IBM Security Systems

Trusteer Apex Live Demo

Christian Meßmer
Technical Sales
IBM Security Systems Division
Phone: +49-(0)172-6226165
E-Mail: christian.messmer@de.ibm.com

BUILD A SMARTER ENTERPRISE

With the power of social, mobile, cloud, big data & analytics.

Christian Meßmer
Technical Sales
IBM Security Systems Division
Phone: +49-(0)172-6226165
E-Mail: christian.messmer@de.ibm.com

Die Motivation für Angriffe ist vielfältig

Nationale Sicherheit

Staatliche Akteure
Stuxnet

Spionage, Aktivismus

Wettbewerber und Hacktivisten
Aurora

Monetärer Nutzen

Organisiertes Verbrechen
Zeus

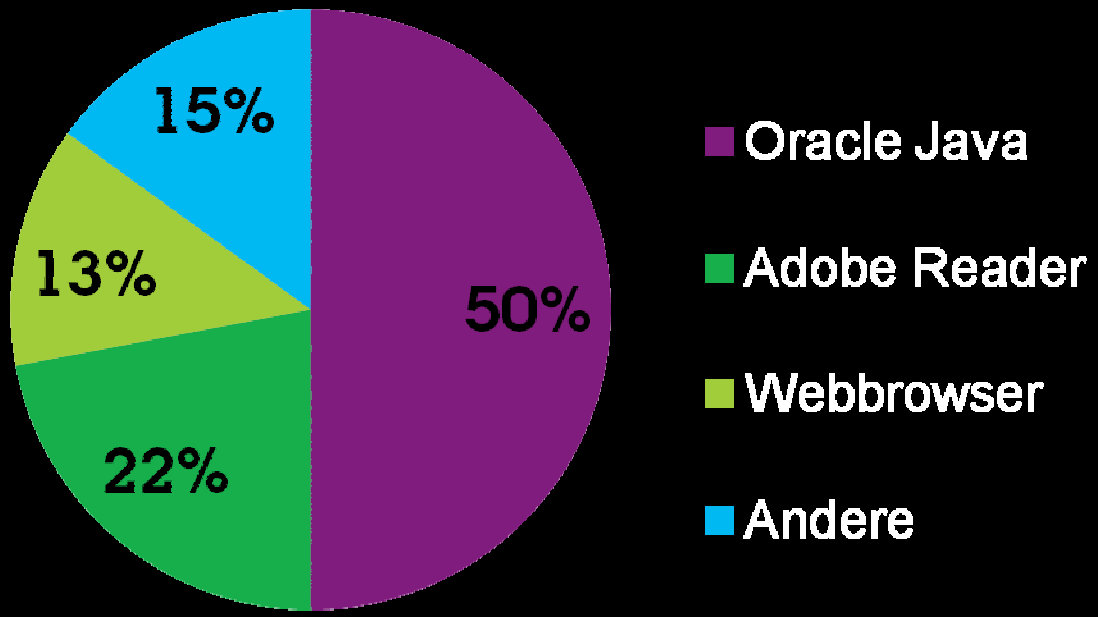
Rache, Neugierde

Insider und Script-kiddies
“I love you”

Was sehen wir heute?
IBM X-Force Threat Intelligence 1Q 2014 Report

Angriffe auf Anwendungen

Ergebnis einer Umfrage unter 1 Mio Trusteer Kunden, Dezember 2013



Quelle: IBM X-Force Research & Development

Was sehen wir heute?
IBM X-Force Threat Intelligence 1Q 2014 Report

5 am meisten angegriffene Branchen

Produktion	Finanzen & Versicherung	Informations-technologie	Gesundheit & Soziale Dienste	Einzel- & Großhandel
26.5 %	20.9 %	18.7 %	7.3 %	6.6 %

Advanced Persistent Threat ist die verbreiteste Methode der professionellen Hacker

Quelle: IBM X-Force Research & Development

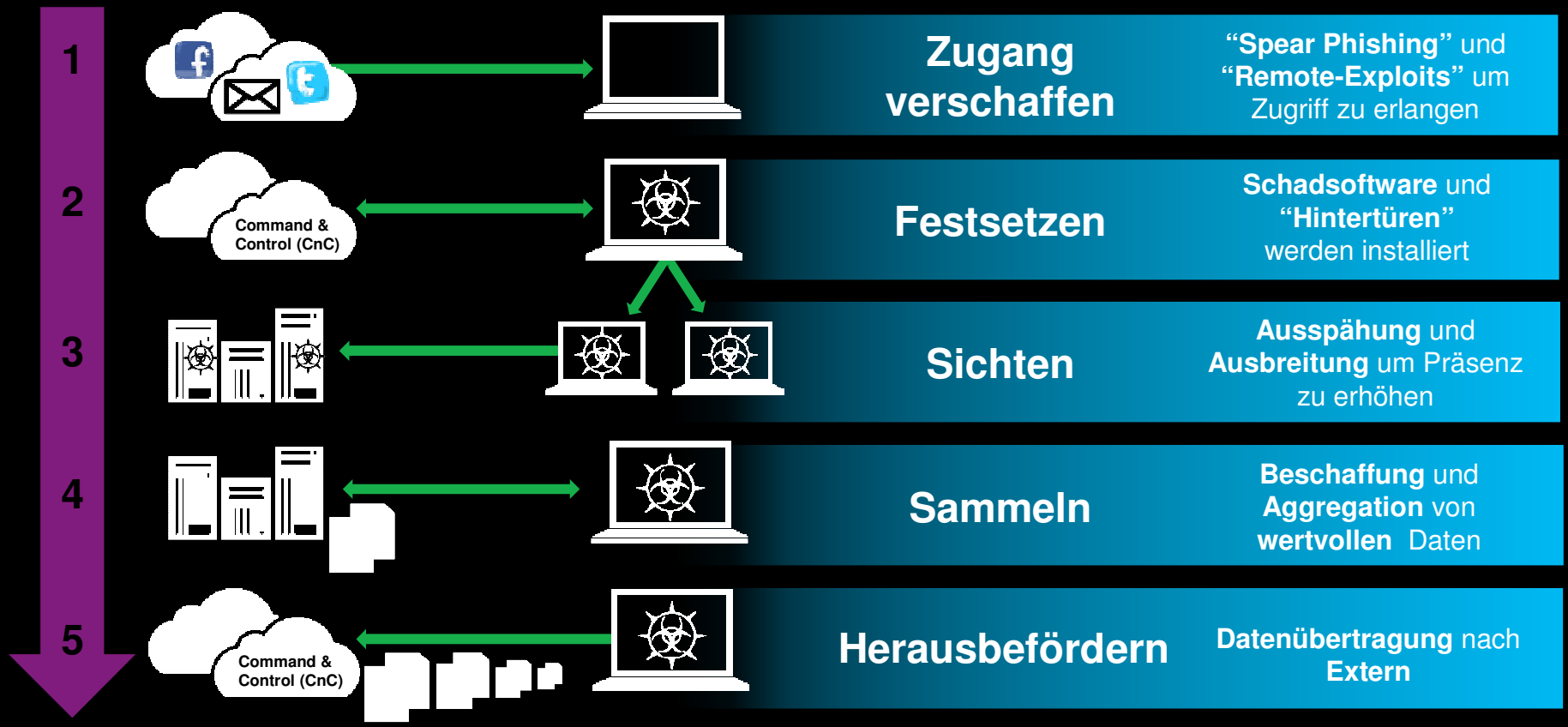
Was ist ein „Advanced Persistent Threat“?

