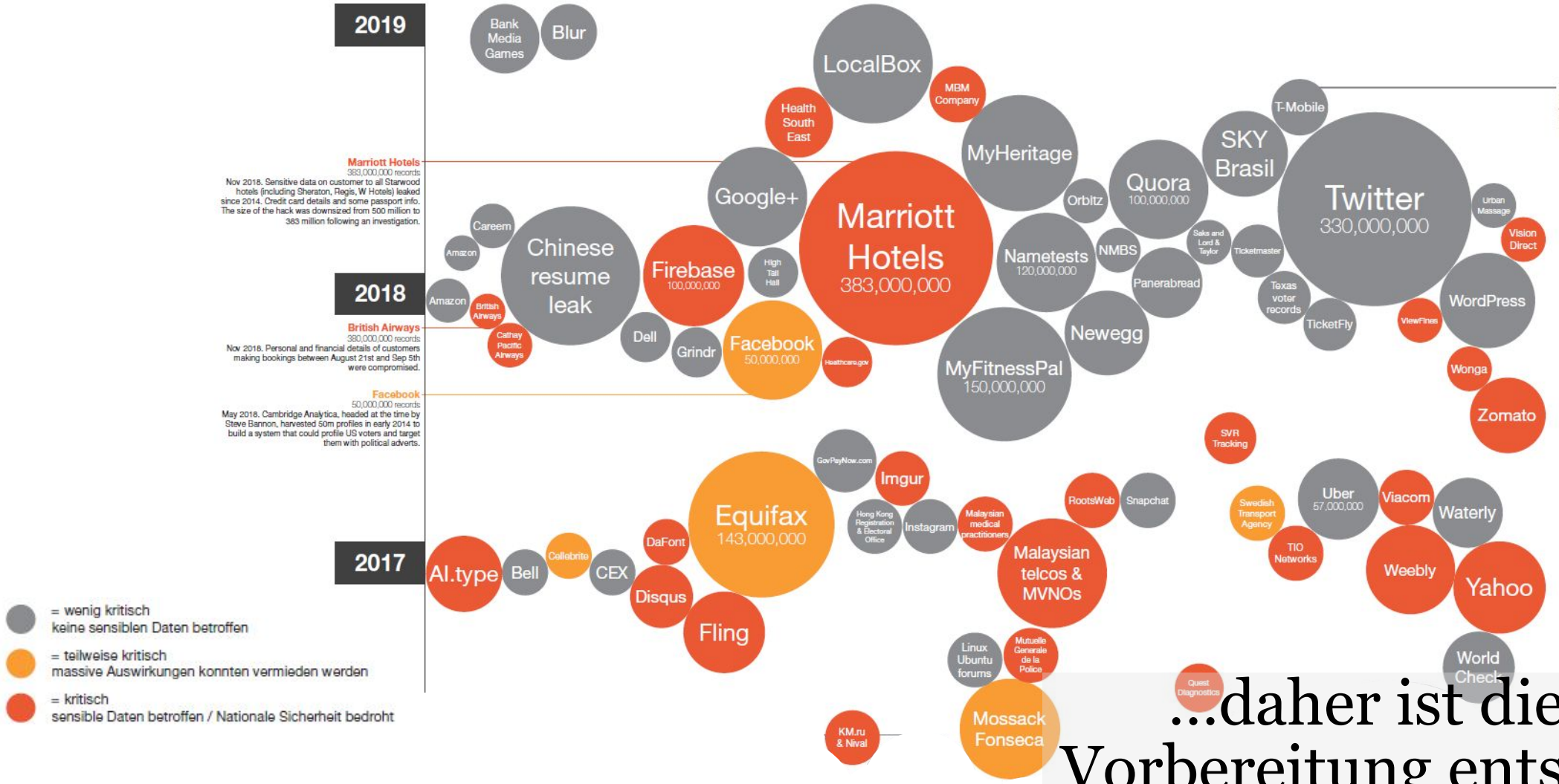
Cyber Threat Intelligence als Enabler für Schwerpunktprüfungen

ISC2/ISACA Konferenz
Oktober 2019

pwc

Cybersecurity Incidents passieren jeden Tag:



...daher ist die passende Vorbereitung entscheidend.

