

SENSORNETZE

Technische Möglichkeiten, Rahmenbedingungen und Herausforderungen

Florian Skopik

Senior Scientist, AIT

florian.skopik@ait.ac.at

IKT Sicherheitskonferenz des AbWA

Villach, AT

27. Sept. 2017



ÜBERSICHT

1. Veränderte Motivationslage
2. Das KIRAS Projekt CISA
3. Erhebung von Daten mittels Sensorik und Ableitung von Informationen
4. Anwendung eines Sensornetzes: TOP-DOWN Ansatz
 1. Welche Aktionen bzw. Entscheidungen sollen abgeleitet werden?
 2. Welche Informationen müssen dafür dargestellt werden?
 3. Welche Daten müssen dafür gesammelt werden?
 4. Wie können geeignete Quellen bewertet werden?
 5. Welche Daten einer Organisation können mittels Sensorik nutzbar gemacht werden?
5. Visuelle Aufbereitung gesammelter Security-Informationen
6. Conclusio

1. VERÄNDERTE MOTIVATIONSLAGE

NIS RL, CSC, CDZ, Cyber-Sicherheitsgesetz, APTs ...



WARUM BRAUCHEN WIR SENSORNETZE?

- Ständig ändernde **Bedrohungslage**
 - APTs, DDoS mit hohen Bandbreiten, Ransomware
 - Immer mehr
 - Immer schneller
- Veränderte **Rahmenbedingungen**
 - Gesetzeslage: NIS RL, DSGVO, Cyber Security Gesetz
 - Neue Einrichtungen bei Behörden: CSC, CDZ
 - Neue Sektor-CERTs, z.B. E-CERT
 - Neue Pflichten (Meldepflicht der KIs, Audits, ...)
- Fundierte **Grundlage zur Entscheidungsfindung** notwendig!
 - Umgang mit Bedrohungen: Risikobewertung durch Trendanalysen
 - Umgang mit Incidents
 - Bewertung von Handlungsoptionen im konkreten Anlassfall

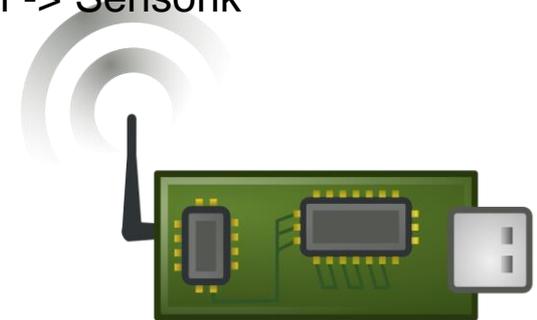
HERAUSFORDERUNGEN BEI DER DATENERHEBUNG

- Dünne Informationslage bei (Branchen-)CERTs bzw. nationalen Behörden, insbesondere zu Beginn einer Angriffswelle
 - WER ist **betroffen**?
 - Geschädigte melden sich spät oder gar nicht
 - Linderung soll hier die Meldepflicht nach NIS RL/Bundesgesetz schaffen; jedoch gilt diese nur für KIs
 - WER hat die **Situation im Griff**?
 - Beispiel Ransomware: Wer ist schon dabei Backups einzuspielen und wer überlegt noch, ob er nicht doch besser zahlen sollte?
- Im Großen und Ganzen ist daher **unbekannt, wie schwerwiegend ein Angriff** bzw. der **Verbreitungsgrad** bzw. der **Impact** ausserhalb der eigenen Organisation tatsächlich ist
- WannaCry: Diverse Aufrufe von CERT.at und CSC Geschädigte mögen sich melden bzw. Vorfälle zur Anzeige bringen.



MOTIVATION FÜR SENSORIK

- Die Forderung nach Sensorik und Automatisierung ist nicht neu, aber ...
- ... der Einsatz von Sensorik um diverse Daten (semi-)automatisiert zu erheben, ist im Detail sehr komplex und stark Anwendungsfallbezogen
- **Beispiel** des „IoC Sightings“
 - Ein IoC ist ein eindeutiges Datum, dass die Kompromittierung eines Systems mit einer spez. Malware verifiziert
 - z.B. Das Vorhandensein einer bestimmten Datei (Name, Hashsumme,...), eines bestimmten Prozesses, einer bestimmten Logzeile, eines Event Eintrags, ...
 - Einige Initiativen in anderen (europ.) Ländern versuchen die Präsenz dieser IoCs in KIs automatisiert zu ermitteln und zentral auszuwerten -> Sensorik
 - WER ist betroffen?
 - WANN/WO das erste mal aufgetaucht?
 - WIE schnell ausgebreitet?
 - Bei WEM bereits eingedämmt?
 - Interpretation der Daten herausfordernd (Kontext?)
 - **DATENSCHUTZ:** Schutz des Bürgers (Privacy) v.s. Schutz der Infrastruktur



WAS IST EIN SENSOR?

