PenQuest

A CYBER DEFENSE GAME

Robert Luh ▪ 16. Forschungsforum der österreichischen Fachhochschulen ▪ 19.04.2023

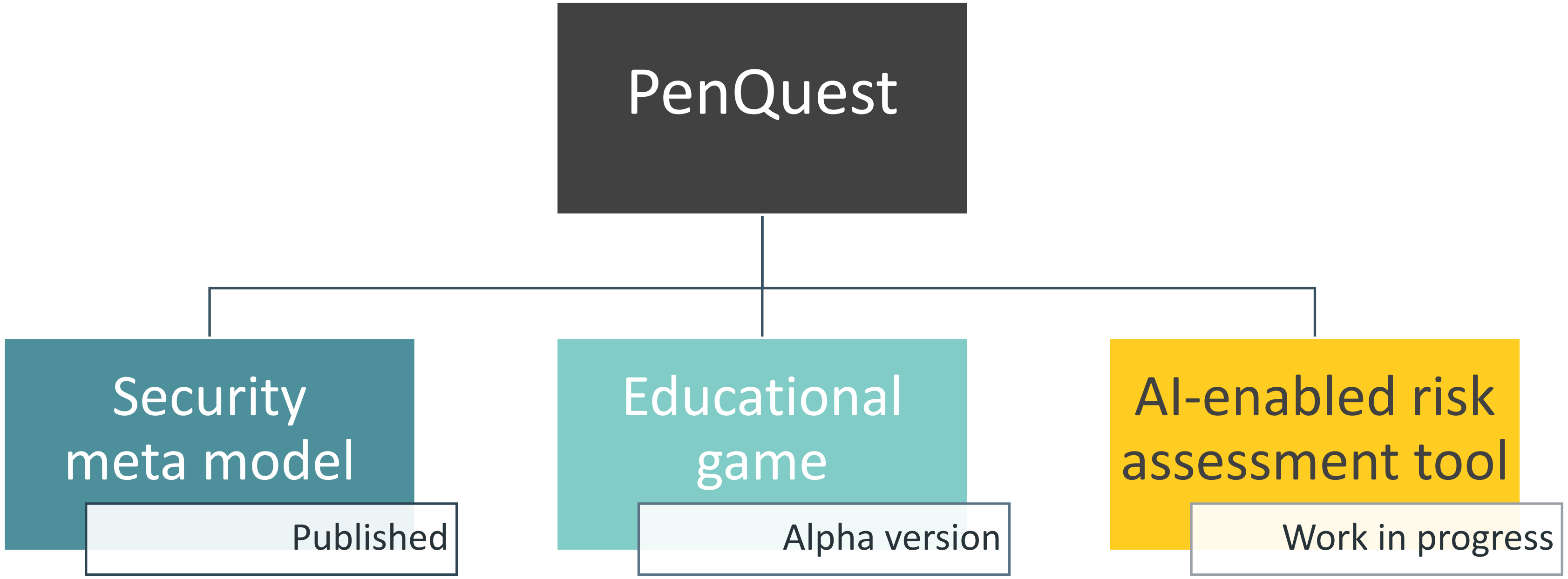
PenQuest Introduction

IT security as strategy game

- PenQuest is a turn-based, digital two-player **board game** based on real (hacking) threats and means of mitigation
- Created to teach **security concepts** & **threat mitigation**
- Mix of **genres**

PenQuest Introduction

IT security as strategy game…and more.



