Angewandtes SIEM bei der Kapo Zürich

Severin Mathis *IT Sicherheitsbeauftragter, Kantonspolizei Zürich*

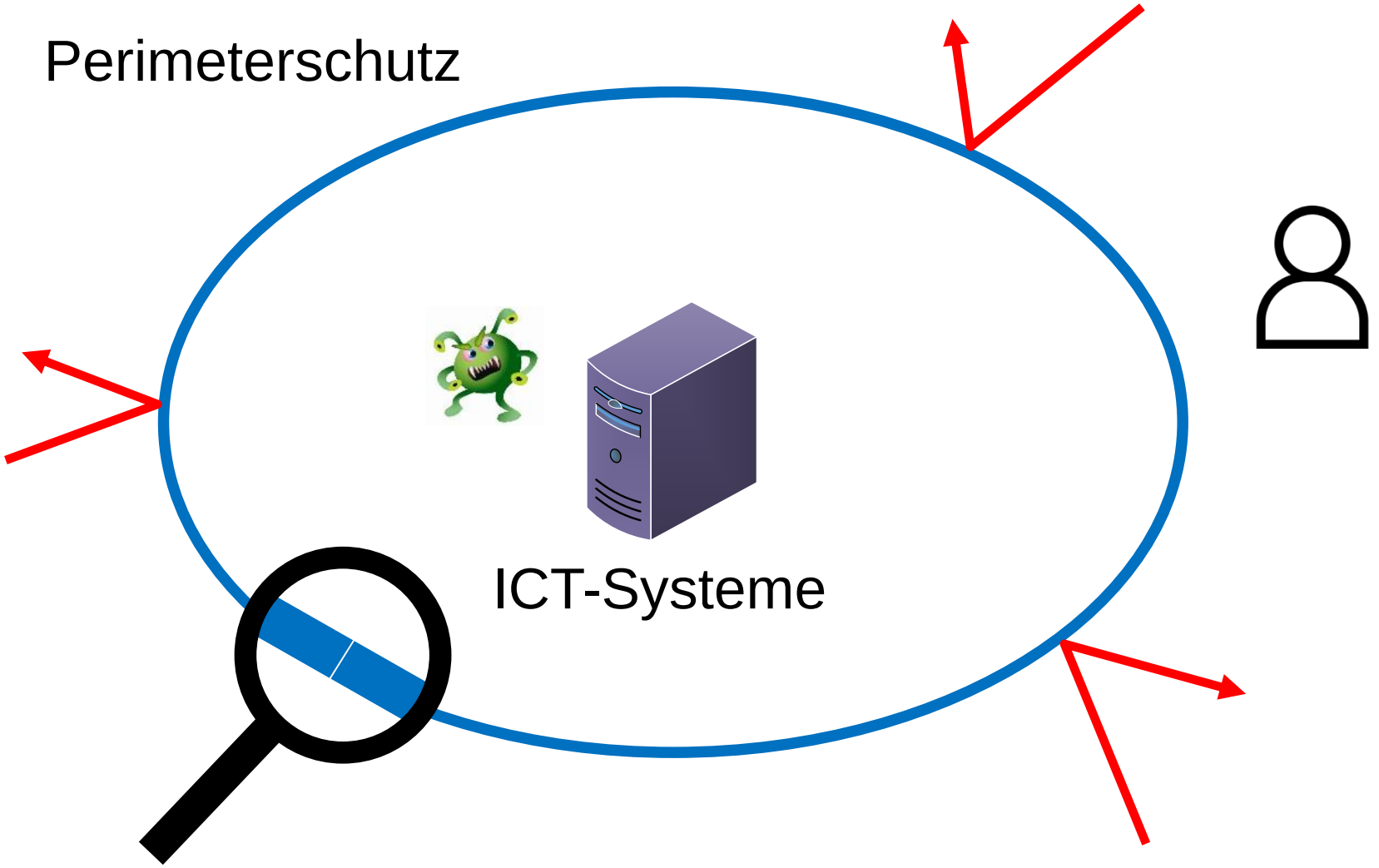
Anton Brauchli *Solution Architekt, Abraxas Informatik AG*

