Event Prioritization & Alert Triage

Chris Adams

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | **F:** +1.703.229.4489
www.ThreatConnect.com

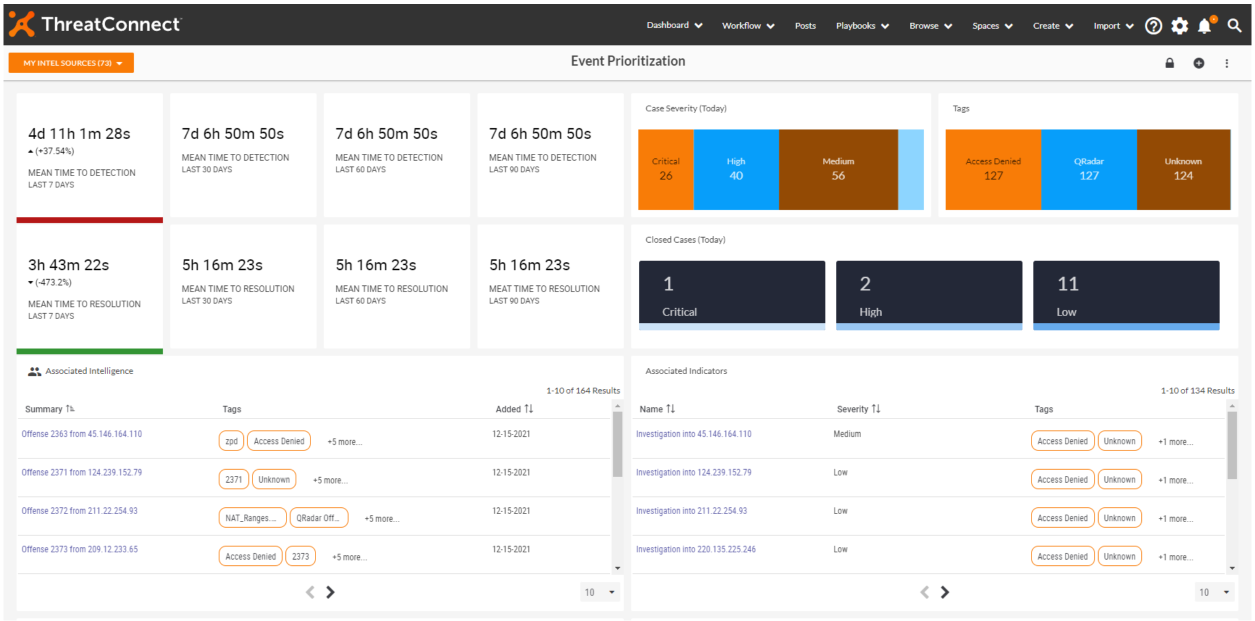
Purpose

This document describes how a security operations center (SOC) analyst can prioritize events and triage alerts in their environment using ThreatConnect and their existing security infrastructure. Additionally, this document introduces a process to guide an analyst through each step in the event prioritization process. Analysts can apply their understanding of this process to suit their specific needs.

Measurable Outcomes

This use case offers several benefits in terms of valuable and measurable outcomes. These benefits, some of which are presented in the **Event Prioritization** dashboard (Figure 1), include:

- A visible means to present metrics, including mean time to detection (MTTD) and mean time to resolution (MTTR), so teams can optimize their processes over time and reduce averages
- Quick identification and classification of events mapped to specific Cases based on associations to existing events or correlation to high-impact threat vectors
- Integrated data sets from Cases, events, tickets, and intelligence to provide a comprehensive view of an incident.



Event Prioritization

4d 11h 1m 28s
▴ (+37.54%)
MEAN TIME TO DETECTION
LAST 7 DAYS

7d 6h 50m 50s
MEAN TIME TO DETECTION
LAST 30 DAYS

7d 6h 50m 50s
MEAN TIME TO DETECTION
LAST 60 DAYS

7d 6h 50m 50s
MEAN TIME TO DETECTION
LAST 90 DAYS

Case Severity (Today)

Critical 26 | High 40 | Medium 56

Tags

Access Denied 127 | QRadar 127 | Unknown 124

3h 43m 22s
▾ (-473.2%)
MEAN TIME TO RESOLUTION
LAST 7 DAYS

5h 16m 23s
MEAN TIME TO RESOLUTION
LAST 30 DAYS

5h 16m 23s
MEAN TIME TO RESOLUTION
LAST 60 DAYS

5h 16m 23s
MEAT TIME TO RESOLUTION
LAST 90 DAYS

Closed Cases (Today)

1 Critical | 2 High | 11 Low

Associated Intelligence

1-10 of 164 Results

Summary	Tags	Added
Offense 2363 from 45.146.164.110	zpd, Access Denied, +5 more...	12-15-2021
Offense 2371 from 124.239.152.79	2371, Unknown, +5 more...	12-15-2021
Offense 2372 from 211.22.254.93	NAT_Ranges..., QRadar Off..., +5 more...	12-15-2021
Offense 2373 from 209.12.233.65	Access Denied, 2373, +5 more...	12-15-2021

10

Associated Indicators

1-10 of 134 Results

Name	Severity	Tags
Investigation into 45.146.164.110	Medium	Access Denied, Unknown, +1 more...
Investigation into 124.239.152.79	Low	Access Denied, Unknown, +1 more...
Investigation into 211.22.254.93	Low	Access Denied, Unknown, +1 more...
Investigation into 220.135.225.246	Low	Access Denied, Unknown, +1 more...

10

Figure 1: Event Prioritization Dashboard

Introduction

A major challenge SOC analysts face is the loss of time spent chasing down alerts and trying to gather a contextual understanding of events that occur in their environment.

Event prioritization is the practice of identifying which events require the most attention from SOC analysts. For example, an event may be prioritized because it is correlated to a malicious threat actor or another security event. Normally, this relationship is determined using a correlation rule in the SIEM where event A and event B have met a specific condition. However, trying to manually review and prioritize events that come into a SIEM is a time-consuming and problematic process for most analysts.

The ever-growing number of security alerts make it difficult for SOC analysts to keep up with their day-to-day responsibilities. To alleviate this problem, ThreatConnect provides an overlay of contextual threat information pertaining to current and emerging threats. This information enables analysts to examine strategic and operational intelligence from sources outside their organization and match it with existing log sources. The outcome of this process is faster threat detection times and the ability to prioritize events as they occur, based on threat levels and asset exposure.

Examples include, but are not limited to, subscription and open-source research and reports describing new tactics, techniques, and procedures (TTPs), threat intelligence from working groups and peers, and law enforcement communications. When this information is tied in and correlated with events, analysts gain a better understanding of what they should pay attention to first.

