Cyber Analysis & Defense

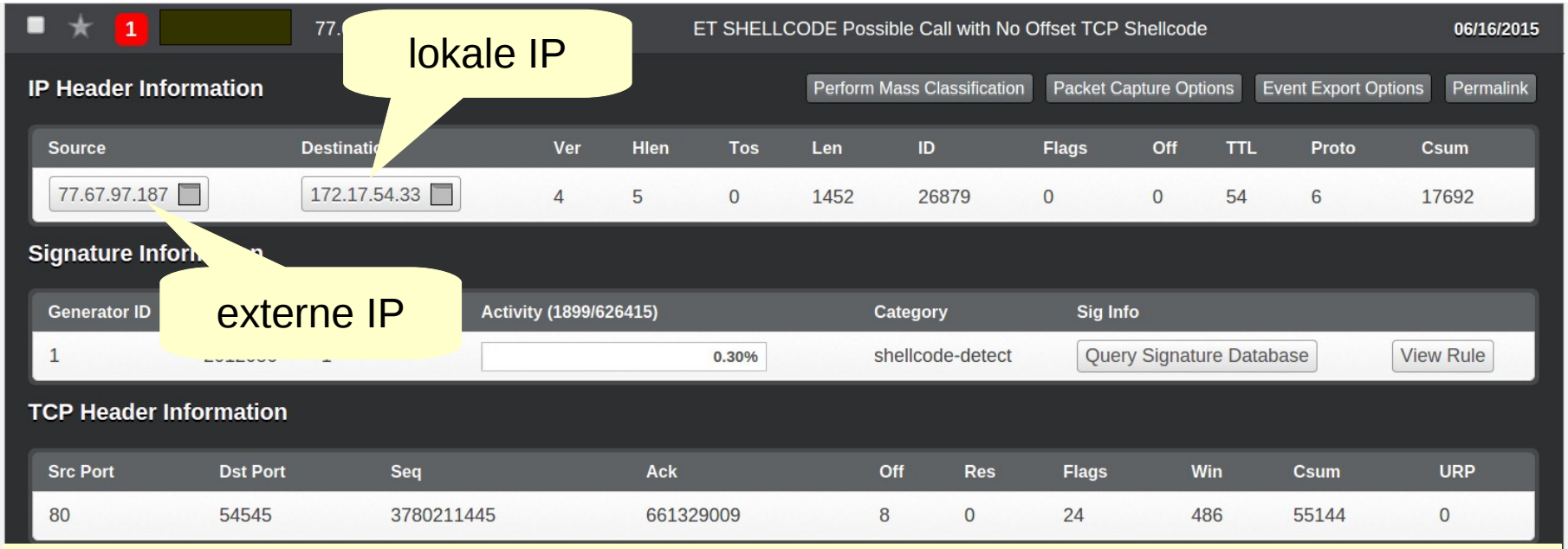
A graph model for incident analysis

Christian Kollee (christian.kollee@fkie.fraunhofer.de)

Vorfallsanalyse

Graphmodell

Herausforderungen und Ausblick



alert tcp $EXTERNAL_NET any -> $HOME_NET any (
msg:"ET SHELLCODE Possible Call with No Offset TCP Shellcode";
flow:established;
content:"|E8 00 00 00 00 58|";
fast_pattern:only;
reference:url,www.networkforensics.com/2010/05/16/network-detection-of-x86-buffer-overflow-shellcode/;
classtype:shellcode-detect;
sid:2012086;
rev:1;)

