Incident Detection and Analysis

Last updated by | Justin Bryant | Aug 25, 2023 at 9:17 AM PDT

Incident Detection and Analysis

Contents

We can become aware of incidents in many ways. We can be alerted by monitoring, through customer reports, or by observing it ourselves.

Triage Incident

Once an incident has been detected by a First Responder , the next step is to assess the incident's severity so the team can decide what level of response is appropriate. In order to do that we ask:

Assessment	Response
What is the impact to customers (internal or external or both)?	*e.g. Investigating*
Does this affect (members, partners, consumers, or all)?	*e.g. Investigating*
What are customers seeing? · How many customers are affected (some or all)?	*e.g. Investigating*
When did it start?	*e.g. Date - Time*
Who/what reported the issue?	*e.g. DataDog -> PagerDuty*
How many support cases have customers opened?	*e.g. Investigating*
Are there other factors, e.g., public attention, security, or data loss?	*e.g. Investigating*
Based on the above criteria, what is the Incident Severity?	*e.g. Investigating*

NOTE: This could be pasted into the Incident Reporting Channel and Service Incident Channel and pinned to the top for everyone to see

Utilize the Severity Classification to make the determination based on the questions listed above.

After an initial assessment has been made, if the incident is a (Major Incidents), create a message post in the Incident Reporting Channel with the assessment questions and responses.

Declare Incident

Once and Incident has been detected and assessed by a First Responder , the next step is to Declare Incident within DataDog . You can check if there's an incident already in progress by looking at the DataDog Incident List or the Virtuoso Status Page

- To declare a DataDog incident, please refer to the defined process for DataDog Incident Creation
- During this time, the First Responder will also act as the Incident Manager , until another team member has been escalated and delegated the Incident Manager role.
- After the incident is created, its incident URL must be used in all internal communications about the incident.
- Severity 3, 4, & 5 incidents (Minor Incidents) are assigned to the responsible teams for resolution as appropriate (normally during business hours), whereas Severity 1 and 2 (Major Incidents) require an immediate response and continuous 24/7 management through to resolution.