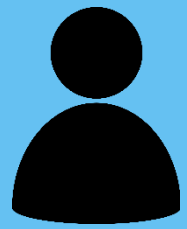
SPIK 2017, Stade de Suisse, Bern
30.03.17

Agenda

- Motivation
- Umsetzung
- Resultate / Ausblick

Vorhandene Gefahren





Erfolgreiche Angriffe

Kantonspolizei Zürich

Hackerangriff in Tschechien

Datendiebe bespitzeln Prags Diplomaten

von Ivo Mijnssen / 3.2.2017, 14:11 Uhr

Ein Jahr lang haben Unbekannte Tausende von heiklen Dokumenten unbemerkt aus dem tschechischen Aussenministerium gestohlen. Die Regierung verdächtigt Russland – und spinnt gleichzeitig Intrigen.

Cyber-Spionage-Angriff auf Ruag

Mehr als 20 Gigabyte Daten entwendet

von Nadine Jürgensen / 23.5.2016, 11:06 Uhr

Vom Hackerangriff auf die Ruag sind wahrscheinlich Daten der E-Mail-Software der Bundesverwaltung betroffen. Das Leck über den Hackerangriff hat eine weitere Beobachtung der Angreifer vereitelt.

Ein Jahr lang haben Unbekannte Tausende von heiklen Dokumenten unbemerkt gestohlen.

Gemäss den Experten des Bundes könne es bei solchen Angriffen bis zur Erkennung der schädlichen Software **sehr lange** dauern…

Gezielte Angriffe auf Verwaltungen

Kantonspolizei Zürich

Regierungsrat;
Baudirektor

Von: "markus.kaegi@bd.zh.ch" <markus.kaegi@mail.com>
An: [redacted]@bd.zh.ch
Datum: 16.01.2017 11:48
Betreff: Wichtig

Baudirektion des
Kantons Zürich

Hallo Herr [redacted],

ich möchte Sie persönlich beauftragen, die Bearbeitung einer vertraulichen Finanztransaktion zu übernehmen.
Ich bin davon überzeugt, dass Sie die durch uns in dieser Angelegenheit beauftragten Rechtsanwälte der Kanzlei KMPG, insbesonderes Fr. Dr. Schmid

Hat Fr, Dr. Schmid Sie bereits kontaktiert?

