OST
Ostschweizer
Fachhochschule

Cyber Defense HS2024

Herzlich Willkommen

Ivan Bütler

17. September 2024

Abteilung Informatik, Rapperswil

Agenda

→ **Begrüssung**

- Wer bin ich?
- Einführung Cyber Defense Modul
- Organisatorisches
- Hacking-Lab
- Teams

OST

Wer bin ich?

https://about.me/ivan.buetler

Ivan Bütler

079 250 06 28

- Lehrbeauftragter OST (Informatik, Security)
- Studiengangsleiter CAS Cyber Security ivan.buetler@ost.ch
- Gründer Compass Security ivan.buetler@compass-security.com
- Mitgründer Verein Swiss Cyber Storm www.swisscyberstorm.com
- Security Experte SATW (Schweizerische Akademie der Technischen Wissenschaften) www.satw.ch

Cyber Defense HS2024

Einführung, Konzept

Abteilung Informatik

Ivan Bütler

17. September 2024

OST
Ostschweizer
Fachhochschule

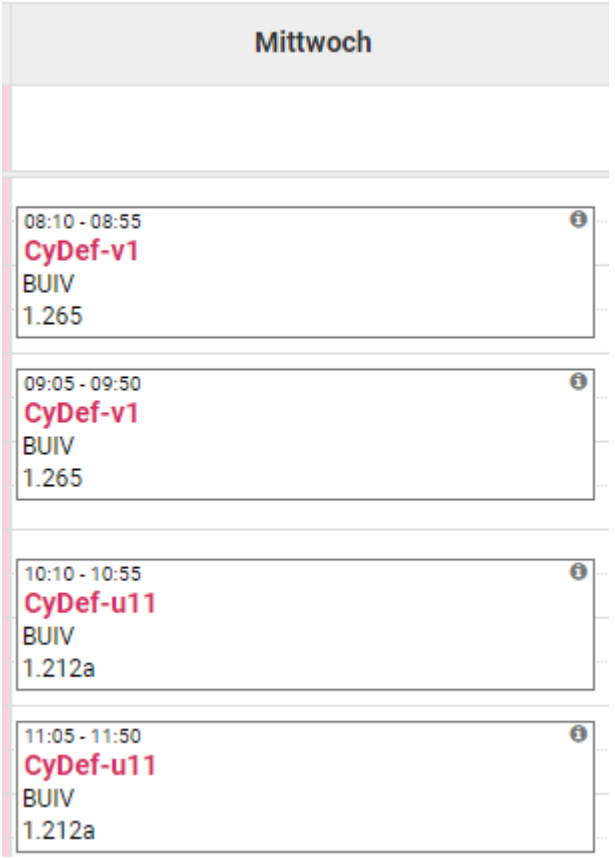
Modul Cyber Defense in der Übersicht

- Das Cyber Defense Modul ergibt 4 ECTS Punkte

- Pro Woche 2 Stunden Unterricht (Frontal)
  - 1.265 Campus Rapperswil 08:10 – 09:50 Uhr

- Pro Woche 2 Stunden Übungen (primär im Hacking-Lab)
  - Raum 2.212a Campus Rapperswil
  - Remote (Home Office)

- Sie erhalten Zugriff auf die Übungen via Hacking-Lab https://ost.hacking-lab.com/



Cyber Defense

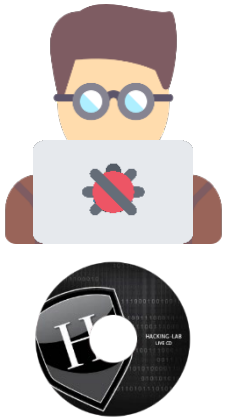
- Präventiv Massnahmen
- Fokus: Schutz eines Unternehmen vor Cyber Attacken
- Monitoring / Splunk / Erkennung Exfiltration
- Content Filter (HTTPS, E-Mail)
- ISMS
- Credentials, 2FA, TPM
- Red Teaming
- Bitlocker, VPN Security, Externer Access
- O365 Security
- Nicht im Scope: Sicherheit in Produkten, ABB, Phonak, …

