Best Practices for Modern IT Incident Management

DevOps.com

There's more riding on the performance and availability of IT environments than ever.

Digital business transformation became necessary for many organizations in the wake of the economic downturn brought on by the COVID-19 pandemic. As the economy continues to recover, businesses now expect IT to be able to respond and pivot to changing conditions no matter how sudden.

Savvy IT teams have learned to expect the unexpected by embracing modern incident management based on best DevOps practices, which enables IT teams to respond swiftly to any outage or sudden degradation in application performance.

The Root of the Problem

Incident response comprises **50% of IT team's time** at 75% of organizations.

27% said **at least 80% of their IT team's time** is spent resolving incidents.[1]

Best Practices for Modern IT Incident Management

1. Detection.

Early detection is crucial. As a core DevOps principle, observability of logs, metrics and traces is a critical first step toward discovering the root cause of an incident as quickly as possible.

2. Response.

Adopt a consistent method to share critical status alerts to critical incident response team members in real-time. Severity status should include both relevant technology status indicators as well as a description of the potential impact to the business.

3. Resolution.

Collaboratively work with engineers, security experts and IT administrators to implement patches and fixes and restore systems as appropriate.

4. Review.

Commit to learning from experience by applying analytics to both the root cause and the response time of the IT incident team in a blameless environment.

5. Recuperate.

Responding to an IT incident always will be stressful. Rather than team members dealing with post-traumatic stress on their own, build in some actual downtime.

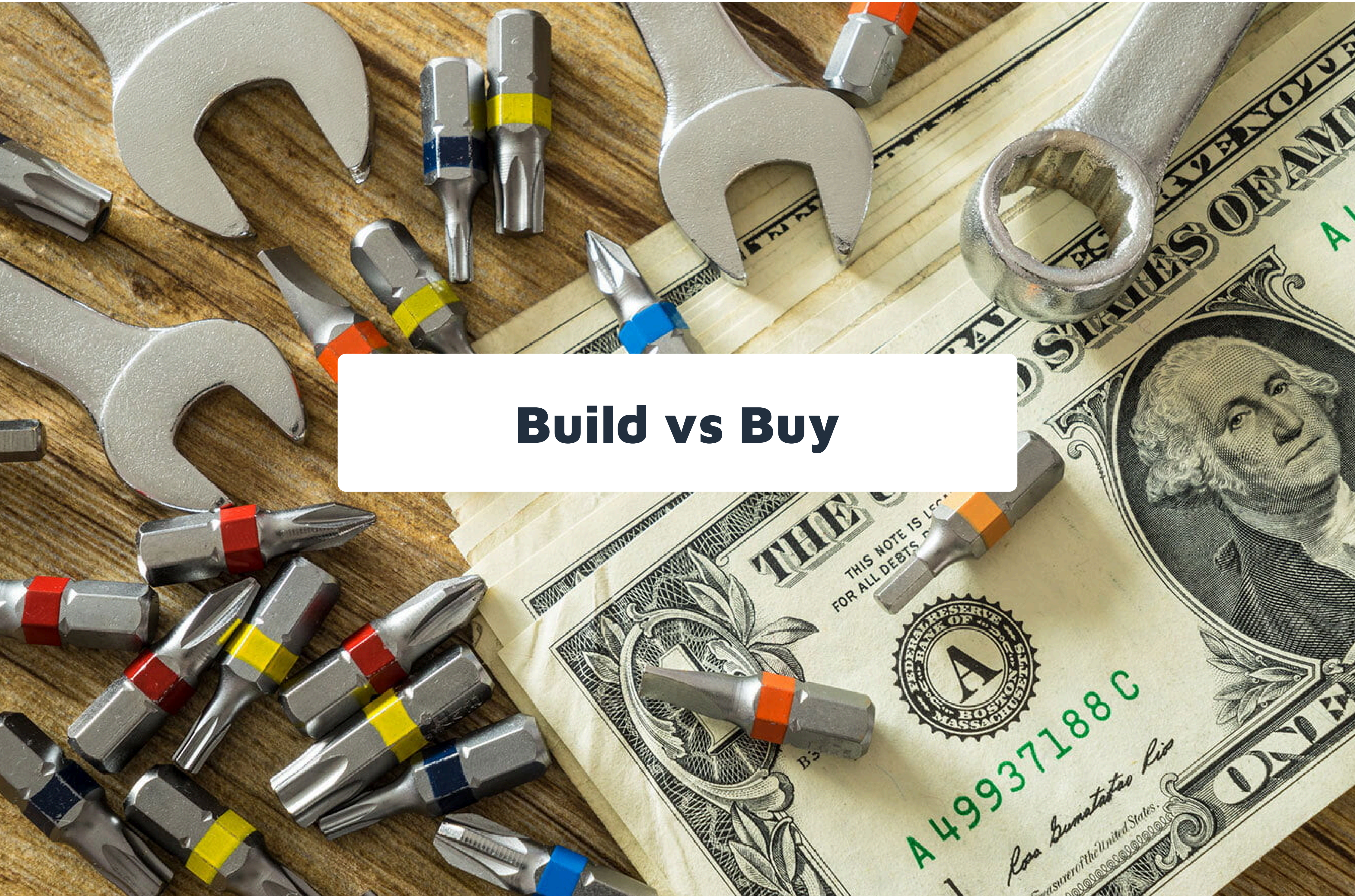
6. Continuous Improvement.