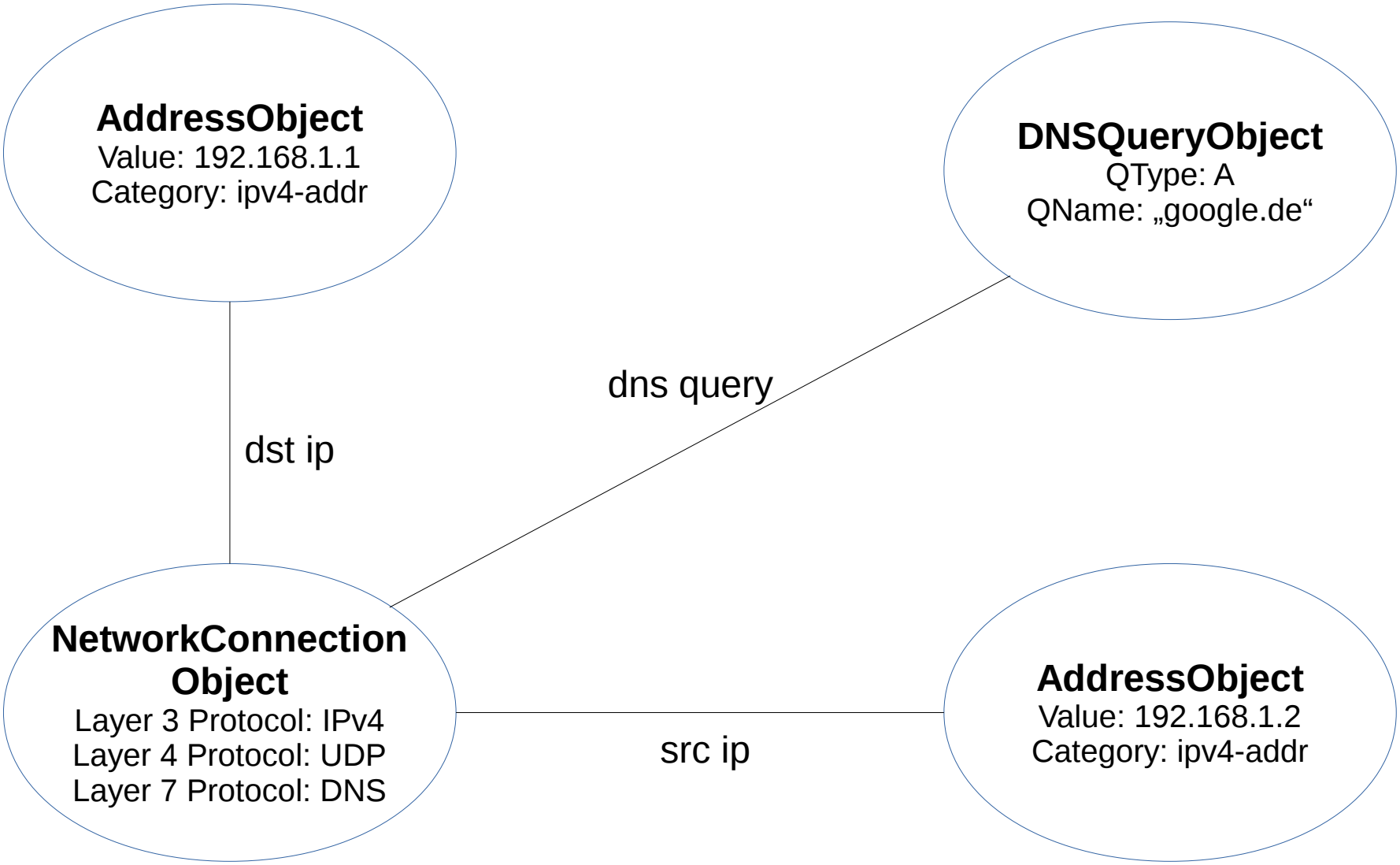
Unterstützung des Analysten

- Analyst benötigt unterschiedliche Informationsquelle
  - Host-Informationen
  - DNS
  - HTTP Session
- Darstellung der Beziehungen zwischen den Informationen

Cyber Observable Expression (CybOX™)

