Das SIEM Dilemma

Ein Aufruf zur Verbesserung

ISACA®
Germany Chapter

Damals, 2022

https://de.freepik.com/vektoren-kostenlos/insel-im-meer-unbewohnte-insel-mit-sandstrand_6993839.html Bild von upklyak auf Freepik
Dieses Bild wurde unter Verwendung von Ressourcen von Flaticon.com erstellt

ISACA Germany Chapter

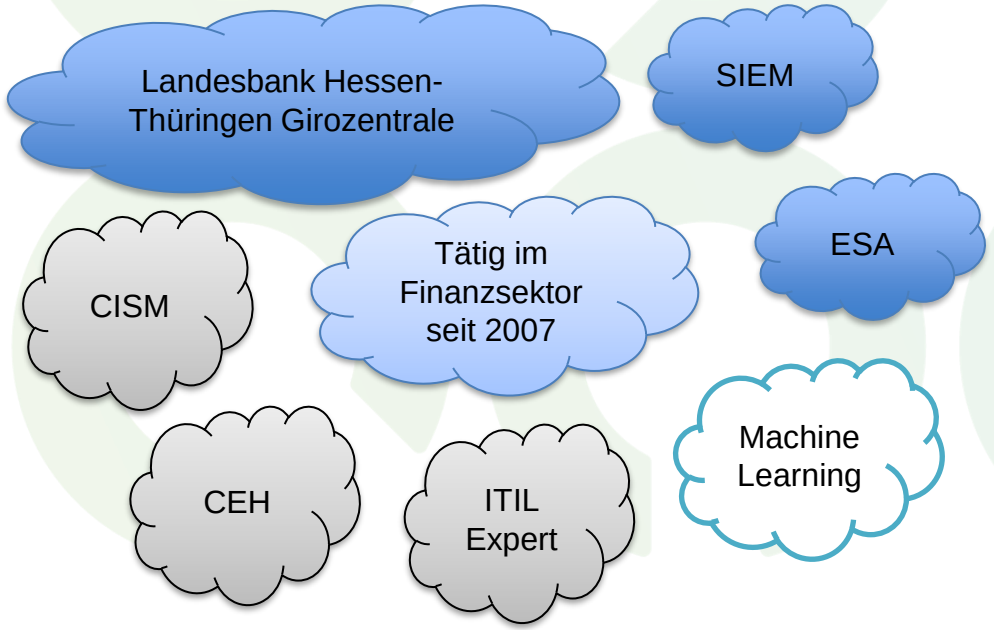
Vielleicht stellen wir uns erst einmal vor:

Dirk Schugardt

Senior Security Consultant

Markus Dreyer

Enterprise Security Architect (Referent)



ISACA Germany Chapter

Wie sind wir auf das Thema gekommen?

Die Suche nach dem SIEM der SIEMs als Lösung für alle Kundengrößen zu akzeptablem Preis

In der Praxis das Problem der ständigen Anpassung …. und kein Ende in Sicht

Gemeinsam in der Fachgruppe Cyber-Security des ISACA e. V. beginnt die Suche nach einer Lösung

