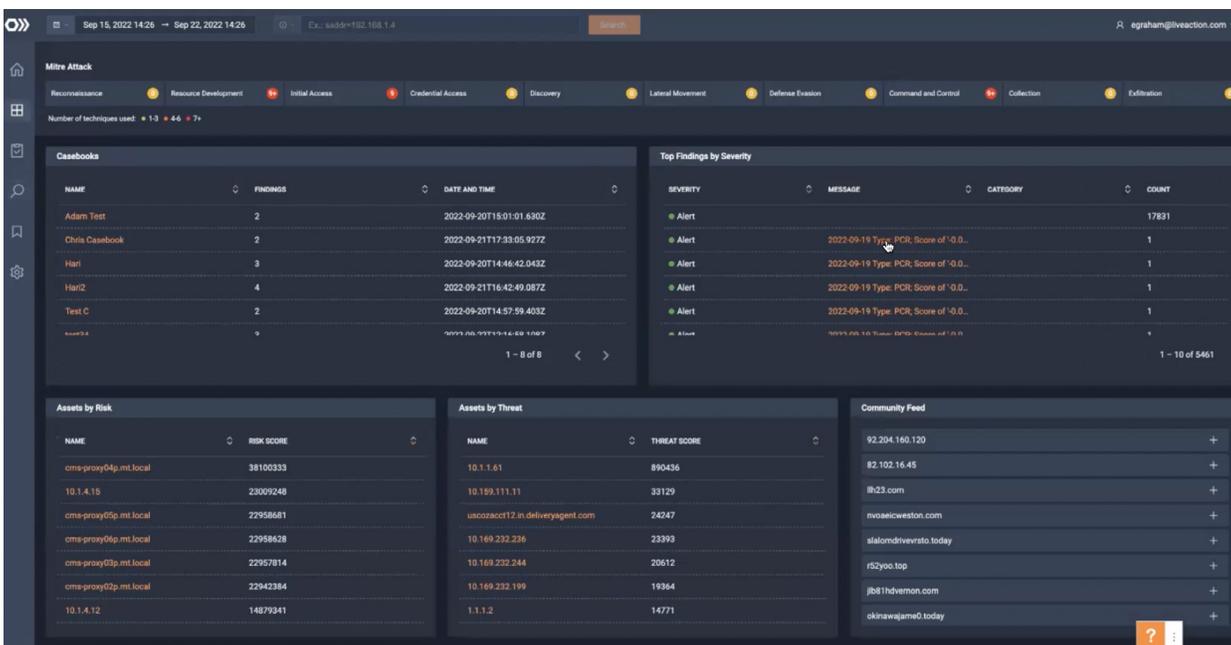
You can accomplish this through the findings area



The screenshot shows the 'Findings Explorer' interface. At the top, there's a search bar and a date range filter set to 'Sep 15, 2022 14:26' to 'Sep 22, 2022 14:26'. Below this is a 'Findings Over Time' section. The main area is a table with columns: TIMESTAMP, TYPE, MESSAGE, HOSTNAME, SOURCE ADDRESS, DEST ADDRESS, CATEGORY, DOMAIN, FLOW COUNT, and TAGS. The table contains several rows of threat indicators, all with a 'loc' type and 'Command and Control' category. A footer note states: 'The table is limited to show 5000 of 392024 total results. Use column filtering to see more targeted results.'

TIMESTAMP	TYPE	MESSAGE	HOSTNAME	SOURCE ADDRESS	DEST ADDRESS	CATEGORY	DOMAIN	FLOW COUNT	TAGS
2022-09-15T14:33:01.0...	loc	threat indicator	141.98.10.90	141.98.10.90	216.197.73.65	Command and Control	none	1	
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	1	
2022-09-15T14:32:45.0...	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.163	Command and Control	none	1	
2022-09-15T14:32:08.0...	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.82	Command and Control	none	1	
2022-09-15T14:31:52.0...	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.172	Command and Control	diag.musictoday.com	1	
2022-09-15T14:30:48.0...	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.163	Command and Control	none	1	
2022-09-15T14:27:44.0...	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.185	Command and Control	none	1	
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	1	
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	1	
2022-09-15T14:26:34.0...	loc	threat indicator	92.63.197.131	92.63.197.131	216.197.73.134	Command and Control	none	1	

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



The screenshot shows the 'Analyst Dashboard' with a 'Mitre Attack' overview. The top navigation bar includes 'Reconnaissance', 'Resource Development', 'Initial Access', 'Credential Access', 'Discovery', 'Lateral Movement', 'Defense Evasion', 'Command and Control', 'Collection', and 'Exfiltration'. Below this is a 'Casebooks' panel with a table of casebooks. To the right is a 'Top Findings by Severity' panel. At the bottom, there are three panels: 'Assets by Risk', 'Assets by Threat', and 'Community Feed'.