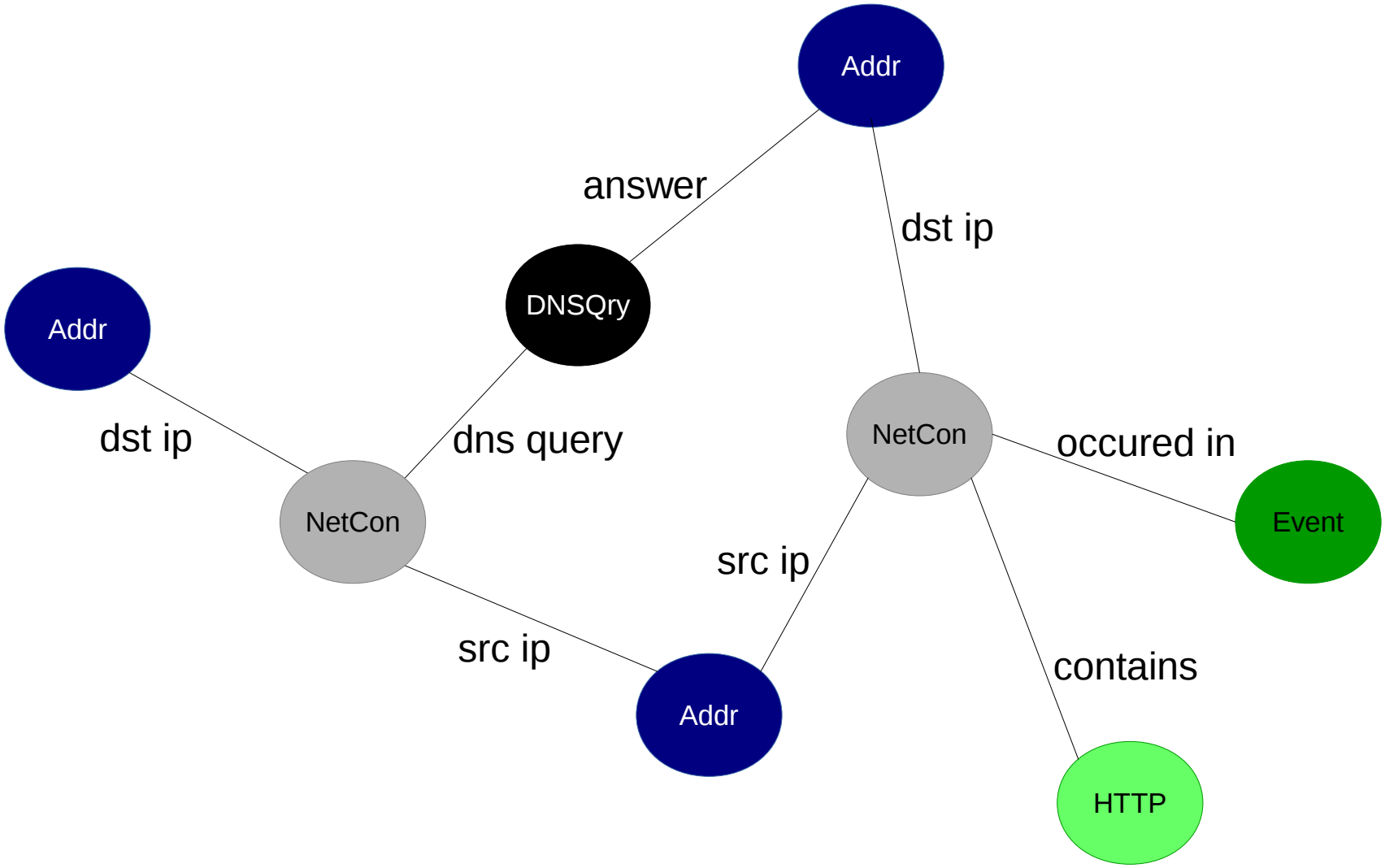
MITRE

```
<?xml version='1.0' encoding='UTF-8'?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2" xmlns:cyboxCommon="http://cybox.mitre.org/common
    <xs:annotation>
        <xs:documentation>This schema was originally developed by The MITRE Corporation. The CybOX XML Schema implementation is maintained by The MITRE Corporati
        <xs:appinfo>
            <schema>Link_Object</schema>
            <version>1.1</version>
            <date>01/22/2014</date>
            <short_description>The following specifies the fields and types that compose this defined CybOX Object type. Each defined object is an extension of t
            <terms_of_use>Copyright (c) 2012-2014, The MITRE Corporation. All rights reserved. The contents of this file are subject to the terms of the CybOX Li
        </xs:appinfo>
    </xs:annotation>
    <xs:import namespace="http://cybox.mitre.org/objects#URIObject-2" schemaLocation="URI_Object.xsd"/>
    <xs:import namespace="http://cybox.mitre.org/common-2" schemaLocation="../cybox_common.xsd"/>
    <xs:element name="Link" type="LinkObj:LinkObjectType">
        <xs:annotation>
            <xs:documentation>The Link Object is intended to characterize links, such as those on a webpage or in an e-mail message.</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:complexType name="LinkObjectType">
        <xs:annotation>
            <xs:documentation>The Link Object is intended to characterize links, such as those on a webpage or in an e-mail message.</xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="URIObj:URIObjectType">
                <xs:sequence>
                    <xs:element name="URL_Label" type="cyboxCommon:StringObjectPropertyType" minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>The URL_Label field specifies the label of the link.</xs:documentation>
                        </xs:annotation>
                    </xs:element>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
</xs:schema>
```