Summary of Phases

Prerequisite: Configure the SIEM

- Create an IBM® QRadar® authentication token.
- Install the **IBM QRadar** Custom Trigger Service App via TC Exchange™.
- Create a Playbook Service for the **IBM QRadar** Custom Trigger Service App.
- Load and enable the custom **Alert Triage Event for QRadar** Playbook for processing intel.

Capture SIEM Events and Initial Context

- Query QRadar offenses.
- Each offense is then translated to an Event Group in ThreatConnect with a noted observation.
- Each Event Group contains associated metadata from the offense, which are translated into Threat and Confidence Ratings in ThreatConnect. Additionally, Attributes are populated with contextual information.

Expand Knowledge With Automated Workflows

- Query existing Cases and identify whether a related investigation is already underway.
- Leverage collective analytics to help define a Case's priority.
- Apply context, associate Event Groups, apply a Workflow Template, enrich data, query internal detective controls, and take action, as prescribed.
- Associate an Event Group to a Case and add newly discovered context to it based upon new findings, such as an event, note, or observation.

Highlight Prioritized Events Within Cases

- Collect SOC metrics and update related ThreatConnect dashboard cards.
- Should all findings warrant a full investigation, start the investigation process by escalating to an incident.
- Take defensive and protective measures.

Logical System Diagram

Figure 2 presents a high-level logical diagram of major system components and general interaction. ThreatConnect serves as the threat library ingesting threat intelligence from multiple sources and then driving operations, with that intelligence, via its Security Orchestration, Automation, and Response (SOAR) platform. ThreatConnect's SOAR platform serves as the quarterback coordinating data flows and orchestrating activity in a step-by-step manner to execute a series of processes that enable events to be prioritized.

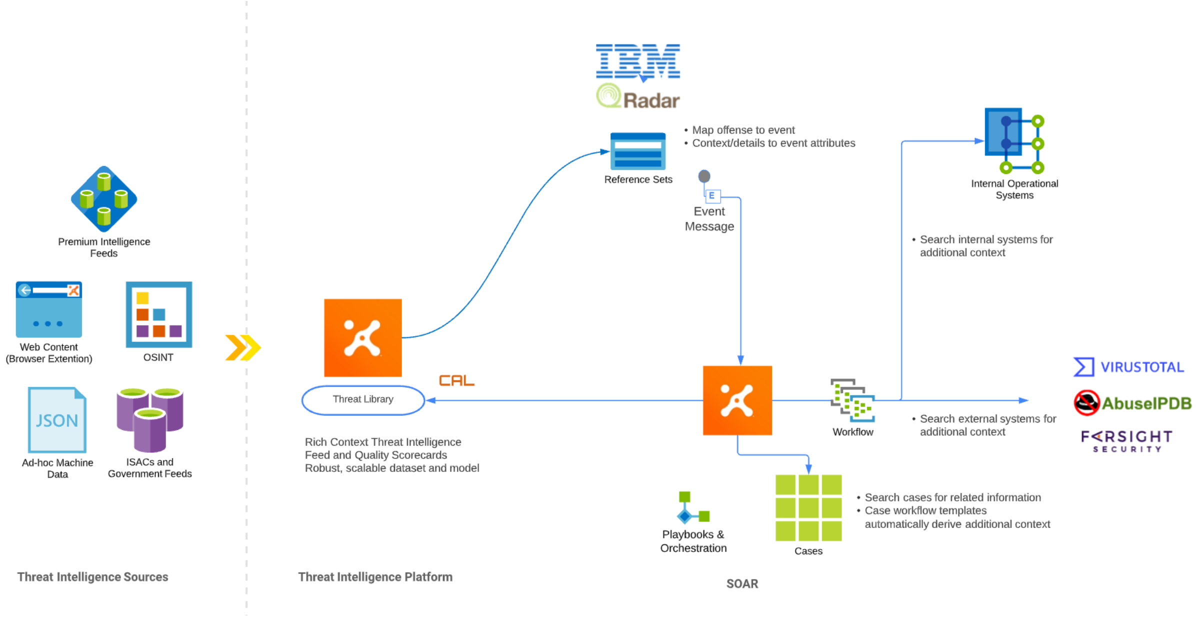

IBM
QRadar
Reference Sets
• Map offense to event
• Context/details to event attributes
E
Event Message
Internal Operational Systems
• Search internal systems for additional context
Premium Intelligence Feeds
Web Content (Browser Extention)
OSINT
JSON
Ad-hoc Machine Data
ISACs and Government Feeds
Threat Library
CAL
Rich Context Threat Intelligence Feed and Quality Scorecards
Robust, scalable dataset and model
Workflow
• Search external systems for additional context
VIRUSTOTAL
AbuseIPDB
FARSIGHT SECURITY
Playbooks & Orchestration
Cases
• Search cases for related information
• Case workflow templates automatically derive additional context
Threat Intelligence Sources
Threat Intelligence Platform
SOAR

Figure 2: Event Prioritization Logical System Diagram

Description

Prerequisite: Configure the SIEM

The preliminary steps in this use case are to install the **IBM QRadar** Custom Trigger Service App via TC Exchange, create a Playbook Service for this App, and load and configure the custom **Alert Triage Event for QRadar** Playbook.

The **IBM QRadar** Custom Trigger Service App functions as a custom Playbook Trigger that allows one or more Playbooks (in this case, the **Alert Triage Event for QRadar** Playbook) to receive a feed of new offenses from QRadar on a defined time interval.

