TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Berlin, 13.06.2019

Standardisierung von Angriffsinformationen

Thomas Hemker, CISSP, CISM, CISA
Director Security Strategy, EMEA CTO Office
Symantec (Deutschland) GmbH

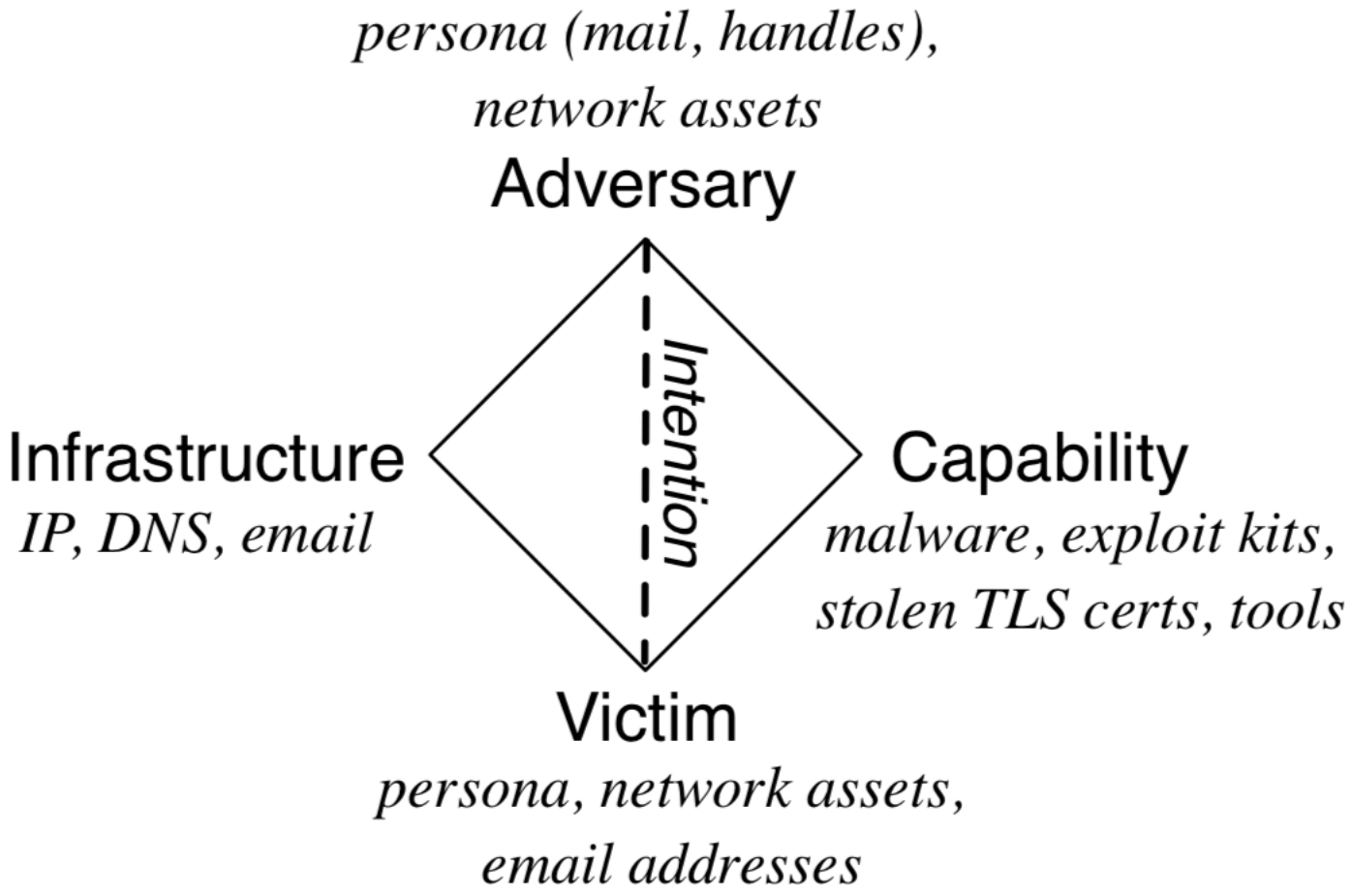
Cyber Threat Intelligence

„The purpose of threat intelligence is to understand the enemy, help anticipate future actions and plan a response“