Incident Response

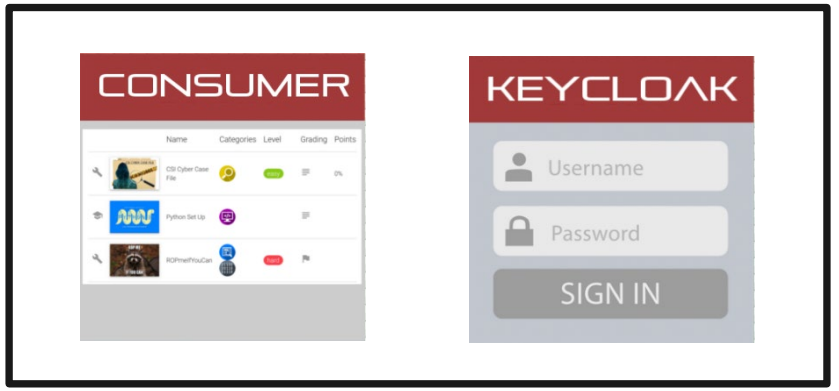
- Reaktive Massnahmen
- Fokus: Reaktion beim Auftreten eines Cyber Angriffs
- CEO Fraud analysieren
- Wie auf ein Botnetz reagieren
- Wie bei Ransomeware reagieren
- Wie auf Phishing reagieren
- APT, Malware, Cyber Kill Chain
- Threat Intelligence
- Forensic Readiness
- Forensik, Disk, Memory, Live Response

Cyber Defense Lab

Hacking-Lab Übersicht



Student Application



Hacking-Lab On-Premise Deployment

Hacking-Lab Cloud Deployment

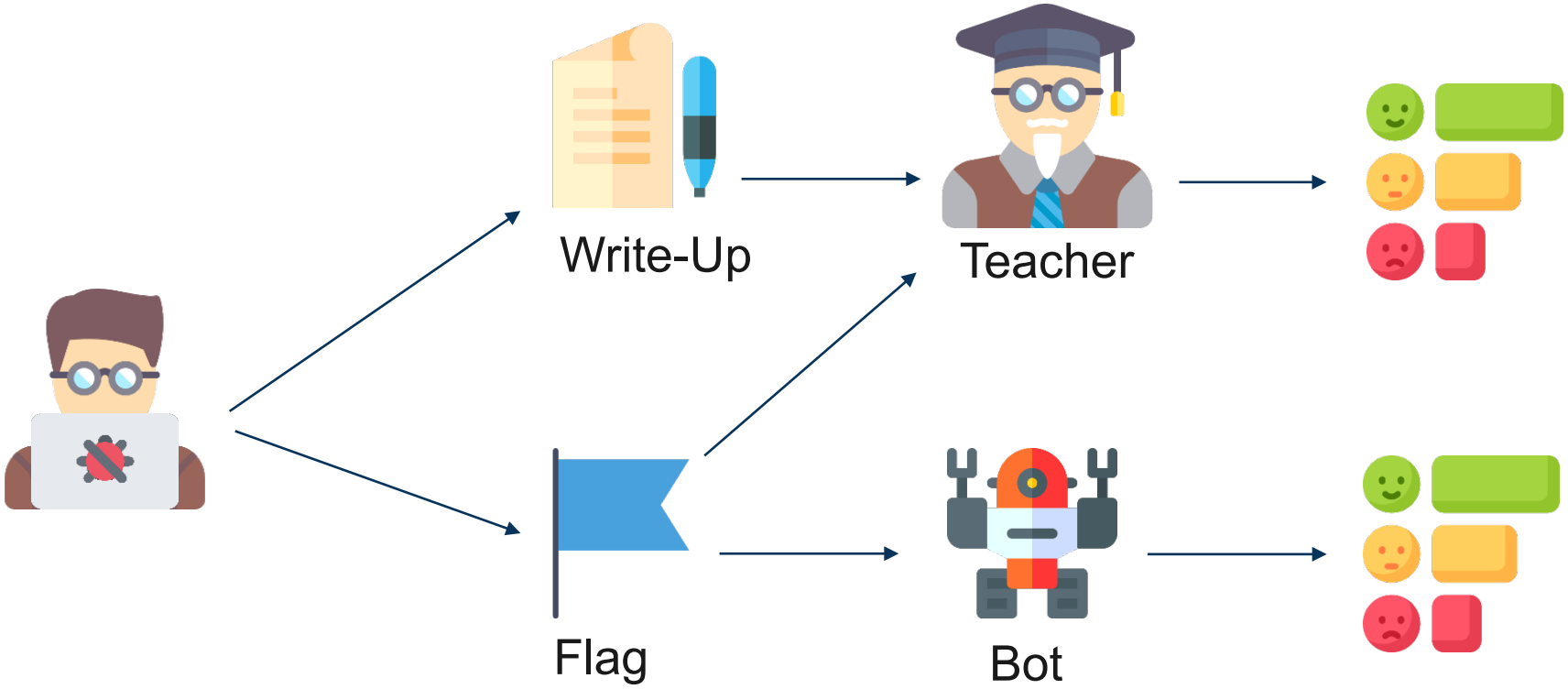
Student Application
- Self-Registration
- Login
- Event Management

