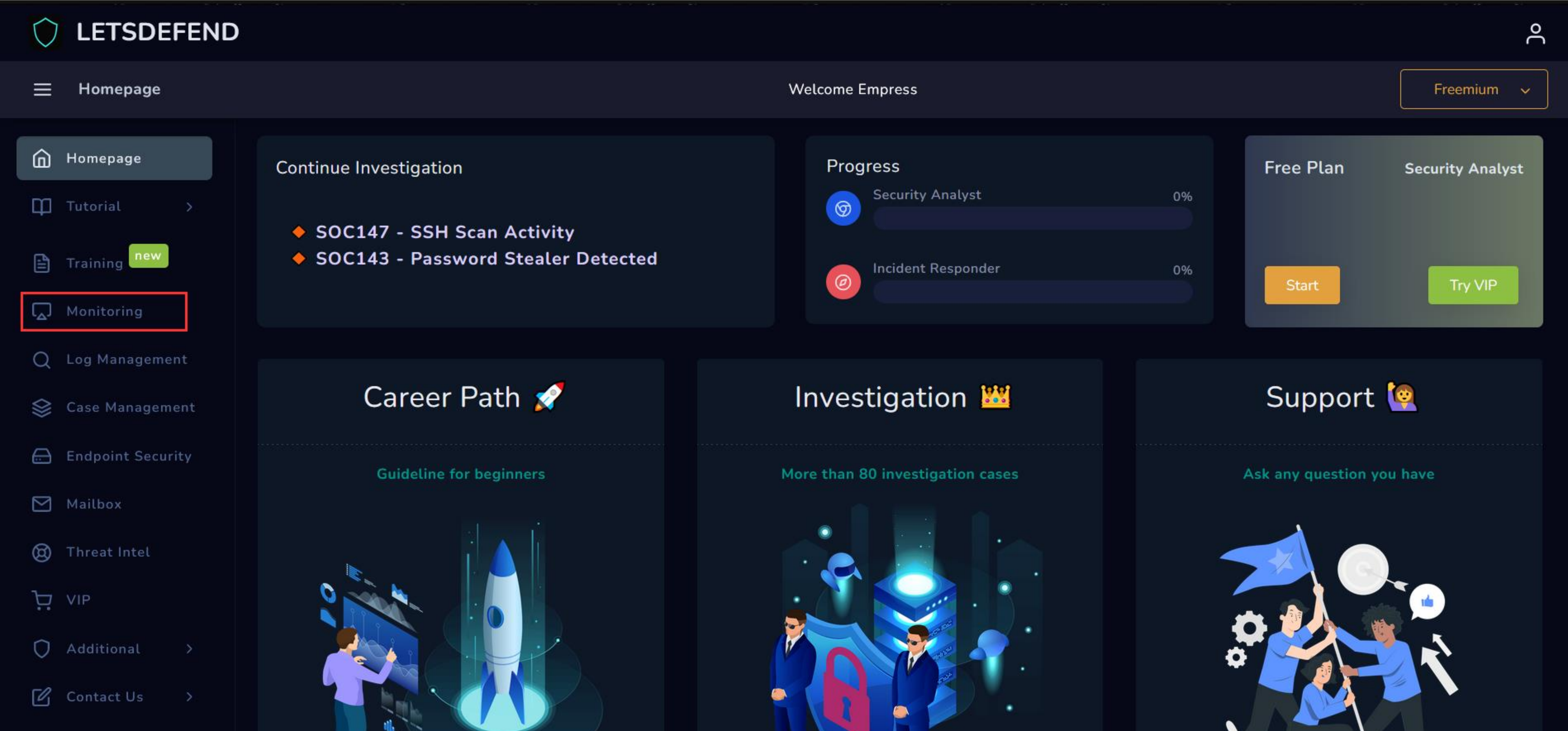
zumaroc

Day 2

ZROC102

Module 2: Monitoring

LETSDEFEND Platform



Welcome Empress

Continue Investigation

- SOC147 - SSH Scan Activity
- SOC143 - Password Stealer Detected

Progress

Security Analyst 0%

Incident Responder 0%

Free Plan Security Analyst

Career Path 🚀

Guideline for beginners

Investigation 👑

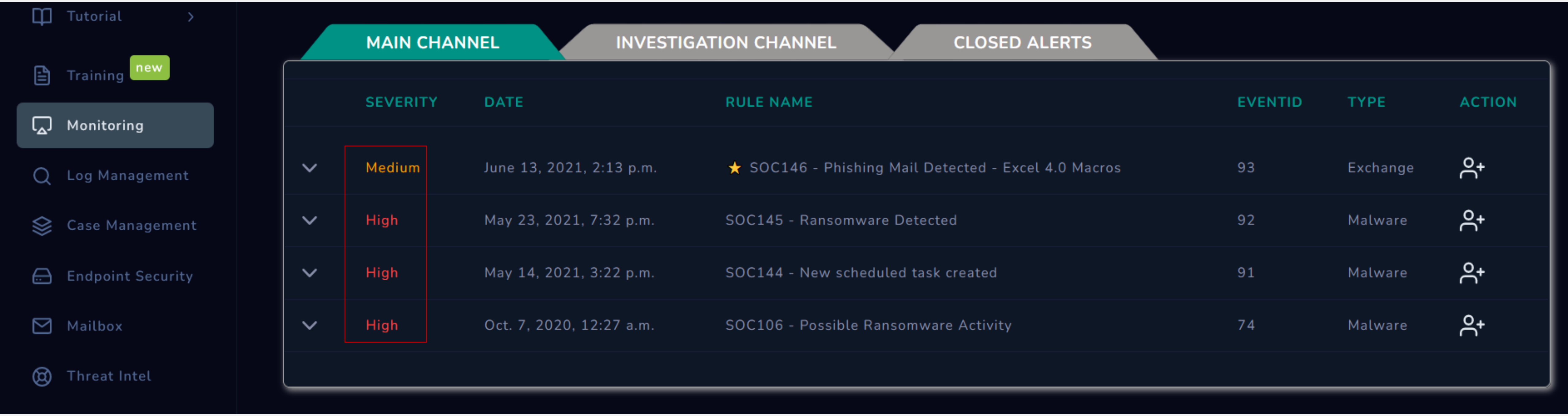
More than 80 investigation cases

Support 🙋

Ask any question you have

Monitoring

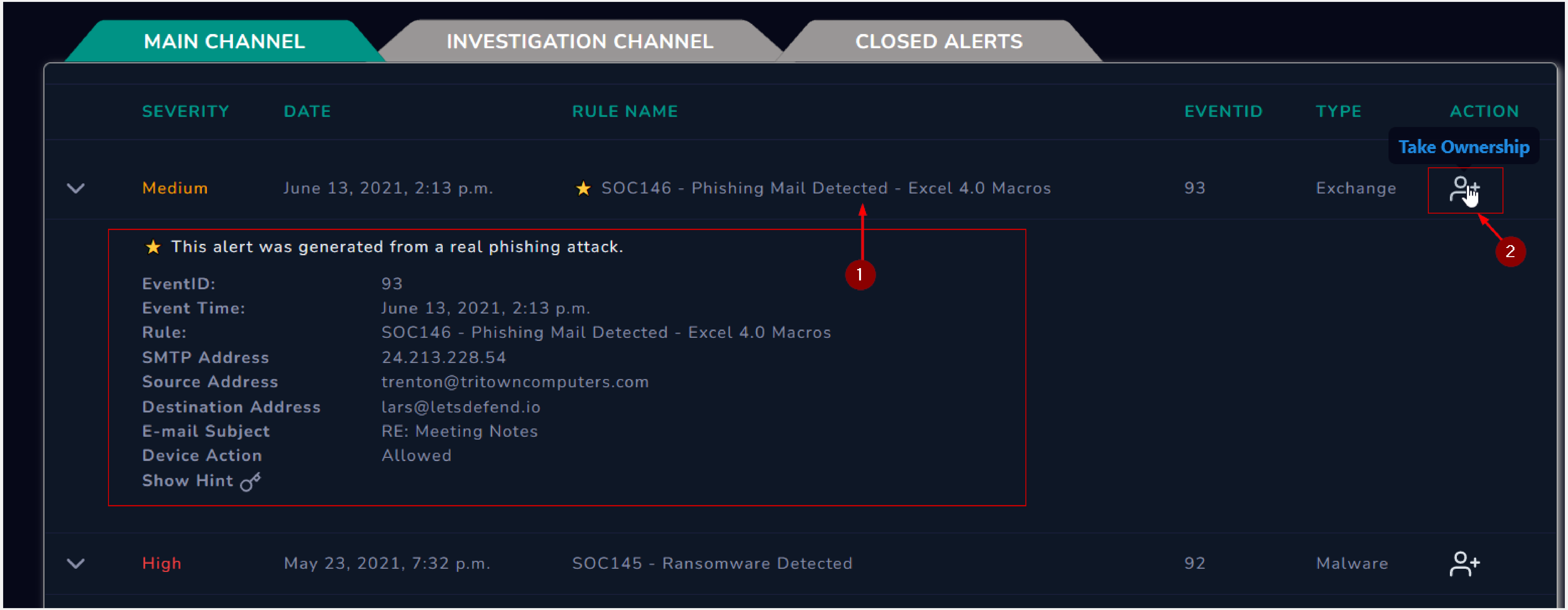
