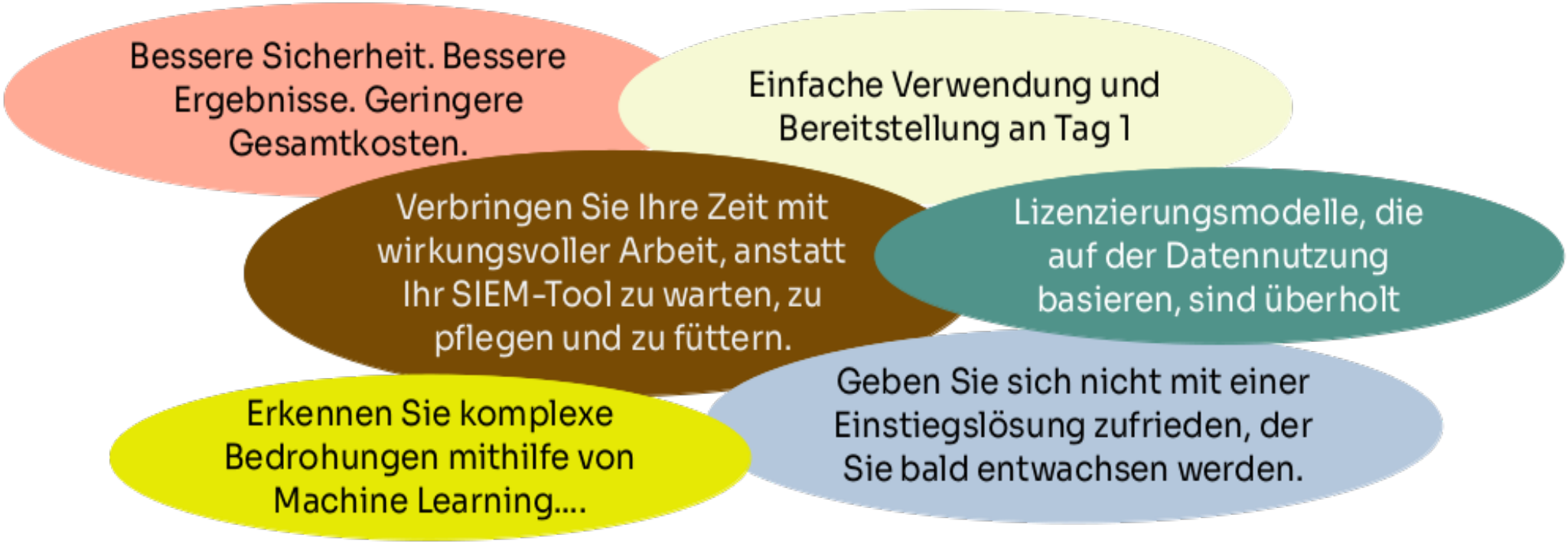
heinlein

23.05.2023 / Torsten Lange

SIEM

„Ich sehe was, was du nicht siehst!“

Was der Markt verspricht …



* Werbeaussagen von vier SIEM Herstellern

Die Realität aus Kundensicht sieht leider so aus …

* Erfahrungen aus dem IT-Sec Consulting

Aber, erst mal der Reihe nach!

SIEM:
Security Information and
Event Management System

Die grundlegenden Funktionen sind

- Normalisieren von Protokolldaten
- Speichern von Protokollinformationen (mit Sicherheitsbezug) aus unterschiedlichen Quellen
- Korrelieren von Informationen
- Detektieren von Regelverstößen
- Alarmieren, wenn gegen Regeln verstoßen wird

Wer sagt, dass wir das brauchen?

Mögliche Anforderungen aus:

- Richtlinien und Rechtsvorschriften
  - BSI IT-Grundschutz, Baustein DER
  - BSI-KritisV
  - Datenschutz, TOMs
  - Branchenspezifische Vorgaben
- Organisatorische Vorgaben
  - IT-Leitlinie der Institution
  - Verträge mit Geschäftspartnern und
  - sonstige Verpflichtungen ggü. Dritten
  - Meldeketten (IT-Sicherheitsvorfall)

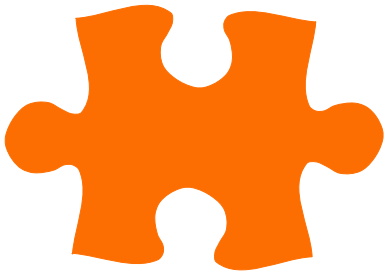
Haben wir einen Plan?

Vorüberlegungen zum SIEM - Einsatz:

- Was verlangen Richtlinien und Vorschriften?
- Was müssen oder wollen wir damit erreichen?
- Art des Systems: On-Prem, Cloud, Hybrid?
- Lizenzmodell: proprietär vs. Open Source
- Wer muss mit ins Boot? (Stakeholder)
- Wie hoch ist das Budget für die Einführung?
- Wie hoch ist das Budget für den Betrieb?
- Ist eine Beschaffung für uns möglich?
- Ist „Managed Security Service“ die Lösung?