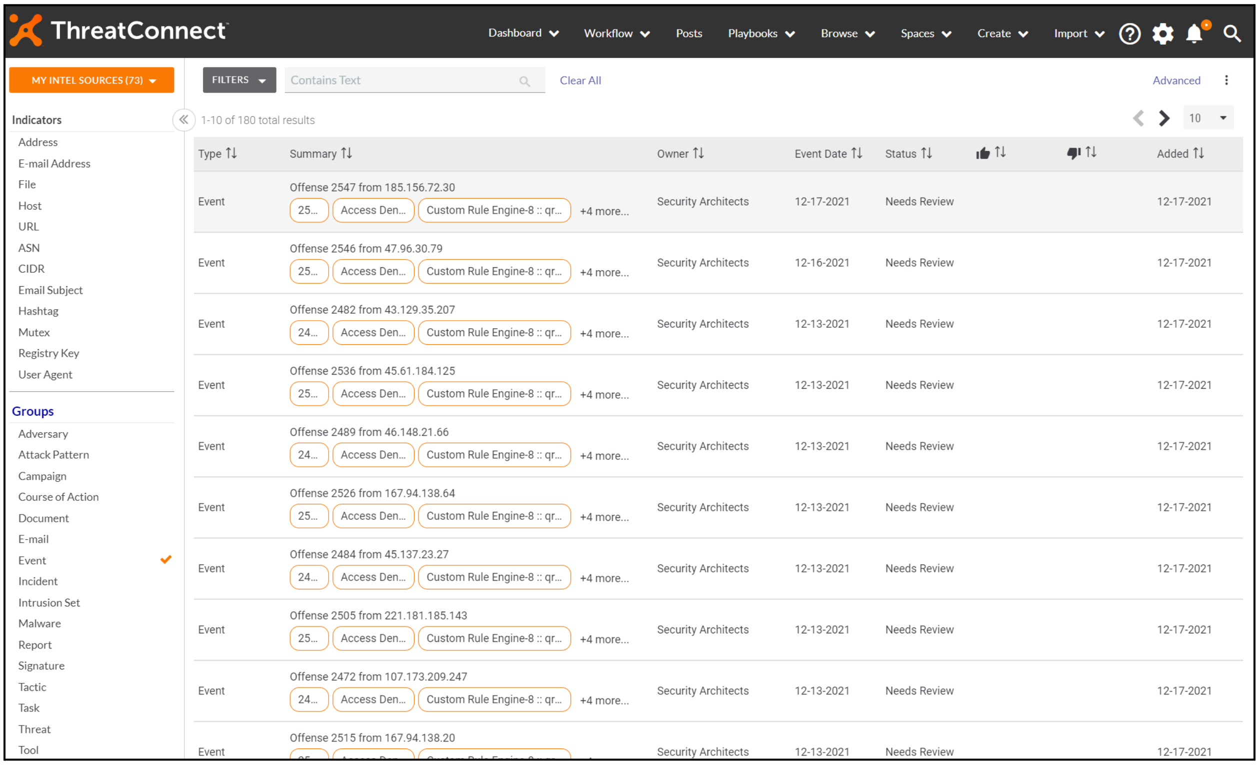
The Playbook requires you to enter a number of self-explanatory variables, such as a QRadar authentication token, which your QRadar administrator can generate for you. The authentication token is required for ThreatConnect to communicate and exchange data with QRadar.

Capture SIEM Event and Initial Context

This use case begins with an event occurring in the environment. An example may be a log recording that access has been denied within a critical system asset, or a connection has been made between an internal server and a host in an unexpected foreign country. In such situations, alerts are typically sent to a SOC analyst to make them aware of the event. This is where automation becomes an analyst's friend.

As event and flow data passes through the QRadar's Custom Rule Engine (CRE), it is correlated against the rules that are configured to validate against the reference set, and an offense is created. Next, ThreatConnect's Playbook logic will translate that offense to an Event Group, associating the Indicator as an observation. The Indicators involved in the event are then subject to the enrichment process, most of which is automated, as discussed in the next section.

Figure 3 displays an event captured in ThreatConnect with the associated observed Indicator.