Alerts are sorted in High, Medium and Low depending on the order of priority. To begin, you must solve the High severity cases first, then Medium and lastly Low.



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	June 13, 2021, 2:13 p.m.	★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros	93	Exchange	
High	May 23, 2021, 7:32 p.m.	SOC145 - Ransomware Detected	92	Malware	
High	May 14, 2021, 3:22 p.m.	SOC144 - New scheduled task created	91	Malware	
High	Oct. 7, 2020, 12:27 a.m.	SOC106 - Possible Ransomware Activity	74	Malware	

Monitoring: Main Channel

Based on the numbering, the first one requires you to click the “v” arrow key/row tab to view “Alert details” and the second requires you to “Take ownership” once clicked.



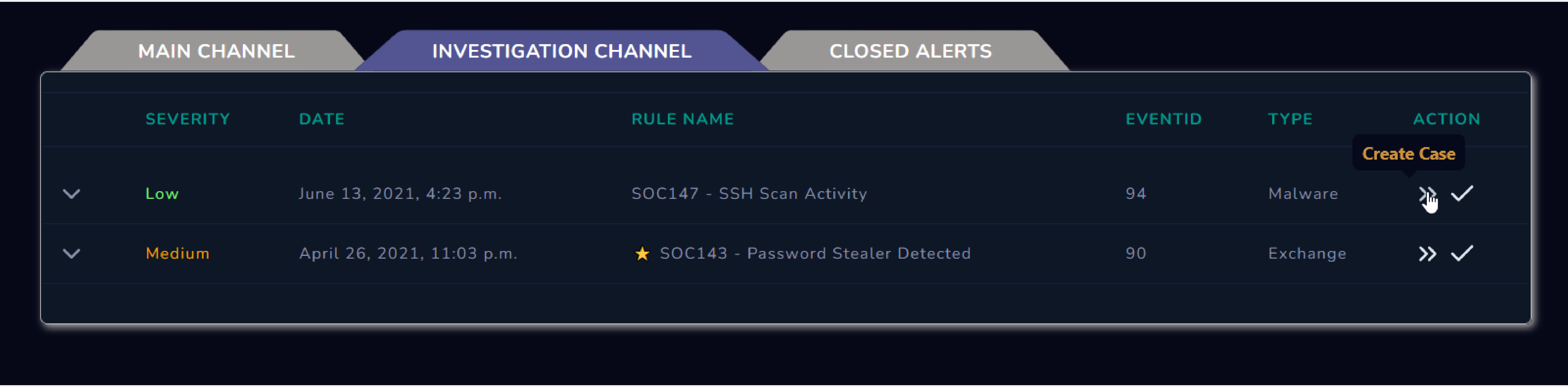
SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	June 13, 2021, 2:13 p.m.	★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros	93	Exchange	
High	May 23, 2021, 7:32 p.m.	SOC145 - Ransomware Detected	92	Malware	

