SIMU

Event-Korrelation in SIEM-Systemen auf Basis von IF-MAP

Kai-Oliver Detken[1] · Felix Heine[2]
Thomas Rix[1] · Leonard Renners[2]

[1]DECOIT GmbH, Fahrenheitstr. 9, D-28359 Bremen
detken/rix@decoit.de
[2]Hochschule Hannover, Ricklinger Stadtweg 120, D-30459 Hannover
felix.heine/leonard.renners@hs-hannover.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Agenda

SIMU

- Kurzvorstellung Projekt
- Architektur

Metadaten

- IF-MAP Standard
- Anwendungsbeispiel

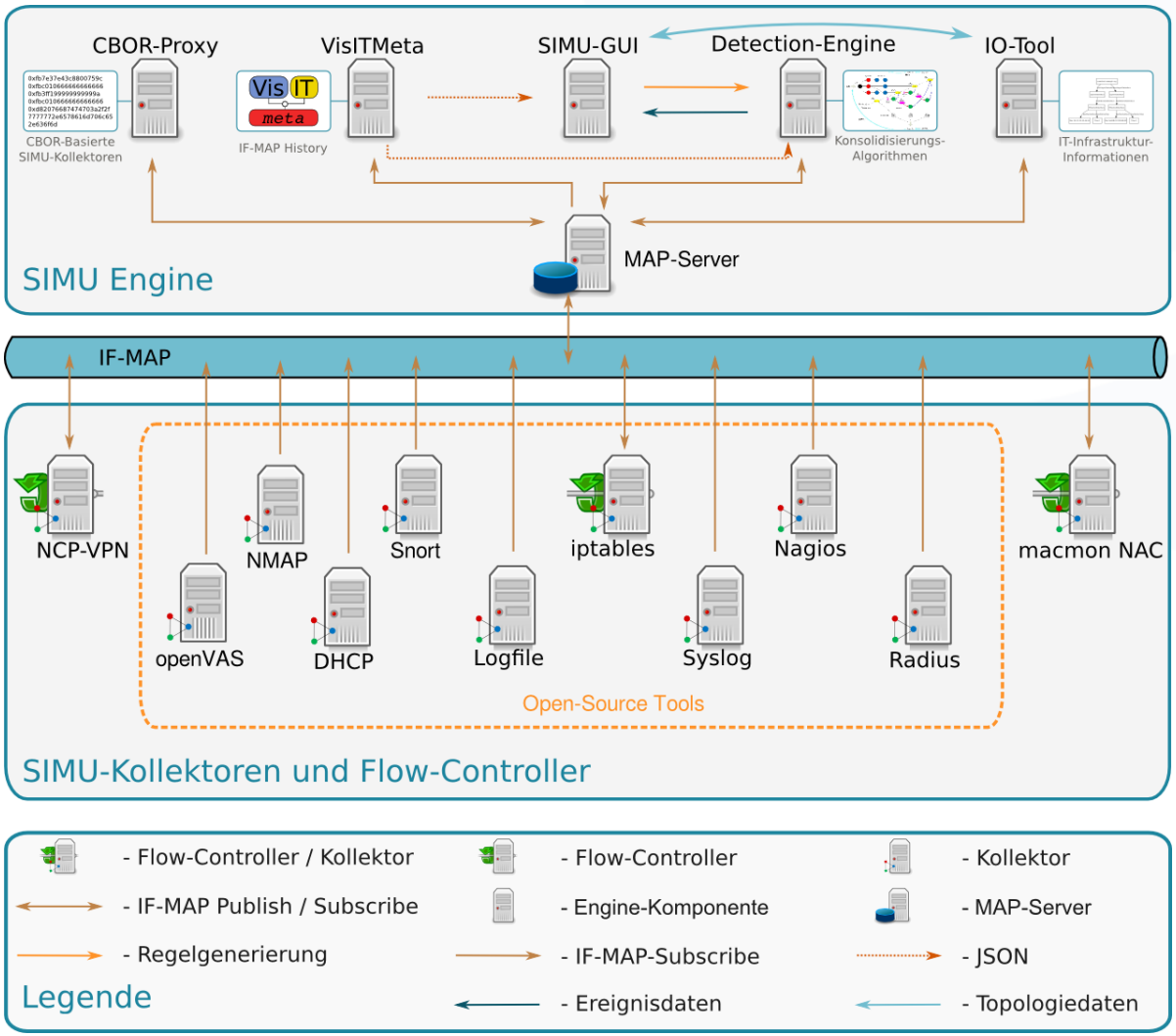
