IBM Security

Cyber Security

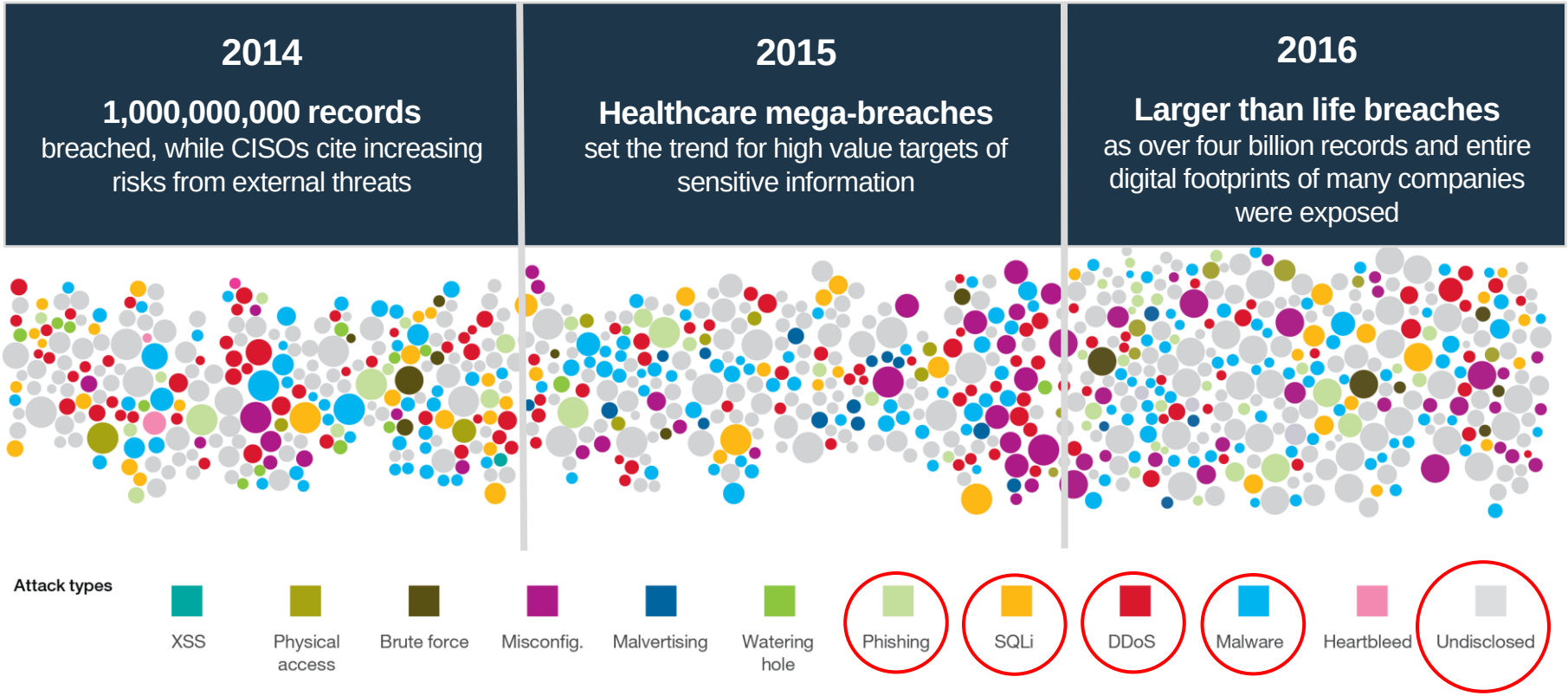
CYBER SECURITY CHALLENGES VON HEUTE – WIE REAGIERT DIE INDUSTRIE DARAUF?

