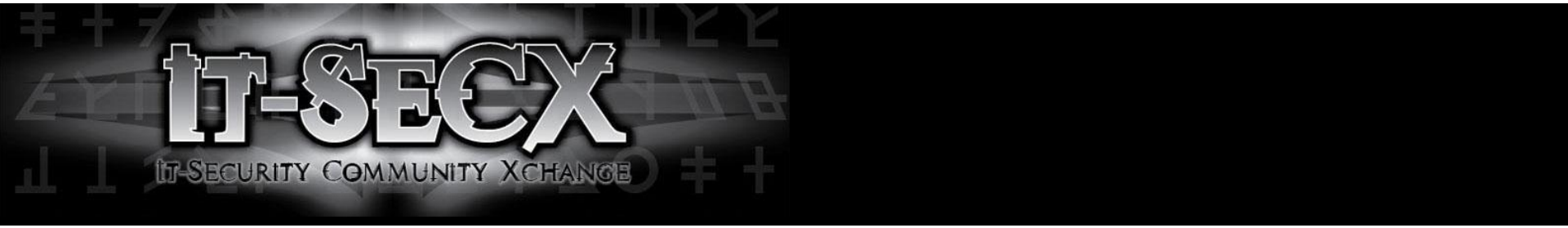
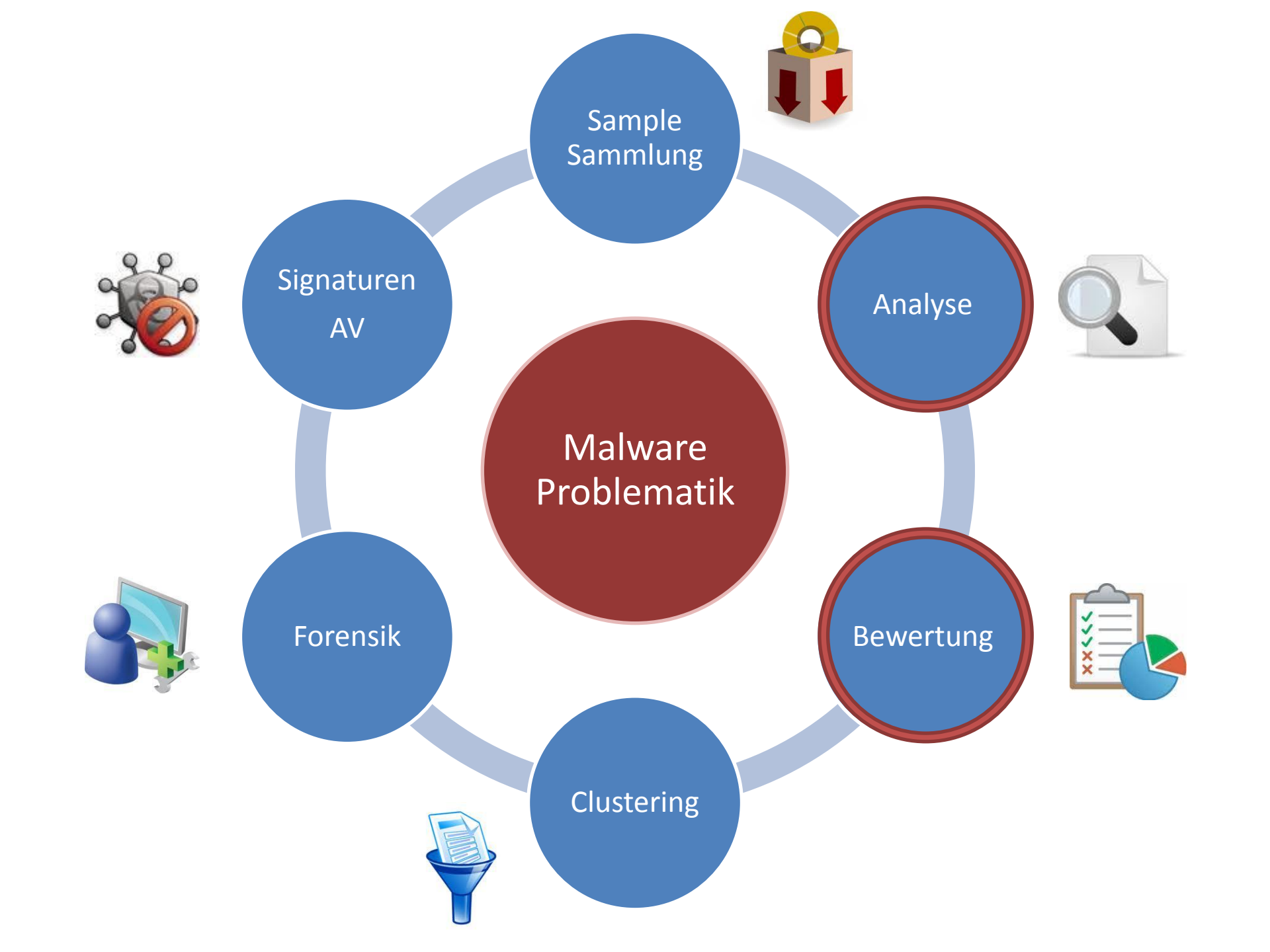