★ This alert was generated from a real phishing attack.

EventID:	93
Event Time:	June 13, 2021, 2:13 p.m.
Rule:	SOC146 - Phishing Mail Detected - Excel 4.0 Macros
SMTP Address	24.213.228.54
Source Address	trenton@tritowncomputers.com
Destination Address	lars@letsdefend.io
E-mail Subject	RE: Meeting Notes
Device Action	Allowed
Show Hint	

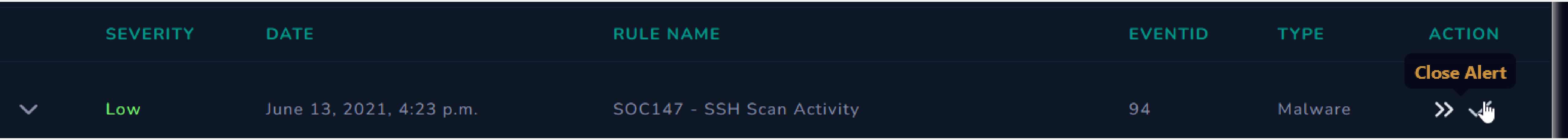
Monitoring: Investigation Channel

You can "Create Case" based on your analysis/investigation of the alert. I.e. If you find the alert suspicious.



	SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
⌄	Low	June 13, 2021, 4:23 p.m.	SOC147 - SSH Scan Activity	94	Malware	» ✓
⌄	Medium	April 26, 2021, 11:03 p.m.	★ SOC143 - Password Stealer Detected	90	Exchange	» ✓

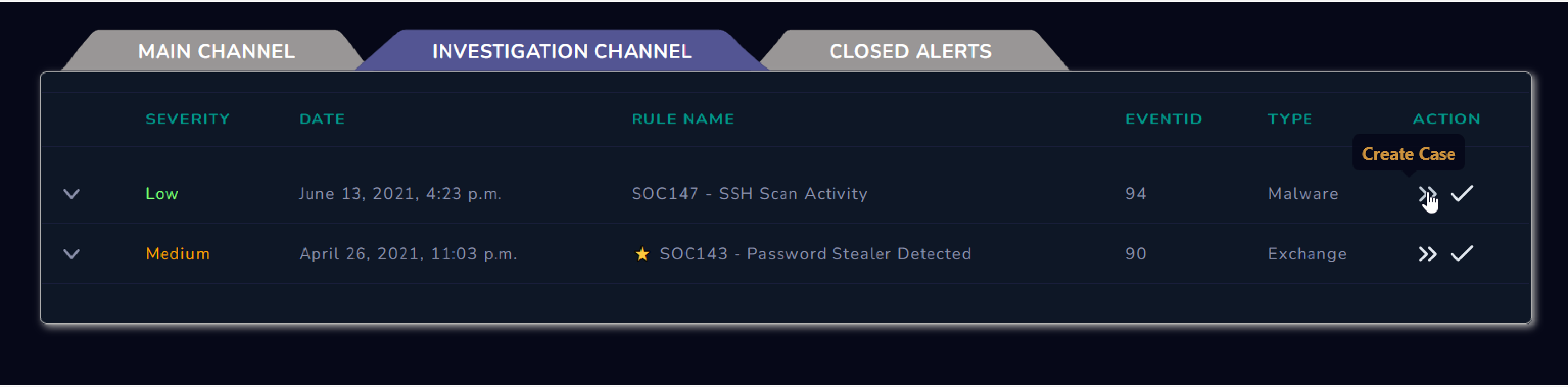
You can also "Close Alert" based on your analysis/investigation of the alert. I.e. If you find the alert not suspicious.



	SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
⌄	Low	June 13, 2021, 4:23 p.m.	SOC147 - SSH Scan Activity	94	Malware	» ✓

Monitoring: Investigation Channel

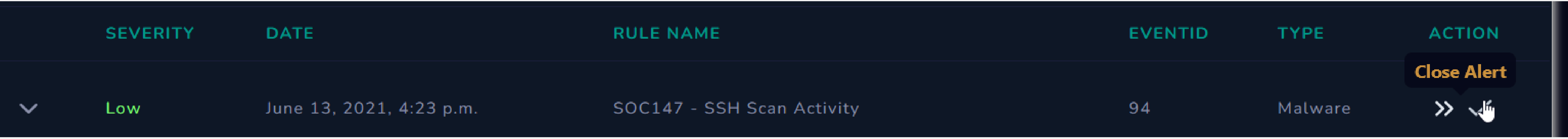
You can "Create Case" based on your analysis/investigation of the alert. I.e. If you find the alert suspicious. The cases created are allocated to the "Case Management" section.



	SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
⌄	Low	June 13, 2021, 4:23 p.m.	SOC147 - SSH Scan Activity	94	Malware	» ✓
⌄	Medium	April 26, 2021, 11:03 p.m.	★ SOC143 - Password Stealer Detected	90	Exchange	» ✓

Create Case

You can also "Close Alert" based on your analysis/investigation of the alert. I.e. If you find the alert not suspicious.

