AN INTRODUCTION TO

INCIDENT ANALYSIS

Learning from incidents to improve organizational resilience

jeli

Learning From Incidents

What is incident analysis? 3
Choosing which incidents to investigate 4
Finding your investigators 6
Gathering data to review 8
Writing up your findings 12
Leading a learning review 14
Making improvements 18
Sharing your findings 20

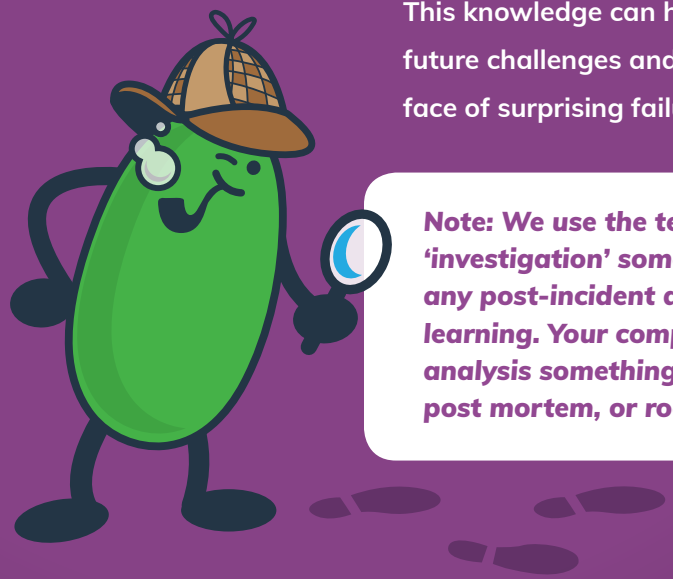
jeli

What is incident analysis?

Incidents occur when software doesn't behave as intended. Every organization experiences these unexpected events but smart organizations use them as opportunites to adapt and grow!

Incident analysis is the process we use to learn from these events. At its heart, the process consists of these core activities:

- Gathering data about the event
- Analyzing the data
- Sharing the learning from the analysis
- Enhancing future resilience



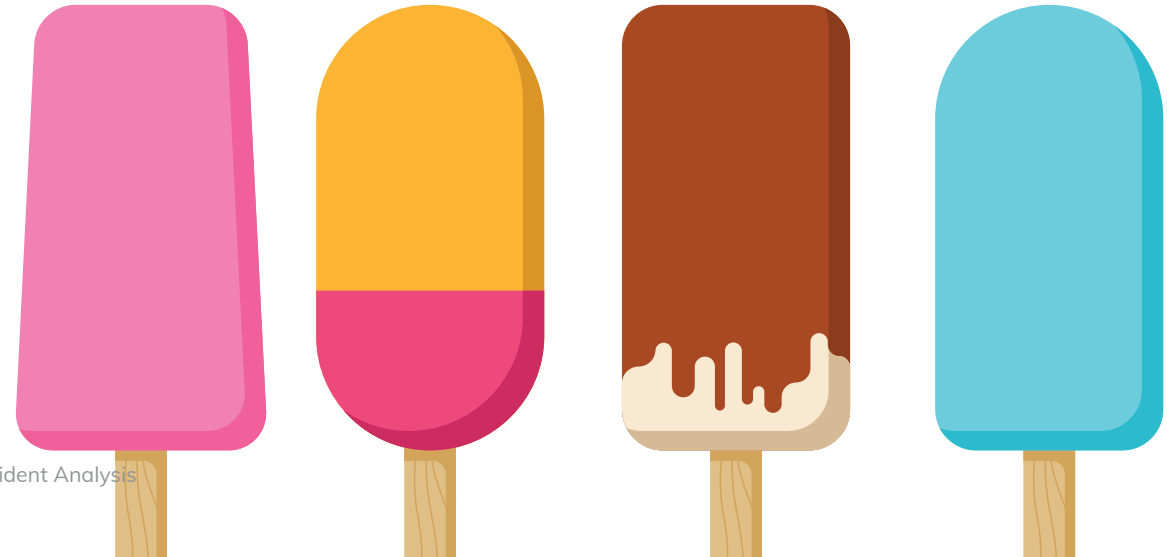
Incidents reveal contributing factors that limit system performance and cause outages. When you analyze and discuss these causes your organization learns how the system functions—how components interact, where hard boundaries leading to total outages are, where the system can degrade without failing, and how your teams make sense of challenging events. This knowledge can help your organization adapt to future challenges and become more resilient in the face of surprising failures.

