FIRST Metrics SIG Update

July 1, 2022

Metrics SIG Overview

- The Metrics SIG looks to bring together interested members of the FIRST community to discuss and identify approaches for internally evaluating and tracking CSIRT and incident management practices and activities within an organization.
- The Metrics SIG is a place for discussion but also focuses on some specific projects to provide guidance to CSIRTs in the development of measurements, metrics, and evaluation mechanisms.
- Co-chairs:
  - Mike Murray, SecureWorks, Director, Incident Response Consulting
  - Robin Ruefle, CERT/CC, SEI, CMU, Team Lead CSIRT Development and Training

Metrics SIG Projects

- Security Incident Timing Metrics
  - This project has developed a set of Timing Metrics to be potentially collected by CSIRTs.
  - A guidance document is currently being developed.
- CSIRT Services and Activity Metrics Develop
  - This project seeks to use the CSIRT Services Framework as a foundation for CSIRT activities and identify methods for measuring the success or effectiveness of the services, functions, and tasks in the Framework
  - The project team is working on the development of this guidance.
- CSIRT Metrics-related Webinars
  - Over the years the SIG has held various webinars to provide SIG and other FIRST members with information on various type of metrics and measurement methodologies.

More Detail – CSIRT Timing Metrics Project

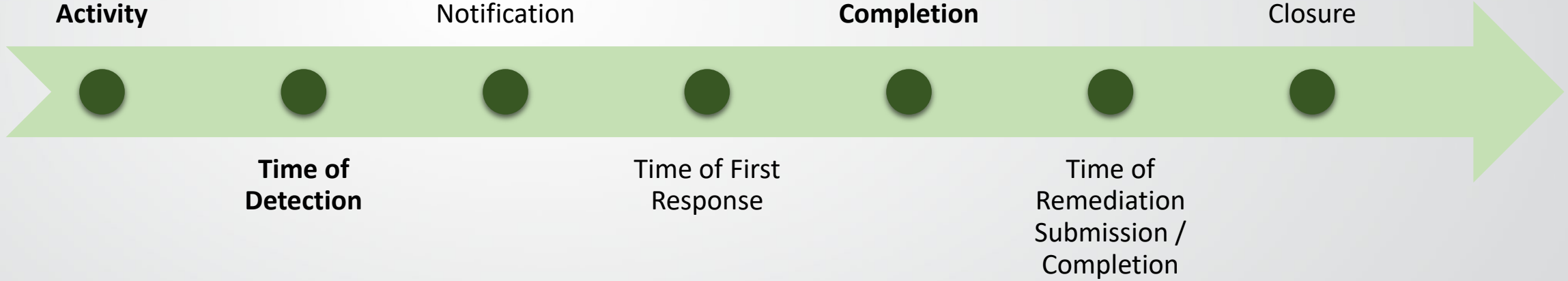
- Co-chairs and project team members:
  - Logan Wilkins – Cisco, CSIRT Engineering, Manager
  - Francesco Chiarini – Standard Chartered Bank, SVP Cyber Resilience
  - Désirée Sacher-Boldewin - Finanz Informatik, SOC Architect
  - Mark Zajicek, CERT/CC, Carnegie Mellon University

- The project team is looking for additional FIRST members to help develop the guidance document.

Security Incident Timing Standard

Recon, Weaponize, Deliver

Exploit, Control, Execute, Maintain



Definitions

Scenarios

- Phishing - Credentials Harvesting
- Ransomware - Payload
- Email Account Compromise

Metrics

- Time of Detection
- Time of First Response
- Time of Containment
- Time of Remediation

Documentation Being Developed

Security Incident Timing Metrics version 1.0: Specification Document

SITM Version 1.0 Release

This page updates with each release of the SITM standard. It is currently SITM version 1.0, released in XXX 2020

Chiarini, Francesco (PI)
Add release date

Security Incident Timing Metrics v1.0: Specification Document

Also available in PDF format.

Chiarini, Francesco (PI)
Add link

The Security Incident Timing Metrics (SITM) is an open standard 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, depending on their importance towards measuring the efficacy of an incident response team, as well as the extended IT team's performance.

The TR are collected during different lifecycle stages of the security incident and their data entry may be performed manually, automated or semi-automated depending on the tools available at the target organization.

The KM are calculated based on TR values and aim to resolve a cross-industry problem of lack of shared incident timing definitions and calculation.

Chiarini, Francesco (PI)
Add link

The most current SITM resources can be found at www.first.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. FIRST reserves the right to update SITM and this document periodically at its sole discretion. While FIRST owns all right and interest in SITM, it licenses it to the public freely for use, subject to the conditions below. Membership in FIRST is not required to use or implement SITM. FIRST does, however, require that any individual or entity using SITM give proper attribution, where applicable, that SITM is owned by FIRST and used by permission. Further, FIRST requires as a condition of use that any individual or entity which publishes security metrics conforms to the guidelines described in this document and provides both the TR and KM scoring methodology so others can understand how the metric was derived.

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 standard 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	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

2. Timeline Records

2.1. Time of First Activity

2.1.1. Record Description

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 in order to determine the start time.

2.1.2. Tracking and Applicability

Data collection of this TR is recommended for all incidents as far as the data is collected by automated tools. Validation of the field should be performed manually by an analyst at incident creation as well as prior to incident closure.

The Time of First Activity entry is highly recommended for all confirmed incidents of priority equal to medium or above, as this TR is fundamental in order to calculate other must-have "Time to" metrics included in this document.

2.2. Time of Detection

2.2.1. Record Description

2.2.2. Tracking and Applicability

...

3. Key Metrics

3.1. Time to Detect

3.1.1. Metric Description

3.1.2. Metric Goal and Actions

3.1.3. Data Processing and Formula

3.2. Time to Respond

3.2.1. Metric Description

3.2.2. Metric Goal and Actions

3.2.3. Data Processing and Formula

...

Appendix A - References

Appendix B - Acknowledgments

Appendix C - On-Line Resources

CSIRT Services and Activity Metrics Development Project Team Members

- Chair and project team members:
  - Logan Wilkins – Cisco, CSIRT Engineering, Manager – chair
  - Désirée Sacher-Boldewin - Finanz Informatik, SOC Architect
  - Mark Zajicek, CERT/CC, SEI, Carnegie Mellon University
  - Robin Ruefle, CERT/CC, SEI, Carnegie Mellon University
- The project team is looking for additional FIRST members to help develop the guidance document.

CSIRT Services and Activity Metrics Development Project Overview

- **Goals:**
  - Define a categorization framework and catalogue for metrics related to incident management and security operations
  - Make the FIRST CSIRT Services Framework as actionable as possible so more people work with it

- Process:
  - Work through CSIRT Services Framework
  - For each section, identify data points needed to:
    - Accomplish goal (what objectives are we trying to meet in that section)
    - Evaluate success (how could the success of meeting that objective be measured

Future Work

1. Define what values need to be measured for each metric
2. Complete descriptions to make the objectives, the metrics as well as the required fields more understandable
3. Create checklists by implementation categories/types, so it can be more easily turned into instructions for technical implementations
4. create mappings/references to other frameworks and specific use cases to highlight the supplementation of the FIRST CSIRT Framework

Webinar Series

- Facilitator: Robin Ruefle, CERT/CC, SEI, Carnegie Mellon University
- A new set of webinars will be set up for the 2022-2023 timeframe.

Questions