Swisscom StartUp Challenge 2021 – Security

Swisscom's three biggest challenges in the cyber security environment

Decentralized Security

Protection of our customers' assets in an increasingly decentralized world where perimeter security is no longer enough.

Examples

- Establishing a Zero Trust approach for more flexibility and usability for our employees and our customers, as well as for stronger security of the organization across all layers (from infrastructure to application).
- Bringing decentralized security and networking functions into one security platform (SASE)
- Ensuring the confidentiality and integrity of information, data and configurations in decentralized (hybrid) environments.
- How do we increase transparency and control of access to our assets and data in hybrid (multicloud) environments?
- Integration and securing of IoT and OT (Operational Technology) components.

Threat detection & automated operations

How do we detect threats and attacks faster and more efficiently? How do we automate the relevant processes?

Examples

- Solutions with new, alternative approaches of detecting threats, such as searching for "known good" links, deception technologies or code similarity.
- How do we increase the value of security data and the degree of automation with the use of AI/ML in the context of security analytics? (System Behavior Analytics, User Behavior Analytics etc.).
- Solutions with an AI/ML based approach instead of a rule-based approach for detection and prevention of data leakage in hybrid environments.
- Solutions and approaches for automation of security operations (tools and processes).
- Solutions for automatic detection of exploitable vulnerabilities.

Humans dealing with security risks

How do we enable people to act in a secure way, how do we support them in dealing with security risks, so that they handle their resources in an attentive and responsible manner, anchoring such positive behavior in their daily routines?

Examples

- New approaches to increase security awareness and promote secure behavior (innovative awareness approaches and training methods). Increased effectiveness of training measures.
- Targeted development of security know-how to address the security knowledge and workforce gap (innovative training methods for security professionals).
- Support people with contextual information to better detect and respond to cyber-attacks such as social engineering, phishing or vulnerabilities in ICT.
- Increase and improve the measurability and view of security posture to reduce complexity and facilitate decision making.