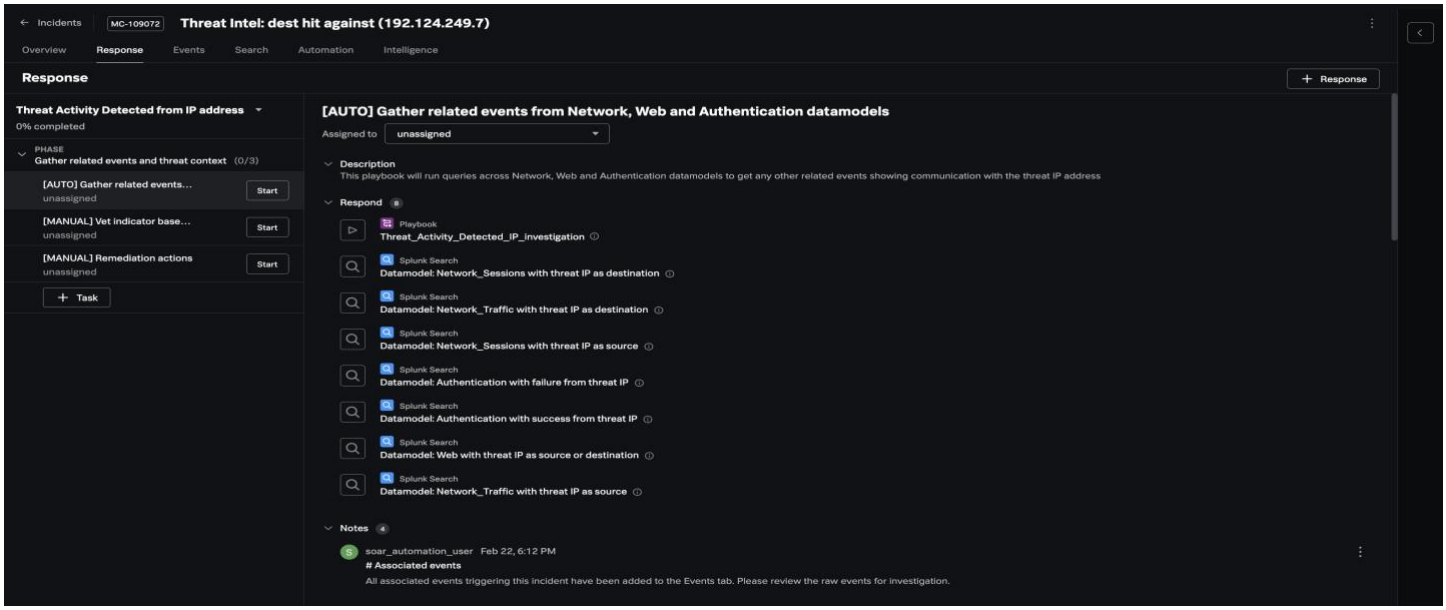
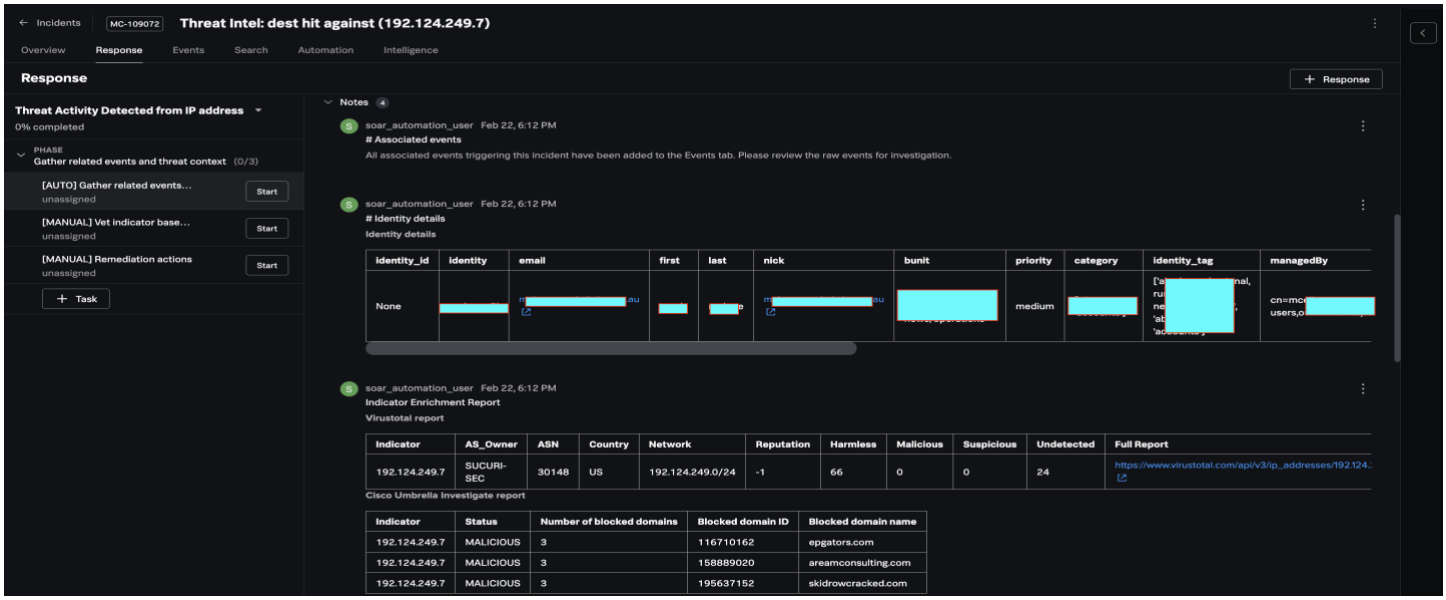
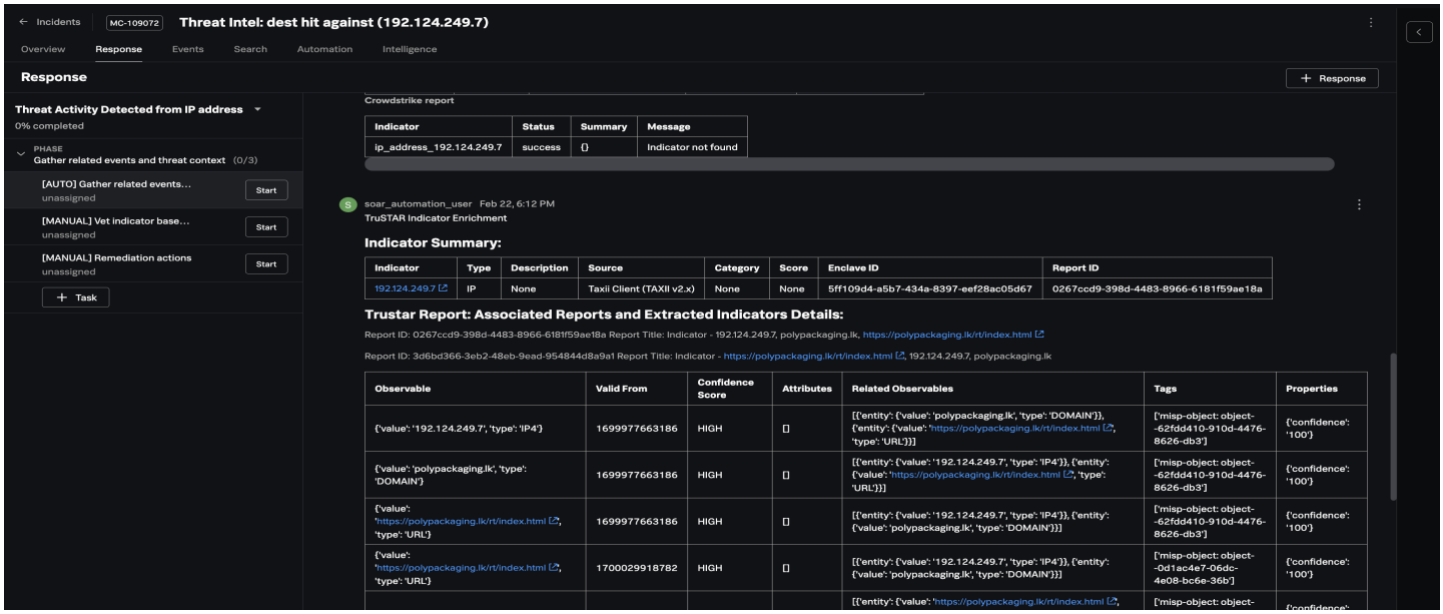

Incidents
MC-109072
Threat Intel: dest hit against (192.124.249.7)
Overview
Response
Events
Search
Automation
Intelligence
Response
Response
Threat Activity Detected from IP address
0% completed
PHASE
Gather related events and threat context (0/3)
[AUTO] Gather related events...
unassigned
Start
[MANUAL] Vet indicator base...
unassigned
Start
[MANUAL] Remediation actions
unassigned
Start
Task
[AUTO] Gather related events from Network, Web and Authentication datamodels
Assigned to
unassigned
Description
This playbook will run queries across Network, Web and Authentication datamodels to get any other related events showing communication with the threat IP address
Respond
Playbook
Threat_Activity_Detected_IP_investigation
Splunk Search
Datamodel: Network_Sessions with threat IP as destination
Splunk Search
Datamodel: Network_Traffic with threat IP as destination
Splunk Search
Datamodel: Network_Sessions with threat IP as source
Splunk Search
Datamodel: Authentication with failure from threat IP
Splunk Search
Datamodel: Authentication with success from threat IP
Splunk Search
Datamodel: Web with threat IP as source or destination
Splunk Search
Datamodel: Network_Traffic with threat IP as source
Notes
soar_automation_user Feb 22, 6:12 PM
Associated events
All associated events triggering this incident have been added to the Events tab. Please review the raw events for investigation.