Bernhard Kammerstetter, Client Technical Professional

IT Future challenges im FLL Wien, 2017-12-11

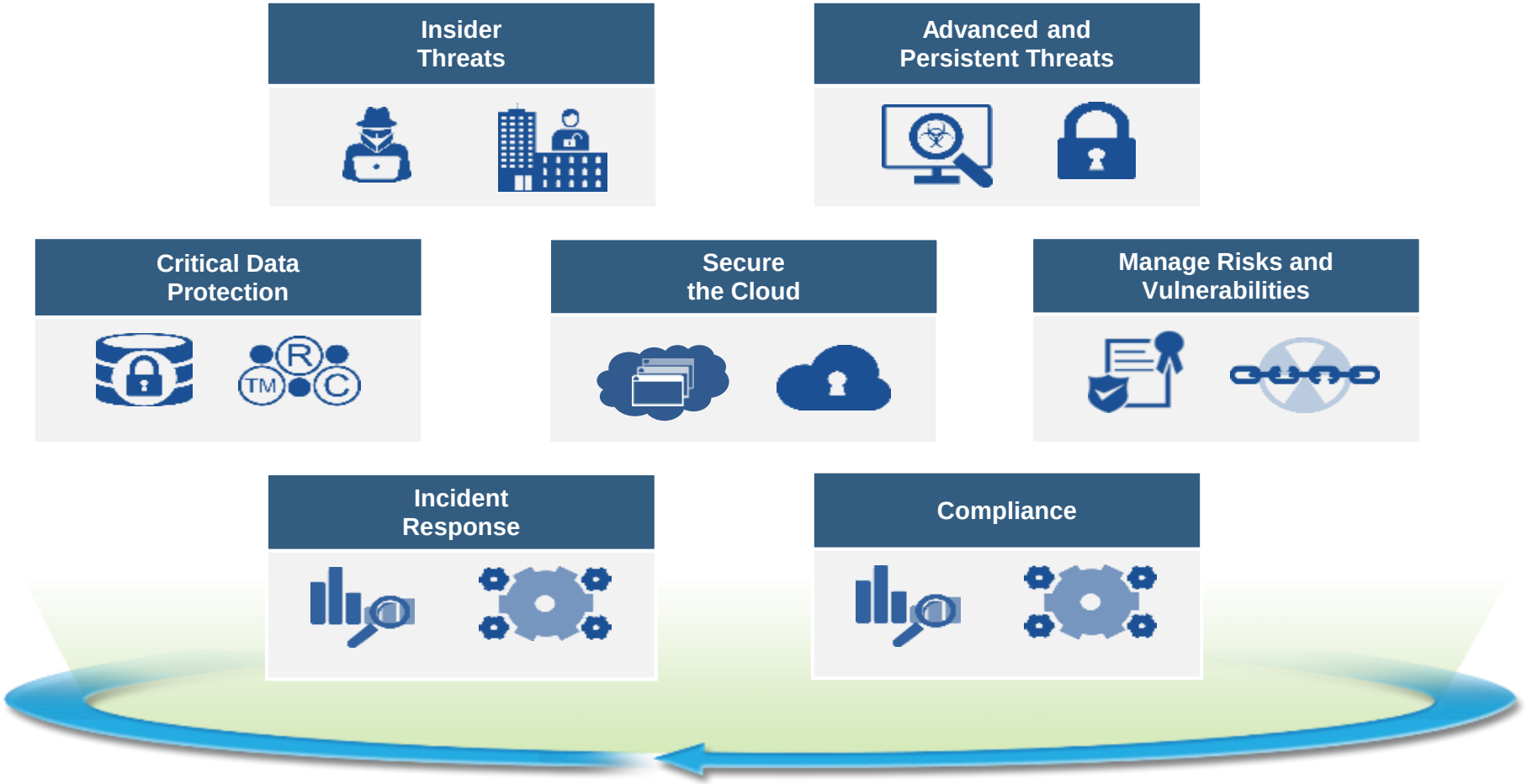
IBM

Bereits 2016 gab es eine noch nie dagewesene Anzahl von verlorengegangenen Datensätzen bzw. unstrukturierten Daten



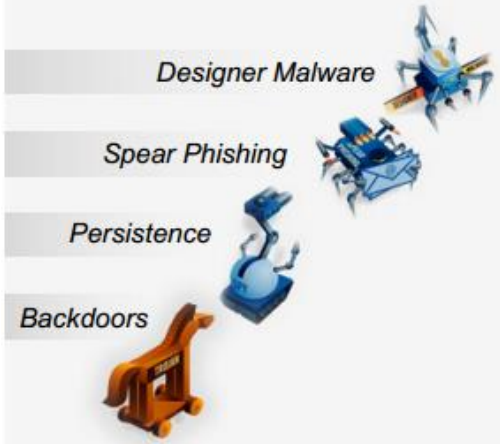
average time to identify data breach: **201 days**

Folgende Themen stehen bei C(I)SOs auf der Agenda:



Security-Herausforderungen steigen exponentiell*

Eskalierende Angriffe



- Neue Angriffsmethoden, gezielt und trickreich
- Perimeter verschwinden
- Steigende Zahl an Sicherheitsvorfällen

