Incident Response

Policy

Table of Contents

1. OVERVIEW

This Incident Response Policy aims to specify exactly how Tracer Mobile Workflow will respond in the event of suspected security incident. This policy defines security incidents, both physical (such as the loss of a laptop) and electronic (a suspected attack or malware infection). Events such as natural disasters, hardware failures, or service outages are all considered high impact issues, but only a limited number of these issues are considered to be *security incidents.* Microsoft defines a security incident in the Online Services as illegal or unauthorized access that results in the loss, disclosure or alteration of Customer Data.

2. SCOPE

This Incident Response Policy is one of the company's most important policies, as it can reduce the risk of a security incident as well as reduce data loss and speed up recovery times in the event an incident was to occur. This Incident Response Policy outlines roles, responsibilities, and actions to take in advance, so that these decisions don't need to be made during the stress of responding to a security incident.

2.1 Non-Security Incident Examples

- Routine response to security vulnerabilities that has not resulted in inappropriate disclosure of customer data
- A security issue that affects Tracer but has not resulted in inappropriate disclosure of customer data
- Investigation of internal alarms or monitoring alerts which are shown to be false positives
- Operations by Tracer's own Team activity
- Security issues within a customer deployment caused by a flaw or weakness introduced by the customer (failure to patch, brute force, configuration error)
- Denial-of-service attack (DoS)
- Compliance events that do not affect confidentiality, integrity, or availability of service or customer data

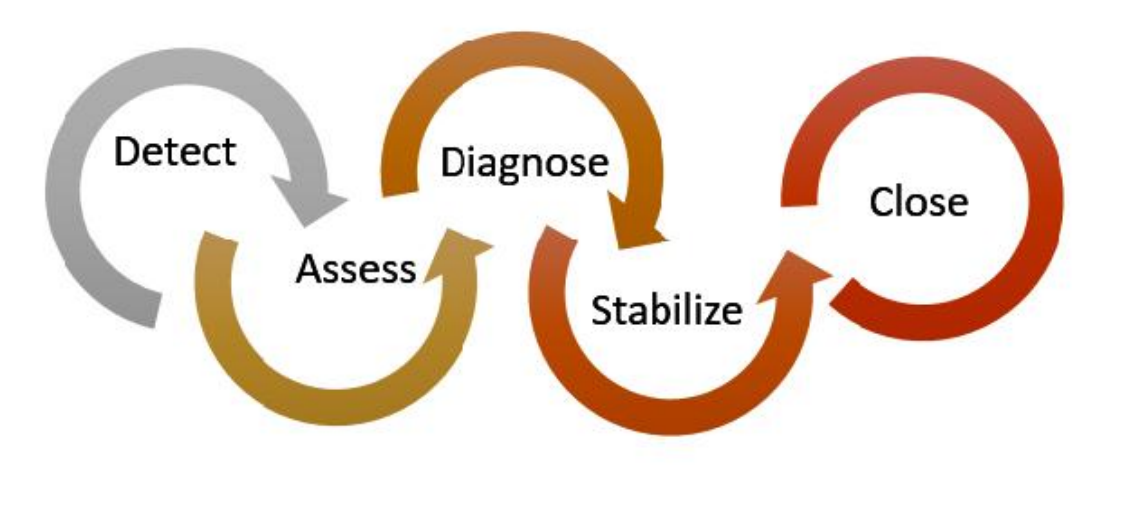
2.2 Security Incidents Examples

- Unauthorized access to Tracer infrastructure systems and exfiltration of customer data
- Unauthorized disclosure of sensitive control data, such as credentials, encryption keys, or API keys, which could be used to alter or access customer data
- Physical intrusion into a data centre hosting Tracer properties which results in theft of unencrypted customer data
- Bug in Tracer code which has resulted in malicious alteration or exposure of customer data
- Intrusion into a customer deployment caused by a flaw or weakness introduced by the Tracer Infrastructure

3. TRACER SECURITY INCIDENT RESPONSE PROCESS

3.1. Step-by-Step Response

Tracer follows a 5-step incident response process when managing both security and availability incidents for the Tracer services. The goal for both types is to restore normal service security and operations as quickly as possible after an issue is detected and an investigation is started. The response is implemented using a five-stage process illustrated in Figure 1, which shows the following activities - Detect, Assess, Diagnose, Stabilize, and Close. The Security Incident Response Team may move back and forth between diagnose to stabilize as the investigation progresses.



1. **Detect** – First indication of an event investigation
2. **Assess** – An on-call incident response team member assesses the impact and severity of the event.
3. **Diagnose** – Security Manager conduct the technical or forensic investigation, identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have become exposed to an unlawful or unauthorized individual, parallel execution of the Customer Incident Notification process begins in parallel.
4. **Stabilise, Recover** – The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned which occur after the immediate risk has passed.
5. **Close/Post mortem** - The incident response team creates a post-mortem that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence of the event.

4. NOTIFICATION

4.1 Customer Security Incident Notification

If during the investigation of a security event, Tracer becomes aware that customer data has been accessed by an unlawful or unauthorized party, the security manager will immediately begin execution of the Customer Security Incident Notification Process. This can occur at any point of the incident lifecycle, but usually begins during the Assess or Diagnose phases. The investigation and mitigation need not be completed before this process begins in parallel.

The goal of the customer security incident notification process is to provide impacted customers with accurate, actionable, and timely notice when their customer data has been breached.

4.1.1 Determine Scope of Impacted Customers

Tracer relies on heavy internal compartmentalization in the operation of our solution. Logs about whose data was where and when are also robust. Due to these factors, most incidents can be scoped to specific customers. The goal is to provide anybody who is impacted as detailed a notice as possible.

4.1.2 Notice Creation

The goal of this notice is to provide customers with detailed enough information so that they can perform an investigation on their end and meet any commitments they have made to their end users while not unduly delaying the notification process. The incident notification team must balance speed with completeness.

Generally, the process of drafting notifications occurs as the incident investigation is ongoing. The security response team will move quickly and accurately.

4.1.3 Confirmation and Incident Declaration

As the incident investigation progresses, the security response team will amass evidence showing whether or not a breach has occurred. This evidence is presented to the designated executive who reviews it with the advice and expertise of the entire team.

If the designated executive is satisfied that unauthorized access or a security incident has occurred, an incident declaration will occur. This declaration triggers the process of sending official notifications.

4.1.4 Customer Incident Notification

When a security incident is declared, Tracer supports an incident notification process that includes:

- Prompt notification to affected customers
- Notification to applicable regulatory authorities if required

Notification of security incidents will be delivered to the listed security contacts of the customer. If contact information is not provided, notification will be sent to one or more of a customer's administrators. Notification will be sent by any means Tracer selects, including via email.

4.1.5 Notification Timeline

In the event of a declared security incident, notification by Tracer will be made without unreasonable delay and in accordance with any legal or contractual commitments. Customers should recognize that an exercise balancing between accuracy/completeness and speed takes place.

5. CONCLUSION

The security incident management program is a critical responsibility for Tracer, and represents an investment that customers using Tracer MW can count on and involves a team of a dedicated team with skill and dedication to protecting Tracer customers.

6. ACKNOWLEDGEMENTS

6.1 Microsoft Cloud Services and Microsoft Authors

Ben Ridgway
Frank Simorjay

6.2 Tracer Contributors and Reviewers

Nadine Fouche
Cobus van Graan