Categorizing Incident Severities Worksheet

Categorizing incidents is the first step of the incident process and determines the level of urgency as well as the who, how, and frequency of communications that follow. There are 5 severity categories. Additionally, SEV 1 & 2 incidents are subcategorized as **major incidents**:

> An **incident** is any unplanned disruption or degradation of service that is actively affecting customers ability to use your product or service.
>
> A **major incident** is an incident that requires a coordinated response between multiple teams.

For your reference, here are the severity 1-5 criteria:

SEV 1	
Critical issue that warrants public notification and liaison with executive teams.	● The system is in a critical state and is actively impacting a large number of customers. ● Functionality has been severely impaired for a long time, breaking SLA. ● Customer-data-exposing security vulnerability has come to our attention. ● **Major incident response.**
SEV 2	
Critical system issue actively impacting many customers' ability to use the product.	● Notification pipeline is severely impaired. ● Incident response functionality (ack, resolve, etc) is severely impaired. ● App is unavailable or experiencing severe performance degradation for most/all users. ● Monitoring of PagerDuty systems for major incident conditions is impaired. ● Any other event to which a PagerDuty employee deems necessary for incident response. ● **Major incident response.**

SEV 3	
Stability or minor customer-impacting issues that require immediate attention from service owners.	● Partial loss of functionality, not affecting majority of customers. ● Something that has the likelihood of becoming a SEV-2 if nothing is done. ● No redundancy in a service (failure of 1 more node will cause outage). ● High-Urgency page to service team.
SEV 4	
Minor issues requiring action, but not affecting customer ability to use the product.	● Performance issues (delays, etc). ● Individual host failure (i.e. one node out of a cluster). ● Delayed job failure (not impacting event & notification pipeline). ● Cron failure (not impacting event & notification pipeline). ● Low-Urgency page to service team.
SEV 5	
Cosmetic issues or bugs, not affecting customer ability to use the product.	● Bugs not impacting the immediate ability to use the system. ● JIRA ticket.

The above is also available on our Incident Response Ops Guide.

If you find you and your interim team having a debate about how to categorize an incident that's ok! Not all incidents are easy to categorize and may have characteristics that fall into different severity levels. In that case, it's best to err on the side of caution and choose the more severe category and proceed, rather than staying stuck. Incidents can always be recategorized later if they reveal themselves to be more, or less, severe than was initially anticipated.

Issues to Triage

The following are some example incidents to triage. Try to do as many as you can, and we'll review after as a group.

Witnessed Behavior	Severity Level
Employees cannot log into the company VPN, required for all work access.	
Monitoring system triggers an alert due to an increase of 500 errors whenever a certain page, or subset of pages, are accessed on your website.	
Elasticsearch cluster triggers an alert due to "high watermark errors" (disk full on cluster, Elasticsearch cannot store new objects).	
Monitoring system triggers an alert that the primary database is at 100% CPU and RAM usage, as well as other alerts that database queries are failing.	
Chef server offline, chef updates cannot be applied to servers / instances in a specific region. This is preventing necessary package updates from being applied.	
Monitoring system detects that a service's containers are failing and not restarting. The service is critical to your company's business structure.	
Customers are reporting that images aren't loading on your company's website, but the website (seems) otherwise functional.	
While troubleshooting the previous "image loading" issue, you find that DNS is or has started to fail to resolve.	