Incident Management

Talk the Talk, Walk the Walk

Hila Fish

Senior DevOps / Infrastructure Engineer / SRE @ Wix.com

hilafish1@gmail.com *LinkedIn: Hila Fish* *twitter@Hilafish1*

Hi! I'm Hila Fish.

Senior DevOps Engineer / SRE @ Wix.com

15 years in tech

AWS Community Builder

Conference co-organizer -

DevOpsDays TLV & StatsCraft

Mentor @ courses, communities

DevOps culture fan

Lead singer in a cover band 🎤

Agenda

Incident Management
for me:

Mindset

Incident flow

Being proactive

Incident Management is...

A set of procedures and actions taken to resolve critical incidents.

Reframe Your Perspective

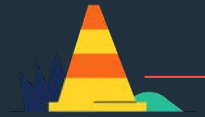
From a “putting out fires” ad-hoc approach

Reframe Your Perspective - Business Mindset.

To a Structured process.

A Structured Process ...of an incident?

Yes!



Identify → **Notify** → **Investigate** → **Resolve** → Incident Closed!

& categorize

& escalate

& diagnose

& recover

Structure reference by OnPage

During an Incident

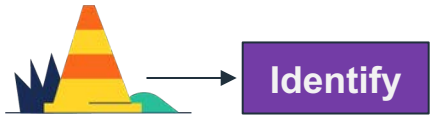
Do I understand the full extent of the problem?

- ➔ **Yes?** Dive in / Notify people
- ➔ **No?** Gather more info

& categorize

Do I understand the full extent of the problem?

- ➔ **Yes?** Dive in / Notify people
- ➔ **No?** Gather more info



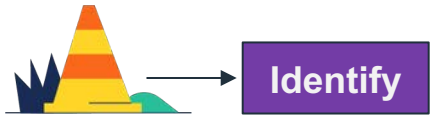
& categorize

Can this wait and be handled in business hours?

- ➔ **Not sure?** Ask.
  Use the info. Escalate if needed.
  Change severity/runbook accordingly

Do I understand the full extent of the problem?

- ➔ **Yes?** Dive in / Notify people
- ➔ **No?** Gather more info



& categorize

Can this wait and be handled in business hours?

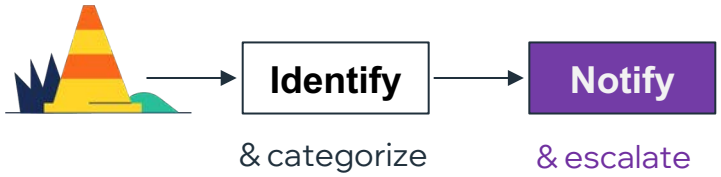
- ➔ **Not sure?** Ask.
  Use the info. Escalate if needed.
  Change severity/runbook accordingly

Was I notified about this from the proper/expected channels?

- ➔ **Yes?** awesome!
- ➔ **No?** add a “note-to-self” to fix that.

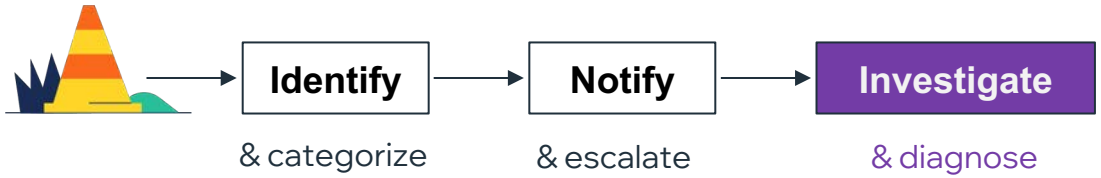
Who should be notified about this incident?

- ➔ During the incident
- ➔ In general



What info is relevant towards incident resolution?

➔ Focus on what's important and relevant.



