IPv6 Kongress 2014

FH | JOANNEUM
University of Applied Sciences

IPv6 Security Incident and Event Management (SIEM)

IPv6-Kongress, Frankfurt/Main, 22.-23. Mai 2014

FH-Prof. DI Ewald Graif
FH JOANNEUM University of Applied Sciences
Institut für Informationsmanagement
Graz, Österreich

ewald.graif@fh-joanneum.at

Agenda

- Network Security Monitoring in IPv4 und IPv6 Umgebungen
- Motivation für Security Incident and Event Management (SIEM)
- Funktionsweise von SIEM
- SIEM Architektur in einer IPv6 Umgebung
- Use Cases: Splunk, ELSA
- Resümee

Herausforderungen für die IT-Sicherheit

- Externe Bedrohungen
  - Zahl der Angriffe steigt laufend
  - Attacken werden vielfältiger und komplexer
  - IPv4 und IPv6 betroffen
  - Neue Bedrohungspotentiale durch Cloud Services

- Interne Bedrohungen
  - Verteilte, heterogene Systemlandschaften
  - Sicherheitskultur
    - Maximale Offenheit versus restriktives Sicherheitsmanagement
    - Sicherheitsbewusstsein der Mitarbeiter/inne/n
  - IPv4 und IPv6 betroffen
  - Kaum Kenntnisse zu IPv6 Bedrohungen
  - IPv6 weniger sicher als IPv4? („Mythenbildung“)

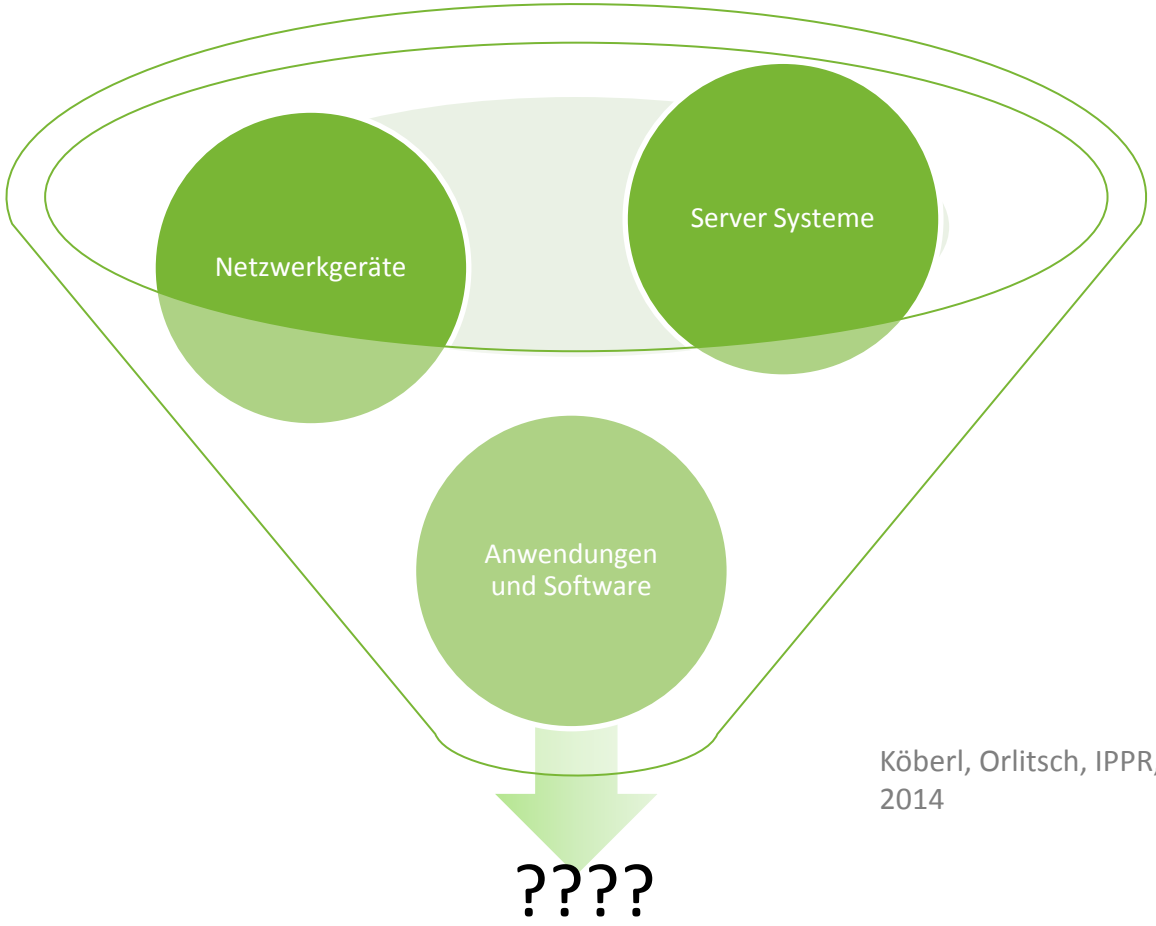
Netzwerk Sicherheits-Monitoring (NSM)

