Incident Response Procedure

Last updated by | Nathan Beier | Jul 25, 2024 at 11:44 AM PDT

Incident Response Procedure

Contents

Child Pages

Stage 1 - Detection and Analysis

1. Monitoring or other alert has detected a potential incident.
   - First Responder can be alerted by DataDog monitoring, PagerDuty on-call pages, through customer reports, or by observing it directly.
2. First Responder performs the triage of the Incident.
   - Assess the incident's Severity Classification
     - If the incident involves PII or Clasified Data being leaked or otherwise compromised, escalate and Page InfoSec team immediately.
   - Post message in Incident Reporting Channel if (Major Incident)
3. Declare Incident within DataDog
   - To declare a DataDog incident, please refer to the defined process for DataDog Incident Creation

---

Stage 2 - Containment and Recovery (Major Incidents Only)

1. Incident Team Channel
   - Incident Manager once the incident is declared, Datadog will automatically create the dedicated Microsoft Team's Incident Channel under the Incident Management Team and link it to newly declared incident
     - Pin the Triage Assessment in the new Incident Channel
     - Share the URL of the incident to the Incident Reporting Channel
     - Spin up a Teams Video Conference within new Incident Channel and add call URL to DataDog Incident
   - If First Responder is unable to resolve issue, escalate to technical leads and tag them in the Incident Channel to engage additional teams, add the appropriate product team to the DataDog incident using the corresponding @mention.
     - Tag the appropriate members in the new Incident Channel. Refer to Technology Product Teams
   - Incident Manager assigns Incident Roles to team members as they join the Video Conference call.
   - Incident Manager records the order of events in the DataDog Incident Timeline as they occur.
2. Initial Notifications
   - For **Internal Notification** , create a post in the MS Team Service Incident Channel
   - For **External Notification** , update Virtuoso Status Page via the StatusPage Login
     - To update Virtuoso Status Page , please refer to the defined process for StatusPage.io
   - Follow-Up Notifications
     - Updating internal staff regularly via Service Incident Channel - (**1x per hour**)
     - Updating S-Team regularly via Email mailto:steam@virtuoso.com - (**1x per hour**)

Stage 2 - Containment and Recovery (Minor Incidents Only)

1. Update DataDog Incident Attributes to include the relevant Technology Teams.
2. Update DataDog Incident Responders to include the relevant Technology Teams members.
3. Create DataDog Incident "New Notification" and specify the relevant Technology Teams by using the facet {@teams-team.alerts-<team name>} to create a DataDog Incident post in that teams designated Alert Channel.
4. Create DataDog Incident "Follow Up Task" to take ownership of the incident and assign Task Owners to Team Leads of the relevant Technology Teams. Set due date for **7 days** of the Incident creation. Also create any additional "Follow Up Task" items as needed, based on the incident details.

Stage 3 - Post-Event Activity

1. Once the Incident has been successfully mitigated, Incident Manager updates DataDog Incident status to "Stable"
2. Update Virtuoso Status Page Product status to "Operational", for final External Notification. Instatus Documentation
3. Send final Internal Notification via Service Incident Channel .
4. Ensure all parties involved have added notes and documentation from the dedicated Incident Channel to the DataDog Incident Timeline for Postmortem.
5. Incident Manager gets accountability for completion of the postmortem.
   - Create any request Incident Task items within the DataDog Incident, and assign Task Owners.
   - Schedule a Postmortem meeting with appropriate Technology Product Teams within **7 days** of incident closure
6. Once the above steps have been completed, Incident Manager updates DataDog Incident status to "Resolved"

Stage 4 - Weekly Incident Review Meeting (IRM)

- The weekly incident review meeting aims to provide a high-level overview of the incidents that occurred during the past week, facilitating cross-team communication, shared understanding, and immediate actions where necessary.
- The meeting will be held weekly at a scheduled time, ensuring regular and consistent review of recent incidents.
- By maintaining a structured yet flexible format, the weekly incident review meeting will help keep all teams aligned, facilitate quick resolutions, and ensure ongoing improvements in incident management processes.
- Incidents that meet certain criteria are identified and a post-incident retrospective (PIR) should be created to discuss the issue in detail.

Stage 5 - Post-Incident Retrospective (PIR)

- Incidents identified in the weekly incident review meeting are discussed in detail in this meeting, specific to the incident.
- By blending the structure of postmortems with the collaborative elements of retrospectives, we can create a more engaging and effective process for learning from incidents and improving team performance.
- For now, the SRE team will execute these meetings when necessary.
- In the future, please follow the process described in the wiki page to run your own PIR.