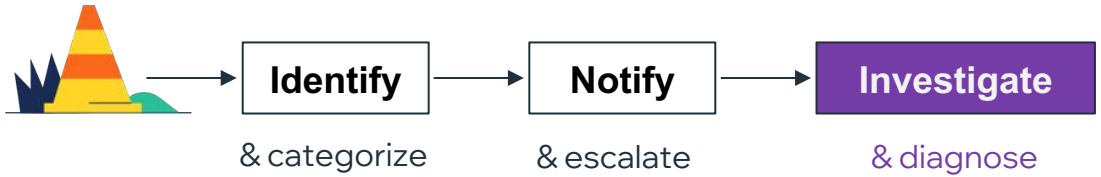
What info is relevant towards incident resolution?

➔ Focus on what's important and relevant.

Did I find the root cause? Do I understand it?

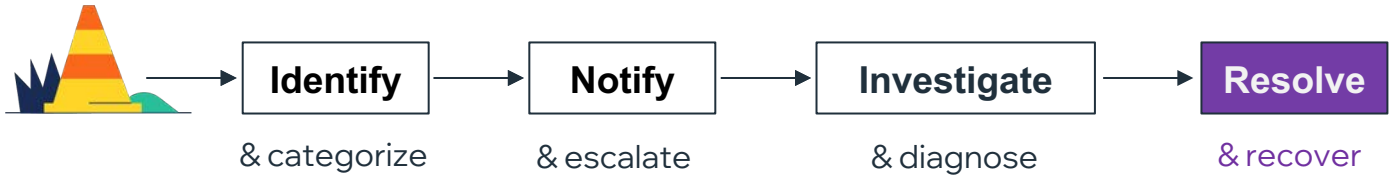
➔ Yes? awesome.
➔ No? investigate more. Escalation if it takes long.

Prioritize root causes over surface-level symptoms.



Which possible remediation step is the best one to take?

➔ Fastest solution to eliminating downtime **without** compromising system's health and stability

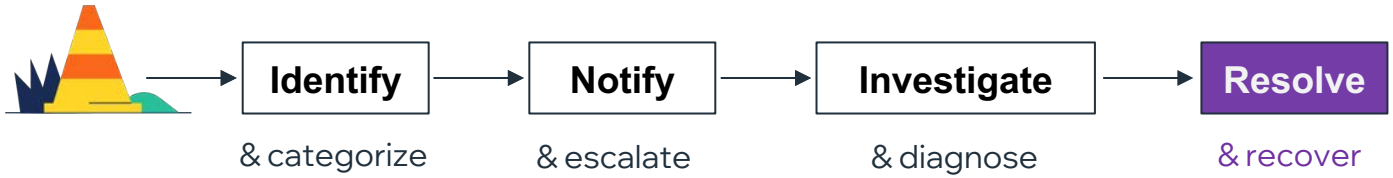


Which possible remediation step is the best one to take?

- ➔ Fastest solution to eliminating downtime **without** compromising system's health and stability

Any action-items needed after resolving the issue?

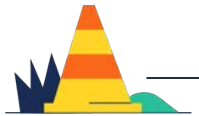
- ➔ Did a patch? - permanently fix it.
- ➔ Preventing recurring issue is a priority.



Do I need to Notify anyone on the incident's resolution?

➔ E2E communicator

Were alerts ok? Or needs tweaking?



Identify → Notify → Investigate → Resolve → Closure

& categorize

& escalate

& diagnose

& recover

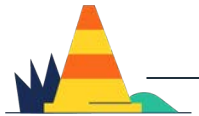
Do I need to Notify anyone on the incident's resolution?

→ E2E communicator

Were alerts ok? Or needs tweaking?

Is a relevant Incident runbook in place? is it outdated, needs updates?

Can I help prevent similar incidents from happening again?



Identify & categorize → **Notify** & escalate → **Investigate** & diagnose → **Resolve** & recover → **Closure**

Do I need to Notify anyone on the incident's resolution?

➔ E2E communicator

Were alerts ok? Or needs tweaking?

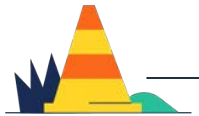
Is a relevant Incident runbook in place? is it outdated, needs updates?

Can I help prevent similar incidents to occur?

Does this incident require a post-mortem?

