Incident Severity Classifications

Last updated by | Justin Bryant | Aug 25, 2023 at 9:24 AM PDT

Incident Severity Classifications

Incident severity levels are a measurement of the impact an incident has on the business. Typically, the lower the severity number, the more impactful the incident.

The core value of SEV levels is that they save teams time. A team with severity levels and a clear roadmap for addressing each level is a team that can dive straight into a fix. A team without severity levels is likely to spend the first crucial minutes of a major incident figuring out how important it is, who should handle it, and how to handle it.

Contents

Major Incidents (SEV1/SEV2)

Severity 1 - SEV1

- **Summary**
  - An incident which has incurred significant damage due to loss of confidentiality or integrity of information (personal data), or may cause an interruption in the availability of information and/or processes for an unacceptable period
- **Response Time**
  - Immediate - All hands on deck
- **Operation Examples**
  - Production system outage / compromise
  - Internal system containing sensitive data compromise
  - Significant adverse impact on a large number of systems and/or people
  - Large financial risk or legal liability to Virtuoso
  - Threatens personal/confidential data
  - Adversely impacts a critical enterprise system or service
  - High probability of propagating to a large number of other systems and causing significant disruption
- **Engineering Examples**
  - Site is down
  - Security breach
  - Data disruption given that the cost of the disruption meets a level of revenue loss
- **Data Examples**
  - Data subject to regulatory reporting requirements (Requires InfoSec Team escalation)
  - Data classified as Highly Confidential (Requires InfoSec Team escalation)
- **Accounts Examples**
  - Domain Admins/Global Admins
  - Employees with access to restricted data (Executives, DBAs, executive assistants, Infrastructure Engineering Team

---

Severity 2 - SEV2

- **Summary**
  - An incident which has the possibility of significant damage due to loss of confidentiality or integrity of information (personal data), or may cause an interruption in the availability of information and/or processes for an unacceptable period
- **Response Time**
  - 1 Hour
- **Operation Examples**
  - Production system event
  - Financial systems event
  - Potential significant adverse impact on a large number of systems and/or people
  - Potential large financial risk or legal liability to Virtuoso
  - Potential to threaten personal/confidential data
  - Potential to adversely impact a critical enterprise system or service
  - Potential of propagating to a large number of other systems and causing significant disruption
- **Engineering Examples**
  - Bug does not meet the P1 definition
  - System isn't down but incident is affecting a widespread audience
  - Partial functionality of a product is completely down
  - Business desired date of completion is immediate and cannot be met without developer interaction and directly impacts revenue
  - Incidents without a workaround
- **Data Examples**
  - Sensitive payroll information
  - Business plans / insider info
  - Contractual agreements
  - Data classified as Confidential
- **Accounts Examples**
  - Service Accounts
  - Employee accounts with access to Confidential data

Minor Incidents (SEV3/SEV4/SEV5)

Severity 3 - SEV3

- **Summary**
  - An incident which cannot significantly impact confidentiality or integrity of information, and cannot cause long-term unavailability
- **Response Time**
  - Same Business Day
- **Operation Examples**
  - Systems containing data not intended for public disclosure
  - Intranet data / documentation not approved for external communication
  - Production systems not meeting criteria for High/Critical
- **Engineering Examples**
  - Degradation of service affects a smaller audience
  - Incidents have a complex alternative solution
  - Intermittent workaround is disruptive
- **Data Examples**
  - Data classified as "Protected" (several events)
  - Internal-use only documents (policies)
  - Staff contact info (bulk)
  - Non-S-Team correspondence
  - User guides / SOPs
- **Accounts Examples**
  - Local admin

Severity 4 - SEV4

- **Summary**
  - No incident occurred, but the event related to a system, process or organization may trigger the occurrence of an incident in the future
- **Response Time**

- Next Business Day

- **Operation Examples**
  - Any non-production system not meeting criteria for Medium (Dev/Pre)
  - General user workstations without privilege escalation
- **Engineering Examples**
  - Does not disrupt service
  - Easy alternative solution in place
  - Impacts a small number of users
- **Data Examples**
  - Data classified as "Protected" (single event)
  - Other documents not meeting Medium criteria (Marketing materials, press releases)
- **Accounts Examples**
  - Single non-privileged user account

Severity 5 - SEV5

- **Summary**
  - No incident occurred, but information is worth noting to prevent the occurrence of an incident in the future
- **Response Time**
  - N/A
- **Operation Examples**
  - Logging that represents a potential event that may occur in the future
- **Engineering Examples**
  - Cosmetic issues
  - Affects a single individual
- **Data Examples**
  - Data classified as "Public"
- **Accounts Examples**
  - None

Grid View of Severity Classifications

Classification	Response Time	Operation Examples	Engineering Examples	Data Examples	Accounts Examples
Severity 1 - SEV1	Immediate (All hands on deck)	-Production system outage / compromise -Internal system containing sensitive data compromise -Significant adverse impact on a large number of systems and/or people -Large financial risk or legal liability to Virtuoso -Threatens personal/confidential data -Adversely impacts a critical enterprise system or service -High probability of propagating to a large number of other systems and causing significant disruption	-Site is down -Security breach -Data disruption given that the cost of the disruption meets a level of revenue loss	-Data subject to regulatory reporting requirements -Data classified as Highly Confidential	-Domain Admins/Global Admins -Employees with access to restricted data (Executives, DBAs, executive assistants, Infrastructure Engineering Team
Severity 2 - SEV2	1 Hour	-Production system event -Financial systems event -Potential significant adverse impact on a large number of systems and/or people -Potential large financial risk or legal liability to Virtuoso -Potential to threaten personal/confidential data -Potential to adversely impact a critical enterprise system or service -Potential of propagating to a large number of other systems and causing significant disruption	-Bug does not meet the P1 definition -System isn't down but incident is affecting a widespread audience -Partial functionality of a product is completely down -Business desired date of completion is immediate and cannot be met without developer interaction and directly impacts revenue -Incidents without a workaround	-Sensitive payroll information -Business plans / insider info -Contractual agreements -Data classified as Confidential	-Service Accounts -Employee accounts with access to Confidential data
Severity 3 - SEV3	Same Business Day	-Systems containing data not intended for public disclosure -Intranet data / documentation not approved for external communication -Production systems not meeting criteria for High/Critical	-Degradation of service affects a smaller audience -Incidents have a complex alternative solution -Intermittent workaround is disruptive	-Data classified as "Protected" (several events) -Internal-use only documents (policies) -Staff contact info (bulk) -Non-S-Team correspondence -User guides / SOPs	-Local admin
Severity 4 - SEV4	Next Business Day	- Any non-production system not meeting criteria for Medium (Dev/Pre) - General user workstations without privilege escalation	- Does not disrupt service -Easy alternative solution in place - Impacts a small number of users	-Data classified as "Protected" (single event) - Other documents not meeting Medium criteria (Marketing materials, press releases)	-Single non-privileged user account
Severity 5 - SEV5	N/A	- Logging that represents a potential event that may occur in the future	- Cosmetic issues - Affects a single individual	- Data classified as "Public"	- None