NAME	FINDINGS	DATE AND TIME
Adam Test	2	2022-09-20T18:01:01.430Z
Chris Casebook	2	2022-09-21T17:33:05.927Z
Hari	3	2022-09-20T14:46:42.043Z
Hari2	4	2022-09-21T16:42:49.087Z
Test C	2	2022-09-20T14:57:59.403Z
test4	1	2022-09-21T14:16:01.100Z

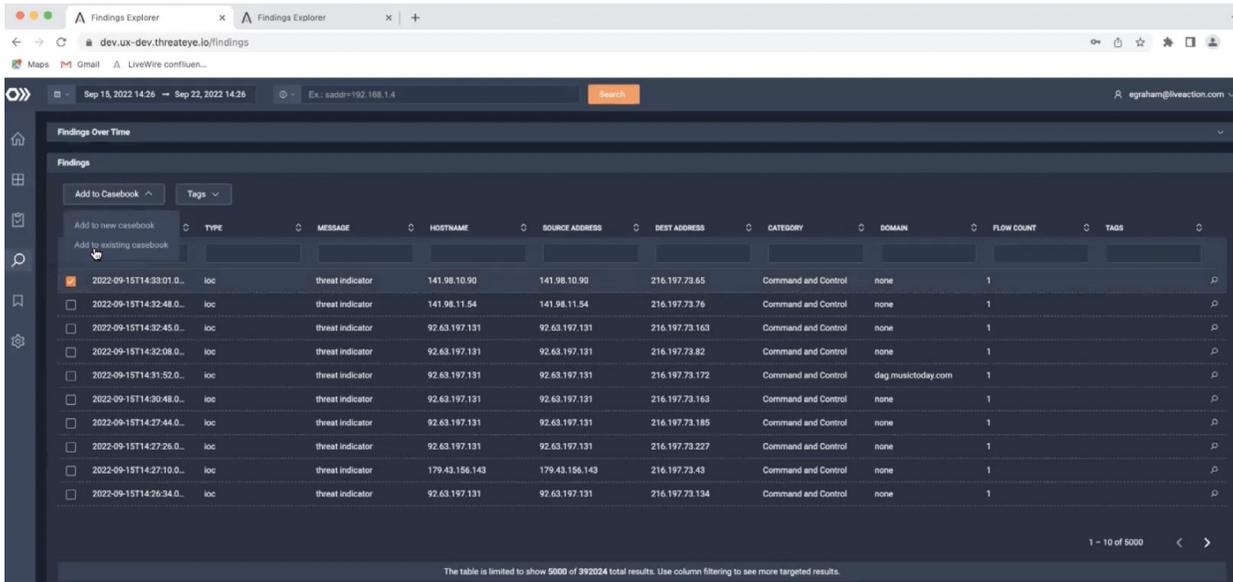
SEVERITY	MESSAGE	CATEGORY	COUNT
Alert			17831
Alert	2022-09-19 Type: PCR, Score of -0.0...		1
Alert	2022-09-19 Type: PCR, Score of -0.0...		1
Alert	2022-09-19 Type: PCR, Score of -0.0...		1
Alert	2022-09-19 Type: PCR, Score of -0.0...		1
Alert	2022-09-19 Type: PCR, Score of -0.0...		1

NAME	RISK SCORE
cms-proxy04p.mt.local	38100333
10.1.4.18	23009248
cms-proxy05p.mt.local	22958681
cms-proxy06p.mt.local	22958628
cms-proxy03p.mt.local	22957814
cms-proxy02p.mt.local	22942384
10.1.4.12	14879341