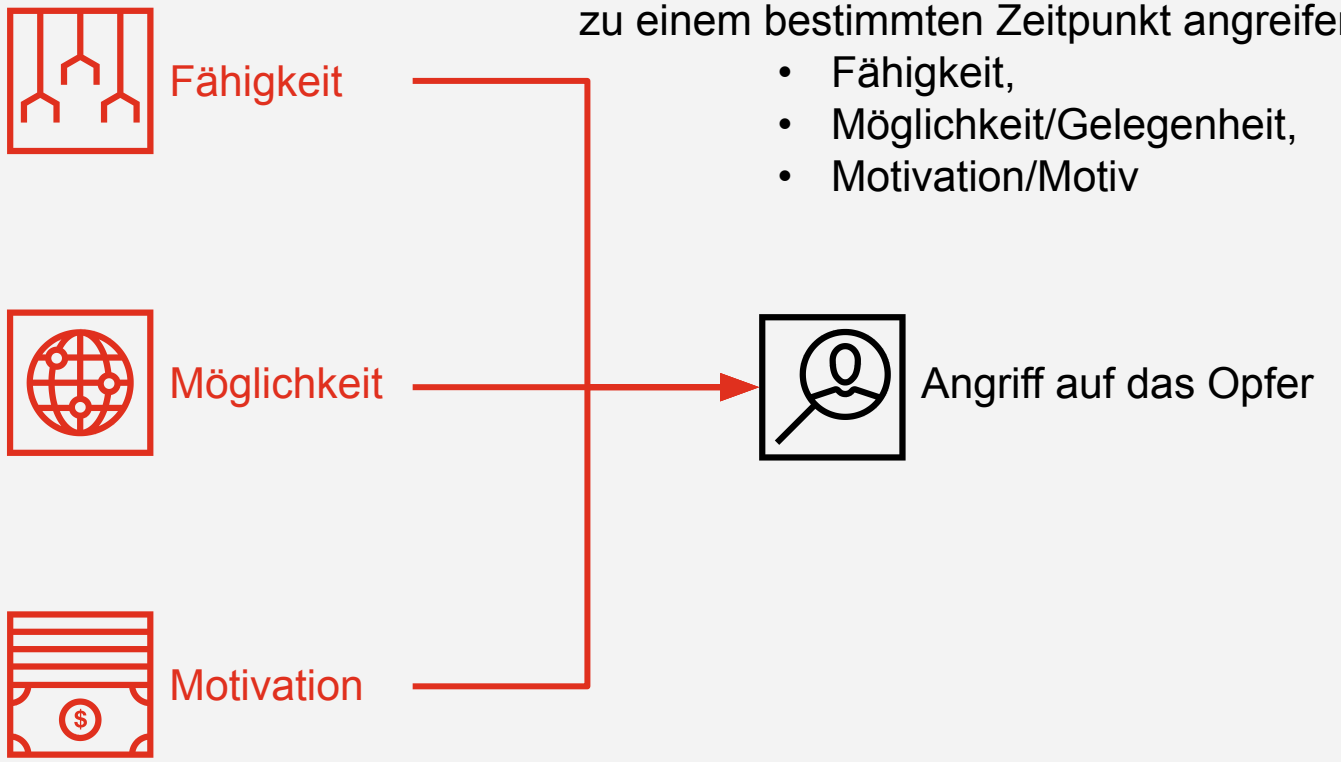
Der Angriff:
Bedrohung – Gefährdung – Risiko

Angriffsakteure

- Script Kiddies
- Hacktivisten
- Cyberkriminelle
- Innentäter
- Staatl. Akteure

Ein Angreifer benötigt drei Dinge um das Opfer zu einem bestimmten Zeitpunkt angreifen zu können:

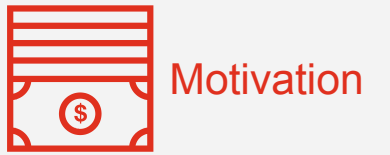
- Fähigkeit,
- Möglichkeit/Gelegenheit,
- Motivation/Motiv



Der Angriff:
Bedrohung – Gefährdung – Risiko

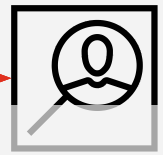

Fähigkeit


Möglichkeit


Motivation

Ein Angreifer benötigt drei Dinge um das Opfer zu einem bestimmten Zeitpunkt angreifen zu können:

- Fähigkeit,
- Möglichkeit/Gelegenheit,
- Motivation/Motiv


Angriff auf das Opfer

Ableitung:

Wir wollen über die Fähigkeiten, Möglichkeiten und Motivation der Akteure Bescheid wissen.

