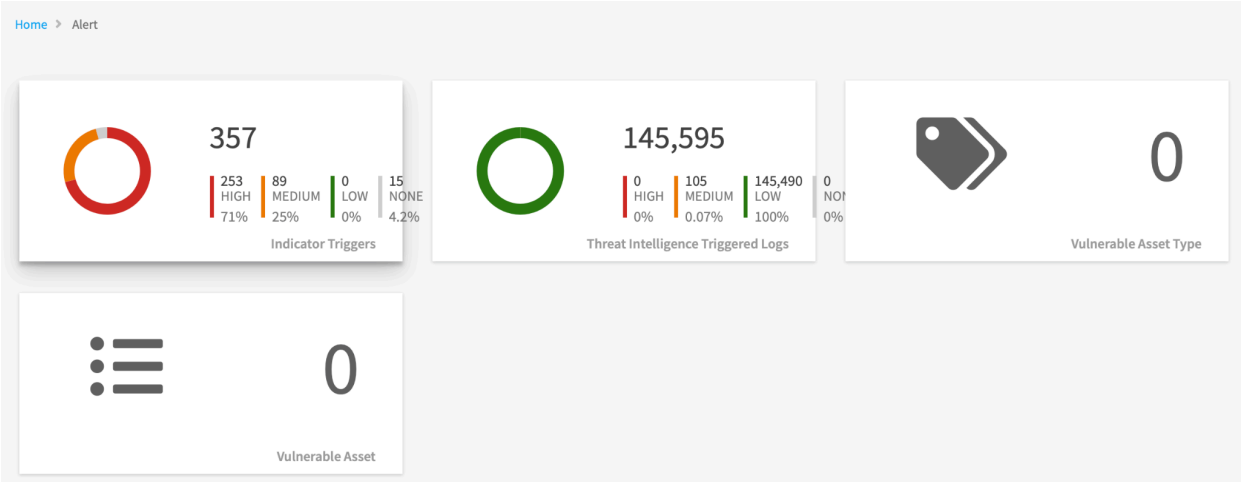
1. What do the numbers on your “Alert” Page indicate? What can you do to reduce the numbers?



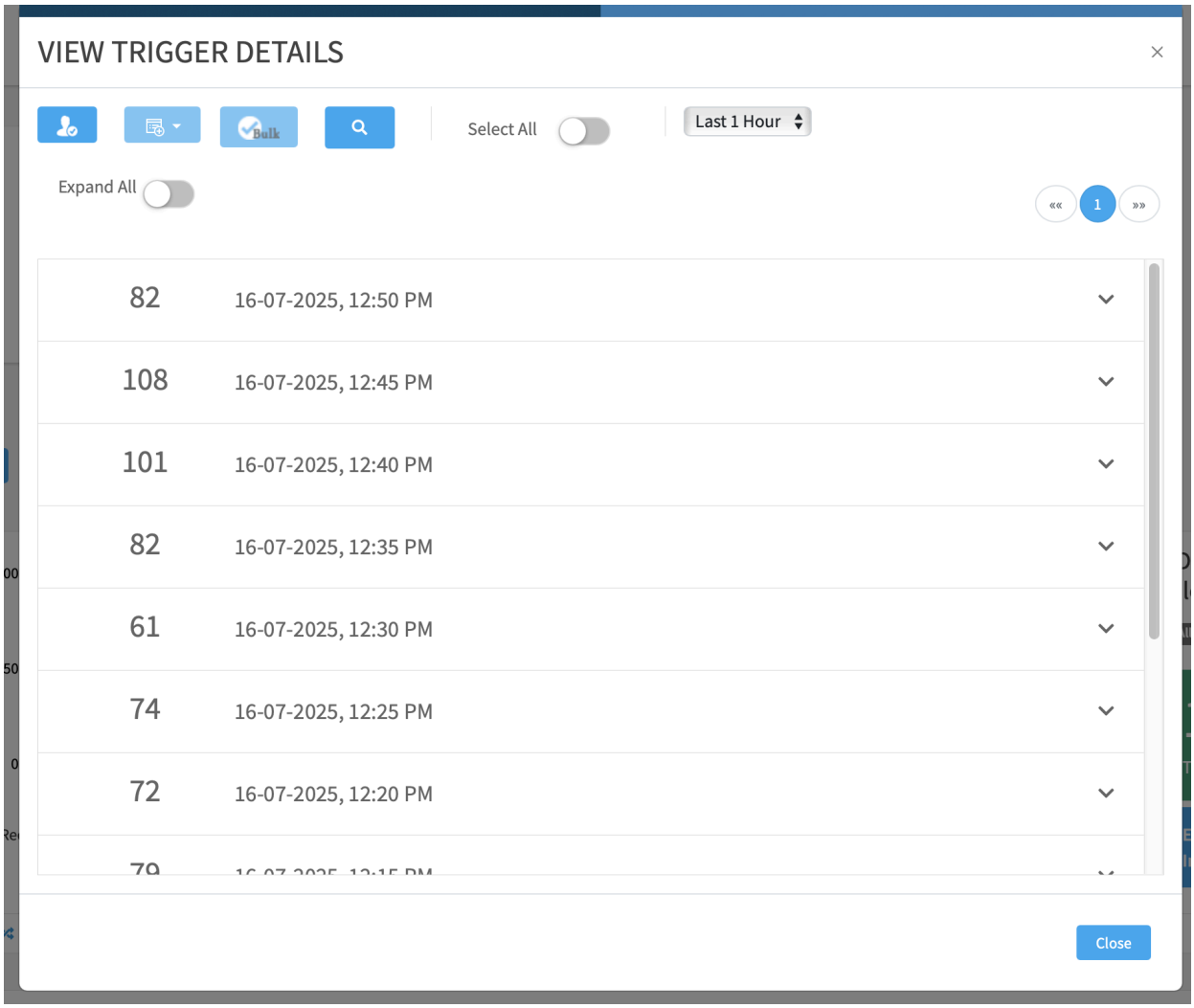
The numbers onthe “Alert” page in MSSGARD indicate the **number of triggered alertss** generated by detection mechanisms such as intrusion detection systems (IDS), behavioral analytics, or SIEM correlation rules. These numbers may be further broken down by:

- **Severity** (High, Medium, Low) and %
- **Time range or time stamp**
- **Source (host/IP) or user**
- **Rule name or trigger**

Below is a PDF Record of the logs

Title	Triggers	Last Seen	Severity	Correlate	Organization	Branch
User Login Activity Monitoring	14	16-07-2025, 11:44:22 AM	High	Yes	Apply to all organization	Apply to all branch
DNS Reconnaissance	24	16-07-2025, 11:43:22 AM	High	Yes	Apply to all organization	Apply to all branch
Malware Host Discovery via ICMP	24	16-07-2025, 11:43:22 AM	Medium	Yes	Apply to all organization	Apply to all branch
Port Scanning	24	16-07-2025, 11:43:22 AM	High	Yes	Apply to all organization	Apply to all branch
SMB Events Monitoring	25	16-07-2025, 11:43:22 AM	High	Yes	Apply to all organization	Apply to all branch
Unauthorized MSSQL Connection	25	16-07-2025, 11:43:22 AM	High	Yes	Apply to all organization	Apply to all branch
Unauthorized Ports, Protocols and Services	25	16-07-2025, 11:43:22 AM	Medium	Yes	Apply to all organization	Apply to all branch
Mass SNMP Scanning	68	16-07-2025, 11:42:22 AM	High	Yes	Apply to all organization	Apply to all branch
Suspected Backdoor Access	19	16-07-2025, 11:42:22 AM	Medium	Yes	Apply to all organization	Apply to all branch
IP Spoofing Attack	22	16-07-2025, 11:39:22 AM	High	Yes	Apply to all organization	Apply to all branch
Boundary Defense - Firewall	4	16-07-2025, 11:18:22 AM	Medium	Yes	Apply to all organization	Apply to all branch
RDP Connection Detection	44	16-07-2025, 10:47:22 AM	High	Yes	Apply to all organization	Apply to all branch
Excessive SMB traffic	2	16-07-2025, 10:01:22 AM	High	Yes	Apply to all organization	Apply to all branch

