Security Incident Timing Metrics version 1.0

Specification Document

SITM Version 1.0 Release

This document will update with each release of the SITM standard. It is currently SITM version 1.0, released on 29th May 2023.

Author: Francesco Chiarini, Chairman of the Cyber Resilience Special Interest Group at ISSA.org
Co-authors: Désirée Sacher-Boldewin, Senior Manager SOC Professional Services at NVISO
Logan Wilkins, Manager at CSIRT Engineering at Cisco
Mark Zajicek, Member of the Technical Staff at CERT Division, Software Engineering Institute, Carnegie Mellon University

---

Summary

The Security Incident Timing Metrics (SITM) is an open reference for standardizing the tracking of security incident timeline and measurement security incident timing metrics. SITM consists of eleven Timeline Records (TR) and four Key Metrics (KM). Both the Timeline Records and Key Metrics are divided into must have, recommended, and nice-to-have, based on their importance towards measuring the efficacy of an incident response team, as well as the extended technology team's performance.

The TR are collected during different lifecycle stages of the security incident and their data entry may be performed manually, automatically or semi-automatically depending on the tools available at a given organization. The KM are calculated based on TR values and aim to resolve a cross-industry issue of lack of shared incident timing definitions and calculation resulting in the inability to benchmark results across incident response organizations.

1. Introduction

Tracking and classification of security incidents is a key outcome of information security report acceptance (Section 6.1 - FIRST CSIRT Services Framework v2.1). This reference aims to provide guidance on how to properly track information security timeline components so that CSIRT teams can produce metrics and increase incident response maturity. Timeline preparation is a key component of information security incident analysis (Section 6.2 - FIRST CSIRT Services Framework v2.1), as thanks to time elements, CSIRT stakeholders will gain substantial understanding of a suspected or confirmed information security incident.
The Security Incident Timing Metrics (SITM) consists of eleven Timeline Records (TR) and four Key Metrics (KM) which will be described in the following sections of this document.

1.1. Timeline Records

SITM is composed of eleven Timeline Records (TR) which are represented in Figure 1 in simplified format with seven key datapoints as plotted on an incident timeline.

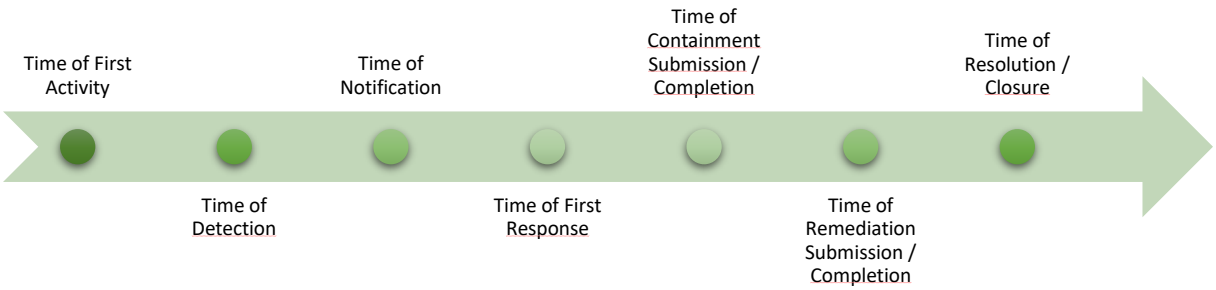

Figure 1

Each TR is described in the table below with the following additional details:

- Timeline Record - title of the given entry
- Tracking Importance - describes the relevance of the TR for each CSIRT entity
- Data Entry - describes the method of data collection and point of time of when the data is collected
- Description - outlines the rationale of each timeline record

