MUNI FI Cybersecurity Laboratory

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

INJECT

Pavel Čeleda

https://inject.muni.cz

Do you have to practice a cybersecurity process?

Let’s rethink how cybersecurity exercises are built and delivered.

INJECT

Tabletop Exercises (TTX)

Communication
Cooperation
Coordination

Preparedness
Gaps identification

Current TTX

- On site
- Injects - on paper, office applications
- Linear progression
- Limited options for evaluation
- It is an experience

Expensive
networking/PR

Current TTX

- On site
- Injects - on paper, office apps
- Linear progression
- Limited options for evaluation
- It is an experience

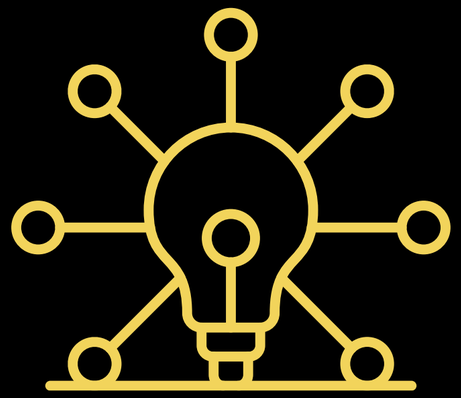
INJECT TTX

- On site & also remote
- Complex approach
- Adaptability
- Semi-Automated Evaluation
- The same or better

The INJECT Exercise Platform significantly streamlines the preparation and execution of exercises.

It delivers a substantial improvement in participants' learning experience — achieving outcomes that traditional approaches cannot match.

Exercise Formats



Micro

- Short, focused sessions
- Designed for user awareness
- Practical skills training
- Ideal for individual participants

Discussion

- Focused on a specific topic
- Useful for identifying gaps and weaknesses
- Supports improving communication
- For managers and leadership teams

Simulations

- Application of real processes and policies
- Most realistic exercise format
- Enables comprehensive team-based training

What exactly does the platform offer
when I’m an exercise participant?

Easy to use website app, no installation

Challenging and engaging scenarios

Personalized feedback

What exactly does the platform offer
when I’m an exercise instructor?

INJECT

- Most of the work is automated by the platform
- Seeing everything a trainee does
- Simplified exercise management

What exactly does the platform offer
when I’m preparing an exercise?

