Opsgenie

The Language of Incident Management

The Language of Incident Management

Introduction

Language used across the high technology ecosystem is dynamic to say the least. Nowhere else can you find a mixture of technical jargon seamlessly intertwined with references from science fiction, mythology, pop-culture, literature, and more.

While this makes conversations heard across technical environments colorful and engaging, it also makes communications allegorical and metaphorical– opening them to variable interpretation.

At times when communication is more relaxed, this style of conversation can be seen as engaging and playful. However, when incidents happen, the level of severity shifts and a different language appears altogether. Based upon the potentially massive impact of IT incidents across business operations, the language of incident management must be technically precise, actionable, and leave no room for misinterpretation.

Why is this shift in communication necessary? Because modern IT operations are the nexus of businesses operations. If a system goes down, the impact is immediate and significant– costing tens to hundreds of thousands of dollars for every minute of downtime.

With this level of severity, it makes sense that many of today's terms used in IT incident management are taken directly from terms widely adopted by disaster response teams. Terms that are clear and understandable in chaotic enviroments. Terms that help teams work together to remediate an incident as quickly as possible.

This white paper was created to serve as a foundation for teams to improve communication through the entirety of an incident. It highlights and defines essential terms that aid in clear and accurate communication during an incident.

For additional context, these terms have been further categorized according to which of the five stages of the incident lifecycle that they are most likely to be used. These stages consist of: Planning, Detection and Alerting, Containment, Remediation, and Analysis and are indicated by a corresponding icon, outlined in the key below.

*For additional information on the stages of an incident,

download "The Five Stages of Incident Management, and How to Improve Them."

Planning

The stage of incident management in which incidents are anticipated and their remediation processes are thought out beforehand.

Detection & Alerting

The stage of incident management in which incidents are made known in whatever service they affect.

Containment

The stage of incident management in which an incident has been detected and now efforts are aimed at making sure the incident does not affect any other service or function.

Remediation

The stage of incident management in which corrective actions are taken to resolve an incident.

Analysis

The stage of incident management in which an incident has been resolved and now needs to be inspected to further improve resiliency, the remediation process, etc.

A

Acknowledge / Ack	⚠	An alert action that notifies other alert recipients that the alert has been seen and is being worked on.
Actionable Alert	📋 ⚠	An alert which clearly describes an issue, is routed to the right people at the right time, and communicates not only the urgency but the issue's scope of impact.
Active Monitoring	📋 ⚠	Method of understanding the current status, or changes in status, of a service via regular checks.
After Action Review (AAR)	🔍	The analysis that takes place after an event, describing specific details surrounding what occurred, why it occurred, and areas for improvement to prevent the event from happening again. After-action reviews are often known as Postmortem or Post Incident Analysis reports.
Agreed Service Time	📋 ⚠	The time period for a service to be available and performing its expected function.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

A

Alert · Responder Alert · Owner Alert · Associated Alert	⚠	An alarm or warning for an event that may affect operations or a service. · An alert sent to the parties/teams who are directly responsible for taking action. · An alert that signifies which team owns the service affected. · An alert that represents a part, or symptom, of a larger event or incident.
Alert Noise	📋 ⚠ 🩹 🔧 🔍	The result of an overwhelming amount of alerts being created in a short amount of time, complicating the ability for alert responders to accurately identify what services are affected.
Alert Fatigue	⚠	When alert responders become overwhelmed with the volume or frequency of alerts and their ability to respond suffers.
Asset / Asset Management	📋 ⚠ 🩹 🔧 🔍	Components of any system or network that holds business value. These components are managed to understand the impact the asset has when deciding to remove or update, for example.
Audit	📋 🔍	A formal examination into a system or process that checks on system availability, use, and/or whether guidelines and policies are being followed.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

A

Availability	📋 ⚠ 🩹 🔧 🔍	The quality of a service to function as expected for users during an agreed service time.

B

Back-out	🔧	The action of restoring a service to a previous reliable state or baseline in order to provide expected functionality to users if an update or release was unsuccessful.
Backup	📋	A stored copy of data or redundant system available to be used in case the original is compromised or lost.
Baseline	📋 🔧	A reference point for expected behavior to measure changes, improvements, or to use as a revert point if the former causes failure.
Benchmark / Benchmarking	📋	A reference point that functions like a baseline to measure progress against past benchmarks and other comparative data.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

B

Best practice
· Good practice

🔧

Best practice is typically thought of as an industry's "best" way to complete a task. However, since technology is ever-changing and environments are unique to each organization, this term is often viewed as being too restrictive by definition as it holding methods up to an impossible standard.