- Ein Sensor greift vorab konfigurierte Datentypen/-flüsse ab
 - WAS wird detektiert?
 - WO wird detektiert?
 - WIE wird detektiert?
 - WIE werden Daten weitergeleitet?
 - WARUM wird detektiert? (Beitrag zu Analysen auf höherer Ebene)
- Beispiel IoC Sighting „WannaCry“
 - WAS: SMB Traffic im NW; Strings & Payload auf HDD und virt. page
 - WO: zwischen Netzsegmenten (Firewalls) bzw. an allen pot. betr. Host
 - WIE: Netflows, DPI; Host Scan
 - Weiterleitung: verschlüsselt, teilanonymisiert
 - WARUM: Verbreitung der Malware abschätzen



https://www.us-cert.gov/sites/default/files/publications/TA17-132A_stix.xml

DAS KLEINE SENSOR 1X1 -- HERAUSFORDERUNGEN

- **WAS** wird detektiert
 - Anzahl an vorselektierten Daten + Auswertung
 - Darüber hinaus überwiegend Rohdaten für spätere Korrelation
- **WO** wird detektiert?
 - BYOD, end2end Verschlüsselung -> Perimeter existiert per se nicht
 - SDN, Virtualisierung/Containerisierung -> Host-basierte Erkennung
- **WIE** wird detektiert?
 - Skalierbarkeit, Performance, Datenschutz, Nachvollziehbarkeit ...
- **WIE** werden Daten **weitergeleitet**?
 - Sicherer Transfer & Verschlüsselung
 - Prioritäten
- **WARUM** wird detektiert?
 - Sinnvolle Anwendungsfälle mit Nutzen für alle Beteiligten
 - Ansonsten: keine Benutzerakzeptanz, Misstrauen, ...



2. DAS KIRAS-PROJEKT CISA

Cyber Incident Situational Awareness (2015 – 2018)



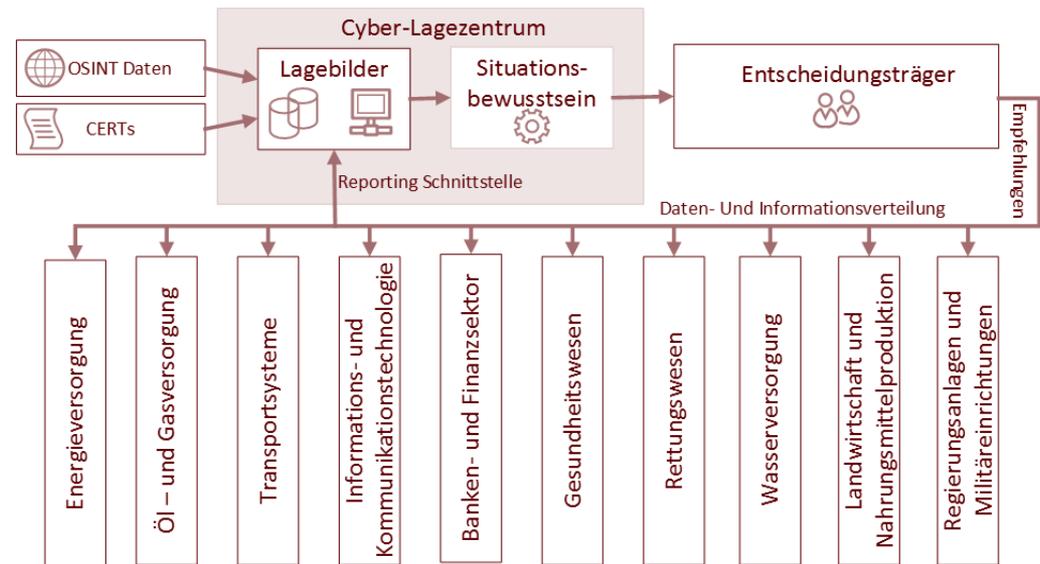


MISSION GOAL UND AKTUELLER STAND



- CISA ist keine „bottom up magic“!
 - **NICHT:** „Wir sammeln alle Daten, die technisch erhoben werden können und überlegen uns dann, wozu sie genutzt werden können“
 - **SONDERN:** TOP-DOWN Ansatz
 - Dazu später mehr!
- CISA Mission Goal:

Realisierung eines Cyber Lagebildkonzepts (insb. aber nicht ausschließlich auf nationaler Ebene), welches in Cyber Lagezentren zur Anwendung kommen soll.



http://www.kiras.at/gefoerderte-projekte/detail/?tx_ttnews%5Btt_news%5D=535&cHash=519847e6fc040eac8cb0a6af14a1f47b

3. ERHEBUNG VON DATEN MITTELS SENSORIK UND ABLEITUNG VON INFORMATIONEN

Einige Herausforderungen – Ergänzungen gerne willkommen!