Bewertung von verdächtigem Code

Malware • Analyse • Bewertung

Robert Luh
IT Security Jahrgang 2008

Paul Tavolato
Projektbetreuer, FH St.Pölten


Sample Sammlung
Analyse
Bewertung
Clustering
Forensik
Signaturen AV
Malware Problematik

Analyse

Statische Analyse

- Keine Ausführung des Codes
- Disassembly/Decompilation
- Ungenau, aufwändig

Dynamische Analyse

- Ausführung des Codes
- Debugger
- Emulatoren
- Netzwerk Sniffer

Virtual Machine	Emulation
Hardware Virtualisierung	+ CPU Emulation
	Architekturunabhängigkeit 
Kann von Malware erkannt werden	

Dynamische Analyse: Anubis

Anubis (Ikarus/iSecLab/securityresearch.at)

Windows PE32 Verhaltens-Analyse

- QEMU (Prozessor Emulator)
- PEiD – PE Signaturerkennung
  - Packer
  - Crypto Verfahren
  - Compiler
- BRO (Network Intrusion Detection)

Anubis: Funktionsweise

Analyseverfahren

- PE32 Datei an Anubis Script in Emulator übergeben (Auto/Interaktiv)
- Ausführung als sample.exe in QEMU (WinXP SP2)
- Analyse der Aktivität




- System/API Calls
- Dateisystem
- Registry
- Netzwerk

- Logging, Vorauswertung

→ langsam…

Output und Bewertung

XML Report

- Aktivitäten
- Vorabanalyse
  - Autostart
  - Internet Settings
  - AV Killer
  - …

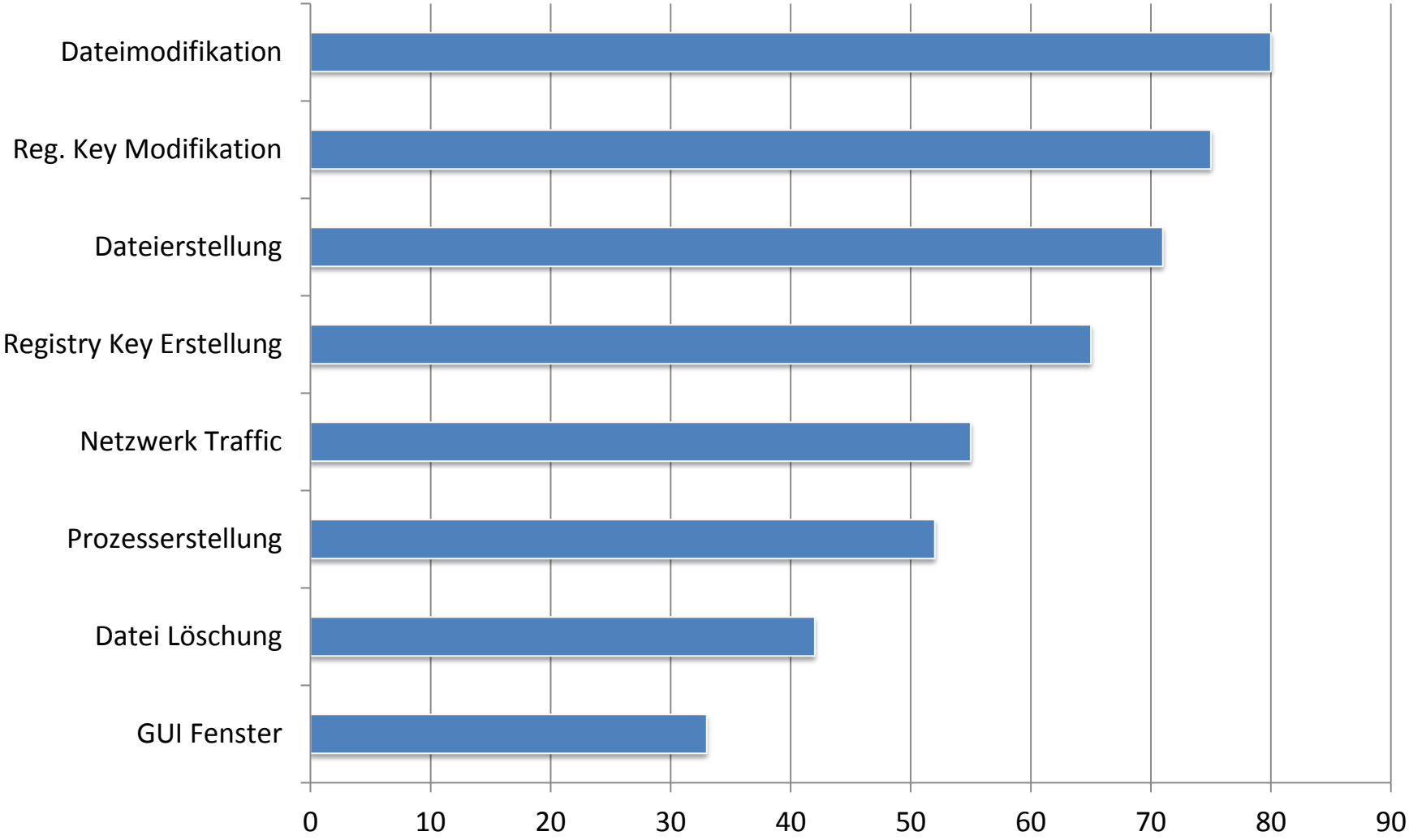
```
<file_activities>
<file_created name="C:\WINDOWS\dxxdv34567.bat"/>
<file_created name="C:\WINDOWS\fdgg34353edfgdfdf"/>
<file_created name="c:\windows\pp12.exe"/>
…
<analysis_reason>Started by sample.exe</analysis_reason>
<virtual_fn>pp12.exe</virtual_fn>
<virtual_path>c:\windows\pp12.exe</virtual_path>
<arguments>c:\windows\pp12.exe C:\sample.exe</arguments>
<status>alive</status>
```

