

Cyber Security

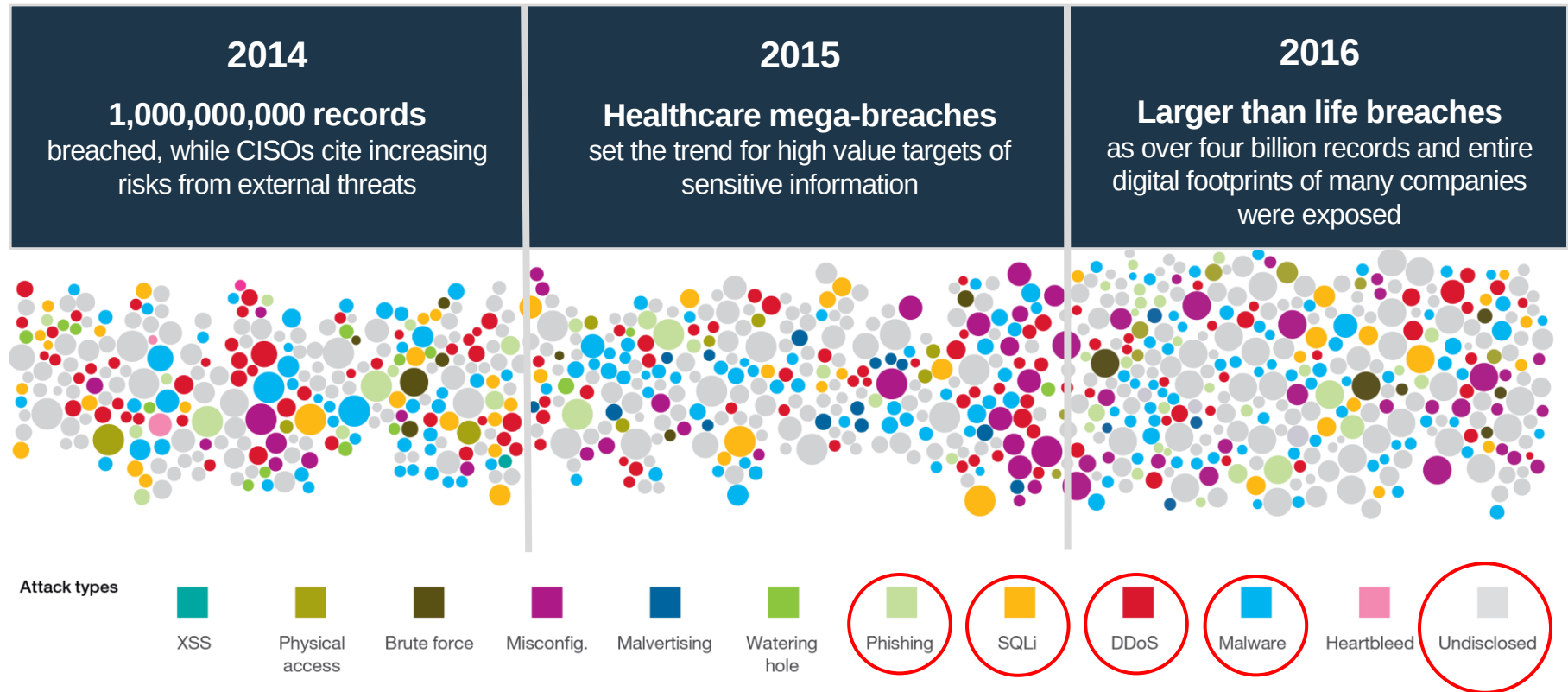
CYBER SECURITY CHALLENGES VON HEUTE –
WIE REAGIERT DIE INDUSTRIE DARAUF?