Title	Triggers	Last Seen	Severity	Correlate	Organization	Branch
Malicious SMB Traffic	12	16-07-2025, 08:12:22 AM	Medium	Yes	Apply to all organization	Apply to all branch
Injection	3	16-07-2025, 07:08:22 AM	High	Yes	Apply to all organization	Apply to all branch
Using Components with Known Vulnerabilities	15	16-07-2025, 07:08:22 AM	None	Yes	Apply to all organization	Apply to all branch
Directory Traversal Attack	2	16-07-2025, 06:41:22 AM	High	Yes	Apply to all organization	Apply to all branch
Broken Access Control	5	15-07-2025, 08:10:22 PM	Medium	Yes	Apply to all organization	Apply to all branch


VIEW TRIGGER DETAILS
Select All
Last 1 Hour
Expand All
«
1
»
82
16-07-2025, 12:50 PM
108
16-07-2025, 12:45 PM
101
16-07-2025, 12:40 PM
82
16-07-2025, 12:35 PM
61
16-07-2025, 12:30 PM
74
16-07-2025, 12:25 PM
72
16-07-2025, 12:20 PM
Close

EVENT ANALYSIS

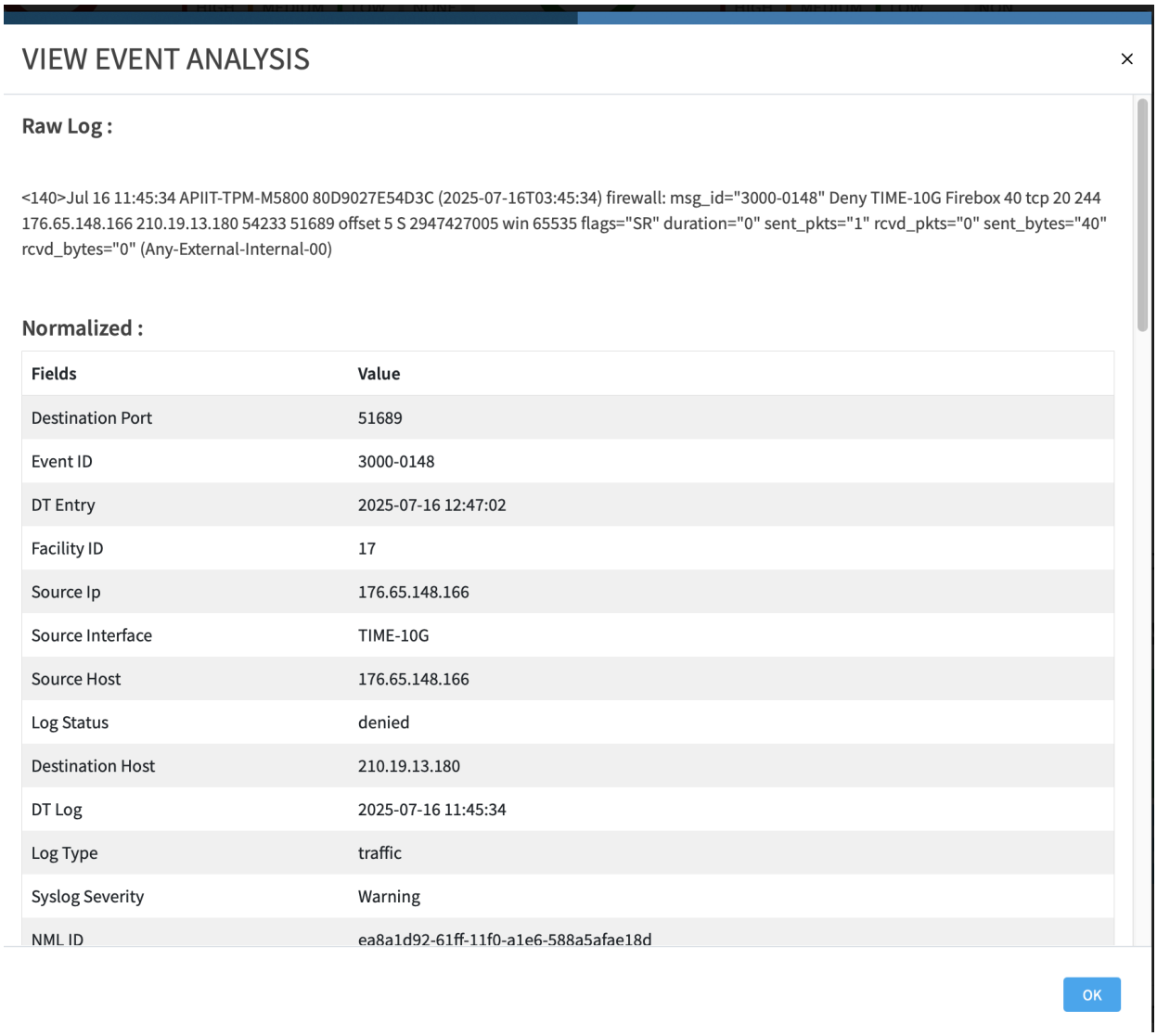
Normalized View | Raw View

Total Events: 82

« 1 2 3 4 5 »

*Processed Time	*Organization	Source Ip	Destination Ip	Attack Type	Attack Name	Malware Name	Event Severity
2025-07-16 12:50:00	APU	176.65.148.166	210.19.13.180	-	-	-	-
2025-07-16 12:49:58	APU	198.235.24.98	210.19.13.169	-	-	-	-
2025-07-16 12:49:55	APU	64.62.156.58	219.93.16.135	-	-	-	-
2025-07-16 12:49:52	APU	176.65.148.207	210.19.13.181	-	-	-	-
2025-07-16 12:49:51	APU	198.55.98.165	219.93.16.132	-	-	-	-
2025-07-16 12:49:51	APU	176.65.148.173	219.93.16.141	-	-	-	-
2025-07-16 12:49:51	APU	198.235.24.198	210.19.13.170	-	-	-	-
2025-07-16 12:49:43	APU	147.185.132.16	210.19.13.186	-	-	-	-
2025-07-16 12:49:43	APU	176.65.148.215	210.19.13.175	-	-	-	-
2025-07-16 12:49:42	APU	205.210.31.254	219.93.16.132	-	-	-	-
2025-07-16 12:49:40	APU	193.163.125.233	210.19.13.186	-	-	-	-
2025-07-16 12:49:36	APU	176.65.148.208	219.93.16.142	-	-	-	-
2025-07-16 12:49:35	APU	147.185.132.42	210.19.13.180	-	-	-	-
2025-07-16 12:49:17	APU	195.184.76.38	219.93.16.131	-	-	-	-