Timeline Record	Tracking Importance	Data Entry	Description
Time of First Activity	High - Must-Have	Automated with manual re-validation by the analyst at the beginning of the incident and prior incident closure.	Time of First Activity is the earliest event in a confirmed or potential chain of events, that caused the incident. This may be the time at which a system's telemetry picks up a given event, but often forensic or investigative actions need to be undertaken to determine the start time. Data collection of this TR is recommended for all incidents.
Time of Detection	High - Must-Have	Automated	Time of Detection is the point in time at which a control (e.g., telemetry, technology) or another detection mechanism (e.g., a human) recognizes that something has occurred. Data collection of this TR is recommended for all incidents.
Time of Containment	High - Must-Have	Automated or manually, depending on CSIRT capabilities.	Time of Containment is the point in time at which the incident can no longer spread nor do damage, i.e., when full containment is achieved and validated. This may be referred to as a set of mitigation activities. This is a critical milestone from an incident timeline perspective. Data collection of this TR is recommended for all incidents.
Time of Remediation	High - Must-Have	Automated or manually, depending on CSIRT capabilities.	Time of Remediation is the point in time at which an affected target asset is returned to its pre-incident state or removed from the environment permanently. Full remediation is achieved and validated. This may indicate a

			measure of an organization's ability to timely respond to the incident. Data collection of this TR is recommended for all incidents.
Time of Closure	High - Must-Have	Closure done manually by analyst; date/time filled in automatically by ticketing tool.	Time of Closure is the point in time at which the required follow up, analysis, reporting, post-mortem etc. has been completed and there is no longer any work being done on the incident. The incident cannot be re-opened at this stage. Data collection of this TR is recommended for all incidents.
Time of First Response	Medium - Recommended	Automated	Time of First Response is the point in time at which someone takes action upon a received notification, likely initiating an investigation. Otherwise called "pick-up time" or "time of assignment". If automated, data collection of this TR is recommended for all incidents; otherwise, just for significant incidents.
Time of Containment Submission	Medium - Recommended	Automated or manually, depending on CSIRT capabilities.	Time of Containment Submission is the point in time at which an asset is given to a process the end goal of which is containment. This may indicate a measure of an analyst's or team's timely response to the incident. Data collection of this TR is recommended for all incidents that require containment.
Time of Remediation Submission	Medium - Recommended	Automated or manually, depending on CSIRT capabilities.	Time of Remediation Submission is the point in time at which an asset is given to a process the end goal of which is remediation. This may indicate a measure of an analyst's or

			team's timely remediation to the incident. Data collection of this TR is recommended for all incidents that require remediation.
Time of Resolution	Medium - Recommended	Closure done manually by analyst; date/time filled in automatically by ticketing tool.	Time of Resolution occurs when the incident has been remediated and business processes return to normal post-incident activities. Auto-closure may happen if no changes within fixed time limit. The incident can still be re-opened at this stage. Data collection of this TR is recommended for all incidents.
Time of Notification	Low - Nice to have	Automated or manually, depending on CSIRT capabilities.	Time of Notification is the point when the party responsible for investigating an event is made aware of a detection. In case of automated alerts, time of detection and time of notification is the same. Data collection of this TR is recommended for significant incidents, given the time/efforts it may take to determine for human detected incidents or alerting tool delays.
Time of External or Legal Notification	Low - Nice to have	Automated or manually, depending on CSIRT capabilities.	Time of External or Legal Notification is not to be used as a timeline item. It is included here with the suggestion that it be used as a tick-box for the analysts to mark when appropriate. There is no associated metric being recommended at this time Data collection of this TR is recommended for incidents involving legal or law-enforcement based scenarios.

Table 1

1.2. Key Metrics

SITM is composed of four Key Metrics (KM) which rely on the availability of seven Timeline Records (TR), as described in section 1.1.

The set of four KM is represented graphically below:

<table>
<tr><td>Time of First Activity</td><td>Time of Detection</td><td>Time of First Response</td><td>Time of Containment</td><td>Time of Remediation</td></tr>
<tr><td colspan="2">Time to Detect</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Time to Respond</td><td></td><td></td></tr>
<tr><td colspan="4">Time to Contain</td><td></td></tr>
<tr><td colspan="5">Time to Remediate</td></tr>
</table>

Figure 2

Each KM is described in the table below with the following additional details:

- Key Metric - title of the given entry
- Metric Importance - describes the relevance of the KM for each CSIRT entity
- Metric Goal - describes the goal for the given metric
- Metric Formula - describes the proposed way to calculate the given KM

