MICROSEC.AI

Cloud IT Security Incident Management Overview With Sample Incident Report

The objective of the IT Security Incident Report is to get IT services back up and operating as quickly as possible. An IT Security Incident management process should include automated detection and remediation tools, a clear workflow process, and detailed incident reports. IT Service Management (ITSM) have been around for a while but in the modern era of cloud computing, there are a few new tools that need to be incorporated.

For both cloud and on-prem environments, an IT Security Incident Report is a vital record that tracks the details of specific incident occurrences. It is used by software development, cybersecurity operations, cloud security, customer service, compliance, and risk management organizations.

An effective incident report includes details such as what happened, when it happened, the nature of the occurrence, the business impact, and so on. A clear and detailed incident report is quintessential to analyze problems holistically and identify solutions to improve service delivery. We have included a sample Security Incident Report form at the end of this document that you can use for personal reference.

Types of Incidents

There distinct types of incidents occur in IT infrastructure: major incidents, repeated incidents, and complex incidents.

- **Major incidents:** Large-scale incidents such as application failures and cyber-attacks don't happen very often. However, when they do they can cause disruptions in businesses. Businesses must be prepared to deal with major incidents swiftly and effectively.
- **Repetitive incidents:**Misconfiguring IT devices or applications can lead to a recurrence of incidents. Escalating and prioritizing the problems are the best ways to deal with it. Such incidents may or may not have a significant impact, but they will accumulate and will require time to resolve.
- **Complex incidents:** The majority of the incidents that occur are of a medium or low severity, which are fairly simple to resolve. However, a critical or high-level incident requires an immediate response and may be more complex to resolve.

Incidents are often categorized based on severity such as: critical, high, medium, and low (or L1, L2, L3). Severity ratings play a key role in assessing impact on the business and urgency of the issue.

Automated Incident Response Tools

Deploy tools to automate and assist with detection, analysis, and remediation of security problems. Modern cloud environment tools include:

- **Cloud Data Loss Prevention (DLP) and Data Security Posture Management (DSPM)** to classify and protect confidential data
- **Network and traffic analysis with microsegmentation** to limit the lateral movement of an attack or confidential data
- **Cloud-Native Application Protection Platform (CNAPP)**, a combination of CSPM and CWPP
- **Anti-malware, Extended Detection and Response (XDR),** to detect threats and attacks
- **Security Information and Event Management (SIEM),** to correlate security information and events from multiple sources
- **Security Orchestration, Automation, and Response (SOAR),** to coordinate and execute tasks between people and tools
- **Firewall, intrusion prevention, and denial of service (DoS),** to block attacks at the perimeter

Incident Management Workflow

Incident reporting and management should always be prioritized. It is imperative to have a well-organized approach for the organization to use to respond to non-compliance, system failures, incidents, accidents, cyber-attacks, outages, and breaches.
Be prepared before an incident occurs. Roles and responsibilities should be clearly defined based on skills and requirements. It must be clear who is responsible for what actions in the case of an incident. Employees need to be trained on the incident management workflow.

An incident management workflow should:

- Identify the incident and assign severity based on impact and urgency
- Notify all impacted stakeholders
- Assigning tasks to the correct individuals
- Tracking the incident from detection to resolution and closure
- Escalation (if required) for breach of SLAs
- Generate reports and documentation for investigation and root cause analysis
- Resolution and remediation
- Closure

*Note: You should have a no-approval process for resolving incidents**

Communication with stakeholders is essential. Stakeholders are not only members of the IT and Risk & Compliance organizations they also include employees, customers, partners, and regulators. Regularly share announcements, notifications, and status updates as appropriate with all stakeholders. Do not rely solely on email, this often requires phone calls and meetings.

Essential Elements of an Incident Report

The individual experiencing a problem or the team supporting related operations creates an incident report with input from others involved in resolving it.

A brief report is recommended if the occurrence is minor and has little impact. However, if the incident is serious, all information must be recorded in addition to preparing an extensive incident report. The person creating the incident report uses input from others involved to resolving the incident.

KEY INFORMATION TO INCLUDE

- Name of the individual who prepared the incident report
- Correct date and time the incident was detected and resolved
- Identification of which services were affected and/or unavailable
- A concise and detailed description of the incident with the actual details
- Whether or not SLAs (service level agreements) were breached, and if the incident requires a penalty or escalation
- Compliance requirements
- Document all remediation actions and troubleshooting methods
- Record any business impacting details including outages, investigations, publicity, customer remediation, regulatory, etc.