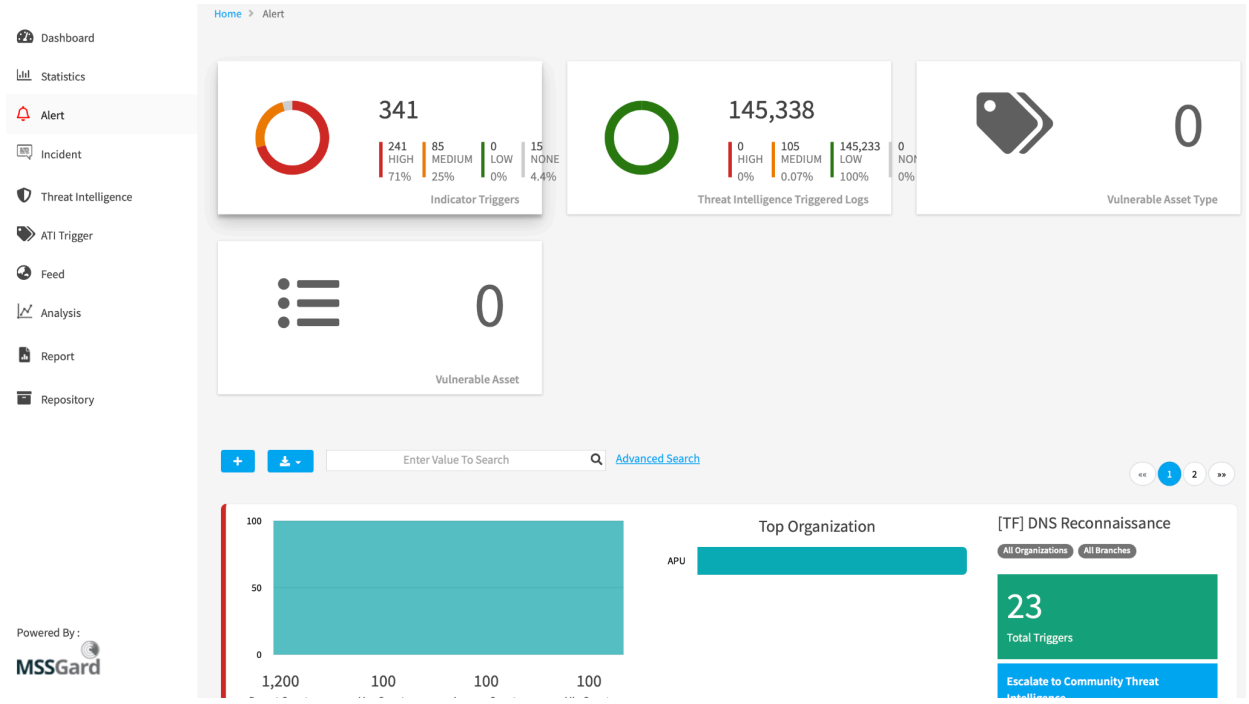
Close

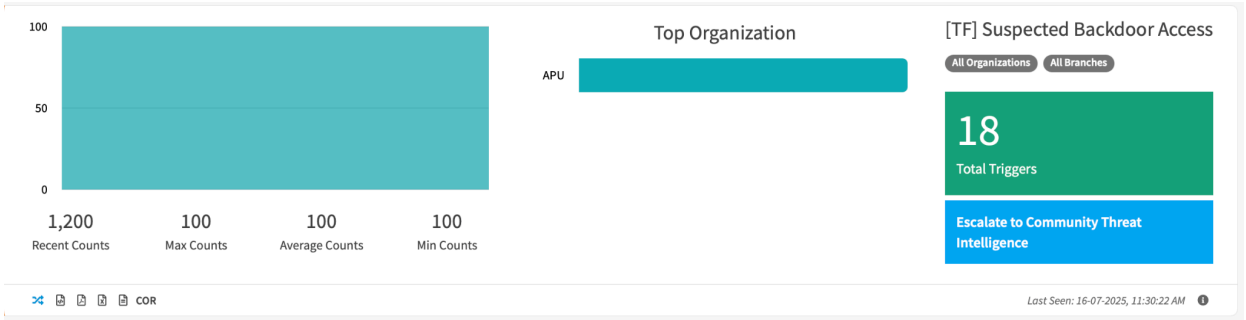


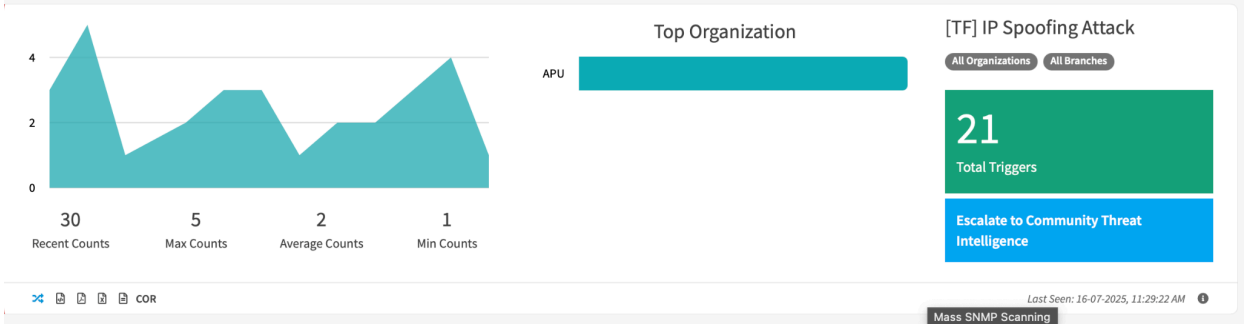
How to reduce spammy alerts in SIEM

- some rules might be too sensitive, so maybe adjust detection thresholds
- whitelist safe tools (like vuln scanners) so they don't trigger alerts every time
- better grouping of assets can help – not everything should be treated as high risk
- keep systems updated or else old vulnerabilities will keep popping up
- threat intel feeds can help filter out useless alerts and focus on actual threats
- also maybe reduce duplicates... no point getting same alert 5 times

2. Escalate an alert into an incident




100
50
0
1,200
Recent Counts
100
Max Counts
100
Average Counts
100
Min Counts
Top Organization
APU
[TF] Suspected Backdoor Access
All Organizations
All Branches
18
Total Triggers
Escalate to Community Threat Intelligence
COR
Last Seen: 16-07-2025, 11:30:22 AM


4
2
0
30
Recent Counts
5
Max Counts
2
Average Counts
1
Min Counts
Top Organization
APU
[TF] IP Spoofing Attack
All Organizations
All Branches
21
Total Triggers
Escalate to Community Threat Intelligence
COR
Last Seen: 16-07-2025, 11:29:22 AM
Mass SNMP Scanning