Parsing und Auswertung – Score

- Aktivität
  - Was, wie oft, wie heikel?
- Simple Zusammenhänge
  - z.B.: Erstellte Datei wird später ausgeführt

Statistik

A View on Current Malware Behaviours (2009, TUWien/Eurecom/UC Santa Barbara)



Ergebnisse

Malware vs. Unbedenkliche Anwendungen

Threat Ranges: 0-32 (low), 33-65 (med), 66-99 (high), 100+ (very high)

1143 Samples

70 Punkte

<X>

71 Samples

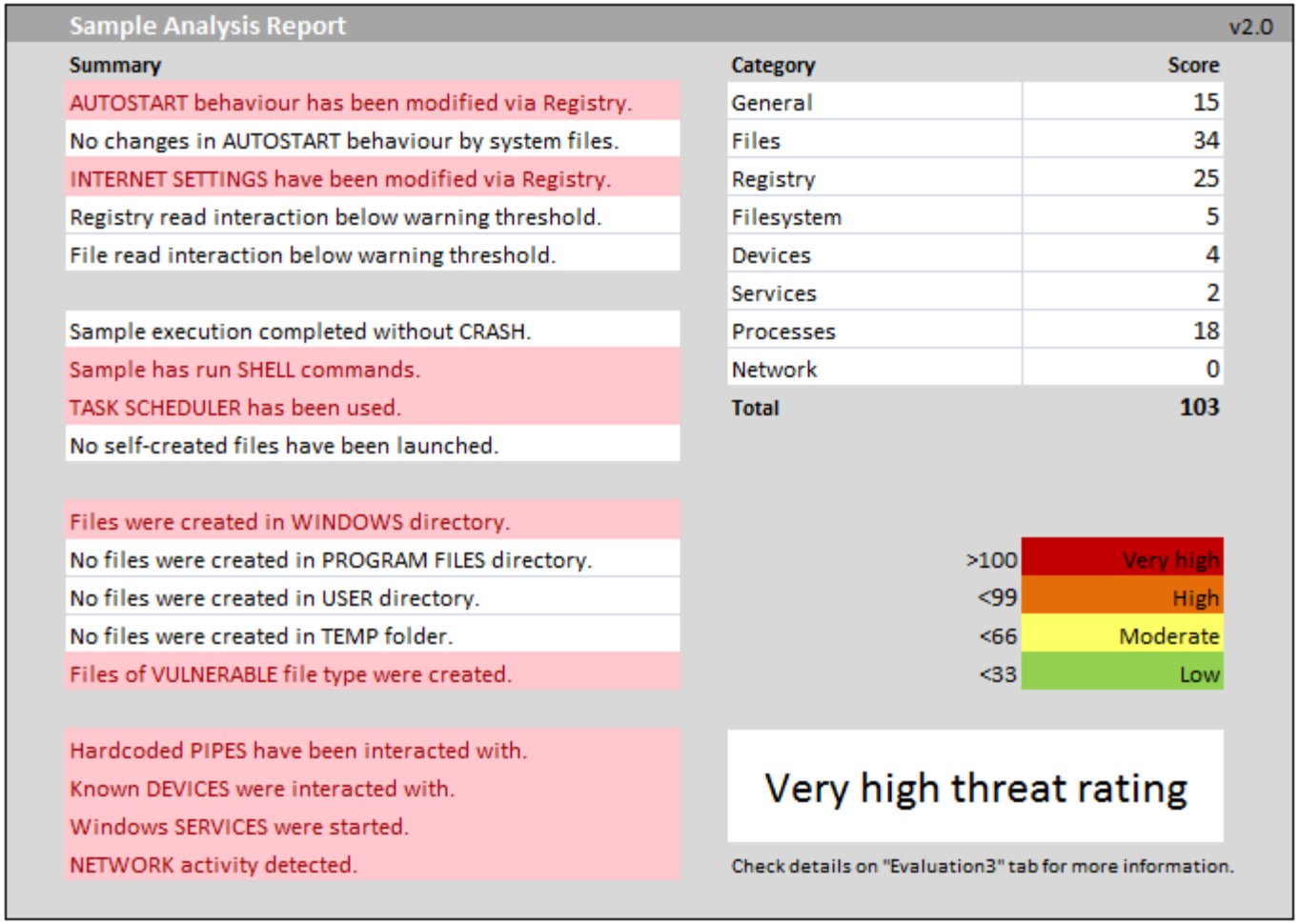
18 Punkte

Problematik

- Ausreißer
- Viren erkennen Emulation
- Inkompatibles OS
- Setup Routinen → viel Systemaktivität

Beispiel

W32.AutoIT



Sample Analysis Report v2.0

Summary
AUTOSTART behaviour has been modified via Registry.
No changes in AUTOSTART behaviour by system files.
INTERNET SETTINGS have been modified via Registry.
Registry read interaction below warning threshold.
File read interaction below warning threshold.
Sample execution completed without CRASH.
Sample has run SHELL commands.
TASK SCHEDULER has been used.
No self-created files have been launched.
