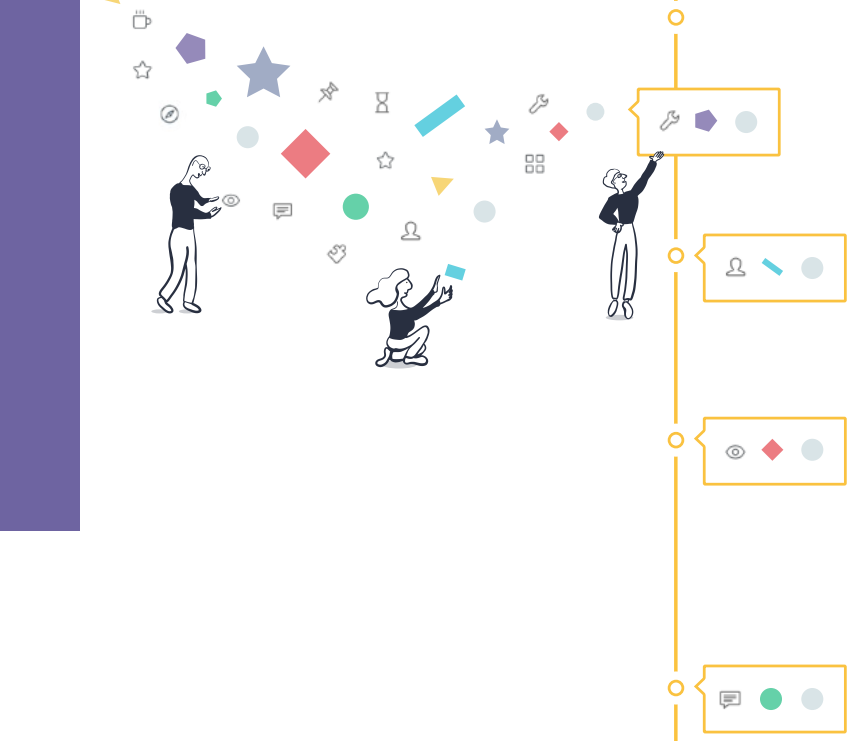
Exigence

The 7 Key Capabilities for Gaining Control & Command of Critical Incidents



“Effective incident management is key to limiting the disruption caused by an incident and restoring normal business operations as quickly as possible.”

Google, Site Reliability Engineering

Contents

It’s a whole different ballgame

Ensuring a speedy and effective process for resolving critical incidents is one of the most important priorities for the IT operations group, the CISO’s teams, Help Desk, the NOC team, and . . . quite frankly – the entire organization, all the way up to the chief executive.

When a critical incident hits, the disruption to service, productivity, and the business itself can be more than considerable.

Whether it’s a productivity system that powers the efficiency of thousands of employees, or an online service that serves millions of customers and drives the company’s revenues - anything less than an immediate and effective resolution means financial loss and damage to customer loyalty, employee satisfaction, and even brand equity.

Indeed, when it comes to critical incidents the stakes couldn’t be higher – and it really is a whole different ballgame.

The Many Faces Of Damage

- Network downtime costs organizations $300K/hour (Gartner)
- Data center outages cost $450K/hour (DataCenter Knowledge)
- Critical failures cost $500K-$1M/hour (IDC)
- 70% say a past critical incident has caused reputational damage (Quocirca survey)

The cyber imperative

When it comes to incidents that constitute cybercrime, the gravity of the consequences is no less, if not more dire.

According to Forbes, cybercrime is at epidemic levels, with losses expected to reach $2 trillion by 2019.

Not even the strongest are immune

- Salesforce went down in August 2017, Business Insider noted: "Salesforce likely lost quite a bit of money on Tuesday."

- Facebook was out for 19 minutes in 2014, with estimated losses at $426,607.

- Amazon went down in 2013, losing an estimated $1.87 million.

It's a mad, mad digital world

In today's complex digital world, it's never been harder to tame a critical incident.

The digitization of organizations and number of devices through which services are consumed by employees and customers is increasing all the time.

Furthermore, infrastructures are much more complex than ever, being dynamic, virtualized, often cloud-based, and mostly siloed.

Moreover, new and innovative products and services are being introduced in a dizzying pace, enabled by these digital transformations and SaaS-based business models.

All this, makes it all the more challenging to keep up, prevent, and mitigate a critical incident.

That's why it's no surprise that:

- The mean time to repair (MTTR) for critical incidents is over 6 hours (Quocirca)
- More than 7 hours are spent on average on root cause analysis (Quocirca)

The basics according to ITIL

According to the ITIL, the framework of best practices for delivering IT services, there is a recommended process flow for how to handle major incidents:

1 **Incident logging**
and categorization

2 **Escalation**
to 2nd-level support

3 **Notifying**
the incident manager

4 **Forming the Major Incident Team**
(MIT, made up of IT managers and technical experts, many from within the company but some potentially from outside), who will work together to resolve the incident

5 **Reporting the incident**
to problem management for future investigation and for developing a permanent solution, once a workaround is discovered

6 **Capturing data**
from the Major Incident Management process and using it to drive continuous improvement throughout the organization's Incident Management practices

But . . .
while the process makes sense, it still doesn’t shed light on what tools should be used in order to ensure speed and efficacy.