1. Nutzt unbekannte (“**Zero-Day**”) Schwachstellen aus

2. Angriffe dauern **Monate** oder **Jahre**
(durchschnittlich: 1 Jahr, höchstens 4,8 Jahre)

3. Visiert **spezielle Personen** oder **Gruppen einer Organisation** an

Angreifer verfolgen eine 5-Phasen Attacke



Vorbereitende Recherchen

Identifizierung

Social Media zur Informationsgewinnung

Gläserne Identität
- Verhaltensweisen
- Bekanntschaften
- Kommunikations-präferenzen

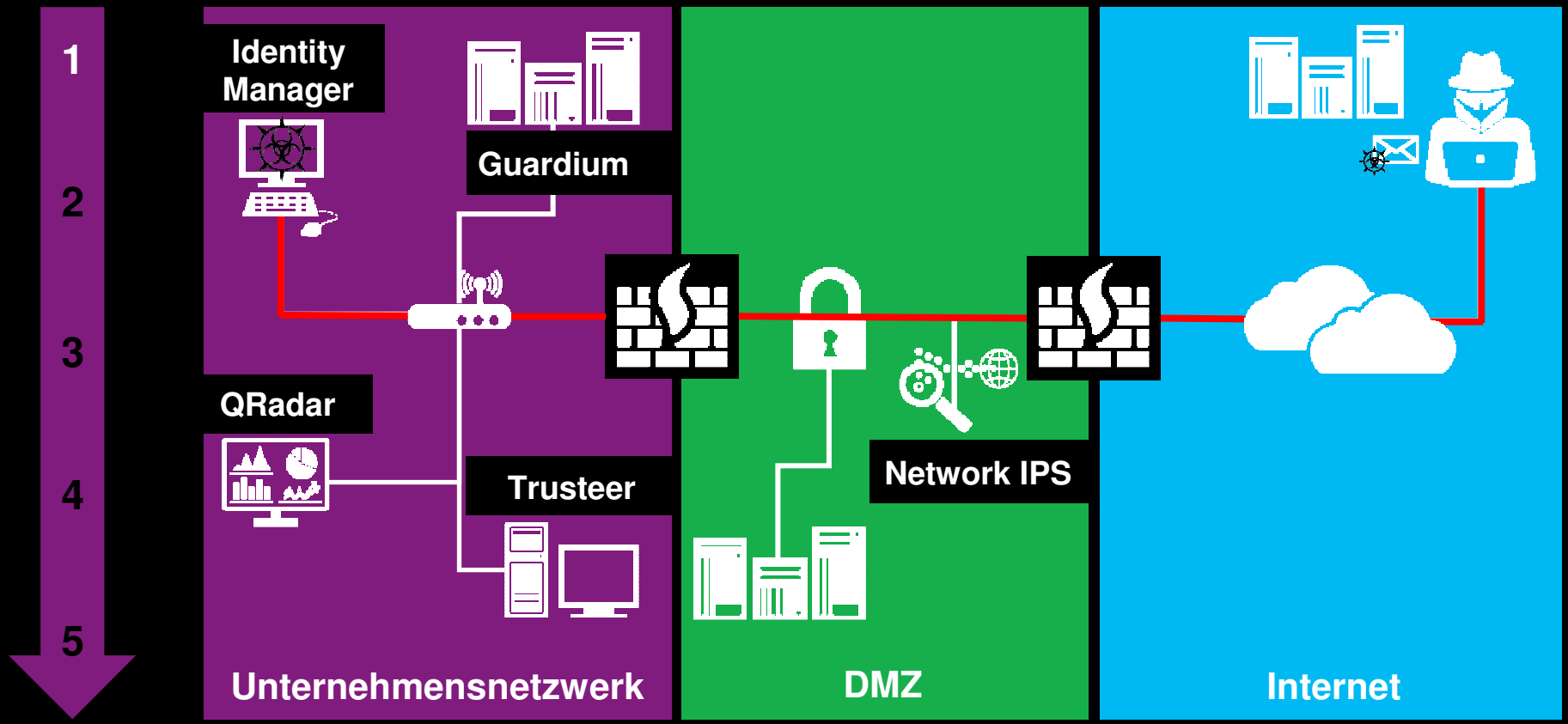
Profiling

Erstellung von **Personen-Profilen** auf Basis der **Social Media Informationen**