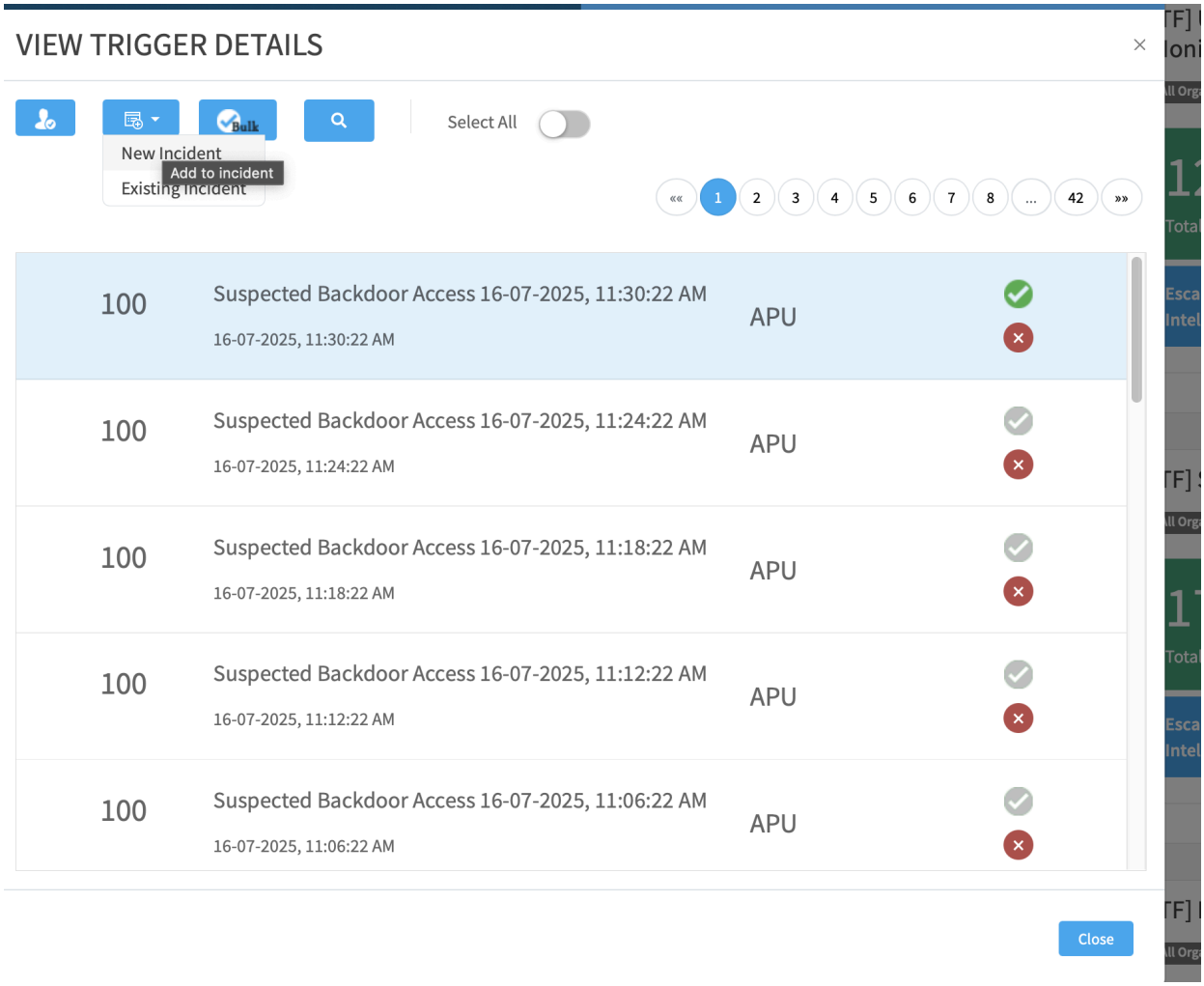
VIEW TRIGGER DETAILS

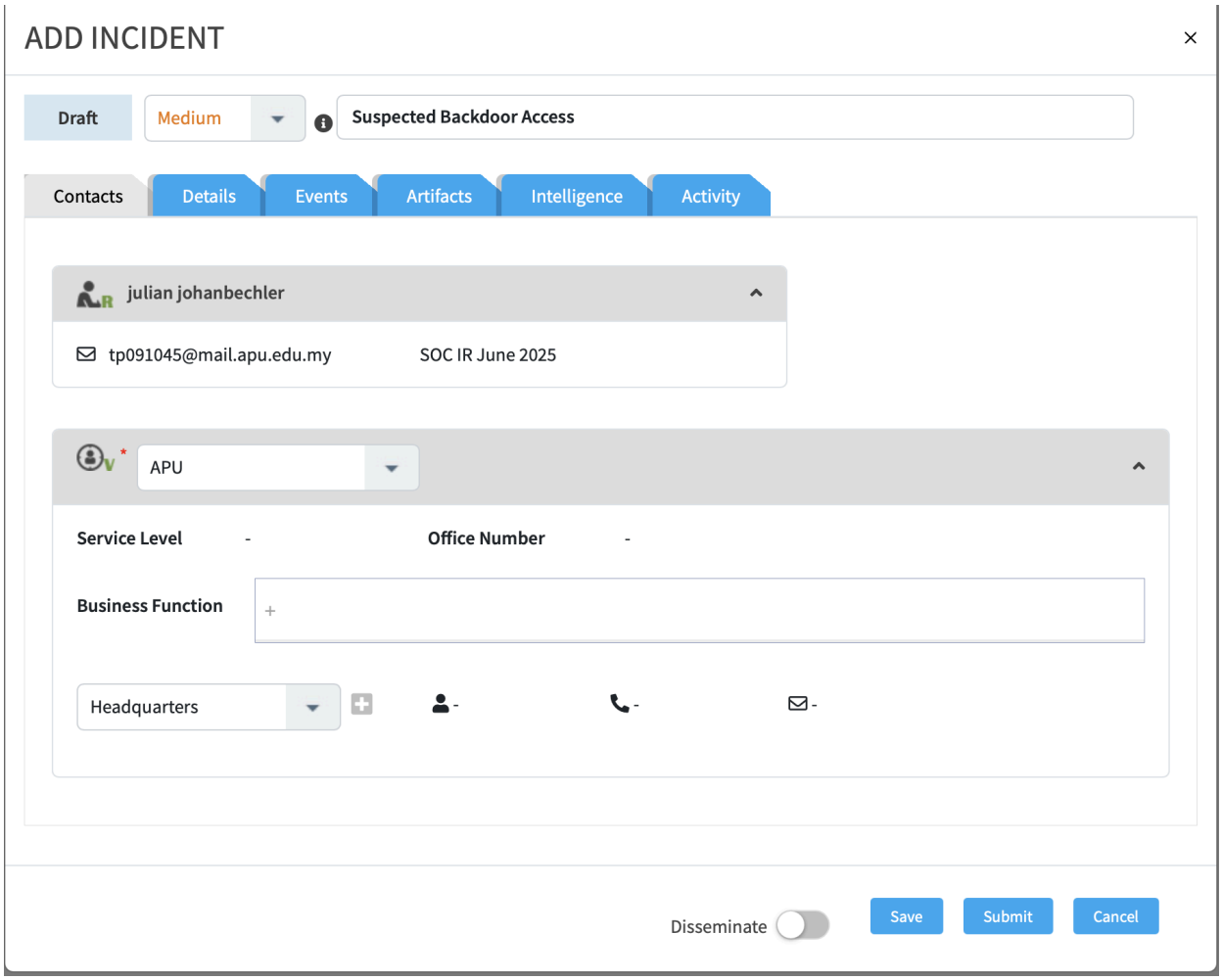
Select All

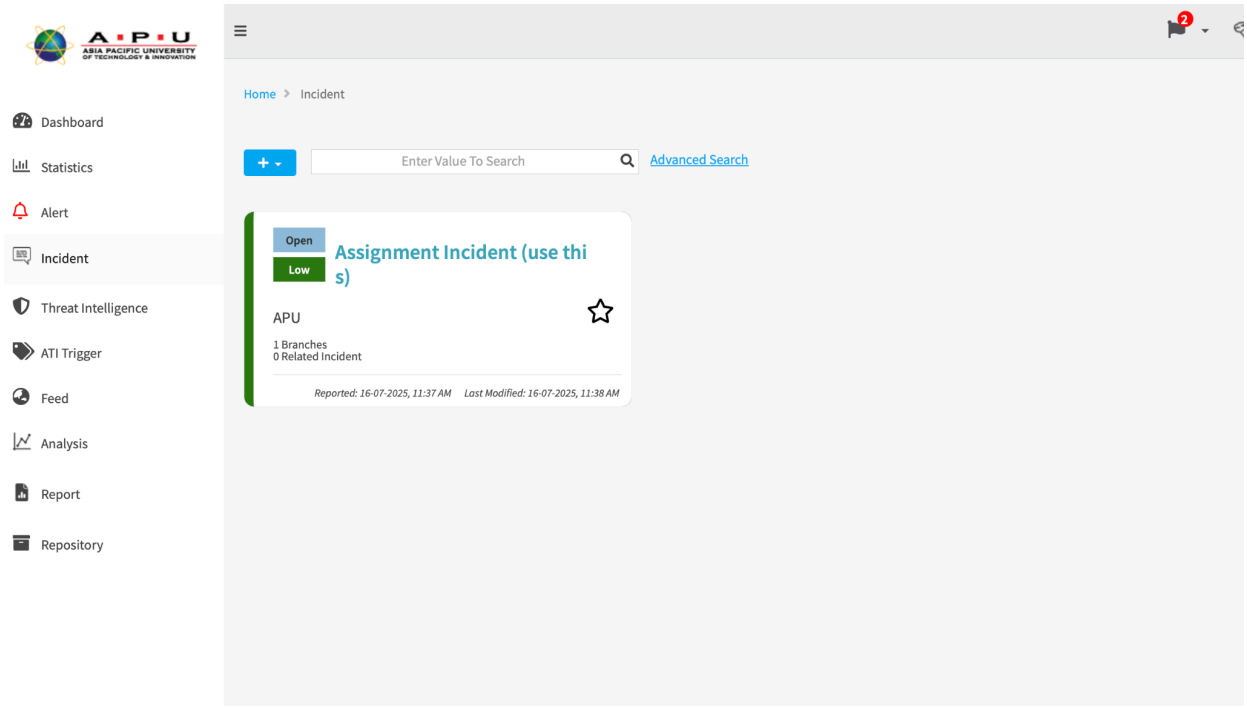
«« 1 2 3 4 5 6 7 8 ... 42 »»