Quelle: https://de.wikipedia.org/wiki/User:Doenertier82

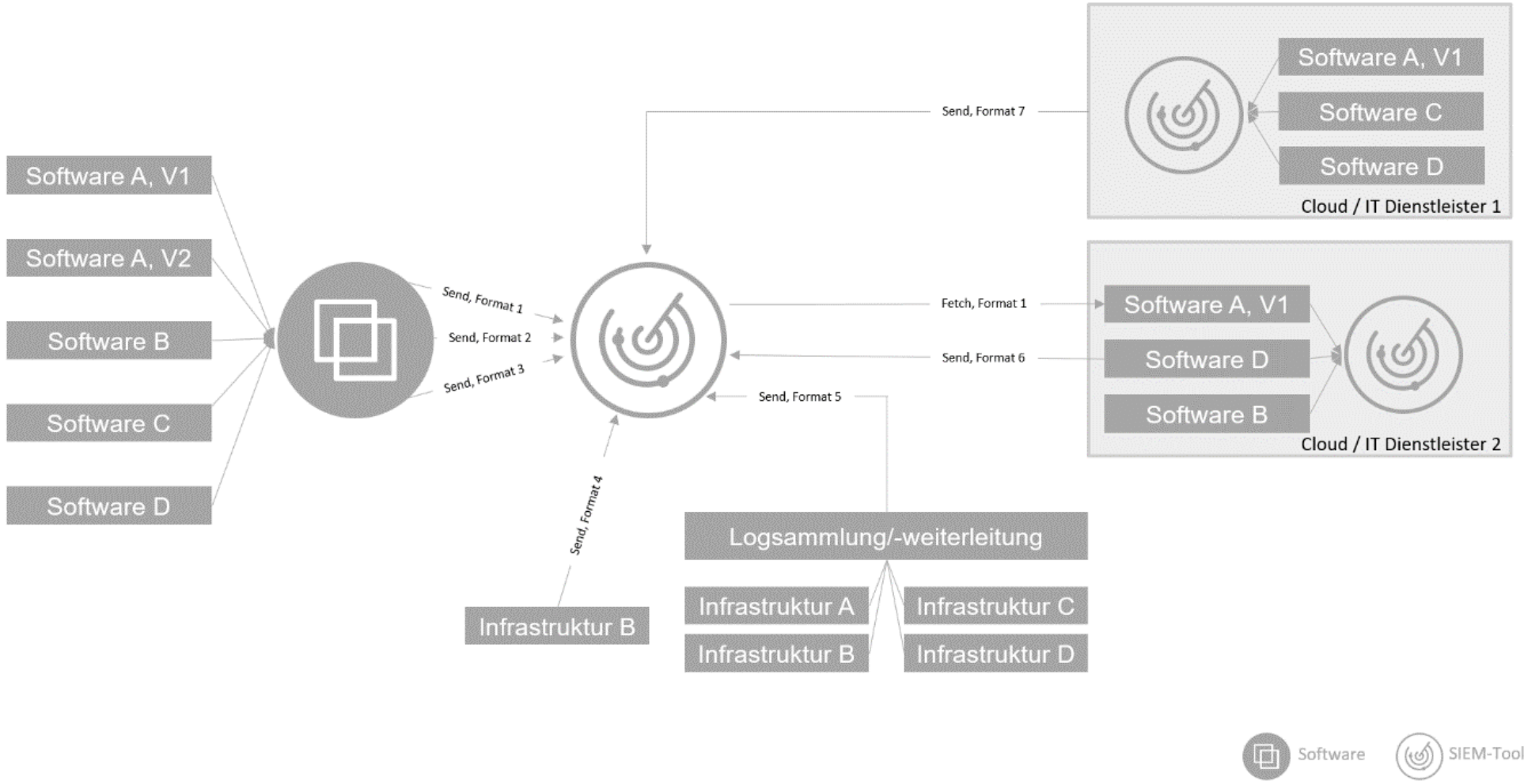
ISACA Germany Chapter

Was sind denn Protokolle (Logs) überhaupt?

Wann sind sie entstanden, für was werden sie benötigt und was gibt es für Unterschiede?