Steigende Komplexität

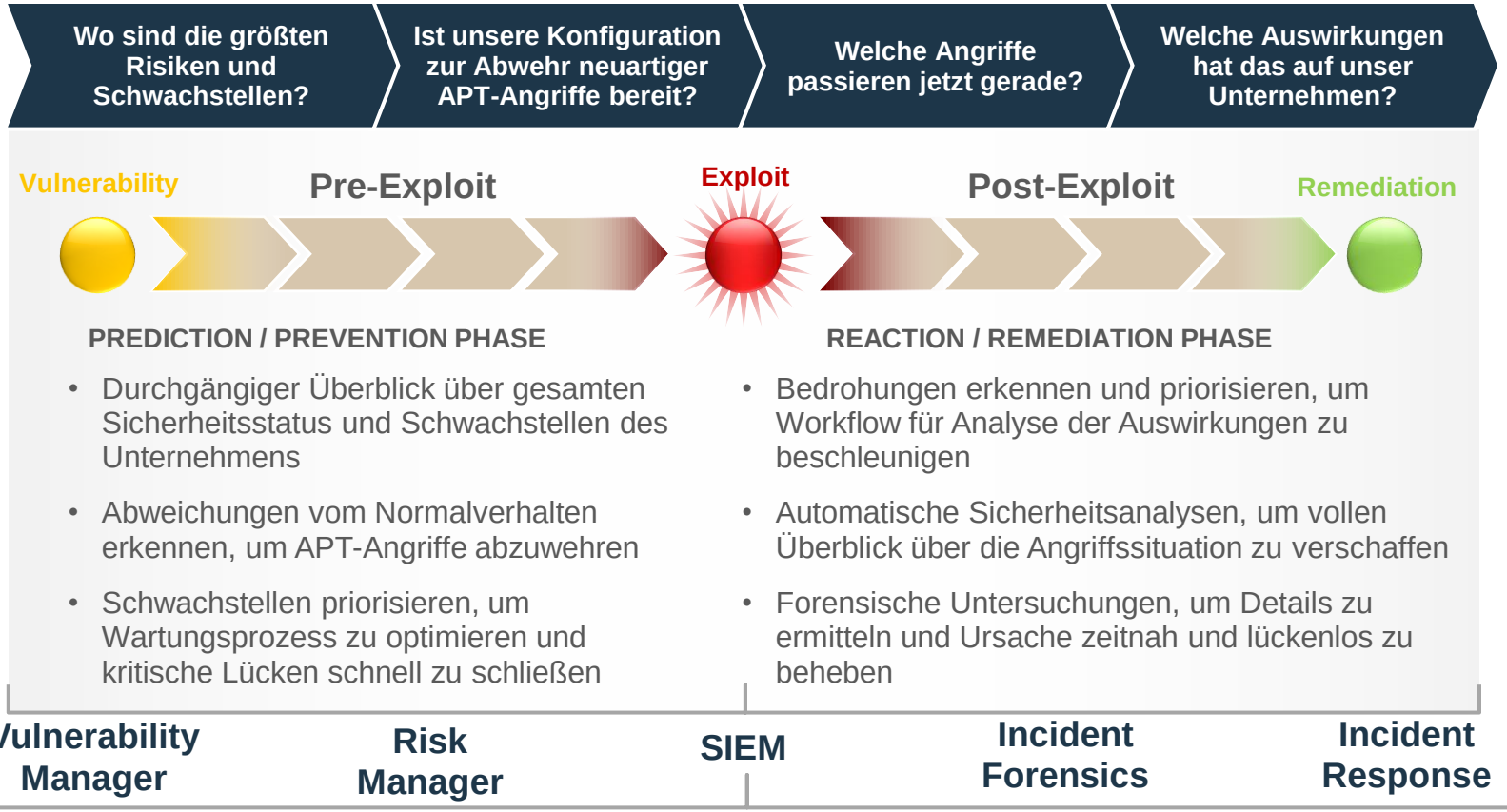
- Infrastruktur ändert sich laufend
- Zu viele Produkte verschiedener Hersteller
- steigende Kosten für Umsetzung und Betrieb
- Ineffiziente Werkzeuge

Mangel an Experten

- Überforderte Sicherheitsteams
- Zu viele Daten für zu wenig Experten
- Steigende Compliance Anforderungen

* Die Anzahl der entdeckten Schwachstellen pro Jahr ist seit 2010 um das 20-fache gestiegen!