Mit freundlichen Grüßen
Markus Kägi

Von meinem iPhone gesendet

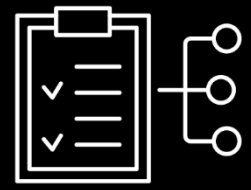
Übersicht

Kantonspolizei Zürich

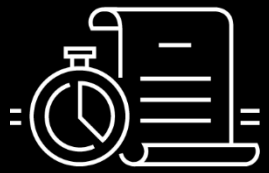
Erwartungen

Erfolgsdefinition

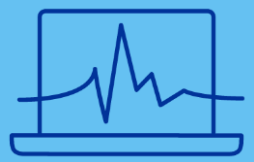
Abgrenzungen



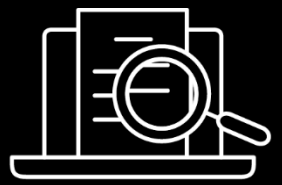
Machbarkeit



Zeitrahmen



Testumgebung



Auswertungen

Ergebnis

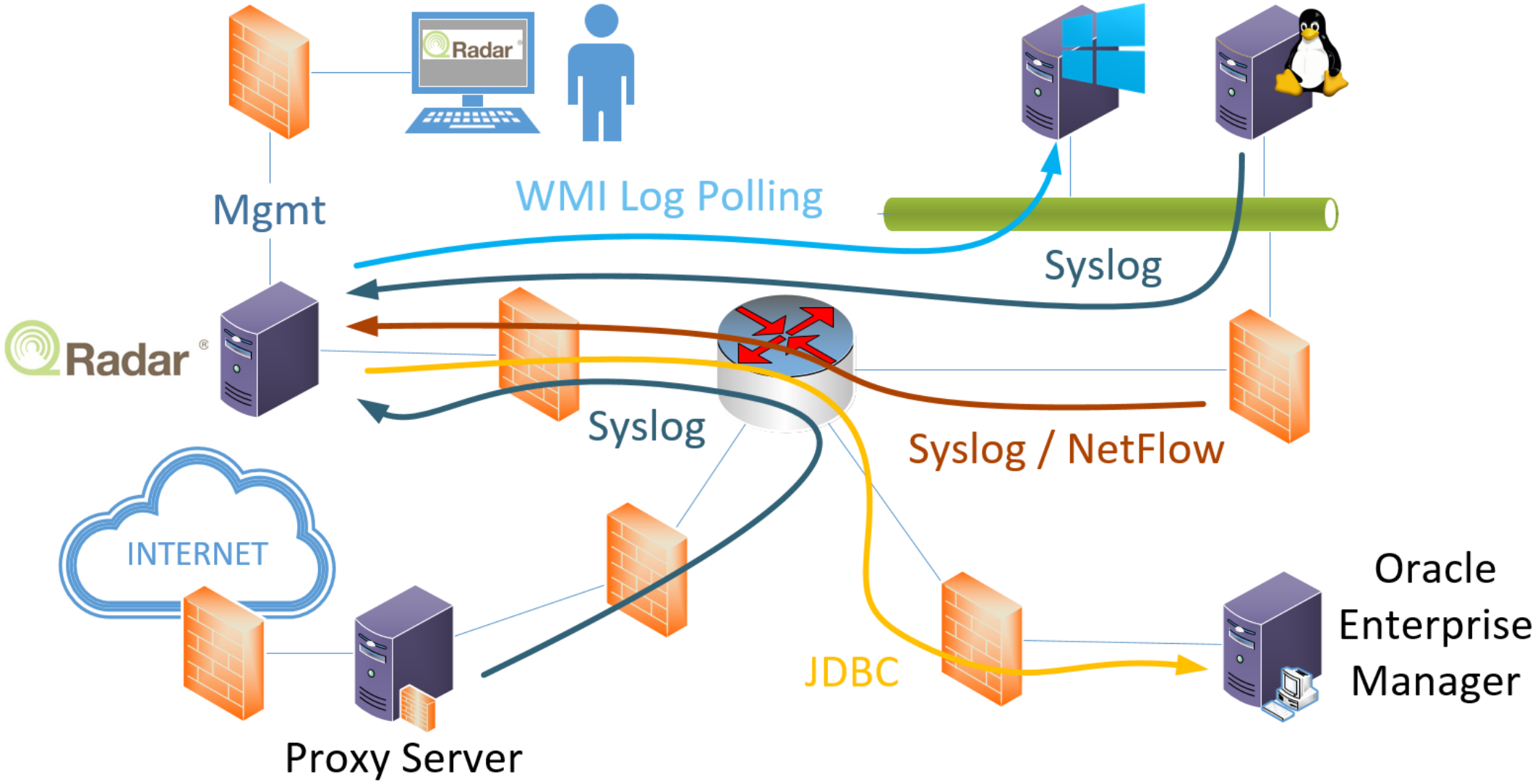
abraxas

Architektur
Use Cases
Dashboard & Reports

abraxas

SIEM = Security Information & Event Management