Note: We use the terms 'incident analysis' and 'investigation' somewhat interchangably to describe any post-incident activities undertaken to promote learning. Your company might call their incident analysis something different like a learning review, post mortem, or root cause analysis.

Choosing which incidents to investigate

Incidents come in all different types and sizes. While we love examining incidents, it usually isn't possible to devote days or weeks to each and every one. We believe that going deeper on incidents with higher potential learning promotes greater organizational value than doing a shallow analysis on all of them. Being selective will get you the most from your time and effort.

On the following page, you'll find a handful of scenarios that can help you get started. These make great candidates for exploration, based on their potential to generate insights that help your teams and organization to learn.



Incidents with high learning potential

Incidents that involve multiple teams

Reviewing incidents that involve multiple teams, people or software can identify expertise that lives within the company—something that may not be listed on organizational charts!

Close calls

Some incidents could have turned out much worse if not for some random event—someone noticing a wonky dashboard or looking at the logs at just the right time. Investigating these events can uncover and codify behaviors you can use to enhance resilience.

Repeat incidents

Investigating even seemingly similar incidents can reveal subtle differences and identify deeper insights such as overloaded teams or limitations in the code that prevented a previous correction being applied.

Seemingly simple incidents

Some incidents are caused by one person's misunderstanding of a seemingly simple process. Rather than passing blame, we can examine these incidents to uncover hidden insights. Oftentimes you'll find other people within your organization who thought the same thing!

Incidents that garner widespread interest

Roles outside of engineering, such as customer support, marketing or senior leaders, may express an interest in understanding more about an event. Engaging in the practice of incident analysis is an excellent way to encourage different parts of the organization to contribute their perspectives and generate support for adapting processes—broadening the impact of the time and effort spent investigating!

Finding your investigators

We believe anyone can be an investigator with the right training and support. A great investigator is one who has expressed an interest in post-incident activities, attended a number of post mortems, and possesses an aptitude for empathy. Many of these attributes can be learned or improved upon over time. For those just jumping in, some of the following tips can help with finding the right person for the job!

Hot tip! Sometimes the best person to lead an investigation is the person most readily available! Having an open mindset is more important here than getting everything "right!"

Avoid conflicts of interest

Identifying someone who wasn't directly involved with the incident can help when details from the analysis surface difficult conflicts. Additionally, investigations shouldn't be led by someone in a position of authority, as these are less likely to be questioned due to imbalances of power.

Training new investigators

We recommend some formal training or mentorship to help set investigators up for success. If your company does not have an internal training program consider pairing a new investigator with more experienced ones until they have the confidence and skills to handle an analysis alone.

Gather a team when possible

As post-incident activities drive more meaningful insights, they drive more value for the organization and tend to attract more support and interest. Take advantage of this interest by building up a team of investigators to include diverse perspectives and increase sharing of knowledge.

Bring in outside help when needed

Some events can be politically tenuous for individual engineers to investigate without explicit support from senior leadership. Even then, it may be more appropriate to hire third-party investigators to help work through an incident that is controversial.

Gathering data to review

Data comes in two categories: hard data, like that which you gather from recordings, chat logs or tickets from customers, and soft data, which you get from activities like interviews. Deciding what to gather can be clarified by examining the questions you're trying to answer and the amount of time and resources you can devote to the investigation.

Common questions you're hoping to answer are:

- What did the responder have access to?
- What made this confusing or difficult?
- How did the system respond to a particular input or intervention?

Your ability to collect data as an investigator may vary depending on availability, time constraints, and difficulties accessing certain kinds of data. You may need to alter your approach to data collection and analysis with each new incident. As you gain skill, you're ability to quickly and flexibly collect and analyze data will improve. Consider pairing with experienced investigators to learn new techniques to level up your skills.