CYBER LAGEBILDER



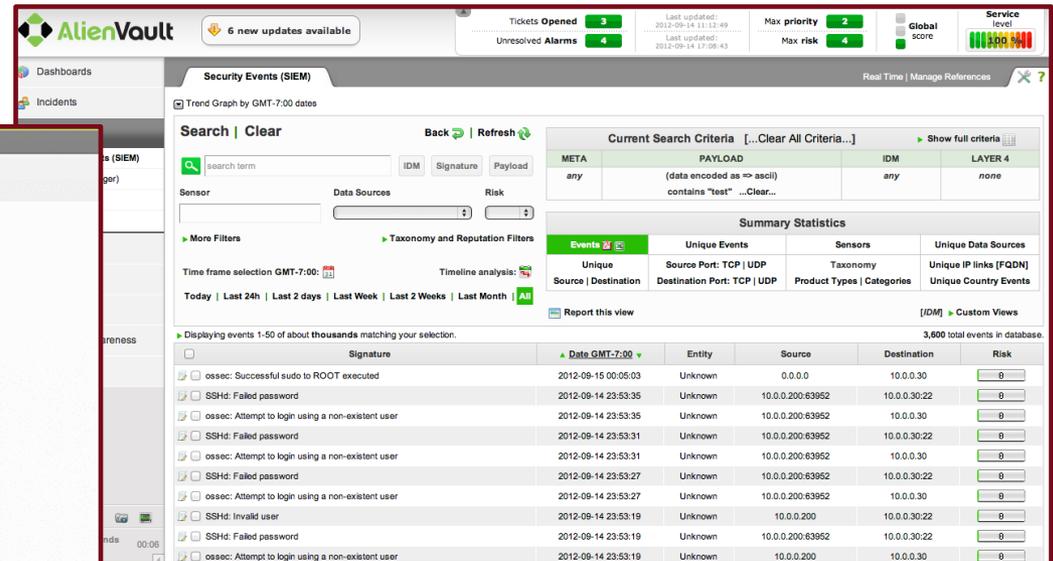
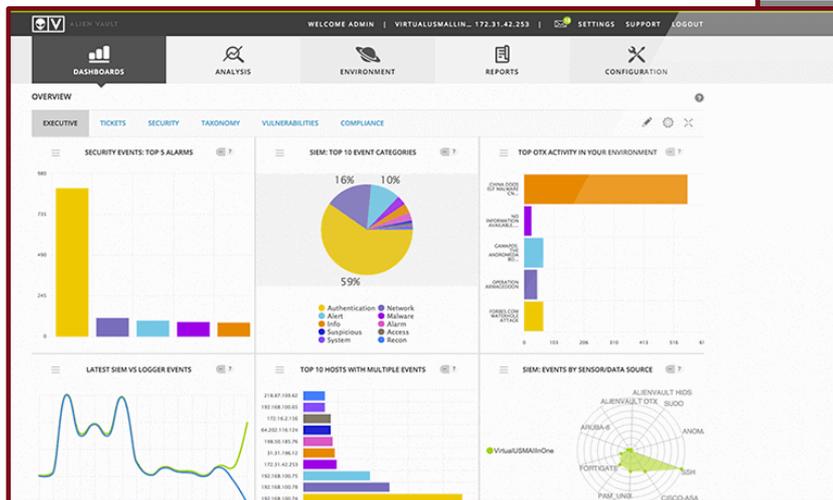
CYBER LAGEBILDER: BASIS-ERKENNTNISSE AUS CISA

- **DAS EINE** Cyber-Lagebild gibt es nicht!
- Sie sind immer Stakeholder- und Aufgabenspezifisch

- **Ebenen-gerecht**
 - Operative Ebene (z.B. Server Admin) benötigt andere Informationen als
 - Taktische Ebene (z.B. CISO), und wiederum anders darüber auf
 - Strategischer Ebene (z.B. Geschäftsführung)
 - Ausserdem: Unterscheidung zwischen Org-Sicht und nat. Sicht
- **Aufgaben-bezogen**
 - Incident Response
 - Risikoeinschätzung und -linderung
 - Strateg. Investments
 - Strafverfolgung
 - ...

DAS DILEMMA DER EBENEN-GERECHTEN INFORMATIONSDARSTELLUNG (1/3): OPERATIV

- Exemplarische Fragestellungen:
 - „Welchen Patch-Level haben die Maschinen der Infrastruktur?“
 - „Ist Port 4711 auf FW-1 nach außen offen?“
 - „Was sind das für merkwürdige periodische http-requests von meinem Web server w1 auf domain x?“
- Lagebewusstsein basiert auf **Verständnis des Systemverhaltens**:
 - Kombination aus Logdaten-Management, Paket Inspection, Endpoint-Security, SIEM
 - Abgleich mit ext. Quellen



DAS DILEMMA DER EBENEN-GERECHTEN INFORMATIONSDARSTELLUNG (2/3): TAKTISCH

- Exemplarische Fragestellungen:
 - „Welche Produkte haben in den letzten 3 Monaten Schwachstellen aufgewiesen, die besonders oft ausgenutzt wurden?“
 - „Welchen Typs waren die häufigsten Incidents?“
 - „Welche Komponenten der Netzarchitektur sind besonders gefährdet?“
- Lagebewusstsein basiert auf:
 - Interpretation der gesammelten und **aggregierten** technischen Daten innerhalb des Unternehmens (im Kontext deren Prozesse)
 - Einbeziehung externer Quellen (TI, CERT, kommerz. Dienste)
 - Ggf. Vergleich innerhalb des Sektors
 - IT Security Reifegrad und erfolgreiche Best Practices im Vergleich zu anderen Unternehmen in einer ähnlichen Situation (gleicher Sektor, ähnlicher Aufbau, ähnliche Dienstleistungen, ähnliche Größe)

DAS DILEMMA DER EBENEN-GERECHTEN INFORMATIONSDARSTELLUNG (3/3): STRATEGISCH

- Exemplarische Fragestellungen:
 - „Welche Schäden haben Cyber Angriffe die letzten 12 Monate im Sektor Energie verursacht?“
 - „Welche Kernprozesse waren besonders stark betroffen?“
 - „Welche Risiken unterliegen einem steigenden Trend?“
- Lagebewusstsein basiert auf:
 - Wie vorher, jedoch **abermals aggregiert und abstrahiert**
 - Losgelöst von Einzelvorfällen
 - Einbeziehung wirtschaftlich-rechtlicher Faktoren
 - Langfristige Auswirkungen



4. ANWENDUNG EINES SENSORNETZES IM TOP-DOWN ANSATZ



ÜBERSICHT: TOP-DOWN ANSATZ

- Informationserhebung nicht als „bottom up“-magic! Kein Big Data, Security Analytics, ...
- SONDERN: ein rigider und durchüberlegter Top-down-Prozess:
 1. Welche Aktionen bzw. Entscheidungen sollen abgeleitet werden?
 2. Welche Informationen müssen dafür dargestellt werden?
 3. Welche Daten müssen dafür gesammelt werden?
 4. Wie können geeignete Quellen bewertet werden?
 5. Welche Daten einer Organisation können mittels Sensorik nutzbar gemacht werden?