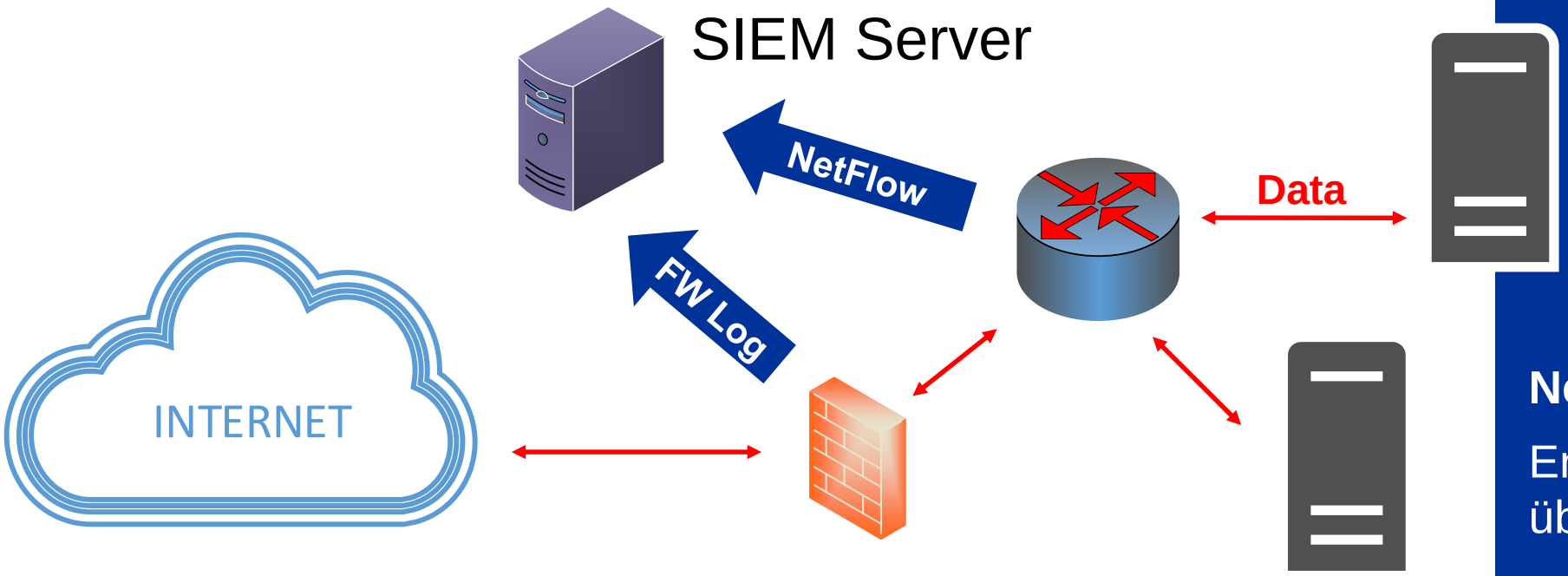
Architektur

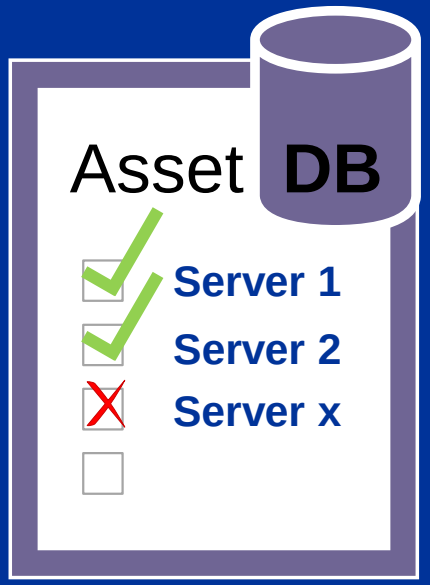


Inventar der aktiven Systeme

Use Case 1: Resultate

- ✓ Automatische Inventarisierung (Asset DB)
- ✓ Erkennen unerlaubter Systeme
- ✓ Kommunikationsverhalten





Netflow

Enthält Informationen über den IP-Datenstrom

Unerlaubter resp. unsicherer Verkehr

abraxas

Use Case 2: Resultate

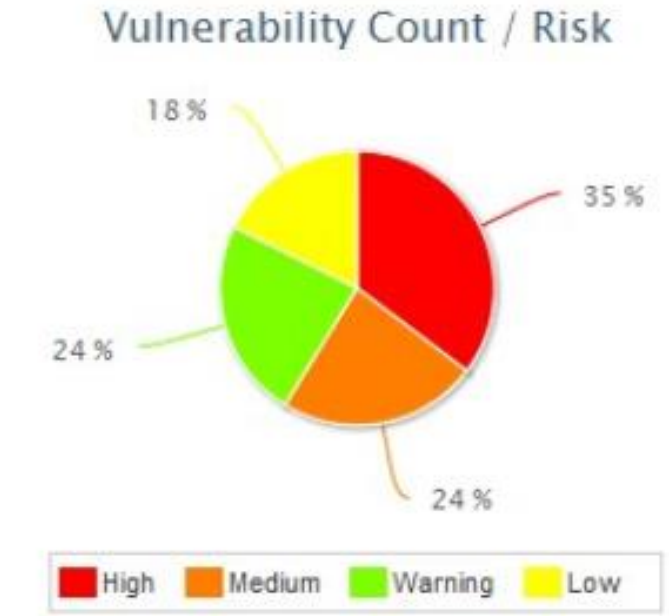
- ✓ Visibilität schaffen
- ✓ Meist verwendeten Protokolle