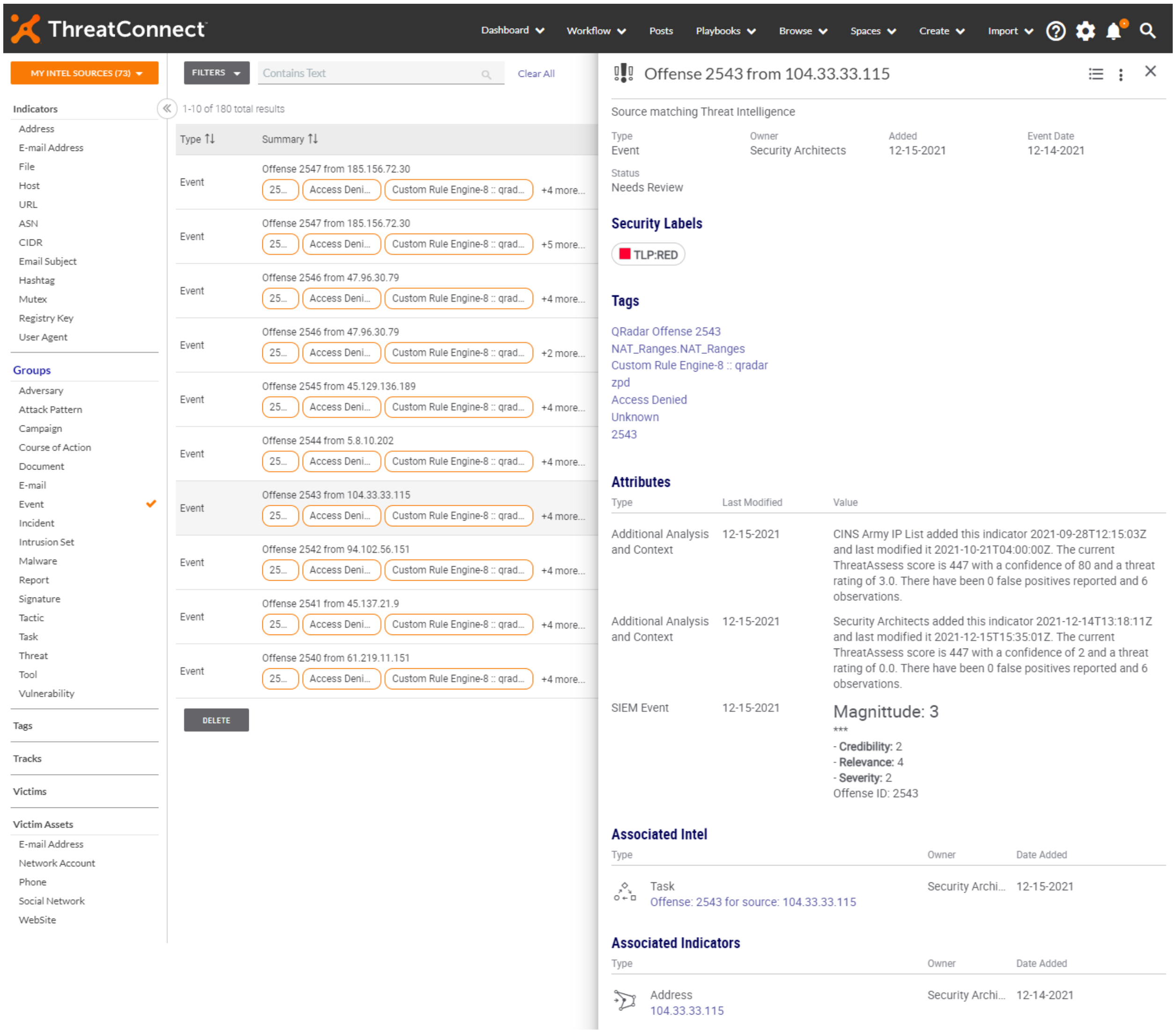
1-10 of 180 total results

Type	Summary	Owner	Event Date	Status	👍	👎	Added
Event	Offense 2547 from 185.156.72.30 25... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-17-2021	Needs Review			12-17-2021
Event	Offense 2546 from 47.96.30.79 25... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-16-2021	Needs Review			12-17-2021
Event	Offense 2482 from 43.129.35.207 24... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2536 from 45.61.184.125 25... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2489 from 46.148.21.66 24... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2526 from 167.94.138.64 25... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2484 from 45.137.23.27 24... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2505 from 221.181.185.143 25... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2472 from 107.173.209.247 24... Access Den... Custom Rule Engine-8 :: qr... +4 more...	Security Architects	12-13-2021	Needs Review			12-17-2021
Event	Offense 2515 from 167.94.138.20	Security Architects	12-13-2021	Needs Review			12-17-2021

Figure 3: Events Captured From SIEM Offenses

Each Event Group contains associated metadata from the offense in QRadar, including the source, credibility, severity, relevance, and magnitude. The QRadar integration automatically translates those scores into comparable Indicator Threat and Confidence Ratings in ThreatConnect, which preserve initial context.

All information collected is added to the Event Group as an **Additional Analysis and Context** Attribute, along with associated intelligence (Group types) and threat Indicators (Figure 4). Analytics from ThreatConnect's Collective Analytics Layer (CAL™) and ThreatAssess are also applied, making it easier for an analyst to reference.



1-10 of 180 total results

Type	Summary
Event	Offense 2547 from 185.156.72.30 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2547 from 185.156.72.30 25... Access Deni... Custom Rule Engine-8 :: qrad... +5 more...
Event	Offense 2546 from 47.96.30.79 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2546 from 47.96.30.79 25... Access Deni... Custom Rule Engine-8 :: qrad... +2 more...
Event	Offense 2545 from 45.129.136.189 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2544 from 5.8.10.202 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2543 from 104.33.33.115 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2542 from 94.102.56.151 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2541 from 45.137.21.9 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...
Event	Offense 2540 from 61.219.11.151 25... Access Deni... Custom Rule Engine-8 :: qrad... +4 more...

Offense 2543 from 104.33.33.115

Source matching Threat Intelligence

Type	Owner	Added	Event Date
Event	Security Architects	12-15-2021	12-14-2021

Status
Needs Review

Security Labels

🟥 TLP:RED

Tags

QRadar Offense 2543
NAT_Ranges.NAT_Ranges
Custom Rule Engine-8 :: qradar
zpd
Access Denied
Unknown
2543

Attributes

Type	Last Modified	Value
Additional Analysis and Context	12-15-2021	CINS Army IP List added this indicator 2021-09-28T12:15:03Z and last modified it 2021-10-21T04:00:00Z. The current ThreatAssess score is 447 with a confidence of 80 and a threat rating of 3.0. There have been 0 false positives reported and 6 observations.
Additional Analysis and Context	12-15-2021	Security Architects added this indicator 2021-12-14T13:18:11Z and last modified it 2021-12-15T15:35:01Z. The current ThreatAssess score is 447 with a confidence of 2 and a threat rating of 0.0. There have been 0 false positives reported and 6 observations.
SIEM Event	12-15-2021	Magnittude: 3 *** - **Credibility:** 2 - **Relevance:** 4 - **Severity:** 2 Offense ID: 2543

Associated Intel

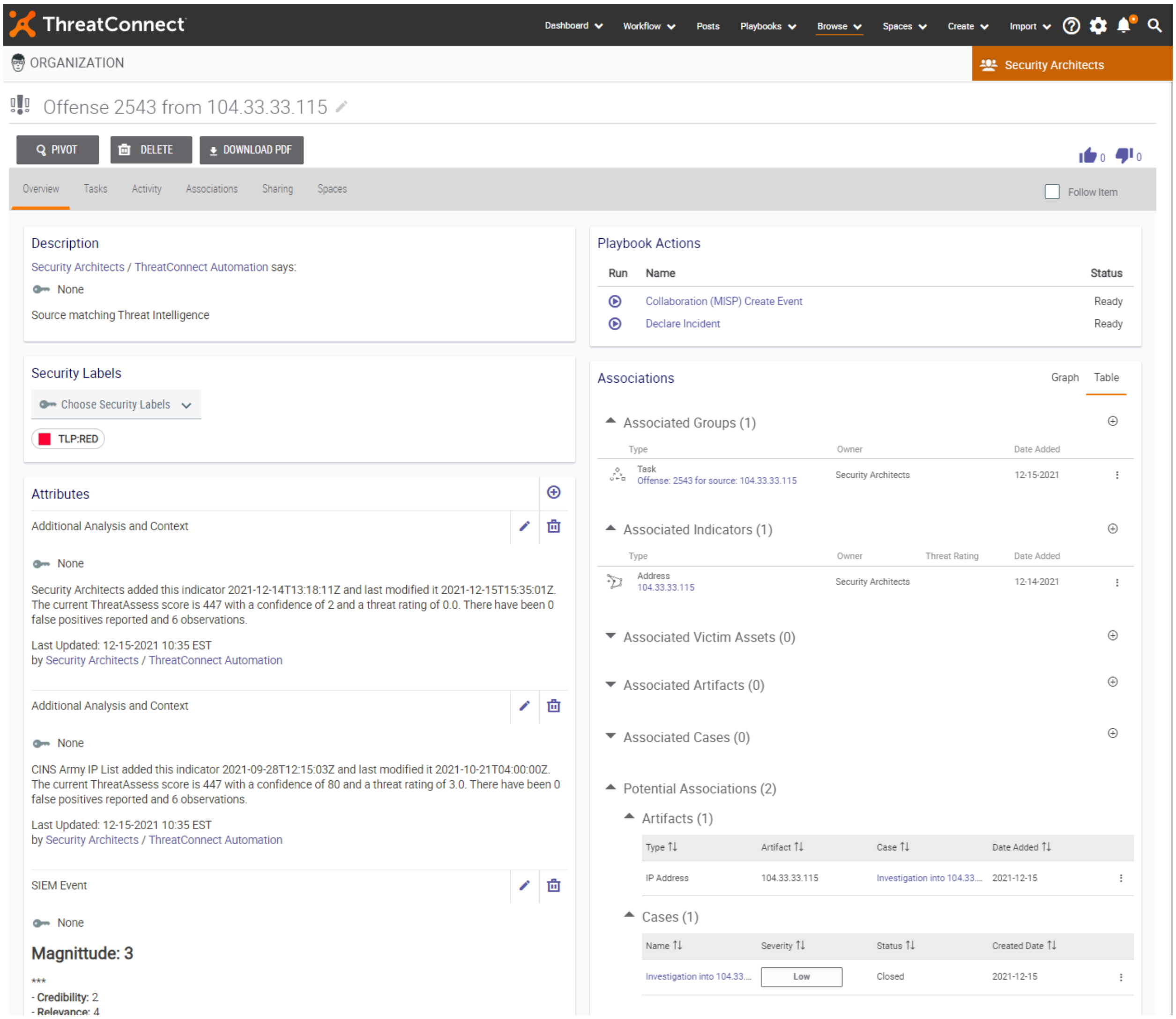
Type	Owner	Date Added
Task Offense: 2543 for source: 104.33.33.115	Security Archi...	12-15-2021

