Incident Containment and Recovery

Last updated by | Shawn Schoenrock | Jun 11, 2024 at 2:26 PM PDT

Incident Containment and Recovery

Contents

This phase focuses on keeping the incident impact as small as possible and mitigating service disruptions. The first goal at this point is to establish and focus all incident team communications in well-known places. The next goal should be creating the initial notifications internally and externally to update stakeholders on the situation. The final goal should be to continue to troubleshoot and mitigate the incident and escalate to additional team members

Containment and Recovery (Major Incidents Only)

1. Datadog will automatically set up the Microsoft Team's Channel dedicated to this particular incident under the Incident Management Team .
   - Add the URL of the Incident Channel to the Production Triage Channel
   - Pin the Triage Assessment in the new Incident Channel
2. The Incident Manager spins up a Teams Video Conference within the Incident Channel and wait for team members who have been paged via PagerDuty based on the established On-Call Schedules to begin joining the call.
   - Add call URL to DataDog Incident
   - From Video Conference, call in First Responder.
   - When the escalated team members engages, they will first come to the Incident Management team channel to start chatting or join the Video chat.
   - The Incident Manager will then delegate an Incident Response Role to them. If they understand what's required of their role, then they will be able to work quickly and effectively as part of the incident team.
3. The Incident Manager begins recording the order of events in the DataDog Incident Timeline as they occur.
4. The Incident Manager creates Initial Notifications and/or continues to update with Follow-Up 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**)
5. If Incident involves PII or Classified Data:
   - First Responder escalates and pages InfoSec Team immediately.
   - The incident is now considered a "Major Security Incident" and all team members should adhere to the Major Security Incident Response Process
6. The First Responder and Team Leads continue to troubleshoot and mitigate the incident.
   - Continuously update Incident Manager on progress and status
7. If First Responder is unable to mitigate 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
8. If Incident duration exceeds X hours:
   - The Incident Response Process should now follow "Long-Term Incident Response Communication Process"
9. Repeat Steps 4-8 until Incident has been mitigated

Containment and Recovery (Minor Incidents Only)

1. The First Responder updates DataDog Incident Attributes to include the relevant Technology Teams.
   - Update DataDog Incident Responders to include the relevant Technology Teams members.
   - 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.
   - 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.
2. The Task Owners / Team Leads follow up on assigned DataDog Tasks
   - Diagnose and Troubleshoot Minor Incident
   - Submit any ADO Bug Issues and/or implement workaround solutions