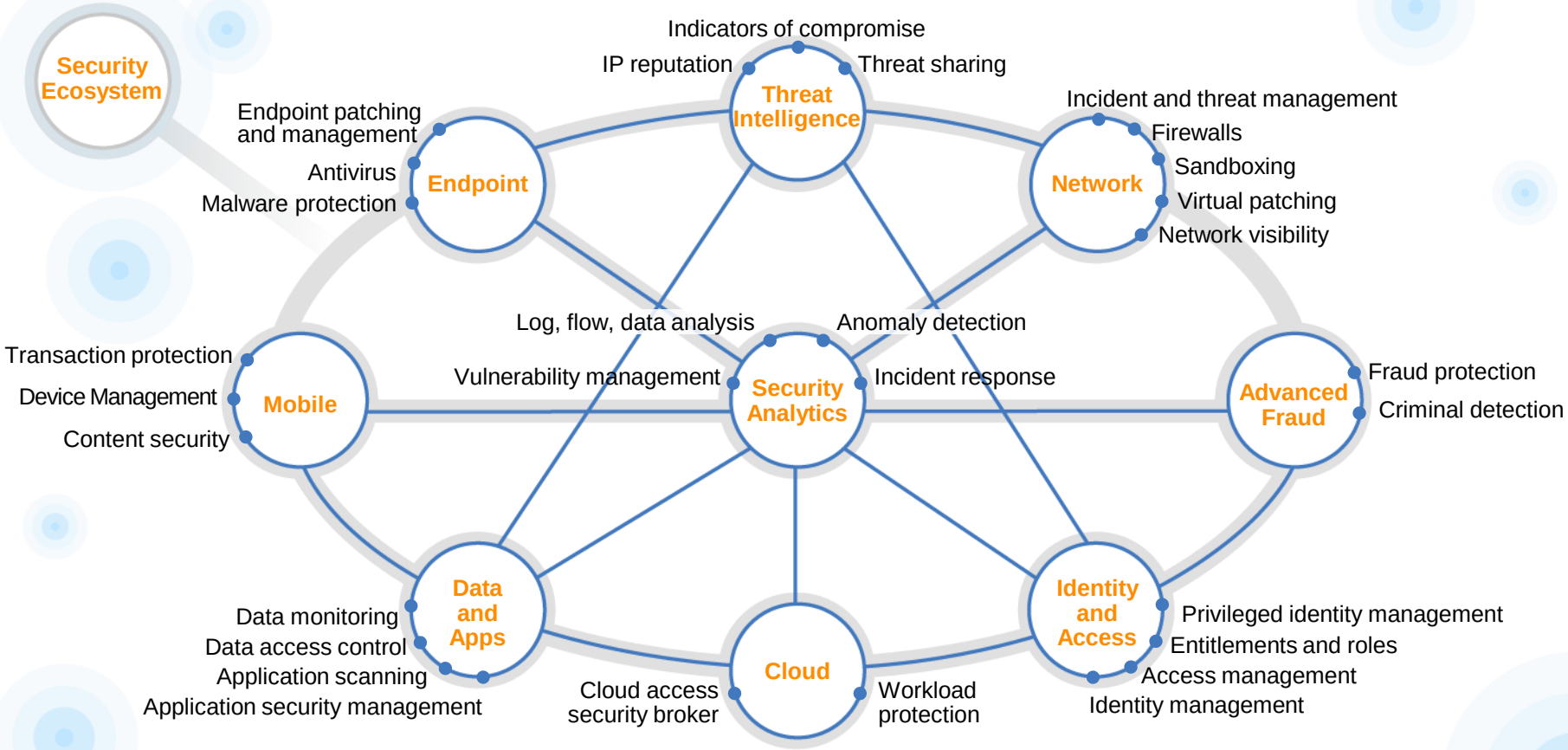
Die entscheidenden Fragen stellen …



Security Intelligence

... liefert handlungsorientierte Informationen durch Analyse sicherheitsrelevanter Daten eines Unternehmens

Erweiterung der Security durch Intelligence und Integration



Was haben folgende Vorgänge gemeinsam?

>99% of cyber attacks traverse the network in some way

Only insider attacks collecting local system data and posting it to removable media do not

- Enterprise Management Associates

The good news:

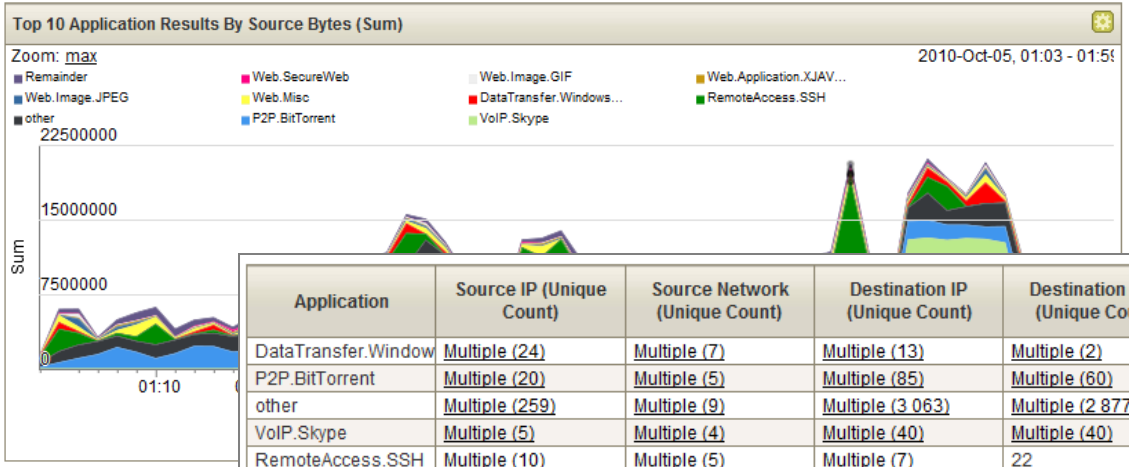
Im Netzwerk finden sich die Daten,

die man für die Erkennung benötigt

… wenn man genau genug hinsieht

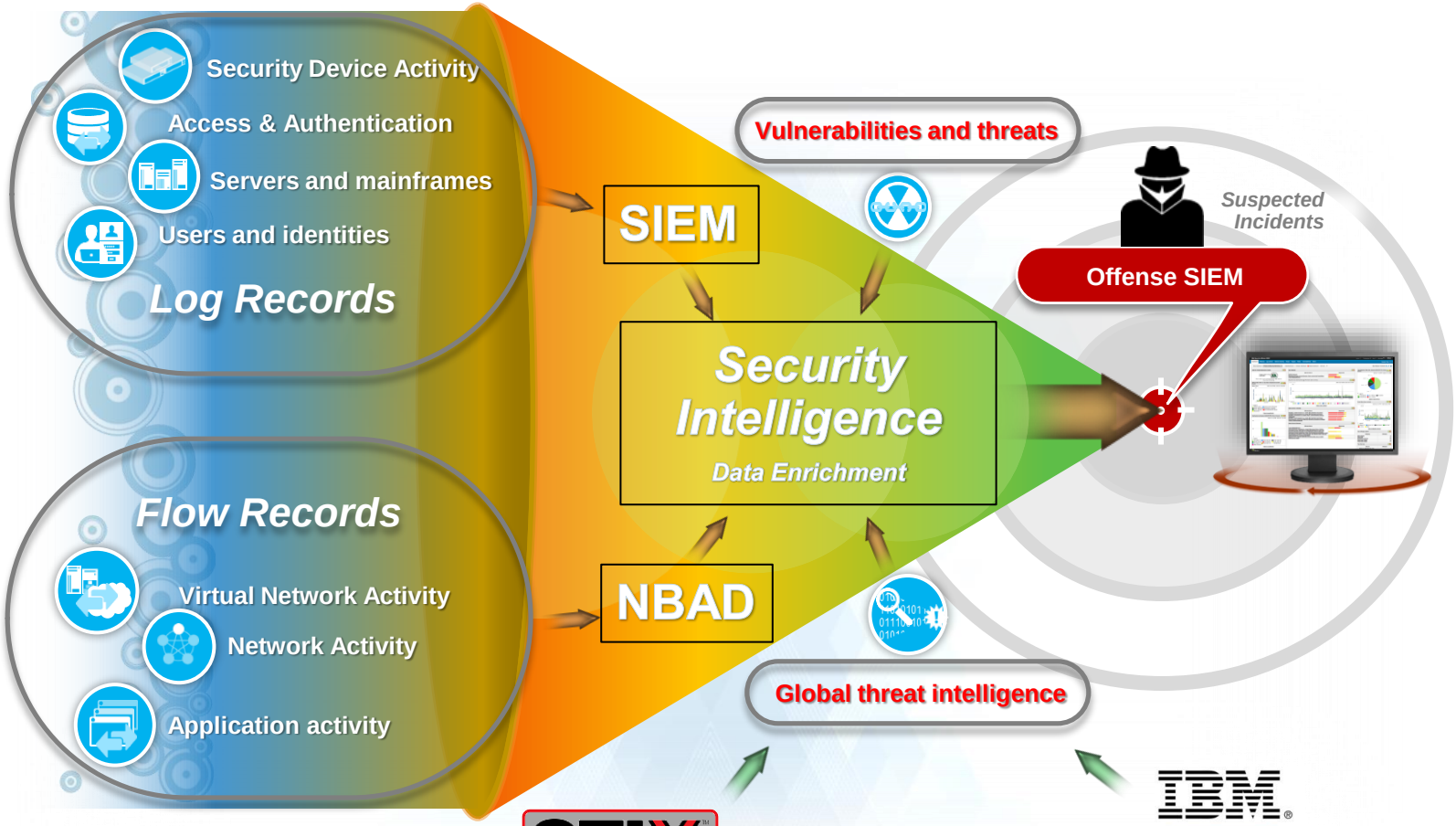
QRadar Network Insight – leuchtet auch tote Winkel aus

- **Network-Traffic lügt nicht!** Angreifer können zwar Logging deaktivieren und Spuren verwischen, sind jedoch auf das Netzwerk angewiesen (flow data)
  - Deep packet inspection für Layer 7 flow data
  - Pivoting, drill-down und data mining für Flow-Sourcen für erweiterte Erkennung oder Forensics
- Hilft beim Erkennen von Anomalien, die ansonsten im Verborgenen bleiben
- Macht die Netzwerk-Aktivitäten von Angreifern sichtbar



