Swisscom StartUp Challenge 2021 – Security

Die drei grössten Herausforderungen von Swisscom im Cyber Security Umfeld

1. Dezentralisierte Security

Schutz unserer Kunden Assets in der immer stärker dezentralisierten Welt, in der der Perimeter Schutz nicht mehr reicht.

Beispiele

- Etablierung vom Zero Trust Ansatz für mehr Flexibilität und Usability für Mitarbeitende und Kunden sowie für höhere Sicherheit für Unternehmen auf allen Ebenen (Infrastruktur bis Applikation)
- Bündelung dezentraler Security und Networking Funktionen zu einer Sicherheitsplattform (SASE)
- Sicherstellung der Vertraulichkeit und Integrität von Informationen, Daten und Konfigurationen in dezentralen (hybriden) Umgebungen.
- Wie erhöhen wir die Transparenz und Kontrolle vom Zugriff auf unsere Assets und Daten in hybriden (Multicloud) Umgebungen?
- Einbindung und Absicherung von IoT und OT (Operational Technology) Komponenten.

2. Detektion von Bedrohungen & automatisierte Vorgänge

Wie detektieren wir die Bedrohungen und die Angriffe schneller und effizienter? Wie automatisieren die relevanten Vorgänge?

Beispiele

- Lösungen mit neuen, alternativen Ansätzen zum Erkennen von Bedrohungen, wie z.B. Suche nach «Known Good» Link, Deception Technologien oder Code Similarity.
- Wie erhöhen wir den Wert der Security Daten und Automatisierungsgrad mit Einsatz von AI/ML in Rahmen von Security Analytics? (System Behaviour Analytics, User Behaviour Analytics und Co.)
- Lösungen mit AI/ML based Ansatz statt rule based Ansatz für Erkennung und Verhinderung vom Datenabfluss in Hybriden Umgebungen.
- Lösungen und Ansätze für Automatisierung von Security Operations (Tools und Prozesse)
- Automatische Erkennungslösungen für ausnutzbare Schwachstellen

3. Mensch im Umgang mit Security Risiken

Wie befähigen wir Menschen sicher zu agieren, sie im Umgang mit Security Risken zu stärken, dass sie achtsam und verantwortungsvoll mit ihren Ressourcen umgehen und in ihrem Alltag positiv verankern?

Beispiele

- Neue Ansätze, um Security Awareness zu erhöhen und sicheres Verhalten zu fördern (Innovative Awareness Ansätze und Trainingsmethoden). Wirksamkeit der Schulungsmassnahmen erhöhen.
- Gezielte Aufbau von Security Know-How um Security Knowledge und Workforce Gap zu adressieren (Innovative Training Methoden für Security Professionals).
- Menschen mit Kontextinformationen unterstützen, Cyber Angriffe wie Social Engineering, Phishing oder Verwundbarkeiten von ICT besser zu erkennen und darauf entsprechend zu reagieren?
- Messbarkeit und Darstellung von Security-Posture erhöhen und verbessern, um Komplexität zu reduzieren und Decision Making zu erleichtern.