Simple Setup
- Vulnerable Systems
- Hackable Targets
- Dockers
- Files

Complex Setup
- Active Directory
- Firewall
- Proxy, Mailsystem
- SOC, Monitoring

OST

Cyber Defense Konzept



Erwartetes Ergebnis im Hacking-Lab

- Ergebnis abhängig von Aufgabe
  - Write-Up: Bitte erstellen Sie pro Hacking-Lab Aufgabe ein PDF
  - Flag: Bitte reichen Sie das Flag (ein String) als Lösung ein

- Feedback bei **Flag-basierten** Aufgaben
  - System meldet direkt ob das Flag korrekt ist oder nicht

- Feedback bei **Write-Up basierten** Aufgaben
  - Manuelle Durchsicht von Ivan Bütler

Notengebung

- Am Schluss des Cyber Defense Moduls gibt es eine Schlussprüfung (2 Stunden)
  - Schriftliche Prüfung
    - Leistungsbewertung

      Während der Prüfungssession:

      Schriftliche Prüfung, 120 Minuten

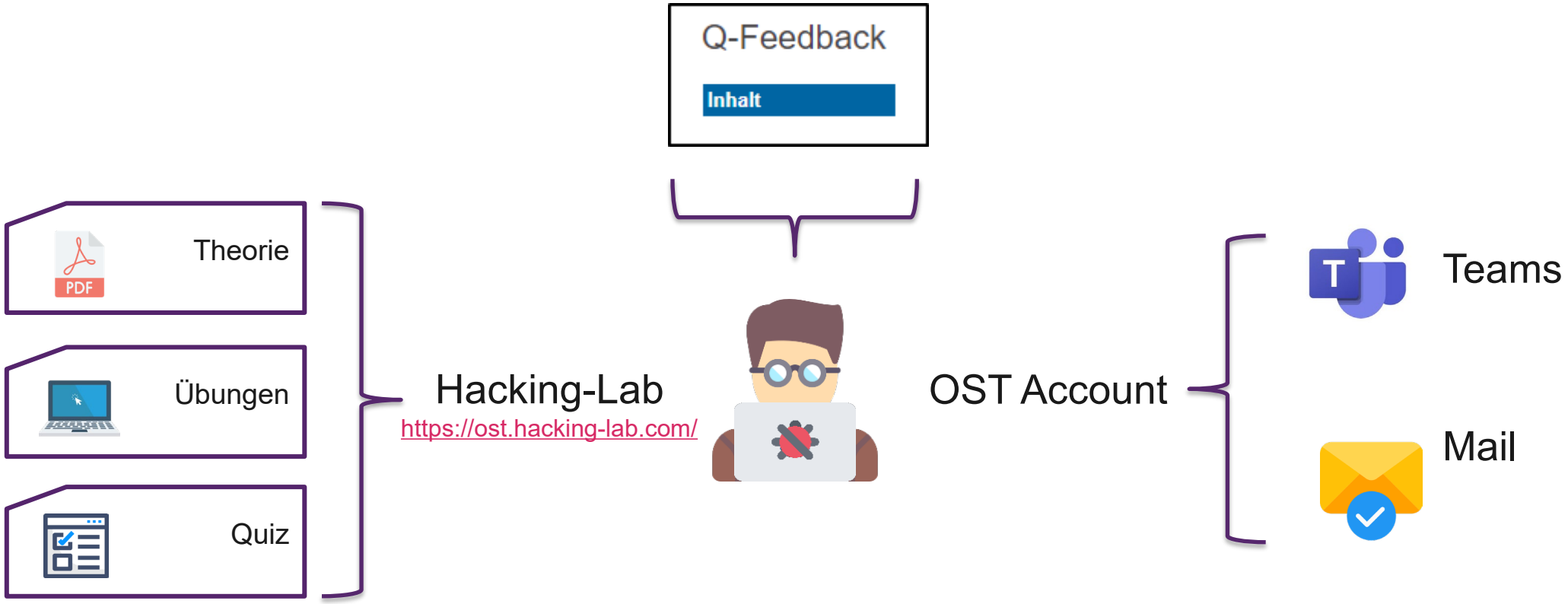
      Zulassungsbedingungen zur Prüfung:

      Testat

- Aufgaben (Testat) im Hacking-Lab ergeben **keine** Note
  - Know-How aus den Übungen fliessen in die Schlussprüfung ein
  - Know-How aus den Übungen sind wichtig für das Verständnis
  - Engagement Hacking-Lab Aufgaben entscheidet über “Aufrunden oder Abrunden”

Cyber Defense Tools in der Übersicht

Cyber Defense HS2023 Tools im Überblick



Organisatorisches

Zugriffe / Sign-Up

Abteilung Informatik

Ivan Bütler

17. September 2024

OST
Ostschweizer
Fachhochschule

Zugriff MS Teams

MS Teams

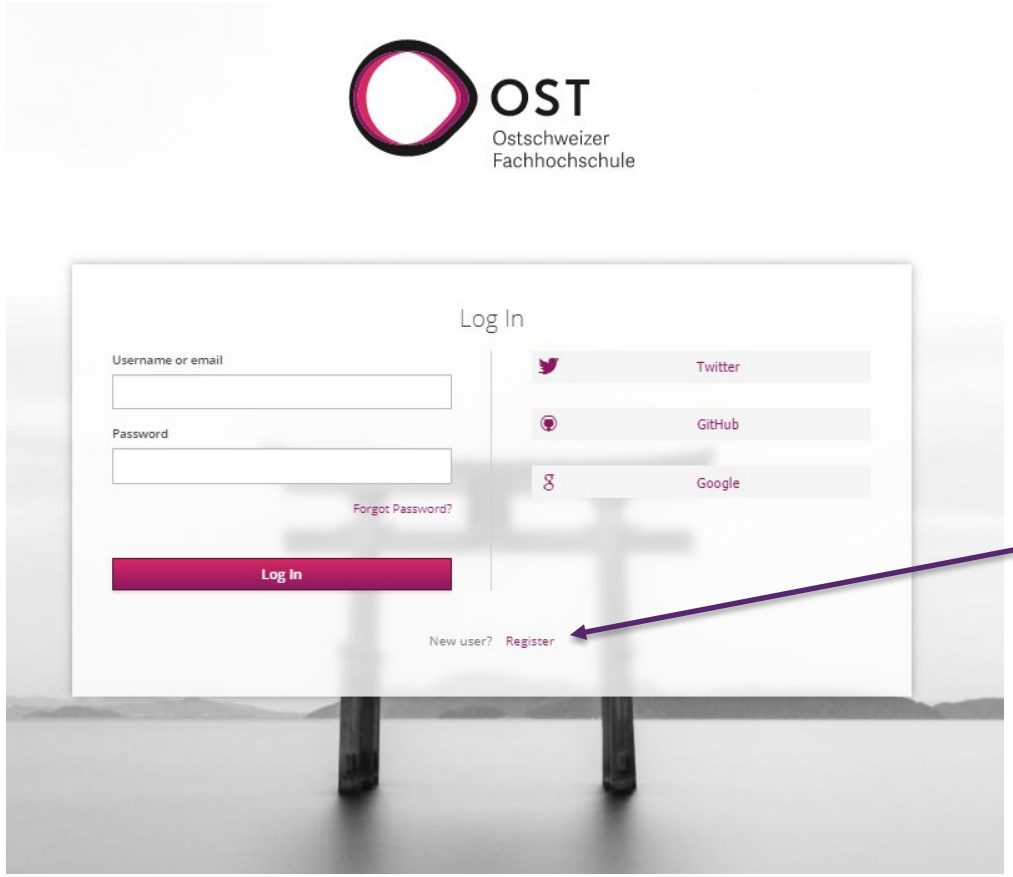
- Ich habe den MS Teams Channel vor rund 2 Wochen eröffnet
- Ist jemand noch nicht im Teams Channel drin?