Threat Intelligence is…

*Evidence-based **knowledge**, including context, mechanisms, indicators, implications and **actionable** advice about an existing or emerging menace or hazard to assets that can be used to **inform decisions** regarding the subject's response to that menace or hazard."*

Gartner

Verschiedene Arten von Threat Intelligence

Taktisch

Handlungsfenster: **sofort**

Informationen, mit denen eine aktuelle Gefahr detektiert oder verhindert bzw. auf einen eingetretenen Incident reagiert werden kann.

Beispiel:

- MD5 Hash
- Malicious Domain/IP

Operativ

Handlungsfenster: **Wochen**

Informationen, die verwendbar sind und einen Incident proaktiv verhindern.

Beispiel:

- Vorhandene Schwachstellen
- Vorgehensanalyse von Akteuren

Strategisch

Handlungsfenster: **Monate bis Jahre**

Abstraktes Niveau, zukunftsgerichtet, Informationen um die Bedrohungslandschaft verstehen und einordnen zu können.

Beispiel:

- Geopolitische Analysen bestimmter Regionen
- Analysen von auftretenden Trends in Cyber Crime /Hacker Communities

Weitere Verwendungsmöglichkeiten von Threat Intelligence zur Security Incident Bearbeitung

Indikatoren

- Dynamische Feeds mit einzelbewerteten Indikatoren im Zusammenhang mit erfolgten Angriffen
- Kontext mit Bedrohungsakteuren, Malware-Familien und anderen Indikatoren

Visuelle Darstellung

Durch visuelle Aufbereitung (bspw. MALTEGO-Graphen), während dem Aufarbeiten von Angriffen, erleichtert Incident Handlern die Indikatoren zu deuten und mit eigenen Deutungen anzureichern.

Signaturen

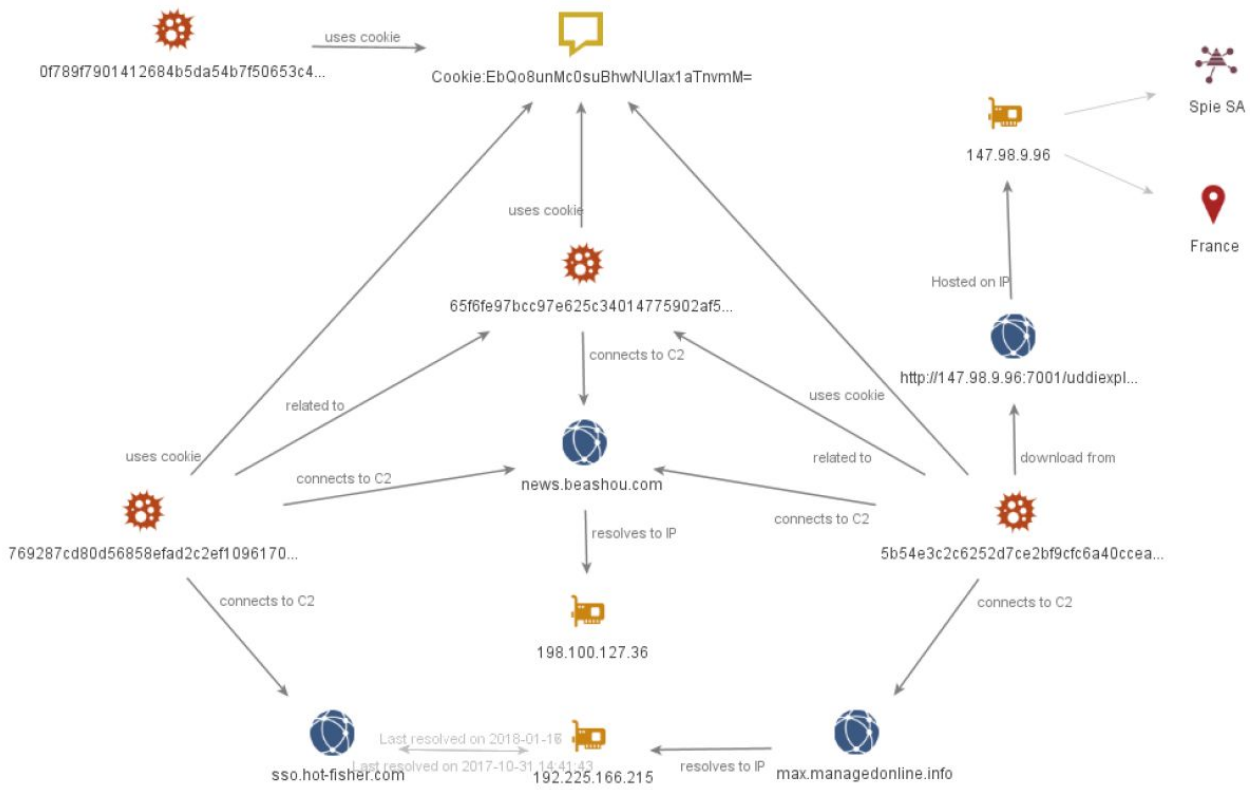
- nutzbare NIDS und HIDS Signaturen
- bspw. Suricata, OpenIOC & YARA