Files were created in WINDOWS directory.
No files were created in PROGRAM FILES directory.
No files were created in USER directory.
No files were created in TEMP folder.
Files of VULNERABLE file type were created.
Hardcoded PIPES have been interacted with.
Known DEVICES were interacted with.
Windows SERVICES were started.
NETWORK activity detected.

Category	Score
General	15
Files	34
Registry	25
Filesystem	5
Devices	4
Services	2
Processes	18
Network	0
Total	**103**

>100	Very high
<99	High
<66	Moderate
<33	Low

Very high threat rating

Check details on "Evaluation3" tab for more information.

Zukunft des Projekts

Bewertung von Samples

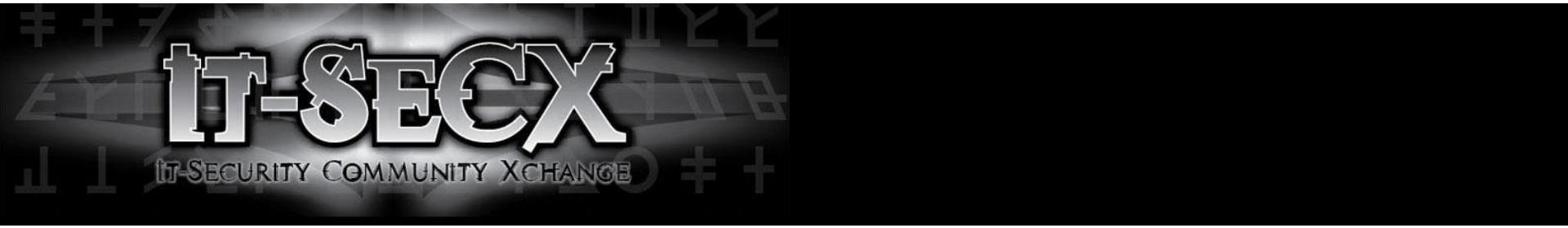
- Komplexere Zusammenhänge
- Reduzierte Abhängigkeit von Quantität
- Mehr Samples (auch non-Malware)

Clustering in Familien

Analyse-System

- Weitere Betriebssysteme (Win, Ux-based)
- Performantere Analyseplattform – Anubis Ersatz

Start: Sommersemester 2011



Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Upload eigener Samples an Anubis:
http://anubis.iseclab.org