INJECT

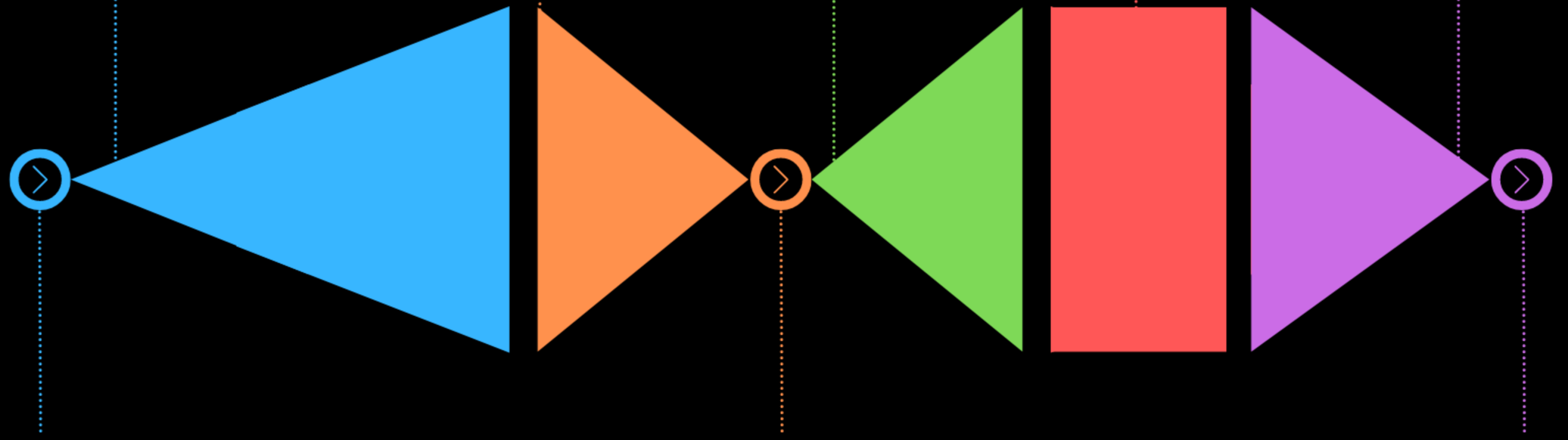
Control over my trainees and my content

Reuse and improvements of my scenarios

From process-technical TTX to high-level policy

How do you prepare an exercise using the INJECT process?

1. Understanding phase
2. Definition phase
3. Preparation phase
4. Execution phase
5. Reflection phase



Initial workshop

Scenario definied

Recommendations

What exactly does the platform offer
when I’m doing exercise evaluation?

INJECT

Data collection

Analysis tools and methods

Machine learning

Example Use Case: Phishing Incident Response Simulation

- Under-2-hour exercise for teams of three junior incident handlers.
- Email communication and simulated tooling (browser analysis, IP blocking, log searches).
- Instructors' role-play key external actors: website operator, victims, users, IT admins, and the data protection officer.
- Used in teaching at the FI MU; scenario available for download.

Automatic message - phishing

abuse@freemail.ex, team-1@mail.uni.ex

Reply

abuse@freemail.ex 2024-11-13 15:26:44 Forward

Our systems have detected that your website address was included in a spoofed email.
It is highly likely that this is a phishing email.
Please check the email as soon as possible (you can find it as an attachment to this email).

FREEMAIL provider

This is automatic email. Please do not respond.

freemail_phishing.zip

doe@mail.uni.ex 2024-11-13 15:31:44 Forward

Dear CSIRT-U,
I'm forwarding yet another phishing mail.

Best regards,
Dr. Doe
Faculty of Science

Today, 1 hour ago, Admin it_department@mail.uni.ex wrote:

https://nice-project.uni.ex/settings/?email=doe@mail.uni.ex
https://nice-project.uni.ex/settings/?email=doe@mail.uni.ex
https://nice-project.uni.ex/settings/?email=doe@mail.uni.ex

Your Account will soon be suspended
Your allowed Email Quota usage has been exceeded on your account.
"doe@mail.uni.ex"
Please kindly verify you are Human and not a robot by following the below link, so we can get your account running normal and retreive all pending mails.
https://nice-project.uni.ex/settings/?email=doe@mail.uni.ex

<="" account="">
Note: You must verify your account using webmail to enable you access your account after 12:00AM before you can send mail.
If no action is taken, you may cease to receive incoming emails
This Email was sent to "doe@mail.uni.ex" as a User from "mail.uni.ex"

Sincerely
mail.uni.ex support team.

user_phishing_mail.txt

jane.taylor@mail.uni.ex 2024-11-13 15:36:45 Forward

To: csirt@mail.uni.ex, harris@mail.uni.ex

Greetings,
could you please investigate what happened at our website? I can see only a folder with some files (see attachment) instead of our web presentation: https://nice-project.uni.ex/
Thanks a lot!