Application	Destination Port	Source (Bytes)	Destination (Bytes)	Connection Count
Secure Web	443	115’129’658	426’266’096	111’585
Kerberos	Multiple (2)	41’976’551	231’055’810	38’262
DNS	53	2’003’503	3’527’200	26’247
Other	Multiple (12)	4’708’587’817	4’389’183’798	8’338
Win. File Sharing	Multiple (2)	126’189’682	1’576’400’012	7’407
Unsecure WEB	80	928’541’594	888’689’015	2’693

Schwachstellenanalyse

Use Case 3: Resultate

- ✓ Linux- und Windows-Server Systemanalyse
- ✓ Inventarisierung der Schwachstellen
- ✓ Identifizierung Systeme mit hohem Risiko



SSL - RC4 Algorithm - **Plaintext-Recovery** Issue
SSL - Server Supports **Weak SSL Ciphers**
SNMP - Various Devices - **Default Password**

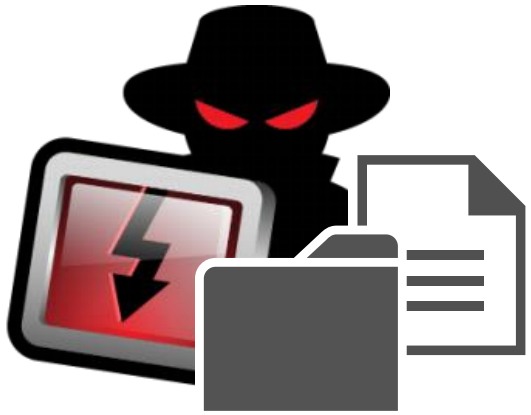
Vulnerability

Schwachstellen, welche durch Angreifer ausgenutzt werden können

Verdächtiges Verhalten

Use Case 4: Resultate

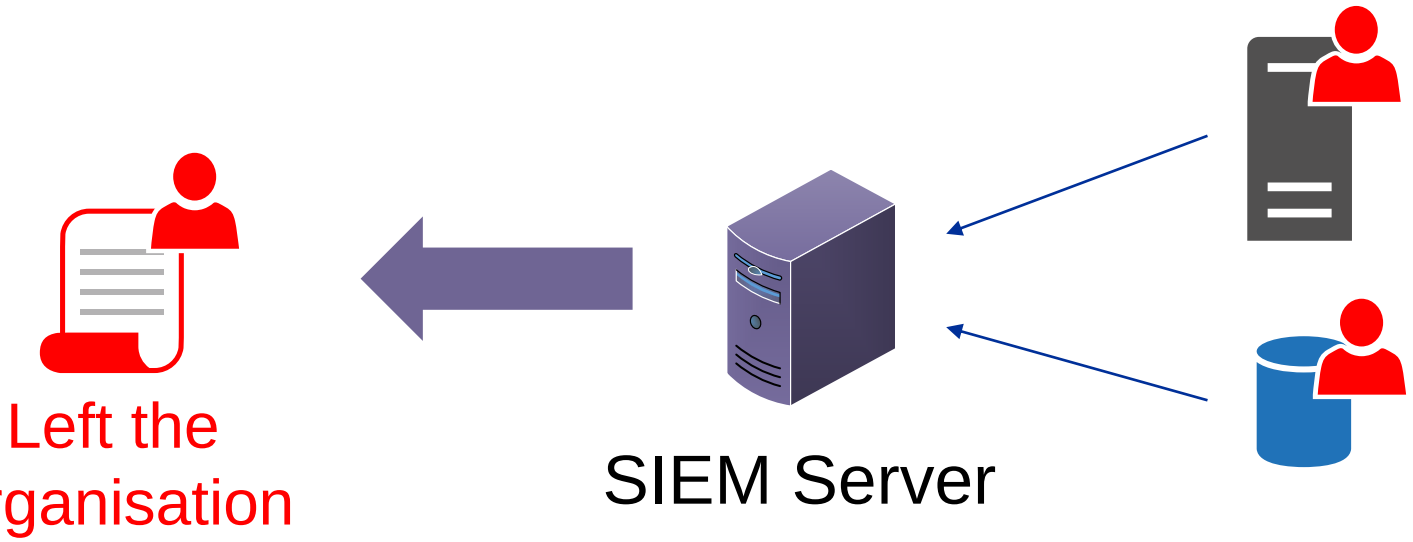
- ✓ Failed Logins erkennen
- ✓ Bad Hosts Communication (IP Reputation)
- ✓ Fileshare (Access, Delete, Chg. Permissions)



