TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

MD Nazmul Hasan 175356IDCR

Design and Implementation of an Automated IT Incident Management System for Small and Medium-Sized Enterprises

Diploma thesis

Supervisor: Md Muhidul Islam
Khan
PHD

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

MD Nazmul Hasan 175356IDCR

Väikeste ja keskmise suurusega ettevõtjate it-intsidentide automaatse haldamise süsteemi kavandamine ja rakendamine

Diplomitöö

Juhendaja: Md Muhidul Islam Khan
PHD

Tallinn 2021

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: MD Nazmul Hasan

07.01.2021

Abstract

IT Incident management is an important part of IT service management. Effective incident management requires a clear incident model, realistic service level agreements, and appropriate incident management systems. The ITIL recommendation for Incident Management can be implemented without special software. This can be challenging over time if an incident occurs quite frequently. A dedicated incident management system can improve the overall uptime of the service. Finding and implementing an incident management system can be challenging for any team.

The goal of this thesis is to find an available system that can automate most of the incident management process. The first part of the thesis will discuss the incident management process and how to evaluate the best incident management system available. The second part of the thesis will discuss open-source alternatives as well as the design and implementation of a custom system to automate incident management. This thesis will discuss possible best practices for incident management for both large enterprises and startups or small teams. The overall outcome of this work will be to improve incident management, reduce digital service downtime, and reduce costs.

This thesis is written in English and is 30 pages long, including 8 chapters, 15 figures and 2 tables.

Annotatsioon

Väikeste ja keskmise suurusega ettevõtjate it-intsidentide automaatse haldamise süsteemi kavandamine ja rakendamine

IT-intsidentide haldamine on IT-teenuste haldamise oluline osa. Tõhus intsidentide haldamine nõuab selget juhtumimudelit, realistlikke teenusetaseme kokkuleppeid ja asjakohaseid intsidentide haldamise süsteeme. ITIL soovitust intsidentide haldamiseks saab rakendada ilma spetsiaalse tarkvarata. See võib olla keeruline aja jooksul, kui vahejuhtum esineb üsna sageli. Spetsiaalne intsidentide haldamise süsteem võib parandada teenuse üldist tööaega. Intsidentide haldamise süsteemi leidmine ja rakendamine võib olla iga meeskonna jaoks keeruline.

Selle teeson eesmärk on leida saadaval süsteem, mis võib automatiseerida enamiku intsidentide haldamise protsessi. Tööes i esimeses osas käsitletakse intsidentide haldamise protsessi ja seda, kuidas hinnata parimat võimalikku intsidentide haldamise süsteemi. Teine osa töös arutab avatud lähtekoodiga alternatiive, samuti töötada ja rakendada kohandatud süsteemi automatiseerida intsidentide haldamine. See tööon arutab võimalikke parimaid tavasid intsidentide haldamiseks nii suurettevõtete kui ka idufirmade või väikeste meeskondade jaoks. Selle töö üldine tulemus on parandada intsidentide haldamist, vähendada digitaalteenuste seisakuid ja vähendada kulusid.

See lõputöö on kirjutatud inglise keeles ja on 30 lehekülge pikk, sealhulgas 8 peatükki, 15 joonist ja 2 tabelit.

List of abbreviations and terms

IM	Incident Management
ITIL	IT Infrastructure Library
ITSM	Information Technology Service Management
SLA	Service-level agreement
PHP	Hypertext Preprocessor
VM	Virtual machine
vCPU	Virtual central processing unit
SaaS	Software as a service

Table of contents

List of figures

List of tables

1 Introduction

Effective IT incident management is often neglected by small IT teams [1]. The main reason is the lack of resources and trained personnel. Small IT teams usually focused on service development. When they move the service from the test system to the production system, many things can go wrong. One of the most important things in planning for adequate computer resources. If the application gets many more users than expected, the computing resources like CPU, RAM & memory could fill up very quickly. This can lead to unexpected downtime. There are always innovative security attacks by hackers which are very difficult to predict even for an experienced IT team.

It is not uncommon for overloads in IT systems to lead to unexpected failures as well as cyber-attacks. In the IT world, unexpected service downtime happens all the time. This is also very common in IT huge companies like Microsoft, Google, Facebook, etc. Large companies usually deploy adequate resources to mitigate IT incidents as soon as possible. In most cases, end users are not directly impacted. However, for startups and small businesses, IT incident handling can be challenging. A lack of resources and experience is the main reason. For effective incident handling, a well-defined incident policy must be in place. As well as trained personnel to mitigate unexpected service outages. A proper incident management tool can make any incident manager's job easier. In a small team, a single person usually handles an incident. He or she has to do a lot of things, such as communicate with business users, resolve the issue, create an incident report, and publish it. Without a proper incident management tool, completing all of these tasks can be very time-consuming. This can lead to additional costs for the company. In the worst-case scenario, it can also violate the service level agreement (SLA) with the business users. This means that customers can ask for a refund or other additional services.

The world is currently experiencing a global COVID -19 pandemic. This pandemic is putting pressure not only on the health care system, but also IT infrastructure. As billions of people are forced to work from home, the use of Internet-based services is skyrocketing. Online video streaming services such as Netflix and YouTube are forced to reduce the quality of videos to reduce the load on their IT infrastructure. The following figure [2] from Network Times shows the increasing use of social networking apps.

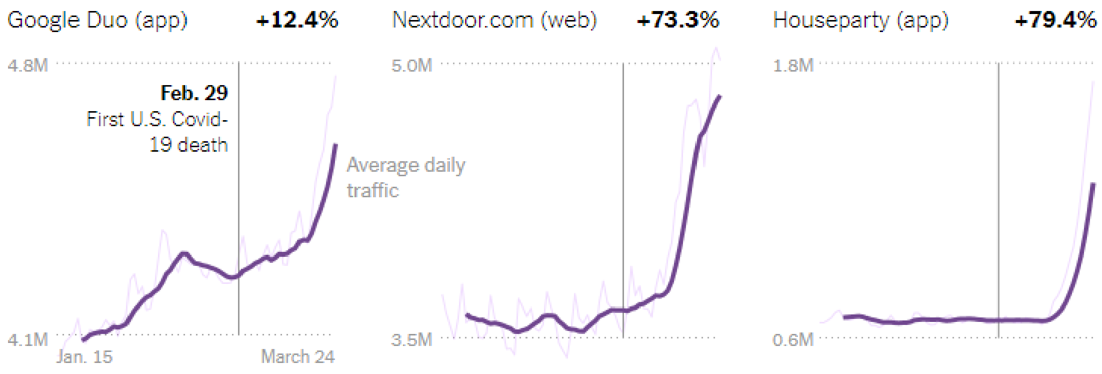


Figure 1: Uses Percent change from January to March

According to a survey by PagerDuty, more than 80% of businesses have experienced stress with digital services since the pandemic began in March 2020. [3] The same companies reported a 47% increase in daily incidents. These facts prove why companies should make efforts to improve the incident management process.

The aim of this thesis is to find an effective incident management system. It emphasizes small and medium-sized enterprises to have an effective incident management policy as well as automating incident management processes by using commercial solutions, open-source solutions, and a mix of custom solutions based on their specific needs. By automating parts of the incident management process, organizations can save time and money [4]. The reliability of digital services will increase.

2 Incident Management process

ITIL (Information Technology Infrastructure Library) describes incident management (IM) as “the incident management process ensures that normal service operation is restored as quickly as possible and the business impact is minimized.” [5]

Here is the list of common ITIL incident management activities [6]:

- Detecting and recording incident details
- Matching incidents against known problems
- Resolving incidents as quickly as possible
- Prioritizing incidents in terms of impact and urgency
- Escalating incidents to other teams to ensure timely resolution

Incident management collaborates with other service management processes [7]. Common service management includes:

- Change management
- Problem management
- Service asset and configuration management
- Service level management

2.1 Components of incident management

According to ITIL, the main goal of incident management is to solve the raised issue as quickly as possible. It does not deal with post-incident activities like root cause analysis or problem resolution.

An established incident management process adds extra value to an organization. It creates the possibility to resolve an incident within a predefined timeframe. It also defines clear roles for support staff, SLA requirements & incident prioritization. These are integral parts of operational incident management [8]:

- Service level agreement
- Incident models(templates)
- Incident categories
- Incident statues and priorities
- Response process for major incidents
- Roles in incident management

In February 2019 ITIL version was introduced, the new ITIL 4 guidelines are pretty much like ITIL version 3. In ITIL 3 the incident escalation process recommendation was a tier-based system. But in ITIL 4 introduces Swarming based incident management. The idea behind Swarming is to manage an incident by the collaboration of different experts together [9].