Some wise words from Google

Even the good folks at Google, who 'wrote the book' on many things – also include a chapter in their SRE book on what makes for effective incident management.

According to Google, the following components make for well-designed incident management:

1 Recursive Separation of Responsibilities

"A clear separation of responsibilities allows individuals more autonomy than they might otherwise have, since they need not second-guess their colleagues."

2 Live Incident State Document

"This can live in a wiki, but should ideally be editable by several people concurrently."

3 Clear, Live Hand-Off

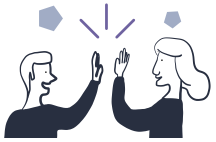
from the incident commander to his/her stand-in.

4 A Recognized Command Post

"Interested parties need to understand where they can interact with the incident commander."

Is good planning good enough?

While the insights from both ITIL and Google are instructive, the question really is, how can organizations implement these processes and plans effectively, and maximize the capabilities of their point-solutions, so they can:

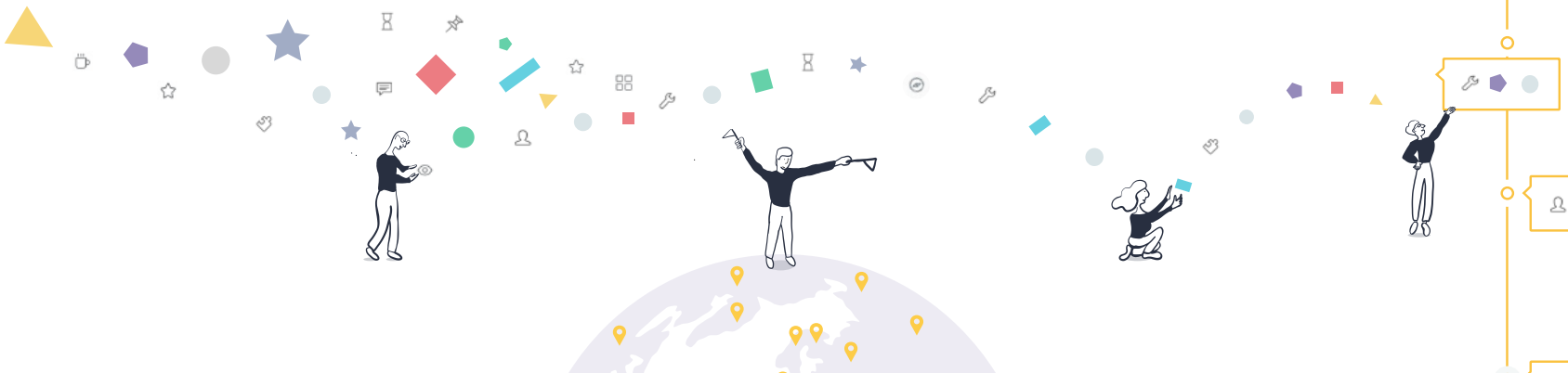


Ensure effective collaboration

Eliminate wasting time on continually repeating summaries

Avoid duplication of efforts

and, ultimately, of course
– ensure the fastest time to resolution.



Point solutions just can’t cut it

Maybe we have good processes on paper, but the tools that are available for handling critical incidents are stand-alone solutions – which don’t cover every aspect of the incident.

These include alerting, ticketing, paging, monitoring, and other communications systems.

They may be very good at detecting and alerting to drive awareness. Some, even enable cross-functional, cross-border communications.

However, these tools are siloed point solutions that fail to cover the entirety of the complex incident management process.

The 7 key capabilities for gaining command & control of critical incidents

As such, these solutions do not enable organizations to acquire the critical capabilities that are mandatory for quickly and effectively resolving a critical incident.

What organizations need is a more comprehensive approach so they can gain command and control of critical incidents by ensuring that:

"Interested parties need to understand where they can interact with the incident commander."