ANWENDUNG SENSORIK IM TOP-DOWN Ansatz (1/5): Welche Aktionen bzw. Entscheidungen sollen abgeleitet werden (Beispiele)?

- **Kurzfristige Entscheidungen (Stunden)**
 - Warnungen ausgeben; potentielle Opfer alarmieren (Early Warning)
 - Ggf. technische Hilfe leisten oder vermitteln (Vuln./Incident Response)
 - Empfehlungen ausgeben
 - Verstärkte Informationsweitergabe oder -austausch innerhalb der Branchen/Sektoren bzw. Trust Circles/IKDOK forcieren
- **Mittelfristige Entscheidungen (Stunden-Tage)**
 - Arbeitsgruppe erstellen / einsetzen um eine Krise zu bewältigen
 - Kontaktaufnahmen mit Anbieter/Hersteller/int'l Orgs.
 - Ggf. Assistenz bei Disaster Recovery
 - Best Practices und Guidelines zusammenfassen/ausgeben
 - Strafverfolgung einleiten
- **Langfristige Entscheidungen (Monate)**
 - Finanzielle Unterstützung/Attraktivierung der Weiterbildung von Experten,
 - Anbieten von Schulungen oder Weiterbildungen für Experten
 - Regelmäßige externe und interne Audits verordnen
 - Gesetzgebung anpassen (z.B. Meldepflicht anpassen usw.)

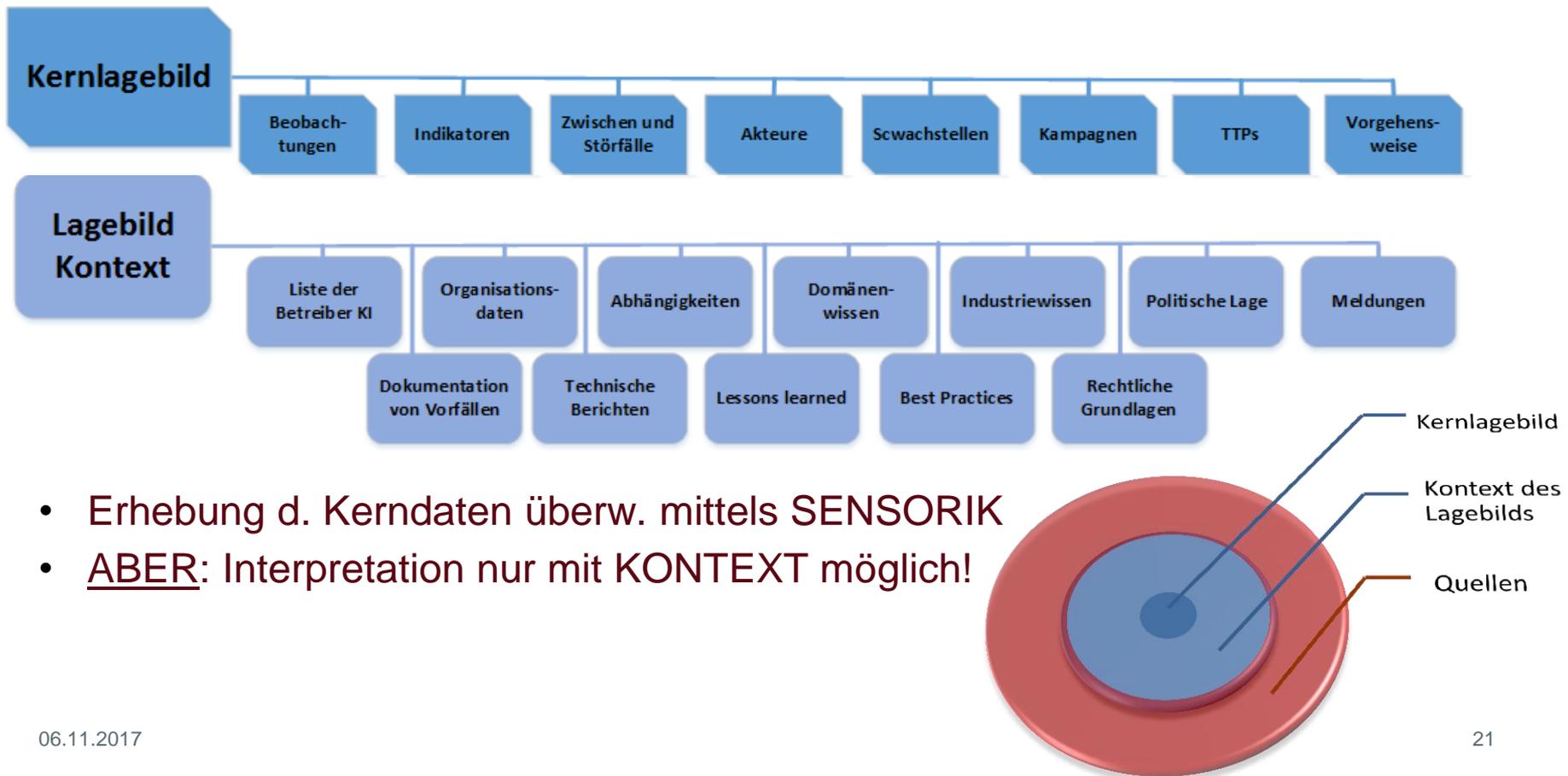
ANWENDUNG SENSORIK IM TOP-DOWN Ansatz (2/5):

Welche Informationen müssen dafür vorhanden/dargestellt werden?