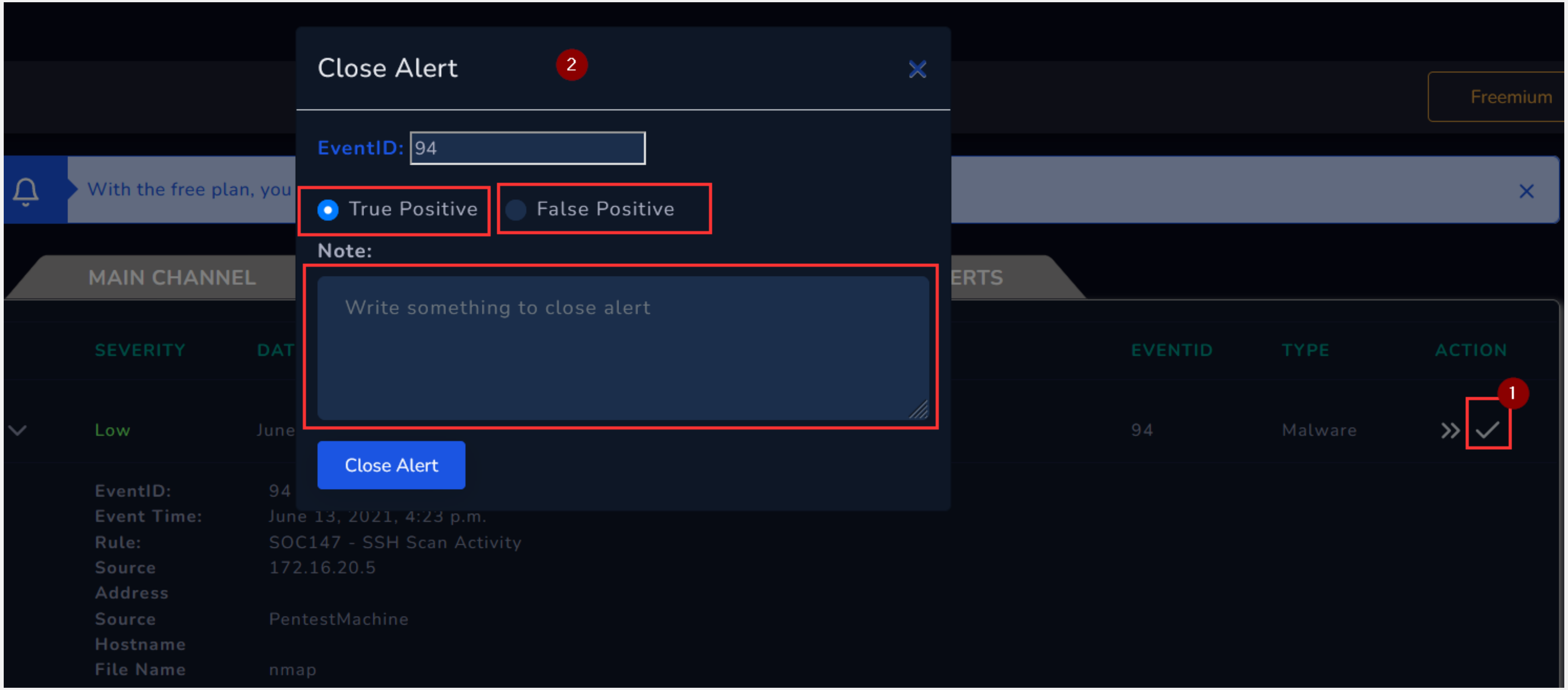


	SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
⌄	Low	June 13, 2021, 4:23 p.m.	SOC147 - SSH Scan Activity	94	Malware	» ✓

Close Alert

Monitoring: Investigation Channel

While trying to close an alert, It can be either “True Positive” or “False Positive”; one must be selected and a Note on why must be provided.



Close Alert

EventID: 94

● True Positive ○ False Positive

Note:

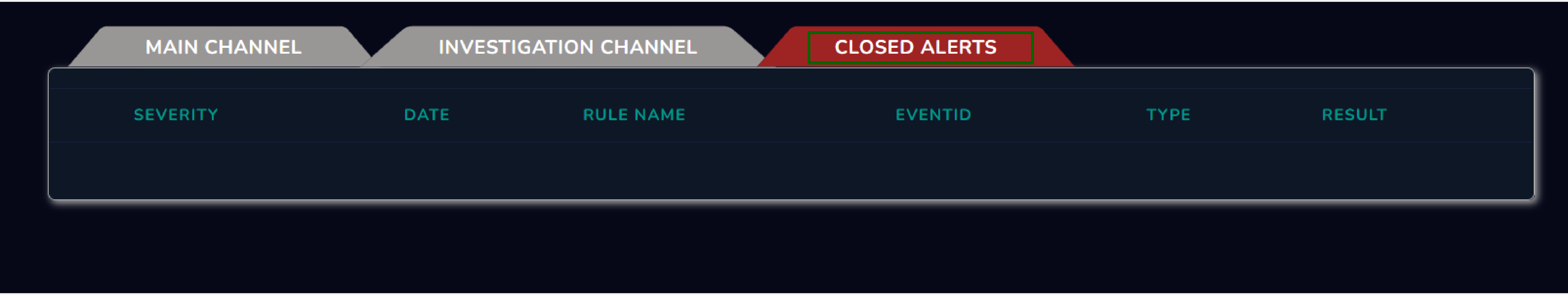
Write something to close alert

Close Alert

EventID: 94
Event Time: June 13, 2021, 4:23 p.m.
Rule: SOC147 - SSH Scan Activity
Source Address: 172.16.20.5
Source Hostname: PentestMachine
File Name: nmap

Monitoring: Closed Alerts

You can “Create Case” based on your analysis/investigation of the alert. I.e. If you find the alert suspicious. suspicious.



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	RESULT

Source

- https://app.letsdefend.io/esm/monitoring/