Privilegierte Benutzer

Use Case 5: Resultate

- ✓ Root-Login auf Linux erkennen
- ✓ Admin-Login auf Windows erkennen
- ✓ Abgleich mit Benutzern, die die Organisation verlassen haben



Admin & Root User

Durch Korrelationen ergeben Daten Sinn

abraxas

5

Use Case 1

Use Case 5

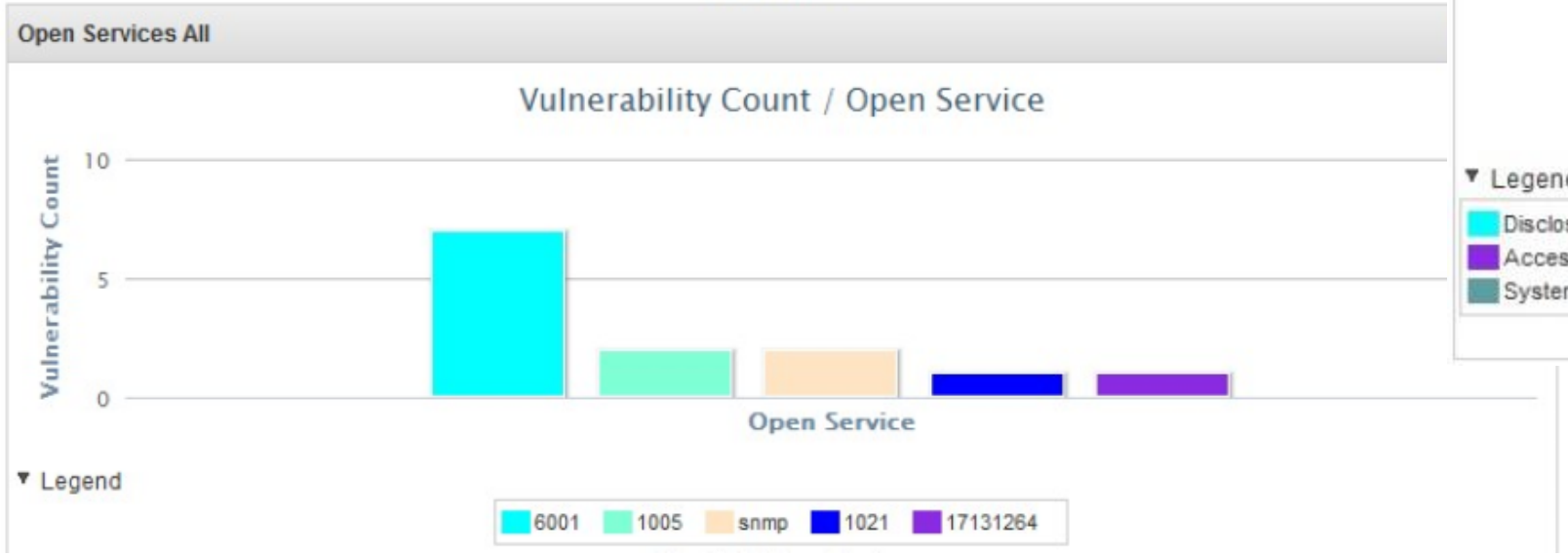
Use Case 5

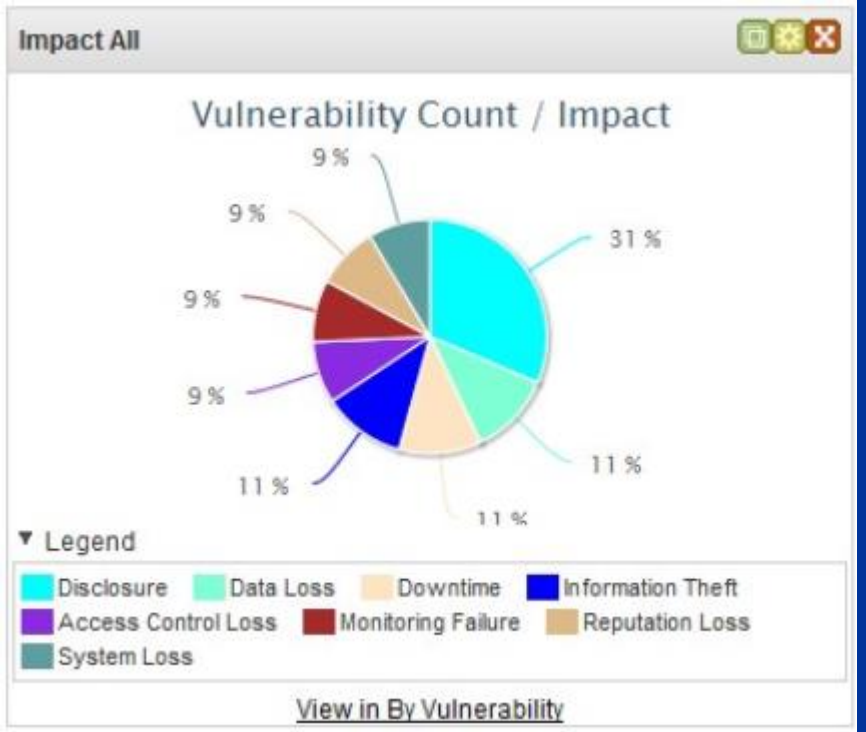
Offense 109 | Summary | Display ▼ | Events | Connections | Flows | View Attack Path | Actions ▼ | Print

Magnitude		**Status**		**Relevance**	6	**Severity**	5	**Credibility**	3
Description	Unknown System detected in the Network preceded by Successful root login to a critical system preceded by Scan Followed By Successful Login preceded by ABX Login for a User who left the Company preceded by ABX Unknown System detected in the Network preceded by ABX Successful root login to a critical system containing Chat.Jabber	**Offense Type**	Source IP						
Source IP(s)	[redacted]	**Start**	10 Feb 2017, 14:55:05						
Destination IP(s)	Local (13) Remote (4)	**Duration**	27d 23h 57m 51s						
Network(s)	Multiple (4)	**Assigned to**	Unassigned						