Key Metric	**Metric Importance**	**Metric Goal**	**Metric Formula**
Time to Detect	High - Must-Have	Understand the time taken by your security team to detect a threat.	Time of Detection - Time of First Activity (minutes / hours)
Time to Respond	Medium - Recommended	Understand the time taken by your security team to respond to a threat.	Time of First Response - Time of First Activity (minutes / hours)
Time to Contain	High - Must-Have	Understand the time taken by your security team to contain a threat.	Time of Containment - Time of First Activity (minutes / hours)
Time to Remediate	Medium - Recommended	Understand the time taken by your security team to remediate a threat.	Time of Remediation - Time of First Activity (minutes / hours)

2. Timeline Records

2.1. Time of First Activity

Time of first activity refers to the earliest event in a confirmed or potential chain of events that led to the incident. It signifies the initial occurrence that triggered the incident. Determining the time of first activity is crucial for understanding the timeline and progression of the incident.

While the system's telemetry may capture a specific event, it often requires forensic or investigative actions to accurately determine the start time of the incident. These actions may involve analyzing logs, conducting digital forensics, or reviewing security alerts to identify the initial indicators or actions of the attacker.

The "time of first activity" is an essential piece of information in incident response and investigation. It helps cybersecurity professionals trace the origin of an incident, identify the affected systems or networks, and assess the extent of the compromise. This information plays a vital role in understanding the incident's impact and formulating an effective response plan.

It is recommended to collect and document the time of first activity for all cybersecurity incidents.

2.2. Time of Detection

Time of detection refers to the specific point in time when a control, detection mechanism, or a human observer recognizes that an incident or suspicious activity has occurred. It represents the moment when the incident or its indicators are identified or brought to the attention of the security team.

The time of detection can vary depending on the nature of the incident and the effectiveness of the detection mechanisms in place. It could be triggered by various factors, such as an alert from an intrusion detection system, a security analyst noticing unusual behavior, or an automated monitoring tool raising an alarm.

Capturing the time of detection is crucial as it allows organizations to understand how quickly they were able to identify the incident, which can have a significant impact on the containment and mitigation efforts. A shorter time of detection is desirable as it enables a faster response, minimizing the potential damage and reducing the time an attacker has to operate undetected.

It is recommended to collect and document the time of detection for all cybersecurity incidents. This information helps organizations assess the effectiveness of their detection controls and mechanisms, identify any delays or gaps in their incident response processes, and make necessary improvements to strengthen their overall security posture. Additionally, documenting the time of detection is valuable for compliance purposes and aids in post-incident analysis and reporting.

2.3. Time of Containment

Time of containment refers to the specific point in time when the incident is effectively controlled and prevented from further spreading or causing damage. It represents the milestone when the necessary containment activities have been executed, and the right measures have been implemented and validated.

Achieving containment involves taking various actions to isolate and neutralize the malicious activity from further spreading. This may include actions such as disabling compromised accounts, quarantining infected systems, or blocking malicious network traffic. The specific measures will depend on the nature of the incident and the guidance provided by incident response protocols.

The time of containment is a critical milestone in the incident timeline as it signifies that the organization has regained control -partially or completely- over the situation and minimized the impact of the incident. It allows the focus to shift towards recovery and restoration efforts, ensuring that normal operations can be resumed as quickly as possible.

Capturing and documenting the time of containment is recommended for all cybersecurity incidents. This information helps organizations evaluate the efficiency of their containment strategies and determine the overall duration of the incident as well as the organization’s agility when engaging multiple groups for containment related work.

2.4. Time of Remediation

Time of remediation refers to the specific point in time when an affected target asset, such as a compromised system or network, is successfully restored to its pre-incident state or permanently removed from the environment. Remediation involves the complete resolution of any vulnerabilities, removal of malicious presence, and restoration of normal functionality.

Achieving remediation requires undertaking a series of actions to address the root causes of the incident and ensure that the affected asset is secure and operational again. This may involve activities such as patching vulnerable software, removing malware or unauthorized access, restoring data from backups, or rebuilding systems from scratch if necessary.

The time of remediation reflects the speed and efficiency with which the organization can restore the impacted systems or remove compromised assets, minimizing the potential for recurring incidents and reducing the overall impact on operations.

Capturing and documenting the time of remediation is recommended for all cybersecurity incidents. This information helps organizations measure their ability to quickly recover from incidents and assess the impact on business continuity.