· Good practice is often used in place of “Best Practice” as the term allows greater flexibility in its application as it compensates for different interpretations from company-to-company, the constant innovations of new technologies, and for the creativity to create new good practices instead of limiting problem solving to one ultimate standard.

Bug

⚠

An unintentional problem in software, code, programs, etc that may cause failure or abnormal behavior.

Business Impact Analysis

📋 🔍

The systematic evaluation of potential effect on business should a service suffer from disruption or downtime, and requirements for recovery in the case of such an incident.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis ✂ Containment

C

Capacity	⚠ 🩹	The measurement for the maximum amount of throughput able to be transferred between networks or delivered via a service.
Change **· Change History** **· Change Management**	⚠ 🩹 🔧 🔍	Any alteration made to an IT service, configuration, network, or process, with a scope that includes documentation. · The comprehensive record of alterations made to any of the above from the beginning of its lifecycle to current state. · The method of controlling the entire change history and lifecycle to understand what changes yielded overall improvements and to minimize the possibility and impact of any change-related incidents.
ChatOps	📋 ⚠ 🩹 🔧 🔍	Leveraging chat and collaboration tools for incident management, especially to automate actions and the retrieval of supporting information.
Closed	🔧	The closed state is conclusive, indicating that all necessary actions have been taken.
Code of Practice	📋	Guidelines that express standards of doing business and reflect objectives of a company.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

C

Cold Standby (Gradual Recovery)	🔧	A recovery option where expected recovery is expected to take days or weeks. Infrastructure is provisioned but hardware and software is not included in this recovery option.
Cold Start	⚠	A latency experienced when a function is triggered.
Communications Lead	📋 ⚠ 🩹 🔧 🔍	The individual who, during an incident, is in charge of orchestrating collaboration and relaying relevant information across teams.
Compliance	📋	Being in accordance with any regulations in place. Can trigger an alert if a system or configuration item falls out of compliance.
Component Failure Impact Analysis	🔍	The process of determining the impact on a service if one component or configuration item stops working as expected.
Concurrency	⚠	The measure of how many of the same things are happening simultaneously in a system, such as how many users are accessing the same operation or performing the same transaction.
Configuration	📋	The arrangement of items or services that help deliver a specified output.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

C

Configuration Management System	📋	A system of organizing all the information used to support various services or products a company uses and provides. Maintains the operational information for configuration items, as well as design, record of incidents, and any other relevant data.
Context	⚠ 🩹 🔧 🔍	The surrounding events or environment that provide relevant information about an incident or alert.
Control	📋 ⚠ 🩹	Procedures and policies that manage risk, ensure the product or service operates as expected, and that compliance is followed.
Core Service	📋 ⚠ 🩹 🔧 🔍	A service that provides a central function for users and/or customers.
Countermeasure	🩹	A specific reactive action taken in effort to protect a system or restore operations.
Customer-facing Service	📋 ⚠ 🩹 🔧 🔍	Services which customers use and interact with.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

C

Cynefin framework

A decision-making construct that has been adapted to incident management processes to help managers identify how they perceive situations and to organize the most effective response. Cynefin defines incidents as being Simple, Complicated, Complex, or Chaotic and then outlines responses based on this assignment.

D

Dashboard ⚠ 🔍

A single-pane visualization of systems, alerts, and incidents designed to organize the presentation of information from disparate tools, with contextual information provided in a clean and precise format.

Dependency 📋 ⚠ 🩹 🔧 🔍

The relationship between two services, processes, or configurations that rely on one another to function.

Deprecation 📋 🔍

A feature or tool that is being taken out of service, is no longer in use, or is no longer being updated.

Diagnosis 🔧 🔍

The process and final result of understanding the incident and what caused the incident to occur.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

D

Diagnostics	🩹 🔧 🔍	The "symptoms" or signs that contribute to a diagnosis during an incident.
Downtime/Outage	🩹 🔧	The period of time or the occurrence of a service not performing or available as expected.