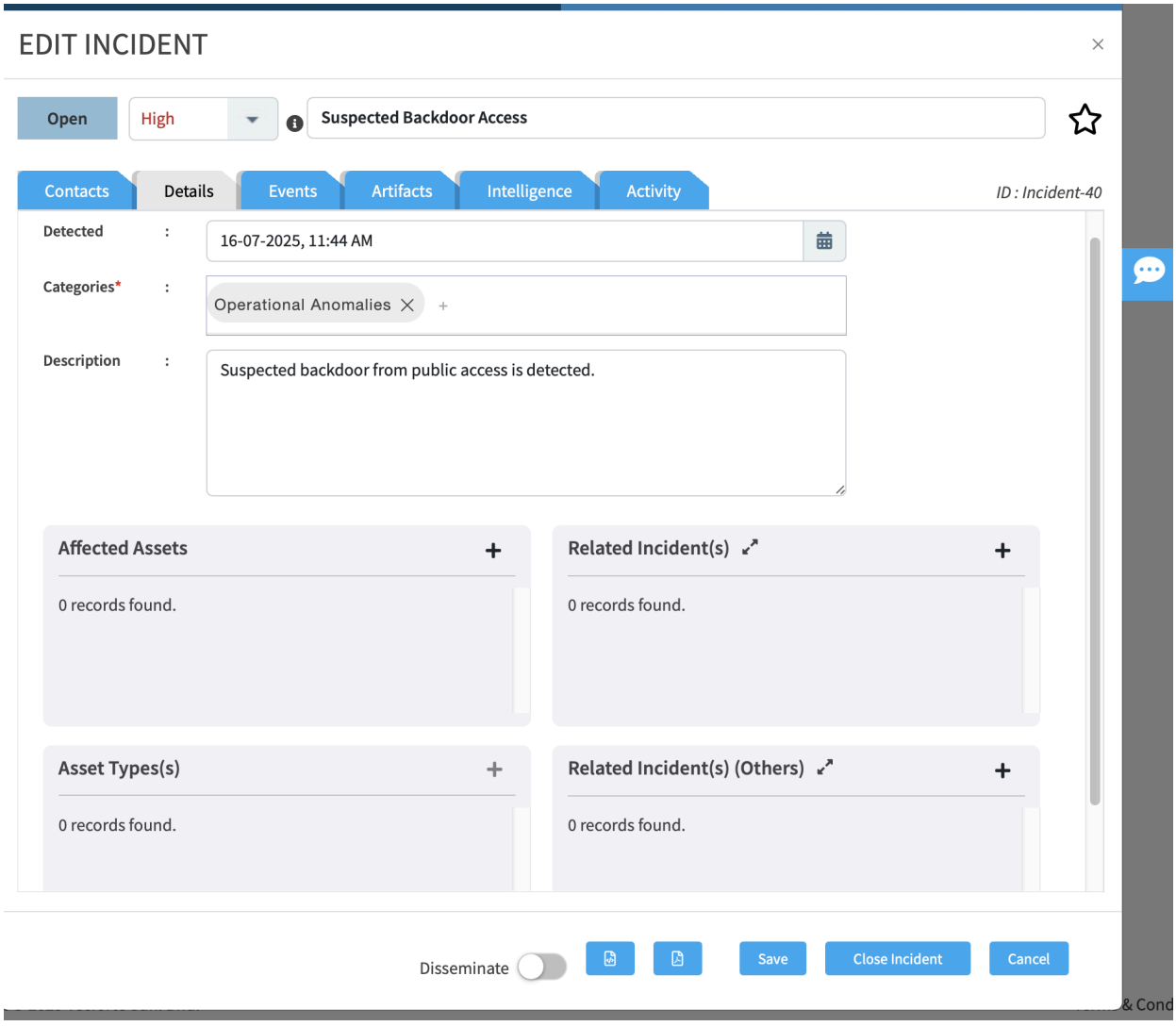
100	Suspected Backdoor Access 16-07-2025, 11:30:22 AM 16-07-2025, 11:30:22 AM	APU	
100	Suspected Backdoor Access 16-07-2025, 11:24:22 AM 16-07-2025, 11:24:22 AM	APU	
100	Suspected Backdoor Access 16-07-2025, 11:18:22 AM 16-07-2025, 11:18:22 AM	APU	
100	Suspected Backdoor Access 16-07-2025, 11:12:22 AM 16-07-2025, 11:12:22 AM	APU	
100	Suspected Backdoor Access 16-07-2025, 11:06:22 AM 16-07-2025, 11:06:22 AM	APU	

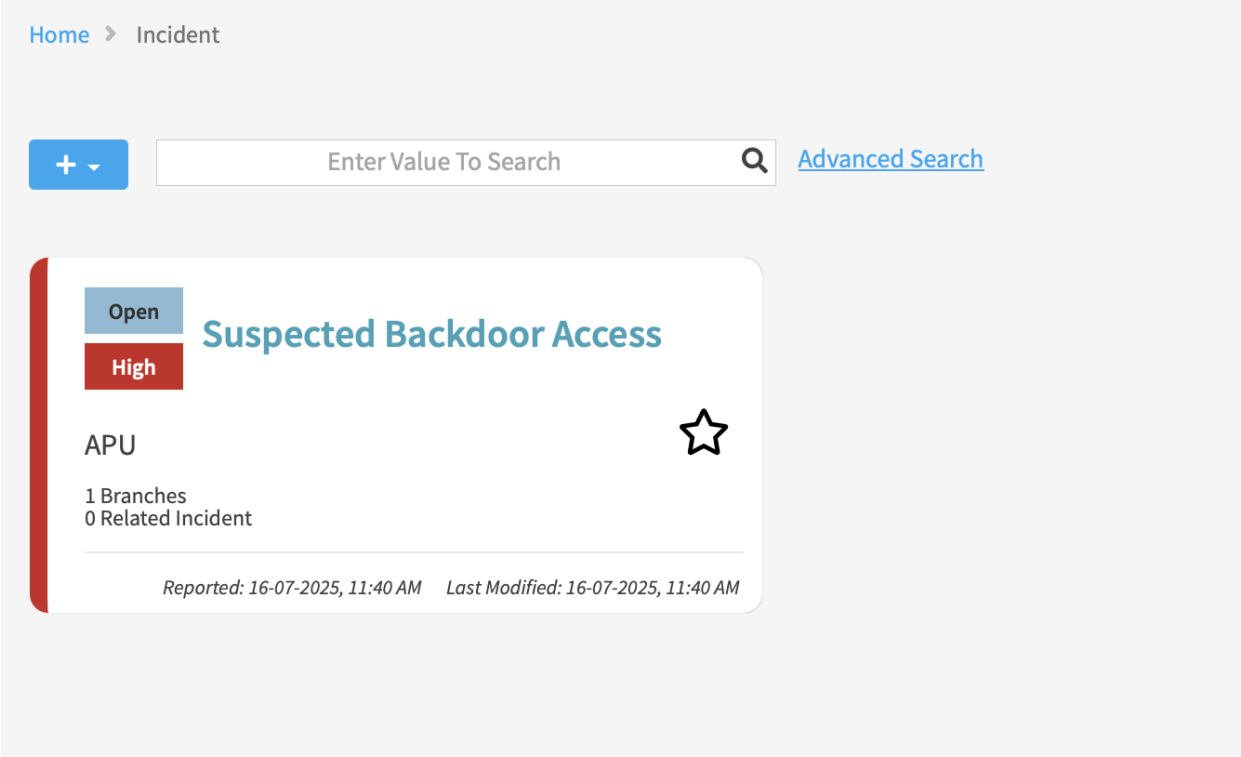
Close


VIEW TRIGGER DETAILS
Bulk
Select All
New Incident
Add to incident
Existing Incident
«« 1 2 3 4 5 6 7 8 ... 42 »»
100
Suspected Backdoor Access 16-07-2025, 11:30:22 AM
16-07-2025, 11:30:22 AM
APU
100
Suspected Backdoor Access 16-07-2025, 11:24:22 AM
16-07-2025, 11:24:22 AM
APU
100
Suspected Backdoor Access 16-07-2025, 11:18:22 AM
16-07-2025, 11:18:22 AM
APU
100
Suspected Backdoor Access 16-07-2025, 11:12:22 AM
16-07-2025, 11:12:22 AM
APU
100
Suspected Backdoor Access 16-07-2025, 11:06:22 AM
16-07-2025, 11:06:22 AM
APU
Close