PenQuest

Security meta model

Published

Educational game

Alpha version

AI-enabled risk assessment tool

Work in progress

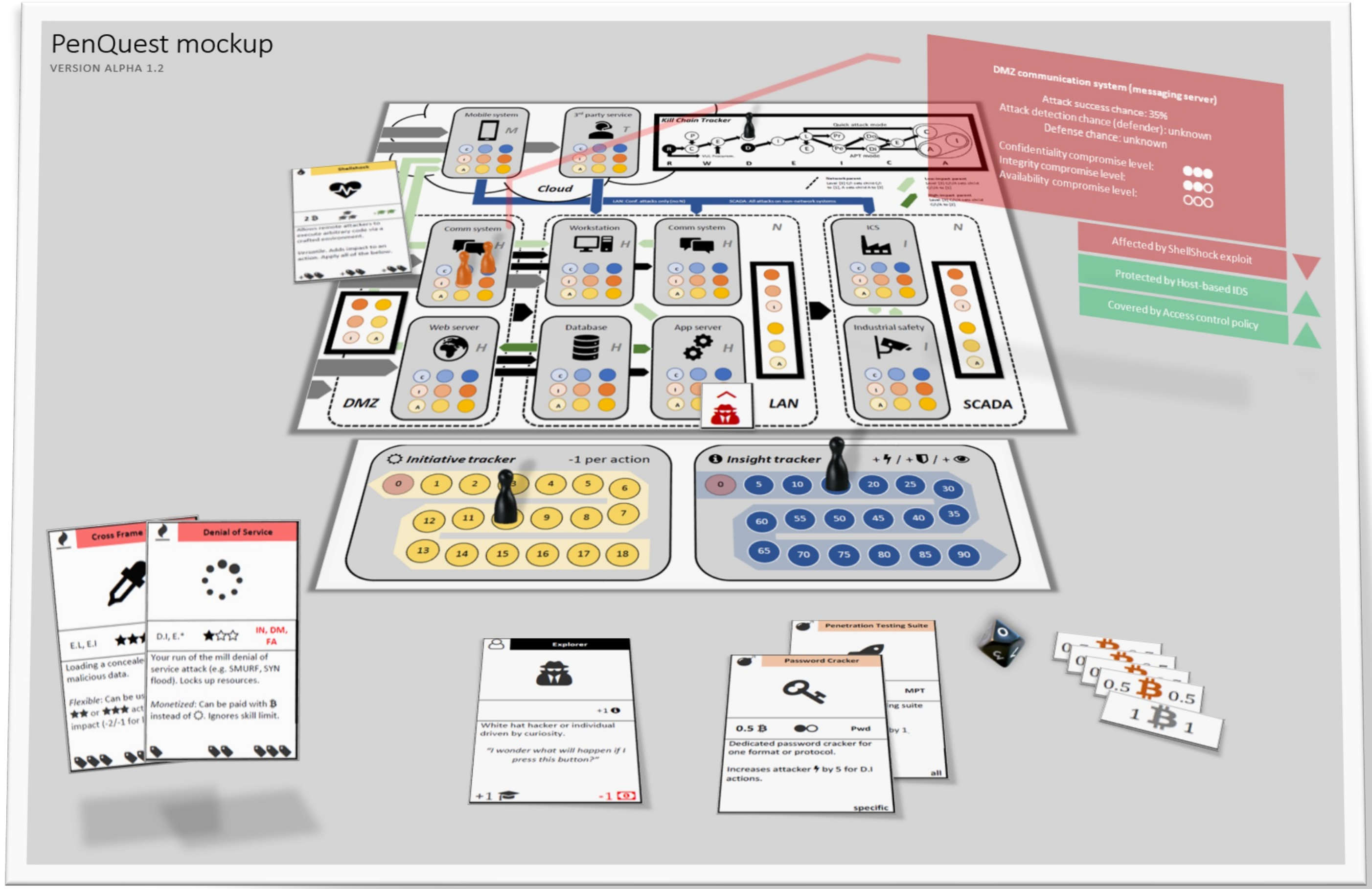
/fh/// st.pölten

universität wien

Evolution

Once upon a time…

- PenQuest was born as conventional **board game** used to gamify a model for intrusion detection **event classification**.
- Required a **human game master**
- And **today**?



PenQuest mockup
VERSION ALPHA 1.2

DMZ communication system (messaging server)
Attack success chance: 35%
Attack detection chance (defender): unknown
Defense chance: unknown
Confidentiality compromise level: ●●●
Integrity compromise level: ●●○
Availability compromise level: ○○○

Affected by ShellShock exploit
Protected by Host-based IDS
Covered by Access control policy

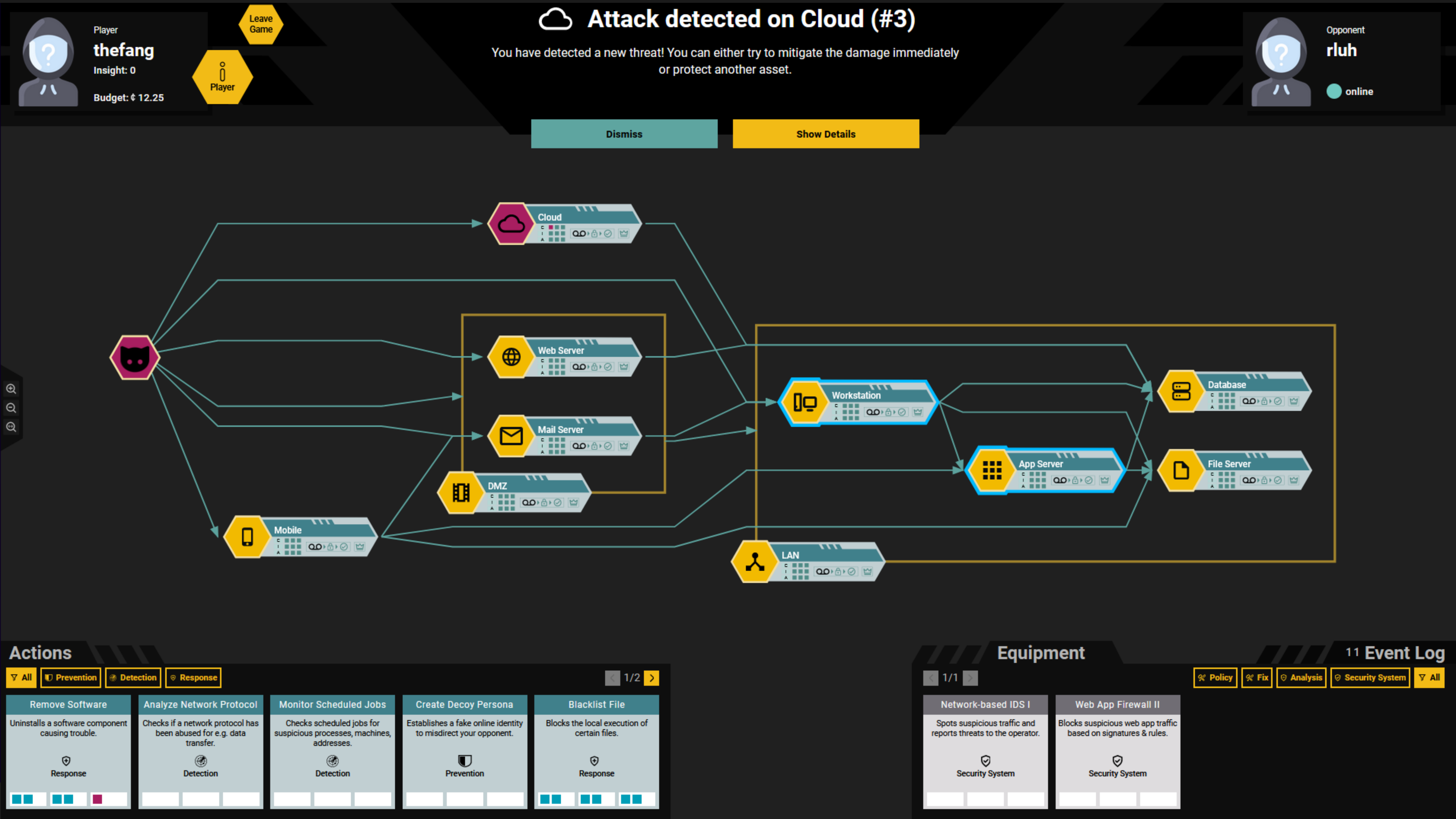
Cross Frame
E.L, E.I ★★★
Loading a conceale… malicious data.
Flexible: Can be us… ★★ or ★★★ act… impact (-2/-1 for …