Vorgehen

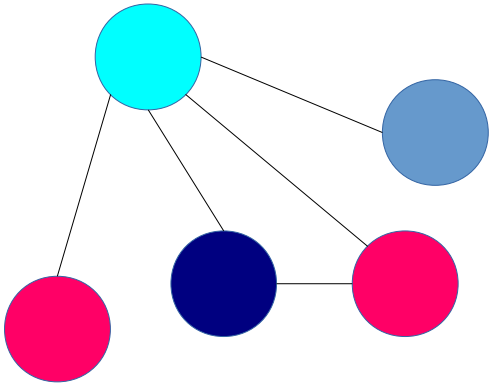
- Auswahl der benötigten CybOX-Objekte
- ausgewählte CybOX-Objekte und deren Beziehungen in einer Datenbank erfassen
- zusätzliche Custom-Objekte, z. B. „Snort Event“
- ermöglicht es einem Analysten sich „durchzuhangeln“



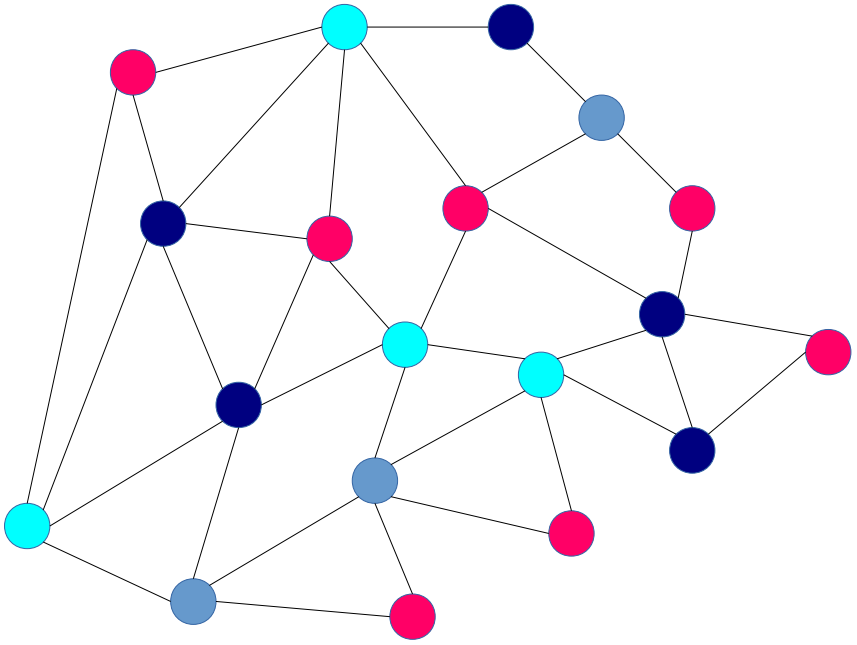
Indicators of Compromise

Atomar	Computed	Behavioral
„badfile.pdf“	md5sum badfile.pdf	(A1, A2, C1)
eddie@evil.com	pcre:"/forum=.*'/"	(B1, A3, C2)
192.168.13.12	count(failedLogins)	