Kontaktaufnahme

Individuelle Kontaktaufnahme, die eine **Malware Falle** beinhaltet

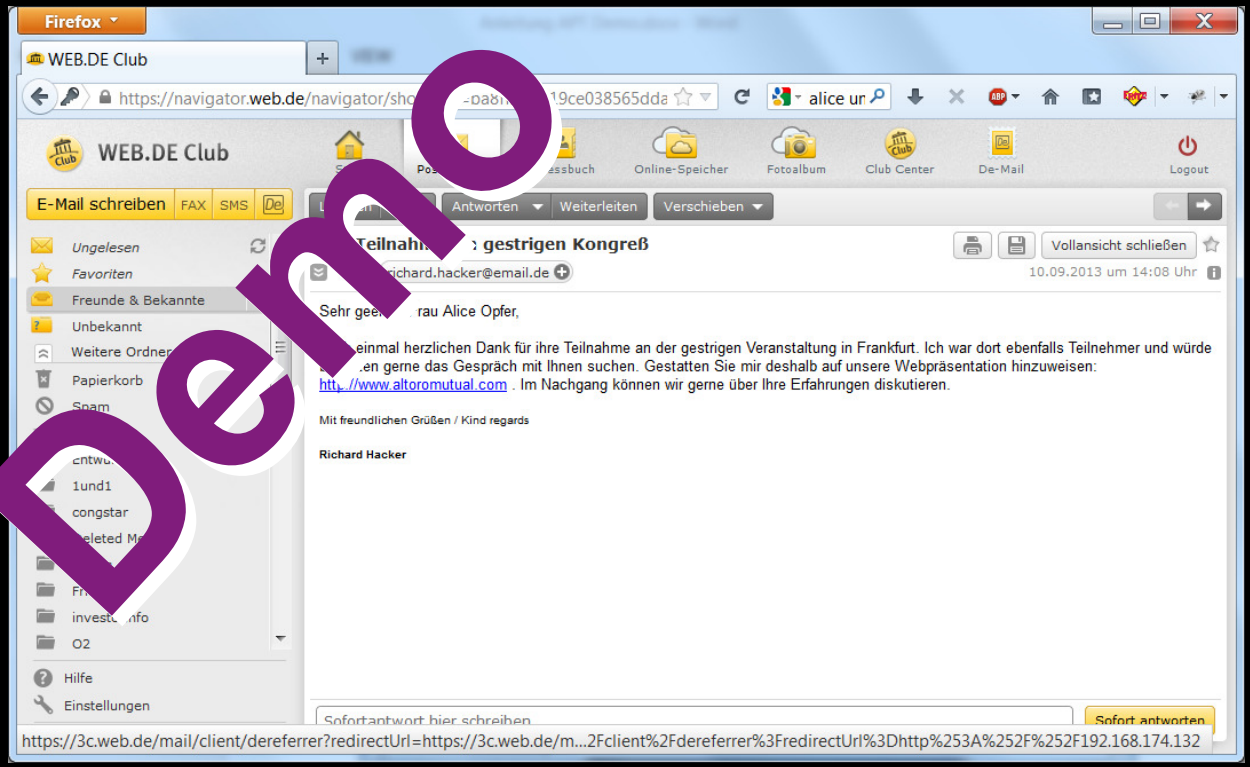
Angriffsszenario – Phase 1: Zugang verschaffen



Live Demo
Ablauf des Angriffs

Mail an das identifizierte Opfer

- Bekannter **Absender**
- Möglichst **allgemeingültige Aussage**
- Kommunikationsstil möglichst angenähert an die **normale Verhaltensweise**
- **Maskierte Links** oder **Anhänge**



Gegenmaßnahmen für Phase 1

Mailverkehr

IBM Protector
- URL-Analysen für Phishing- und Spyware-Erkennung

Aufruf des Links

IBM Security Network Protection, XGS
- Überwachung und mögliche Unterdrückung der Kommunikation

IBM QRadar
- Überwachung der Netzwerkkommunikation über Flow Analysis

IBM Trusteer Apex
- Anwendungsüberwachung

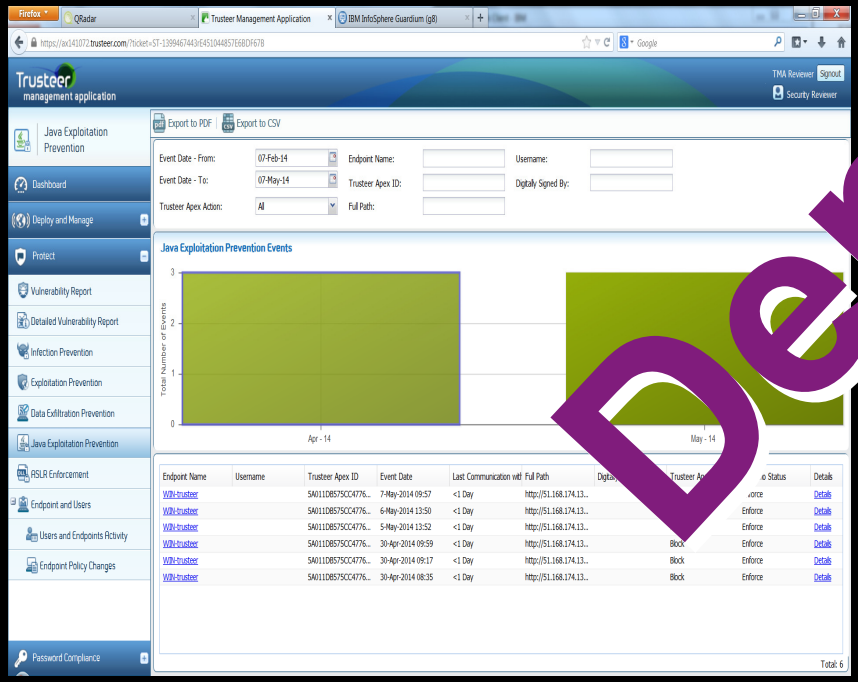
Vorbeugung & Reaktion

Awareness

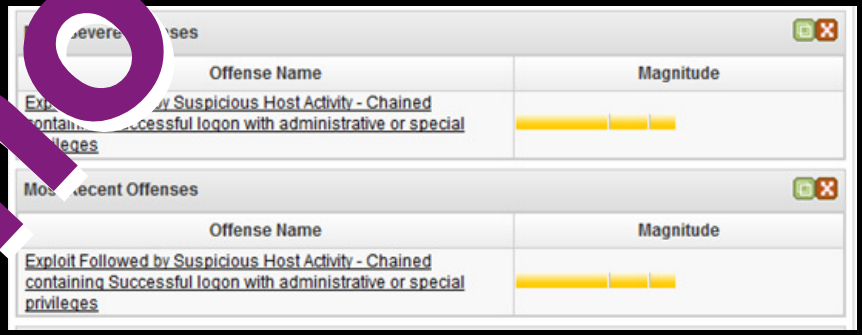
Etablierung vorbeugender Security-Policies im Unternehmen

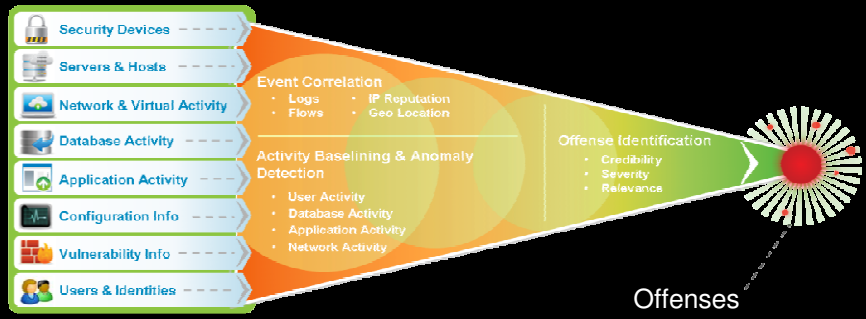
IBM Endpoint Manager
- Systems Management