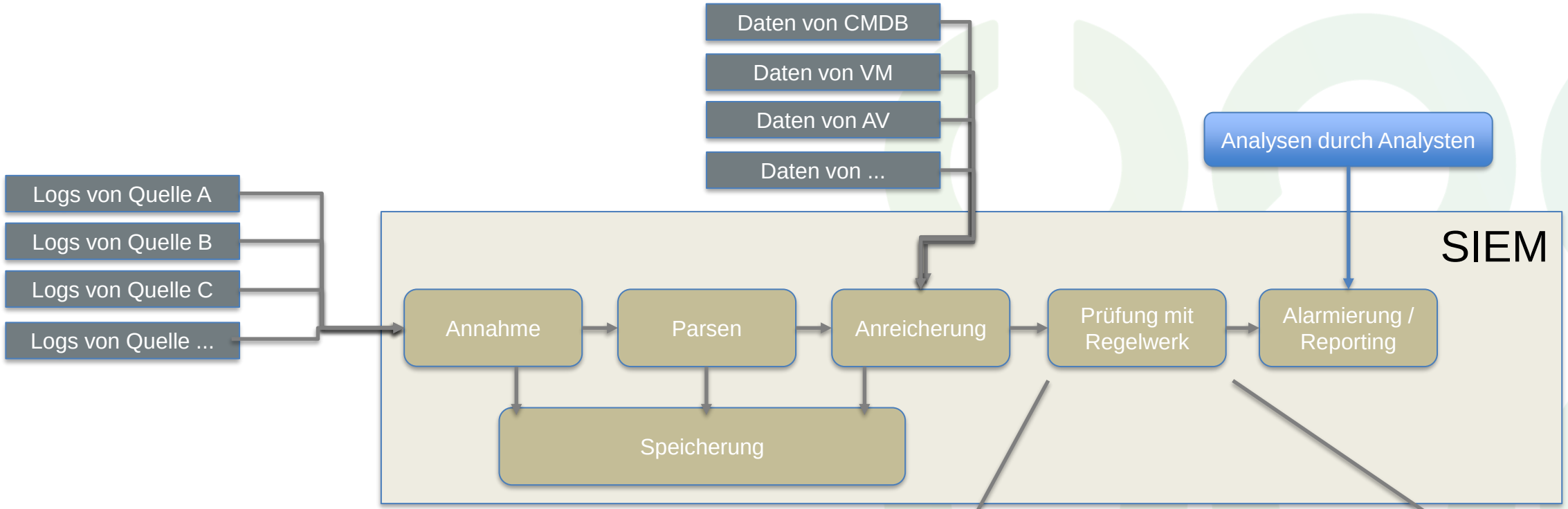
- Werden aufgezeichnet durch alle Arten von IT-Assets, bspw. Router/Switches, Firewalls, Datenbanken, Betriebssysteme, Anwendungssoftware usw.
- Dienen sowohl der Betriebsüberwachung als auch der Security-Überwachung
- Sehr unterschiedlich:
  - Form: (nicht öffentlich dokumentierte) Binärformate, strukturierte Daten (XML, JSON, …), Freitexte; unterschiedliche Encodings
  - Inhalte: Je nach Typ des Assets unterschiedliche Arten, bspw.
    - Firewalls: Verbindungsdaten…
    - Intrusion Detection Systeme: Verdächtige Netzwerkmuster…
    - Antivirus: Scaninformationen, gefundene Viren, verdächtige Verhaltensweisen…
    - Betriebssysteme: Benutzeraktivitäten, Rechtemanagement, Kommandos, Dateizugriffe, Prozesse…
    - Anwendungssoftware: Benutzeraktivitäten, Rechtemanagement, spezifische Anwendungsinformationen…
- Umfang: zwischen sehr umfangreich (viele Arten von Aktivitäten werden erfasst) bis gar nicht (keine Protokollierung)

Was ist ein SIEM?



ISACA Germany Chapter

Was macht ein SIEM?