Implement new policies to prevent any recurrences whenever possible. Incident data should be shared to prevent others from making the same mistake.

Modern Incident Management Defined

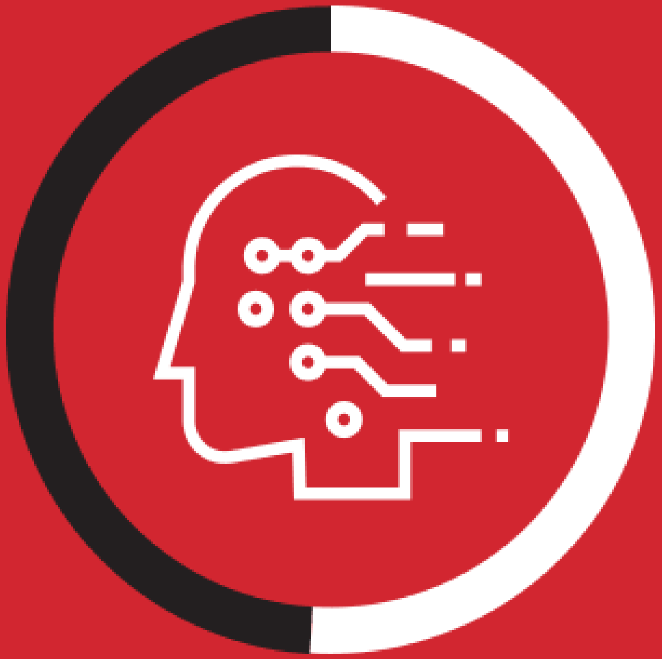
A modern incident management process embraces:

- Containers and microservices, in addition to virtual machines
- Opinionated Gitops processes in addition to DevOps workflows
- Declarative programming tools
- Accessible to engineers and incident response leaders via the cloud
- ChatOps to streamline communications



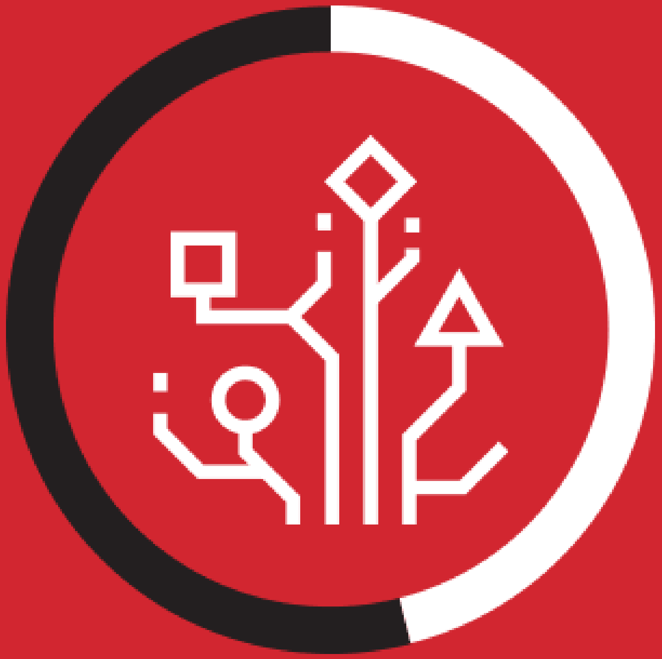
Build vs Buy

Many IT teams have built their own incident management platforms to create workflows that closely align with their business processes. However, as IT environments become more complex and AI becomes more accessible, the practicality of building and maintaining a custom IT incident management platform needs to be called into question.