Bernhard Kammerstetter, Client Technical Professional

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



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:

Insider Threats



Advanced and Persistent Threats



Critical Data Protection



Secure the Cloud



Manage Risks and Vulnerabilities



Incident Response



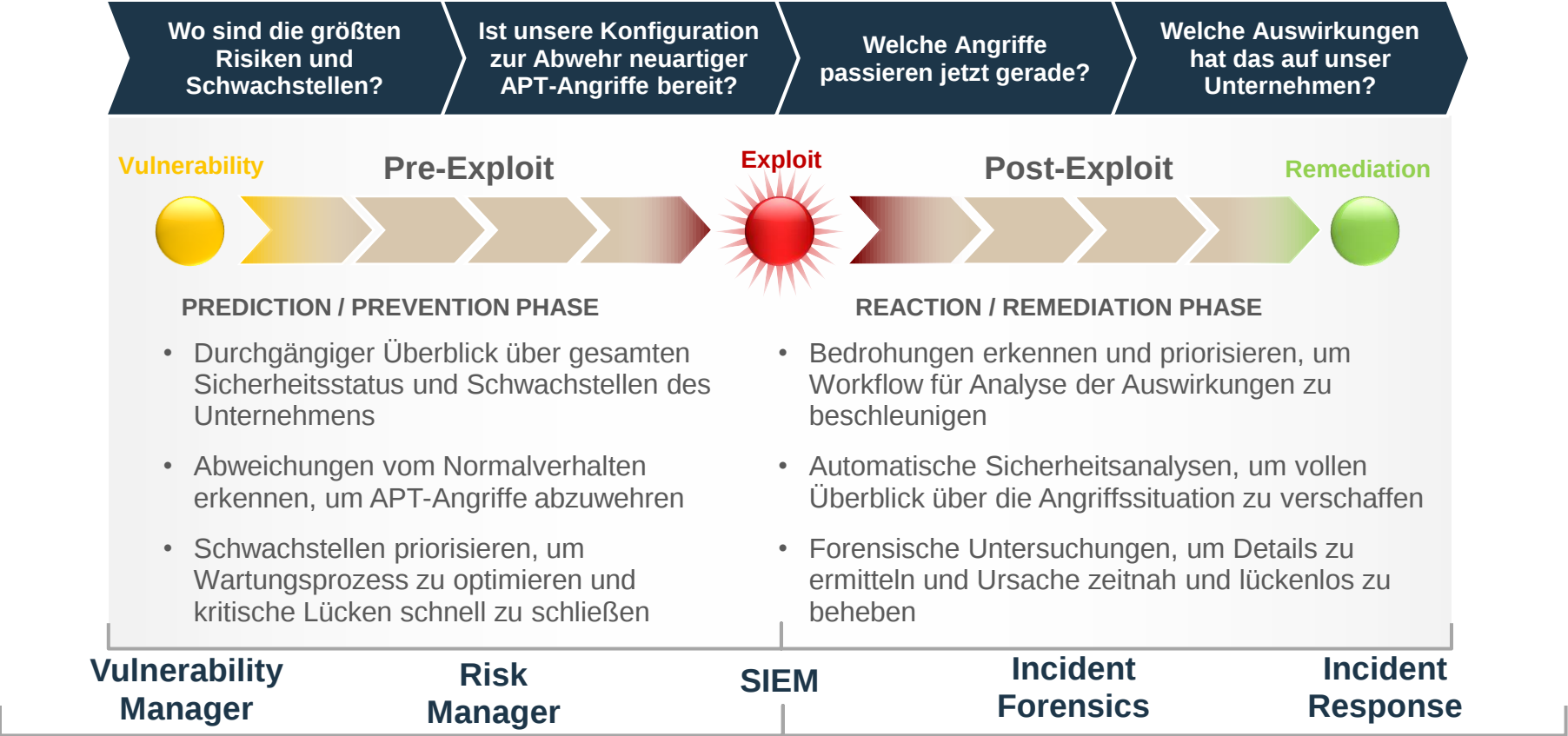
Compliance



Security-Herausforderungen steigen exponentiell*

Eskalierende Angriffe	Steigende Komplexität	Mangel an Experten
<i>Designer Malware</i> <i>Spear Phishing</i> <i>Persistence</i> <i>Backdoors</i> • Neue Angriffsmethoden, gezielt und trickreich • Perimeter verschwinden • Steigende Zahl an Sicherheitsvorfällen	 • Infrastruktur ändert sich laufend • Zu viele Produkte verschiedener Hersteller • steigende Kosten für Umsetzung und Betrieb • Ineffiziente Werkzeuge	 ITSecurityJobs.com Keine Bewerber gefunden • Überforderte Sicherheitsteams • Zu viele Daten für zu wenig Experten • Steigende Compliance Anforderungen