Chat logs

Chat logs are a readily available source of data. With careful analysis, they can reveal insights about a responder's mental model about what was happening during the event and how this changed over time. Chat logs provide a great frame of reference to help conduct interviews and reconstruct an event as it unfolded.

Video Recordings

Video recordings can add important context that chat logs miss such as the entry and exit of certain responders from the incident response effort. They can also give an investigator more insight into where the diagnosis or repair got more or less challenging by viewing the participants facial expressions, body language and tone of voice. These can provide important cues to focus questions or ask for more detail about what was difficult.

Interviews

Taking the time to interview participants after an incident allows you to unlock each individual's expertise and share it across the organization—invaluable to learning about and refining existing practices and processes.

Deciding who to interview

Key players from key moments

Responders that were heavily involved in the detection, diagnosis or resolution of the incident will likely have information to aid your investigation. Key players can also be from customer support, field engineering or the sales side of the business. Even the customers themselves can give you broad and specific perspectives about the event!

People that may feel blamed

It's important that people who feel in some way "responsible" for the incident get to share their perspective to help create a psychologically safe environment. It's important people feel as though their perspective is not only being heard, but that they won't be blamed for incidents. These interviews can also surface additional contributing factors around organizational processes that may have been missed from other data sources.

Owners of impacted systems

Owners or former owners tend to have a high-level understanding of the system, which can make for a more productive retrospective and richer post incident write up. Seemingly basic knowledge about how the full system works puts the incident in valuable context which makes it more likely to be read and shared down the line.

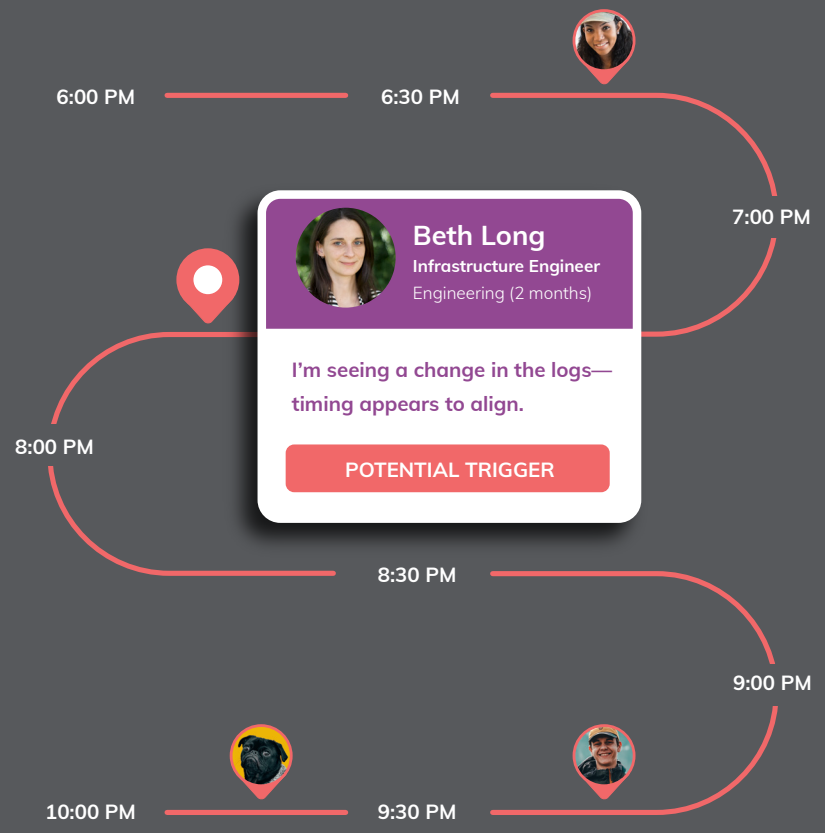
Subject-matter experts

Anyone with expertise in the components involved in the incident are good to interview. Those who are "the only person who knows how to resolve an outage" represent expertise that should be widely distributed. Oftentimes, experts have a hard time sharing their knowledge across the organization. We often ask these experts "how well known is this across your team" and find a surprising number of times the answer is "not well known at all!"

Creating a timeline

Timelines help organize data to reveal gaps or patterns that help with ongoing data collection and analysis. Timelines document the way the event took place over time which can provide important insights into potential improvements in the incident response.