E

Emergency Change	🩹	An update or patch fix to be deployed rapidly, usually as part of incident resolution efforts.
Enabling Service	📋 ⚠ 🩹 🔧 🔍	A service which is necessary for a core service to work and be available to customers, but is not offered to customers outright itself.
Environment **· Development Environment** **· Test Environment** **· Production Environment**	📋 ⚠	A type of IT infrastructure in which to work on a particular process. It also provides context for which and what kind of exterior conditions are affecting whatever process is being worked on. · The infrastructure in which a service, feature, process, configuration item, etc. is being worked on and created. · The infrastructure in which a service, feature, process, configuration item, etc is verified for expected functionality. This environment is controlled more closely to replicate the actual production environment. · The infrastructure in which a service is delivered to a customer. The deliverables in this environment are live, therefore it is also referred to as live environment.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

E

Error	⚠ 🩹 🔧	A mistake which causes failure of a configuration item or service entirely. This can be a mistake in the design, processing, or plain human error.
Event	⚠ 🔍	A notable system or service occurrence. Can occur due to user action or be indicative of an alert or incident.
Exception Report	📋	An account of defined thresholds being exceeded for key performance indicators, usually in a negative way.

F

Failure	⚠ 🩹	When something with an expected output stops functioning and delivering that output.
Fault Tolerance	⚠ 🩹	The ability of a service to continue operating even if some configuration item or part fails.
Fault Tree Analysis	🔍	A technique used to determine the different events which le d to an incident. This analysis is used to predict what may cause incidents in the future, and often is used in trying to determine the root cause.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

F

Fix	🔧	An action or method of repair.
Fixed Asset	📋	A physical valued part of a business that has longevity. An office, computer, or license can be considered fixed assets.
Forensics **· Investigation**	🔧 🔍	The programmatic investigation into a computer system for the purpose of identifying incidents. · The gathering of the scientific elements and evidence that point to the cause of an incident.
Functional	📋 🔍	Able to perform as expected.

G

Gradual Recovery	🔧	[See Cold Standby]

H

Hot Standby	🔧	A recovery option in which there are redundant assets running simultaneously to support an IT service in case of failure.
Hotfix	🩹	An update applied to a software in order to solve a problem or software bug. Often used to solve a customer issue specifically.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

I

Immediate Recovery	🔧	A recovery option that uses redundancy, or mirroring, to restore systems in case of failure. See [Hot Standby].
Impact	📋 ⚠ 🩹	A measurement for the cost, whether financial or of reputation, that a service disruption, incident, or change causes.
Inactionable Alert	⚠	An alert that does not empower a responder to take action- often lacking contextual information, is routed to the wrong people, and has an unclear scope.
Incident **· Incident Response** **· Incident Management**	📋 ⚠ 🩹 🔧 🔍	An event of unplanned failure, service interruption, or reduction of expected quality of service, which often impacts business needs. · The manner in which an incident is reacted to, often planned in preparation for an incident. Methods and protocols set forth to be carried out, and individuals are established to act when an incident occurs. · The process of planning, monitoring and alerting, containing, remediating, and analyzing incidents.
Incident Commander	📋 ⚠ 🩹 🔧 🔍	The individual who holds ultimate control and decision making capacity during an incident.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

I

Incident “Lifecycle”	📋 ⚠ 🩹 🔧 🔍	The series of changes an alert/incident undergoes from creation to resolution.
I/O Metrics	📋	Input and output data. Often the basis for companies to base goals upon, input metrics are behaviors controlled by a company in order to achieve particular output metrics.
Incident (Response) Orchestration	📋 ⚠ 🩹 🔧 🔍	An Opsgenie offering which consists of components and features for users to utilize during incident resolution to help organizations quickly and effectively identify problems, notify the right people, facilitate communications across business units, and collaborate.
Incident Record	🔍	The compilation of details and process of resolution for a given incident.
Incident Responder	⚠ 🩹 🔧	Individuals and/or teams responsible for the investigation and remediation of an incident.
Incident Stakeholders & Observers	⚠ 🩹 🔧 🔍	Individuals who need to be kept abreast of an incident, and who may influence incident resolution, but are not active responders.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

I

Intermediate Recovery 🔧

A gradual recovery option which has some fixed components but restoration and most configuration will need to be performed to get systems recovered, which can take more than 24 hours. See [Warm Standby].