Vorfälle

- Erkennung
- Darstellung und Bearbeitung

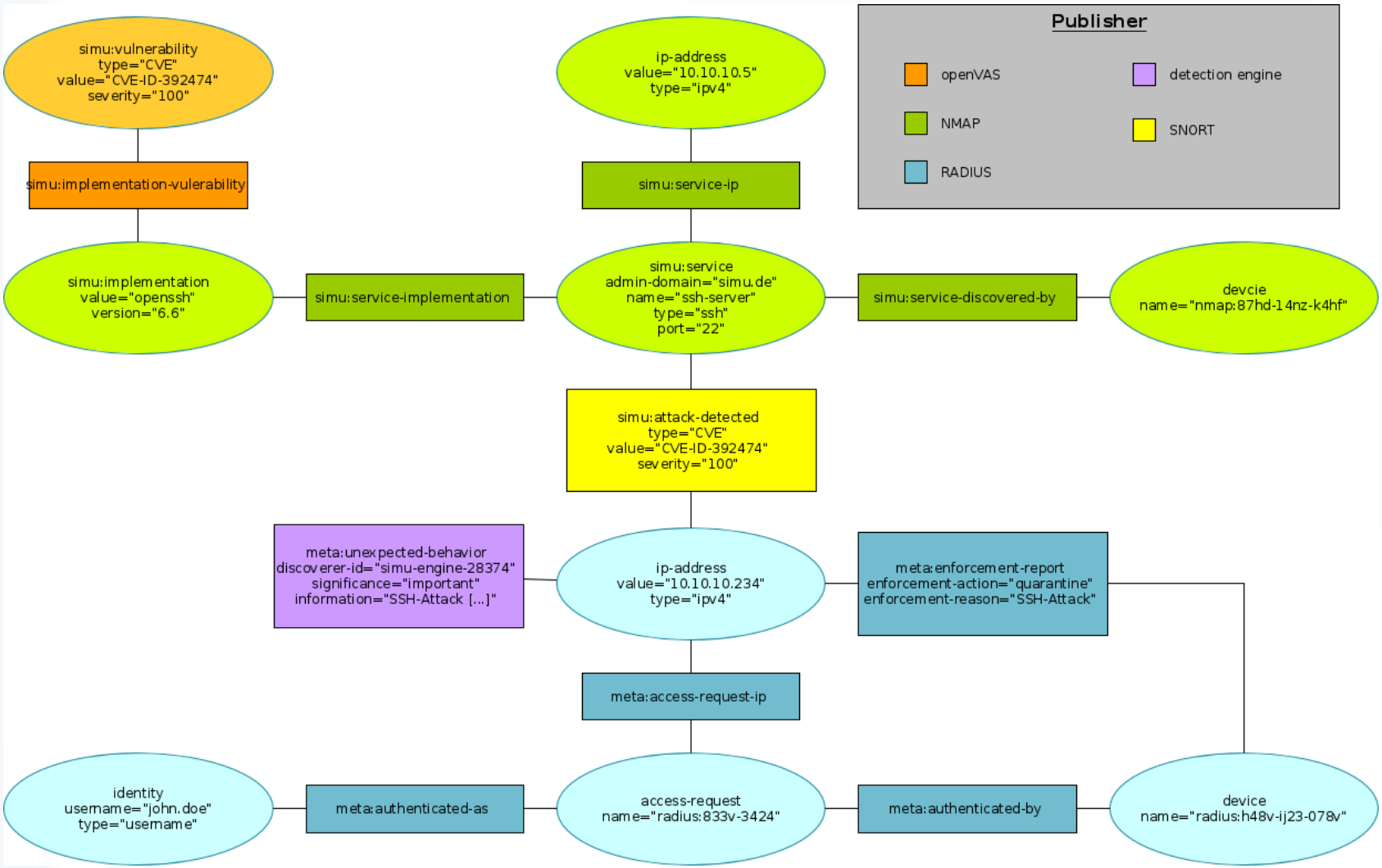
SIMU in a Nutshell

- Entwicklung eines SIEM-Systems für KMU
  - SIEM: Security Information and Event Management
  - Zentrale Speicherung und Auswertung sicherheitsrelevanter Informationen
- Ziel: Einfachheit!
- Datenintegration auf Basis von IF-MAP
  - Standard der TCG
  - Graphbasiertes Modell
- Oberfläche (SIMU GUI / VisITMeta)
  - Visualisierung der Daten und Ereignisse
  - Nachverfolgung der Ereignisse