- Host Intrusion Detection Systeme (H-IDS)
  - IPv4, IPv6
- Network Intrusion Detection Systeme (N-IDS)
  - IPv4, IPv6
- Netzwerk Monitoring
  - Z.B. Erkennung von massivem Ressourcenverbrauch durch Denial of Service Attacken
  - IPv4, IPv6
- Spezielle Tools zur Erkennung von Attacken
  - IPv4, IPv6

Herausforderungen für NSM

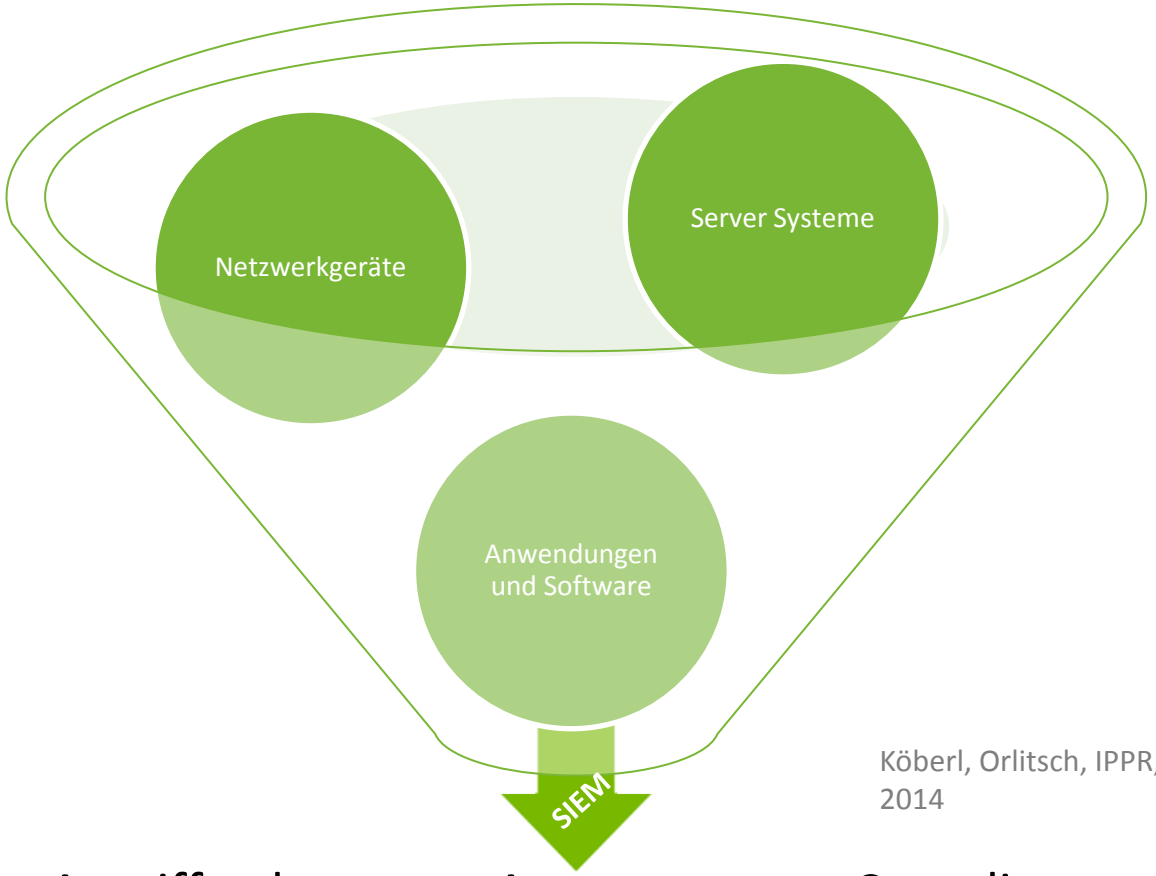
- Vielfalt an Tools für Angriffserkennung
- Fehlen von gemeinsamen Sicherheits-Dashboards
- Vielfalt an Geräten, Systemen, Diensten und Anwendungen, die große Mengen an Logs produzieren
- Logs werden kaum ausgewertet
- Keine Korrelation von sicherheitsrelevanten Ereignissen bei komplexen Angriffen

Lösungsansatz?



Köberl, Orlitsch, IPPR, FH JOANNEUM 2014

Lösungsansatz: SIEM



Köberl, Orlitsch, IPPR, FH JOANNEUM 2014

Angriffserkennung, Auswertungen, Compliance

Was ist Security Incident and Event Management (SIEM) ?