IBM Trusteer APEX & QRadar Security Intelligence Platform

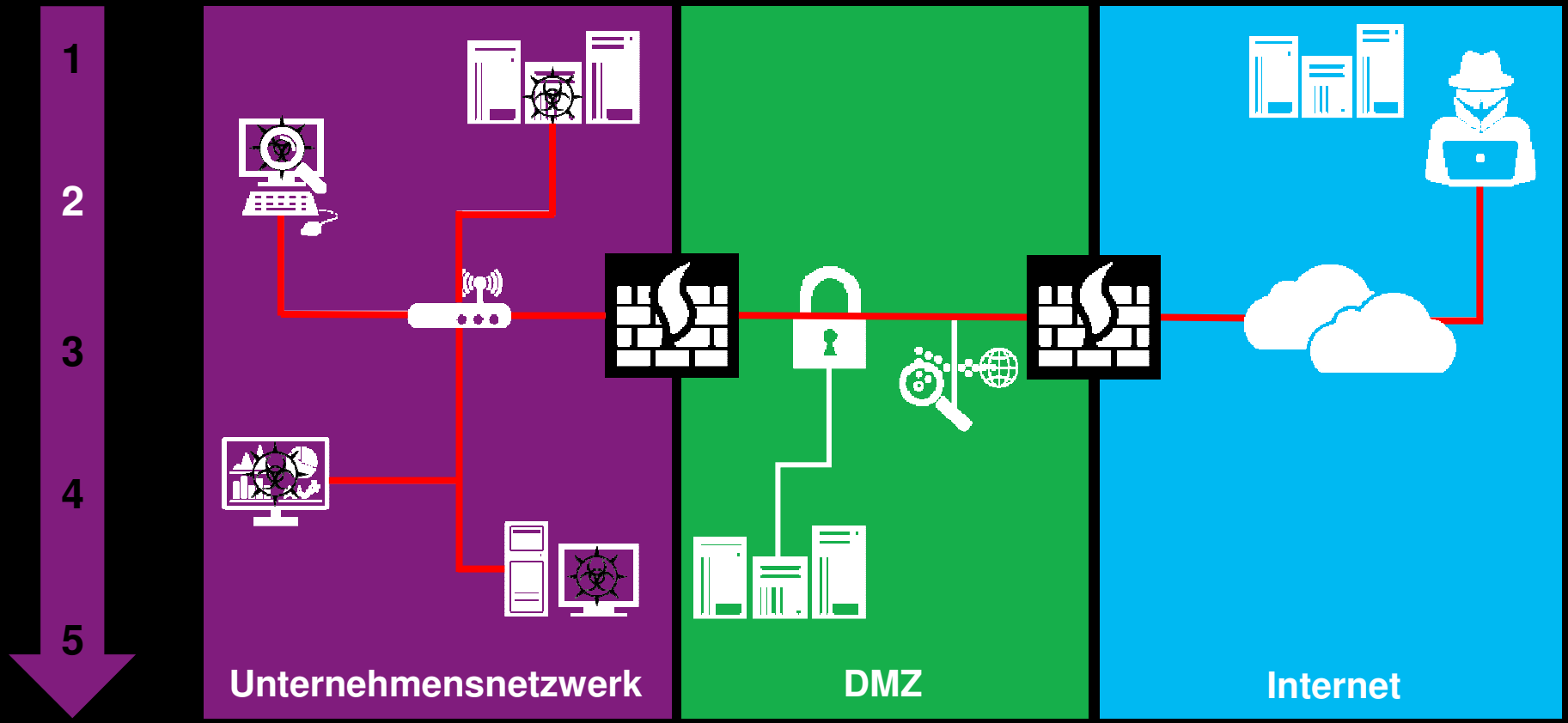


Demo

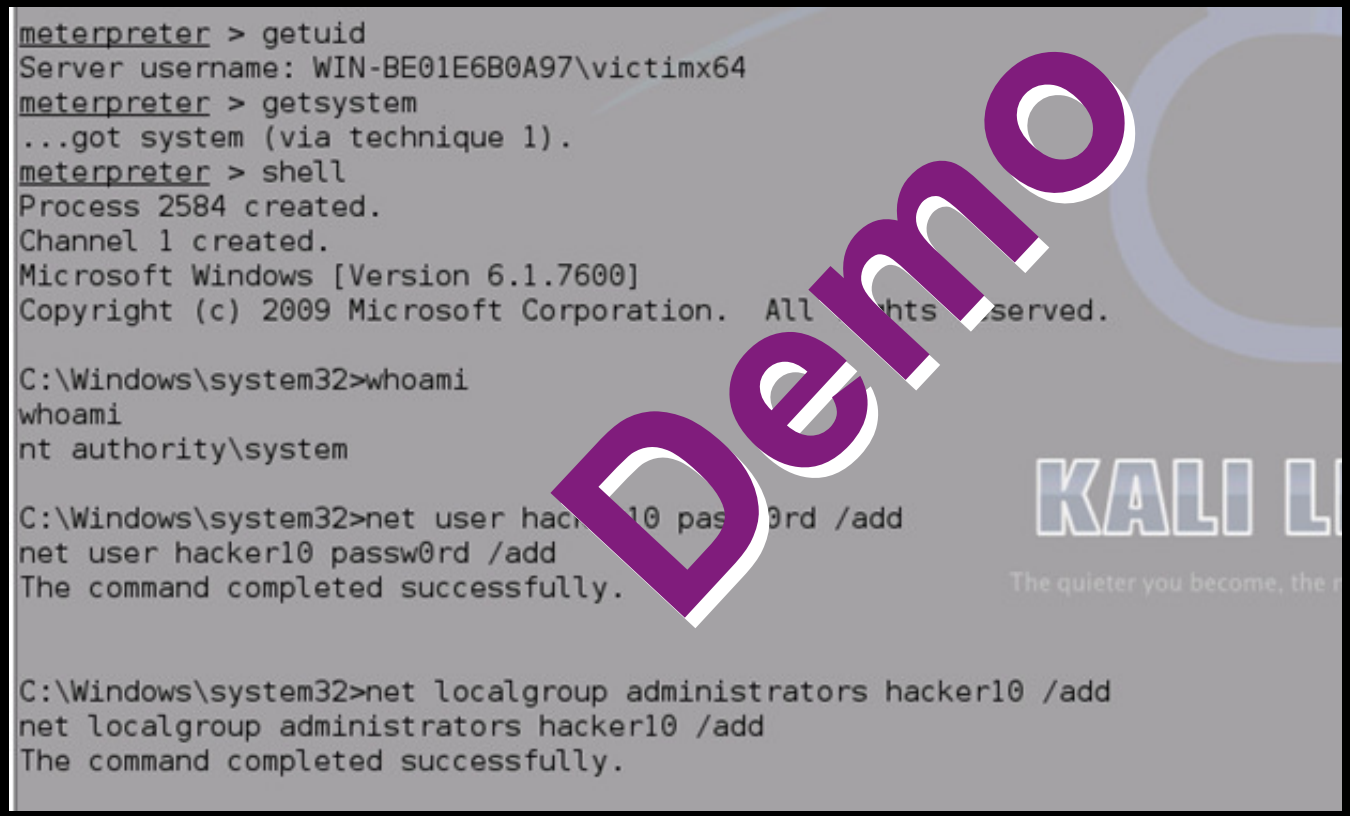




Angriffsszenario – Phase 2: Festsetzen



Anlegen weiterer Accounts



Gegenmaßnahmen für Phase 2

Netzwerkverkehr

IBM Security Network IPS

IBM QRadar Flow Analysis
- Erkennen von anomalem Verhalten und Vorgehen auf den Netzwerken

Systemen

IBM Identity Management
- Überwachung von Benutzern und unerlaubten Berechtigungsänderungen

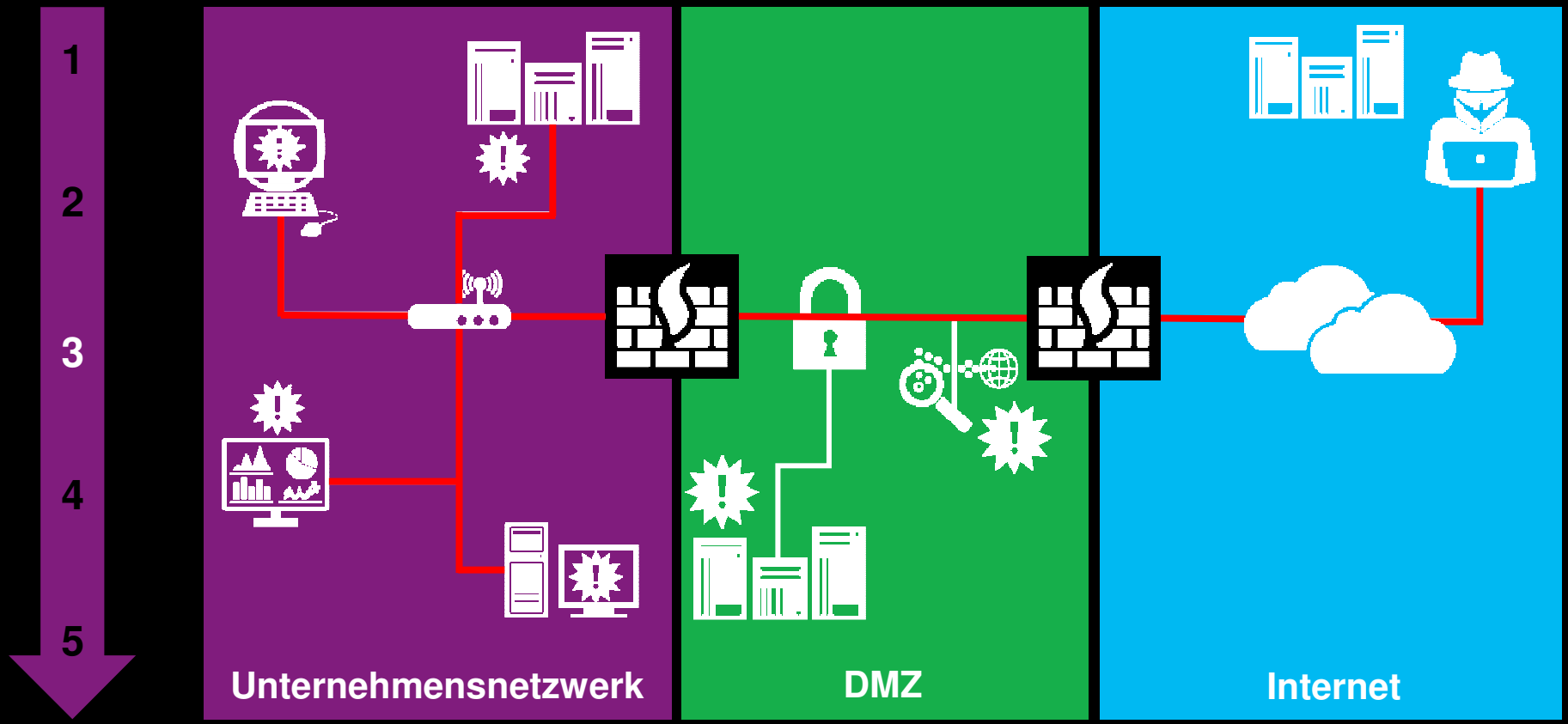
Vorbeugung & Reaktion

IBM Endpoint Manager
- Patch Management

Virenscanner
- Erkennen von kompromittierten Maschinen

Schwachstellen Management
- Absicherung unternehmensinterner Anwendungen

Angriffsszenario – Phase 3: Sichten



Scannen eines Servers nach aktivierten Diensten

```
Discovered open port 631/tcp on 172.17.96.209
Discovered open port 427/tcp on 172.17.96.209
Discovered open port 1521/tcp on 172.17.96.209
Discovered open port 5901/tcp on 172.17.96.209
Completed Connect Scan at 09:48, 53.54s elapsed (1000 total ports)
Nmap scan report for 172.17.96.209
Host is up (0.00090s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
389/tcp   open  ldap
427/tcp   open  svrloc
631/tcp   open  ipp
1521/tcp  open  oracle
5801/tcp  open  vnc-http-1
5901/tcp  open  vnc-1
50001/tcp open  unknown

Read data files from: C:\hackertools
Nmap done: 1 IP address (1 host up) scanned in 53.82 seconds
```

Demo

Gegenmaßnahmen für Phase 3

Netzwerkverkehr

Netzwerksegmentierung
- Verhindert das Scannen großer Teile des Unternehmensnetzwerks