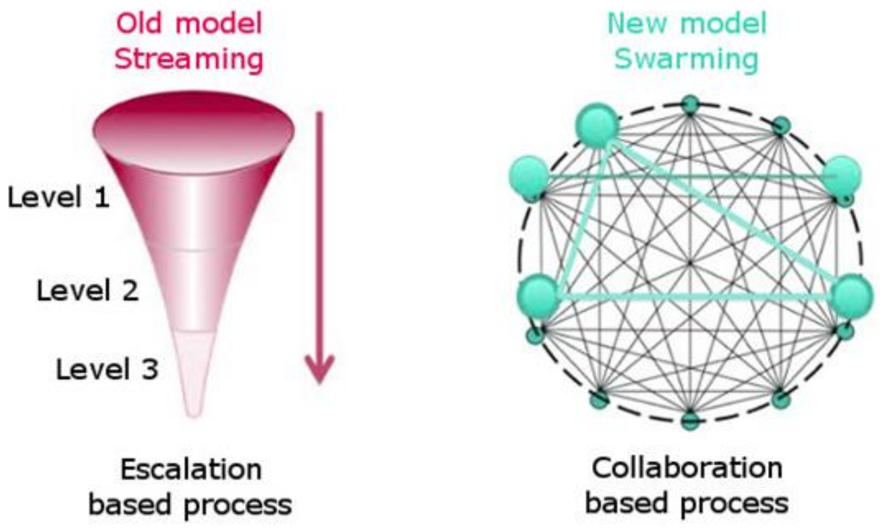


Figure 2: ITIL 3 vs ITIL 4

2.2 Incident management steps

ITIL recommends incidents should follow a structured workflow with combined interest from digital service provides & customers. ITIL provides these steps [10]:

- Incident Identification
- Incident logging
- Incident categorization
- Incident prioritization
- Incident response
    - Initial diagnosis
    - Incident escalation
    - Investigation and diagnosis
    - Resolution and recovery
    - Incident closure

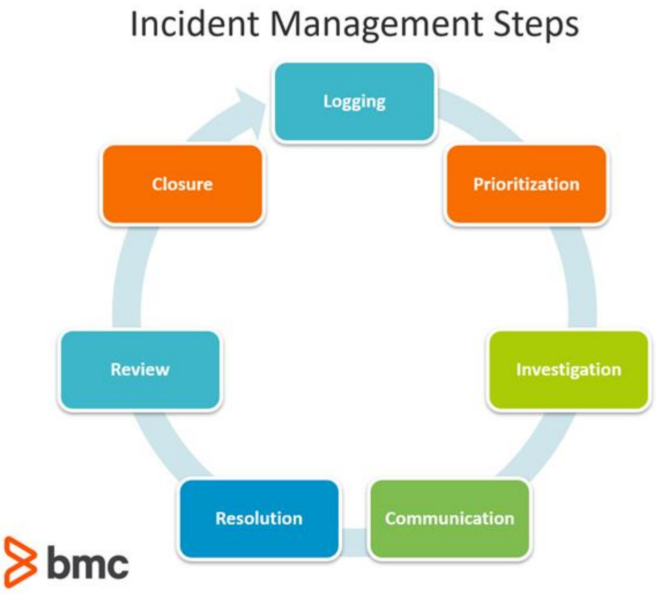


Figure 3: ITIL incident management steps [11]

The above processes outlined efficient incident handling that can help to maintain maximum possible uptime for digital services.

Every incident is not critical, in that regard incident prioritization is a vital step. Incident priority should be based on business impact & urgency. A simple incident can be resolved by first level support team or simple automation. Incident prioritization categorized as:

- Low-priority incidents or Severity 3
- Medium-priority incidents or Severity 2
- High-priority incidents or Severity 1

Incident response should use incident statuses. Incident statuses reflect the incident process. It is also vital in incident communication. Incident statues include:

- New
- Assigned
- In progress
- On hold or pending
- Resolved
- Closed

By following these processes an incident can be handled effectively. Incident logging provides vital data to track incident types and resolution.

2.3 Importance of automating incident management process

In order to understand the importance of incident management, it would be better to look at real incident data from an IT team. In this thesis, data from a team, which manages a mission-critical application of a large corporation will be presented. For security reasons, the details of the team or application will not be shared.

The following table represents the number of incidents & total downtimes during the period 2018 to 2020:

Year	Total incident	Low-priority incidents	Medium-priority incidents	High-priority incidents	Total Downtime
2018	5	2	2	1	58
2019	8	1	6	1	64
2020	11	8	3	0	79

The team almost follows the ITIL best practice during incident handling. The team selects one person for 24/7 on-call duty weekly. This team like another team in the same office doesn’t use any full fledges incident management solutions. It only uses commercial software for on-call management. The rest of the incident management process like incident communication, incident announcement, the incident resolution is done manually by the engineer responsible for on-call duty in that week. The one person must do multiple tasks during an incident, it usually takes a bit longer time to resolve the issue.

In this kind of situation, the team can automate the following process for faster service availability & incident resolution.

- One-click predefined incident announcement via email
- Store all incidents data in a database
- One-click incident status update
- Crete automating incident timeline form the incident status update
- Automated incident report

Otherwise, it can also use feature-rich incident management solutions like PagerDuty, OpsGenie, or xMatters. In later chapters, the commercially available & open-source alternatives will be discussed.

3 Evaluation of existing IM Solution

One of the main goals of this thesis is to find the most effective exiting incident management tool. These tools will be evaluated on based following criteria:

- ITSM Incident management best practices
- Incident communication
- Ease of use
- On-premise and cloud solution
- Integration with logging & monitoring solution
- Cost

Based on online recommendation this dissertation will compare the following incident management software based on the criteria mentioned above:

- OpsGenie
- PagerDuty
- Xmatters

3.1 Overview of OpsGenie, PagerDuty, Xmatters

3.1.1 OpsGenie

OpsGenie is an alerting and incident management system from the company Atlassian. Atlassian has some of the most popular software solutions like Jira, Bitbucket & Confluence in the IT world. Atlassian marketed OpsGenie in short as “Modern incident response” [12]. Here are some of the features of OpsGenie:

- Alerting

- On-call management & escalations
- Reporting & analytics
- Integrates with over 200 monitoring, ITSM, Chatops & collaboration tools.
- On-premise & cloud solution

3.1.2 PagerDuty

PagerDuty an American SaaS based IT incident response system provider company. It marketed as "PagerDuty is the central nervous system for your digital ecosystem." [13] It has the following features:

- On-call management
- Incident response
- Event Intelligence
- Analytics
- Integrated with 370+ solutions

3.1.3 Xmatters

Xmatters is an American start-up that provides incident management solution. It marketed itself as "Introducing adaptive incident management for a changing world" [14]. It has the following features:

- IT event Management & Notifications
- Integration Platform
- On-call Management
- Workflow & process automation
- Analytics

3.2 Feature Comparison of OpsGenie, Pagerduty, Xmatters

This table has been composed based on data from Saasworthy [15], Stackshare [16], IT central station [17] & Capterra [18]. Each of these websites provides a vendor-independent feature review.