Security Information Management	Security Event Management
Archivierung (Langzeit)	Datenerfassung in Echtzeit
Auswertung und Analyse	Normalisierung und Korrelation
Reporting (Compliance)	Alarmierung

Köberl, Orlitsch, IPPR, FH JOANNEUM 2014

Funktionsweise von SIEM

Köberl, Orlitsch, IPPR, FH JOANNEUM 2014

Anwendung von SIEM

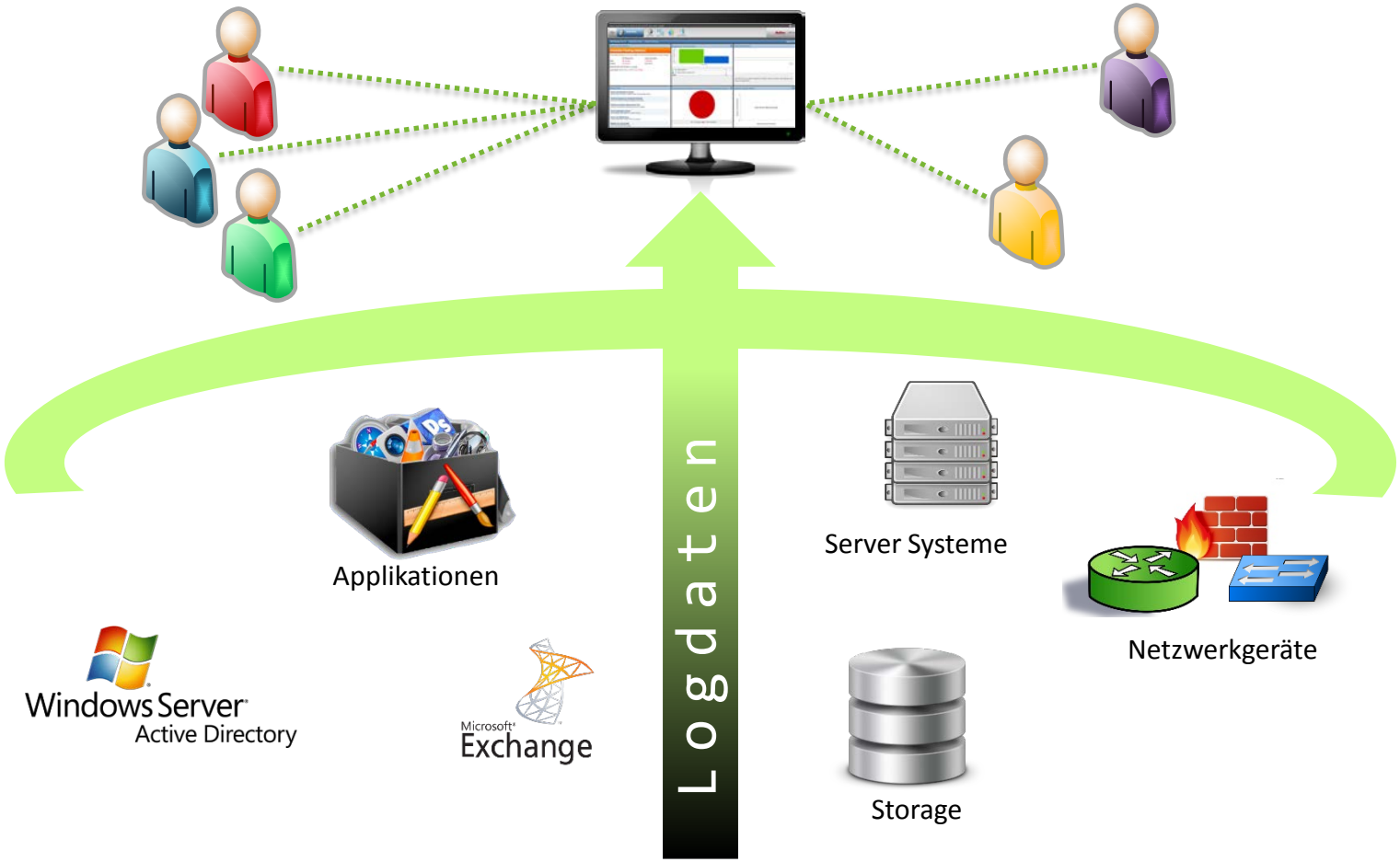
- Echtzeit von Angriffserkennung
- Analyse von Sicherheitsvorfällen (Forensik)
- Troubleshooting
- Monitoring
  - … Verdächtiges Verhalten im Netzwerkverkehr
  - … Unberechtigte Logins bei administrativen Accounts
  - … Zugriff auf IT-Ressourcen
- Sicherheits-Compliance
  - Einhaltung von Sicherheitsstandards
  - Generierung von Reports