ITIL / Information Technology Infrastructure Library 📋

A set of widely accepted practices that aim to help companies set their IT services to directly correspond with their business needs and goals.

ITSM / Information Technology Service Management 📋

All aspects of the processes and procedures followed to deliver an IT service to customers. This involves all aspects of the service lifecycle from design to delivery.

K

Kepner and Tregoe analysis 🔍

A problem solving method which evaluates all aspects of a problem, separate from a final decision on cause. The goal of this analysis is to determine cause after a comprehensive understanding of the problem.

Key Performance Indicators 📋 🔍

The individual measurements of the success of a service or IT process or configuration. These KPIs are decided upon in advance to establish alerting thresholds or base reports on goal achievement.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

K

Known Error	📋	A preexisting bug or problem that has been identified in a service and for which a workaround has already been implemented.

L

Latency	⚠	A delay experienced during the transfer of data.
Logs	🔧 🔍	The records of all events related to a service or application. Data transferred, times and dates, incidents, changes, errors, etc.

M

Maintainability	📋 🩹 🔍	The property of a service that describes how easily changes can be applied successfully in a desired time frame.
Manual Workaround	🩹 🔧	A solution executed "by hand" i.e, not automatically.
Mean Time Between Failures	📋 🔍	Measurement of average time between a service malfunctioning and not delivering expected outputs. These analytics are useful for reports and are measured from the time the service becomes healthy from one failure, to the time when the next failure occurs.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

M

Mean Time Between Service Incidents	📋 🔍	Measurement of average time between service interruptions that are classified as incidents, the service is unavailable, or not performing at the quality expected.
Mean Time to Repair	📋 🔍	Measurement of average time between initial notification and final remediation of a problem.
Mean Time to Restore Service	📋 🔧 🔍	Measurement of average time required to bring a service back to operational functionality and availability Mean Time to Restore may or may not reflect final resolution of an incident and/or the systems involved in it.
Model / Modeling	📋 🔍	A representation of an actual system, service, application, etc.
Monitoring	📋 ⚠ 🩹 🔧 🔍	The repeated process of checking a service or process to ensure it is functioning as expected and to detect events that indicate a disruption or change in status.

N

Normal Change	📋	An expected update/fix that follows the change management process and is not done in an emergency or as a workaround.
Notification	⚠	A delivered message in some form (mobile, email, etc.).

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

On-Call Terms

Escalation **· Functional** **· Hierarchical**	📋 ⚠ 🩹 🔧 🔍	The method used to notify responders of an incident or alert according to a pre-configured order and timeline. · An escalation method where the alert or incident is transferred to an individual with more expertise for assistance. · An escalation method where the alert or incident is transferred to a more senior individual for assistance.
First-line Support	⚠	The responder expected to react first to an incident. This is often the support person on-call.
Follow the Sun Schedule	📋 🔍	A method of customer support or incident management leveraging rotating on-call rotations across timezones to provide 24/7 coverage.
Incident Mitigations	🔧	Initial actions performed by First Responders with the goal of beginning remediation efforts before a full investigation has been completed for the incident.
On-Call Rotation	📋	The change in responsibility from one IT responder to another to respond to issues during a specified time period. On-call rotations are components of on-call schedules.
On-Call Schedule	📋	The organization and assignment of the responsibility for IT responders to respond to issues during a specified time period.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

O

Observability	📋 🔍	The property of a system for how much can be inferred accurately from outputs.
Operations Bridge	📋	The physical location where monitoring of IT services takes place.
Operations Lead	📋 ⚠ 🩹 🔧 🔍	The individual responsible for overseeing daily operations, that services are running as expected. During incidents, the Operations Lead is reported to by engineers with updates on a resolution.
Outage Period	⚠ 🩹 🔍	The interval of time in which a service or part of a service is not functioning as expected.
Outcome	⚠ 🔧 🔍	The result of an IT related event, process, or change. Outcomes can be discussed as both what is anticipated and the actual result.

