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

Definitions

- Time of First Activity
- Time of Detection
- Time of First Response
- Time of Containment Submission / Completion
- Time of Remediation Submission / Completion
- Time of Resolution / Closure

Scenarios

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

Metrics

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

TLP: Amber

Recon, Weaponize, Deliver
Exploit, Control, Execute, Maintain

• Recon, Weaponize, Deliver
• Exploit, Control, Execute, Maintain
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 security log entry records a new event, or the time a security investigation team begins to analyze the incident. This time is determined at 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 and available. The TR should be performed manually by an analyst at incident creation as well as prior to incident closure.

This TR 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 inci-end "Time of Activity" 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