Alert Input

Input mode

● Form ○ JSON

Thread ID (for checkpointing)

demo-thread

Run mode

● Native streaming (parallel)

○ Sequential stepper

Step delay (sequential mode)

0.60

Policy (from config.yaml)

```
{
  "thresholds" : {
    "validity_tp_min"
     : 0.65
    "severity_min"
     : 2
```

AI SOC – Multi-Agent (A2A) Orchestration

Parallel scoring → Playbooks → Decision → XSOAR / Human → Status

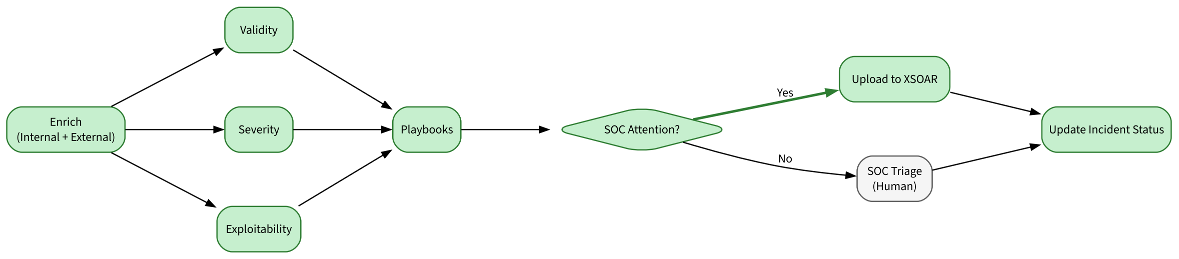
Alert

```
{
  "id" : "ALRT-1001"
  "source" : "SIEM"
  "title" :
  "Outbound connection to known brute-force
  IP"
  "description" :
  "FW logs show repeated egress to
  suspicious IP by host srv-42."
  "indicators" : [
    0 : {
      "type" : "ip"
      "value" : "203.0.113.55"
      "context" : NULL
    }
    1 : {
      "type" : "host"
```

How it works

- **Native streaming** mode uses LangGraph events.
- **Sequential** mode uses a stepper for deterministic UI.

```
            "value" : "srv-42"
            "context" : NULL
          }
        ▼ 2 : {
            "type" : "user"
            "value" : "svc-backup"
            "context" : NULL
          }
      ]
      "created_at" :
      "datetime.datetime(2025, 9, 5, 12, 31, 5,
      475090)"
  }
```



Validity (TP likelihood)

0.90

True Positive

Severity Level

3

High

Exploitability Likelih…

0.85

Critical

Path

—

Pending decision

Progress: 100% — Elapsed 12.4s — ETA 0.0s

Block IP, Quarantine Host, Forensics, Alert Team

Enrichment — Internal

```
[
  0 : {
    "source" : "EDR"
    "hit" : true
    "host" : "srv-42"
    "note" :
    "Process spawn chain"
  }
  1 : {
    "source" : "CMDB"
    "owner" : "Payments"
    "criticality" : "High"
  }
  2 : {
    "source" : "EDR"
    "hit" : true
    "host" : "srv-42"
    "note" :
    "Process spawn chain"
  }
  3 : {
    "source" : "CMDB"
    "owner" : "Payments"
```

Enrichment — External

```
[
  0 : {
    "source" : "AbuseIPDB"
    "score" : 85
    "ip" : "203.0.113.55"
    "tags" : [
      0 : "bruteforce"
    ]
  }
  1 : {
    "source" : "GreyNoise"
    "classification" :
    "malicious"
    "ip" : "203.0.113.55"
  }
]
```

```
    "criticality" : "High"
  }
  4 : {
    "source" : "EDR"
    "hit" : true
    "host" : "srv-42"
    "note" :
    "Process spawn chain"
  }
  5 : {
    "source" : "CMDB"
    "owner" : "Payments"
    "criticality" : "High"
  }
]
```

2025-09-05 12:31:05.685622 — enriched

```
{
  "internal" : 6
  "external" : 2
}
```

2025-09-05 12:31:11.512009 — scored_validity

```
{
  "score" : {
        "label" : "True Positive"
        "likelihood" : 0.9
        "rationale" :
        "The alert indicates repeated egress to a known brute-force
        IP (203.0.113.55) from host srv-42, which is corroborated
        by multiple internal EDR hits and external sources
        (AbuseIPDB and GreyNoise) confirming the IP's malicious
        nature. The criticality of the host (Payments) further
        emphasizes the potential risk, leading to a high likelihood
        of the alert being valid."
    }
}
```

2025-09-05 12:31:12.095571 — scored_severity

```
{
    "score" : {
        "level" : 3
        "impact" : "High"
```

```
      "rationale" :
      "The alert indicates that a critical host (srv-42)
      associated with the Payments department is making repeated
      outbound connections to a known malicious IP address
      (203.0.113.55) that is tagged for brute-force attacks.
      Given that the Payments department handles sensitive
      financial transactions, any compromise could lead to
      significant financial loss, data breaches, or regulatory
      penalties. The high criticality of the host and the nature
      of the threat elevate the severity of this incident to a
      high level."
    }
}
```