P

Pain Value Analysis	📋 🔍	The process of identifying the impact of incidents. This is usually based on several factors: duration of incident or outage, users affected, cost, etc.
Passive Monitoring	⚠	The process of monitoring (checking the functionality of a service) where the only indication of an issue is via an alert or notification.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

P

Peacetime	📋	The time for which services and operations are functioning as expected, without any service disruptions.
Performance	📋 ⚠ 🩹 🔧 🔍	A measure of achievement for any IT-related person, system, service, configuration item, etc.
Performance Degradation	⚠ 🩹 🔧 🔍	The measurement of how much the performance of an IT-related item has decreased due to an event.
Planned Downtime	📋	A period of time where an IT service is expectedly and intentionally unavailable for the purpose of maintenance or updates.
Postmortem / Post-Incident Analysis	🔍	The process of understanding an incident after it has been resolved for the purpose of improving response processes or understanding causation.
Priority	⚠ 🩹 🔧	Conveys the severity, urgency, and/or potential impact by assigning a level to an alert/incident so that responders can react accordingly.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

P

Problem Record	📋 🔍	A document which covers every aspect of an issue, from its entire lifecycle.
Process Manager/Owner	📋	The individual in charge of overseeing the operations around protocols and steps required to achieve certain goals. They oversee the entire lifecycle of a process, from the planning to execution.
Projected Service Outage	📋	A document which outlines how future maintenance or tests will affect normal service levels.

Q

Quality Assurance	📋	The process of testing to ensure standards are met for anything IT-related, from documentation instructions to a new feature.
Quality Management System	📋	The framework in place to ensure and evaluate that an organization is meeting objectives and expected outcomes.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis ✱ Containment

R

Reactive Monitoring	⚠ 🩹 🔍	The process of monitoring (checking the functionality of a service) that is only done in the event of an error or incident.
Recovery **· Recovery point objective** **· Recovery time objective**	🔧 🔍 🩹	The process of returning a service, system, etc. back to baseline functionality and health. · The maximum amount of data to be lost during restoration in relation to the amount of downtime. · The maximum amount of time tolerated for a service interruption.
Release **· Release Management**	📋	A change that is deployed to users. Could be any kind of configuration item. · The planning, design, testing, scheduling, troubleshooting, and deployment of changes. Basically, the overseeing of the entire lifecycle of a release.
Resiliency	📋 🔍	The property of an IT system or service for the capacity to recover in a desired time frame and to resist failure in the first place.
Resolution	🔧	The action or process of taking an action to bring systems to normal functionality.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

R

Response Team (AKA Team)

📋 ⚠ 🩹 🔧 🔍

The operational units in a organized structure that respond to alerts and incidents. These units can be grouped by technical specialization, activity, services responsible, geography, or any combination of those (or others).

Response Time

⚠ 🩹

The measure of time that it takes to recognize and take initial action for any single event which warrants a response.

Risk
• Assessment
• Management

📋

An event that can harm a valuable business asset.
· The process of identifying the value of an asset, potential threats to that asset and their potential impact, and how susceptible an asset is to those threats.
· The process of handling threats by identifying them and then controlling them in regards to the asset they potentially impact.

Root Cause

🔧 🔍

Typically thought of as the true singular reason for the failure of a service or application. However, there are many factors that contribute to failures and outages, so the use of this term is debatable as it can be potentially misleading when multiple factors are interconnected in the cause of an incident.

Runbooks

⚠ 🩹

Detailed procedures and processes executed by a system administrator or NOC. Runbooks can be created in digital or physical form.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

S

Scope	🩹	The extent of a problem, solution, project, capability, etc.
Scribe	🔧	The individual responsible for documenting the incident and processes during remediation.
Second Line Support	📋 🩹 🔧	The individuals who are included in the remediation process who have more capability (time, experience, knowledge, resources) to solve the issue in the case that first responders need help.
Service (IT Centric) **· "Always-On" Services** **· Service Change**	📋 ⚠ 🩹 🔧 🔍	An offering made to customers that holds value and solves a customer's pain point. · A service that is expected to run continuously for whatever purpose a user intends. · Alterations made to a service, such as updates, fixes, or deprecation of a feature.
Service Desk	📋	A service or team of individuals which takes customer support requests and serves as a point of contact between customers and internal IT personnel.
Service Failure Analysis	🔍	The process that inspects a service disruption for cause. This is done to investigate opportunities to improve resilience of an IT service.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