Denial of Service
D.I, E.* ★☆☆ IN, DM, FA
Your run of the mill denial of service attack (e.g. SMURF, SYN flood). Locks up resources.
Monetized: Can be paid with ₿ instead of ○. Ignores skill limit.

Explorer
+1
White hat hacker or individual driven by curiosity.
"I wonder what will happen if I press this button?"
+1 -1

Password Cracker
0.5 ₿ ●○ Pwd
Dedicated password cracker for one format or protocol.
Increases attacker ϟ by 5 for D.I actions.
specific

Penetration Testing Suite
MPT
…ing suite
…by 1
all



Attack detected on Cloud (#3)

You have detected a new threat! You can either try to mitigate the damage immediately or protect another asset.

Remove Software
Uninstalls a software component causing trouble.
Response

Analyze Network Protocol
Checks if a network protocol has been abused for e.g. data transfer.
Detection

Monitor Scheduled Jobs
Checks scheduled jobs for suspicious processes, machines, addresses.
Detection

Create Decoy Persona
Establishes a fake online identity to misdirect your opponent.
Prevention

Blacklist File
Blocks the local execution of certain files.
Response

Network-based IDS I
Spots suspicious traffic and reports threats to the operator.
Security System

Web App Firewall II
Blocks suspicious web app traffic based on signatures & rules.
Security System