Features	PagerDuty	xMatters	OpsGenie
Audit Trail	No	Yes	Yes
Auto-Assign (Incidents)	Yes	No	No
Corrective & preventive action (CAPA)	No	No	NO
Disaster Recovery	No	Yes	Yes
Enriched Notifications	Yes	Yes	Yes
Incident Prioritization	Yes	Yes	Yes
Incident Reporting	Yes	Yes	Yes
Real-time Dashboard	Yes	Yes	Yes
Root-cause Diagnosis	No	No	No
Safety Management	No	Yes	No

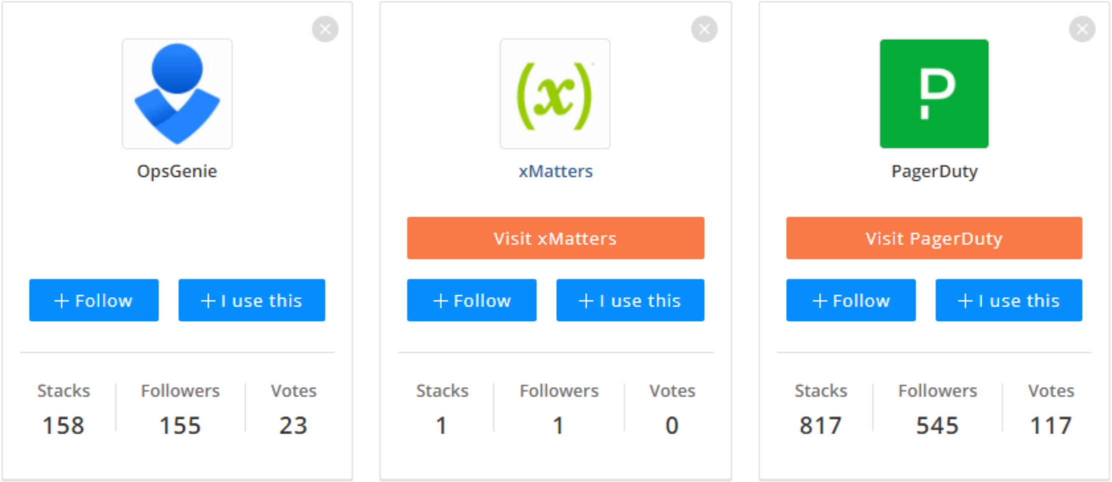
Task Management	No	Yes	No
Ticket Management	Yes	Yes	No
API	Yes	Yes	Yes
Cloud	Yes	Yes	Yes
On-premise	No	No	No
Open-source	No	No	No
Subscription	Yes	Yes	Yes
Free Trial	Yes	Yes	Yes
Freemium	Yes	Yes	Yes

4 Use cases of exiting solution in companies

In this section, the adoption rate & use cases of OpsGenie, Pagerduty & Xmatters will be discussed. Primarily the independent software rating & comparison site data will be used. Data from two popular websites stackshare.io & saasworthy.com will be used to determine the popularity and user acceptance rate of these IM solutions.

Stackshare is a unique platform where developers & companies share their technology stack. Users also can vote, share their reviews & compare almost any software solution. Stackshare doesn't have its rating system rather it aggerate user-provided review, vote & other information.

At the time of writing this thesis in November 2020, according to stackshare.io [19] the most popular IM system is Pagerduty. Pagerduty has been reportedly used by 392 companies including Slack, Stripe, and GitHub. OpsGenie is in the second position, which is reportedly used by 74 companies Tokopedia, Immowelt AG, and Queue-it. Xmattters the newly listed tool in satckshare.io. So, it doesn't have enough data in stackshare.io to compare against other tools.



	Stacks	Followers	Votes
OpsGenie	158	155	23
xMatters	1	1	0
PagerDuty	817	545	117

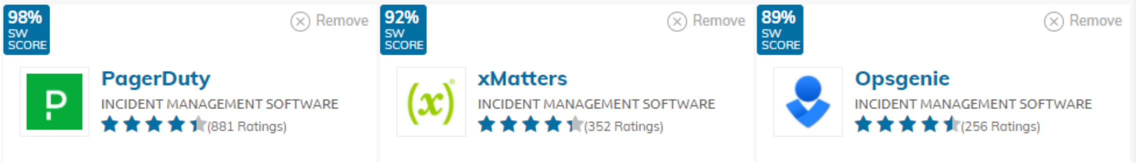
Figure 4: Stackshare comparison [20]

Another very popular software rating site saasworthy.com. Saasworthy has a sophisticated rating system. It called their rating system as SW score [21]. Saasworthy rate a software based on the following six criteria:

- Product features

- User ratings
- Social media presence
- Web presence
- Velocity

In saasworthy.com Pagerduty has the height SW score of 98%. Xmatters has SW score of 92 % followed by OpsGenie which has 89% of SW score.



98% SW SCORE ⊗ Remove

PagerDuty

INCIDENT MANAGEMENT SOFTWARE

★★★★½(881 Ratings)

92% SW SCORE ⊗ Remove

xMatters

INCIDENT MANAGEMENT SOFTWARE

★★★★½(352 Ratings)

89% SW SCORE ⊗ Remove

Opsgenie

INCIDENT MANAGEMENT SOFTWARE

★★★★½(256 Ratings)

Figure 5: Saasworthy comparison

Based on the data from Stackshare & Saasworthy, Pagerduty has the highest rating & users. Xmatters & OpsGenie are quite close to each other in the same perspective.

The 12 months Google trend shows a potential user also has lots of interest in PagerDuty followed by OpsGenie & Xmatters.

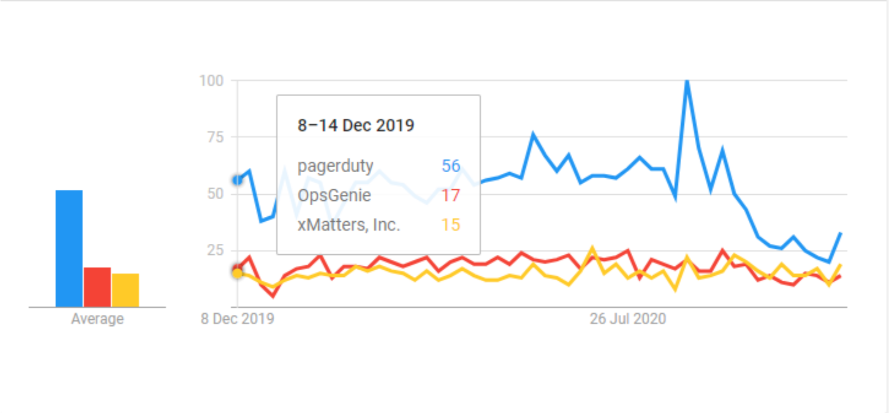


Figure 6: Google treads of PagerDuty, OpsGenie & Xmatters from Dec 2019 to Dec 2020 [22]

5 Demand for a custom tool

From the above chapters, it has been clear that commercially available incident management solutions come with notable complexity & cost. This software needs to be maintained, need to integrate with other software solutions the company already using. For a small team or start-up with limited manpower that can be a changeling. Also, all these solutions come with a lot of features that may not be needed for a small team. By contrast, for medium to large corporations, these solutions could be very impactful.

According to Cyber Security Breaches Survey 2018, about 82% and 70% of small– and medium-sized organizations do not have an incident response policy [23]. On the other hand, 43% of cyber-attacks target small companies. In order to maintain incidents, a small team or start-up can create a custom tool that can integrate with their IT service seamlessly. Simple incident management solutions will reduce cost & complexity. In recent research published by xMatters, 72.3% of respondents reported that half of their team’s time spent resolving incidents [24]. The traditional approach for IM trends to be time-consuming. Automation in the IM process can help reduce the time spent for IM, thus it drives innovation for service development stated in the same research.

6 Design of a custom tool using the open-source system for automating IM

Small teams or startups can design and develop their own IM tool to automate parts of the incident management lifecycle. It will solve the most common incident scenarios they face or will face. Right now, there is no full-fledged open-source incident management system. But many open-source tools can be used by integrating with each other to create a very effective open-source incident management solution. Artificial intelligence can also help to automate some critical parts of incident management [25]. This chapter discusses the various open-source systems that can be used to automate all or parts of incident management.

The parts of automating incident handling could be divided into the following parts [26]:

- Logging, Monitoring & Alerting
- On-call management
- Incident communication
- Post-incident documentation
- Root cause Analysis
- Security incidents

6.1 Logging, Monitoring & Alerting

In order to predict any potential issue for any IT service logging & monitoring solution can tell a lot about the health of the application. This part of incident management is the easiest to implement. There are already very good free logging & monitoring solutions are in the IT space.

The Elastic stack is notable logging and partly monitoring solution. It consists of Elasticsearch, Logstash/Beats & Kibana [27]. Elasticsearch is a very powerful Apache Lucene based search engine. Logstash & Filebeat process & carry logs for Elasticsearch.

Kibana is the visual dashboard. Here is a diagram of Elastic stack collecting logs from Nginx, Apache server & an application written in GO programming language.