Sinkhole Monitoring

Monitoren der IP-Range in unserem Malware-Sinkholes und Warnung in Echtzeit, wenn beobachtete Schadsoftware aktiv ist.

Malware Repositories

Nutzen des Repositories um statische Malware-Informationen oder passive DNS-Einträge abzufragen



Darstellung der Netzwerk Infrastruktur- und Cookie-Verwendung von einem analysierten DLL

Threat Intelligence als Enabler für Schwerpunktprüfungen

Motivation

Threat Landscape

Identifikation mittels OSINT, Analyse und Bewertung von Bedrohungen gegenüber physischer und digitaler Infrastruktur sowie gegenüber Personen. Identifikation von Leaks und erstellen Threat Landscape

Ziel: Potentielle Akteure anhand Threat Landscape ableiten.

Fähigkeit

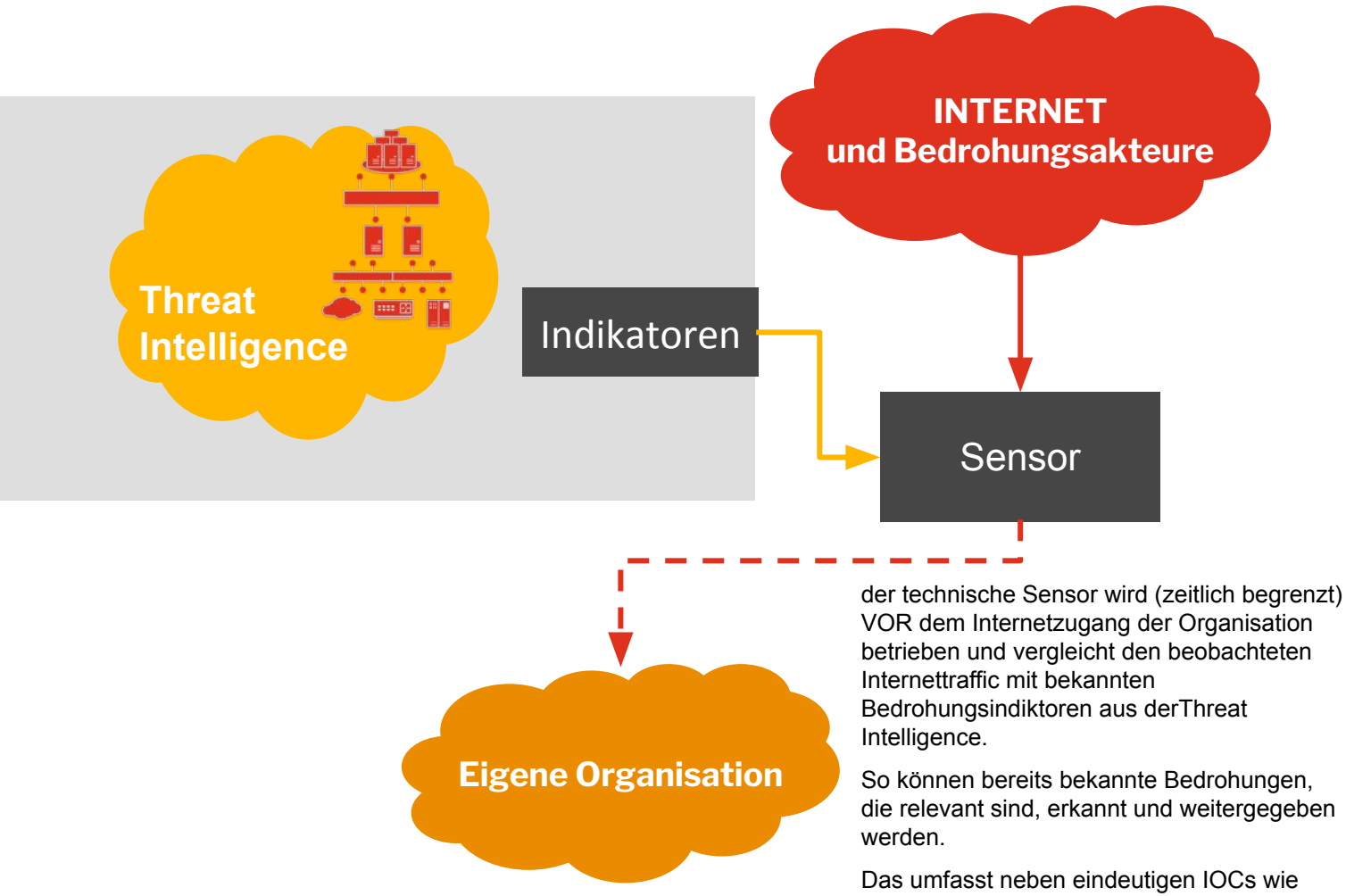
Tactics Techniques and Procedures

Detailreports über Fähigkeiten, Mittel, Methoden und Ziele der identifizierten Akteure inkl. Möglichkeiten zur Detektion, Mitigation oder Vermeidung deren Wirkungsfähigkeit. Anhand von Berichten durch PwC.UK oder zumindest ihrer Daten.

Ziel: (Gegen-)Maßnahmen gegen Angriffsvektoren

Wussten Sie, dass PwC 2018 insgesamt 209 verschiedene Threat Intelligence Berichte veröffentlicht hat?

Threat Intelligence als Enabler für Schwerpunktprüfungen



der technische Sensor wird (zeitlich begrenzt) VOR dem Internetzugang der Organisation betrieben und vergleicht den beobachteten Internettraffic mit bekannten Bedrohungsindiktoren aus derThreat Intelligence.

So können bereits bekannte Bedrohungen, die relevant sind, erkannt und weitergegeben werden.