Wesentliche Mehrwerte von SIEM

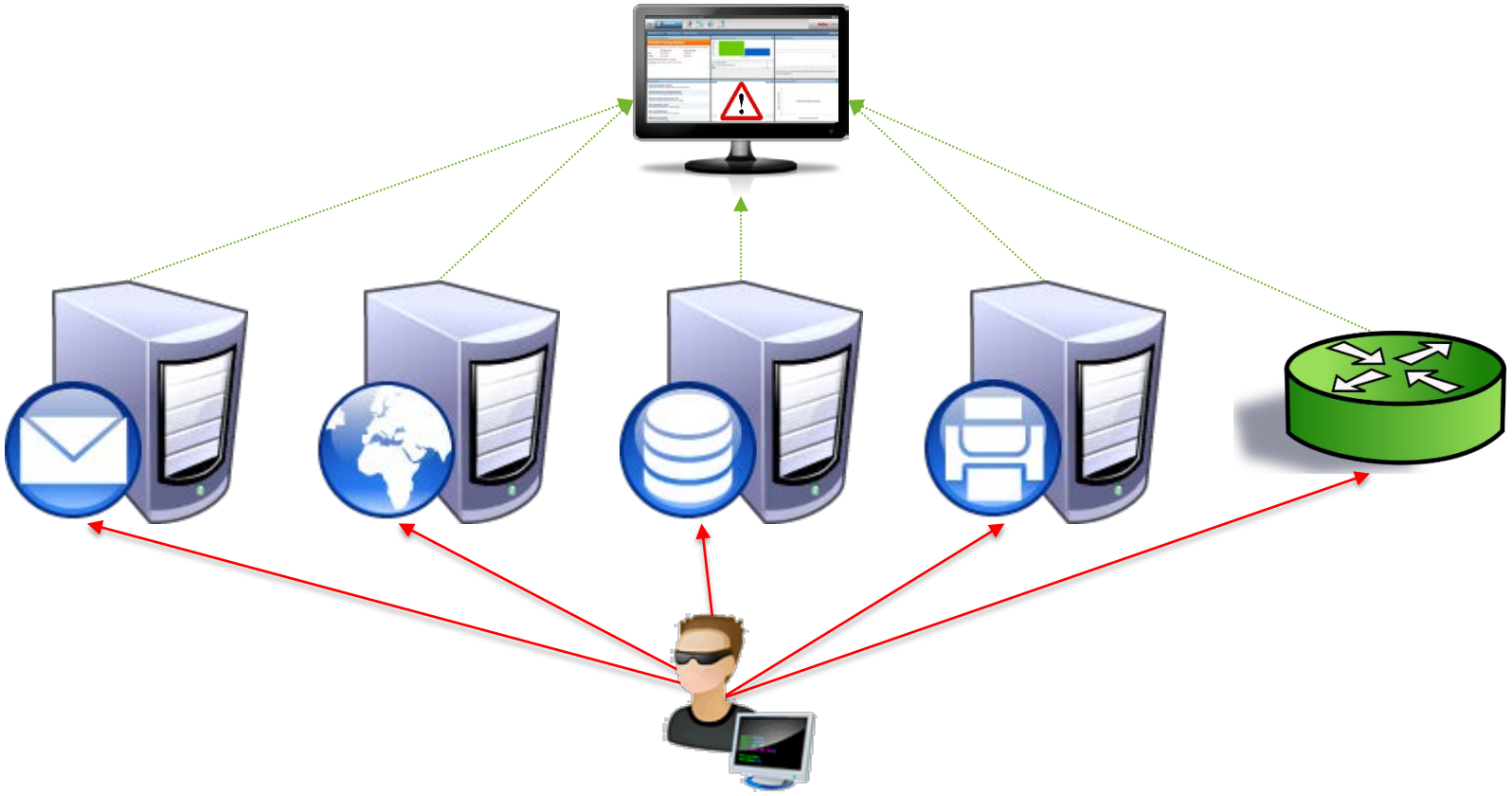
- SIEM ist ein „Umbrella“ System
- Durch SIEM wird es ermöglicht, IT-Sicherheit der Infrastruktur in ihrer Gesamtheit zu überwachen:
  - Sicherheitsrelevante Ereignisse werden in einem Dashboard zusammengeführt
  - Administrator/inn/en müssen nicht mehr einzelne Überwachungstools konsultieren
- Zentrale Verwaltung, Aggregation und Korrelation von Logdaten verschiedener Systeme
- Sicherheitsrelevante Ereignisse können korreliert werden