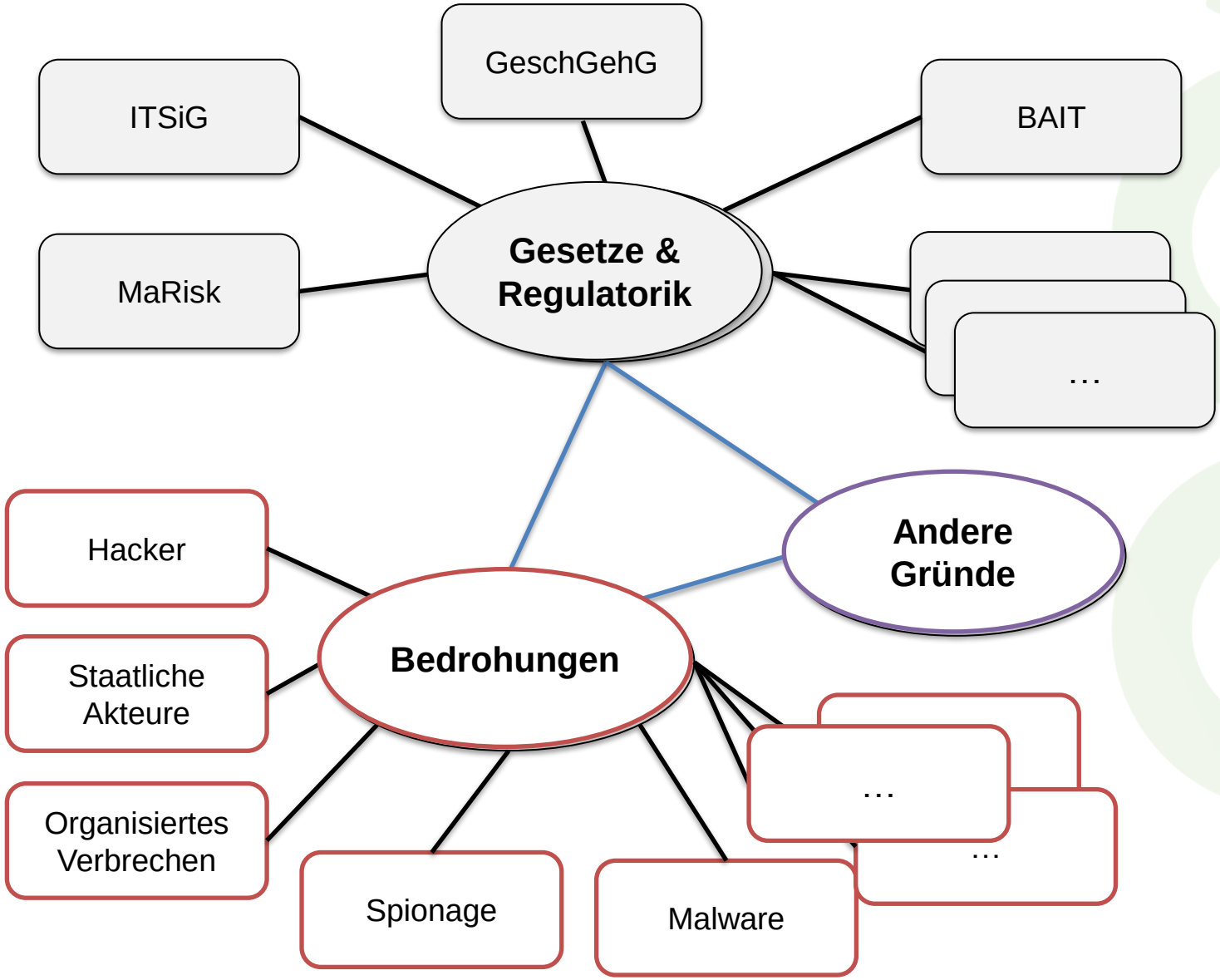


Beispielregeln:

- Deaktivierung Protokollierung SAP: Codes AUE/AUF/AUI/AUG
- Windows Änderung Systemzeit: Code 4616 UND User ID ungleich Admin
- Unix: Login mit „root“
- …

ISACA Germany Chapter

Und worin liegt jetzt das Dilemma?



Unternehmen X will Security Monitoring umsetzen, weil

- es muss (Gesetze wie ITSiG) erfüllen
- es das aufgrund seiner Bedrohungslage sinnvoll findet (Angreifer)
- es andere Gründe hat (Forderungen von Partnern, Produktbezug etc.)

→ Es beauftragt IT, das zu tun.

