Cyber Capacity Building Program

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

Proven.
Transparent.
Independent.

kaspersky BRING ON THE FUTURE

Learn more on
www.kaspersky.com

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:

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:

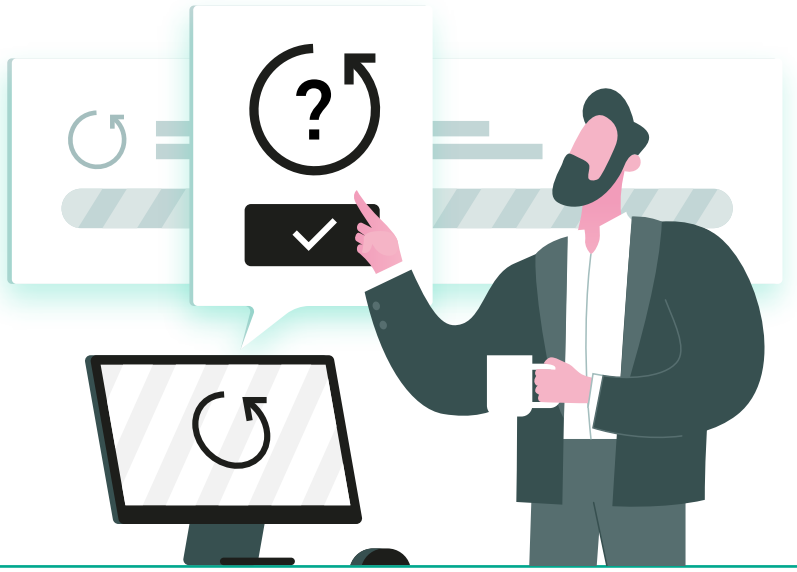
- Approaches for threat modeling;
- Actor identification; and
- Risk identification and prioritization.

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.

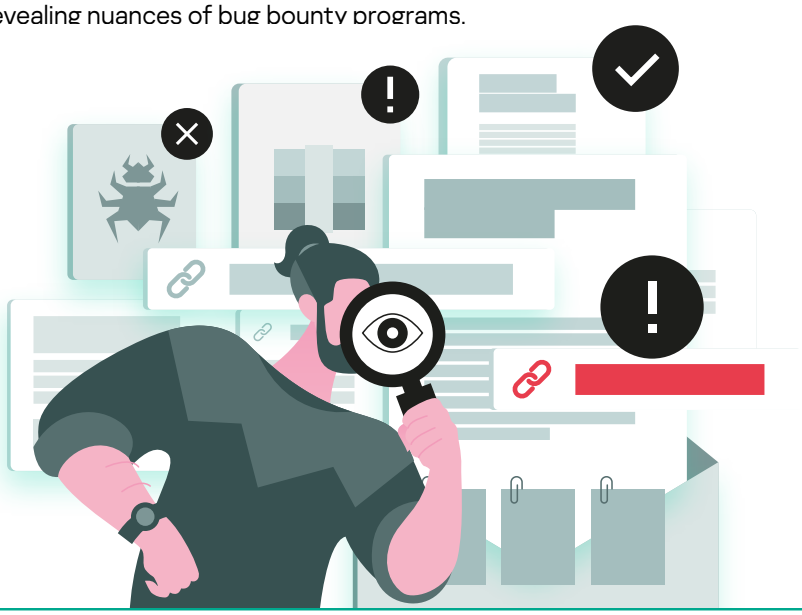


4. Vulnerability management

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;
- 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.



kaspersky

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