- **Fallbezogen! Ebenen-bezogen! Stakeholder-bezogen!**
- **Beispiel: Risikoeinschätzung CyberCrime via DDoS**
- Bedrohungslage:
 - Was kostet ein DDoS Angriff mit 5 GBit/s für 1 Woche im Darknet? (600 USD; Stand 2016)
 - Hat jemand spezielles Interesse Org./Sektor X zu Schaden (Drohungen)?
- Risikoabschätzung basierend auf hist. Daten/Trends:
 - Wieviele/welche Unternehmen waren von derartigen Angriffen bisher betroffen?
 - Wie gut sind Unternehmen im Sektor X auf solche Angriffe vorbereitet (BCP; krit. Kernprozesse, Abhängigkeiten)?
 - Welche lindernden Maßnahmen wurden bereits gesetzt (traffic scrubbing)?
- Anlassbezogen im Falle eines Incident (Lessons learned für andere)
 - Art des Angriffs (bekanntes Botnet, Modus Operandi)?
 - Art und Kritikalität der betroffenen Systeme?
 - Höhe der Forderung – Wie viel Lösegeld wird von Erpressern verlangt, wohin ist dieses zu senden?

ANWENDUNG SENSORIK IM TOP-DOWN Ansatz (3/5): Welche Daten müssen zur Info-Erhebung gesammelt werden?

- **Kerndaten:** Kontinuierlich erhobene technische Daten (z.B. STIX)
- **Kontextdaten:** alle zur Interpretation der Kerndaten zweckdienlichen Infos

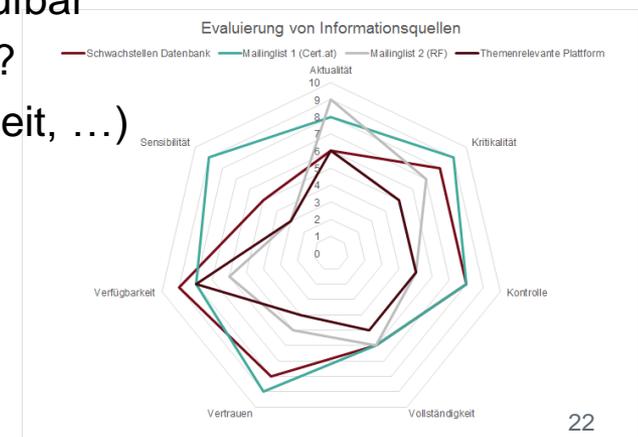


- Erhebung d. Kerndaten überw. mittels SENSORIK
- ABER: Interpretation nur mit KONTEXT möglich!

ANWENDUNG SENSORIK IM TOP-DOWN Ansatz (4/5): Wie können geeignete Quellen bewertet/gewichtet werden?

- **Anforderungen an Qualität** der Daten für Anwendungsfall
 - Abwägen bei widersprüchlichen Daten aus unterschiedlichen Quellen

- Umfangreiche Liste an **Bewertungsmetriken**
 - Aktualität – Zeitpunkt u. Dauer von Datengewinnung und Veröffentlichung
 - Relevanz – Relevanz zur Erstellung eines zweck-spez. Lagebilds
 - Kontrolle – Wer besitzt die Kontrolle über die Quelle
 - Vollständigkeit – keine Lücken; keine Ergänzungsquellen erforderlich
 - Vertrauen – Quelle und Daten vertrauenswürdig, d.h. nicht manipuliert
 - Verfügbarkeit – technisch und rechtlich jederzeit abrufbar
 - Sensibilität – Personenbezug, Schutzbestimmungen?
 - U.v.m. (Redundanzfreiheit, Genauigkeit, Unverzerrtheit, ...)



ANWENDUNG SENSORIK IM TOP-DOWN Ansatz (5a/5): Welche Daten einer Org. können mittels Sensorik nutzbar gemacht werden?

- **Basis-Betriebsinformationen (von aussen)**
 - Welche IP Adressen verwendet eine Organisation nach außen?
 - Welche (Kern-)Services bietet sie an?
 - Verwendete Zertifikate/Encrypt. für Komm. nach aussen (SSL/TLS, S/MIME...)
- **Sicherheitsrelevante Infos (Org-intern)**
 - Assets und Konfigurationen im Einsatz; SNMP(v3)
 - Abgleich mit bekannten Vulnerabilitäten und deren Scores/Kritikalität
 - Informationen zur Systemnutzung
 - Normal: Bandbreiten, Systemauslastung, Systemreserven udgl.
 - Betriebsanomalien und angegriffene Dienste
 - Info Sammlung mittels Honey Pots/HoneyNets, v.a. TTPs
 - Ergebnisse regelmäßiger Malwarescans, internen Audits udgl.
 - IoC Sightings; inkl. Sandbox-Analyse-Ergebnisse
- **Abgeleitete Informationen (correlation/inference)**
 - Patch-Mentalität (outdated patch level; Zeitspannen Release -> Anwendung)
 - Betriebs-Best Practices (user management, password policies, ...)
 - Malwarebefall trotz verfügbarer Patches
 - Incident Response „Quality“

ANWENDUNG SENSORIK IM TOP-DOWN Ansatz (5b/5):

