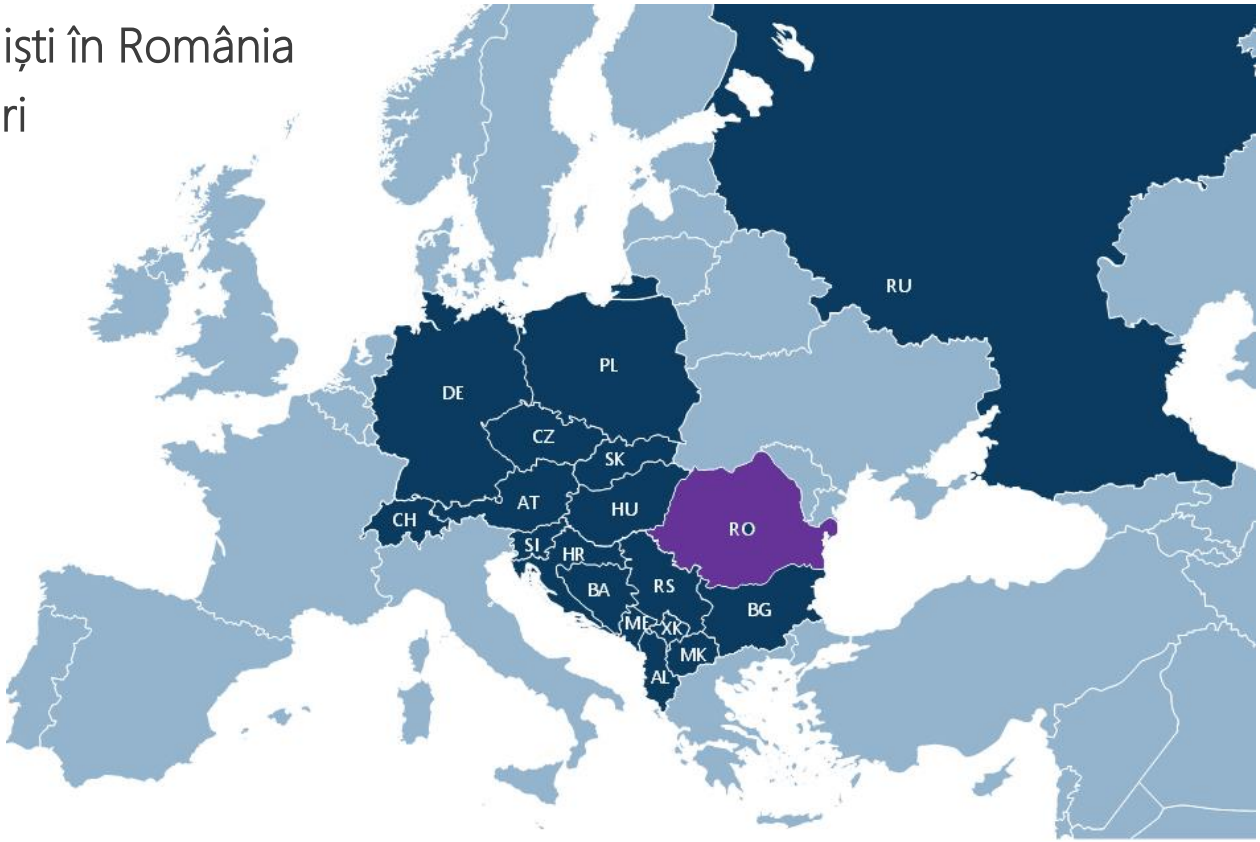
TAPIR - Threat Analysis and Proactive Incident Response

Bogdan Matache
Consultant Cyber Security

2016

Compania S&T AG

- Companie listată la Bursa Prime Standard din Germania
- 22 ani de prezență pe piața din România
- 46 mil Euro cifra de afaceri în 2015 în România
- Peste 180 specialiști în România
- Prezență în 19 tari