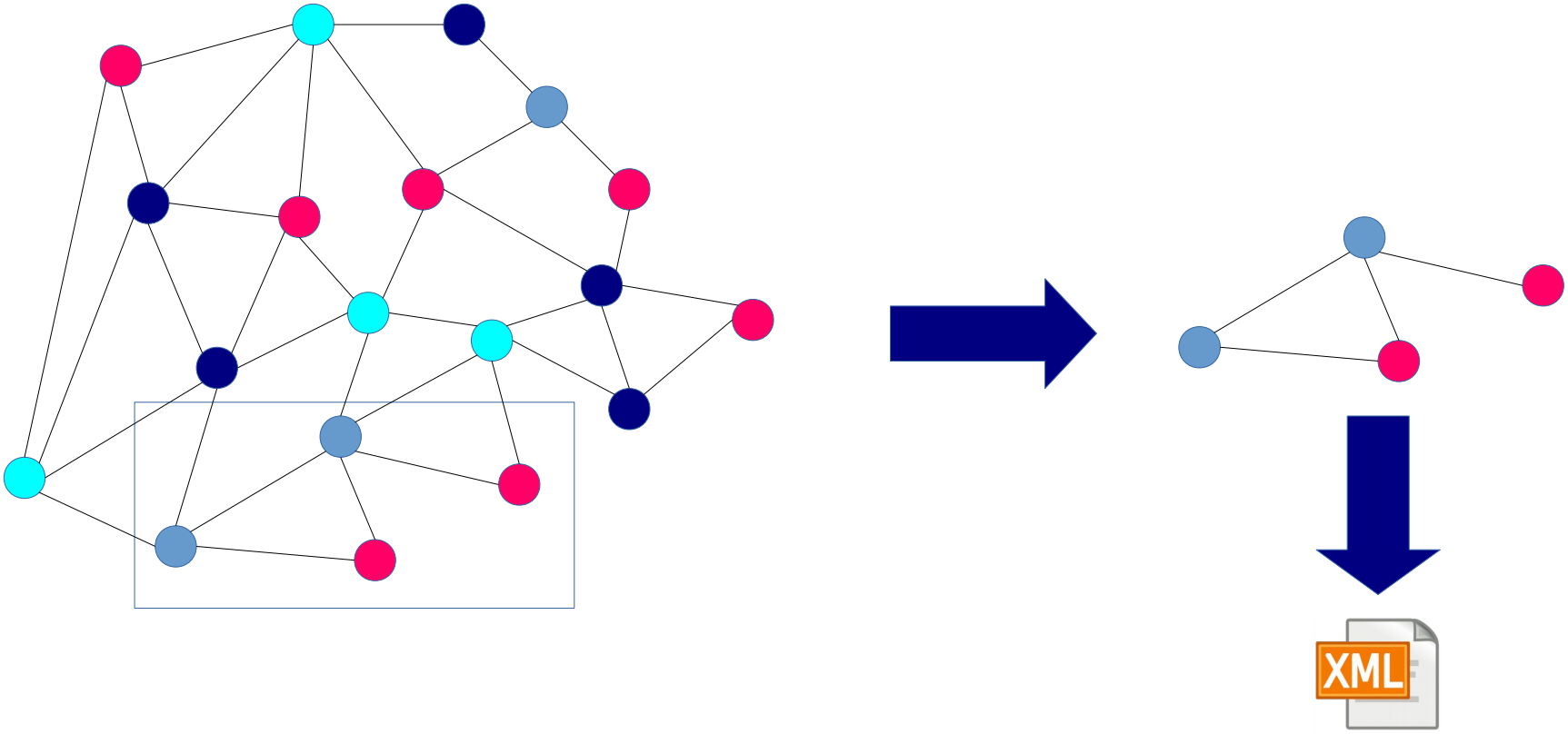
Sanders, Applied Network Security Monitoring, S.151ff



Darstellung eines IOC als (Teil-)Graph



Ist der IOC-Graph enthalten?



Herausforderungen

- Auswahl der CybOX-Objekte und geeignete Abstraktion
- Datenmengen
- Zeitliche Beziehungen
- Anbindung der benötigten Datenquellen

Weiteres Vorgehen

- Erweiterung um Host-basierte Objekte
- Weitere Custom-Objekte (z. B. Reputation, Reports)
- Prototypische Implementierung
- Erprobung im CERT-Umfeld

- Datenschutz- und Privatsphäre
- Weitere Möglichkeiten zur Unterstützung des Analysten

Zusammenfassung

- Analysten benötigen Informationen aus unterschiedlichen Quellen
- Graphmodell ermöglicht es Beziehungen zwischen den Informationen zu verdeutlichen
- Verwendung von CybOX als Grundlage ermöglichen Im- und Export von IOCs