Systeme

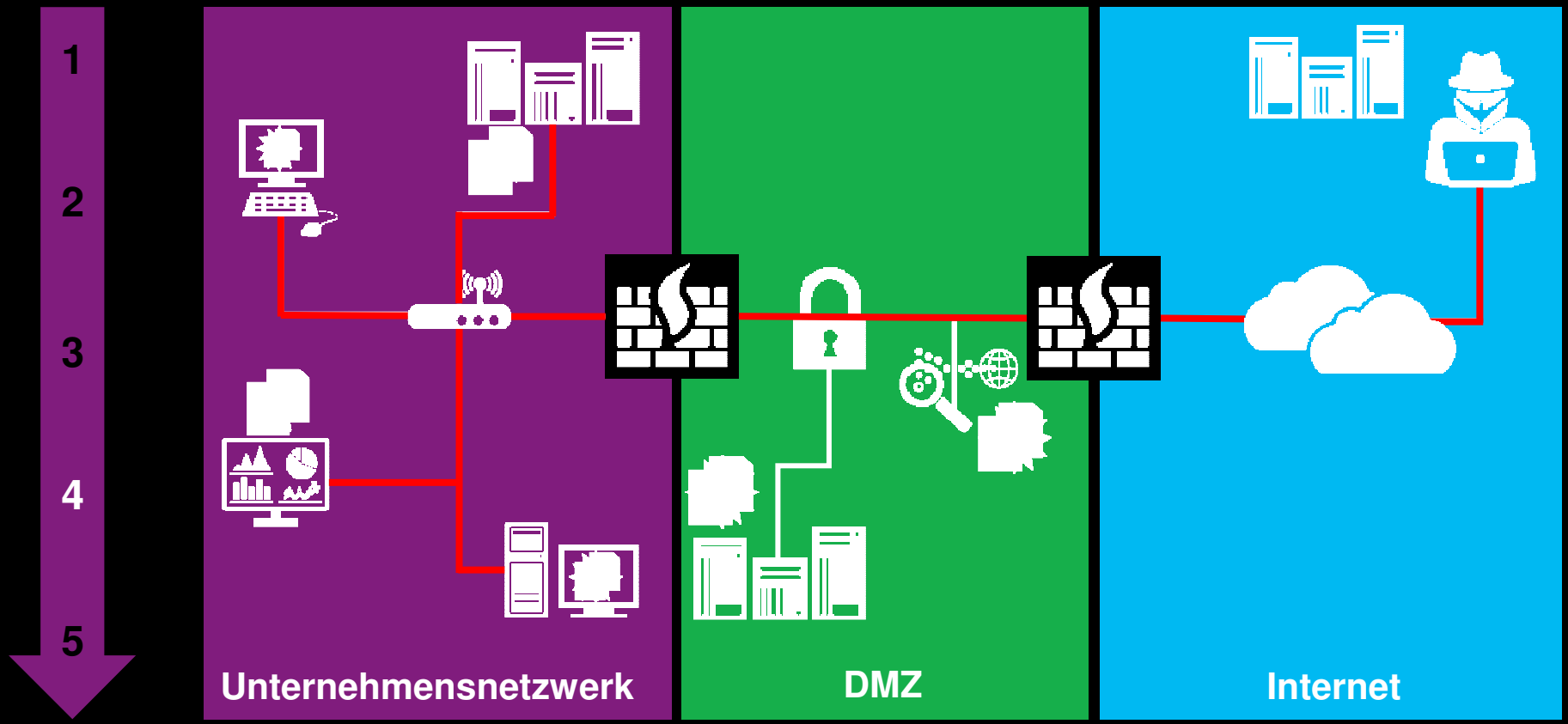
IBM Access Management
- Blockieren von unerlaubtem Abspeichern von Dateien auf den Endgeräten

Vorbeugung & Reaktion

IBM Endpoint Manager
- Patch Management

Policies
- Eingeschränkte Nutzung von Ports und Kommunikations-Protokollen

Angriffsszenario – Phase 4: Sammeln



Datenbank-Abfragen mittels gestohlener Zugangsdaten

```
Connected to:
Oracle Database 11g Express Edition Release 11.2.[illegible] - 64bit Production

SQL> select firstname, lastname, cardnumber from [illegible]editcard where rownum < 10;

FIRSTNAME       LASTNAME                  CARDNUMBER
--------------- ------------------------- -------------------------
Tom             Jones                     [illegible]7890126276
Tom             Craven                    [illegible]4567890126277
Tom             Shapiro                   1234567890126278
Tom             King                      1234567890126279
Tom             Lynch                     1234567890126280
Tom             Williams                  1234567890126281
Tom             Davis                     1234567890126282
Tom             Wilson                    1234567890126283
Tom             Miller                    1234567890126284

9 rows selected.

SQL>
```

Demo

Gegenmaßnahmen für Phase 4

Datenbanken

IBM Guardium
- Entdecken und Unterbinden von unberechtigten SQL-Abfragen
- Logging, Terminierung und Quarantäne der SQL-Kommunikation

„Separation of Duties“

Systeme

IBM QRadar
- Anomalie-Erkennung für direkte Dateizugriffe

Vorbeugung & Reaktion

Überwachung des Netzwerk-Datenverkehrs
- Anomale File-Transfers

Was passiert bei aktiver, gezielter Blockierung durch Guardium?