SIMU Architektur



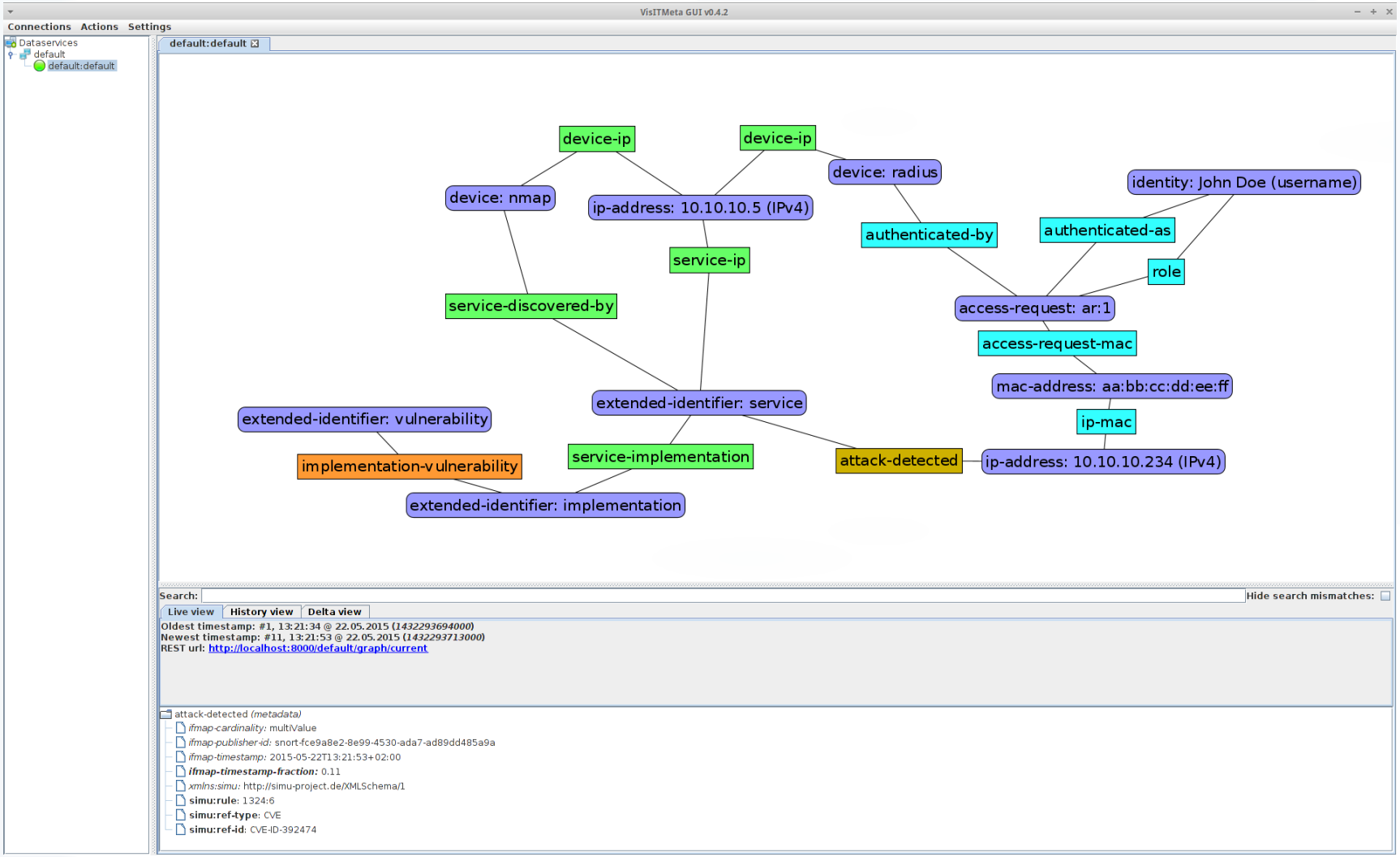
IF-MAP: Anwendungsfall



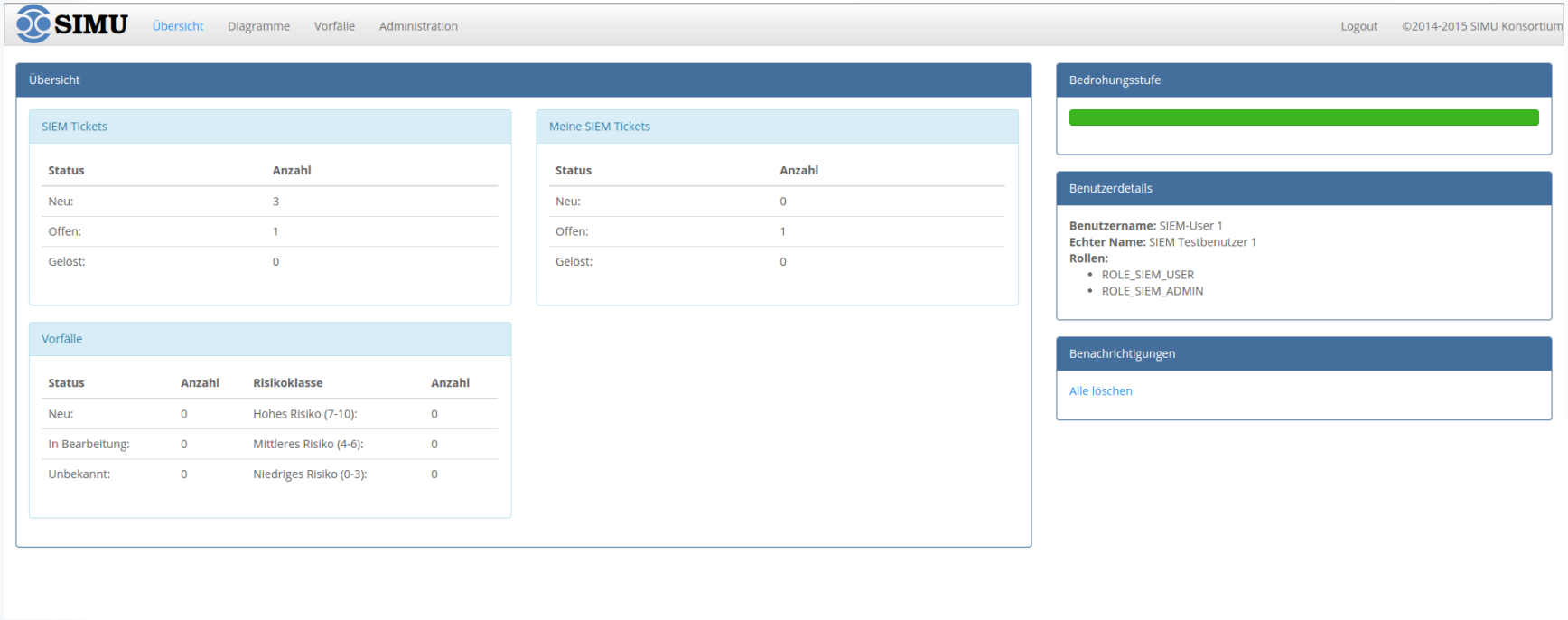
Detection Engine

- Regelbasierte Erkennung von Vorfällen
- Definiert Muster im IF-MAP-Graphen, die sicherheitsrelevante Vorfälle beschreiben
- Aktionen: Vorfall melden, ggf. Enforcement (z.B. Benutzer ausschliessen)
- Visualisierung der erkannten Vorfälle durch VisITMeta
- Weitere Bearbeitung mit der SIMU GUI

VisITMeta


VisITMeta GUI v0.4.2
Connections Actions Settings
Dataservices
default
default:default
default:default
device-ip
device-ip
device: radius
identity: John Doe (username)
device: nmap
ip-address: 10.10.10.5 (IPv4)
authenticated-by
authenticated-as
service-ip
role
service-discovered-by
access-request: ar:1
access-request-mac
mac-address: aa:bb:cc:dd:ee:ff
extended-identifier: service
extended-identifier: vulnerability