➔ **Yes?** Jot down the notes ASAP, while it's still fresh in your mind

➔ **No?** Share knowledge – Runbook/daily brief



Identify → **Notify** → **Investigate** → **Resolve** → **Closure**

& categorize | & escalate | & diagnose | & recover

War Room Conduct

- ➔ Incident manager
- ➔ Too many people = Too noisy

Necessary qualities for an incident Manager

critical incident resolved!

Think on your feet – Impromptu action taker

Necessary qualities for an incident Manager

critical incident resolved!

Think on your feet – Impromptu action taker

Differentiate relevant & irrelevant info

Necessary qualities for an incident Manager

critical incident resolved!

Think on your feet – Impromptu action taker

Operate under pressure

Differentiate relevant & irrelevant info

Necessary qualities for an incident Manager

Think on your feet – Impromptu action taker

Operate under pressure

Differentiate relevant & irrelevant info

Methodical work -> Faster incident resolution

Necessary qualities for an incident Manager

Think on your feet – Impromptu action taker

Operate under pressure

Be humble – Stuck? ASK FOR HELP.

Differentiate relevant & irrelevant info

Methodical work -> Faster incident resolution

Necessary qualities for an incident Manager

Think on your feet – Impromptu action taker

Operate under pressure

Be humble – Stuck? ASK FOR HELP.

Differentiate relevant & irrelevant info

Methodical work -> Faster incident resolution

Problem solver – whatever needed

Can-do approach

Necessary qualities for an incident Manager

Think on your feet – Impromptu action taker

Operate under pressure

Be humble – Stuck? ASK FOR HELP.

Sense of Ownership and initiative

Differentiate relevant & irrelevant info

Methodical work -> Faster incident resolution

Problem solver – whatever needed

Can-do approach

Necessary qualities for an incident Manager

Think on your feet – Impromptu action taker

Differentiate relevant & irrelevant info

Operate under pressure

Methodical work -> Faster incident resolution

Be humble – Stuck? ASK FOR HELP.

Problem solver – whatever needed

Can-do approach

Sense of Ownership and initiative

Good communicator

Necessary qualities for an incident Manager

Think on your feet – Impromptu action taker

Operate under pressure

Be humble – Stuck? ASK FOR HELP.

Sense of Ownership and initiative

Caring

Good communicator

Differentiate relevant & irrelevant info

Methodical work -> Faster incident resolution

Problem solver – whatever needed

Can-do approach

Lead without authority [2+ people involvement]

Agenda

Incident Management
for me:

- ✓ Mindset
- ✓ Incident flow

Being proactive

Ready?

It doesn't really matter, actually.
They will find you.

Can We Do Better?

The Proactive Approach

After the Fact

1. **On-Call shifts handoffs**
   - ➔ audit purposes
   - ➔ team members success
2. **Post-Mortem notes** - asap
3. **New tasks** - prevent the next incident, stabilize the env
4. **Modify alerts** - fix ‘false positive’ (don’t wait for the next on-call to do it)
5. **Incident runbooks**
6. **Automation** - candidates for self-remediation?
7. Issue handled? **Share the knowledge**

Can We Do Better?

The Proactive Approach

Day-to-Day

1. **On-Call shifts handoffs** - On-going Basis
2. **Escalation POCs**
3. **Understand System Architecture**
   - ➔ Weaker areas/vulnerabilities
   - ➔ Sensitive/blast radius scopes
4. **Learn application flows**
5. **Team members tasks**
6. **Deployments/Changes in prod**
7. **Bonus: Be a go-to person** - “if you build it, they will come”

Incident manager!

Talk the Talk, Walk the Walk -

- ❤️ Qualities in check
- ❤️ Make it structured
- ❤️ Be proactive

Incident manager!

Talk the Talk, Walk the Walk -

- ❤️ Qualities in check
- ❤️ Make it structured
- ❤️ Be proactive

So you'll -

Come prepared to any incident that will cross your way

and -

Prevent the next incident from happening!

Less Incidents →→
Less Downtime →→
Business Success →→

Your Success

Thank You!

Hila Fish

Senior DevOps / Infrastructure Engineer / SRE @ Wix.com

hilafish1@gmail.com *LinkedIn: Hila Fish* *twitter@Hilafish1*