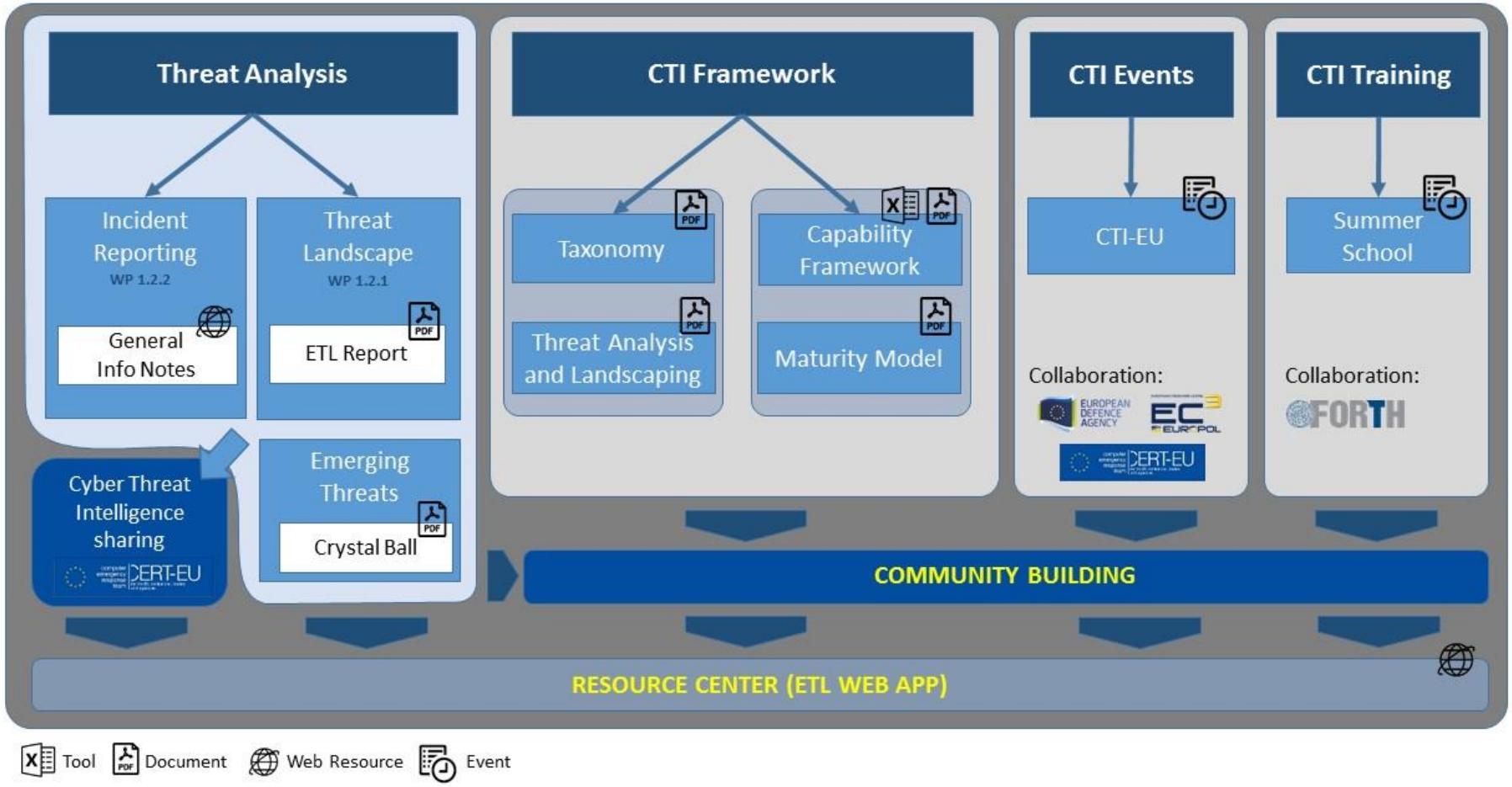
Christian Doerr, TU Delft CTI Lab https://www.cyber-threat-intelligence.com/

Den Angreifer verstehen

- Attack Kill Chain
  - Reconaissance
  - ....
  - Actions
- Diamond Model
  - Intrusions
  - Series of Events
  - Connections
  - Active Threats
  - Common elements