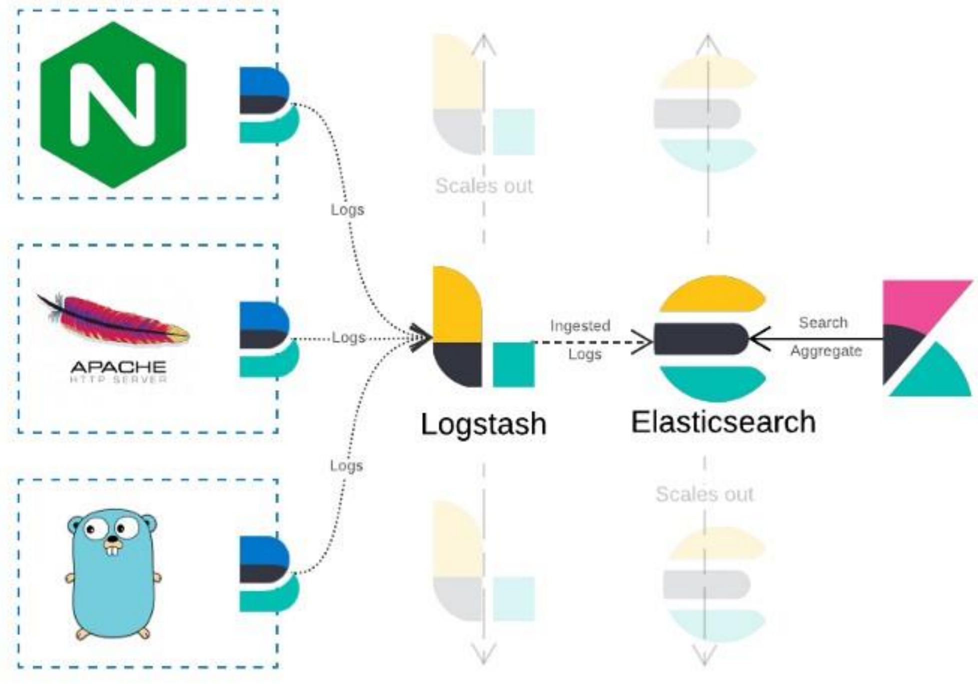


Figure 7: Implementation of Elastic Stack [28]

Another notable open-source monitoring and alerting system are Prometheus [29]. It is also used as a time series database. Prometheus is developed by SoundCloud. Prometheus specializes in system metrics collection and monitoring. Elastic stack’s strongest feature is log management & monitoring. For complex IT systems using both tools would be beneficial.

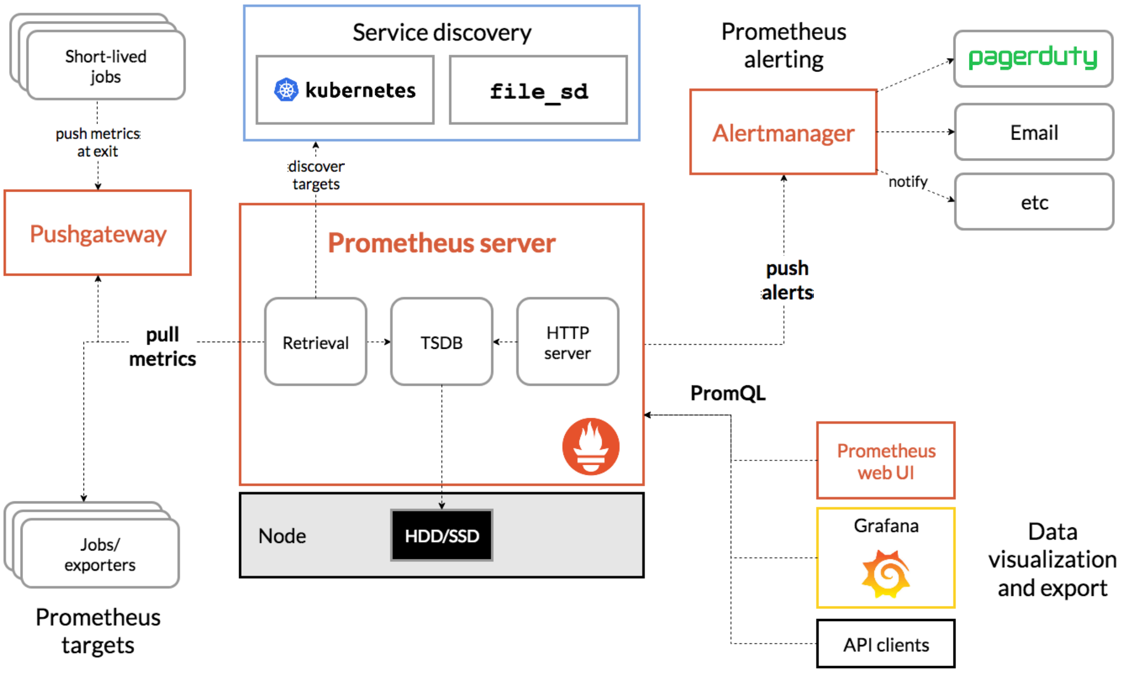


Figure 8: The architecture of Prometheus [30]

Elastic stack & Prometheus both have support for alerting. Elastic Stack calls it Kibana alerts & Prometheus call it Alertmanager. In the free version of Elastic Stack, the Kibana alerts feature is still in beta & limited. Alertmanager centralizes alerts from the client application. It can also integrate with a third-party receiver like email, PagerDuty, or OpsGenie.

6.2 On-call management

It is very important to notify the right person to resolve an incident. Best way to notify an incident to an incident manager via call or SMS. Now, there are almost no free phone call or SMS provider. But it is possible to notify the right person via email or chat client line Zoom or slack. As discussed above commercial solutions like PagerDuty & OpsGenie both support on-call management.

One of the notable opensource on-call management & scheduling system is Oncall [31] developed by LinkedIn. It has a good feature for on-call scheduling for on-call shifts. For incident escalation OpenDuty [32] can be used Which has support for SMS, phone calls, email & Slack etc. OpenDuty still in beta, not recommended for production yet.

6.3 Incident communication

Incident communication is a very important part of an incident. Based on the severity of an incident, the incident manager should provide the current status to the client, business unit & developer team. The most common approach to incident communication is via email, chat, or dedicated status page. In an effort to automate incident communication the following steps can be taken:

- Predefined email template based on incident severity and current incident status (acknowledge, on-going, resolved), with this incident update, can be provided in a click of a button.

- If the communication method is chatting, then also predefined text could be useful. By using Python script that can also be sent by a click of a button. Any dedicated system status page can be updated by python script & system corn job.

- The chatbot can be another option for organizations using mainly chat clients like Slack, Zoom. A chatbot can provide or describe the current incident status to end-users.

6.4 Post-incident documentation

Consistent reliability & availability of digital services can benefit business growth. Post-incident documentation is another vital part to resolve similar incidents faster. It will help to create a realistic SLA for managers. The historical incident data will be helpful for the training of new incident responders. As previously discussed, for a small team collecting incident data manually could be overlooked for lack of resources.

It is possible to create another small Python script that can create an automatic incident timeline based on the incident update provided via email or chat. This small step can save a significant amount of time.

6.5 Root cause Analysis

Root cause analysis of an incident is not a mandatory part of the ITIL incident management process. But it is often required by managers to provide a root cause analysis after an incident has been closed. An important part of RCA is the timeline of the incident as it happened. By the following, the previous step timeline inclusion in RCA should be very simple.

A simple web form can be used to collect the root cause of an incident. The developers will just fill the form with the root cause. The automated script will create a full RCA based on the incident timeline & provided the root cause. These steps could also save a significant amount of time in post-incident management.

6.6 Security incidents

Security incidents can be difficult to solve if there is no IM process in place [33]. Security incidents are increasing daily [34]. Some recent data and common security incidents include:

- Phishing attacks – 350 % rise in phishing websites in 2020
- DDoS – 595% year-over-year increase
- Ransomeware attacks – 20% increase in ransomware attacks.
- SQL injections – 8000% rise from 2018 to 2019
- Malware attacks – 176% increase mostly as MS office file types

There are some effective tools for automating security incident management. Netflix open-sources its crisis management software Dispatch. Netflix created Dispatch to manage security incidents, but it can be used for any other incidents. Dispatch can integrate with Slack, PagerDuty, etc. It also tracks all incident data centrally [35].

Dispatch has the following components for crisis management [36]:

- Resource Management: It documents all incident response metadata, screenshots, logs, etc.

- Individual Enagagement: It connects incident participents with incident reponders.
- Life Cycle Management: It provides the tools necessary tools to the incident commander for the entire incident life cycle.
- Incident Learning: It analyses past incidents for faster future incident resolution.

Dispatch can be an obvious choice for organizations that prefer a self-hosted incident management system.

7 Implementation of a custom solution

In this chapter, the design and implementation of a custom incident management solution will be discussed. Open-source and free tools can be used to build a full-featured incident management system. Most of the open-source systems that will use in the demonstration are already discussed in the previous chapter.