Das umfasst neben eindeutigen IOCs wie IP-Adressen und Domainnamen auch Abuse-Data oder Vulnerable-Services

Möglichkeit

Threat Identification

Vorgehenskonzept:

- Durch den Einsatz von Sensoren vor oder hinter dem Perimeter können auch heterogene IT-Landschaften abstrakt auf Bedrohungen in Echtzeit gemonitored werden.
- Ziel ist es Anomalien zu erkennen und den IT-Betrieb auf Bedrohungen vorzubereiten
- Am Ende des Beobachtungszeitraumes wird das von außen sichtbare Cyberrisiko dokumentiert
- Die Ergebnisse können durch Penetration Tests oder Red Team Assessments verdichtet werden.

Ziel:

- Matchen, ob die IT-Sicherheitsmaßnahmen an der Bedrohungslandschaft angepasst sind und erkennen des realistischen Bedrohungspotentials

Kontaktieren Sie uns

Führend
PwC recognized as “a leading provider of threat intelligence services against nation state actors. PwC “combines its digital forensics consulting with internal intelligence […] which enables robust outcomes”

Passend
“PwC is the best fit for companies that wish to outsource their threat intelligence capability.”

Analytisch
“PwC’s threat intelligence service leads with the analytic core of its operations and people and the global reach and size of capabilities grounded in technical intelligence.”

Forrester WAVE – External Threat Intelligence Services – August 2018

Philipp Mattes-Draxler

Senior Manager,
Cybersecurity & Privacy

+43 699 16305022

philipp.mattes-draxler@pwc.com

Thank you

pwc.at