Exkurs: AIT Sensor AMiner

- **AMiner** ist eine leichtgewichtige Komponente zum Erstellen von System-Verhaltensmodellen basierend auf Log-Daten am Host
 - GPLv3; im stable Branch von Ubuntu und Debian
 - Optionale intelligente Lernkomponente
- Anwendungsfälle:
 - **Network Interaction/Link Graph:**
 - Welche Maschinen kommunizieren über welche Protokolle mit welchen anderen Maschinen?
 - **Authentication Graph:**
 - Welche Benutzer melden sich über welche Maschinen auf welche anderen Maschinen an?
 - **Syscall Sequenzen und Profiling über Maschinen hinweg**
 - Welche syscall Sequenzen (über auditd) sind für Maschinen eines gewissen Typs (Web-Server, DB usw.) „normal“?
 - *Die ermittelten Profile sind üblicherweise relativ stabil. Abweichungen deuten damit entweder auf Updates oder auf Folgen eines Angriffs hin.*
- **Mehr Informationen auf unserem Stand!**



<https://launchpad.net/logdata-anomaly-miner>

5. VISUELLE AUFBEREITUNG GESAMMELTER SECURITY-INFORMATIONEN

Beispielhafte Darstellungen (aus CISA)



MOCKUP #1: MELDUNGEN

Cyber Lagebild

- Übersicht
- Sektor auswählen
- Weitere Details

Letzte Meldungen

Meldung Art	Vollständigkeit	Sektor	CERT Bemerkung	Score
-M #1 <i>freiw.</i>	Vollständig	Finanz	Vorwarnung nötig	7,3
-M #2 <i>Pflicht</i>	Lückenhaft	TelCo	Fehlkonfiguration	5,4
-M #3 <i>Pflicht</i>	Vollständig	Energie	-	-
-M #4 <i>freiw.</i>	Vollständig	Transport	Vorsicht	4,2
...
...

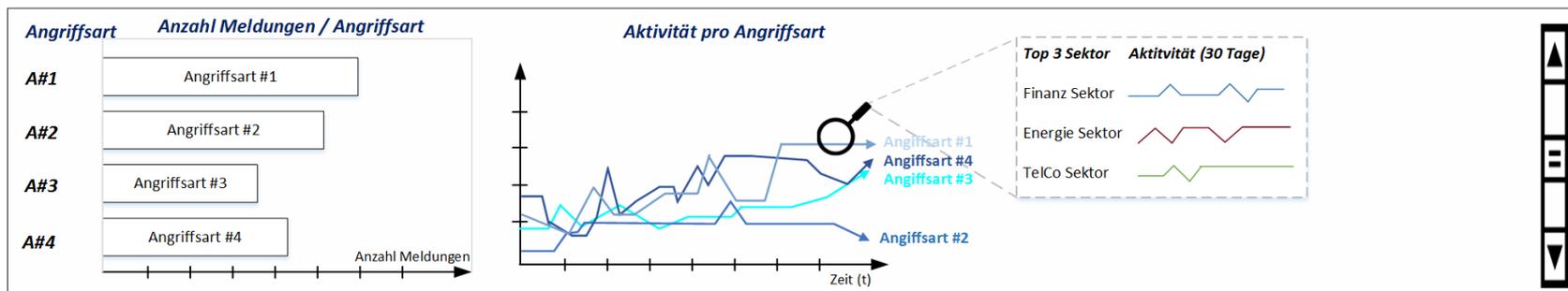
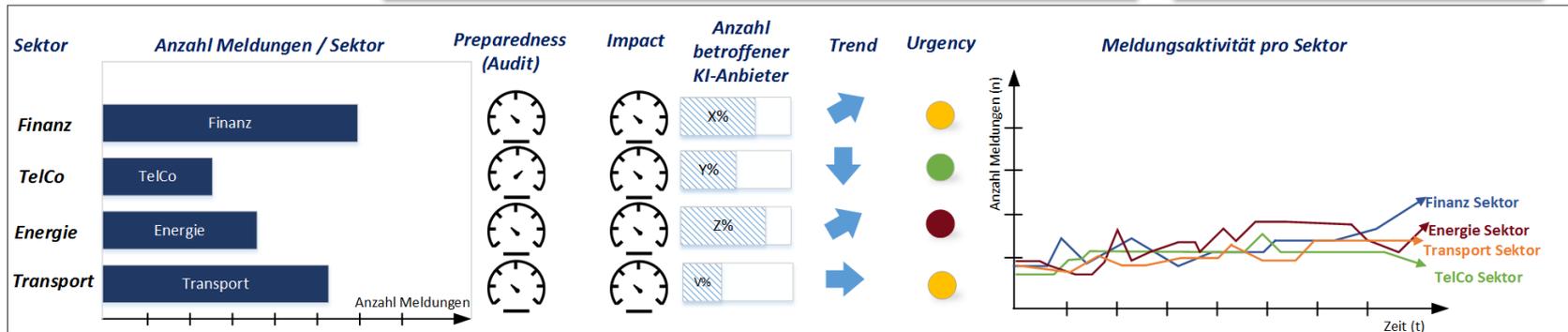
News

Österreich

XYZ
WZQ...