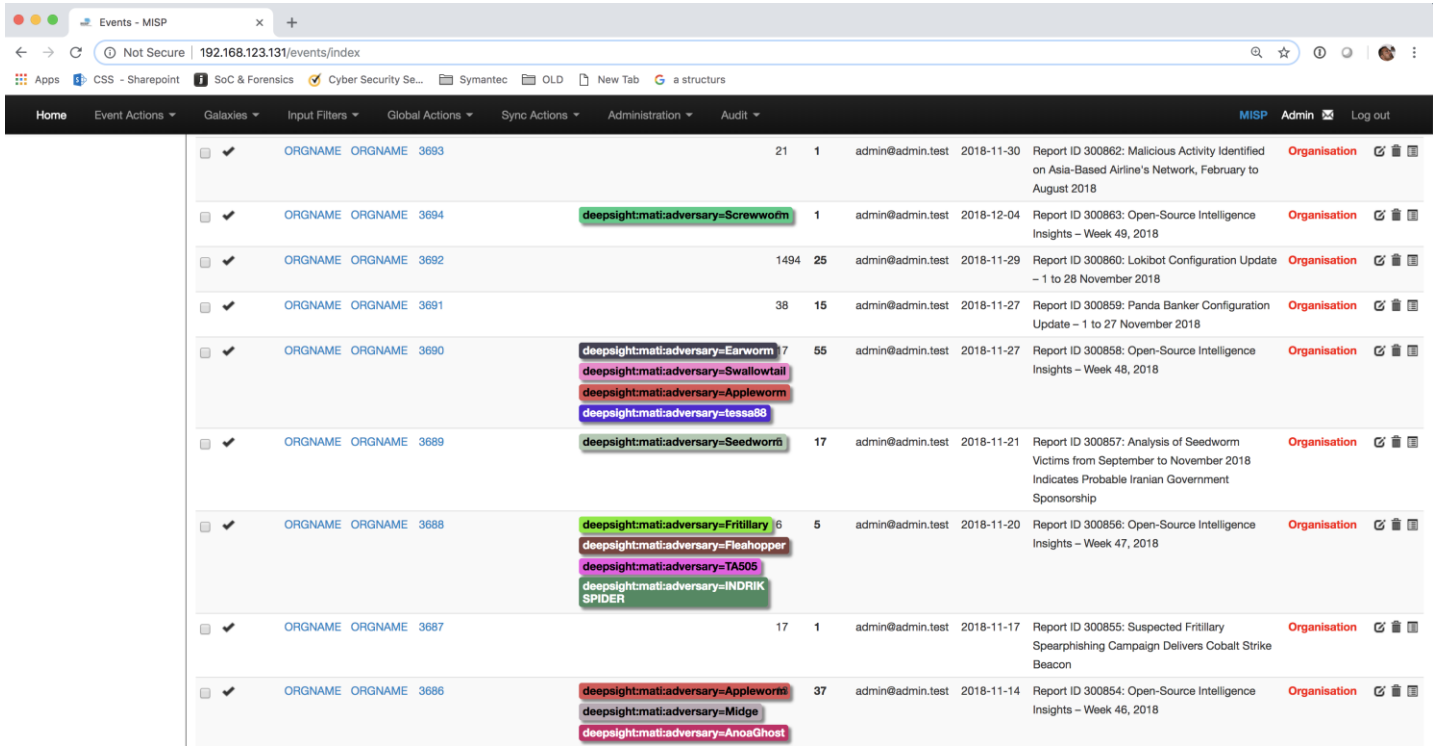


ENISA CTI Modules



Interaktion und Standards – Quellen

- Open Data Sources /OSINT
  - OASIS Stix Taxii (JSON), IODEF
- Kommerzielle Feeds
  - E.g. Symantec Deepsight (xml, etc.)
  - REST-API, Portals,
- Shared Intelligence
  - MISP
  - CERT Verbund etc.
- Asset Information
  - Internal standards?



Interaktion und Standards – Detection/Response

- Quality Standards
  - Education &Training, Decision making support, Security Policy adjustments, resource allocation, security by design
- Threat Modelling, Ontologien
  - Administrators, CSIRTS, CERT,
  - OWASP, TARA, VERIS
- Detektion Formate
  - SIEM/SOC/Incident Response
  - Pentesting, Forensics
  - Snort, Bro, YARA, (Security Analytics)
  - Modelling Adversarial Behaviour MITRE Att&ck

MITRE Att&ck

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted	Exploitation for	Bootkit	Exploitation for	Component Firmware	Hooking	Peripheral Device	Remote File	Email	Scheduled	Fallback Channels

Weiteres Vorgehen?

- Stand der Technik
- Best Practice
- Austausch
- Plattform – Brokerage
- Vernetzung
- Adaption
- ?