ISACA Germany Chapter

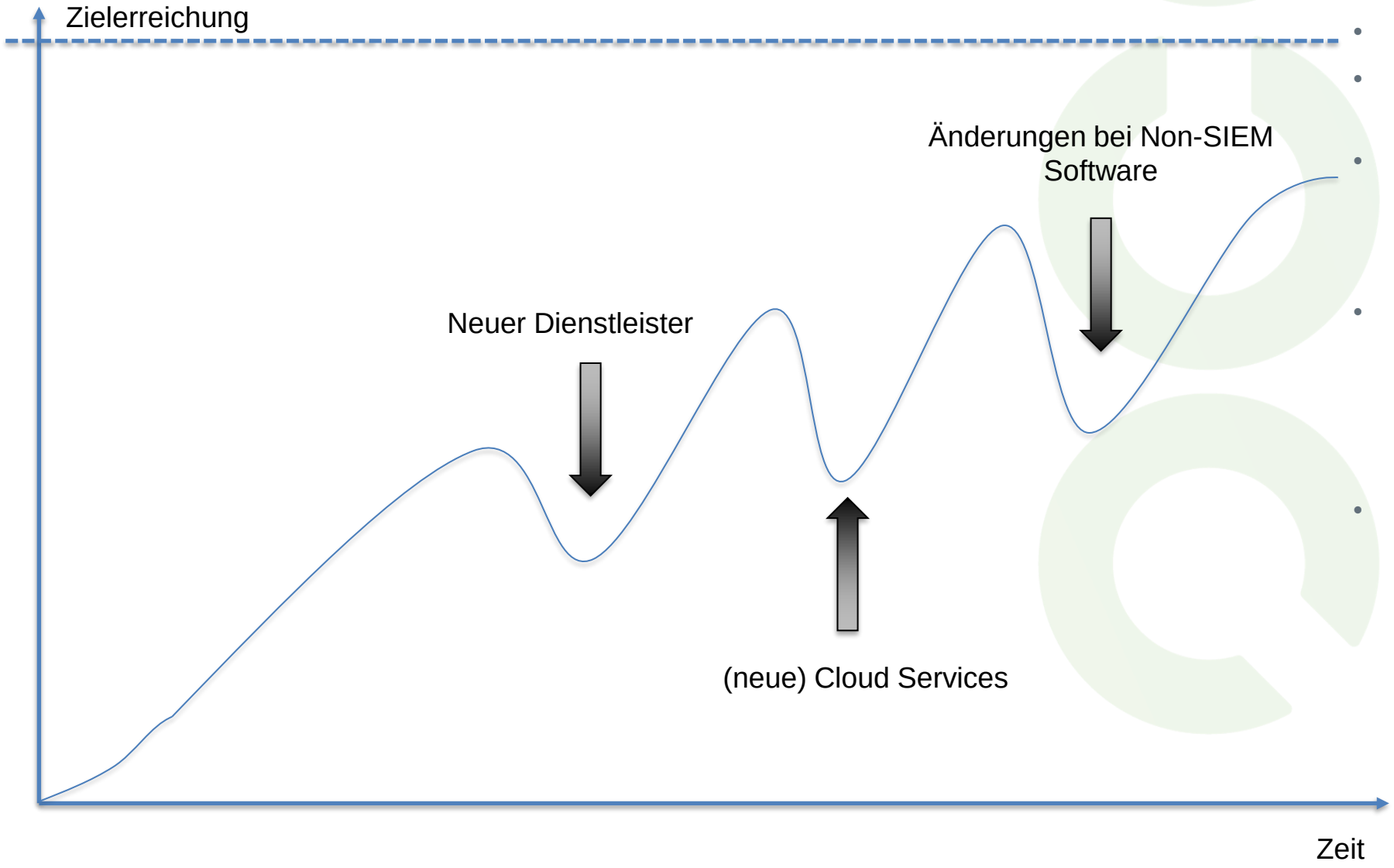
Herausforderungen wachsen

- IT schaut sich seine Software und Infrastruktur an
- Feststellung: u Versionen von v Paketen, x Dienstleister und y Clouds…
- Prüft geeignete Software, Betriebsmodelle etc. Entscheidung wird getroffen

→ Vorgehen benötigt Monate... oder Jahre?

ISACA Germany Chapter

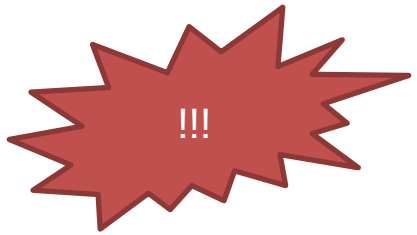
Umsetzung verläuft nicht nach Plan



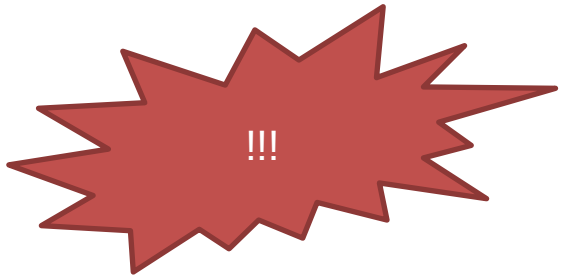
- Implementierung beginnt.
- Geeignetes Fachpersonal schwer zu finden
- Anpassungen:
  - Änderungen an Software
  - ein Dienstleister wird gewechselt
  - eine neue Cloud kommt hinzu…
- Dies führt zu
  - ständigen Nachbesserungen
  - steigenden Kosten
  - externe Experten gehen
- Das gesteckte Ziel wird nicht erreicht, aber man hat eine Basis.

ISACA Germany Chapter

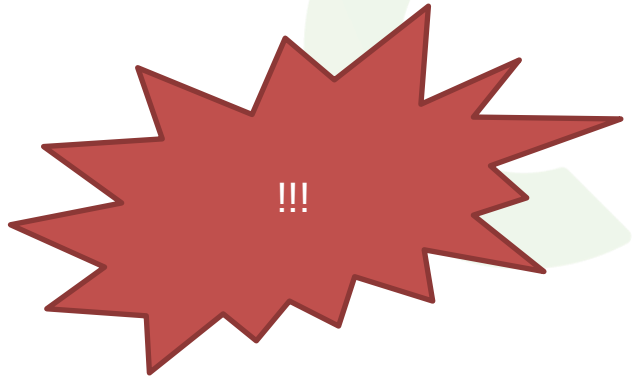
Ein Jahr später...