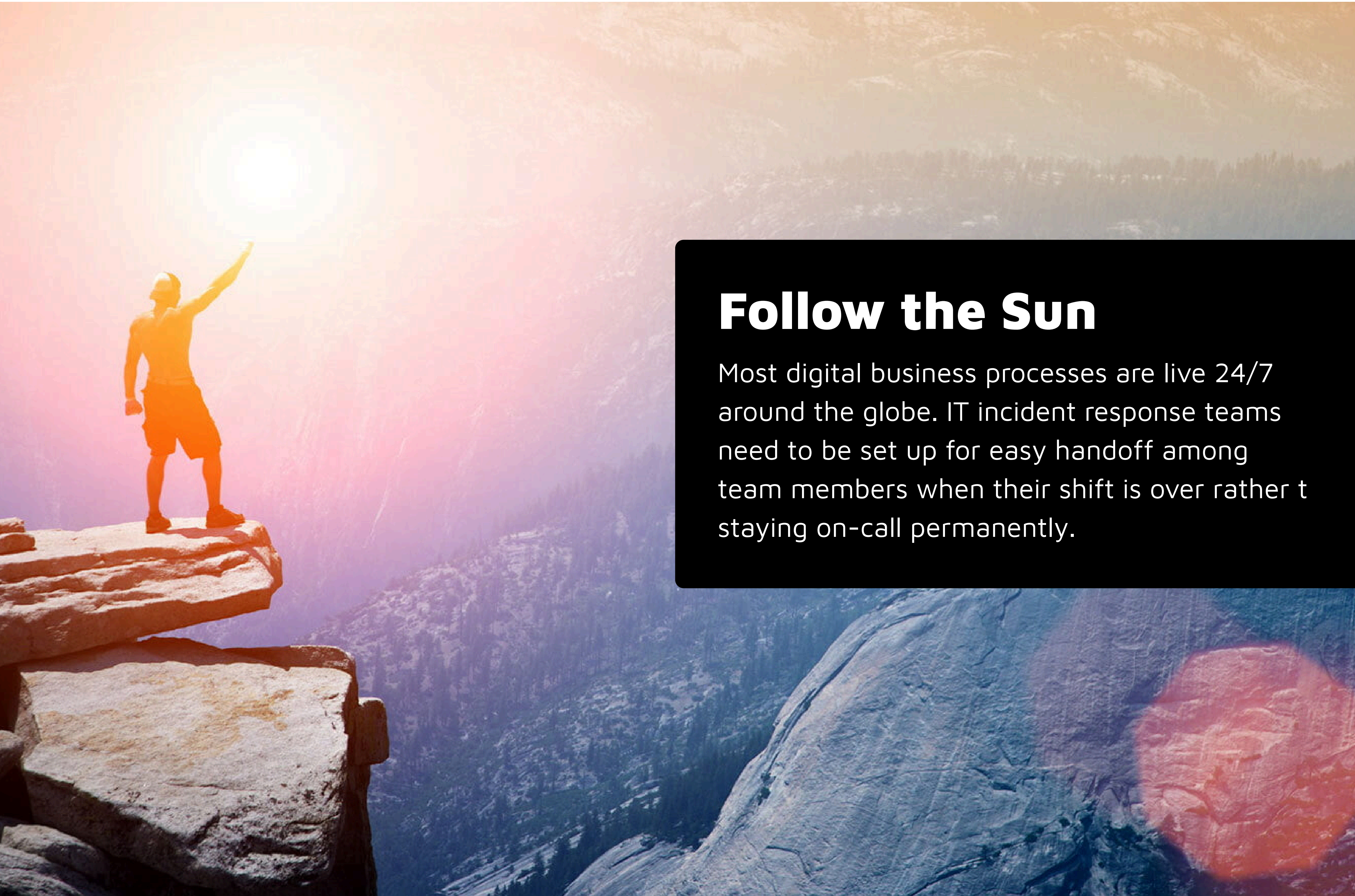
51%

of IT teams are deploying automation and AIOps to employ machine learning algorithms and process automation to cut down alert noise, drive faster root cause identification and handle repetitive activities.



46%

of IT teams also expect to drive agility and faster resolution using a modern incident response platform that provides greater situational context.[2]



Follow the Sun

Most digital business processes are live 24/7 around the globe. IT incident response teams need to be set up for easy handoff among team members when their shift is over rather t staying on-call permanently.

Thank you for reading

Best Practices for Modern IT Incident Management