Assignment Day 13

Incident Management

AMULYA AH

Incident management processes are the procedures and actions taken to respond to and resolve incidents. This includes who is responsible for response, how incidents are detected and communicated to IT teams, and what tools are used.

When designed well, incident management processes ensure that all incidents are addressed quickly and that a certain quality standard is maintained. Processes can also help teams improve their current operations to prevent future incidents.

There are five standard steps to any incident resolution process. These steps ensure that no aspect of an incident is overlooked and help teams respond to incidents effectively.

1. Incident Identification, Logging, and Categorization

Incidents are identified through user reports, solution analyses, or manual identification. Once identified, the incident is logged and investigation and categorization can begin. Categorization is important to determining how incidents should be handled and for prioritizing response resources.

2. Incident Notification & Escalation

Incident alerting takes place in this step although the timing may vary according to how incidents are identified or categorized. Additionally, if incidents are minor, details may be logged or notifications sent without an official alert. Escalation is based on the categorization assigned to an incident and who is responsible for response procedures. If incidents can be automatically managed, escalation can occur transparently.

3. Investigation and Diagnosis

Once incident tasks are assigned, staff can begin investigating the type, cause, and possible solutions for an incident. After an incident is diagnosed, you can determine the appropriate remediation steps. This includes notifying any relevant staff, customers, or authorities about the incident and any expected disruption of services.

4. Resolution and Recovery

Resolution and recovery involve eliminating threats or root causes of issues and restoring systems to full functioning. Depending on incident type or severity, this may require multiple stages to ensure that incidents don't reoccur.

For example, if the incident involves a malware infection, you often cannot simply delete the malicious files and continue operations. Instead, you need to create a clean copy of your infected systems, isolate the infected components, and fully replace systems to ensure that the infection doesn't spread.

5. Incident Closure

Closing incidents typically involves finalizing documentation and evaluating the steps taken during response. This evaluation helps teams identify areas of improvement and proactive measures that can help prevent future incidents.

Incident closure may also involve providing a report or retrospective to administrative teams, board members, or customers. This information can help rebuild any trust that may have been lost and creates transparency regarding your operations.

➢ LIFE CYCLE OF INCIDENT MANAGEMENT

This most recent version discusses the 5 steps you should be following throughout an incident management lifecycle:

1. Incident identification
2. Incident logging
3. Incident categorization
4. Incident prioritization
5. Incident response

1. Incident Identification and Logging:

Incident Identification is either done via testing (using tools or otherwise), user feedback, infrastructure monitoring, etc.

Logging an incident simply means recording the following info:

- Exact/Appropriate date and time of occurrence.
- Incident title along with type and brief description
- Name of the person who logged the incident and more detailed description with error codes when applicable
- Details of the person assigned to the incident for follow up
- Current Status of the incident
- Attachments including technical discussions, decisions and approvals

2. Classification and Prioritization:

Classification of incidents helps us partition them based on their type (software, hardware, service request, etc.) so it makes for easier reporting and analysis. Prioritization helps to identify the order/priority of incidents to be

handled. It depends on the impact, severity and most importantly the Risk Factor.

3. Investigation and Analysis
This step is to better understand the problem so we not only fix it right now, but gather information for preventing from re-occurrence.

4. Resolution and Recovery
Steps are taken to remove the incident and bring the system back to its previous working condition.

5. Incident Closure
The resolution is retested and in case the system is working as intended, the incident is closed.

6. Incident Management System
Incident management can very well be done manually or statically using spread sheets but it is much more effective, dynamic and systematic when done via a tool.

