Threat Intelligence in a SECRET Environment

Martin Ebner

SIGS 15 05 24

SIGS Roundtables / Talks

Fortress of Insane

12 Layer Model

Fortress of Insane

- Roundtable SIGS – need for TI and RM
  - We are constructing „ICT-Sec fortresses“ on weak standards
  - What guards are doing – the only look to inner side

- **Need for TI (Threat Intel) and a flexible RM (RiscManagement)**

12 Layer Model (Talk at SIGS)

- need for new layers and approaches
- tactical / operational / strategic
  - 7 OSI + 5 Layers
    - real world
    - 7 OSI
    - user
    - social
    - political
    - culture and religion

Stakes

- Tactical (SOC)
- Operative (S) Staff
- Strategic (J) Joint Staff

Information on tactical level

- IOC‘s
- TTP‘s
- Malwarecode
- Targeted Systems / Assets
- …

Information on operative level

- targeted systems / assets (Impact)
  - information for re-operation
- impact on systems and business
  - containment
  - re-operation
  - …

Information on strategic level

- extend of demage
- impact on current strategies and operations
- ways to limit demages
- deterrence strategies
- development of future strategies
- ---

TI Threat Intelligence and SECRET?

Expl.: ongoing Investigation (loss of data / changed data / system loss)

Would you classify or not?

PROCESS:	OUTPUT:	
• Process 1 – collection of data / information	information on problem	<> TIt
• Process 2 – interpretation	impact in systems	<> TIt
• Process 3 – stabilisation	first respond	<> TIo
• Process 4 – reaction	closing gaps and change	<> TIo
• Process 5 – re-operation / future operation	ops, sys and sensors	<> TIs

TI ?

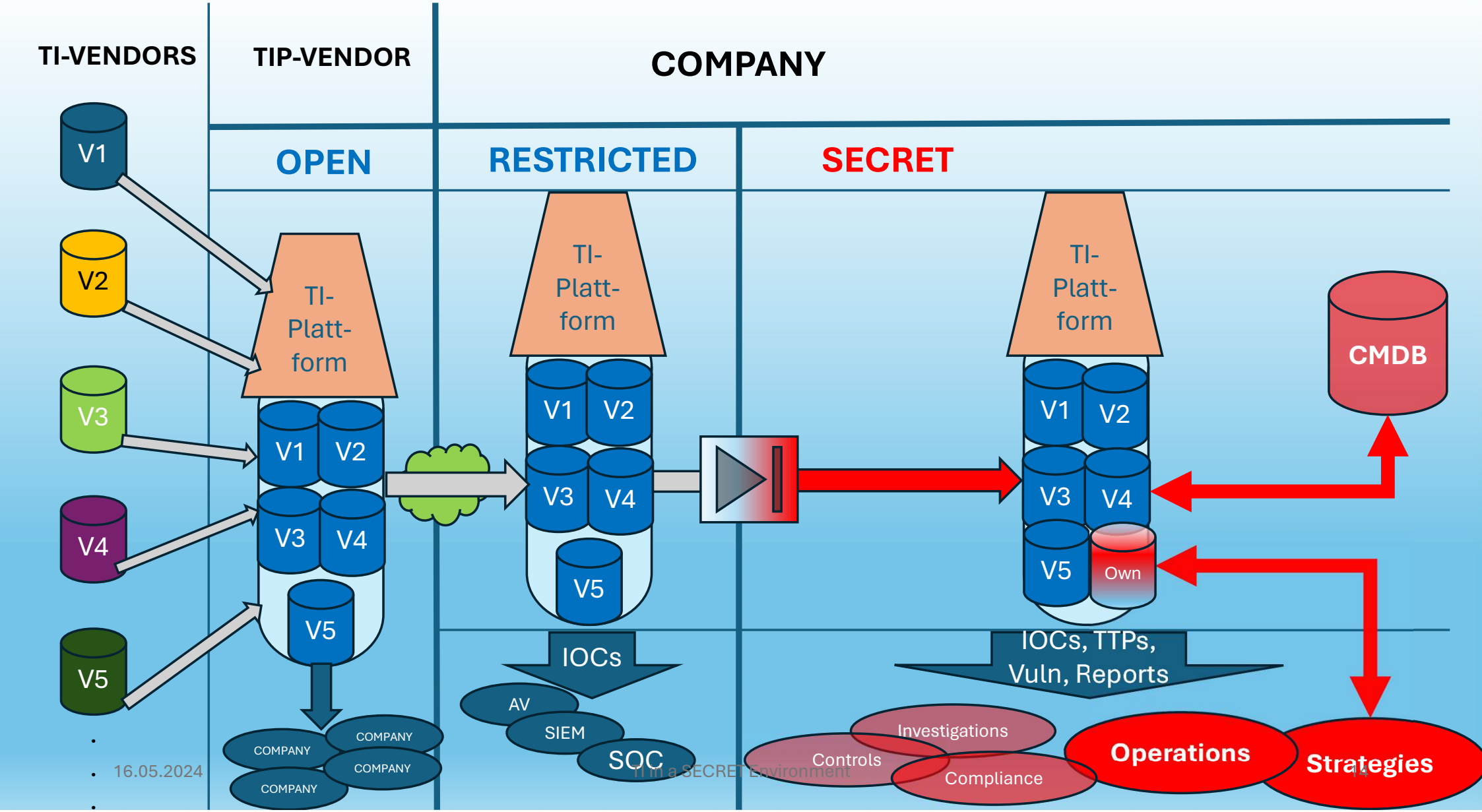
- how?
- **what do we await on these levels?**
  - Tactical TIt
  - Operational TIo
  - Strategic TIs
- which vendor/s?
- **Cloud or not Cloud based? Cloud based is against secrecy! (NATO / EU Std)**

Our way – the TIP

- TIP Threat Intel Platform – the model
- Vendor DB – more than one?
  - **differencies** in vendor databases t/o/s
  - **normalize** the DB
- Plattform on Top
  - Tac IOCs
  - Op impact
  - Strat approach

Construction

- **Trusted Partner (AUT)**
- **Plattform Vendor** – selection – cooperation
- **TI Vendors** – selection – the best on the market – flexible
- **Classification**
  - BMLV tactical level – max RESTRICTED
  - BMLV operational level – up to SECRET
  - BMLV strategic level – SECRET


TI-VENDORS
TIP-VENDOR
COMPANY
OPEN
RESTRICTED
SECRET
V1
V2
V3
V4
V5
TI-Platt-form
TI-Platt-form
TI-Platt-form
V1
V2
V3
V4
V5
V1
V2
V3
V4
V5
CMDB
Own
COMPANY
COMPANY
COMPANY
COMPANY
IOCs
AV
SIEM
SOC
IOCs, TTPs, Vuln, Reports
Investigations
Controls
Compliance
Operations
Strategies

Questions? / Discussion

Thank You