2025-09-05 12:31:12.290076 — scored_exploitability

```
{
  "score" : {
      "level" : "Critical"
      "likelihood" : 0.85
      "rationale" :
      "The outbound connection to a known brute-force IP
      indicates a high likelihood of an ongoing attack or
      compromise. The IP has a high abuse score and is classified
      as malicious, suggesting that srv-42 may be compromised or
      being used to facilitate further attacks. The criticality
      of the host (Payments) further elevates the risk, making
      this situation critical."
  }
}
```

2025-09-05 12:31:15.592249 — selected_playbooks

```
{
  "playbooks" : {
    "names" : [...]
    "rationale" :
    "Given the high severity and critical exploitability of the
    alert, immediate actions are necessary to mitigate
    potential risks. 'Block IP' will prevent further outbound
    connections to the known malicious IP (203.0.113.55).
    'Quarantine Host' is essential to isolate srv-42 to prevent
    any potential compromise from spreading. 'Forensics' will
    help in investigating the extent of the breach and
    understanding how the host was compromised. Finally, 'Alert
    Team' ensures that the incident response team is informed
    to take further necessary actions."
  }
}
```

2025-09-05 12:31:17.966788 — decision_made

```
{
  "decision" : {
    "soc_attention" : false
    "path" : "UPLOAD_XSOAR"
```

```
      "rationale" : "The alert meets all policy thresholds: the validity likelihood (0.9) exceeds the minimum threshold (0.65), the severity level (3) is above the minimum severity (2), and the exploitability level is classified as Critical. Given the high risk associated with the Payments department and the confirmed malicious activity, it is appropriate to upload this incident to XSOAR for further automated response and investigation."
    }
}
```