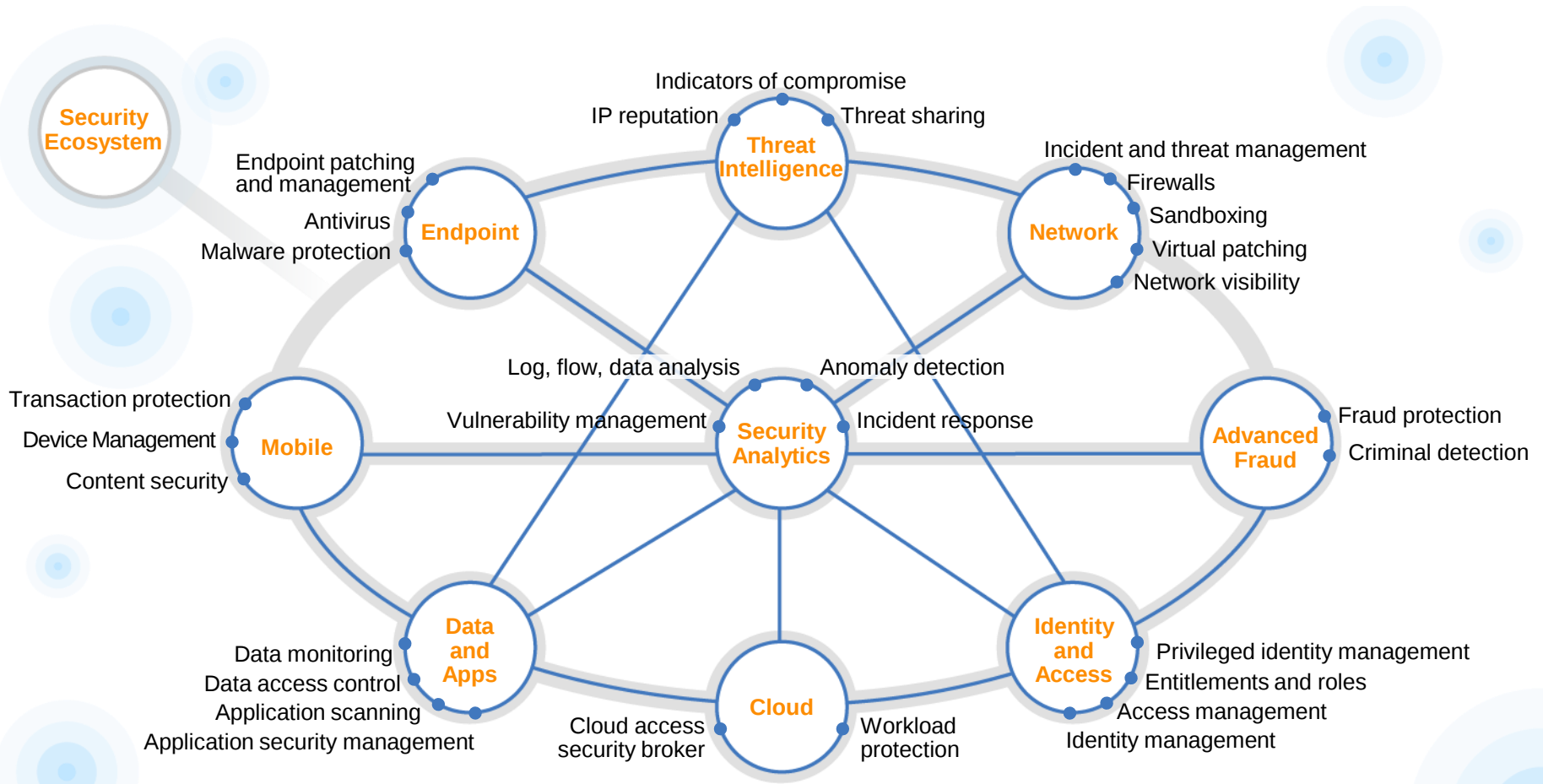
Die entscheidenden Fragen stellen ...