		Event/Flow count	1,289,867 events and 906,529 flows in 30 categories						

Dashboard & Reports

- ✓ Es können Tendenzen aufgezeigt werden
- ✓ Die Daten werden angereichert und bekommen dadurch einen Mehrwert
- ✓ Real-Time-Korrelationen (IBM QRadar)





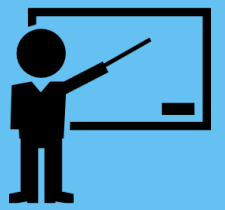
Kantonspolizei Zürich

Lessons learned
Mehrwert

Lessons learned

Kantonspolizei Zürich

- Use-Cases vor der Implementation genau beschreiben
- Umsetzung in kleinen Schritten
- Nutzen kann vielfältig sein
- SIEM kann helfen, die IT-Infrastruktur «sauber» zu halten
- Relevante Logs und Informationsquellen einbinden



Erwarteter Mehrwert

Kantonspolizei Zürich

- Detailinformation über die vorhandenen Systeme
- Frühzeitiges Erkennen von abnormalem Verhalten
- Abwehr von Angriffen
- Verhindern von Datenabflüssen
- Unterstützung bei der Untersuchung von Vorfällen, Nachvollziehbarkeit

➔ **Besserer Schutz der ICT-Systeme und Daten**

➔ **Reputation der Kapo erhalten**

Wie gut sind Sie aufgestellt?

Security Analysts

Security Analytics

No SIEM

SIEM assisted

IBM QRadar Watson Advisor assisted