TOOLS USED IN INCIDENT MANAGEMENT

ManageEngine ServiceDesk Plus

Zendesk

HaloITSM

BigPanda

OnPage

NinjaRMM

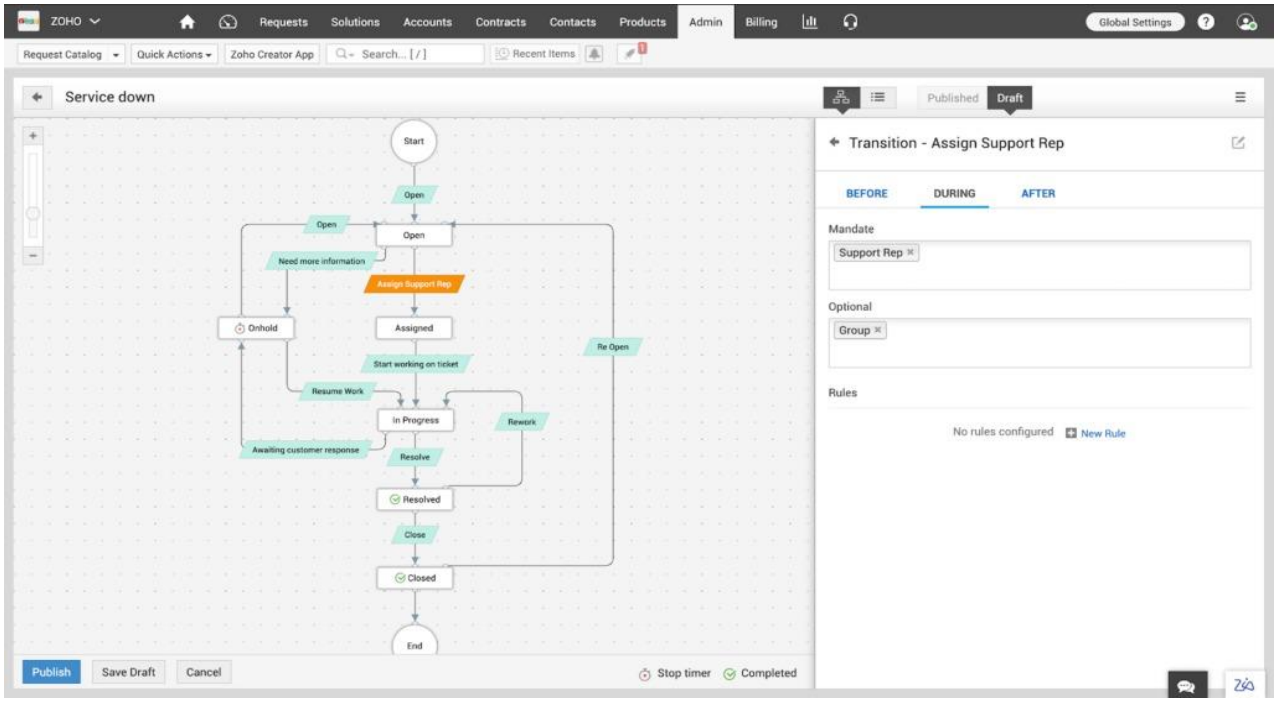
Rundeck

ServiceNow

Issuetrak

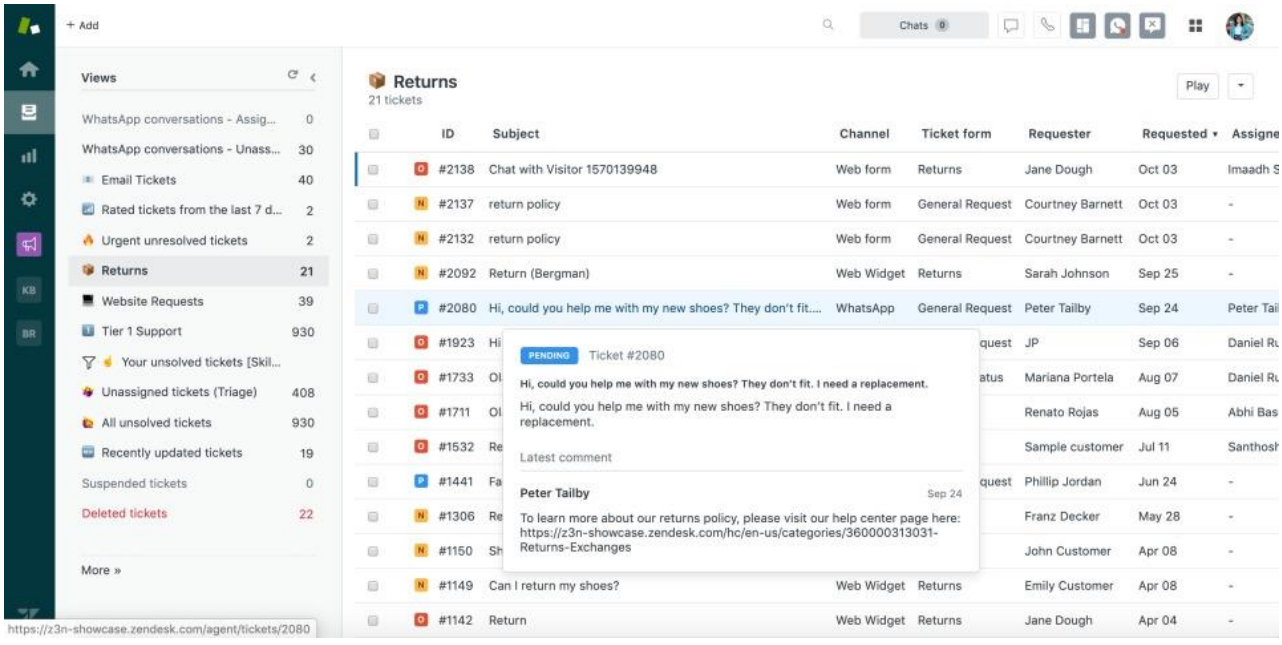
Spiceworks

1.**ManageEngine ServiceDesk Plus** – Best for multi-channel incident logging



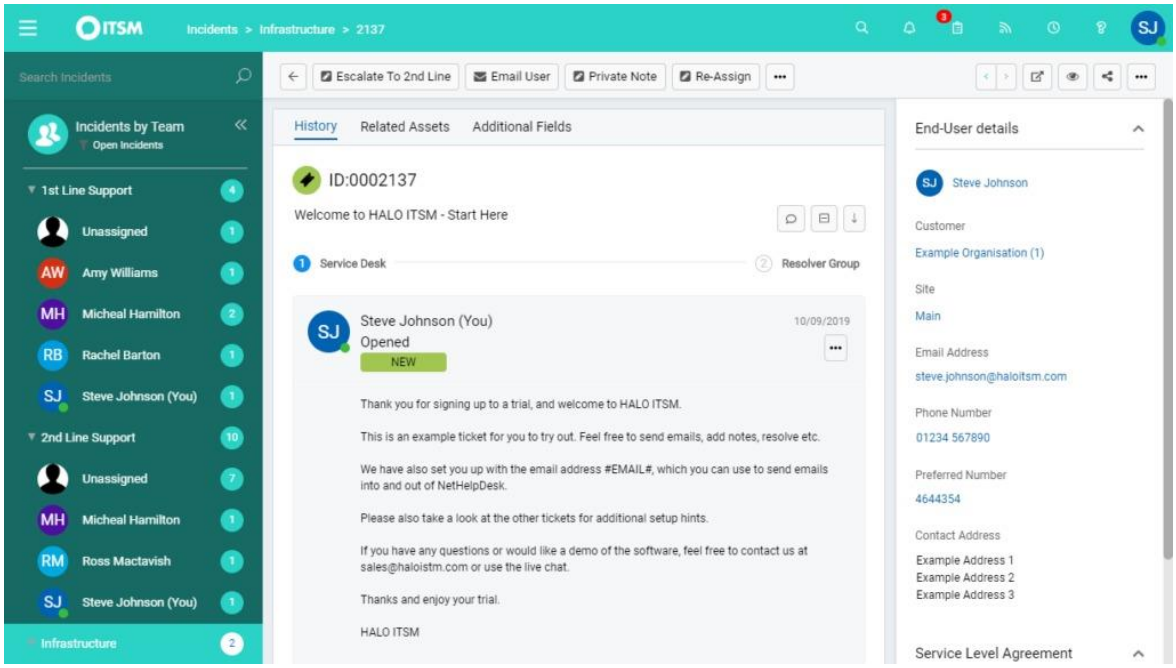
ServiceDesk Plus is the full-stack ITSM solution from ManageEngine, the enterprise IT management division of Zoho Corporation. ServiceDesk Plus has received Pink Elephant's ITIL® 4 compatibility certification for its Incident Management practice, meeting 100% of the evaluation criteria.

2. Zendesk – Best for small to medium businesses



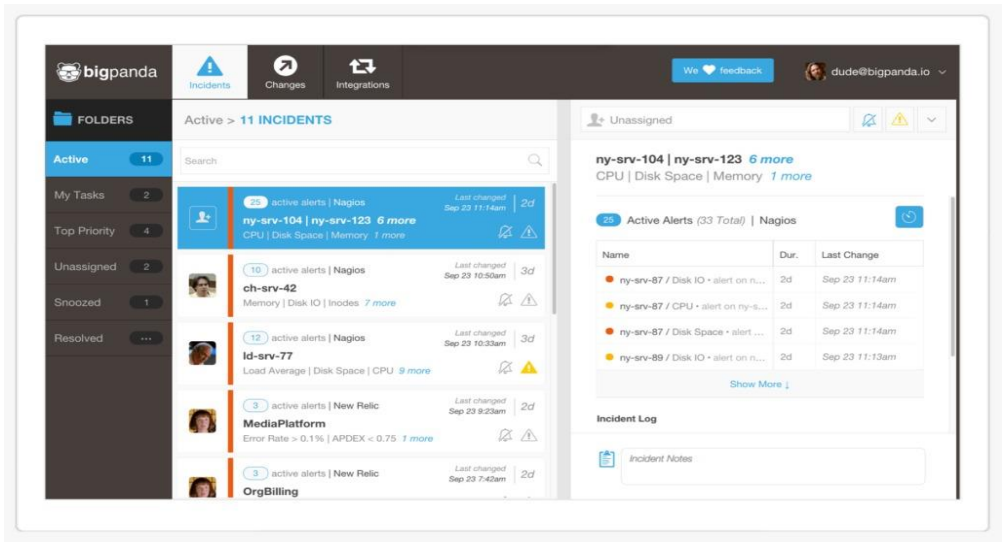
The Zendesk Support Suite allows your team to work seamlessly with a single set of tools and processes that work the same on any channel: email, chat, voice, and even social messaging apps like Facebook, WhatsApp, Twitter, WeChat, and more.

3. HaloITSM – Best for Enterprises



HaloITSM is a leading IT service management (ITSM) solution that can cover all of your service management needs, including incident management and enterprise service management. This award-winning software boasts customers like Siemens, The University of Cambridge, NHS, and Suzuki.

4. BigPanda – Best for machine learning and autonomous operations



BigPanda's autonomous operations platform can help capture alerts, changes, and topology data from all your tools and uses machine learning to detect problems and identify their root cause in real-time so that users have fewer outages and faster resolution.

5. OnPage – Best for usability and customer support

OnPage is the industry-leading HIPAA to secure an incident alert management system. Built around the incident resolution lifecycle, the platform enables organizations to get the most out of their digitization investments, ensuring that sensors and monitoring systems and people have a reliable means to escalate abnormality notifications to the right person immediate