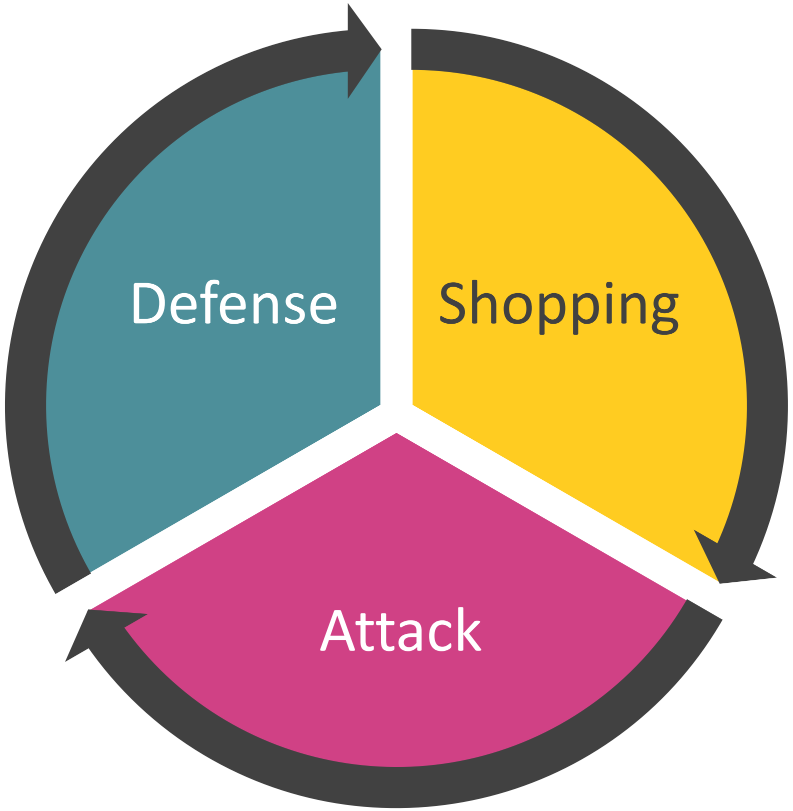
Game mechanics

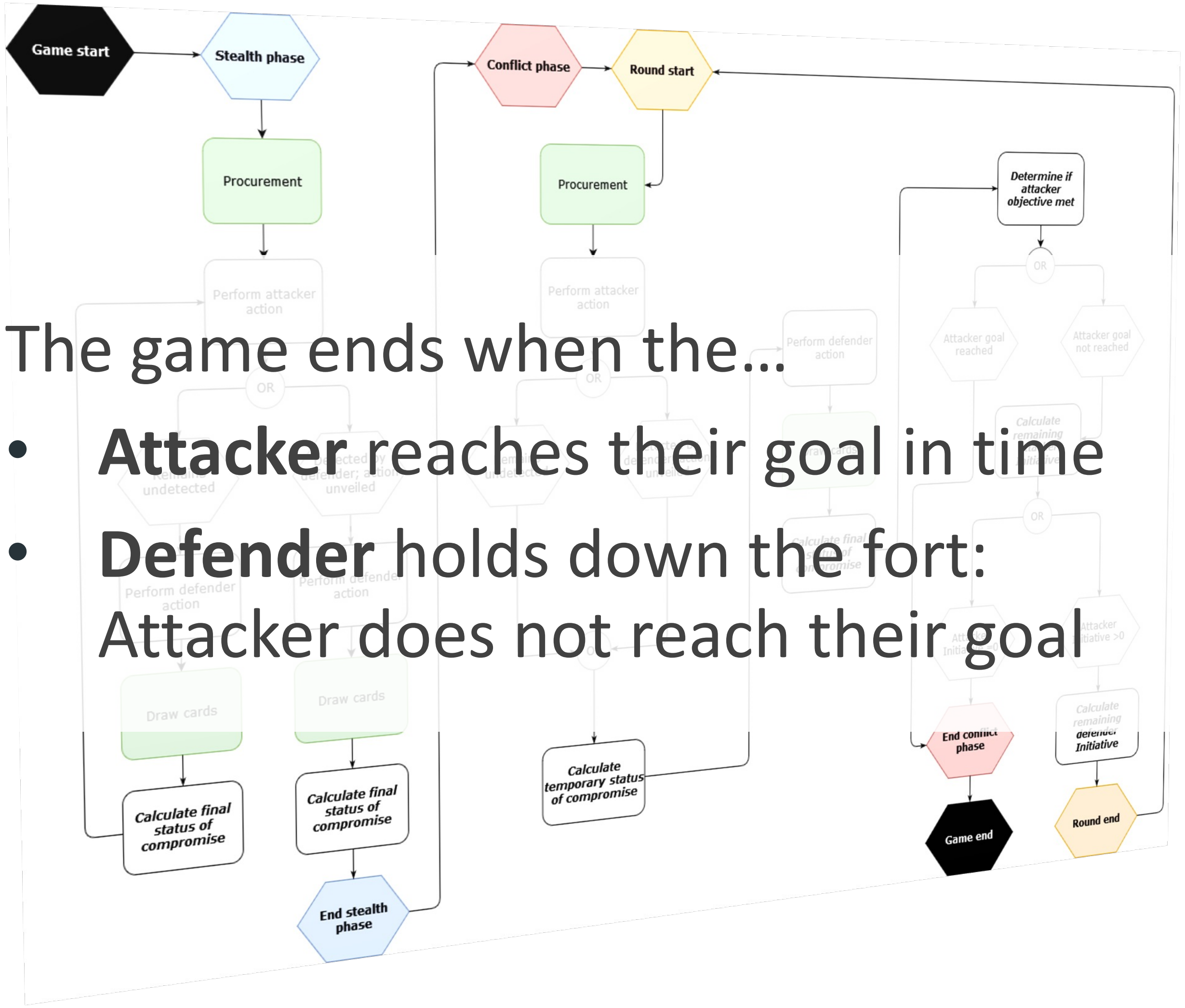
Game loop

- Attacker is assigned a **target** (e.g., database server) and **goal** and plays **actions** to achieve his or her malicious objective
  - **Confidentiality** ▶ Data theft
  - **Integrity** ▶ Manipulation of data, sabotage
  - **Availability** ▶ Denial of service
- Defender uses different **actions** to **prevent** or **mitigate** the damage
- Both sides can procure and use **tools** (software, systems, etc.)
  - Permanent equipment (password crackers, firewalls, etc.)
  - Malware, exploits & fixes