2.5. Time of Closure

Time of closure refers to the specific point in time when all necessary follow-up activities, analysis, reporting, and post-mortem processes related to the incident have been completed. It signifies that no further work is being done on the incident, and it is considered officially closed. Once the time of closure has been reached, the incident cannot be re-opened.

Closure activities may include conducting a thorough investigation to understand the root causes and impact of the incident, documenting lessons learned, implementing remediation measures to prevent similar incidents in the future, and finalizing any required incident reports or documentation.

The time of closure is a significant milestone in the incident response process as it indicates the conclusion of the incident and the transition to normal operations. It demonstrates that all necessary steps have been taken to address the incident, learn from it, and implement any required changes or improvements.

Capturing and documenting the time of closure is recommended for all cybersecurity incidents. This information helps organizations assess the time and resources required to fully address and close incidents. It also supports post-incident analysis, regulatory compliance, and reporting requirements.

Documenting the time of closure provides a clear indication of when incident response activities can be officially concluded, and resources can be reallocated to other security priorities.

2.6. Time of First Response

Time of first response refers to the specific point in time when someone acts upon receiving a notification or alert related to the incident. It represents the moment when an individual or a designated team acknowledges the notification and initiates the investigation or incident response process.

The time of first response can also be referred to as "pick-up time" or "time of assignment." It signifies the start of active engagement with the incident, where appropriate personnel begin to assess the situation, gather necessary information, and determine the appropriate course of action.

If certain incident response capabilities are partially automated, it is recommended to collect and document the time of first response for all incidents. This allows organizations to track the efficiency of their automated systems, measure the speed at which notifications are received and acted upon, and evaluate the effectiveness of their incident response automation.

For incidents that require manual intervention or human involvement, data collection of the time of first response is particularly recommended for significant incidents. These are incidents that have a high potential impact, involve critical assets or sensitive data, or pose a significant risk to the organization's operations or reputation.

Capturing the time of first response is essential for measuring the timeliness of incident response efforts, identifying any delays or bottlenecks in the process, and ensuring a swift and effective

response to mitigate the incident's impact. It provides valuable data for analysis, performance evaluation, and improvement of incident response procedures and practices.

2.7. Time of Containment Submission

Time of containment submission refers to the specific point in time when an asset, such as a compromised system or network, is handed over to a process or procedure with the ultimate objective of containing the incident. It represents the moment when the responsible analyst or team takes action to isolate or mitigate the impact of the incident.

Containment submission typically involves following established incident response protocols and procedures to implement measures that restrict the incident's spread and minimize its damage. These measures can include isolating affected systems from the network, blocking malicious traffic, disabling compromised accounts, or implementing temporary security controls to prevent further harm.

The time of containment submission serves as a metric to measure the timeliness of an analyst's response to the incident or -depending on organizational context- to measure the timeliness of the receiving team that needs to address the containment actions. It indicates how quickly the responsible party initiated the containment efforts once they assumed control or responsibility for the affected asset.

Data collection of the time of containment submission is recommended for all incidents that require containment measures. This information helps organizations evaluate the effectiveness and efficiency of their incident response processes end-to-end, measure the timeliness of their containment efforts, and identify opportunities for improving response times especially in regard to supporting teams (beyond the incident response organization).

By capturing the time of containment submission, organizations can track and analyze response metrics, identify trends, and refine incident response procedures.

2.8. Time of Remediation Submission

Time of remediation submission refers to the specific point in time when an asset affected by the incident is handed over to a process or procedure with the goal of achieving full remediation. It represents the moment when the responsible analyst or team initiates the necessary actions to address the underlying vulnerabilities or issues that led to the incident.

Remediation submission involves following established incident response protocols and procedures to implement measures aimed at resolving the root causes of the incident and preventing similar incidents from occurring in the future. This can include activities such as patching software

vulnerabilities, removing malware manually from a host or reimaging an asset or implementing additional security controls.

The time of remediation submission is a metric used to measure the timeliness of an analyst or team's response to the incident and their efforts to remediate the affected systems. It indicates how quickly the responsible party began the remediation process once they assumed control or responsibility for the affected asset.

Data collection of the time of remediation submission is recommended for all incidents that require remediation efforts. This information helps organizations evaluate the timeliness of their remediation activities and identify areas for improvement in their response capabilities.