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

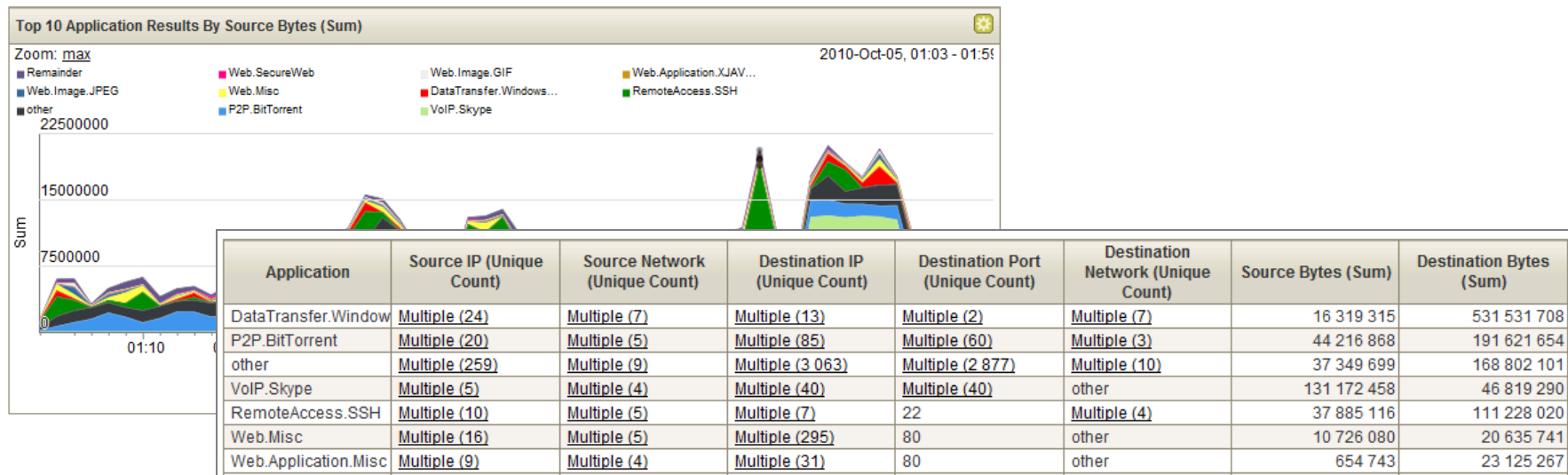
- Enterprise Management Associates

The good news:

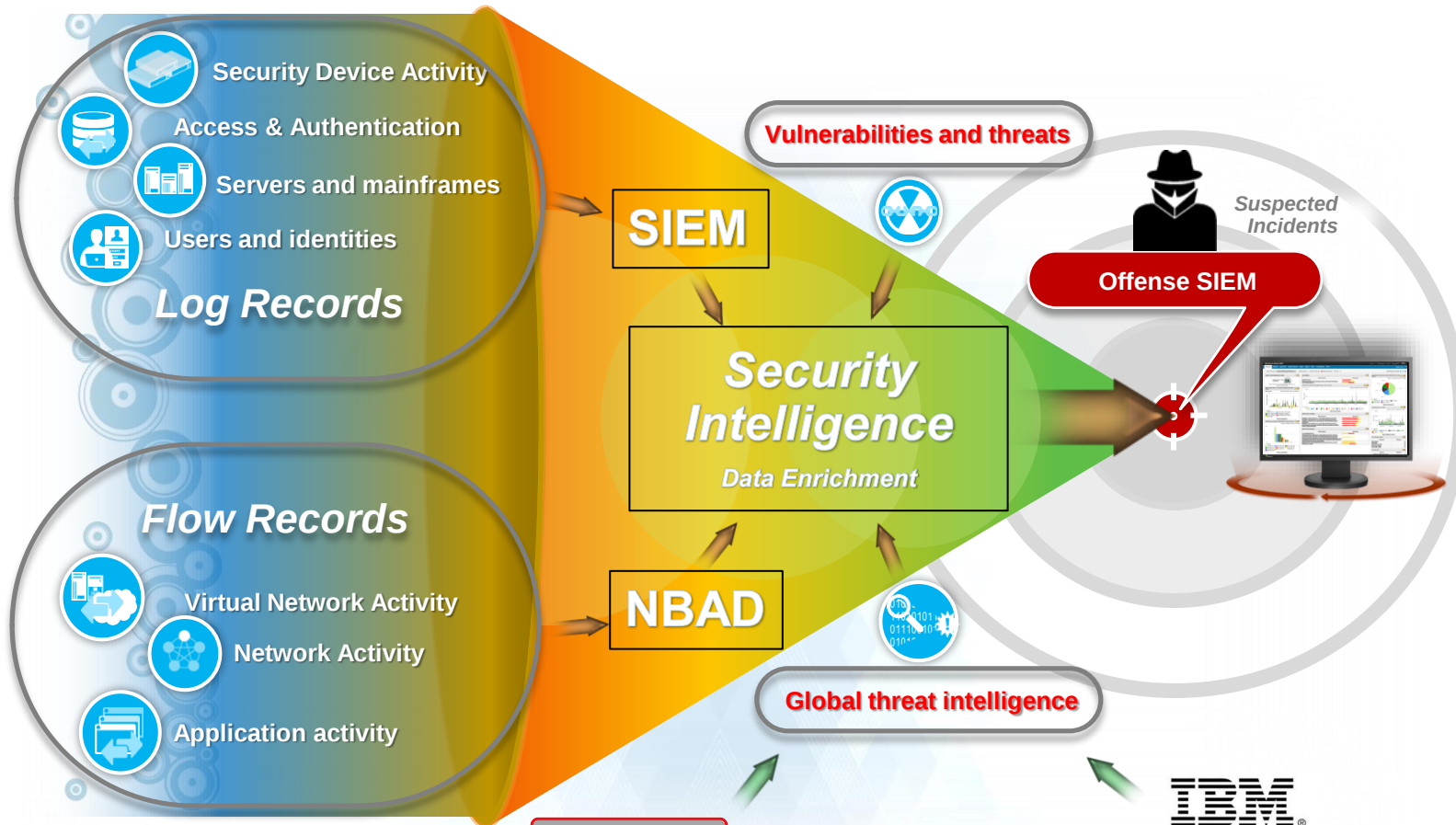
**Im Netzwerk finden sich die Daten,
die man für die Erkennung benötigt
... wenn man genau genug hinsieht**