Game mechanics

Game loop





The game ends when the…

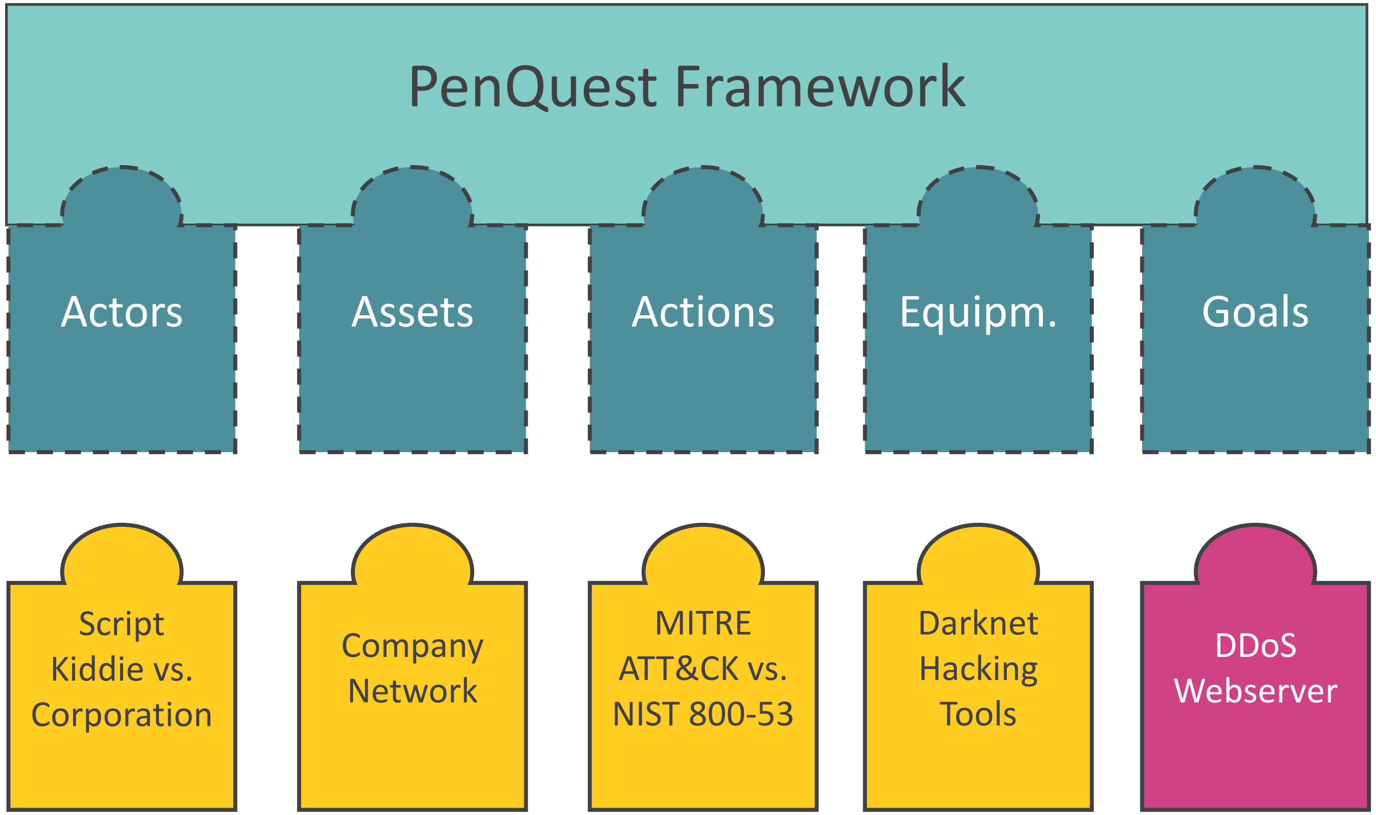
- **Attacker** reaches their goal in time
- **Defender** holds down the fort: Attacker does not reach their goal