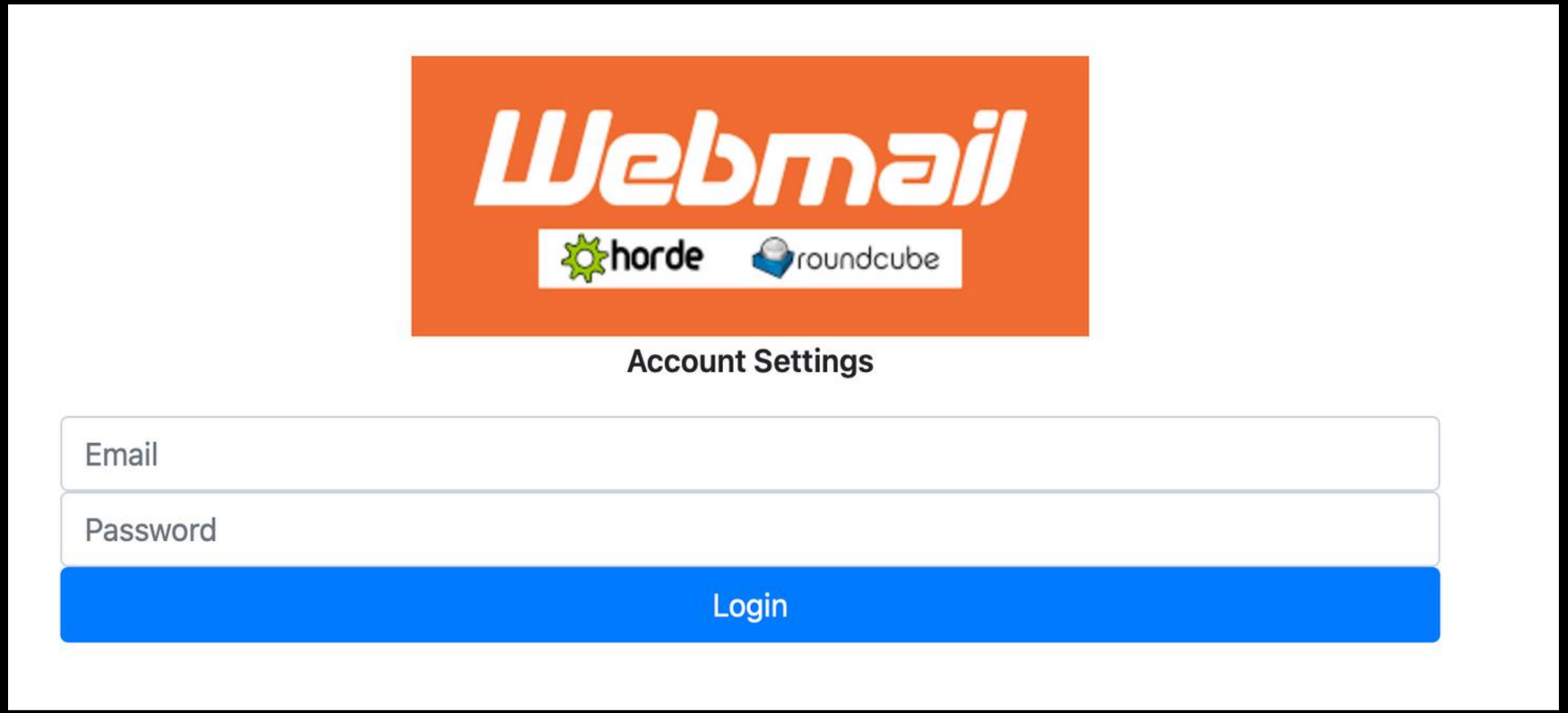
Jane Taylor
project manager
Nice project