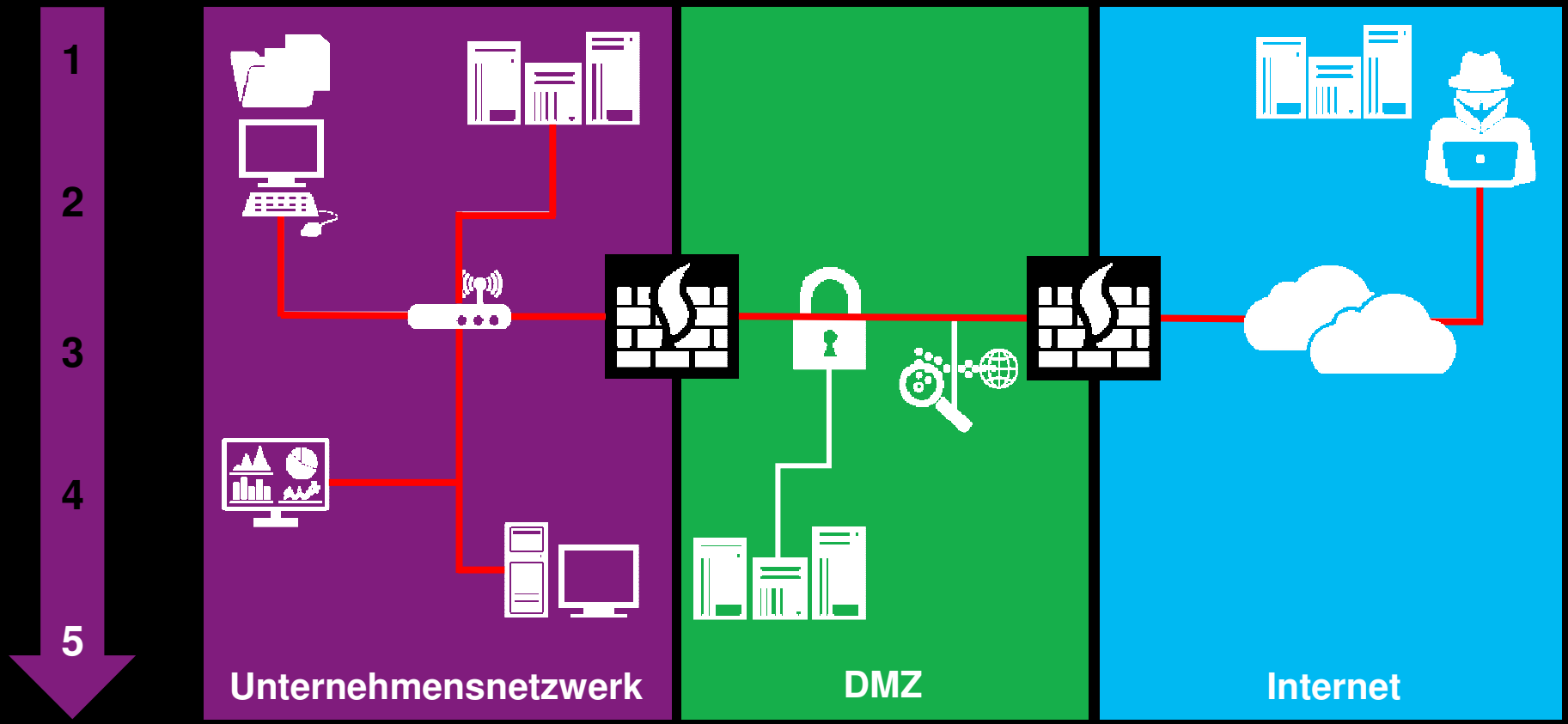
Angreifer hat **keine Chance** auf **sensitive** Objekte zuzugreifen

```
Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL> select firsname, lastname, cardnumber from joe.creditcard;
select firsname, lastname, cardnumber from joe.creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel
Process ID: 6073
Session ID: 32 Serial number: 15


SQL>
```

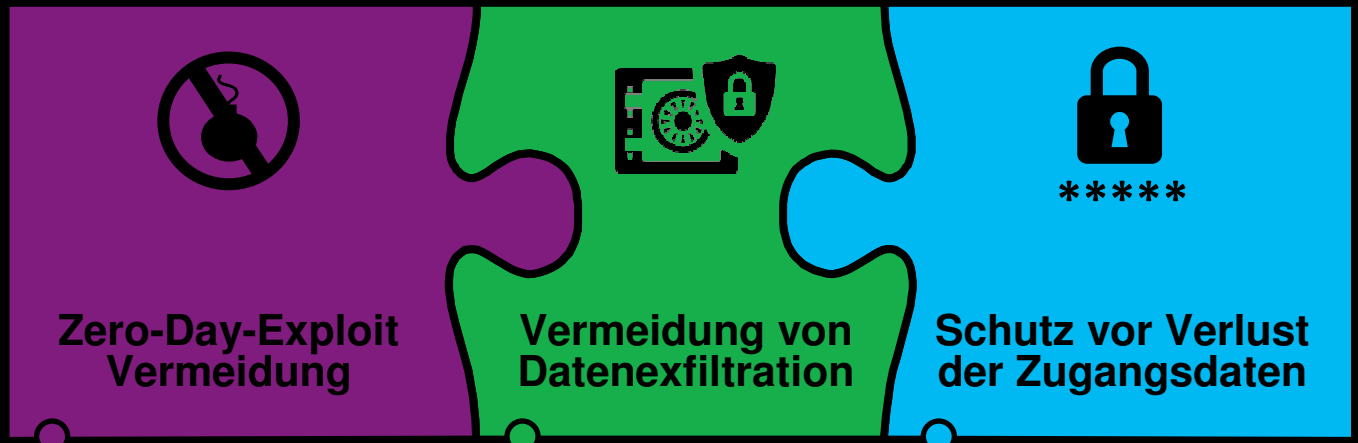
Angriffsszenario – Phase 5: Herausbefördern



Gegenmaßnahmen für Phase 5

Netzwerkverkehr	Systemen	Vorbeugung & Reaktion
IBM QRadar ▪Verdeckte Datenströme anzeigen mit QFlow Analyse **Data-Loss-Prevention (DLP) Systeme**	**IBM Trusteer Apex** ▪Verhindert unerwünschten Kommunikationsaufbau nach Außen	**Vorbeugende Kommunikations-Regeln**