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-Source für erweiterte Erkennung oder Forensics
- Hilft beim Erkennen von Anomalien, die ansonsten im Verborgenen bleiben
- Macht die Netzwerk-Aktivitäten von Angreifern sichtbar



Integrierte Intelligenz bietet automatisierte Identifikation von Angriffen mittels SIEM (Security Information and Event Management) wie z. B. IBM QRadar



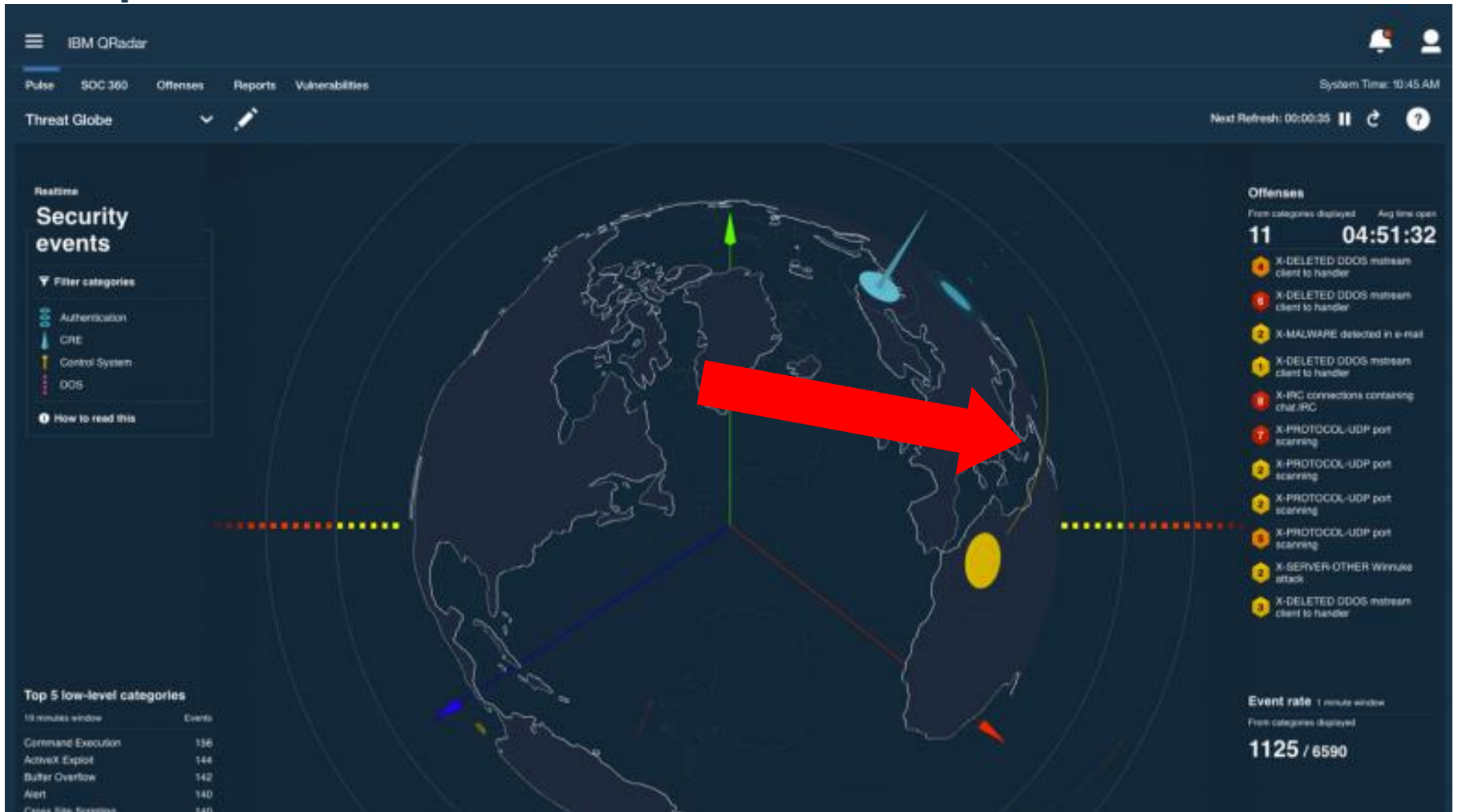
STIX: Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner.



<https://exchange.xforce.ibmcloud.com/>



Beispiel aus der Praxis:



Die nächste Security-Ära



**PERIMETER
CONTROLS**

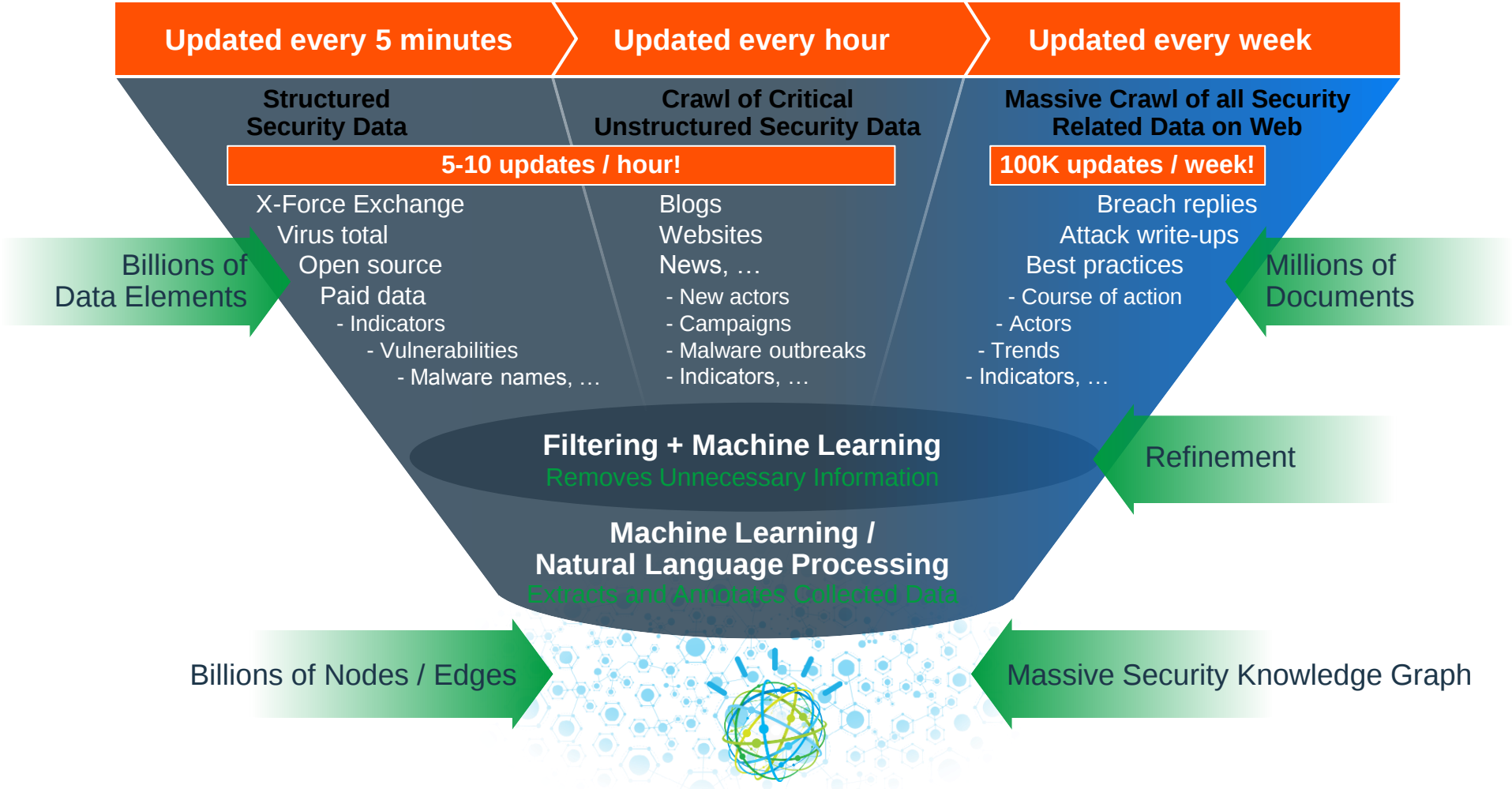


**INTELLIGENCE, INTEGRATION,
and ORCHESTRATION**



**COGNITIVE, CLOUD,
and COLLABORATION**

IBM Watson for Cyber Security bildet die Basis für Cognitive Security



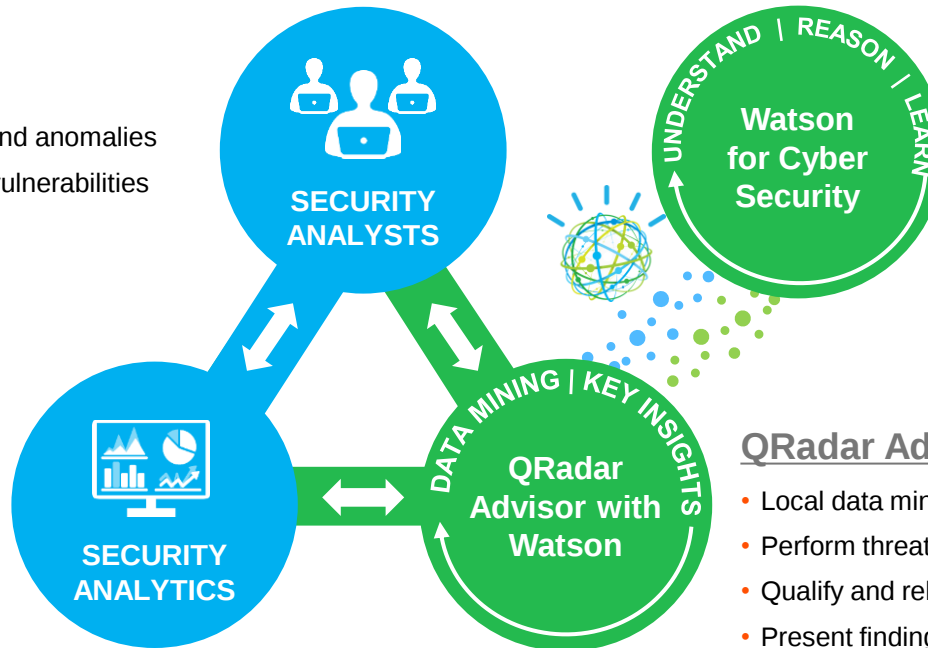
QRadar Advisor with Watson nutzt Watson for Cyber Security für die Analyse von erkannten Offenses

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



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>



THANK YOU

www.ibm.com/security

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