- neue Software kam, Prüfung und Anbindung ist aufwändig
- Versionsupdates haben die bisherigen Anbindungen zerschossen
- ein Dienstleister kann auf Shared Assets keinen direkten Datenzugriff ermöglichen, Spezialparser sind erforderlich

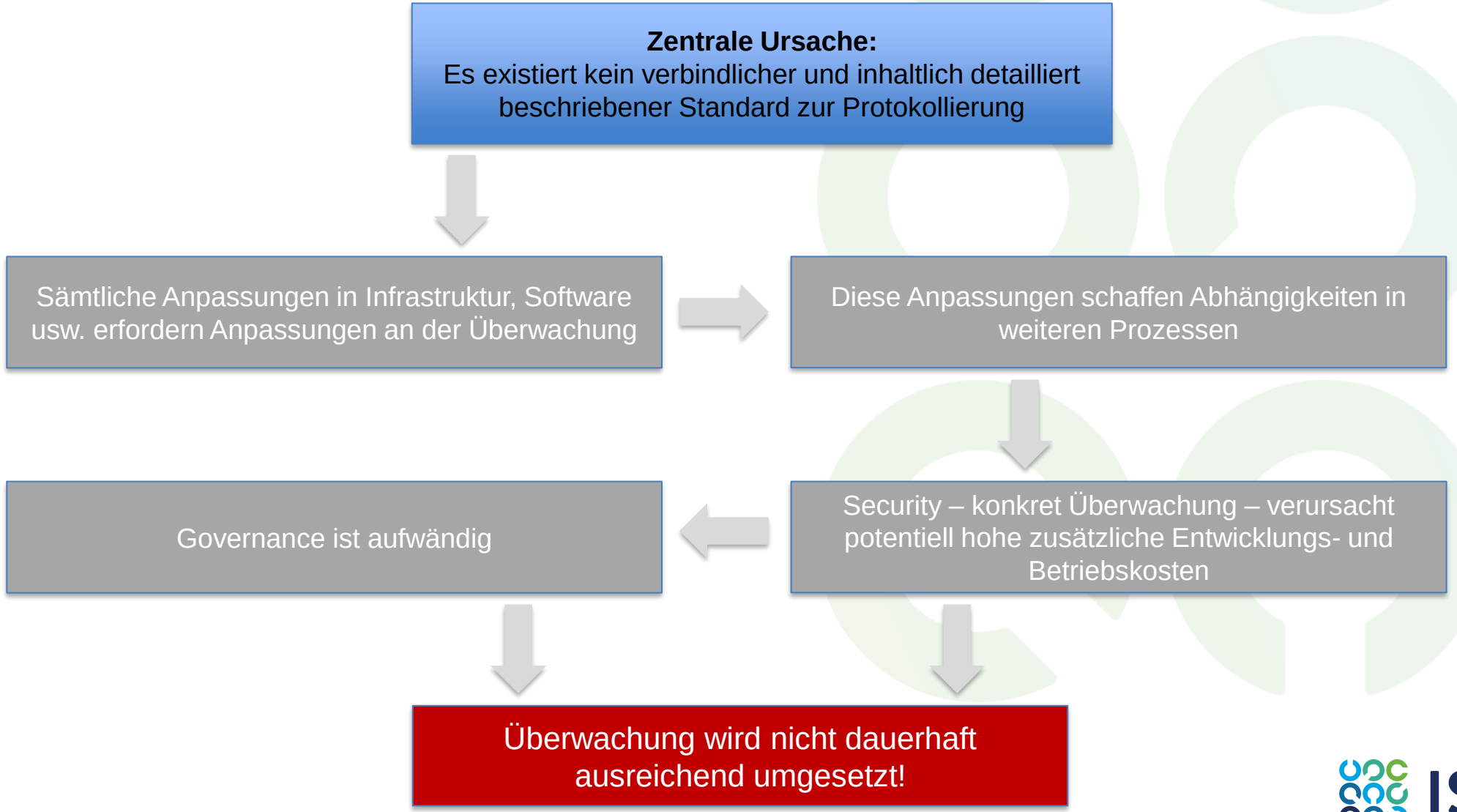


- ausufernde Kosten
- fehlende Experten
- Vertragsverhandlungen und Due Dilligence Prüfungen verzögern sich
- Unzufriedenheit beim Management, Business, IT: "Security behindert den Geschäftsablauf"



ISACA Germany Chapter

Wo ist es schiefgegangen?