INCIDENT REPORT DOS

- Describe relevant issues in detail
- Focus on the facts
- Assume that the report will be made public (even if it is initially confidential)
- Make sound professional decisions based on severity and business impact
- Consider underlying circumstances
- Determine if the incident indicates a security breach has occurred
- Developed a feasible remediation strategy
- Understand your incident reporting policy and procedure
- Use professional terms and write legibly
- Include the names and addresses of any person (employees, contractors, partners, customers, etc.) who are aware of the situation

INCIDENT REPORT DON'TS

Speculate and assume without knowing the facts
Discuss sensitive occurrences
Talk about money, costs, and spending decisions
Discuss failures or delays in acting
Predict what will happen if nothing is done
Include insignificant facts that implicate or blame anyone for the occurrence

Sample Incident Report

Incident response teams should make an initial incident report and then continue to report updates and additional information to their Chain-of-Command-Security Specialist (as collected).

1. CONTACT

Full Name
Job Title
Division or Office
Work Phone
Mobile Phone
Email Address

Additional Contact Information:

2. ISSUE (CHECK ALL THAT APPLY)

- ☐ Account Compromise (lost password, suspicious account behavior, etc)
- ☐ Unauthorized Access (cloud, systems, applications, storage devices)
- ☐ Denial-of-Service (including distributed)
- ☐ Data Exposure (public access, public share, breach of sensitive data)
- ☐ Malware (virus, worm, trojan, crypto, etc)
- ☐ Misconfigurations (exposed secrets, default passwords, risky setting, etc)
- ☐ Misuse of Systems (acceptable use)
- ☐ Social Engineering (phishing, scams)
- ☐ Reconnaissance (scanning, probing)
- ☐ Technical Vulnerability
- ☐ Unpatched or Unmanaged System
- ☐ Theft/Loss of equipment or media
- ☐ Open Port

Description of Incident:

3. SEVERITY AND SCOPE (CHECK ALL THAT APPLY)

- ☐ Critical (affects system-wide information resources)
- ☐ High (entire network, cloud, or critical business systems)
- ☐ Medium (affects infrastructure, network, cloud, servers, or admin accounts)
- ☐ Low (only affects workstations or user accounts)
- ☐ Unknown/Other (please describe below)

**Note: All incidents deemed critical or high require additional notification by phone*

Estimated quantity of assets affected
Estimated quantity of users affected
Third parties involved or affected (vendors, contractors, partners)

Additional Information:

4. IMPACT (CHECK ALL THAT APPLY)

- ☐ Loss of Access to Services
- ☐ Propagation (other regions, segments, assets, partners, customers...)
- ☐ Loss of Productivity
- ☐ Unauthorized Disclosure of Information
- ☐ Loss of Reputation
- ☐ Unauthorized Modification of Information
- ☐ Loss of Revenue
- ☐ Unknown/Other (please describe below)

Additional Impact Information:

5. SENSITIVITY OF AFFECTED DATA/INFORMATION (CHECK ALL THAT APPLY)

- ☐ Critical Information
- ☐ Personally Identifiable Information (PII)
- ☐ Non-Critical Information
- ☐ Intellectual/Copyrighted Information
- ☐ Publicly Available Information
- ☐ Secrets (critical infrastructure/key resources)
- ☐ Financial Information
- ☐ Protected Healthcare Information (PHI)
- ☐ Payment Card Information (PCI)
- ☐ Unknown/Other (please describe below)

Data encrypted?
Location of data (bucket/blob, file, queue, attached volume, persistent volume, network segment)
Quantity of data affected (number of records, files, accounts, locations, assets...)

Additional Affected Data Information:

6. SYSTEMS AFFECTED (PROVIDE AS MUCH DETAIL AS POSSIBLE)

Attack Sources (IP address, port, etc)
Attack Destinations (IP address, port, etc)
IP Addresses
Domain Names
Primary Functions of Affected Systems (web server, domain controller, etc)
Operating Systems of Affected Systems (versions, service pack, configuration, etc)
Patch Level of Affected Systems (latest patches loaded, hotfixes, etc)
Security Software on Affected Systems (anti-malware, firewall, versions, date of latest update, etc)
Affected Systems/Assets Configuration (group account, security group, asset ID, etc)

Additional System Details:

9. REMEDIATION (PROVIDE AS MUCH DETAIL AS POSSIBLE)

Actions taken to identify affected resources
Actions taken to remediate incident
Actions planned to prevent similar future incidents

Additional Remediation Details:

In Conclusion

Incidents happen and should be viewed as an opportunity to learn and improve. Avoid the blame game, it must be safe for employees to report incidents when they are detected. You do not want team members hiding incidents to avoid negative repercussions.

Close documentation and a postmortem analysis of an incident is a valuable tool to improve team execution. If you always close out an incident with a review of what you have learned and how you can improve, you'll perform better when faced with similar issues in the future.

About Microsec.ai

Get easy-to-deploy, runtime visibility, protection, and compliance monitoring for cloud serverless, VM, and Kubernetes environments. Microsec.ai is the only agentless, data-centric, runtime cloud-native application protection platform (CNAPP) that protects your data and applications with data loss prevention (DLP), east-west network traffic control with self-healing micro segmentation, security posture management, and compliance analysis in one unified solution.

MICROSEC.AI