With this information, organizations can also track and analyze bottlenecks or delays in the remediation process.

2.9. Time of Resolution

Time of resolution refers to the specific point in time when the incident has been fully remediated, and business processes have returned to their normal state. It represents the milestone when all necessary actions have been taken to resolve the incident and restore the affected systems or networks to their pre-incident condition.

Resolution involves completing the remediation efforts, verifying the effectiveness of the implemented measures, and ensuring that the organization's operations can resume without any disruption or compromise. It may also include transitioning to post-incident activities, such as conducting a post-incident review, documenting lessons learned, and updating incident response plans.

In some cases, incidents may be automatically resolved if no changes or new indicators of compromise are observed within a specified number of days. However, it is important to note that even after resolution, incidents can still be re-opened if new information or evidence emerges that requires further investigation or action. This is different than time of closure, whereas a closed incident cannot be re-opened anymore.

Data collection for time of resolution is recommended for all incidents. This information helps organizations track the overall duration of incidents including post-mortem work, including root-cause analysis. As incident re-opening rate is an important incident response metric, time of resolution can equally help to have an informed view of the time required to realize an incident requires further actions and hence needs to be re-opened.

By documenting the time of resolution, organizations can have a clear record of when the incident was officially considered resolved, ensuring accountability and providing valuable data in regard to resolved incident trending and volumes.

2.10. Time of Notification

Time of notification refers to the specific point in time when the individuals responsible for investigating an event or incident are made aware of its detection. It represents the moment when the relevant personnel receive information or an alert indicating the presence of a potential security issue.
If automated detection systems or alerts are in place, the time of detection and the time of notification are usually the same. In such cases, the automated system detects the incident and immediately notifies the appropriate individuals or teams for further investigation.
However, for incidents that are manually detected by human analysts or when there are delays in alerting tools, the time of notification may be different from the time of detection. It is the moment when the responsible individuals become aware of the incident, either through manual monitoring, analysis of logs, or receiving reports from other sources.
Data collection of the time of notification is recommended for significant incidents, particularly those that require human involvement or where alerting tool delays are possible. This information helps organizations track the response time from the initial detection to the point when the incident is formally acknowledged by the incident response team.
Capturing the time of notification is essential for measuring the timeliness of incident response efforts, identifying any delays or gaps in the notification process, and ensuring that incidents are addressed promptly.

2.11. Time of External or Legal Notification

Time of external or legal notification refers to the point in time when relevant external parties or legal authorities are formally notified about the incident. This notification typically occurs when there is a need to involve external entities, such as law enforcement agencies, regulatory bodies, or legal representatives, due to the nature or severity of the incident.
The time of external or legal notification is not intended to be used as a timeline item or a metric for measuring incident response performance. Instead, it serves as a record or documentation of when the formal notification to external or legal entities took place.
Data collection of the time of external or legal notification is recommended for incidents that involve legal or law enforcement-based scenarios. These scenarios can include incidents that potentially violate privacy regulations, involve sensitive data, or have other criminal implications such as financial fraud or insider threat.
By capturing the time of external or legal notification, organizations can demonstrate their adherence to legal and regulatory obligations, maintain a record of compliance, and facilitate effective collaboration with external parties involved in the incident response process.

3. Key Metrics

3.1. Time to Detect

Metric Description

"Time to detect" is a cybersecurity incident response metric that measures the duration it takes for an organization's security team to identify and detect a potential threat or security incident. It quantifies the time elapsed from the occurrence of the initial activity related to the incident to the moment the security team becomes aware of the threat.

Metric Goal and Actions

The goal of tracking the time to detect metric is to minimize the time it takes to identify and recognize potential security threats or incidents. By monitoring this metric, organizations aim to enhance their threat detection systems, and reduce the dwell time of malicious activities within their environment.

Data Processing and Formula

To calculate the time to detect metric, the formula is as follows:

```
Time to Detect = Time of Detection - Time of First Activity
```

The metric can be measured in minutes or hours, depending on the organization's preference and the incident's urgency. By subtracting the time of the first activity from the time of detection, organizations can determine the elapsed time and assess the effectiveness of their detection processes.
Analyzing the data collected from this metric over time allows organizations to identify trends, measure improvements in their incident response capabilities, and take proactive measures to reduce the time to detect future incidents.