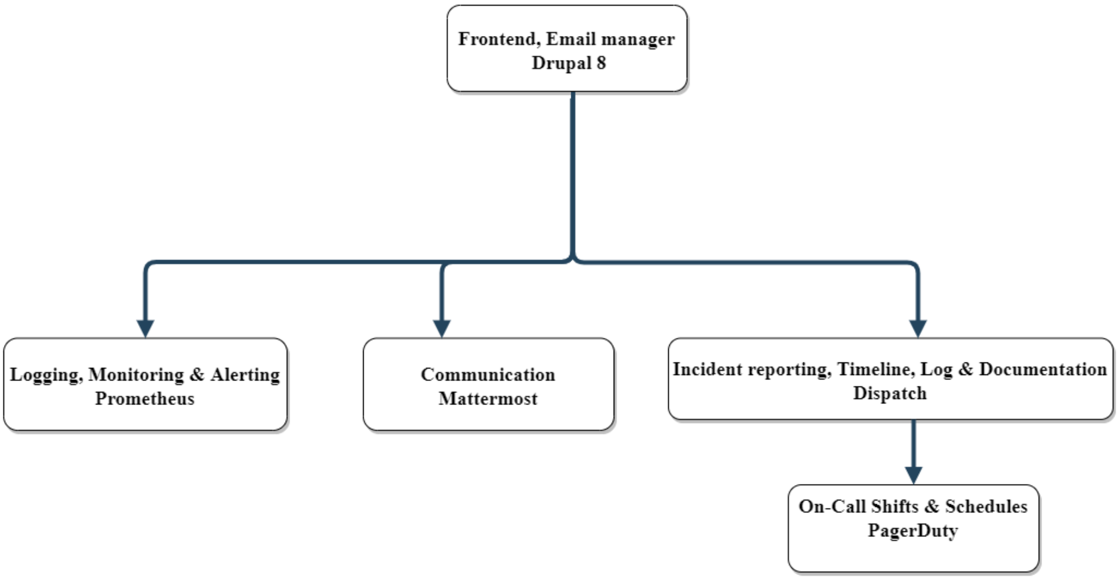
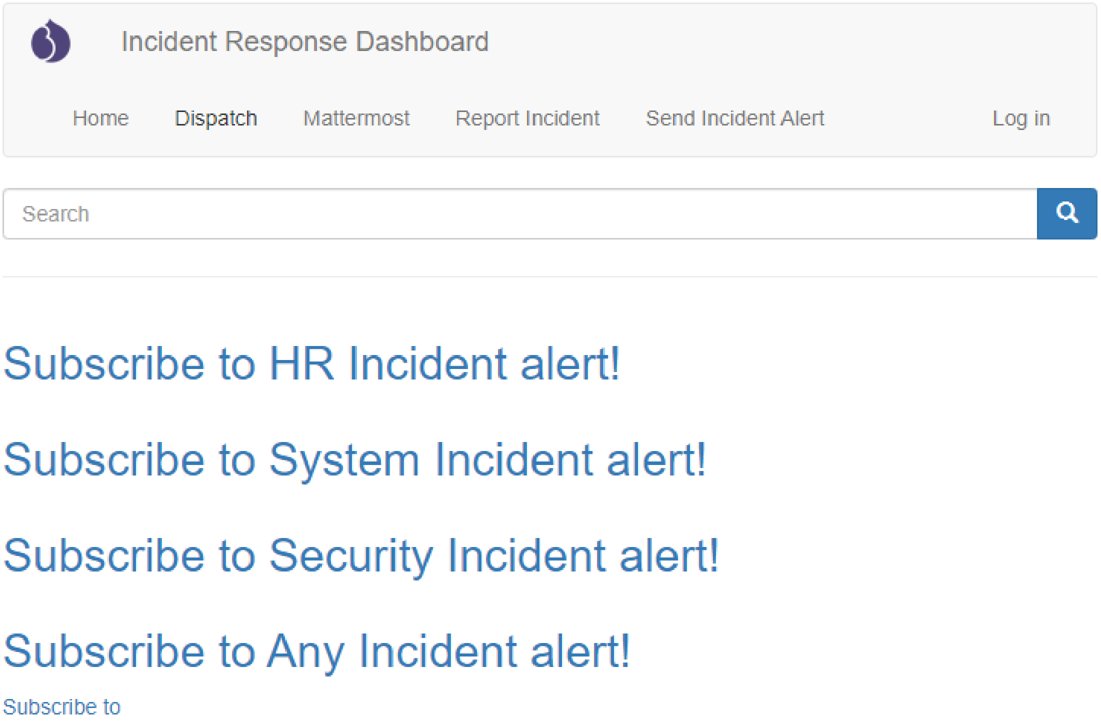

Frontend, Email manager
Drupal 8
Logging, Monitoring & Alerting
Prometheus
Communication
Mattermost
Incident reporting, Timeline, Log & Documentation
Dispatch
On-Call Shifts & Schedules
PagerDuty

Figure 9: Simple custom incident management systems diagram

The following systems have been used to create custom incident management systems:

7.1 Drupal 8

Drupal 8 [37] – Open source content management systems based on PHP. Drupal has powerful extensions called modules that can be used to create very complex web-based solutions. In this demo, Drupal will be used as a frontend incident management dashboard. Incident responders can create email templates, send emails, and subscription options for different incident participants. Drupal is also connected to the Mattermost for internal incident communication. Incident participants can also subscribe to different incident notifications they would like to receive.



Subscribe to HR Incident alert!

Subscribe to System Incident alert!

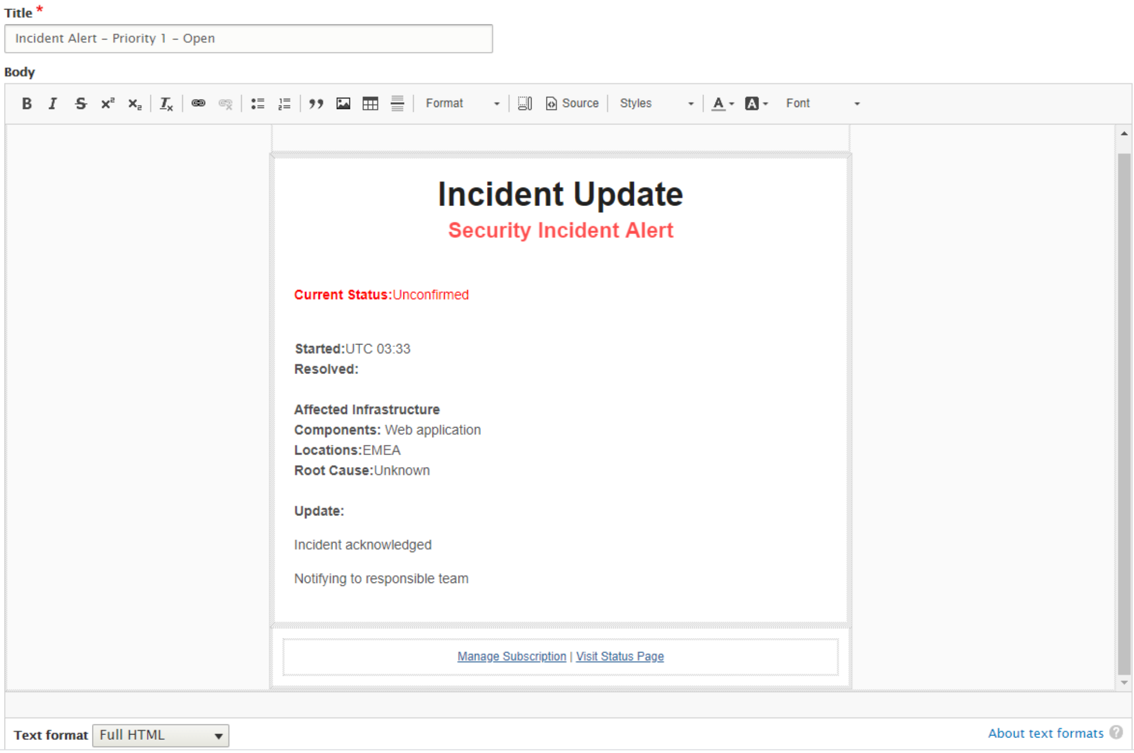
Subscribe to Security Incident alert!

Subscribe to Any Incident alert!

Subscribe to

Figure 10: Drupal Front-end

Drupal menu system will provide links to Prometheus, Mattermost & Dispatch Dashboard. By using Drupal as a single point of communication will save a significant amount of time & complexity.



