Cyber Capacity Building Program

Evaluating Product Security for enhancing the Cyber-Resilience of the ICT Ecosystem

Proven.
Transparent.
Independent.

Contributing to greater security of the ICT ecosystem

___

The dedicated training program to provide security evaluation knowledge to businesses, government organizations and academic institutions for assessing supply chain cyber-resilience.

The fast-growing digitalization of both economies and society requires the integration of a multitude of software and hardware components into smoothly running systems. It is usually required to use different solutions to build effectively working infrastructure. However, the content of such solutions could raise the question of how secure and, therefore, trustworthy, such products in use are. If they are not trustworthy, this puts the larger ICT ecosystem and its cyber-resilience at risk since many components, solutions, companies and organizations, as a part of global supply chains and/or critical infrastructure networks could easily be compromised and, thus, cause harm to public security and economic and social wellbeing. It's in the interest of each organization to be able to evaluate and ensure the security and integrity of these components.

To ensure the security and integrity of these components and applications deeply integrated into organizations' networks, which are part of the global ICT ecosystem, those organizations should be able to identify cybersecurity risks related to these applications and mitigate them.

Kaspersky is launching its Cyber Capacity Building Program with dedicated training on evaluating product security to help companies, government organizations and academia develop mechanisms to secure their ICT infrastructure through "testing and understanding what goes on in products and services"[1]. With this program, organizations would know how to identify cybersecurity risks, as well as to manage and mitigate them.

The training aims to assist in:

- **Building capacity** in companies, government organizations and academia to identify, evaluate and estimate risks related to external applications in their ICT infrastructure;
- **Managing identified risks** and conducting an assessment of external applications for their integrity and security;
- **Forming a list of requirements** for external applications to minimize cybersecurity risks related to them;
- **Developing an understanding** of industry best practices for building a secure ICT ecosystem with regard to external applications.

The training is for:

Prerequisites for trainees are:
- Basic understanding of information security and secure software development lifecycle;
- Basic knowledge of C/C++, JS, PHP, Python;
- Minor programming experience; and
- Experience in threat modelling will be an advantage.

Those who want to understand how to adapt security practices in order to identify, evaluate and estimate risks related to external applications in their ICT infrastructure.

The training requires a basic knowledge of the software development lifecycle, programming, and information security and information security management topics. Experience in threat modeling is an advantage.

This training will be given in English.

___

1 Arne Schönbohm, president of the German Federal Office for Information Security (BSI), at the Munich Cyber Security Conference in 2020 with regard to digital sovereignty
www.politico.eu/pro/german-cyber-chief-well-never-have-digital-sovereignty

The training plan

1. Evaluating product security

Duration:
1 hour

Introduction to applications and system security; building reliable and resilient ICT infrastructure:

- Approaches for evaluating product security;
- Assessment techniques of a vendor's software development process;
- Analyzing a vendor's data processing practices; and
- Static and dynamic examination techniques of a software product for its security.

2. Threat modelling

Duration:
1.5 hours

Introduction to the process of identifying and mitigating potential threats, such as structural vulnerabilities or the absence of appropriate safeguards. The purpose of threat modelling is to provide a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.

The sections includes:
- Approaches for threat modeling;
- Actor identification; and
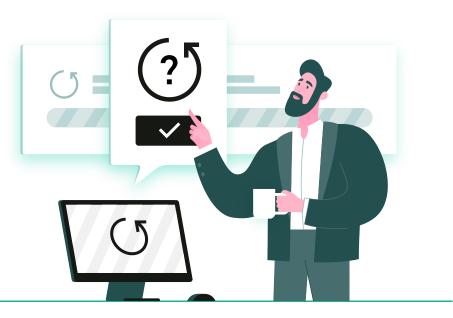- Risk identification and prioritization.

3. Secure code review

Duration:
2.5 hours

Introduction to basic techniques of identifying vulnerabilities in software code. The purpose of the code review is to ensure that a product has no potential vulnerabilities or backdoors. We will also share best practices of Kaspersky's Transparency Centers and how processes are organized for external reviews of our source code and software development.

This section includes:
· Approaches for automated source code analysis;
· Static analysis of source code;
· Dynamic analysis of source code; and
· Approaches for manual analysis of source code.

4. Code fuzzing

Duration:
2.5 hours

Code Fuzzing gives an introduction to the process of defining, developing and testing Windows-based applications through fuzzing to identify bugs and vulnerabilities. Though the training focuses on native Windows-based applications, most of the concepts – as well as the methodology and tools – can be applied to other platforms.

After completing this course, trainees will be able to:
· Understand the different fuzzing techniques and when to apply them;
· Choose the appropriate tools and prepare a target for fuzzing; and
· Generate interesting fuzzing input depending on the target.

5. Vulnerability management and disclosure

Duration:
1 hour

Introduction to and definition of approaches for the building process of managing vulnerabilities within an organization's ICT infrastructure.

This section includes:
· Sharing best practices for vulnerability management and disclosure;
· Sharing best practices for coordinated vulnerability disclosure;
· Sharing Kaspersky's experience in handling vulnerability reports from the research community; and
· Revealing nuances of bug bounty programs.

What our partners say

Dr. Sanjay Bahl,
Director General, CERT-In, Ministry of Electronics and Information Technology, Government of India:

"The topics covered in the program were very relevant to the participants and also provided them with valuable information and insights. I would like to appreciate the entire Kaspersky team who were behind this meticulously planned and well organized program packed with quality content. The interactive sessions and the problems given to the participants clearly showed the dedication and the level of efforts taken by your team to organize this program".

Mr. Tran Quang Hung,
NCSC Vietnam, Authority of Information Security, Ministry of Information and Communications, Government of Vietnam:

"The Kaspersky Cyber Capacity Building Program is wholly comprehensive and practical for government agencies and all organizations. We are living in the era of digitalization and disruptive technologies; hence, the call to enhance cybersecurity skills and mechanisms is crucial.

The National Cyber Security Center of Vietnam (NCSC Vietnam, a unit of the Authority of Information Security, part of the Ministry of Information and Communications) is always ready and willing to support Kaspersky on this program and other cybersecurity practices".

Mr. Hinsa Siburian,
Head of National Cyber and Crypto Agency (BSSN) of Indonesia:

"BSSN always strives to foster and develop the human resources competencies in cybersecurity and cryptography, including through this cooperation with Kaspersky. The Cyber Capacity Building Program established a structured Cybersecurity Human Resources posture that will produce professional human resources who can adapt to technological development and have technical competencies in cybersecurity".

kaspersky

More informatin: https://www.kaspersky.com/capacity-building.