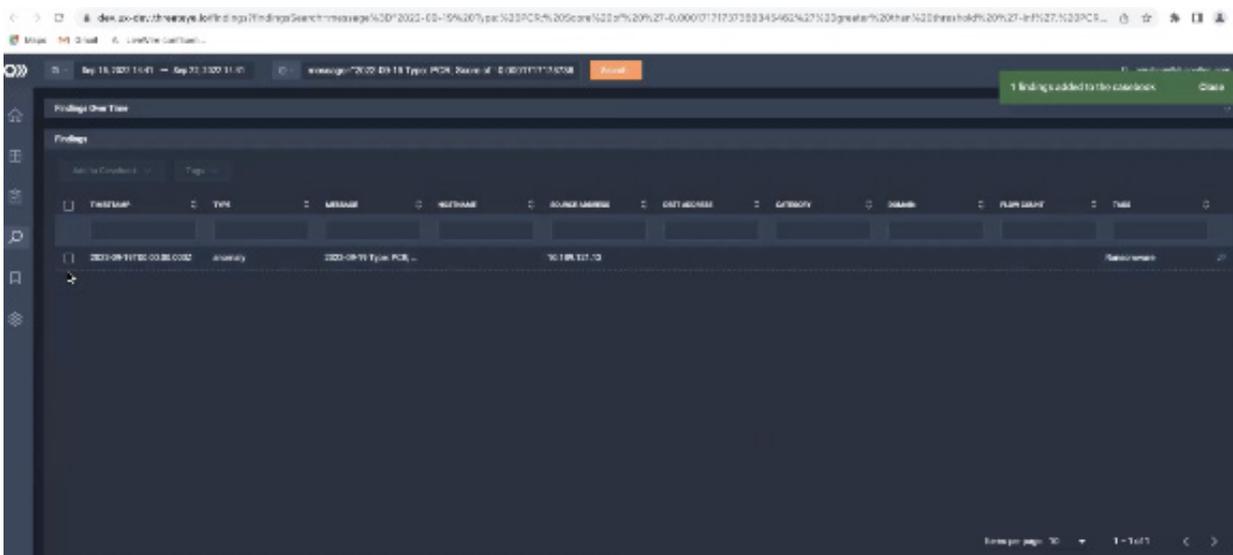
NAME	THREAT SCORE
10.1.1.61	890436
10.189.111.11	33129
uscozacct12.in.deliveryagent.com	24247
10.169.232.236	23393
10.169.232.244	20612
10.169.232.199	19364
1.1.1.2	14771

IP/Domain	Action
92.204.160.120	+
82.102.16.45	+
ib23.com	+
nvaseicweston.com	+
slalomdriveinfo.today	+
r5yoo.top	+
jb61hdvemon.com	+
oksnawajam0.today	+

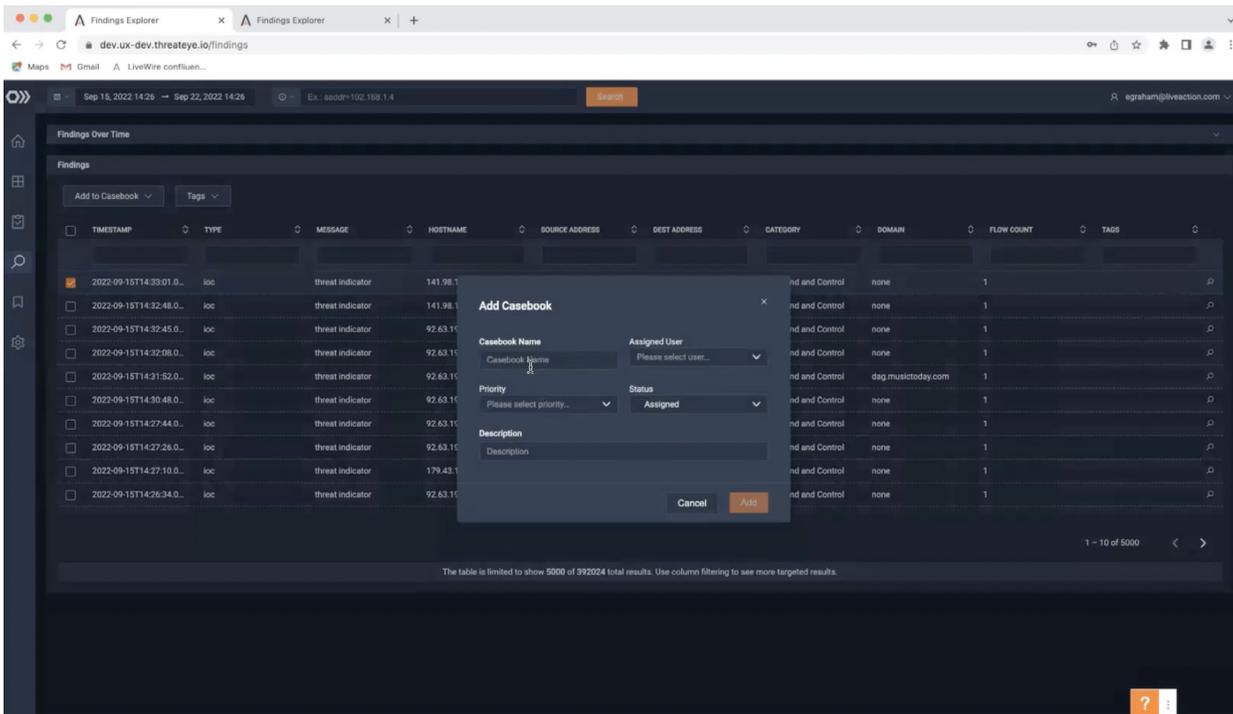
Select a finding that you want to add to a casebook or create a new case book by clicking "Add to existing" OR "Add to new."



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.



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.



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