Associated Indicators

Type	Owner	Date Added
Address 104.33.33.115	Security Archi...	12-14-2021

Figure 4: Auto-Generated Context and Associations For an Event Group

Knowing whether threat data in the Event Group has been seen before in previous Cases or correlated events is a major benefit of an integrated threat intelligence platform (TIP) and SOAR capability. We can see all associated and potentially associated Artifacts in other Cases to give more context. Within a single pane of glass, analysts can see the intelligence in terms of severity and context, historical knowledge, previous Cases, and associated threat intelligence data (Figure 5).



Offense 2543 from 104.33.33.115

Description

Security Architects / ThreatConnect Automation says:

None

Source matching Threat Intelligence

Security Labels

Choose Security Labels

🟥 TLP:RED

Attributes

Additional Analysis and Context

None

Security Architects added this indicator 2021-12-14T13:18:11Z and last modified it 2021-12-15T15:35:01Z. The current ThreatAssess score is 447 with a confidence of 2 and a threat rating of 0.0. There have been 0 false positives reported and 6 observations.

Last Updated: 12-15-2021 10:35 EST
by Security Architects / ThreatConnect Automation

Additional Analysis and Context

None

CINS Army IP List added this indicator 2021-09-28T12:15:03Z and last modified it 2021-10-21T04:00:00Z. The current ThreatAssess score is 447 with a confidence of 80 and a threat rating of 3.0. There have been 0 false positives reported and 6 observations.

Last Updated: 12-15-2021 10:35 EST
by Security Architects / ThreatConnect Automation

SIEM Event

None

Magnittude: 3

***

- **Credibility:** 2
- **Relevance:** 4

Playbook Actions

Run	Name	Status
▶	Collaboration (MISP) Create Event	Ready
▶	Declare Incident	Ready

Associations

Associated Groups (1)

Type	Owner	Date Added
Task Offense: 2543 for source: 104.33.33.115	Security Architects	12-15-2021

Associated Indicators (1)

Type	Owner	Threat Rating	Date Added
Address 104.33.33.115	Security Architects		12-14-2021

Associated Victim Assets (0)

Associated Artifacts (0)

Associated Cases (0)

Potential Associations (2)

Artifacts (1)

Type	Artifact	Case	Date Added
IP Address	104.33.33.115	Investigation into 104.33....	2021-12-15

Cases (1)

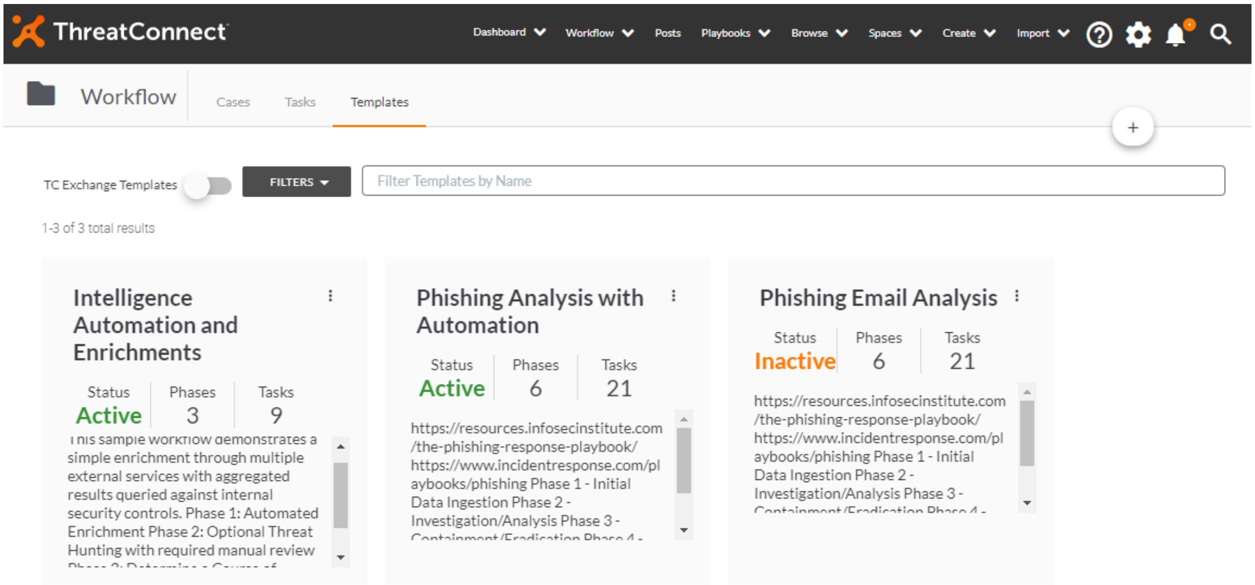
Name	Severity	Status	Created Date
Investigation into 104.33....	Low	Closed	2021-12-15

Figure 5: An Event Group's Details Screen Displaying Potential Associations to Existing Artifacts and Cases

Expand Knowledge With Automated Workflows

In this next phase, ThreatConnect leverages automation to populate the Event Group with additional Attributes that contain relevant contextual information derived from internal and external sources. This is where Workflow and integrated automated Tasks come into play. Typically, SOC analysts perform these steps manually, which can lead to a significant loss of time or results that are lost or forgotten. ThreatConnect's integrated TIP capability are tightly meshed to provide a seamless experience that helps drive operations based on the derived intelligence.

The **Intelligence Automation and Enrichments** Workflow Template (Figure 6) is selected because it contains all steps that analysts researching events typically want to perform. Tasks can be modified and customized as desired, but we're leaning forward in this use case with some of the more popular Tasks.