Zugriff Hacking-Lab

Sign-Up Account

Nur nötig, falls Sie noch keinen Account haben

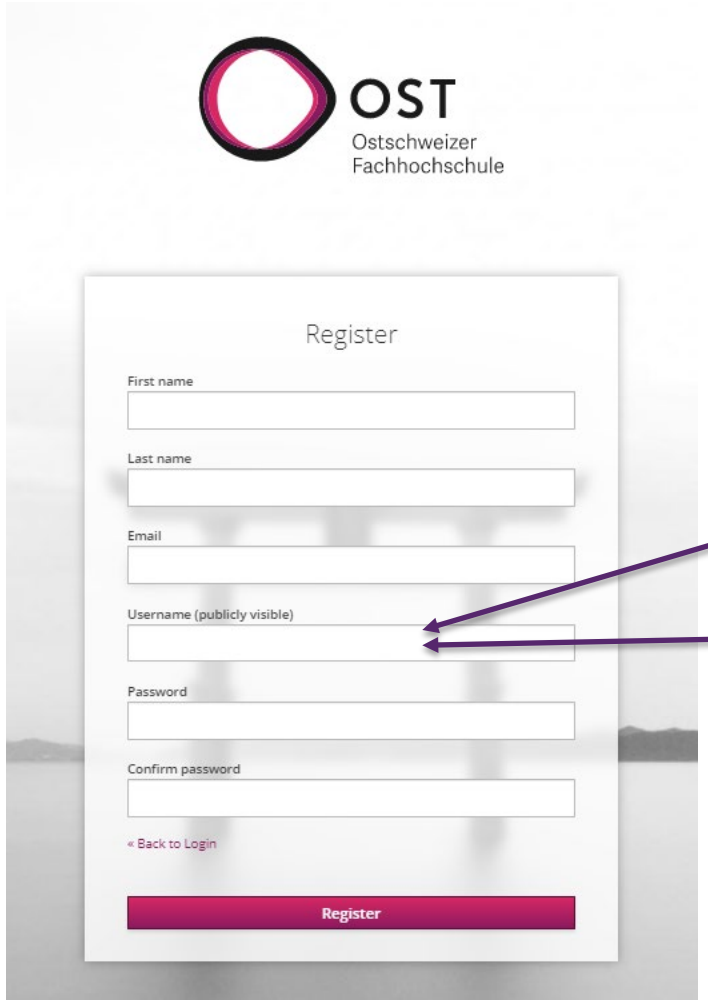
- Bitte unter https://ost.hacking-lab.com/ einen persönlichen Account anlegen



Register Account

Sign-Up Account

Nur nötig, falls Sie noch keinen Account haben



- Username soll ein Nickname sein. Bitte **keine** E-Mail als Username eingeben
- Den gewählten Username sehen später andere Benutzer im Hacking-Lab

Join HackLab

- https://ost.hacking-lab.com/events/redeem/KXEFA-5VR6X-HBBN5-DTXWJ

Nutzung von MS Teams

- Bitte stellen Sie Ihre Fragen in Teams
- Bitte stellen Sie ihre Fragen öffentlich (public), damit Andere von den Antworten profitieren können
- Bitte möglichst keine PM (Direktnachrichten)

keine Mails

- Fragen per Mail werden **nicht** beantwortet. Über Teams sehen alle Studenten die Fragen und entsprechenden Antworten. **Bitte keine privaten Chat Messages in Teams nutzen**.