International

XYX
XYZ



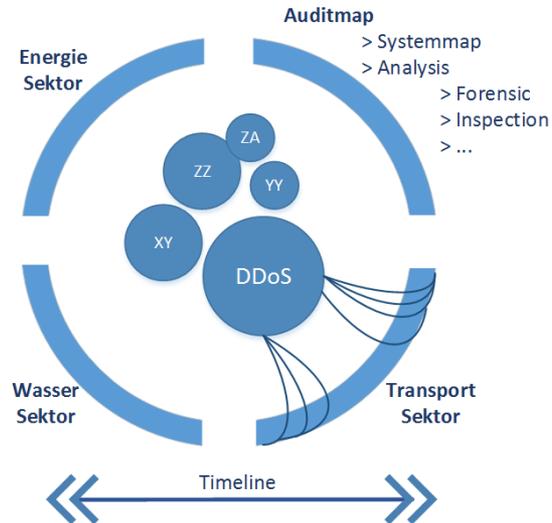
MOCKUP #2: VULNERABILITIES / RISIKEN

International

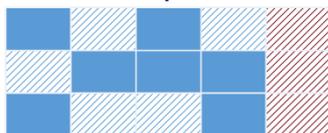
Vulnerabilitäten

Datenbank: NIST, MITRE

- Services
- OS
- Port (SSH, DNS ...)
- Vulnerabilität



Score Treemap

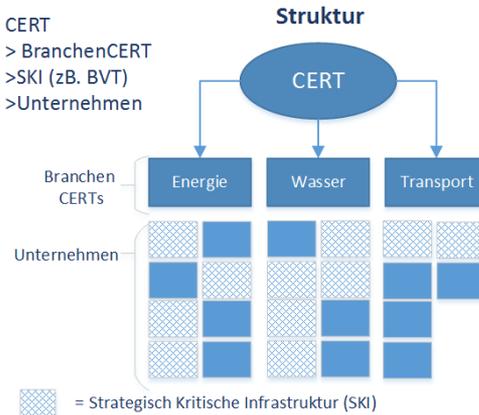


Gridbox
0-10
Rot > 7,5
(Use case)

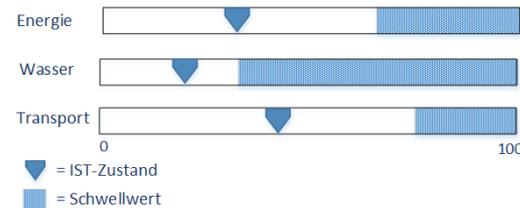
National

Lagebild Dashboard

CERT
> BranchenCERT
> SKI (zB. BVT)
> Unternehmen



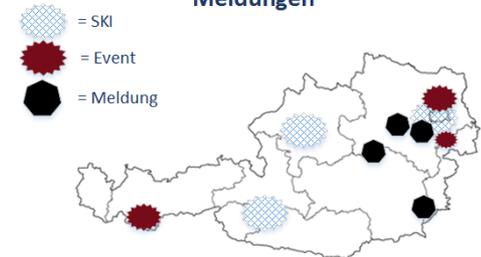
Schwellwert



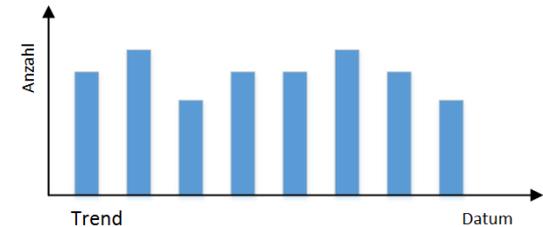
Newsmap

Österreich
DDoS
im Burgenland...

Meldungen



Meldung (STIX)	Type	Datum	Zeit	Suche
XYA	XYAB	
XYB	XYBB	
XYC	XYBC	



- 1 Std
- 3 Std
- 18 Std

Reaktionen

	R#1	R#2	R#3	R#4	
Option I.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	DDoS
Option II.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	APT
Option III.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ZeroDay

MOCKUP #3: INCIDENTS

Übersicht - KI-Domäne

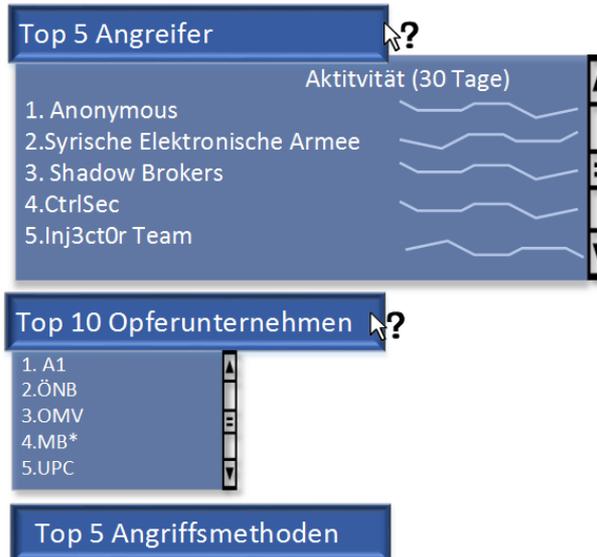


Zeitspanne
 24 Std
 48 Std
 Letzter Monat

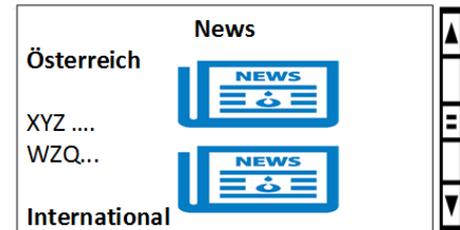
Legende
 Farbe = Schwellwert
 Pfeil = Trend