Intelligence Automation and Enrichments

Status	Phases	Tasks
Active	3	9

This sample workflow demonstrates a simple enrichment through multiple external services with aggregated results queried against internal security controls. Phase 1: Automated Enrichment Phase 2: Optional Threat Hunting with required manual review Phase 3: Determine a Course of

Phishing Analysis with Automation

Status	Phases	Tasks
Active	6	21

https://resources.infosecinstitute.com/the-phishing-response-playbook/ https://www.incidentresponse.com/playbooks/phishing Phase 1 - Initial Data Ingestion Phase 2 - Investigation/Analysis Phase 3 - Containment/Eradication Phase 4 -

Phishing Email Analysis

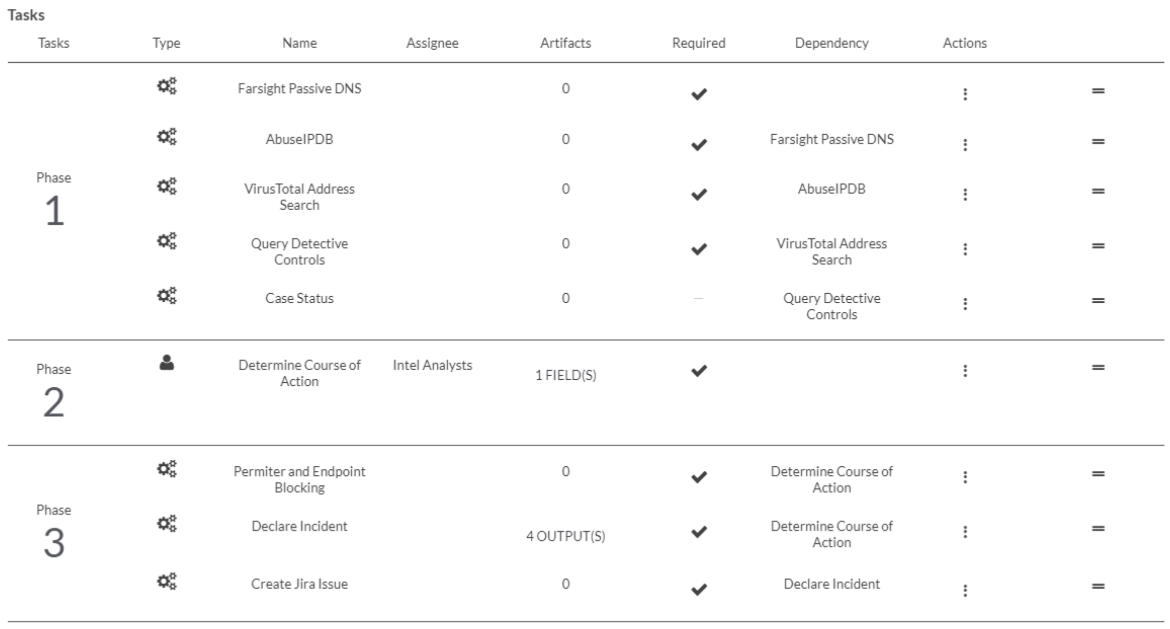
Status	Phases	Tasks
Inactive	6	21

https://resources.infosecinstitute.com/the-phishing-response-playbook/ https://www.incidentresponse.com/playbooks/phishing Phase 1 - Initial Data Ingestion Phase 2 - Investigation/Analysis Phase 3 - Containment/Eradication Phase 4 -

Figure 6: Event Prioritization Leverages the Intelligence Automation and Enrichments Workflow Template

A great thing about Workflow Templates is that they offer analysts a practical way to share tradecraft and integration services. Many times, analysts that are new to the field or your organization may not know when certain enrichments can be helpful or how to leverage an integration service. Workflow Templates serve as a means to provide process and structure to new team members.

Figure 7 provides a listing of the Workflow steps broken down into phases. Phases 1–3 include both manual and automated Tasks that involve enrichment, querying internal systems or detective controls, and automatically adding that information to the Case.



Tasks

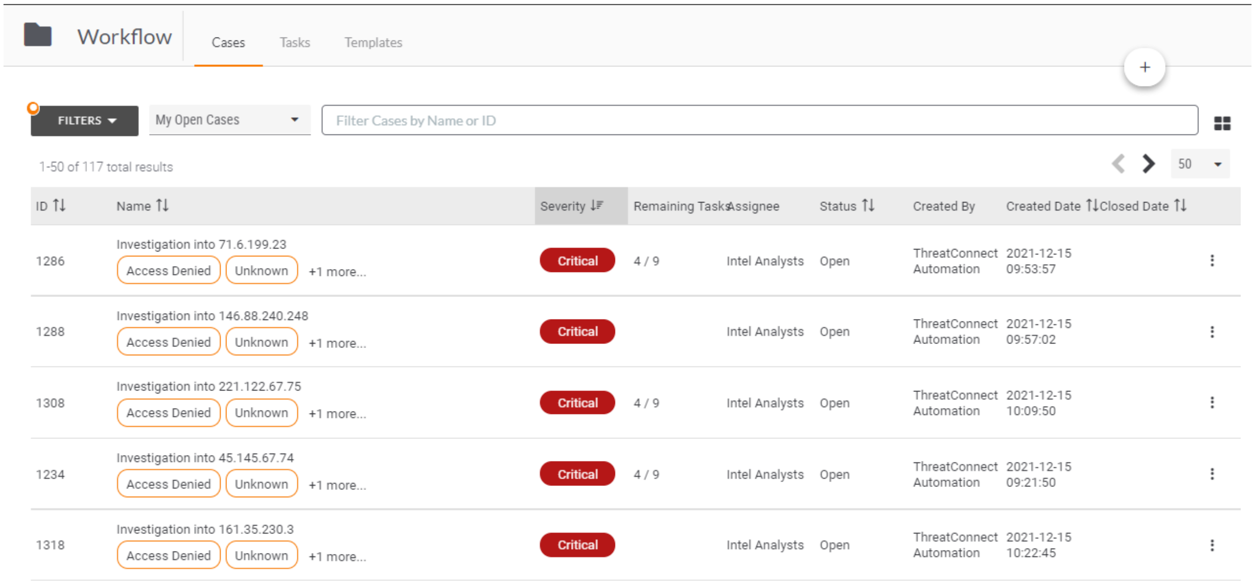
Tasks	Type	Name	Assignee	Artifacts	Required	Dependency	Actions	
Phase 1	⚙	Farsight Passive DNS		0	✓		⋮	═
	⚙	AbuseIPDB		0	✓	Farsight Passive DNS	⋮	═
	⚙	VirusTotal Address Search		0	✓	AbuseIPDB	⋮	═
	⚙	Query Detective Controls		0	✓	VirusTotal Address Search	⋮	═
	⚙	Case Status		0	–	Query Detective Controls	⋮	═
Phase 2	👤	Determine Course of Action	Intel Analysts	1 FIELD(S)	✓		⋮	═
Phase 3	⚙	Permiter and Endpoint Blocking		0	✓	Determine Course of Action	⋮	═
	⚙	Declare Incident		4 OUTPUT(S)	✓	Determine Course of Action	⋮	═
	⚙	Create Jira Issue		0	✓	Declare Incident	⋮	═

Figure 7: Workflow Tasks for Processing Events

Highlight Prioritized Events Within Cases

Workflow Tasks will populate the respective Case with all aggregated details and set the Case's status based on findings. This provides analysts with a prioritized list of Cases to investigate, highlighting the real power of an automation platform where intelligence drives operations and priority. Figure 8 displays a list of Cases that are prioritized based on severity. A Case's severity can be driven by a number of factors, such as insights from CAL, results from threat intel sources, and enrichment services.