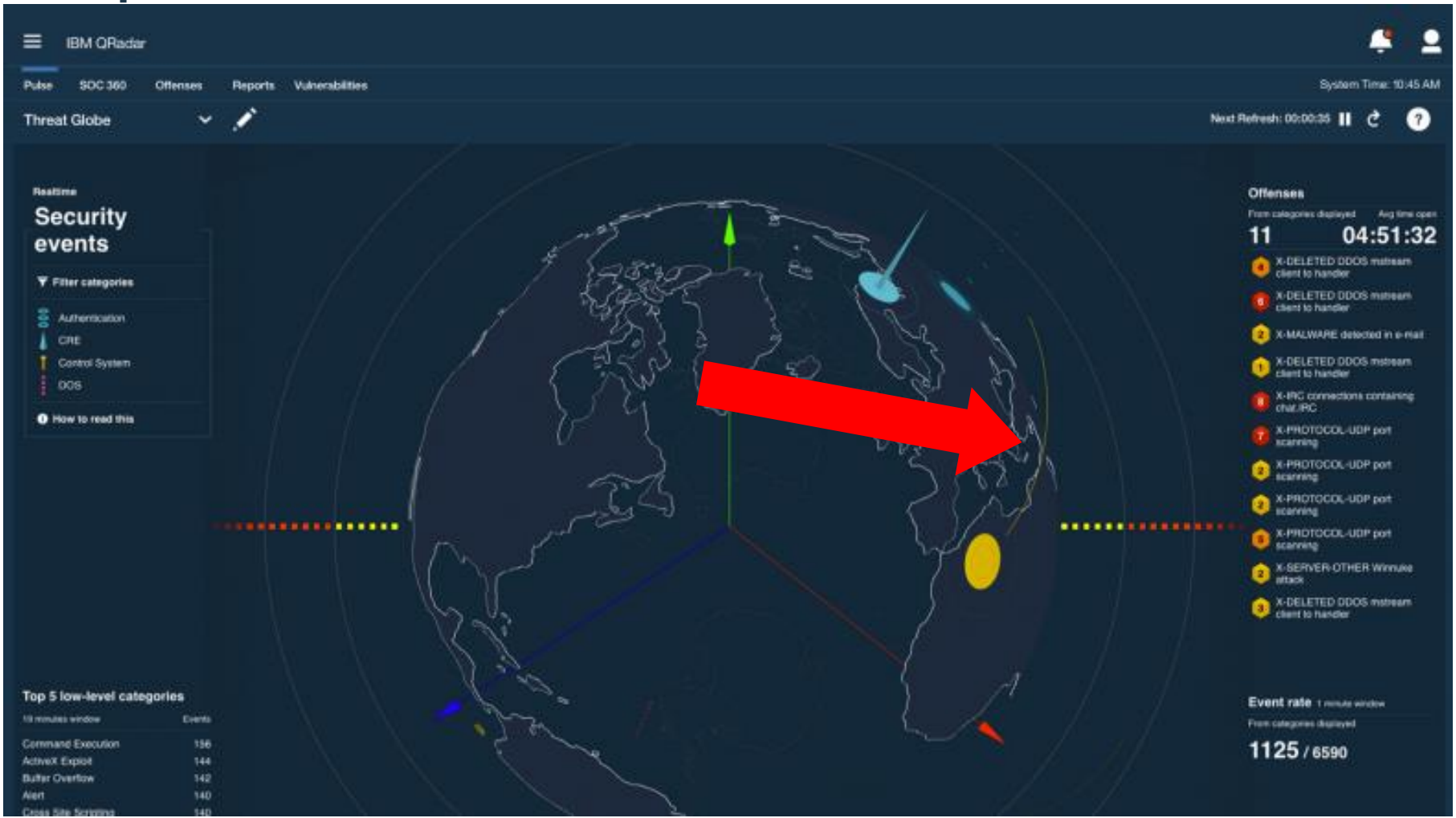
Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267

Integrierte Intelligenz bietet automatisierte Identifikation von Angriffen mittels SIEM (**S**ecurity **I**nformation and **E**vent **M**anagement) wie z. B. IBM QRadar



STIX: Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner.