2025-09-05 12:31:17.969296 — xsoar_uploaded

```
{
    "api_response" : {
      "result" : "ok"
      "incident_id" : "INC-1757075477.969284"
    }
}
```

```
{
  "alert" : "id='ALRT-1001' source='SIEM' title='Outbound connection to known brute-force IP' description='FW logs show repeated egress to suspicious IP by host srv-42.' indicators=[Indicator(type='ip', value='203.0.113.55', context=None), Indicator(type='host', value='srv-42', context=None), Indicator(type='user', value='svc-backup', context=None)] created_at=datetime.datetime(2025, 9, 5, 12, 31, 5, 475090)"
```

```
"enrichment" : {
  "internal" : [
    0 : {
      "source" : "EDR"
      "hit" : true
      "host" : "srv-42"
      "note" : "Process spawn chain"
    }
    1 : {
      "source" : "CMDB"
      "owner" : "Payments"
      "criticality" : "High"
    }
    2 : {
      "source" : "EDR"
      "hit" : true
      "host" : "srv-42"
      "note" : "Process spawn chain"
    }
    3 : {
      "source" : "CMDB"
      "owner" : "Payments"
      "criticality" : "High"
    }
    4 : {
      "source" : "EDR"
```

```
        "hit" : true
        "host" : "srv-42"
        "note" : "Process spawn chain"
      }
      5 : {
        "source" : "CMDB"
        "owner" : "Payments"
        "criticality" : "High"
      }
    ]
    "external" : [
      0 : {
        "source" : "AbuseIPDB"
        "score" : 85
        "ip" : "203.0.113.55"
        "tags" : [
          0 : "bruteforce"
        ]
      }
      1 : {
        "source" : "GreyNoise"
        "classification" : "malicious"
        "ip" : "203.0.113.55"
      }
    ]
  }
```

```
"validity" :
"label='True Positive' likelihood=0.9 rationale="The alert indicates repeated egress to a known brute-force IP (203.0.113.55) from host srv-42, which is corroborated by multiple internal EDR hits and external sources (AbuseIPDB and GreyNoise) confirming the IP's malicious nature. The criticality of the host (Payments) further emphasizes the potential risk, leading to a high likelihood of the alert being valid.""
"severity" :
"level=3 impact='High' rationale='The alert indicates that a critical host (srv-42) associated with the Payments department is making repeated outbound connections to a known malicious IP address (203.0.113.55) that is tagged for brute-force attacks. Given that the Payments department handles sensitive financial transactions, any compromise could lead to significant financial loss, data breaches, or regulatory penalties. The high criticality of the host and the nature of the threat elevate the severity of this incident to a high level.'"
"exploitability" :
"level='Critical' likelihood=0.85 rationale='The outbound connection to a known brute-force IP indicates a high likelihood of an ongoing attack or compromise. The IP has a high abuse score and is classified as malicious, suggesting that srv-42 may be compromised or being used to facilitate further attacks. The criticality of the host (Payments) further elevates the risk, making this situation critical.'"
```

```
"playbooks" :
"names=['Block IP', 'Quarantine Host', 'Forensics', 'Alert Team']
rationale="Given the high severity and critical exploitability of
the alert, immediate actions are necessary to mitigate potential
risks. 'Block IP' will prevent further outbound connections to the
known malicious IP (203.0.113.55). 'Quarantine Host' is essential
to isolate srv-42 to prevent any potential compromise from
spreading. 'Forensics' will help in investigating the extent of
the breach and understanding how the host was compromised.
Finally, 'Alert Team' ensures that the incident response team is
informed to take further necessary actions.""
"decision" :
"soc_attention=False path='UPLOAD_XSOAR' rationale='The alert
meets all policy thresholds: the validity likelihood (0.9) exceeds
the minimum threshold (0.65), the severity level (3) is above the
minimum severity (2), and the exploitability level is classified
as Critical. Given the high risk associated with the Payments
department and the confirmed malicious activity, it is appropriate
to upload this incident to XSOAR for further automated response
and investigation.'"
"status" : "XSOAR Open"
▼ "logs" : [
    0 :
    "at=datetime.datetime(2025, 9, 5, 12, 31, 5, 685622)
    event='enriched' details={'internal': 6, 'external': 2}"
```

```
1 :
"at=datetime.datetime(2025, 9, 5, 12, 31, 12, 290076)
event='scored_exploitability' details={'score': {'level':
'Critical', 'likelihood': 0.85, 'rationale': 'The outbound
connection to a known brute-force IP indicates a high
likelihood of an ongoing attack or compromise. The IP has a
high abuse score and is classified as malicious, suggesting
that srv-42 may be compromised or being used to facilitate
further attacks. The criticality of the host (Payments) further
elevates the risk, making this situation critical.'}}"
2 :
"at=datetime.datetime(2025, 9, 5, 12, 31, 12, 95571)
event='scored_severity' details={'score': {'level': 3,
'impact': 'High', 'rationale': 'The alert indicates that a
critical host (srv-42) associated with the Payments department
is making repeated outbound connections to a known malicious IP
address (203.0.113.55) that is tagged for brute-force attacks.
Given that the Payments department handles sensitive financial
transactions, any compromise could lead to significant
financial loss, data breaches, or regulatory penalties. The
high criticality of the host and the nature of the threat
elevate the severity of this incident to a high level.'}}"
```

```
3 :
"at=datetime.datetime(2025, 9, 5, 12, 31, 11, 512009)
event='scored_validity' details={'score': {'label': 'True
Positive', 'likelihood': 0.9, 'rationale': "The alert indicates
repeated egress to a known brute-force IP (203.0.113.55) from
host srv-42, which is corroborated by multiple internal EDR
hits and external sources (AbuseIPDB and GreyNoise) confirming
the IP's malicious nature. The criticality of the host
(Payments) further emphasizes the potential risk, leading to a
high likelihood of the alert being valid."}}"
4 :
"at=datetime.datetime(2025, 9, 5, 12, 31, 15, 592249)
event='selected_playbooks' details={'playbooks': {'names':
['Block IP', 'Quarantine Host', 'Forensics', 'Alert Team'],
'rationale': "Given the high severity and critical
exploitability of the alert, immediate actions are necessary to
mitigate potential risks. 'Block IP' will prevent further
outbound connections to the known malicious IP (203.0.113.55).
'Quarantine Host' is essential to isolate srv-42 to prevent any
potential compromise from spreading. 'Forensics' will help in
investigating the extent of the breach and understanding how
the host was compromised. Finally, 'Alert Team' ensures that
the incident response team is informed to take further
necessary actions."}}"
```

```
      5 :
      "at=datetime.datetime(2025, 9, 5, 12, 31, 17, 966788)
      event='decision_made' details={'decision': {'soc_attention':
      False, 'path': 'UPLOAD_XSOAR', 'rationale': 'The alert meets
      all policy thresholds: the validity likelihood (0.9) exceeds
      the minimum threshold (0.65), the severity level (3) is above
      the minimum severity (2), and the exploitability level is
      classified as Critical. Given the high risk associated with the
      Payments department and the confirmed malicious activity, it is
      appropriate to upload this incident to XSOAR for further
      automated response and investigation.'}}"
      6 :
      "at=datetime.datetime(2025, 9, 5, 12, 31, 17, 969296)
      event='xsoar_uploaded' details={'api_response': {'result':
      'ok', 'incident_id': 'INC-1757075477.969284'}}"
      7 :
      "at=datetime.datetime(2025, 9, 5, 12, 31, 17, 972201)
      event='xsoar_status_updated' details={'response': {'result':
      'ok', 'incident_id': 'INC-PLACEHOLDER', 'status': 'Open'}}"
   ]
}
```

Download diagram (SVG)

✓ Flow completed

Execution Timeline

Playbooks

Playbook rationale

Given the high severity and critical exploitability of the alert, immediate actions are necessary to mitigate potential risks. 'Block IP' will prevent further outbound connections to the known malicious IP (203.0.113.55). 'Quarantine Host' is essential to isolate srv-42 to prevent any potential compromise from spreading. 'Forensics' will help in investigating the extent of the breach and understanding how the host was compromised. Finally, 'Alert Team' ensures that the incident response team is informed to take further necessary actions.

Final State