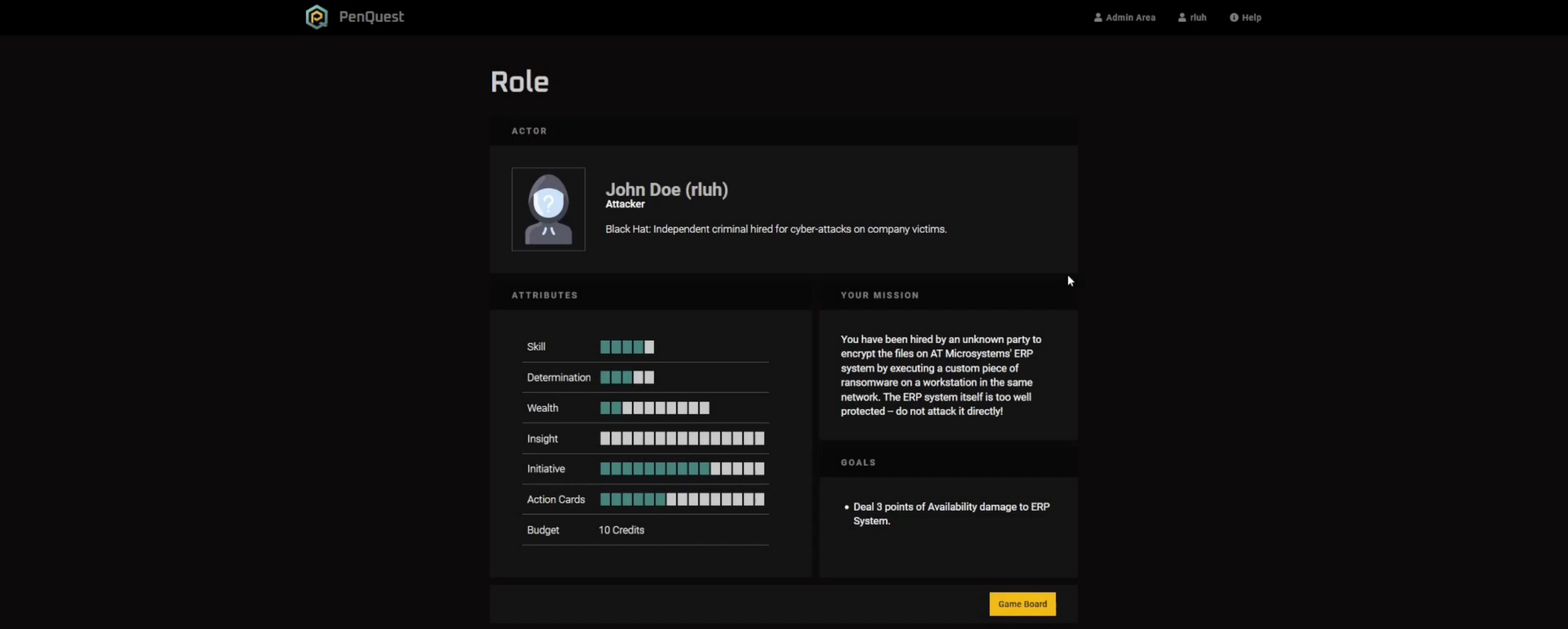
Framework

Game components

At its heart, PenQuest is very **flexible**:

- Everything can be **customized**
- Focus e.g., on more **technical** or **organizational** aspects
- Small **demo** to huge multi-stage **campaign**





Role

ACTOR

John Doe (rluh)
Attacker

Black Hat: Independent criminal hired for cyber-attacks on company victims.

ATTRIBUTES

Skill	🟩🟩🟩🟩⬜
Determination	🟩🟩🟩⬜⬜
Wealth	🟩🟩⬜⬜⬜⬜⬜⬜⬜⬜
Insight	⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜
Initiative	🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩⬜⬜⬜⬜⬜
Action Cards	🟩🟩🟩🟩🟩🟩⬜⬜⬜⬜⬜⬜⬜⬜⬜
Budget	10 Credits

YOUR MISSION

You have been hired by an unknown party to encrypt the files on AT Microsystems' ERP system by executing a custom piece of ransomware on a workstation in the same network. The ERP system itself is too well protected – do not attack it directly!

GOALS

- Deal 3 points of Availability damage to ERP System.

Actors

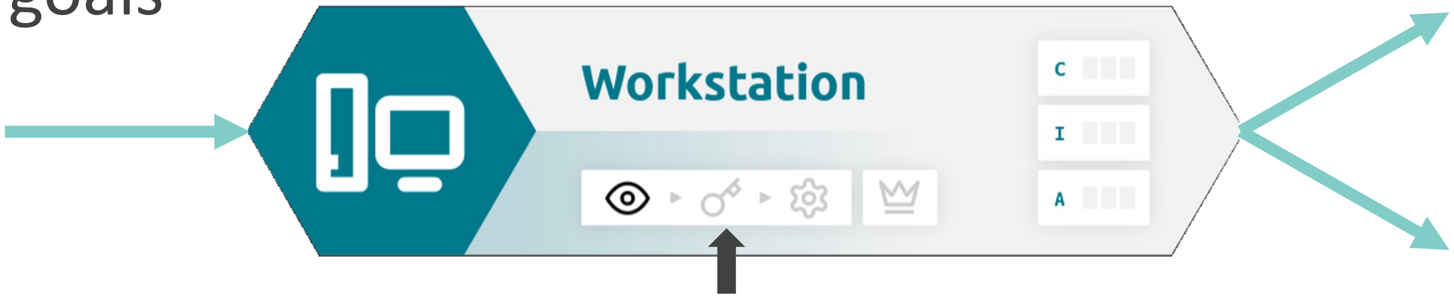
Every player has a role and defining attributes

Game components

Assets

…define the game board & represent **targets**

- Each asset has 3 separate **damage indicators** corresponding to an attacker’s possible goals
  - Confidentiality
  - Integrity
  - Availability