Start by identifying high level moments, like when a problem was identified, how information was acquired and shared, what fixes were employed, and when resolution was achieved. Many investigators do this by cutting and pasting quotes or key pieces of information into a document. If you are working from a transcript you might add tags to flag their meaning. In doing so, you're doing more than collecting data. You're building an engaging story to later tell your organization!



Writing up your findings

Writing up your findings helps to organize your progress, consolidate what you've learned, and share with others. A written version of your findings allows others to comment, showing how the multiple perspectives you have gathered in your investigation fit together. Creating this consolidated view of the incident can broaden everyone's understanding of the event. Don't worry about getting it perfect the first time. You will be iterating on the report throughout this process!

There are two steps to the writing process. The first, a calibration document, serves to help you organize your analysis and gather feedback from interviewees or incident participants. The second step is to formalize the findings into a report.

Find templates online to get started!

- Calibration Document
- How We Got Here report

Calibration Document

The calibration document is shared in advance of a review meeting. This gives those you've interviewed a place to preview your findings, correct any misunderstandings, and comment on the themes you have chosen to highlight. This makes the meeting more productive by focusing the time on deeper discussions, as opposed to simply recounting a timeline. Time is knowledge, folks!

To create your calibration document, look for themes, or significant findings, in your data. They may be recurring patterns, insights into the software itself, or findings with a high learning value. You might have more themes than you have time for in a meeting. As an investigator, your role is to prioritize them. One way to do this is by asking participants what the most important themes are to them. You don't have to worry about this being perfect—this isn't a final report, it's a chance to organize your findings thus far and to give the event participants a prompt for feedback to the investigator!

The Final Report

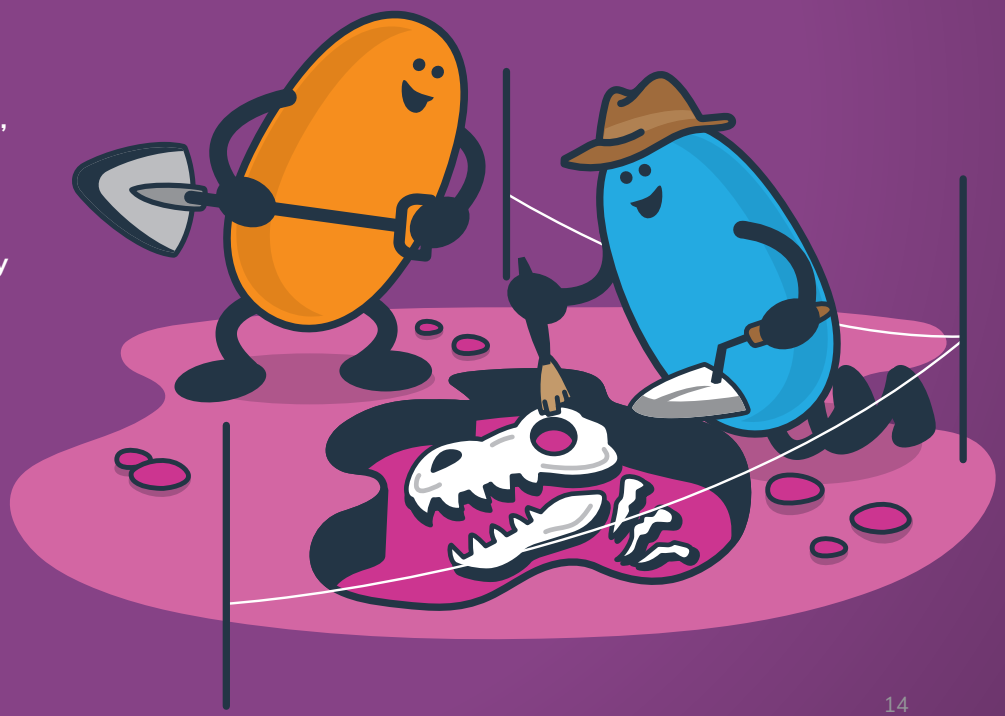
To write the final report, we suggest the "how we got here, or Howie, report" that tells the story of how the event unfolded from the many perspectives that you uncovered. "Howie" is built to be different from a traditional postmortem process. Instead of simply reviewing what happened, this report focuses on how the event came to be in the first place. Feel free to tailor this to your organization's needs. For example, if a recording of the meeting is your thing, no problem, link it in the write up!