Title *

Incident Alert – Priority 1 – Open

Body

Incident Update

Security Incident Alert

Current Status: Unconfirmed

Started:UTC 03:33
Resolved:

Affected Infrastructure
Components: Web application
Locations:EMEA
Root Cause: Unknown

Update:

Incident acknowledged

Notifying to responsible team

Manage Subscription | Visit Status Page

Text format Full HTML

About text formats

Figure 11: Drupal email templating interface

Drupal modules Simplenews and Webfrom used to manage email templates and subcriptions. Drupal 8 is hosted on a Ubuntu 20.04 VM. It uses the Nginx web server and MySQL database. The computational resources for this VM:

Memory	vCPUs	Transfer	SSD Disk
1GB	1vCPU	1TB	25GB

7.2 Prometheus

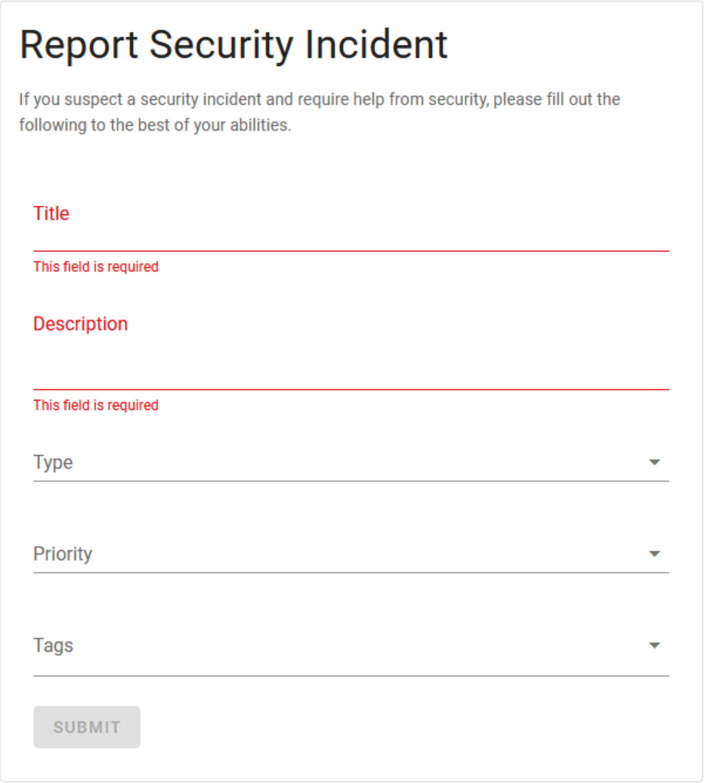
As discussed in chapter 6.1, Prometheus is a powerful monitoring & altering system. Prometheus can alter the IT front desk or incident manager for any possible system failure. In this implementation, Prometheus is used as the primary monitoring & alerting system.

Prometheus 2.9.2 has been installed on Ubuntu 18.04. The computational resources for this VM:

Memory	vCPUs	Transfer	SSD Disk
4GB	2vCPU	4TB	80GB

7.3 Dispatch

Dispatch has been introduced in chapter 6.6. Dispatch will be used as the main incident management system. Incident participants can report incidents via webform. Incidents responders can assign a task, provide updates & create workflows within its dashboard. Dispatch will create a timeline & report after an incident gets closed.



Report Security Incident

If you suspect a security incident and require help from security, please fill out the following to the best of your abilities.

Title

This field is required

Description

This field is required

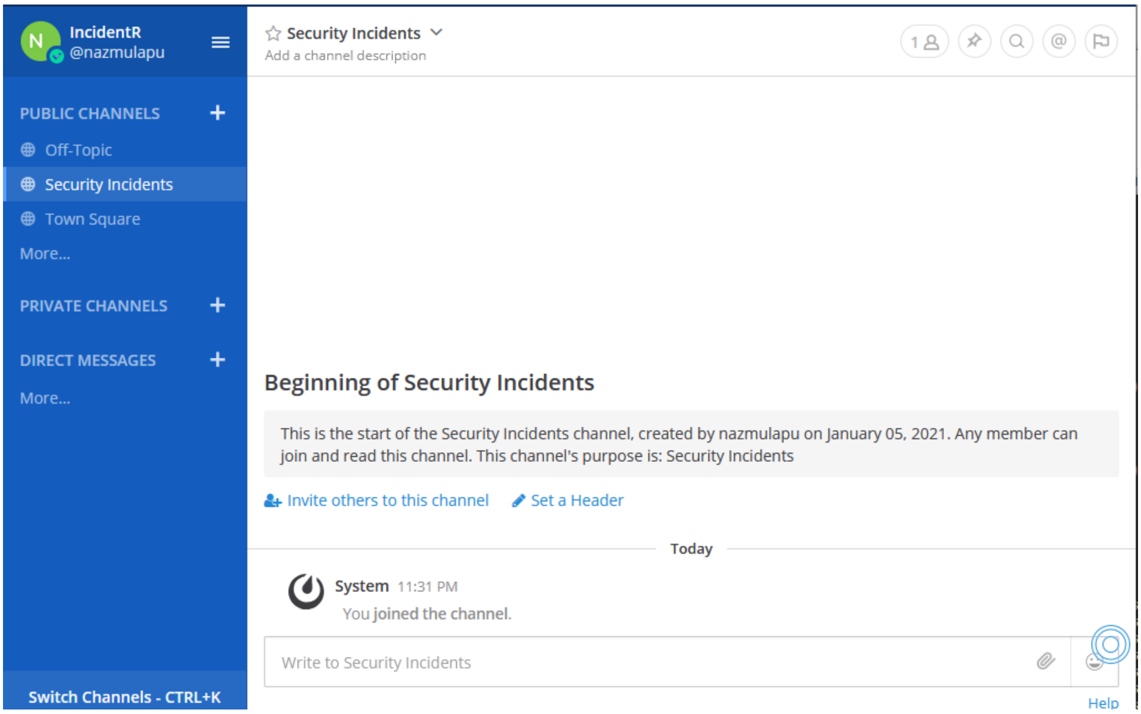
Figure 12: Incident report form in Dispatch

Dispatch has been installed using Docker on Ubuntu 20.04. The computational resources for this VM:

Memory	vCPUs	Transfer	SSD Disk
8GB	4vCPU	5TB	160GB

7.4 Mattermost

Mattermost is an open-source, self-hosted SaaS messaging system [38]. It has mobile & multi-OS desktop clients. Users can create different channels & teams. Mattermost has been a popular choice for the DevOps team. Mattermost can be integrated with other systems like Drupal. In this implementation, Mattermost will be used together with Drupal for main incident communications.



Beginning of Security Incidents

This is the start of the Security Incidents channel, created by nazmulapu on January 05, 2021. Any member can join and read this channel. This channel's purpose is: Security Incidents

System 11:31 PM
You joined the channel.

Figure 13: Self-hosted Mattermost Dashboard

Mattermost 5.16.3 is installed on Ubuntu 18.04. The computational resources for this VM:

Memory	vCPUs	Transfer	SSD Disk
4GB	2vCPU	4TB	80GB

7.5 PagerDuty

In chapter 3, the best commercial incident management system has been discussed. PagerDuty among height rated commercially available system. At the time of writing this thesis, PagerDuty provides a free account with on-call management. Dispatch has a plugin for PagerDuty integration. For on-call shifts & schedules, this implementation uses PagerDuty. Whenever an incident will be reported in Dispatch, Dispatch will notify the incident responders on duty via PagerDuty. An alternative to PagerDuty could be Linkedin OnCall but by the of writing this thesis, there are no OnCall plugins for Dispatch.

