New Guide by ENISA: Actionable Information for Security Incident Response

ENISA publishes a good practice guide on Actionable Information for Security Incident Response, aiming to provide a picture of the challenges national CERTs and other security organizations encounter as they try to generate actionable output from large amounts of data.

The study gives a broad overview of the current information-sharing landscape in the context of generating actionable information, identifies existing tools and standards, reports best practices and gaps, and provides recommendations for improvement.

The main part of the report, describes how actionable information is obtained, utilized, and shared in a systematic manner. The conceptual model proposed which forms the structure for the study, introduces a generalized information processing pipeline with five steps: collection, preparation, storage, analysis and distribution. The purpose of the model is to facilitate the way CERTs deal with information, with the goal of streamlining the incident handling process.

ENISA's Executive Director Udo Helmbrecht commented: *"CERTs are the first line of our cyber-defence.*
As their daily work relies on processing increasing amounts of data, the challenge is to make sense out of it and generate actionable output. Actionable Information is identified as a fundamental building block for incident response. *This study is the first attempt to provide a reference guide on the topic for CERTs. ENISA welcomes the opportunity to support further work in the field, with reporting, research and further development of tools".*

The gaps commonly found in CERT processes for handling actionable information are explored, and a set of general recommendations is provided for organizations with information-dissemination responsibilities. Overall conclusion is that information exchanges have not yet reached maturity and the sharing environment will need to develop further before the benefits of these exchanges is fully realised.

The work includes three case studies covering various aspects of actionable information handling by CERTs. These scenarios capture the operational processes of real CERT teams and the actual features of the tools used, indicating how they can be applied to improve CERT team's ability to produce, share and use actionable information.

Inventory for information sharing

The study is complemented by an inventory entitled Standards and tools for exchange and processing of actionable information that can be applied to information-sharing activities. It explores the relationships among the different standards by providing a better understanding of the underlying protocols.

In the first part, the inventory covers a total of fifty-three different information sharing standards, a mix of formats, protocols, technical approaches and frameworks in common use. These are broken down into seven main categories based on the scope of the standard.

In the second part, the inventory consists of sixteen information sharing tools and platforms relevant to the exchange and processing of actionable information. These are primarily open source solutions that are available to CERTs.

A Hands-on exercise: Using indicators to enhance defence capabilities-Actionable information

As part of the project a new hands-on exercise scenario was created as training for Incident Response Team members and other IT security professionals responsible for security incident response.

The goal of this exercise is to teach how to create and deploy indicators of compromise using Collaborative Research into Threats (CRITs) platform. Additionally, it demonstrates how to leverage CRITs to visualize relationships among different elements of a campaign, how to extract indicators from incident data, develop mitigation actions, and track those actions. The exercise was created for a more structured approach to indicator management, ultimately resulting to be better equipped to secure networks.

For full reports:

- Actionable Information for Security Incident Response
- Standards and tools for exchange and processing of actionable information
- Using indicators to enhance defence capabilities-Actionable information

Notes to Editors:

https://www.enisa.europa.eu/activities/cert/support/awa

https://www.enisa.europa.eu/activities/cert/support/proactive-detection

For interviews: Cosmin Ciobanu, NIS Expert, **Email:** Cosmin.Ciobanu@enisa.europa.eu, **Phone:** (+30) 2814 409663