The first step is to query existing Cases to determine whether a similar Event Group exists or a related investigation is already underway in ThreatConnect. This background check ensures analysts are leveraging previous work and matching similar events. If a Case is discovered, the Event Group will be associated with that Case; otherwise, a new Case will be created with the Event Group's information populated.



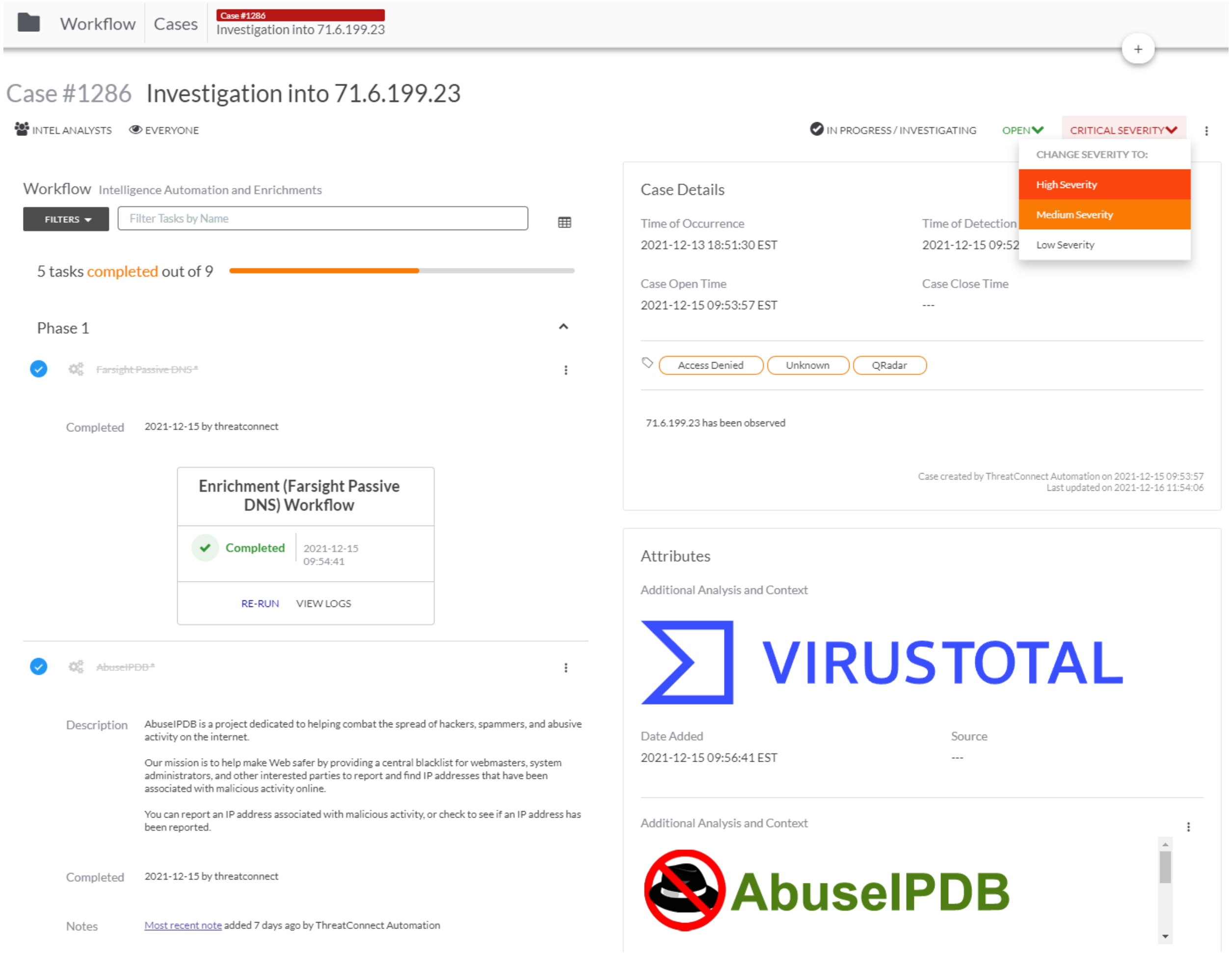
1-50 of 117 total results

ID	Name	Severity	Remaining Tasks	Assignee	Status	Created By	Created Date	Closed Date
1286	Investigation into 71.6.199.23 Access Denied Unknown +1 more...	Critical	4 / 9	Intel Analysts	Open	ThreatConnect Automation	2021-12-15 09:53:57	
1288	Investigation into 146.88.240.248 Access Denied Unknown +1 more...	Critical		Intel Analysts	Open	ThreatConnect Automation	2021-12-15 09:57:02	
1308	Investigation into 221.122.67.75 Access Denied Unknown +1 more...	Critical	4 / 9	Intel Analysts	Open	ThreatConnect Automation	2021-12-15 10:09:50	
1234	Investigation into 45.145.67.74 Access Denied Unknown +1 more...	Critical	4 / 9	Intel Analysts	Open	ThreatConnect Automation	2021-12-15 09:21:50	
1318	Investigation into 161.35.230.3 Access Denied Unknown +1 more...	Critical		Intel Analysts	Open	ThreatConnect Automation	2021-12-15 10:22:45	

Figure 8: Prioritized List of Cases on Which Analysts Can Focus

After a Case is selected, all details for that Case will be displayed (Figure 9). An analyst can select any of the Tasks to highlight the results and review them during the investigation if more information is required before making a decision. Links are also provided as a quick reference to external enrichment services. The goal here is to present as much information as possible to the analyst and enable them to gain confidence during the decision-making process.