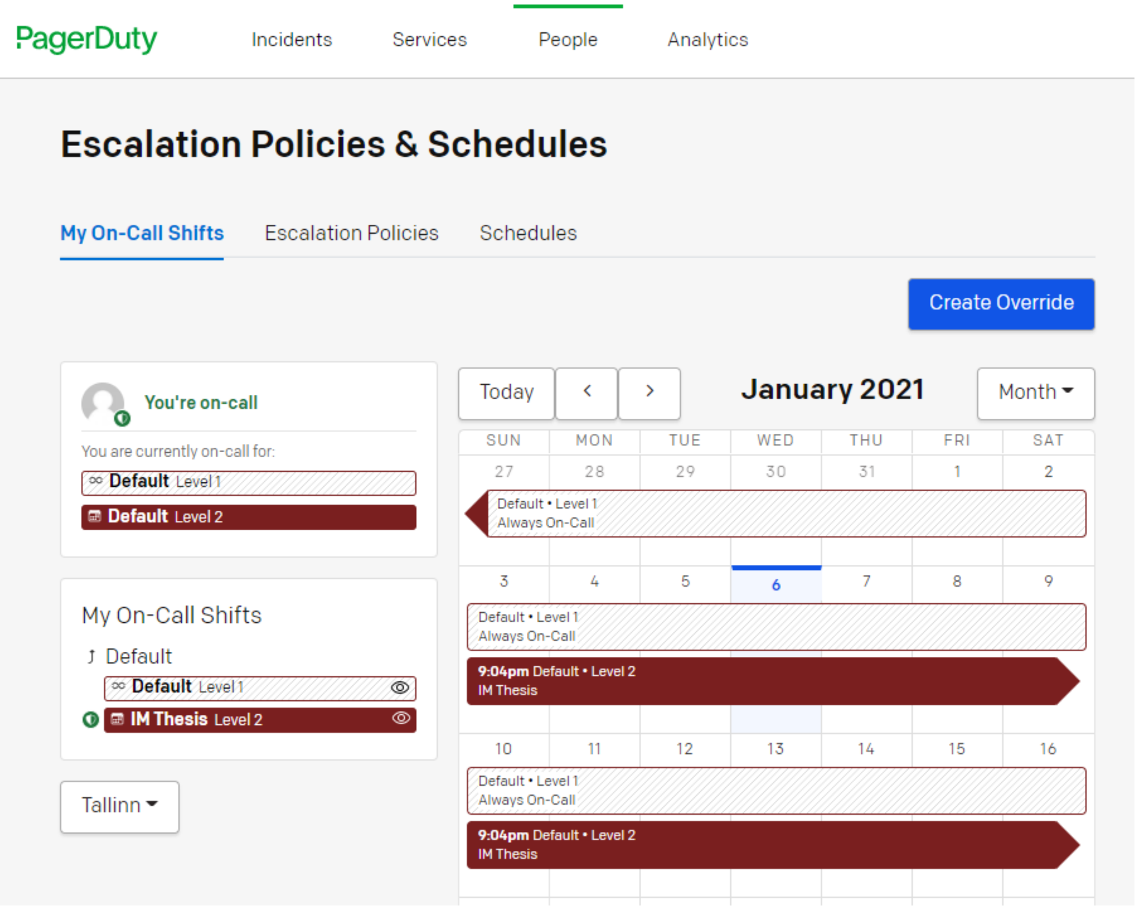


Figure 14: PagerDuly On-call Manager

7.6 The result, cost, and limitation

After the all system configuration the custom incident management system will look like figure 9 below. The following steps describe the incident management processes that can be resulted from using this custom open-source based solution.

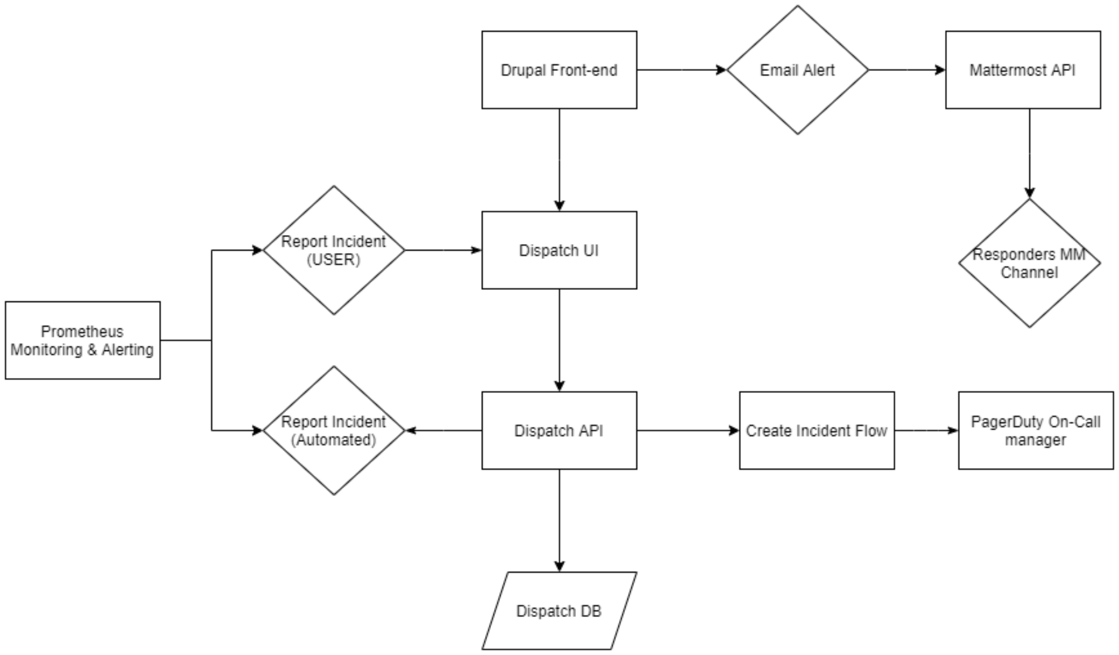


Figure 15: System diagram of a custom incident management system [39]

- Most of the issues in the infrastructure or software will be detected by the Prometheus monitoring and alerting system. The monitoring and the alerting system can extend with other tools like Elastic stack & Centreon.

- If any issue is detected by the Prometheus or any unavailability of service, the IT front-desk or incident participants can report the incident by going to the Drupal front-end & clicking on to Report Incident menu. The IT front-desk needs a dispatch user account.

- After any reported incident & based on its priority Dispatch will notify the on-call staff via PagerDuty API.

- The incident responder will receive notification for any high priority incident. The incident responder can log in to Drupal front-end & send incident acknowledgment via predefined email templates. The acknowledgment will automatically send a status update to the Mattermost channel.

- In the Drupal front-end, the incident participants can subscribe to any particular incident they are interested in. They will be notified whenever the incident responder provides any updates via email & Mattermost.
- Incident responders will focus on solving the incident & provide a timely update via Drupal front-end and Dispatch.
- After resolving the issue, the incident responder can send an email via Drupal front-end. The incident case can be close in Dispatch.
- Dispatch will record all the incident statuses. A final report can also be generated from Dispatch.
- Dispatch stores all past incidents record. So the future incidents can be resolved easily.

The cost of running these applications is approximately 100 euros from simple cloud providers like Digital Ocean, Linode, Vultr, etc [40]. This implementation can be implemented in any on-premise server running Linux.

The above custom incident management system will automate key parts of the incident management process. That will be beneficial for any size team. The limitations of this system include:

- Lack of plugins – connecting Dispatch with Prometheus & Linkdins OnCall.
- Lack of open-source on-call management system
- Not as feature-rich as commercial counterparts.
- Learning curve

The detailed user guide for the demo of this custom implementation will be attached in Appendix-2.

8 Summary

With the growing demand for digital services, regardless of the size of an organisation, it is highly recommended to have an effective incident management process/model in place once a digital service goes into production. Establishing an incident management process not only increases customer confidence, but also the confidence of the development team.

In the complex world of IT services, it can be a daunting task to choose a perfect solution to improve the overall performance of the service. This is also true in the case of incident management systems. An organisation must find the best tool for its specific needs.

From the facts of the previous discussions, it has been shown that any of the three (PagerDuty, OpsGenie, xMatters) commercially available incident management systems can improve the overall incident management for any organisation. But these solutions increase the ongoing cost of IT service. For large enterprises, this increase in operational costs may not be a problem. In the case of a startup or small team, these solutions can be costly and overwhelming. Many of these features may not be necessary for a small business. These solutions are not suitable for a business that does not want to share its data with a third-party cloud-based system. The cloud-based system is not completely secure and it may also have some downtime.

To save costs and data, companies can build their own solution, as described in Chapter 7. The combination of open source and commercial solutions not only saves costs but also makes it an effective solution. A custom, automated incident management solution can be easily modified for any in-house application whose features may not be available in a commercial solution. Using a custom incident management solution is more secure when running on an intranet. As more and more companies make the move to effective incident management, it is foreseeable that more interesting tools will join the open-source incident management ecosystem. This way, any team with moderate DevOps skills can manage their automated incident management solution.