nice-project-root.png

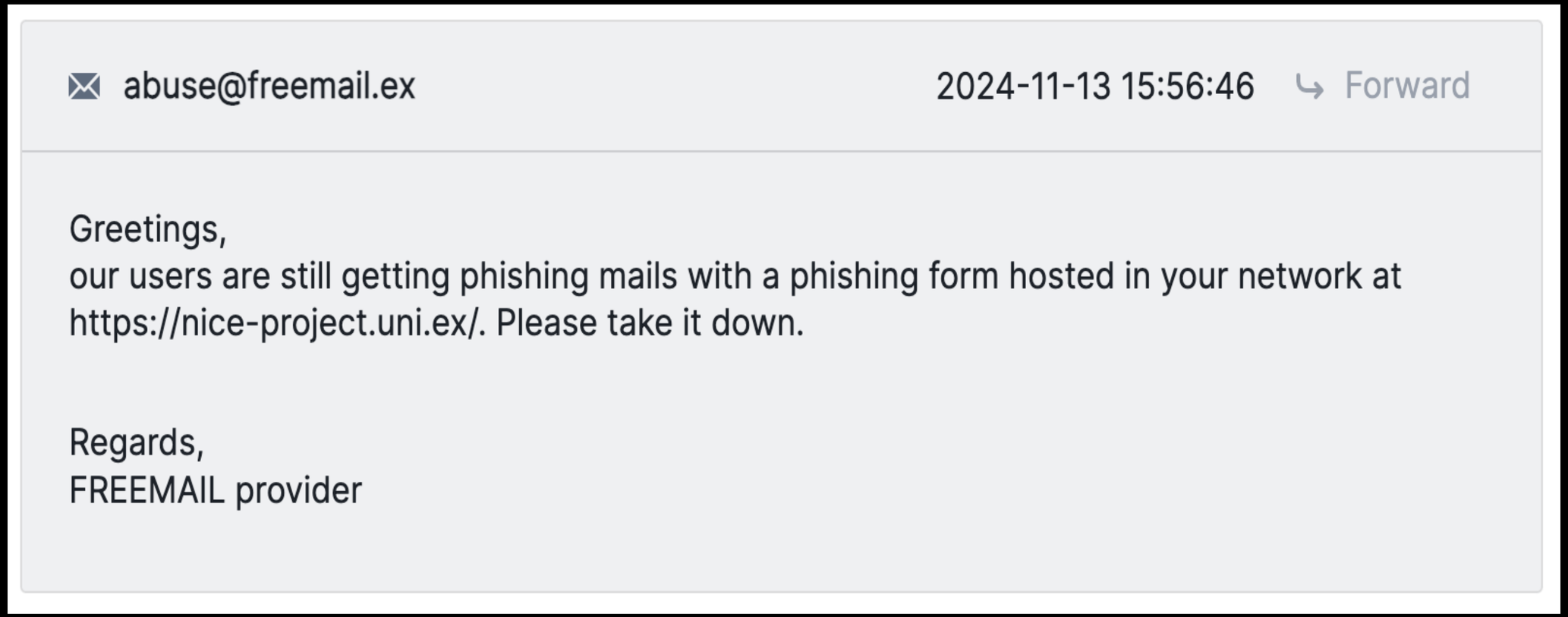
Index of /

Name	Last modified	Size	Description
Parent Directory		-	
birthdays.txt	2021-09-10 10:27	1.2K	
schema.jpg	2021-09-10 10:02	0	

Need to use the tools – Output of the simulated browser tool.



Hint for teams that have not yet blocked the phishing page.
Before sending, the system checks whether the team has already used the tool.
If they have, the email will not be delivered.



INJECT in a nutshell

Simplified Preparation & Delivery

Improved Learning Experience

INJECT

It’s here, open-source, and ready to use.

Significant potential for enhancing security and resilience.

You can start now and influence it.

INJECT Exercise Platform

- Home
- Technical documentation
  - Technical Overview
  - Installation
  - System architecture
  - Authorization and User Management
  - API Documentation
  - Backend changelog
- How to prepare an exercise?
  - INJECT Process
  - 01 Understand
  - 02 Define
  - 03 Prepare
  - 04 Execute
  - 05 Reflect
- Glossary of Terms
- Authors
- Report bugs
- Acknowledgements
- How to cite

INJECT EXERCISE PLATFORM DOCUMENTATION

Welcome to the INJECT Exercise Platform Documentation portal! Here, you'll find comprehensive resources to guide you through every aspect of the INJECT Exercise Platform, from installation to advanced usage.

OVERVIEW

The INJECT Exercise Platform revolutionizes tabletop exercise management by providing a versatile and intuitive solution for organizations of all sizes. Whether you're a small team looking to improve emergency response protocols or a large corporation conducting complex training scenarios, INJECT Exercise Platform offers the flexibility and power to meet your needs.

TECHNICAL DOCUMENTATION

Explore the technical documentation to gain a deeper understanding of the platform's architecture, APIs, security measures, and installation procedures.

- **Installation Guide**: Step-by-step instructions for deploying INJECT Exercise Platform using Docker Compose and Nginx.
- **Security**: Details on the security measures and practices implemented in the INJECT

Table of contents

- Overview
- Technical Documentation
- INJECT Process
- Additional Resources