Beispiel aus der Praxis:



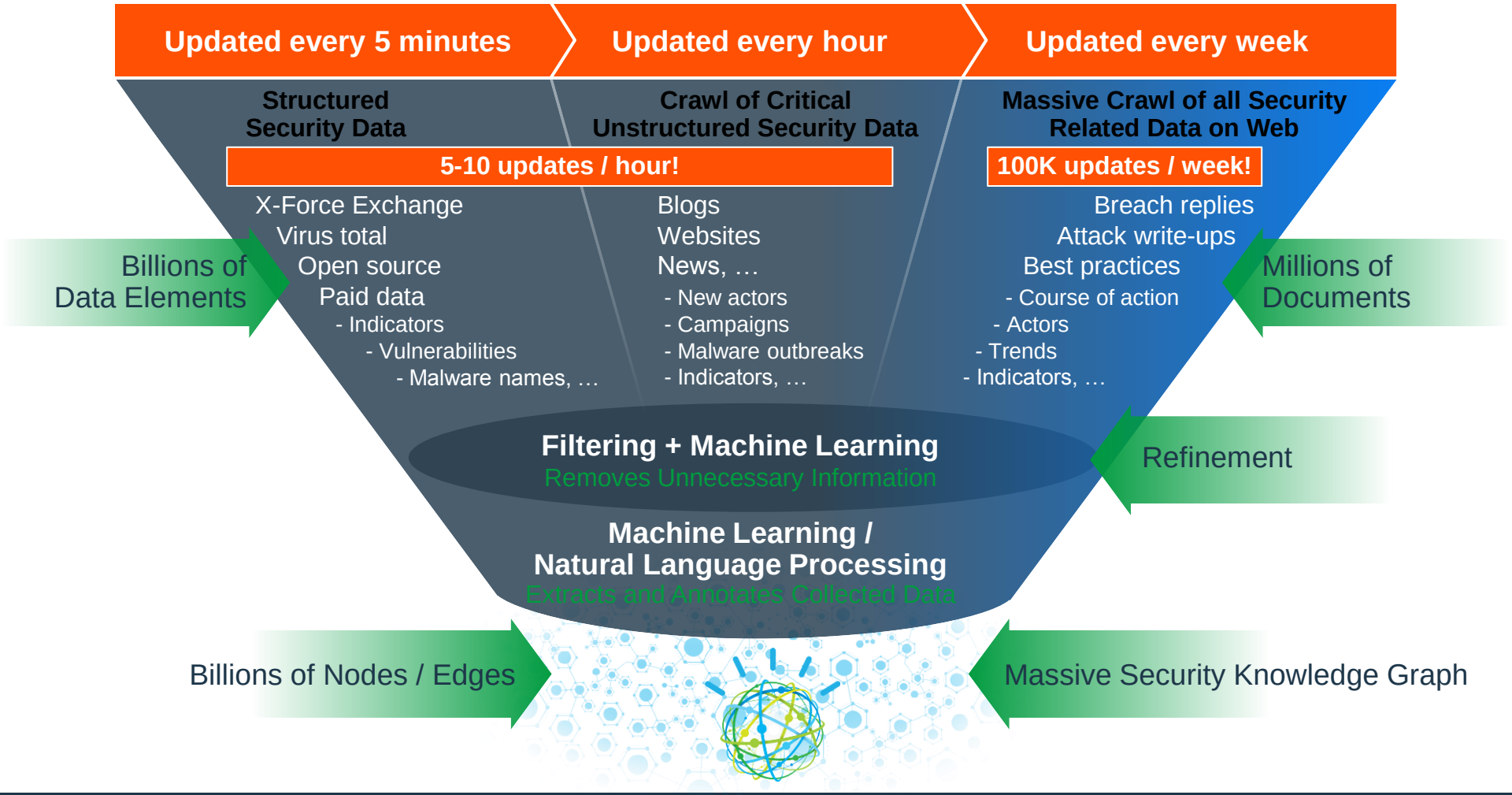
Die nächste Security-Ära

PERIMETER CONTROLS

INTELLIGENCE, INTEGRATION, and **ORCHESTRATION**

COGNITIVE, CLOUD, and **COLLABORATION**

IBM Watson for Cyber Security bildet die Basis für Cognitive Security



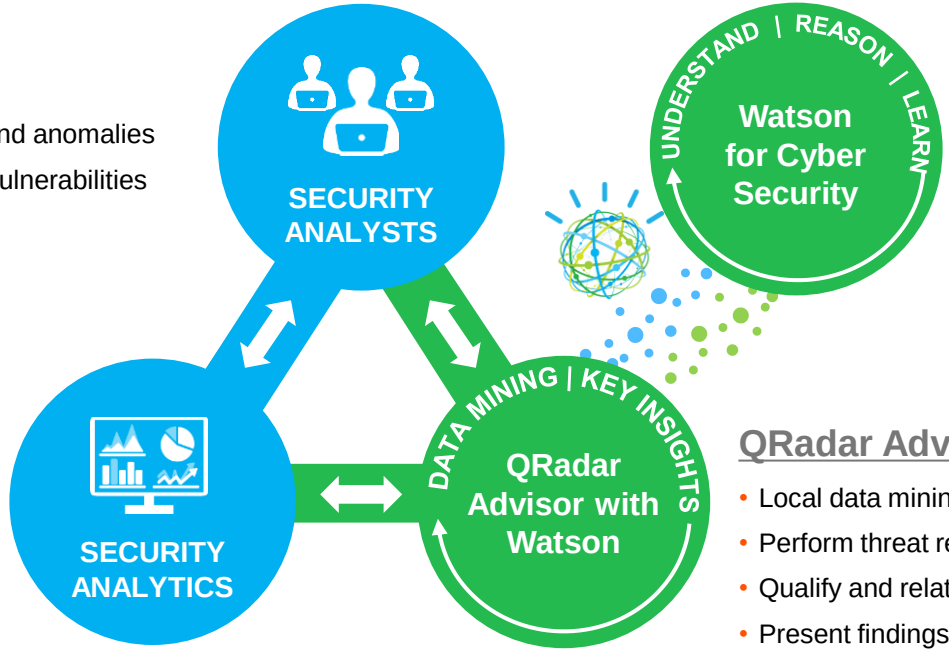
QRadar Advisor with Watson nutzt Watson for Cyber Security für die Analyse von erkannten Offenses

Security Analysts

- Manage alerts
- Research security events and anomalies
- Evaluate user activity and vulnerabilities
- Configuration
- Other

Security Analytics

- Data correlation
- Pattern identification
- Thresholds
- Policies
- Anomaly detection
- Prioritization



Watson for Cyber Security

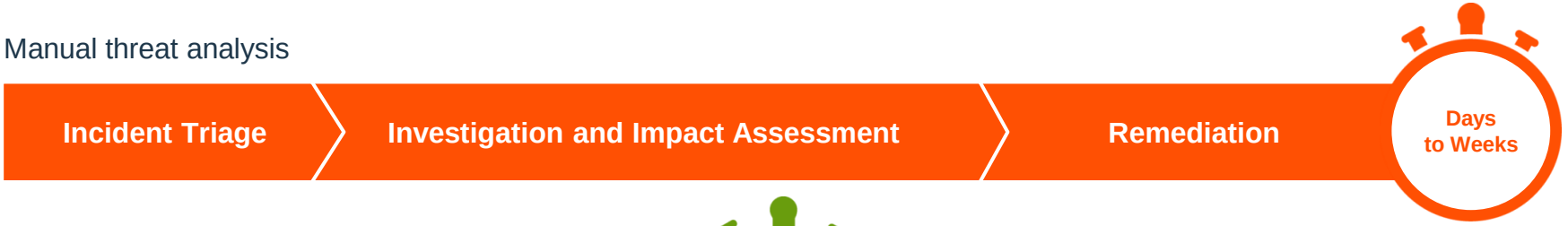
- Security knowledge
- Threat identification