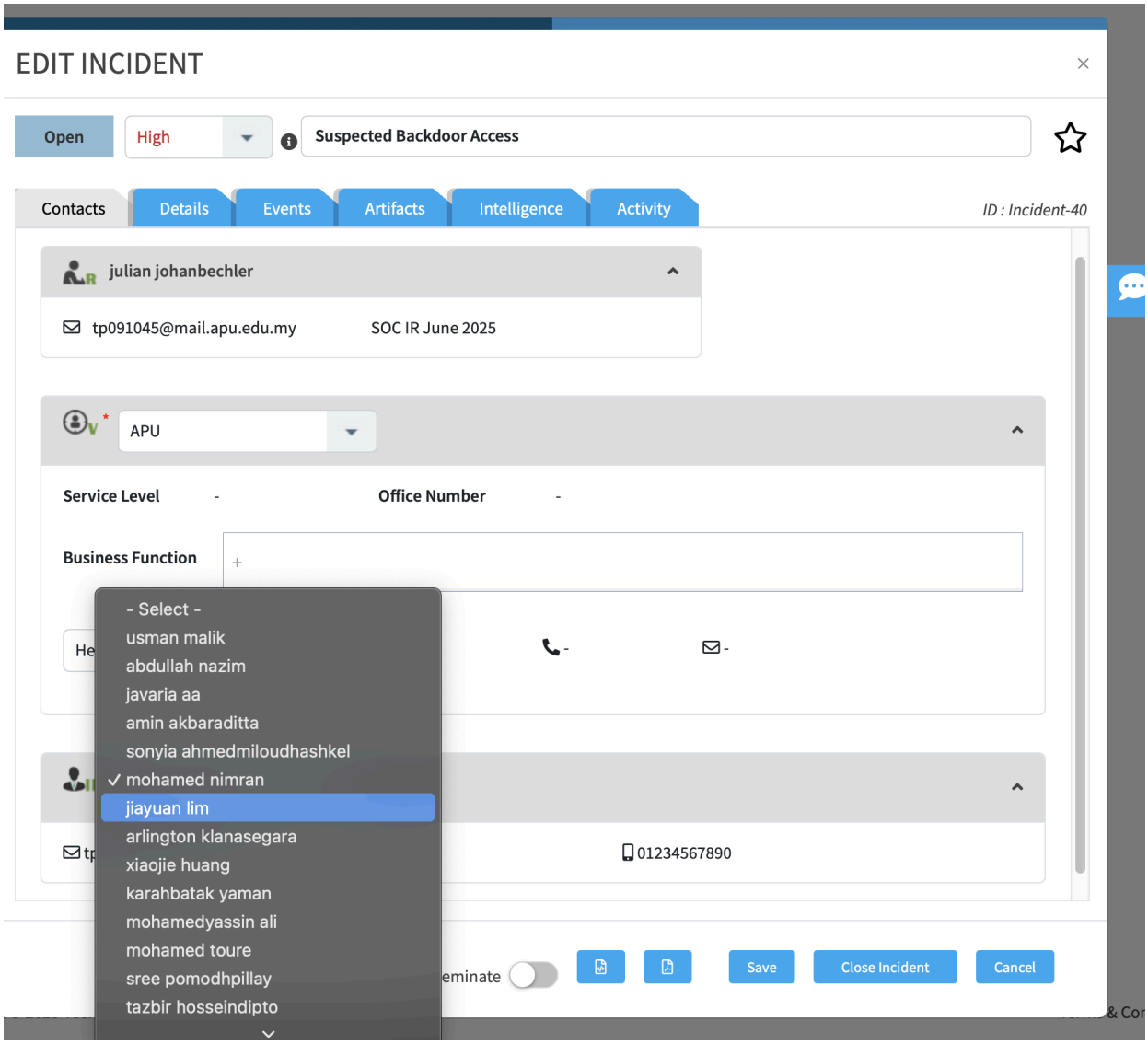

ADD INCIDENT
Draft
Medium
Suspected Backdoor Access
Contacts
Details
Events
Artifacts
Intelligence
Activity
julian johanbechler
tp091045@mail.apu.edu.my
SOC IR June 2025
APU
Service Level
-
Office Number
-
Business Function
Headquarters
Disseminate
Save
Submit
Cancel

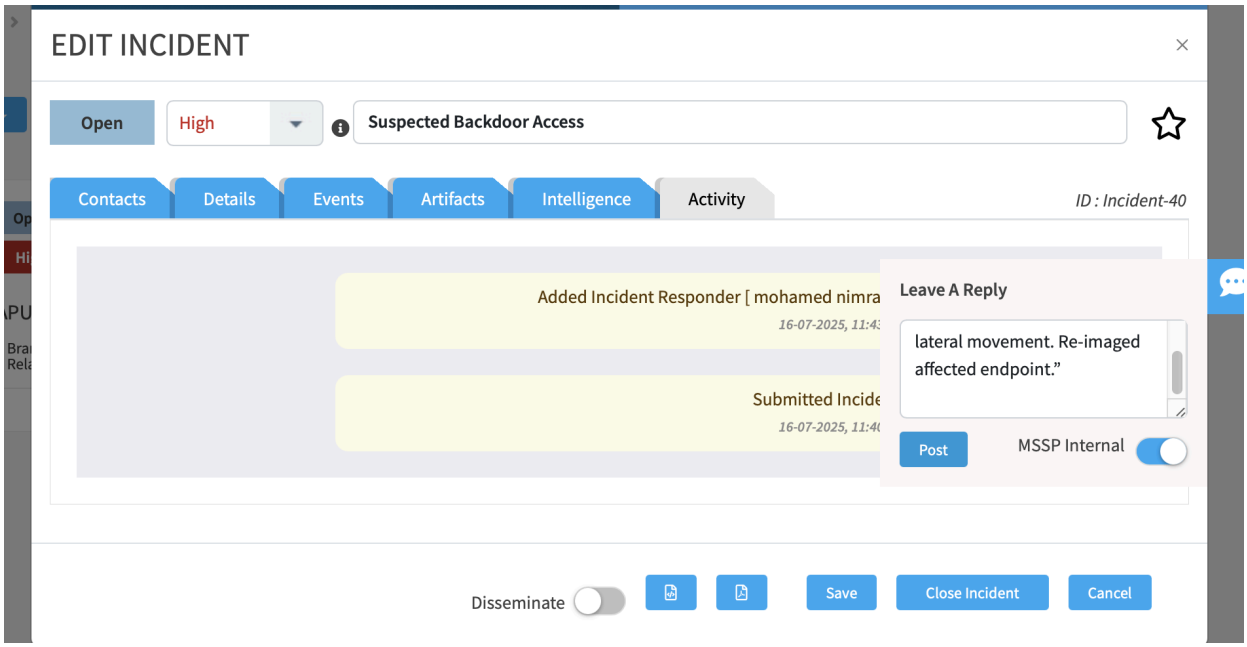

A·P·U
ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION
2
Dashboard
Statistics
Alert
Incident
Threat Intelligence
ATI Trigger
Feed
Analysis
Report
Repository
Home
Incident
Enter Value To Search
Advanced Search
Open
Low
Assignment Incident (use this)
APU
1 Branches
0 Related Incident
Reported: 16-07-2025, 11:37 AM
Last Modified: 16-07-2025, 11:38 AM