If you generate action items after publishing the report it's important to update the report with those items. This helps future readers understand the event as a whole, and what came of it. Also, we recommend sharing this report in a place that has some sort of analytics, at the very least how much it has been read. This can help you figure out what ways of sharing are especially effective and what readers are interested in learning.

Leading a learning review

Who's invited?

Ideally, we'd like all of the responders involved in the incident and anyone you've interviewed to attend so they can share their perspective and recount their experiences. "Responders" are not limited to oncall engineers—include other roles involved in the incident such as customer support, incident management, security, and escalation teams. Inviting a broader range of roles improves understanding of how other parts of the company work and of larger organizational goals.



Think like a facilitator

You may have gathered information, interviewed participants, analyzed and written up findings, but this does not make you the expert—you are there to facilitate the sharing of knowledge and expertise of those who participated in the incident. Everyone experienced the event from their specific point of view, and getting it directly from the source helps create a shared understanding of what occurred and gives us an opportunity to learn from each other.

Share your findings ahead of time

Share the calibration document at least 24 hours prior to the meeting so participants can get a feeling of how you've interpreted the events. Allow them to clarify, elaborate or correct as needed. Giving them advance notice that you'd like them to speak, and helping them understand what to expect, will help to ease any stage fright or defensiveness to create an ideal environment.

Create an agenda

When scheduling the meeting, consider how much time it will take to get through the timeline and themes you've prepared. If the incident went on for several hours (or days!) a thirty minute review meeting won't give you enough time. Conversely, the longer a meeting goes, even with important content, it is harder to secure broad attendance and retain attention spans. A good rule of thumb is to keep it between thirty minutes to two hours. You might indicate in the agenda that people can attend for however long they are able.

The following structure is a great place to start when planning your agenda: opening remarks, an overview of the analysis, narrative summary, themes discussion, call for questions, and steps already taken and next steps.

Set the ground rules

You're about to start a journey through a potential minefield of events and topics; navigate them successfully by first acknowledging where they are and how to move past them. When you see data coupled with detailed analysis, it's easy to assume choices made during an incident were informed by details that weren't available until afterwards. Point these out if you see folks falling into that trap. And don't forget to acknowledge the sneaky, innate predisposition present in every learning review—*hindsight bias*. Remind attendees that the incident responders did what they could with the information they had available to them at the time.

Being "blame aware"

Often in the pursuit of a "blameless" review, we avoid saying individual's names or skip over sensitive parts of the event. But to truly learn from an incident, we need to understand all the circumstances around an action, including the thought process of each individual as they responded in the moment. We can't afford to be "blameless" if it means avoiding the parts of an incident that are difficult to talk about.

Analysis overview

Talk through the data you analyzed (which message channels, various docs, previous incident reports, Jira tickets, Zoom recordings, etc.), and through the amount and scope of the interviews you conducted. Keep this short. Summarize where you started, where the analysis took you, and what your overall approach was while investigating this incident. This helps folks understand where you got the information that will be shared.

Narrative summary

Now it's time for your timeline to shine. Start by providing a short description of the event, cuing the folks you interviewed to describe what unfolded from their perspective. Use the timeline to prompt different responders to share their experiences, and have various subject matter experts provide background knowledge on how the relevant pieces of the system/technology work. Leave space for discussion—the facilitator should not be doing the majority of the talking here.

Themes discussion

Take time before the meeting to prioritize the most important themes you want to cover, as you will rarely have all the time you need. Ask for commentary from the responders, subject matter experts, and stakeholders present. It's okay if all the themes in the calibration document aren't covered. How people respond and dig into your themes help to indicate which ones warrant a closer look!

Call for questions

Now is the time to refer folks back to any questions they may have held onto during the discussion, any topics not addressed, or unresolved concerns. If the group doesn't have any of their own, share some that came up for you during your investigation. If there are a lot of unresolved questions, acknowledge they might not all be answered in this learning review, and may warrant further discussion.