Sicherheitsüberwachung ohne SIEM

Sicherheitsüberwachung mit SIEM



Zentrale Alarmierung durch SIEM



SIEM Produktübersicht und Einordnung

Figure 1. Magic Quadrant for Security Information and Event Management

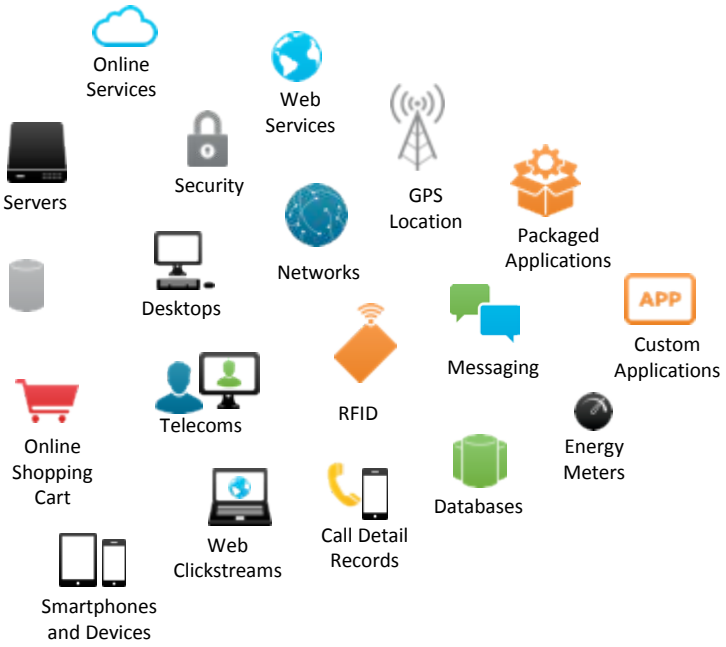
Source: Gartner (May 2013)

Use Case mit Splunk als SIEM

- Splunk Steckbrief:
  - Installation unproblematisch
  - Ausführliche Produktdokumentation
  - Etablierte Online-Community
  - Frei verfügbare und kommerzielle Version
  - SIEM geeignet für Big Data
  - Frei konfigurierbares Regelwerk
  - IPv6 wird unterstützt

SIEM als „Security Intelligence Platform“

Machine Data



Security Use Cases

SIEM als „Big Data Platform“

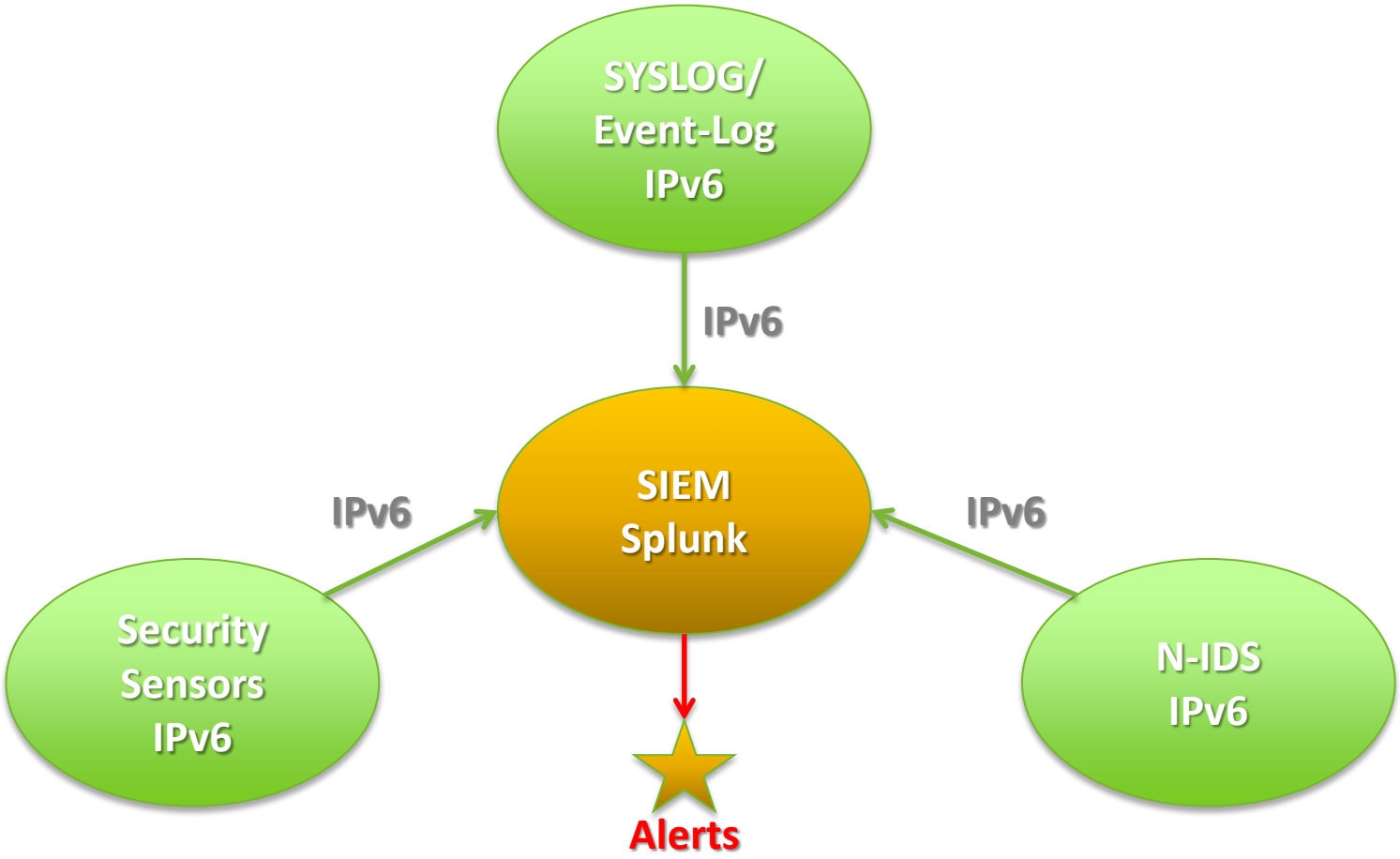
Erfahrungen mit SIEM/Splunk in einem IPv4Testszenario