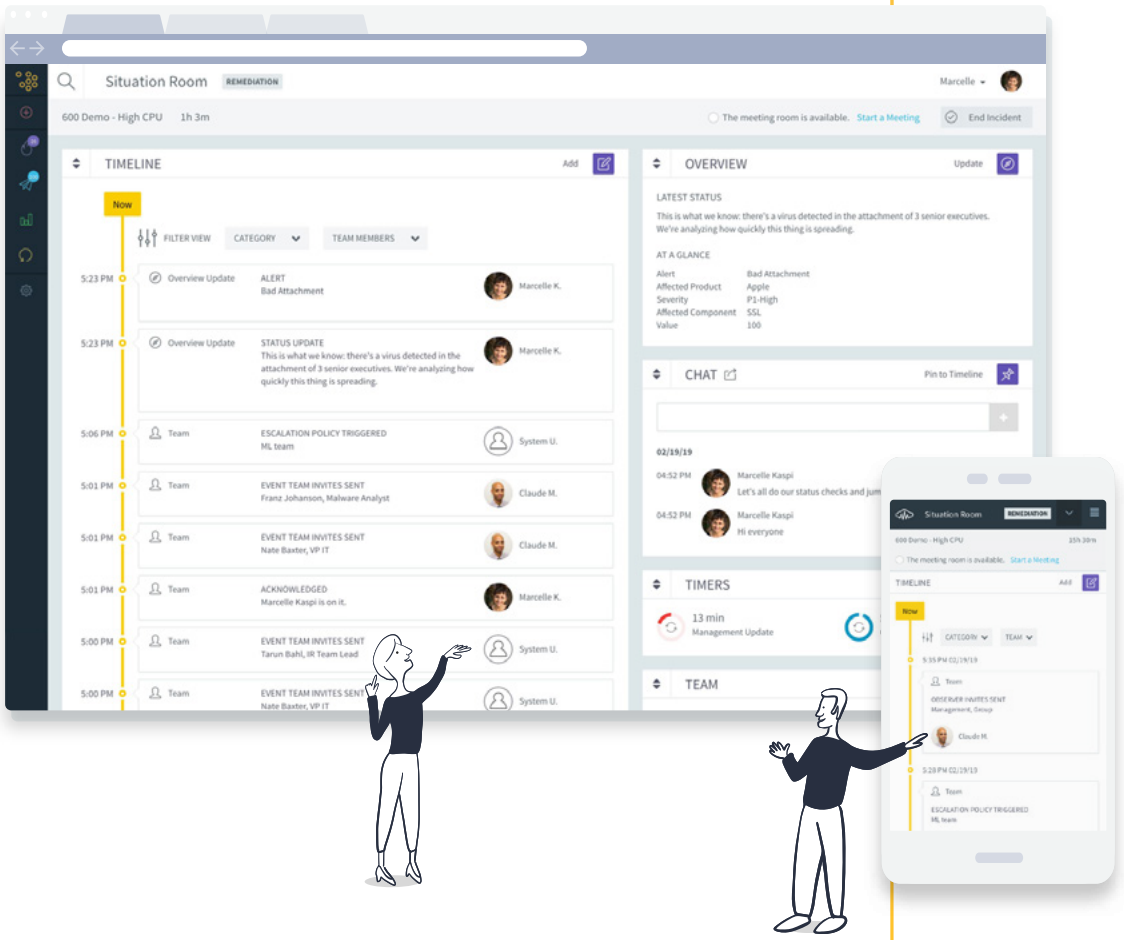
1. All the right people, whether inside or outside the organization are onboarded immediately
2. Everyone is always on the same page
3. Alerts and updates are automatically pushed to the right people at the right time
4. Workflows are seamlessly executed
5. Documentation is effortless and easily accessible
6. Post-mortems are prepared quickly and with accuracy
7. All the relevant incident management and response tools are seamlessly integrated into the process, with unified actions, updates, and documentation

How Exigence can help

Exigence offers a platform that provides complete command and control of critical incidents, whether for technology operations, security, or drills and business continuity tests.

It uniquely addresses every aspect of the incident, turning an unstructured situation into one that is structured and easy to manage.

The platform coordinates all stakeholders and systems all the time, orchestrating complex workflows from trigger to resolution, simplifying the post-mortem, and leveraging lessons learned for ongoing optimization.



Delivering the key capabilities for command & control of critical incidents

Exigence enables organizations to:
Management practices

1 Automatically onboard internal and external incident stakeholders

2 Optimize all relevant incident management tools through seamless integration

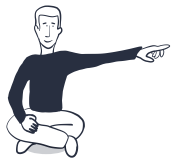
3 Have one single, integrated interface for tracking and managing every aspect of the incident including tasks and actions

4 Automatically push alerts and updates to the right people at the right time

5 Have a centralized repository for real-time knowledge access and management

6 Effortlessly and easily access to incident summary, reports, and other documentation

7 Accelerate the root cause analysis to a minimum



Critical Incident Resolved

About Exigence

Exigence was founded in 2016 in heart of the ‘Silicon Wadi’ in Israel. The Exigence team brings extensive experience in complex, cross-organizational workflows, optimizing operations, global IT and IS organizations, cloud-based computing, and ideating – developing – and bringing to market technology solutions for strategic business challenges.

To learn more how Exigence can help you gain command and control of your critical incidents, we invite you to reach out to us at info@exigence.com

It’s time to show critical incidents who’s boss!

www.exigence.io