S

Service Level Agreement	📋	A commitment made between a service provider and a consumer or customer. This agreement outlines expectations surround quality or targeted functionality.
Service Level Indicators	⚠ 🩹 🔧	The actual metrics that represent the reliability of a service.
Service Level Objectives	📋 🔧	The targeted goals for the reliability of a service.
Severity	⚠ 🩹 🔧	The degree to which a service is affected by an incident, including: duration of outage, effort required to remediate, and potential business impact.
Single Point of Failure	📋 🩹 🔍	The one variable for which an incident depends on to function, such as an essential configuration item or personnel involved.
SLAM Chart	📋 🔍	A Service Level Agreement Monitoring Chart records progress and data on the service level targets.
Specification	📋	A formal record of requirements of some IT-related configuration item. For the purpose of adhering to Code of Practices and Standards.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

S

SRE (Site Reliability Engineer)	📋 ⚠ 🩹 🔧 🔍	Individuals whose focus includes: automating manual tasks, managing SLOs, sharing tools with developers to understand the services of their organization, and heavy involvement in the incident remediation processes.
Standby	📋	Resources not actively used but still available to support IT continuity plans.
Status **· Status Page**	⚠ 🩹 🔧 🔍	The current condition of a service. · A page that includes the current condition of a service, often accompanied by status updates from the responsible company or team.
Subject Matter Expert (SME)	🩹 🔧	An individual with a specific knowledge on a particular issue, service, etc.

T

Tech Stack		The programming languages, software, and components that make up an application. There are two sides to a tech stack: the front-end (customer-facing) and back-end (developer-facing).
Technical Observation	⚠	A technique used by IT professionals of monitoring and IT Service to understand availability, problems, and areas for potential improvements.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

T

Tension Metrics	⚠ 🩹 🔧 🔍	Data which, when one set or point is changed, affects other data points negatively.
Threat	📋 ⚠ 🩹 🔧	A potential event which could harm a service via a vulnerability.
Threshold	⚠	A point identified for which alerts are generated when crossed.
Timeline	⚠ 🩹 🔧 🔍	The comprehensive listing of events that occur, changes/fixes applied, outcomes, etc and when they occured during an incident.
Trend Analysis	📋 🔍	An investigation into time-related patterns.
Triage	⚠ 🩹 🔧	The process of identifying all parts of an incident or problem and planning the remediation process.

U

Urgency	⚠ 🩹 🔧 🔍	A measurement for how long it may take for a service disruption or incident to impact business. Urgency contributes to the priority assigned to an incident.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

V

Variance		Inconsistencies between values.
Verification	⚠ 🔧	An activity which confirms that an incident has occurred, or has been resolved to the expected standards.

W

Wartime	⚠ 🩹 🔧	The time during which an incident has occurred and is being triaged and remediated.
Workaround	🩹 🔧	A successful way of implementing a fix to the point that most functionality is still available but the underlying incident is not yet resolved.
Workload	⚠ 🩹 🔧	The resources (time, and both human and machine labor) needed to deliver an IT service.

📋 Planning 🔧 Remediation ⚠ Detection & Alerting 🔍 Analysis 🩹 Containment

Conclusion

Fast and effective incident management is the lifeblood of any organization's IT operations. With high costs at stake, it is easy to see why the most successful teams adopt a "wartime" posture during an incident. It's also easy to see why communication during wartime must be must be specific, direct, and actionable in order to communicate clearly while identifying an issue, what actions need to be taken, and by who.

As our technology platforms have become infinitely more complex and intertwined, the frequency and severity of incidents will only continue to grow. By focusing language used during an incident, teams can better collaborate in finding the fastest resolution possible.

For additional reading on modern incident management, visit the OpsGenie Resource Library:

https://www.opsgenie.com/resource-library

About the author

Elizabeth Reizinger

Elizabeth Riezinger is a Technical Writer for OpsGenie (acquired by Atlassian). She works collaboratively with the engineering team to write and edit documentation, optimize documentation with relevant visuals, and execute content strategy with documentation collateral. Due to her understanding of DevOps principles, she has helped deliver many projects that support organizations that are modernizing their incident management processes.