- Integriertes Praxisprojekt FH JOANNEUM mit Master-Studierenden „Informationsmanagement“ (AIM), 2013/2014
  - Studierende: Florian Köberl, Andreas Orlitsch
- Verwendung von System-(Sys)Logs
  - Server
  - Firewall
  - Sensor (ARPWATCH)
- Angriffserkennung
  - Gute Angriffserkennung
  - Komplexe Angriffe werden durch Korrelation erkannt
  - Security Dashboard von Splunk sehr hilfreich

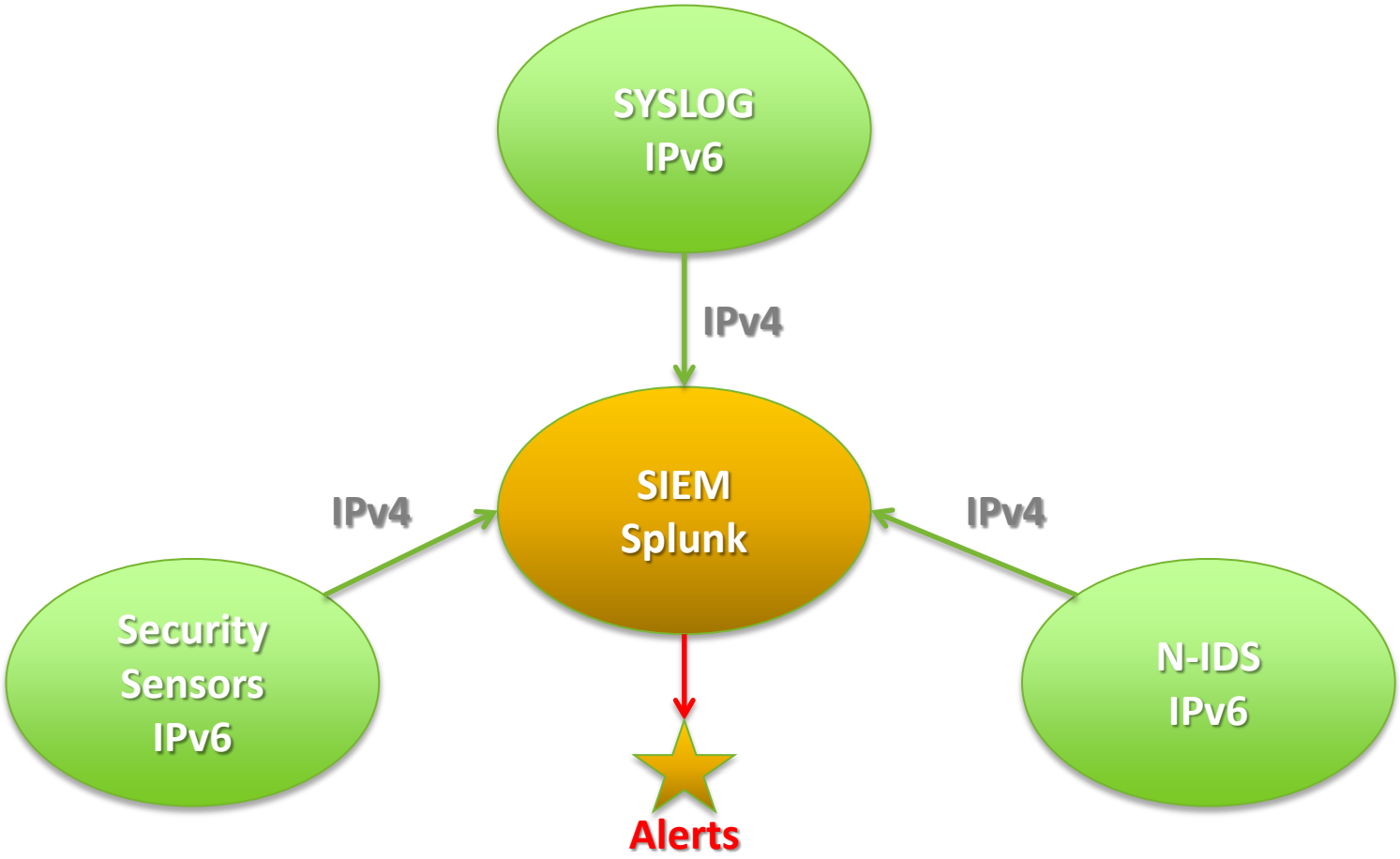
SIEM/Splunk in einem IPv6 Szenario

- Splunk unterstützt IPv6
- Herausforderung: Richtiges Parsen von IPv6 Adressen aus Logging-Quellen
- Log-Forwarding in IPv6 möglich
- Manche Netzwerkgeräte unterstützen nicht Syslogging unter IPv6
  - Ausweg: Syslogging unter IPv4 an Splunk weiterleiten
- Splunk ist im IPv6 Umfeld wirksam:
  - Überwachung in allen ISO/OSI Layern möglich
- Mächtige Abfragemöglichkeiten (Queries) der indizierten Logs
- Scripting für Auswertungen
  - Manueller Aufwand
- Generierung von Dashboards für Sicherheitsmonitoring
  - Alerting auch in IPv6 Umgebungen möglich

SIEM/Splunk Sicherheitsarchitektur in IPv6