Incidents
MC-109072
Threat Intel: dest hit against (192.124.249.7)
Overview
Response
Events
Search
Automation
Intelligence
Response
Response
Threat Activity Detected from IP address
0% completed
PHASE
Gather related events and threat context (0/3)
[AUTO] Gather related events...
unassigned
Start
[MANUAL] Vet indicator base...
unassigned
Start
[MANUAL] Remediation actions
unassigned
Start
Task
Notes
soar_automation_user Feb 22, 6:12 PM
Associated events
All associated events triggering this incident have been added to the Events tab. Please review the raw events for investigation.
soar_automation_user Feb 22, 6:12 PM
Identity details
Identity details
identity_id
identity
email
first
last
nick
bunit
priority
category
identity_tag
managedBy
None
medium
soar_automation_user Feb 22, 6:12 PM
Indicator Enrichment Report
Virustotal report
Indicator
AS_Owner
ASN
Country
Network
Reputation
Harmless
Malicious
Suspicious
Undetected
Full Report
192.124.249.7
SUCURI-SEC
30148
US
192.124.249.0/24
-1
66
0
0
24
https://www.virustotal.com/api/v3/ip_addresses/192.124.
Cisco Umbrella Investigate report
Indicator
Status
Number of blocked domains
Blocked domain ID
Blocked domain name
192.124.249.7
MALICIOUS
3
116710162
epgators.com
192.124.249.7
MALICIOUS
3
158889020
areamconsulting.com
192.124.249.7
MALICIOUS
3
195637152
skidrowcracked.com


Incidents
MC-109072
Threat Intel: dest hit against (192.124.249.7)
Overview
Response
Events
Search
Automation
Intelligence
Response
Response
Threat Activity Detected from IP address
0% completed
PHASE
Gather related events and threat context (0/3)
[AUTO] Gather related events...
unassigned
Start
[MANUAL] Vet indicator base...
unassigned
Start
[MANUAL] Remediation actions
unassigned
Start
Task
Crowdstrike report
Indicator
Status
Summary
Message
ip_address_192.124.249.7
success
{}
Indicator not found
soar_automation_user Feb 22, 6:12 PM
TruSTAR Indicator Enrichment
Indicator Summary:
Indicator
Type
Description
Source
Category
Score
Enclave ID
Report ID
192.124.249.7
IP
None
Taxii Client (TAXII v2.x)
None
None
5ff109d4-a5b7-434a-8397-eef28ac05d67
0267ccd9-398d-4483-8966-6181f59ae18a
Trustar Report: Associated Reports and Extracted Indicators Details:
Report ID: 0267ccd9-398d-4483-8966-6181f59ae18a Report Title: Indicator - 192.124.249.7, polypackaging.lk, https://polypackaging.lk/rt/index.html
Report ID: 3d6bd366-3eb2-48eb-9ead-954844d8a9a1 Report Title: Indicator - https://polypackaging.lk/rt/index.html, 192.124.249.7, polypackaging.lk
Observable
Valid From
Confidence Score
Attributes
Related Observables
Tags
Properties
{'value': '192.124.249.7', 'type': 'IP4'}
1699977663186
HIGH
[]
[{'entity': {'value': 'polypackaging.lk', 'type': 'DOMAIN'}}, {'entity': {'value': 'https://polypackaging.lk/rt/index.html', 'type': 'URL'}}]
['misp-object: object--62fdd410-910d-4476-8626-db3']
{'confidence': '100'}
{'value': 'polypackaging.lk', 'type': 'DOMAIN'}
1699977663186
HIGH
[]
[{'entity': {'value': '192.124.249.7', 'type': 'IP4'}}, {'entity': {'value': 'https://polypackaging.lk/rt/index.html', 'type': 'URL'}}]
['misp-object: object--62fdd410-910d-4476-8626-db3']
{'confidence': '100'}
{'value': 'https://polypackaging.lk/rt/index.html', 'type': 'URL'}
1699977663186
HIGH
[]
[{'entity': {'value': '192.124.249.7', 'type': 'IP4'}}, {'entity': {'value': 'polypackaging.lk', 'type': 'DOMAIN'}}]
['misp-object: object--62fdd410-910d-4476-8626-db3']
{'confidence': '100'}
{'value': 'https://polypackaging.lk/rt/index.html', 'type': 'URL'}
1700029918782
HIGH
[]
[{'entity': {'value': '192.124.249.7', 'type': 'IP4'}}, {'entity': {'value': 'polypackaging.lk', 'type': 'DOMAIN'}}]
['misp-object: object--0d1ac4e7-06dc-4e08-bc6e-36b']
{'confidence': '100'}
[{'entity': {'value': 'https://polypackaging.lk/rt/index.html',
['misp-object: object-
{'confidence':