? Mit Auswählen erhält man weitere Informationen

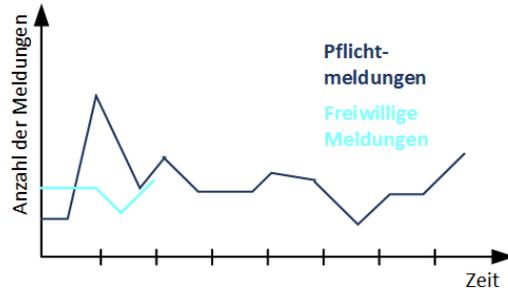
Österreich Aktuell



Newsfeed



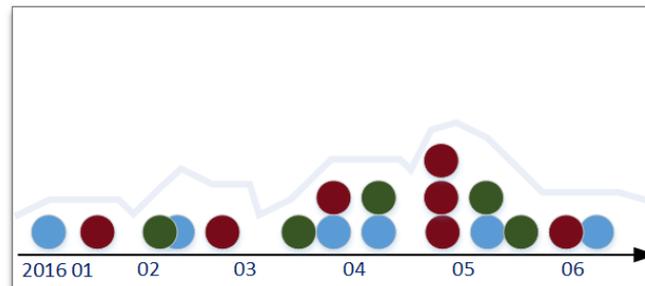
Meldungen



Zeitspanne: In den letzten 3 Monaten

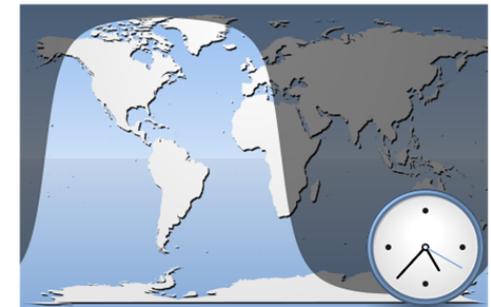
06.11.2017

Malicious Activity (landesweit)



Legende:
 Angriffsart Nr1. ● Angriffsart Nr1. ● Angriffsart Nr1. ●

Daylight Karte



6. CONCLUSIO



CONCLUSIO UND TAKE-AWAY

- Datensammlung mittels Sensorik und Aufbereitung ist immer **Ebenen- und Anwendungsfallspezifisch**
 - WER soll WAS auf Basis der gewonnenen Daten machen bzw. WIE handeln?
- Beispiel: Ein besserer Überblick über den Zustand kritischer Infrastrukturen kann helfen **Gegenmaßnahmen** noch besser zu **koordinieren**
 - Wer ist betroffen und zu welchem Grad?
 - Wo müssen Gegenmaßnahmen gezielt getroffen werden?
- **NIS RL** und **Cyber-Sicherheitsgesetz** werden Situation massiv verändern
 - Pflichtmeldungen; Anreicherung mit freiwilligen Meldungen; DSGVO
- Einsatz von **Sensorik um** entweder vorab **klar definierte Informationen** zu **erheben** oder low-level Rohdaten zu sammeln.
 - **Kontextualisierung**: z.B. Ist betroffenes System kritisch für Business Prozess?
 - Im Falle von Rohdaten ist eine spätere Interpretation extrem herausfordernd
- **Transparenz des Erhebungsprozesses und begründete Datenermittlung ist unabdingbar**
 - Alle Beteiligten müssen profitieren: **Win-Win Situation!**



Zurück zu den Ergebnissen

Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks on National Level (Englisch) Gebundene Ausgabe – 1. November 2017

von Florian Skopik (Herausgeber)

▶ Alle Formate und Ausgaben anzeigen

Gebundene Ausgabe
EUR 72,73
Aktuelle Angebote Vorbesteller-Preisgarantie 1 Werbeaktion(en) ▾

 Dieser Artikel kann nach Österreich versendet werden. [Siehe Details.](#)

1 neu ab EUR 72,73

Threat intelligence is a surprisingly complex topic that goes far beyond the obvious technical challenges of collecting, modelling and sharing technical indicators. Most books in this area focus mainly on technical measures to harden a system based on threat intel data and limit their scope to single organizations only. This book provides a unique angle on the topic of national cyber threat intelligence and security information sharing. It also provides a clear view on ongoing works in research laboratories world-wide in order to address current security concerns at national level. It allows practitioners to learn about upcoming trends, researchers to share current results, and decision makers to prepare for future developments.

▲ Weniger lesen

Falsche Produktinformationen melden


Weitere Bücher auf Englisch, Französisch, Spanisch und in vielen weiteren Fremdsprachen:

 Entdecken Sie Empfehlungen, Bestseller und vieles mehr in unserem Shop für fremdsprachige Bücher. [Hier klicken.](#)

Teilen

EUR 72,73

Alle Preisangaben inkl. USt

Vorbesteller-Preisgarantie

Kostenlose Lieferung.
Dieser Artikel ist noch nicht erschienen.

Bestellen Sie jetzt vor und wir liefern Ihnen den Artikel sobald er verfügbar ist.

Verkauf und Versand durch Amazon. Geschenkverpackung verfügbar.

Menge: 1 ▾

Jetzt vorbestellen

Loggen Sie sich ein, um 1-Click® einzuschalten.

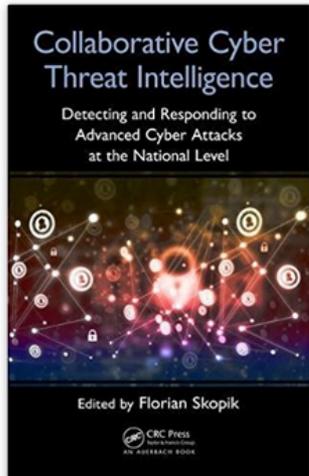
Lieferort:

Florian Skopik- Stockerau - 2000 ▾

Auf die Liste

Möchten Sie verkaufen?

Bei Amazon verkaufen



Dieses Bild anzeigen

BESTEN DANK FÜR IHRE AUFMERKSAMKEIT!

Jegliche Anregungen und Anfragen richten Sie bitte gerne an:

Dr. Dr. Florian Skopik
Senior Scientist ICT Security

AIT Austrian Institute of Technology GmbH

Center for Digital Safety & Security
Donau-City-Straße 1 | 1220 Wien | Austria
M +43 664 8251495 | F +43(0) 50550-4150

florian.skopik@ait.ac.at