SIEM/Splunk Sicherheitsarchitektur in IPv6 mit IPv4 Transport



Beispielattacken

- Router Advertisement Flood Attack
  - KALI Linux
  - http://samsclass.info/ipv6/proj/RA_flood2.htm
- Man in the Middle (MitM): IPv6 Neighbor Spoofing
  - KALI Linux, SCAPY Scripts
  - http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/
- Brute Force Logins
  - Windows Server 2008R2
  - Debian Server

Angriffserkennung mit Splunk

- IPv6 Router Advertisement Flood Attack
  - Debian Sensor mit NDPMon (http://ndpmon.sourceforge.net)
  - Syslog Forwarding - - > Splunk - - > Alerting
- IPv6 Neighbor Spoofing
  - Debian Sensor mit NDPMon (http://ndpmon.sourceforge.net)
  - Syslog Forwarding - - > Splunk - - > Alerting
- Brute Force Logins
  - Ungewöhnliche Anzahl von Login-Versuchen pro Zeiteinheit
  - Debian: Forwarding - - > Splunk - - > Alerting
  - Windows Server: Windows Event-Log Agent - - > Splunk - - > Alerting

Erfahrungen mit Splunk und IPv6

- Integration in IPv6 Umgebungen möglich
- Effektives Sicherheitsmonitoring auch für IPv6