References

[1] DFLabs, “The Overlooked Importance of Incident Management,” 24 01 2018. [Online]. Available: https://www.dflabs.com/resources/blog/the-overlooked-importance-of-incident-management/. [Accessed 04 12 2020].

[2] Ella Koeze, Nathaniel Popper, “nytimes.com,” 7 04 2020. [Online]. Available: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html. [Accessed 06 01 2021].

[3] “ITOps and DevOps Spending 10 Extra Hours Per Week Resolving Incidents During Pandemic,” 04 11 2020. [Online]. Available: https://www.apmdigest.com/itops-and-devops-spending-10-extra-hours-per-week-resolving-incidents-during-pandemic. [Accessed 06 01 2021].

[4] Gupta, R., Prasad, K. H., & Mohania, M., “Automating ITSM incident management process,” *International Conference on Autonomic Computing,* pp. 141-150, June 2008.

[5] W. Edwards, Incident Management for Newbies: Expert Guidance for Beginners (ITSM Book 2), 2015.

[6] “ITIL Incident Management | ITIL Version 2,” [Online]. Available: https://www.helpsystems.com/solutions/optimization/service-support-itil-version-2/incident-management#:~:text=ITIL%20incident%20management%20(IM)%20is,component%20of%20ITIL%20service%20support.&text=Detecting%20and%20recording%20incident%20details,inciden. [Accessed 06 01 2021].

[7] “ITIL incident management 101,” [Online]. Available: https://www.bmc.com/blogs/itil-v3-incident-management/. [Accessed 06 01 2021].

[8] C. Skelton, Major Incident Management for IT Operations, 2017.

[9] E. Flora, “AN OVERVIEW OF THE INCIDENT MANAGEMENT PRACTICE IN ITIL 4,” 05 05 2020. [Online]. Available: https://www.beyond20.com/blog/an-overview-of-the-incident-management-practice-in-itil-4/. [Accessed 06 01 2021].

[10] “ITIL Incident Management: An Introduction,” 13 05 2020. [Online]. Available: https://www.bmc.com/blogs/itil-v3-incident-management/. [Accessed 06 01 2021].

[11] “Incident Management in ITIL 4,” 14 05 2019. [Online]. Available: https://www.bmc.com/blogs/itil-incident-management/. [Accessed 06 01 2021].

[12] “opsgenie,” [Online]. Available: https://www.atlassian.com/software/opsgenie. [Accessed 06 01 2021].

[13] “pagerduty,” [Online]. Available: https://www.pagerduty.com/. [Accessed 06 01 2021].

[14] “xmatters,” [Online]. Available: https://www.xmatters.com/. [Accessed 06 01 2021].

[15] "PagerDuty vs xMatters vs Opsgenie," 07 01 2021. [Online]. Available: https://www.saasworthy.com/compare/opsgenie-vs-pagerduty-vs-xmatters?pIds=6261,6265,6268. [Accessed 07 01 2021].

[16] "opsgenie-vs-pagerduty-vs-xmatters-incident," [Online]. Available: https://stackshare.io/stackups/opsgenie-vs-pagerduty-vs-xmatters-incident. [Accessed 07 01 2021].

[17] "Compare OpsGenie vs. PagerDuty vs. xMatters IT Management," [Online]. Available: https://www.itcentralstation.com/products/comparisons/opsgenie_vs_pagerduty_vs_xmatters-it-management. [Accessed 07 01 2021].

[18] "Opsgenie vs PagerDuty vs xMatters," [Online]. Available: https://www.capterra.com/website-monitoring-software/compare/170236-125693-116750/OpsGenie-vs-PagerDuty-vs-xMatters. [Accessed 07 01 2021].

[19] "PagerDuty," [Online]. Available: https://stackshare.io/pagerduty. [Accessed 07 01 2021].

[20] [Online]. Available: https://stackshare.io/stackups/opsgenie-vs-pagerduty-vs-xmatters-incident. [Accessed 07 01 2021].

[21] "SW Score Methodology," 07 01 2021. [Online]. Available: https://www.saasworthy.com/sw-score-methodology. [Accessed 07 01 2021].

[22] "google trends," [Online]. Available: https://trends.google.com/trends/explore?q=pagerduty,%2Fg%2F11dxr05yqb,%2Fg%2F11f00zcg2n. [Accessed 07 01 2021].

[23] "INCIDENT RESPONSE PLAN FOR SMALL TO MEDIUM-SIZE ORGANIZATIONS," 24 04 2020. [Online]. Available: https://blog.eccouncil.org/incident-response-plan-for-small-to-medium-size-organizations/. [Accessed 07 01 2021].

[24] "Incident management tools and processes insufficient to enable innovation," 18 09 2020. [Online]. Available: https://www.helpnetsecurity.com/2020/09/18/incident-management-tools-and-processes-insufficient-to-enable-innovation/. [Accessed 07 01 2021].

[25] Chen, Z., Kang, Y., Li, L., Zhang, X., Zhang, H., Xu, H., ... & Lyu, M. R, "Towards intelligent incident management: why we need it and how we make it," in *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering,* 2020.

[26] Cusick, J. J., & Ma, G, "Creating an ITIL inspired Incident Management approach: Roots, response, and results," *IEEE/IFIP Network Operations and Management Symposium Workshops,* no. 2010, pp. 142-148, 2010.

[27] "THE ELASTIC STACK," [Online]. Available: https://www.elastic.co/elastic-stack. [Accessed 07 01 2021].

[28] S. Abdel-Naby, "Run, Secure, and Deploy Elastic Stack on Docker," 14 04 2020. [Online]. Available: https://towardsdatascience.com/running-securing-and-deploying-elastic-stack-on-docker-f1a8ebf1dc5b. [Accessed 07 01 2021].

[29] "OVERVIEW," [Online]. Available: https://prometheus.io/docs/introduction/overview/. [Accessed 07 01 2021].

[30] [Online]. Available: https://prometheus.io/assets/architecture.png. [Accessed 07 01 2021].

[31] [Online]. Available: https://oncall.tools/. [Accessed 07 01 2021].

[32] [Online]. Available: https://github.com/openduty/openduty. [Accessed 07 01 2021].

[33] Tøndel, I. A., Line, M. B., & Jaatun, M. G, "Information security incident management: Current practice as reported in the literature," *Computers & Security,* no. 45, pp. 42-57, 2014.

[34] "What is Incident Response?," [Online]. Available: https://www.eccouncil.org/what-is-incident-response/. [Accessed 07 01 2021].

[35] "About Dispatch," [Online]. Available: https://hawkins.gitbook.io/dispatch/. [Accessed 07 01 2021].

[36] "Introducing Dispatch," 24 02 2020. [Online]. Available: https://netflixtechblog.com/introducing-dispatch-da4b8a2a8072. [Accessed 07 01 2021].

[37] [Online]. Available: https://www.drupal.org/8. [Accessed 07 01 2021].

[38] "Welcome to Mattermost!," [Online]. Available: https://docs.mattermost.com/help/getting-started/welcome-to-mattermost.html. [Accessed 07 01 2021].

[39] "Dispatch user guide," [Online]. Available: https://hawkins.gitbook.io/dispatch/user-guide. [Accessed 07 01 2021].

[40] J. Hans, "VPS Comparison 2020: Linode vs DigitalOcean vs Vultr vs SSD Nodes," 11 02 2020. [Online]. Available: https://blog.ssdnodes.com/blog/vps-comparison-linode-digitalocean-vultr-ssdnodes/. [Accessed 07 01 2021].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis

I MD Nazmul Hasan (author’s name)

1. grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis

Design and Implementation of an Automated IT Incident Management System for Small and Medium-Sized Enterprises (*title of the graduation thesis*)

supervised by Md Muhidul Islam (*supervisor's name*)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

07.01.2021 (date)

Appendix 2 – Online demo links & user guide for the custom incident management system

Drupal front-end: http://aim.boonot.tech/

User guide with screenshot for all systems: http://aim.boonot.tech/node/16

Drupal documentation: https://www.drupal.org/documentation

Dispatch dashboard: http://188.166.20.53:8000/dashboard/incidents

Dispatch documentation: https://hawkins.gitbook.io/dispatch/user-guide

Prometheus homepage: http://167.99.210.121:9090/graph

Prometheus documentation:https://prometheus.io/docs/prometheus/latest/getting_started/

Mattermost Channel: https://nazmulapu.live/incidentr/channels/security-incidents

Mattermost documentation: https://docs.mattermost.com/

PagerDuty Documentation: https://developer.pagerduty.com/docs/get-started/getting-started/