3.2. Time to Respond

Metric Description

"Time to respond" is a cybersecurity incident response metric that measures the duration it takes for an organization's security team to initiate a response once a threat or security incident has been detected. It quantifies the time elapsed from the moment the security team becomes aware of the incident to the start of the incident response activities.

Metric Goal and Actions

The goal of tracking the time to respond metric is to minimize the time it takes for an organization to mobilize its incident response efforts and begin taking proactive steps to mitigate the impact of the

incident. By monitoring this metric, organizations aim to enhance their incident response efficiency, reduce the potential damage caused by the incident, and minimize the overall risk exposure. Regular drills, tabletop exercises, and simulations can also help improve response readiness.

Data Processing and Formula

To calculate the time to detect metric, the formula is as follows:

```
Time to Respond = Time of First Response - Time of First Activity
```

It is typically measured in minutes or hours, depending on the urgency and severity of the incident. Data for this metric can be collected by timestamping the moment the incident is officially acknowledged by the security team or the incident response coordinator. This timestamp can be obtained from incident tracking systems, incident management tools, or manual documentation.

3.3. Time to Contain

Metric Description

"Time to contain" is a cybersecurity incident response metric that measures the duration it takes for an organization's security team to effectively contain a detected threat or security incident. It quantifies the time elapsed from the initiation of incident response activities to the point at which the incident is deemed contained, meaning it can no longer spread or cause further damage.

Metric Goal and Actions

The goal of tracking the time to contain metric is to minimize the time it takes for an organization to halt the progression and impact of a security incident. By monitoring this metric, organizations aim to limit the potential damage caused by the incident, prevent further compromise of systems or data, and minimize the disruption to normal business operations.
To achieve this goal, organizations can take several actions. These include promptly isolating affected systems or network segments, implementing security controls or countermeasures to prevent the incident's spread, removing or neutralizing malicious components, and implementing temporary or permanent remediation measures to address vulnerabilities or weaknesses exploited by the threat.

Data Processing and Formula

To calculate the time to detect metric, the formula is as follows:

```
Time to Contain = Time of Containment - Time of First Activity
```

It is typically measured in minutes, hours, or days, depending on the complexity and severity of the incident. Data for this metric can be collected by timestamping the moment when containment measures are effectively implemented and verified. This timestamp can be obtained from incident tracking systems, security logs, or documented evidence of containment activities.
This metric enables organizations to assess the speed and efficiency of their containment measures, optimize incident response workflows, and minimize the time it takes to contain future incidents.

3.4. Time to Remediate

Metric Description

"Time to remediate" is a cybersecurity incident response metric that measures the duration it takes for an organization's security team to fully remediate a detected threat or security incident. It quantifies the time elapsed from the initiation of incident response activities to the point at which the affected systems or assets are returned to their pre-incident state or permanently removed from the environment.

Metric Goal and Actions

The goal of tracking the time to remediate metric is to minimize the time it takes for an organization to restore normalcy and eliminate the root cause of a security incident. By monitoring this metric, organizations aim to reduce the overall impact of the incident, minimize the potential for recurrence or reinfection, and restore the affected systems or assets to their desired security posture.
Organizations willing to improve their remediation time metrics may need to implement long-term measures such as strengthening security controls, improving security awareness and training programs, and conducting vulnerability assessments and penetration testing to address any underlying weaknesses in the infrastructure.

Data Processing and Formula

To calculate the time to detect metric, the formula is as follows:

$$\textit{Time to Remediate} = \textit{Time of Remediation} - \textit{Time of First Activity}$$

It is typically measured in hours, days, or weeks, depending on the complexity and scope of the incident. Data for this metric can be collected by timestamping the moment when all remediation actions are completed and validated. As with other metrics, this timestamp can be obtained from incident tracking systems, change management logs, or documented evidence of remediation activities.

Security Incident Timing Metrics version 1.0

Specification Document

SITM Version 1.0 Release

Contact for queries and suggestions:

francesco.chiarini@issa.org.pl

Francesco Chiarini

Chairman of the Cyber Resilience Special Interest Group ISSA.org

SITM is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world.