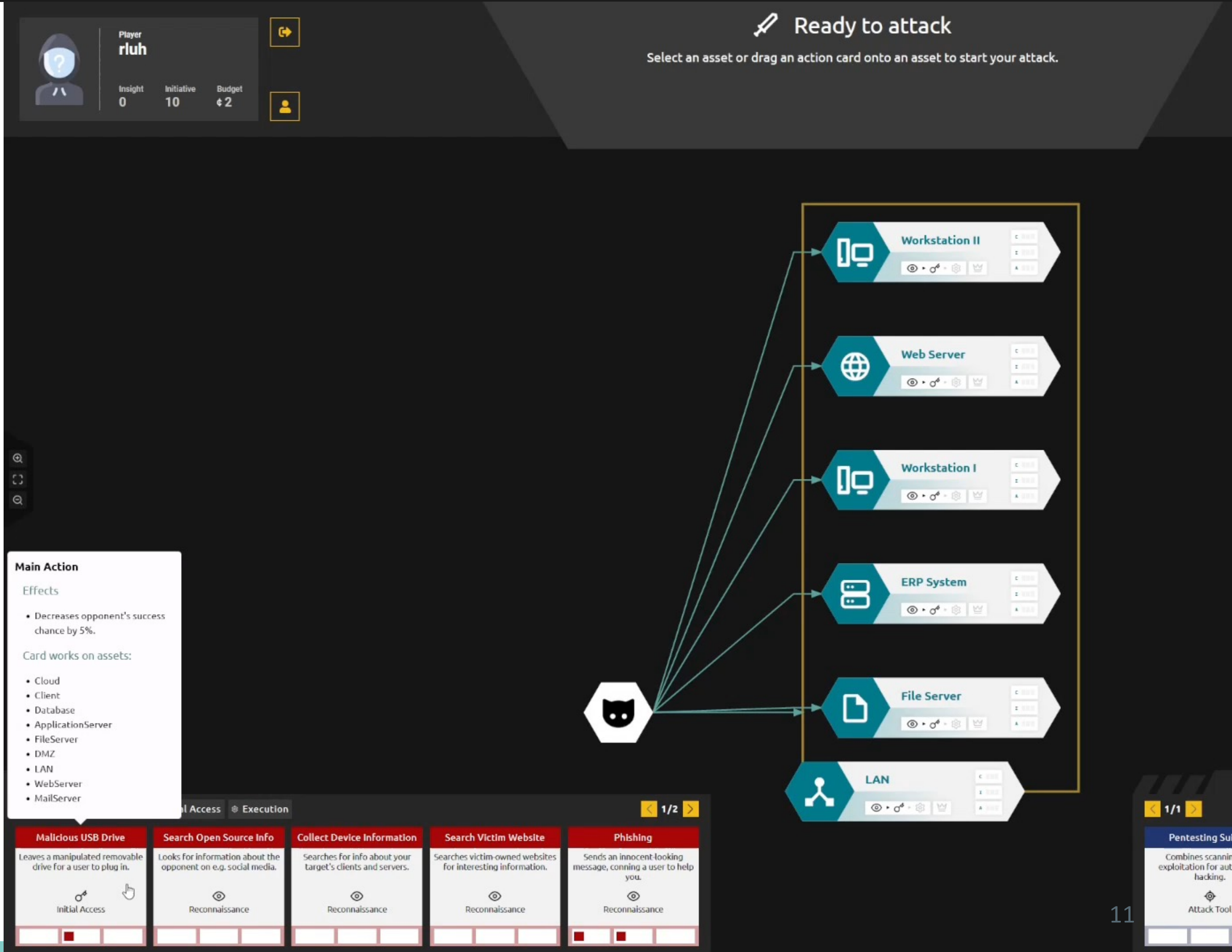
- Attacker has to progress along a simplified **cyber kill chain**
- Arrows between assets indicate possible **lateral movement**
- **Dependencies** between assets, **privilege requirements**, and more.

Game components

Actions

...represent what attackers & defenders can do in the game. We use **established frameworks**:

- **Attacker**: Derived from MITRE ATT&CK, CAPEC
- **Defender**: NIST 800-53, MITRE D3FEND



Player
rluh

Insight 0 · Initiative 10 · Budget ¢2

Ready to attack

Select an asset or drag an action card onto an asset to start your attack.

Main Action

Effects

- Decreases opponent's success chance by 5%.

Card works on assets:

- Cloud
- Client
- Database
- ApplicationServer
- FileServer
- DMZ
- LAN
- WebServer
- MailServer

Malicious USB Drive: Leaves a manipulated removable drive for a user to plug in. (Initial Access)

Search Open Source Info: Looks for information about the opponent on e.g. social media. (Reconnaissance)

Collect Device Information: Searches for info about your target's clients and servers. (Reconnaissance)

Search Victim Website: Searches victim-owned websites for interesting information. (Reconnaissance)

Phishing: Sends an innocent-looking message, conning a user to help you. (Reconnaissance)