ip-mac
service-implementation
attack-detected
ip-address: 10.10.10.234 (IPv4)
implementation-vulnerability
extended-identifier: implementation
Search:
Hide search mismatches:
Live view
History view
Delta view
Oldest timestamp: #1, 13:21:34 @ 22.05.2015 (1432293694000)
Newest timestamp: #11, 13:21:53 @ 22.05.2015 (1432293713000)
REST url: http://localhost:8000/default/graph/current
attack-detected (metadata)
ifmap-cardinality: multiValue
ifmap-publisher-id: snort-fce9a8e2-8e99-4530-ada7-ad89dd485a9a
ifmap-timestamp: 2015-05-22T13:21:53+02:00
ifmap-timestamp-fraction: 0.11
xmlns:simu: http://simu-project.de/XMLSchema/1
simu:rule: 1324:6
simu:ref-type: CVE
simu:ref-id: CVE-ID-392474

SIMU GUI


SIMU
Übersicht
Diagramme
Vorfälle
Administration
Logout
©2014-2015 SIMU Konsortium
Übersicht
SIEM Tickets
Status
Anzahl
Neu:
3
Offen:
1
Gelöst:
0
Meine SIEM Tickets
Status
Anzahl
Neu:
0
Offen:
1
Gelöst:
0
Vorfälle
Status
Anzahl
Risikoklasse
Anzahl
Neu:
0
Hohes Risiko (7-10):
0
In Bearbeitung:
0
Mittleres Risiko (4-6):
0
Unbekannt:
0
Niedriges Risiko (0-3):
0
Bedrohungsstufe
Benutzerdetails
Benutzername: SIEM-User 1
Echter Name: SIEM Testbenutzer 1
Rollen:
ROLE_SIEM_USER
ROLE_SIEM_ADMIN
Benachrichtigungen
Alle löschen

Zusammenfassung

- SIEM-System mit geringer Einstiegshürde
- IF-MAP Basis zur Integration von sicherheitsrelevanten Informationen
- Sicherheitsvorfälle:
  - Musterbasierte Erkennung im IF-MAP-Graphen
  - Darstellung in VisITMeta
  - Bearbeitung mit SIMU GUI

SIMU

Vielen Dank

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Copyright 2013-2015

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „16KIS0041K“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.