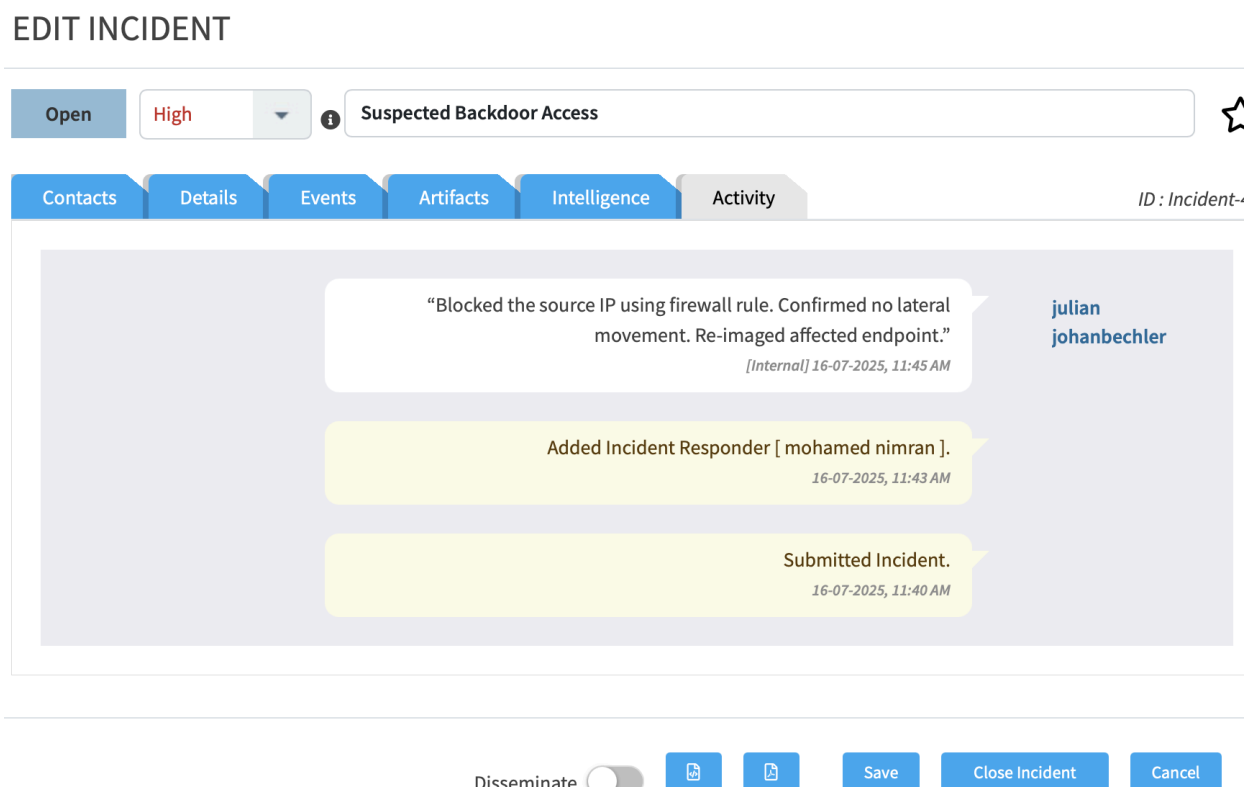

EDIT INCIDENT
Open
High
Suspected Backdoor Access
Contacts
Details
Events
Artifacts
Intelligence
Activity
ID : Incident-40
Detected
16-07-2025, 11:44 AM
Categories*
Operational Anomalies
Description
Suspected backdoor from public access is detected.
Affected Assets
0 records found.
Related Incident(s)
0 records found.
Asset Types(s)
0 records found.
Related Incident(s) (Others)
0 records found.
Disseminate
Save
Close Incident
Cancel



3. Assign an Incident Responder and resolve the incident


EDIT INCIDENT
Open
High
Suspected Backdoor Access
Contacts
Details
Events
Artifacts
Intelligence
Activity
ID : Incident-40
julian johanbechler
tp091045@mail.apu.edu.my
SOC IR June 2025
APU
Service Level
-
Office Number
-
Business Function
- Select -
usman malik
abdullah nazim
javaria aa
amin akbaraditta
sonyia ahmedmiloudhashkel
mohamed nimran
jiayuan lim
arlington klanasegara
xiaojie huang
karahbatak yaman
mohamedyassin ali
mohamed toure
sree pomodhpillay
tazbir hosseindipto
01234567890
Save
Close Incident
Cancel


EDIT INCIDENT
Open
High
Suspected Backdoor Access
Contacts
Details
Events
Artifacts
Intelligence
Activity
ID : Incident-40
Added Incident Responder [mohamed nimra
16-07-2025, 11:4
Submitted Incide
16-07-2025, 11:4
Leave A Reply
lateral movement. Re-imaged affected endpoint."
Post
MSSP Internal
Disseminate
Save
Close Incident
Cancel


EDIT INCIDENT
Open
High
Suspected Backdoor Access
Contacts
Details
Events
Artifacts
Intelligence
Activity
ID : Incident-
"Blocked the source IP using firewall rule. Confirmed no lateral movement. Re-imaged affected endpoint."
[Internal] 16-07-2025, 11:45 AM
julian johanbechler
Added Incident Responder [mohamed nimran].
16-07-2025, 11:43 AM
Submitted Incident.
16-07-2025, 11:40 AM
Disseminate
Save
Close Incident
Cancel

4. What is STIX and what does it do in SIEM?

STIX (Structured Threat Information eXpression) is basically a standard format for sharing cyber threat info. It helps people and systems share stuff like:

- indicators (like IPs, file hashes, dodgy domains)
- attacker tactics & techniques (aka TTPs)
- threat actor profiles
- observables + attack patterns

In a SIEM, STIX helps a lot by:

- auto-pulling in external threat intel feeds
- making it easier to match local logs with known threats
- helping detect more advanced stuff based on patterns
- giving extra info to incidents in a standard way

Example STIX JSON:

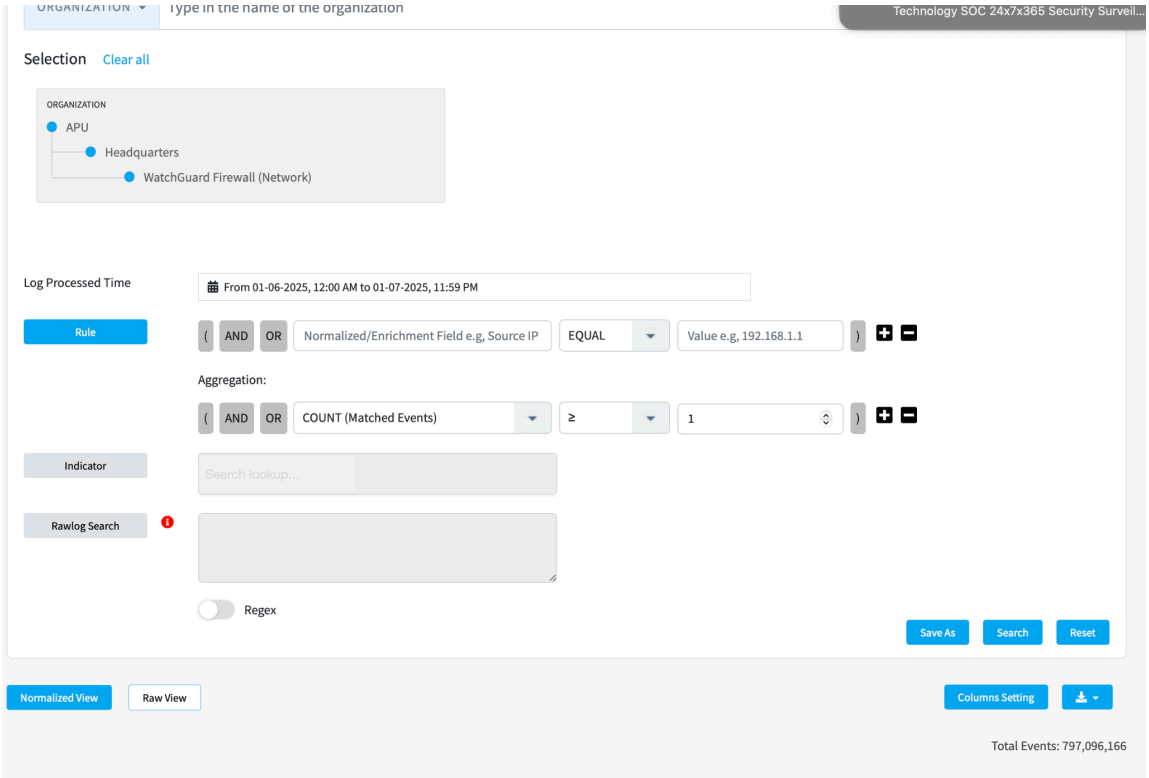
```
json
CopyEdit
{
  "type": "indicator",
  "pattern": "[file:hashes.'SHA-256' = 'abc123...']",
  "valid_from": "2025-07-16T00:00:00Z"
```