After the Case has been declared a threat or incident, it is escalated to the incident response (IR) team so they can respond accordingly. Here, the IR team updates the security controls related to the incident or threat. Some updates may include a combination of perimeter building, review of the incident-handling process, patch management response measures, or improvement of the organization's software development life cycle as it relates to security of the company's website and applications.



Workflow Cases Case #1286 Investigation into 71.6.199.23

Case #1286 Investigation into 71.6.199.23

INTEL ANALYSTS EVERYONE

IN PROGRESS / INVESTIGATING OPEN CRITICAL SEVERITY

CHANGE SEVERITY TO:
High Severity
Medium Severity
Low Severity

Workflow Intelligence Automation and Enrichments

FILTERS Filter Tasks by Name

5 tasks completed out of 9

Phase 1

~~Farsight Passive DNS*~~

Completed 2021-12-15 by threatconnect

Enrichment (Farsight Passive DNS) Workflow

Completed 2021-12-15 09:54:41

RE-RUN VIEW LOGS

~~AbuseIPDB*~~

Description AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the internet.

Our mission is to help make Web safer by providing a central blacklist for webmasters, system administrators, and other interested parties to report and find IP addresses that have been associated with malicious activity online.

You can report an IP address associated with malicious activity, or check to see if an IP address has been reported.

Completed 2021-12-15 by threatconnect

Notes Most recent note added 7 days ago by ThreatConnect Automation

Case Details

Time of Occurrence	Time of Detection
2021-12-13 18:51:30 EST	2021-12-15 09:52
Case Open Time	Case Close Time
2021-12-15 09:53:57 EST	---

Access Denied Unknown QRadar

71.6.199.23 has been observed

Case created by ThreatConnect Automation on 2021-12-15 09:53:57
Last updated on 2021-12-16 11:54:06

Attributes

Additional Analysis and Context

VIRUSTOTAL

Date Added	Source
2021-12-15 09:56:41 EST	---

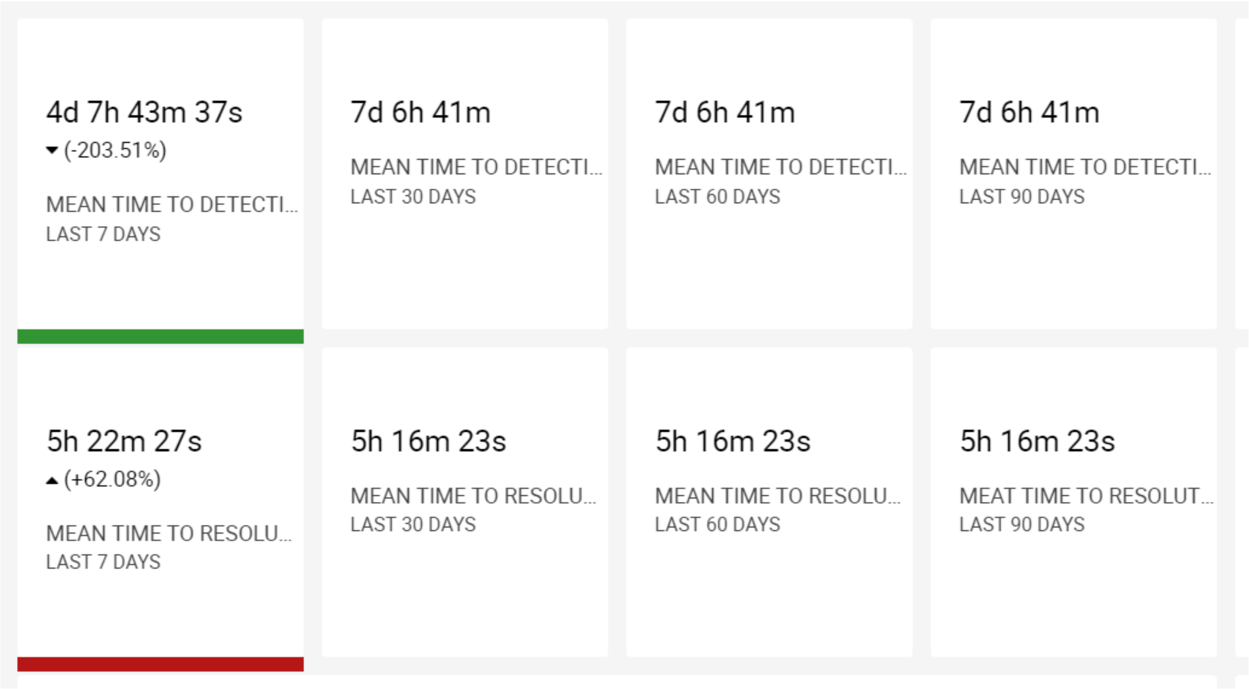
Additional Analysis and Context

AbuseIPDB

Figure 9: Case Involving the Investigation of an Event

The **Case Details** section at the top right of the screen (Figure 9) provides the **Time of Occurrence** (actual timestamp within the event), **Time of Detection** (when the event was discovered by detective tools), and the Case's **Open Time**. These timestamps are leveraged in the computation of MTTD and MTTR so that teams can track their performance in threat detection and resolution over time, which can be presented as statistics within a dashboard for all team members to reference.

While one of this use case's goals is to help prioritize events while providing as much context around the event as possible, the true goal for a SOC analyst is to reduce the time it takes to detect threats overall and resolve those threats. Teams can track those rates and present them in a dashboard, such as the one in Figure 10.



4d 7h 43m 37s
▾ (-203.51%)
MEAN TIME TO DETECTI...
LAST 7 DAYS

7d 6h 41m
MEAN TIME TO DETECTI...
LAST 30 DAYS

7d 6h 41m
MEAN TIME TO DETECTI...
LAST 60 DAYS

7d 6h 41m
MEAN TIME TO DETECTI...
LAST 90 DAYS

5h 22m 27s
▴ (+62.08%)
MEAN TIME TO RESOLU...
LAST 7 DAYS

5h 16m 23s
MEAN TIME TO RESOLU...
LAST 30 DAYS

5h 16m 23s
MEAN TIME TO RESOLU...
LAST 60 DAYS

5h 16m 23s
MEAT TIME TO RESOLUT...
LAST 90 DAYS

Figure 10 : MTTD and MTTR Averages Over the Last 7, 30, 60, and 90 Days

Take a moment to look back at Figure 1, which is a summary dashboard of each key outcome we aim to achieve for analysts. It should now be clear where key metrics, such as MTTD and MTTR, are derived from, and how Workflow and automation can assist in reducing those numbers for teams. Dashboard cards also highlight and provide a classification of events mapped to specific Cases, directing a team's focus each day. Another common metric to compute and present in dashboard cards is the amount of time and effort saved with automation by calculating the number of times Playbooks run versus needing to do so manually.