IBM Trusteer Apex

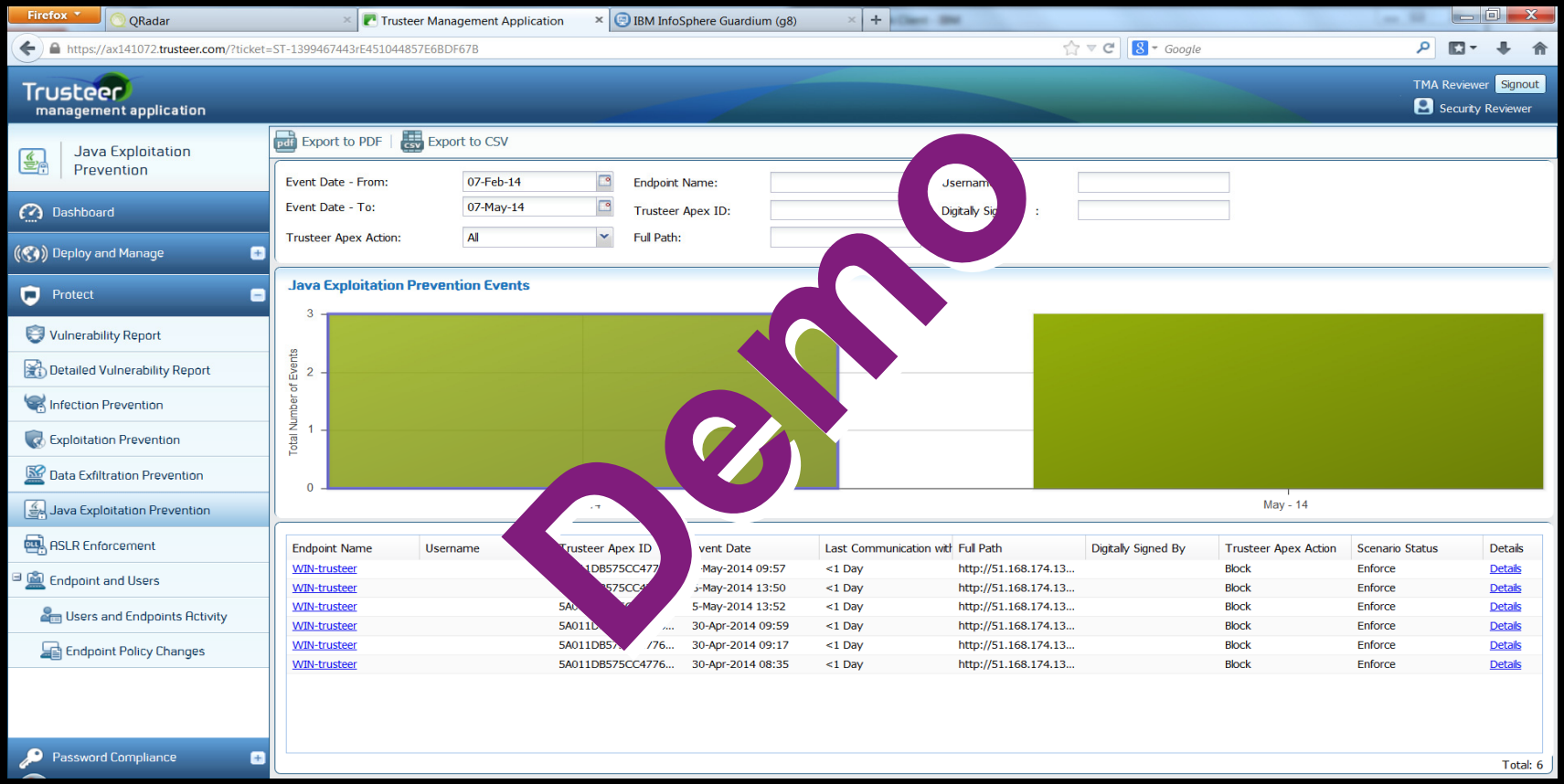


- Stoppt die **Ausnutzung von Schwachstellen** in Applikationen
- Verhindert das **unbewusste Herunterladen** von Schadsoftware

- Blockt die **Kommunikation** von Malware
- Verhindert Informations-diebstahl

- Blockt Key-Loggers
- Verhindert die **Eingabe von Zugangsdaten** auf Phishingseiten

Trusteer APEX Security Administration Dashboard



IBMs Ansatz zur Abwehr von Dynamischen Angriffen

1	**Zugang verschaffen**	**Network and Endpoint Security** Nutzt adaptiven Angriffsschutz und Endgeräte-Management, um Risiken zu reduzieren und Angriffe abzuwehren
2	**Festsetzen**	**Network Security** Nutzt SIEM und adaptiven Angriffsschutz zur Identifizierung sowie Hinderung der Angreifer, Schadsoftware zu installieren
3	**Sichten**	**Secure Users** Sicheres Identitätsmanagement erzwingt Zugriffsrichtlinien & Überwachungen, um verdächtiges Verhalten aufzudecken
4	**Sammeln**	**Data Security** Tief integrierte Sicherheitsschranken im Datenarchiv und Datenaktivitäten-Überwachung
5	**Herausbefördern**	**Network and System Security** Proaktive Überwachung des Netzwerks; Echtzeit-Blockaden

Security Analytics

Durch “Security Intelligence” werden **Aktivitäten** im gesamten Unternehmen **geprüft, analysiert und korreliert**

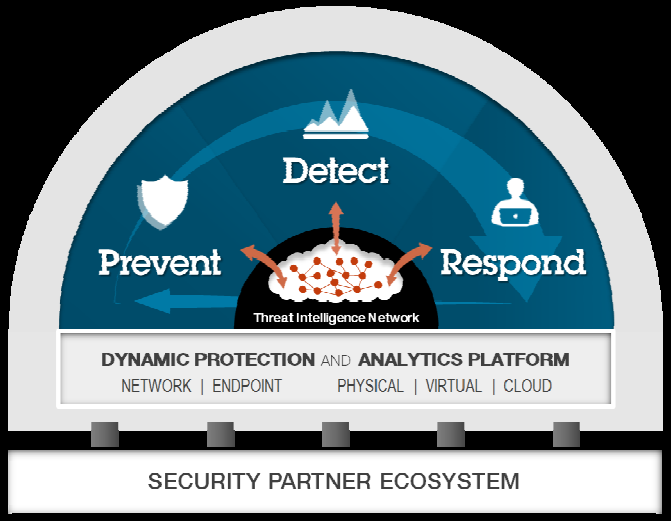
Erweiterung um **Big Data** Kapazitäten, um **unstrukturierte Daten** zu analysieren

Klare Anweisungen und Hinweise im Falle eines Angriffs oder versuchten Datendiebstahls

IBM Threat Protection System

Ein **dynamisches**, **integriertes System** um fortschrittliche Angriffe zu unterbrechen und vor Datendiebstahl zu schützen

Prevent. Detect. Respond.



Die Roadmap von Morgen

Bedeutende Investitionen in 10 Entwicklungslabore um Schutz vor fortschrittlichen Bedrohungen zu liefern

Einzigartige Integration

Strategischer Fokus auf der Integration und der intelligenten Verbindung der IBM Security Produkte

Neue Partnerschaft

Industrieübergreifender Koordination zur Produktzusammenführung für unsere Kunden

IBM Security Systems Portfolio

Security Intelligence and Analytics

QRadar SIEM	QRadar Log Manager	QRadar Risk Manager	QRadar Vulnerability Manager	QRadar Incident Forensics

Advanced Fraud Protection

Trusteer Rapport	Trusteer Pinpoint Malware Detection	Trusteer Pinpoint ATO Detection	Trusteer Mobile Risk Engine

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity Management	Guardium Database Security	AppScan Source	Network Intrusion Prevention	Trusteer Apex
Access Management	Guardium Database Security	AppScan Dynamic	Next Generation Network Protection	Mobile & Endpoint Management
Privileged Identity Manager	Guardium / Optim Data Masking	DataPower Web Security Gateway	SiteProtector Threat Management	Virtualization and Server Security
Federated Access and SSO	Key Lifecycle Manager	Security Policy Manager	Network Anomaly Detection	Mainframe Security

IBM X-Force Research

IBMs „Keep in Mind“

Security Intelligence.
Think Integrated.

1. **Motivation** für Angriffe hat sich geändert

2. **Dynamische Angriffe** ist die am meisten verbreitete Methode der professionellen Hacker

3. **IBM QRadar & Trusteer**

Vielen Dank

Kontaktdaten

Christian Meßmer
Technical Sales
IBM Security Systems Division
Phone: +49-(0)172-6226165
E-Mail: christian.messmer@de.ibm.com