}

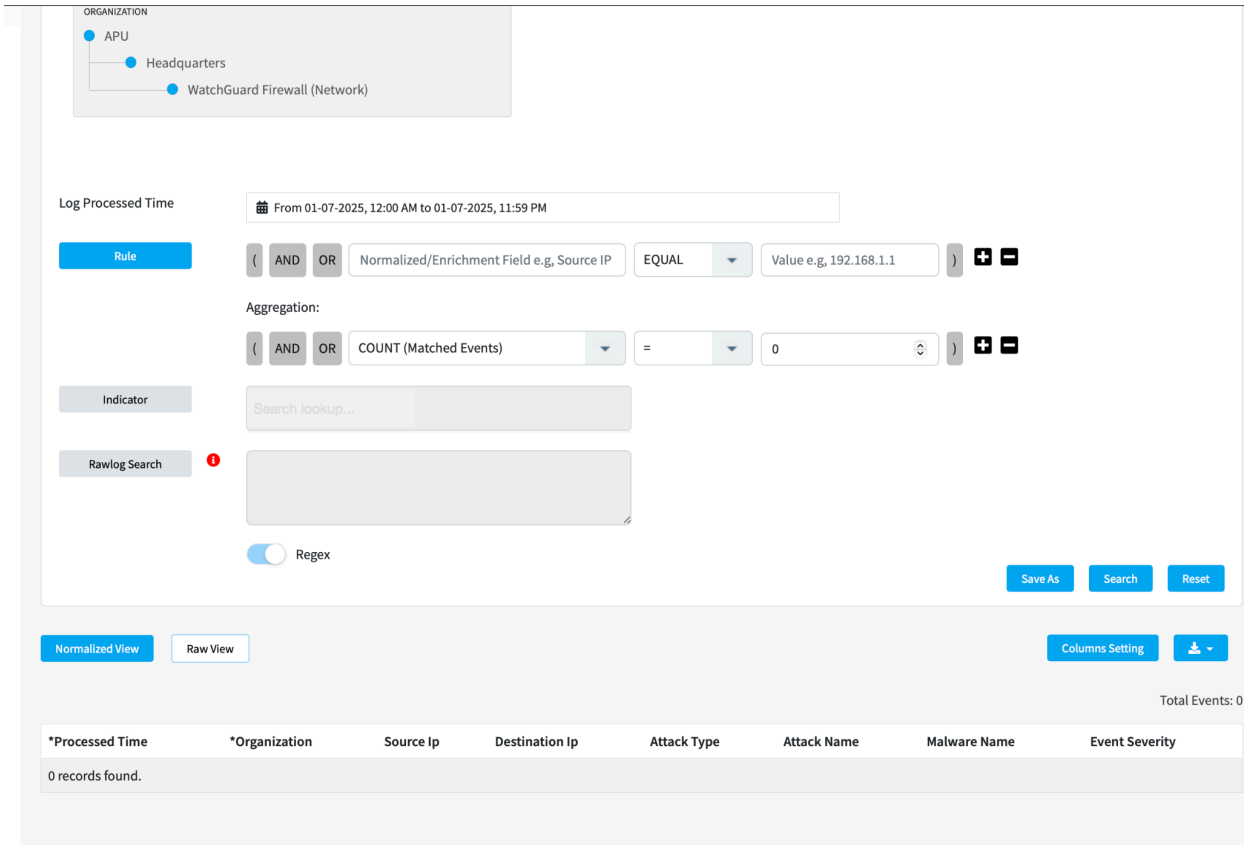
5. How many events were detected in June 2025 and on July 1st 2025?

- **01 June 2025 - 01 July 2025**

797,096,166 (Rawlog search: data collected & detected) >= 1

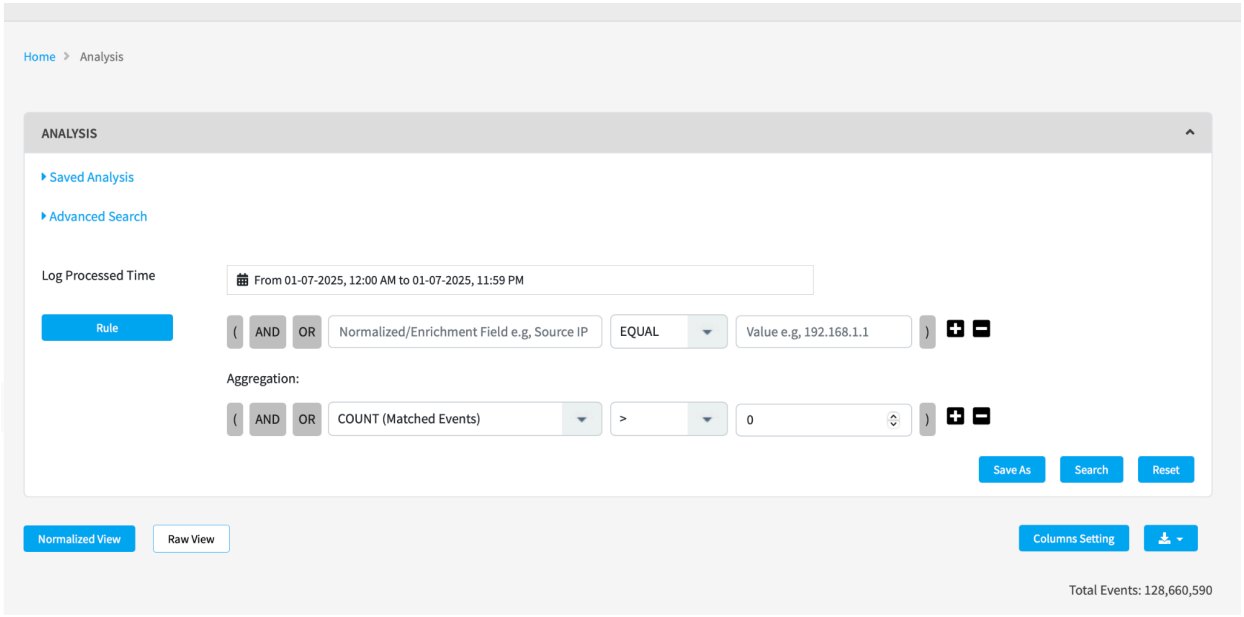


- **01 July 2025**



It seems that all raw incidents that have been collected have been also detected immediately.

Either im doing something wrong or the rules/firewalls are overly sensitive (?)


Home
Analysis
ANALYSIS
Saved Analysis
Advanced Search
Log Processed Time
From 01-07-2025, 12:00 AM to 01-07-2025, 11:59 PM
Rule
(
AND
OR
Normalized/Enrichment Field e.g, Source IP
EQUAL
Value e.g, 192.168.1.1
)
Aggregation:
(
AND
OR
COUNT (Matched Events)
>
0
)
Save As
Search
Reset
Normalized View
Raw View
Columns Setting
Total Events: 128,660,590

128,660,590