Steps already taken and next steps

Review the work that has already been done so far and discuss the next steps for action items. The next steps also include transitioning the calibration document into a final report, if your organization does one. Get people excited to read and discuss your write up and direct folks to make it a living document through commenting and sharing. Make sure to invite attendees who may not have already read the calibration document to provide their input. Collecting feedback helps improve your process, clarify any lingering concerns, and makes the entire process more engaging.

Making improvements

There are likely multiple ways to make improvements following a learning review, including changing, updating, abolishing, or creating new processes. They might involve learning more about a particular technology, investigating some part of the system, or even teaching others—for example, holding an architecture overview to reorient the understanding of how things work together.

Focus on learning

The goal of incident analysis is to build a more resilient system. To achieve this outcome, technical remediations, or steps to make sure the incident doesn't happen again, are not enough. The insights we gain from each incident are how we continue to learn to better understand our systems, and each other. When we prioritize learning as our response when things go wrong, we focus on understanding what we didn't know previously or as the incident was unfolding. When making suggestions for changes, it's best to focus on the system as a whole rather than on just a part, like one individual. If the action item is a policy change to "not make X mistake again," that's a clue that there is still more to be learned!

Allow responsible parties to own improvements

Plans for improvement should be created and owned by those responsible for implementing the changes and doing the work. Creating plans for others leads to confusion, debate, and resistance. The folks who work in these areas are the best people to figure out what needs to be done, whether it should be done, and how to make it happen!

Don't assign deadlines

It may be tempting to assign due dates for improvements, but doing so only accomplishes one thing: for improvements to be sized specifically to be completed within that time frame. Unless your project and product managers plan for the work coming out of an incident to immediately take priority over all existing deadlines, requiring these items to be completed within a specific time frame is forcing engineers to make tradeoffs against other critical priorities.

Sharing your findings

It's important to establish a practice where everyone in your organization—even those who couldn't attend the review—learns from the outcomes of your investigation, instead of just filing them away to check that procedural box. Mix and match the following techniques depending on your organization's style, and they will help keep everyone informed and engaged with the important output from your incident review sessions!

Any effort you invest to promote what you've learned from your incident investigations is deeply important— share it your way. Just make sure you share it!

Abstract

An Abstract is the #1 thing we recommend folks do and should include one to two paragraphs on what happened, why we should care about this event, contributing factors, learnings, and themes. Think of it as an elevator pitch: if people are going to learn from this incident in one minute, what information do they need to know? This way, you can be sure your audience is getting the gist, even if they don't have a ton of time! An abstract can also help them decide if they want to commit to reading the report or watching the recording. However, that being said, the abstract is brief, so it may lose nuance or depth. Readers will benefit from being linked to another, more comprehensive artifact if they have more questions.

Summary

The summary is a slightly more comprehensive version of the incident. It builds on the information included in the abstract, and adds a more detailed overview of the theme's discussion. If you are including possible action items, include who suggested them. The summary gives folks more context on what was discussed in the review meeting. The reader should be able to get an understanding of the key themes discussed, as well as any next steps suggested. This is a fairly standard artifact in many organizations, but yours will be a bit different as it orients the reader to what was learned, rather than just relaying what happened!

Recording

This is exactly what it sounds like—a recording of the actual review call. When sharing it is helpful to include a message with timestamps of when key moments were being discussed to orient your reader. This will be the medium that most resembles the experience of attending the actual review. However, it takes your audience more time to get through than the other formats, which could result in lower engagement. And while they get to listen to what happened, they can't participate.

Presentation

The presentation can take multiple shapes, like a storytime, where you pick one incident and talk through what happened, the themes, and learnings. Or something more along the lines of a prepared talk, where you share multiple incidents and your learnings with a specific goal. Either way, definitely allow time for Q&A!

This is your chance to drive the narrative to a captive audience. A good presentation can rally individual contributors and get support from leadership. Well-crafted slides can do wonders to drive your themes and to drive buy-in from stakeholders.

Weekly Update

The weekly update consists of a quick review of all the incidents that were analyzed that week. It can be a list of the incidents with their abstracts and a link to the full report. You can also include additional data points like “teams impacted” for quick access to more thorough learnings.