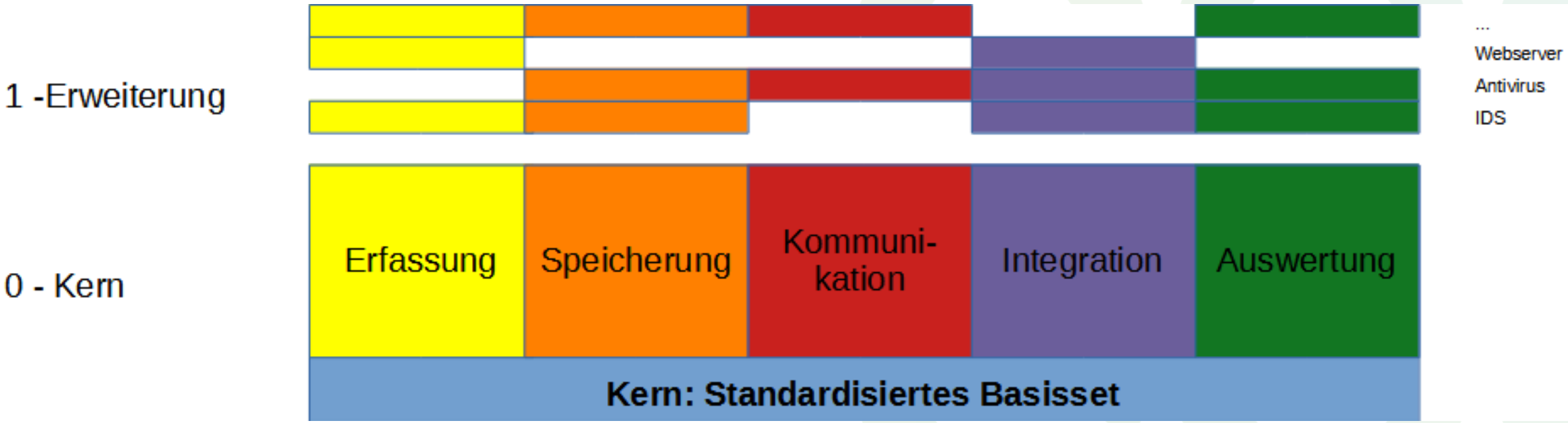
ISACA Germany Chapter

Was ist eine Lösung? Schaffung eines Standards!

Komponenten der Norm	Beschreibung
Erhebung: Spezifizierte Erfassung	Was in welchem Detailgrad von welcher Art von Software aufgezeichnet werden soll
Speicherung: Spezifiziertes Logformat	Wie es aufgezeichnet werden soll – Formate, Kodierung, Inhalte, Integrität etc.
Kommunikation: Spezifizierte Übertragungsmechanismen	Wie die Logs zum Auswertungsort gelangen
Integration: komplexe Unternehmensstrukturen	Wie Logs bei Auslagerungen dennoch einheitlich von Dienstleistern bereitgestellt werden können
Auswertung: Standardisierte Use Cases	Einheitliche Regelwerke, die auf Basis der standardisierten Logs ausgewertet werden können
Rahmen: Erfüllung von gesetzlichen und regulatorischen Anforderungen und Best Practices	Beachtung bei der Spezifikation der Norm

ISACA Germany Chapter

So könnte der Standard aussehen:



ISACA Germany Chapter

Gibt es das nicht schon?