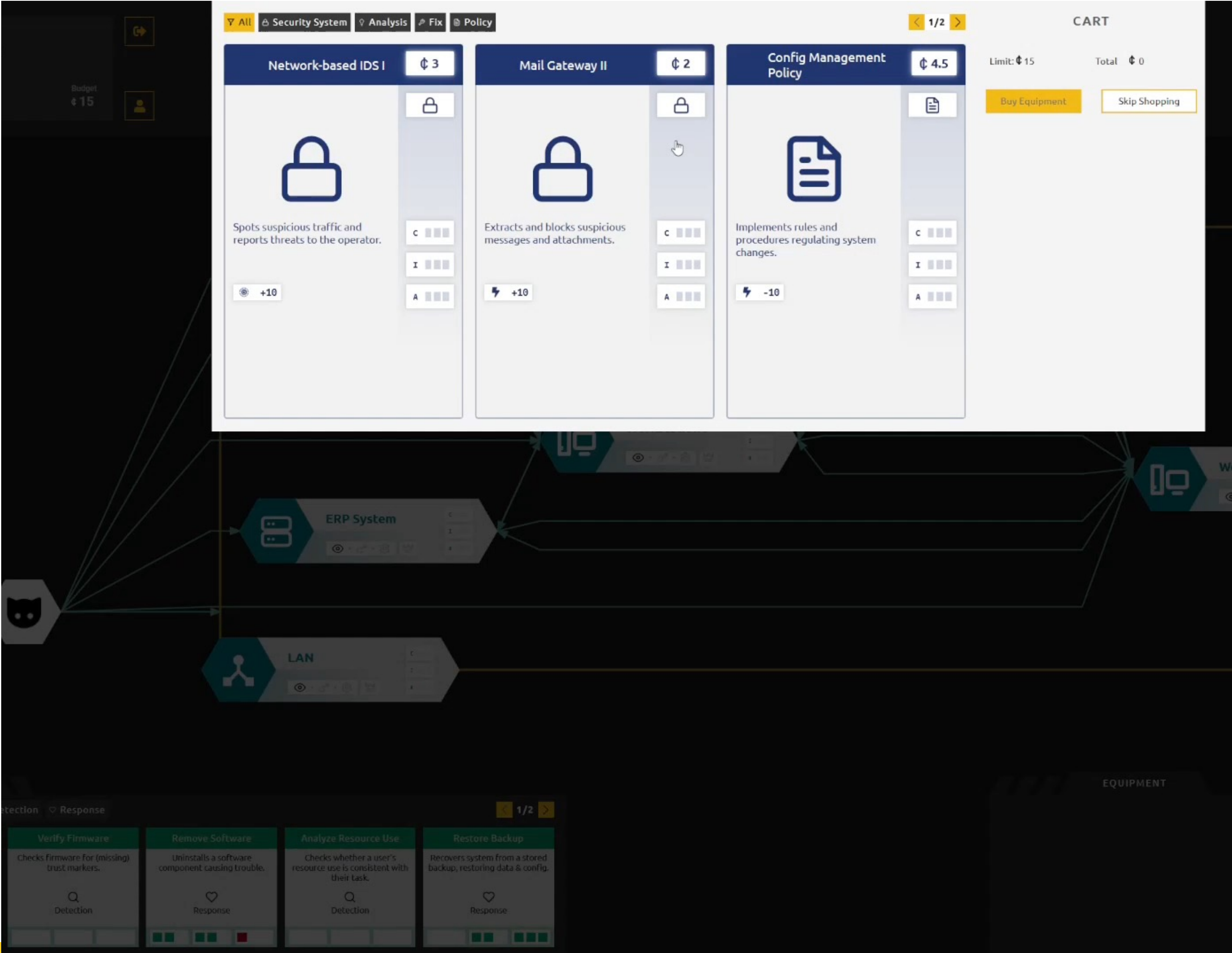
Pentesting Su: Combines scannin exploitation for aut hacking. (Attack Tool)

Game components

Equipment

…supports actions thru additional effects:

- Malware & exploits
- Pentesting tools
- Scanners
- Antimalware solutions
- Security appliances
- Fixes for exploits
- …



Network-based IDS I — ₵ 3

Spots suspicious traffic and reports threats to the operator.

+10

Mail Gateway II — ₵ 2

Extracts and blocks suspicious messages and attachments.

+10

Config Management Policy — ₵ 4.5

Implements rules and procedures regulating system changes.

-10

Limit: ₵ 15 Total ₵ 0

Verify Firmware — Checks firmware for (missing) trust markers. Detection

Remove Software — Uninstalls a software component causing trouble. Response

Analyze Resource Use — Checks whether a user's resource use is consistent with their task. Detection

Restore Backup — Recovers system from a stored backup, restoring data & config. Response

What's next?

INferring Optimal DEfense Strategies from PenQuest

- **INODES** (University of Vienna) is a follow-up project based on our educational game

Main objective: Infer the **best possible defense strategy** for a given attack on an information system infrastructure.

- We focus on 2 **approaches**:
  - **Model checking**
  - **Reinforcement learning**

Conclusion

PenQuest links worlds

- Real **attacks**, real **controls**
- Numbers are derived from common **data sources** ▶
- Allows you to build your own **network topology**
- PenQuest is (or will be)…
  - **Security model**
  - **Educational game**
  - **Risk assessment tool**
  - **Attack simulator** (we hope that „penquesting“ catches on)
  - **Strategy optimizer**

NIST

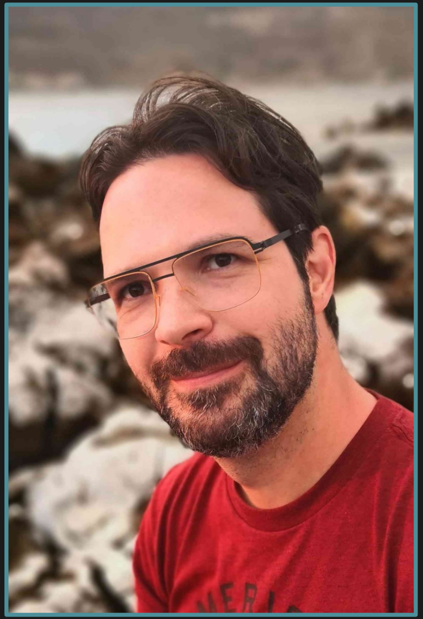
MITRE ATT&CK™

CAPEC™

CVE®

CWE™

Who are we?



🟨 🟦	**Robert Luh**	▶ Idea, security model, rules
🟨 🟦	**Sebastian Eresheim**	▶ Backend development, RL
🟩 🟨	**Thomas Petelin**	▶ Frontend & backend dev.
🟨	**Simon Gmeiner**	▶ RL
🟦	**Florian Mayr**	▶ Design, HTML & CSS
🟨	**Paul Tavolato**	▶ Model checking

🟩 Volunteer

🟦 PenQuest (FHSTP)

🟨 INODES (FWF)

PenQuest

A CYBER DEFENSE GAME

Let’s play!

Contact

robert.luh@fhstp.ac.at
https://www.pen.quest