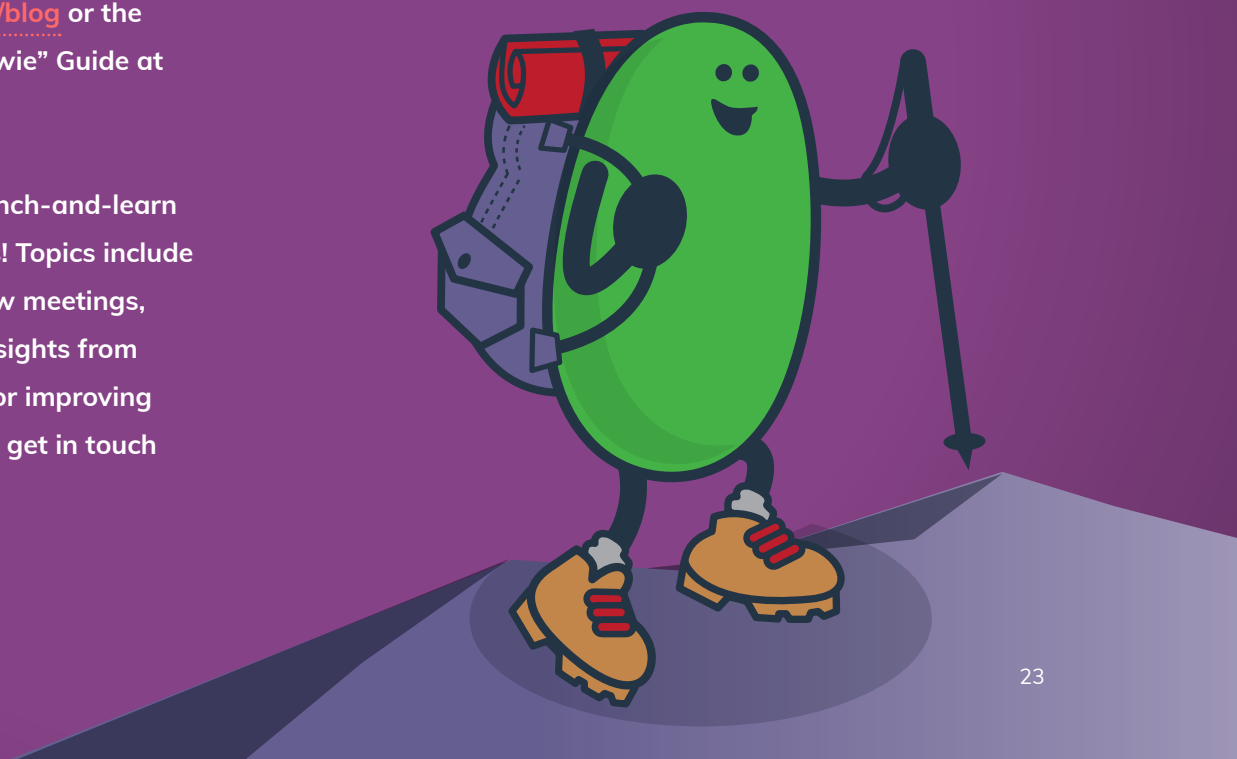
This is a great option for larger organizations with lots of incidents or with silos. Everyone can take a quick glance at this list, find incidents they are interested in based on keywords (e.g. services impacted, technologies involved), and read further into what they find interesting.

Be careful to not allow this format to develop into a shallow, tabular form. You can combat this shallowness by hoisting up themes or other colorful findings from the underlying artifacts and linking to them so the reader can satisfy any curiosity.

Learning from Incidents is an ongoing journey

This guide is intended to get you starting on leveling up your own practices. If you want to learn more, check out the full Incident 101 series at jeli.io/blog or the comprehensive How We Got Here "Howie" Guide at jeli.io/howie-the-post-incident-guide.

Jeli also offers a variety of one hour, lunch-and-learn style sessions and half-day workshops! Topics include Incident 101, facilitating incident review meetings, interviewing techniques, generating insights from your incident reviews, and strategies for improving organizational learning. To learn more, get in touch with us at workshops@jeli.io.



Improving the process is just one way we're making the industry more proactive. You in?

Learn more at jeli.io