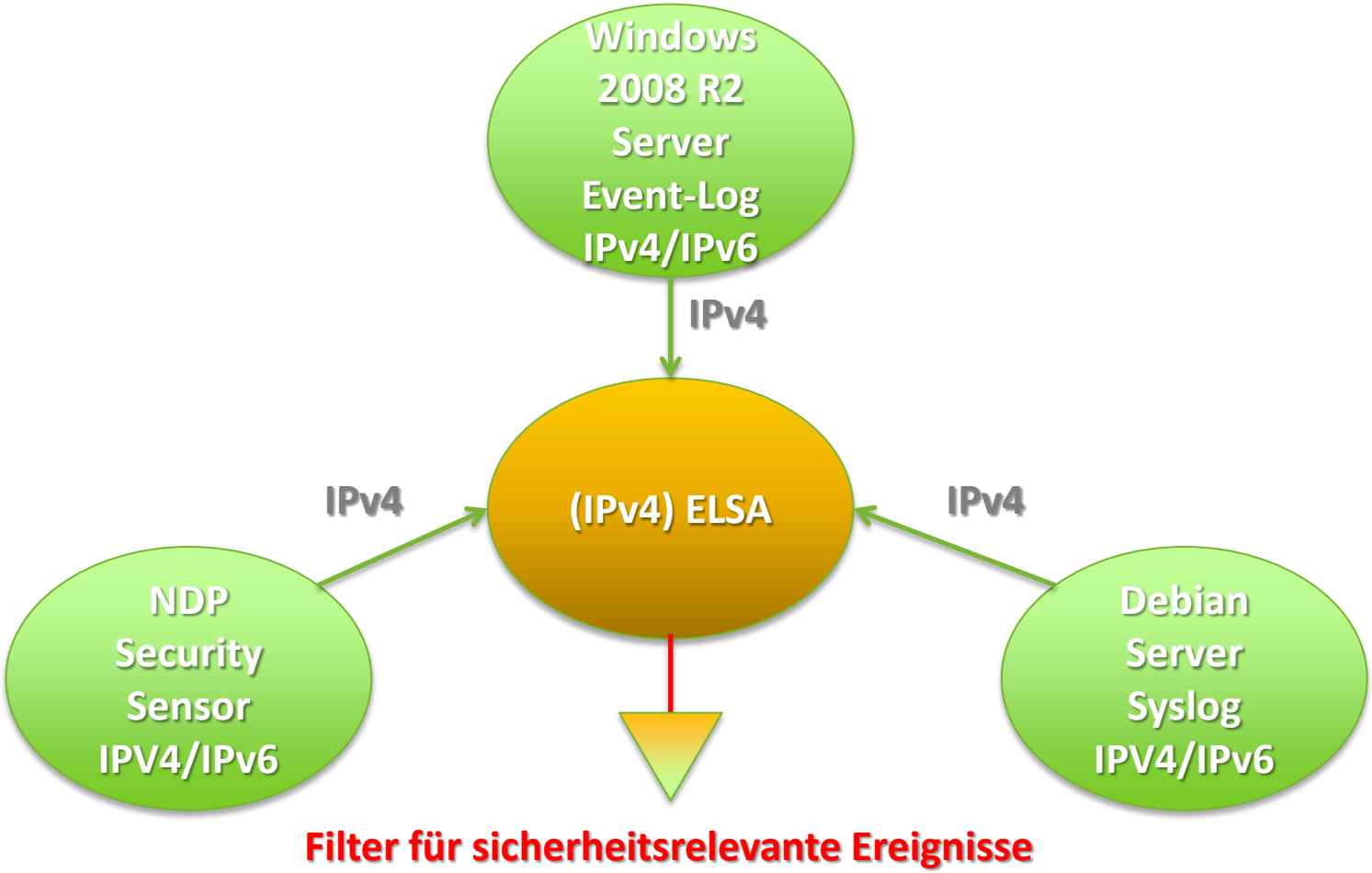
- Mächtiges Werkzeug für Angriffserkennung
- Korrelation von sicherheitsrelevanten Ereignissen möglich
- Manueller Aufwand für Regelwerk notwendig!
- Der Einsatz der komfortablen Enterprise Security Apps für IPv6 derzeit kaum möglich (*)

(*) http://answers.splunk.com/answers/127959/splunk-es-30-asset-support-for-ipv6, Eintrag vom 19.3.2014

Integration von IPv4 SIEM Systemen

- Log-Reporter werden im IPv4/IPv6 Dualstack betrieben
  - Windows und Linux Server
  - Sensoren
  - Logging von aktiven Netzwerkkomponenten
- Reporting an SIEM erfolgt über IPv4
- Flexible Auswertemöglichkeiten am SIEM System müssen gegeben sein, um Alerting von sicherheitsrelevanten Ereignissen in IPv6 Umgebungen zu gewährleisten
- Beispielszenario mit ELSA (Enterprise Log Search and Archive) in einer “Security Onion” Instanz (http://blog.securityonion.net/p/securityonion.html)

(IPv4) ELSA in einer IPv6 Umgebung



Filter für sicherheitsrelevante Ereignisse

Resümee

- SIEM ist ein äußerst wirksames Mittel für die Sicherheitsüberwachung von IT-Infrastrukturen
- SIEM ist sowohl in IPv4- als auch in IPv6-Umgebungen einsetzbar und effizient
- SIEM Produkte unterstützen zunehmend IPv6
  - Z.B. Splunk, IBM Qradar, McAfee SIEM/ESM, HP ArcSight
- Das IPv6 Regelwerk muss bei Splunk erst erweitert werden. Manueller Aufwand ist deshalb notwendig
- Empfehlungen:
  - Aktive SIEM/IPv6 Community
  - Impulse seitens der Kunden für komfortablere IPv6 Unterstützung der SIEM Systeme
- IPv4 basierende SIEM Systeme sind durch Dual Stacking in IPV6 Umgebungen einsetzbar
  - Voraussetzung: Flexible Auswertemöglichkeiten, konfigurierbare Dashboards zur Sicherheitsüberwachung und adäquate Reporting Tools