Verschiedene Ansätze existieren:

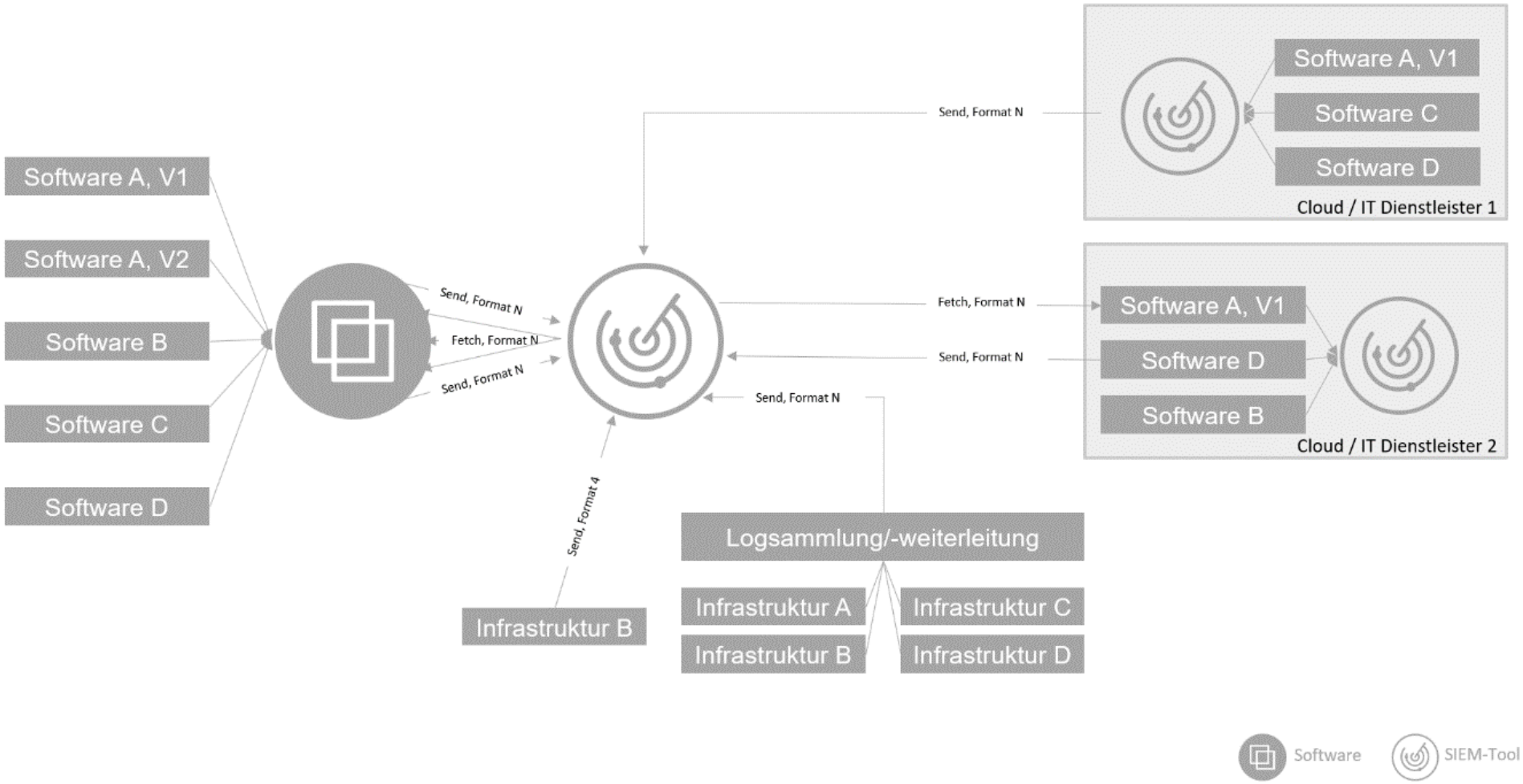
- CEF
- JSON
- SIGMA
- OCSF
- ...

Leider ist keiner davon heute geeignet, da sie…

- … rein auf Formate abzielen, aber keine Inhalte beschreiben
- … auf bestimmte Produkte eingeschränkt sind
- … keine konkreten Implementierungsanforderungen vorgeben

ISACA Germany Chapter

So funktioniert dann das SIEM der Zukunft:



Einheitliche Logs und Formate!

ISACA Germany Chapter

Wie kommen wir zu der Lösung?

Zusammenarbeit:

ISACA Germany Chapter

bitkom

INTERNATIONAL DATA SPACES ASSOCIATION

Bundesamt für Sicherheit in der Informationstechnik

VDMA

Allianz für Cyber-Sicherheit Multiplikator

TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V. IT Security Association Germany

ZVEI: Die Elektroindustrie

ISACA Germany Chapter

ISACA®

Germany Chapter