- Reveal additional indicators
- Surface or derive relationships
- Evidence

QRadar Advisor with Watson

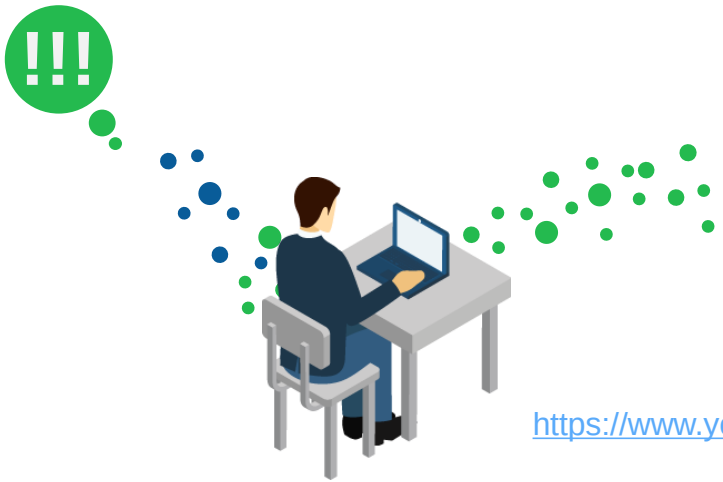
- Local data mining
- Perform threat research using Watson for Cyber Security
- Qualify and relate threat research to security incidents
- Present findings

Reduziert den Aufwand für die Untersuchung von Alarmen wesentlich

Manual threat analysis



QRadar Watson Advisor assisted threat analysis



Security Knowledge

Quick and accurate analysis of security threats, saving precious time and resources

- Accelerates incident triage with more automation
- Alleviates pressure of skills gap
- Augments contributions of security teams
- Empowers security analysts in clearing backlog

https://www.youtube.com/watch?v=MYZOIdK4o1M

IBM Security

THANK YOU

www.ibm.com/security

IBM