Echipa

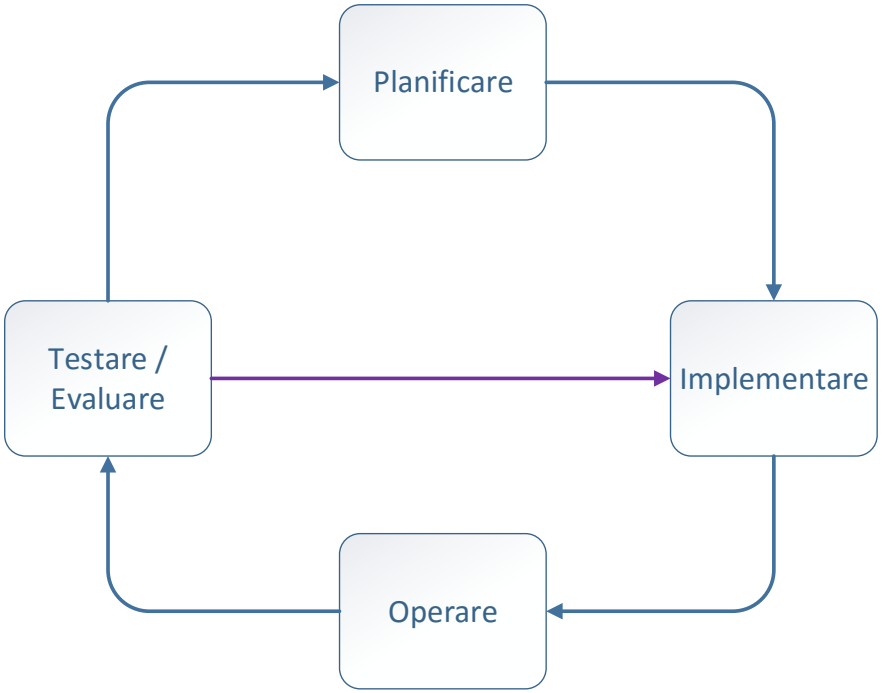
- Dedicată pentru Cyber Security

- Competențele echipei:

- CEH,
- CISSP,
- CISA, CISM,
- CRISC,
- CGEIT, GREM, GWAPT,
- OSINT,
- SCADA Security,
- OSCP,
- Certified Fraud Examiner, etc.

Servicii de securitate a informației

- sisteme informatice sigure cu costuri de operare optime
- acoperă întregul ciclu de viață al securității informației



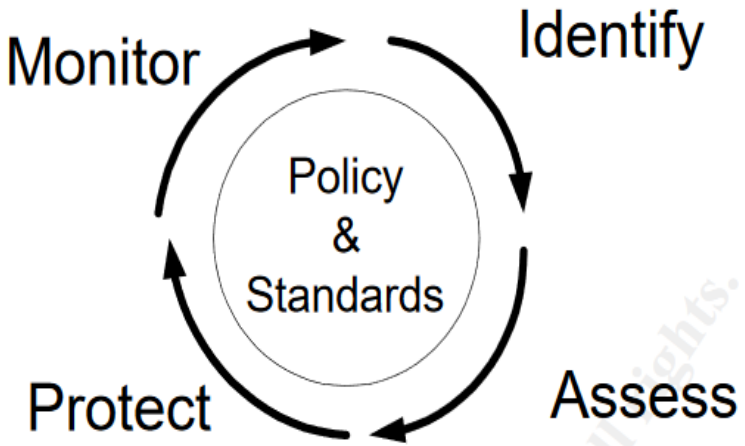


Figure 1: Security Lifecycle

Focus pe următoarele verticale

- FinTech, HealthCare, Telecom, ENR, Government

În acord cu:

- **proiectul de lege privind securitatea informatiei:** Legea privid Securitatea Cibernetica a Romaniei din 04.04.2016
- HG 245/2015 Strategia Nationala privind Agenda Digitala care are pilonul Securitate Cibernetica
- **directiva UE – Privacy Data Protection privind Protectia datelor cu caracter personal** Regulamentul EU 2016/679 si Directiva EU 2016/680
- **directiva UE – NIS** Network and Information Security, Published on 16/03/2015

Servicii de securitate a informației

- Testare, evaluare, planificare, implementare, operare

- Osint (culegere de date), Teste de penetrare, vulnerability assessment, analiză forensic in urma incidentelor de Securitate, analiză Malware, analiză cod sursă

- Integritate, confidențialitate, disponibilitate tratate in mod diferit în funcție de specificul beneficiarului

ex: teste de penetrare non-invazive pentru sistemele SCADA

sau

teste de penetrare pentru sistemele de plată de pe terminalele mobile

etc.

Soluția
TAPIR powered by ENERSEC

suntem

Managed Security Service Provider - MSSP

construim și operăm

Security Operations Center – SOC

avem

Cyber Emergency Response Team – S&T CERT

*Puteți externaliza către noi serviciile de Securitate IT

Soluția
TAPIR powered by ENERSEC

Threat Analysis and Proactive Incident Response

- Colectare de Log-uri, Colector Smart (Source Agnostic)
  - **Integrare cu SCADA, ICS, SmartCity, Smart Metering, SmartGrid, IoT**
- Analiză ultrarapidă, de ordinul secundelor pentru TB de date
- Retentie distribuita de Log-uri (in cloud privat dar si hybrid sau public)

- Sistem Dimensionat la peste 1.000.000 EPS / 2mil IOps
- Scalabilitate infinita folosind orchestrarea resurselor din Cloud

Soluția
TAPIR powered by ENERSEC

Folosim Tehnologii Avansate

- Machine Learning pentru fluxurile de date în mișcare (colaborare cu universitate)
- Ticketing generat de AI – Artificial Intelligence
- Analiza big data pentru depistarea comportamentului deviant (cu universitate)

- Crawlere pentru DarkWeb (date din deepweb)
- Retea de HoneyPots cu posibilitatea de integrare in IoT – Internet of Things

Mulțumesc pentru atenție !

Bogdan Matache
Consultant Cyber Security

2016