Der Plan wird konkret, im Konzept. 1/4

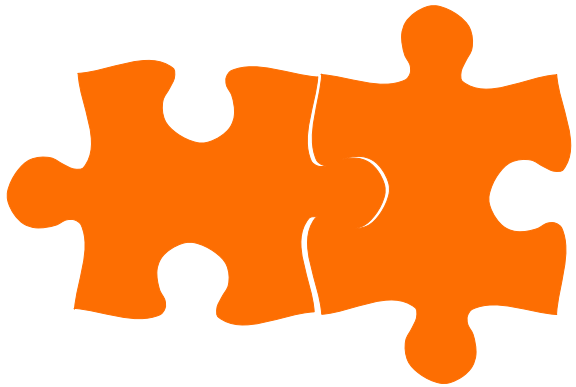
SIEM-Konzept entwickeln:



- Das Vorhaben beschreiben. Worum geht es?
- Bezug auf Richtlinien und Vorschriften nehmen.
- Was sind mögliche Bedrohungsszenarien?
- Scope des SIEM festlegen. Abgrenzen!
- Architektur skizzieren und Zielbild zeichnen.
- Die Organisation um das SIEM:
  - Rollen- und Verantwortlichkeiten festlegen
  - Prozesse beschreiben oder einbinden
  - Kennzahlen festlegen. Stichwort „Reifegrad“

Der Plan wird konkret, im Konzept. 2/4

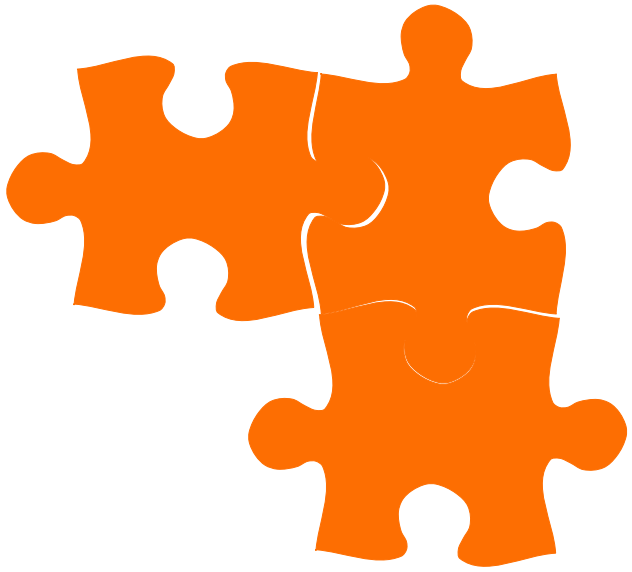
SIEM-Konzept entwickeln:



- Eine Risikoanalyse gehört zur Wahrheit dazu.
  - Risiken, die aus dem Betrieb des SIEM entstehen
  - Risiken aus technischer- , organisatorischer- und rechtlicher Sicht betrachten
  - Als Matrix sehr übersichtlich darstellbar
- Das Thema Datenschutz gehört dazu!
  - Berechtigtes Interesse (Art. 6, Abs. 1 DSGVO)
  - Datenschutzfolgeabschätzung (DSFA)
  - Pseudonymisierung und Vieraugen-Prinzip

Der Plan wird konkret, im Konzept. 3/4

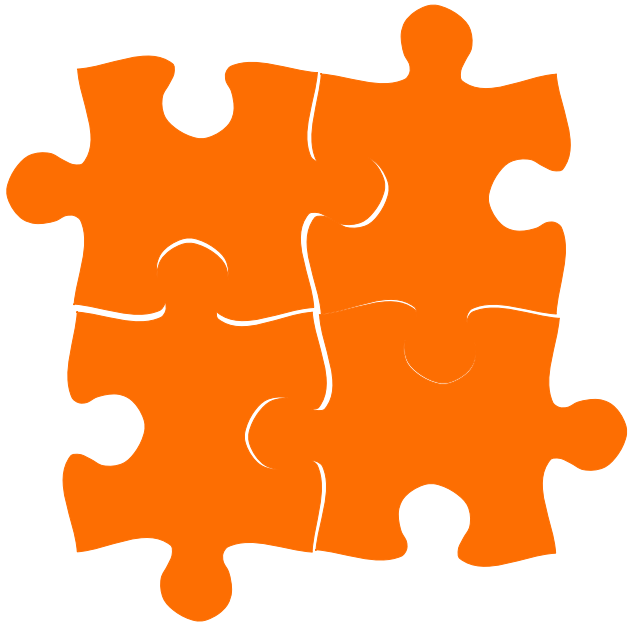
SIEM-Konzept entwickeln:

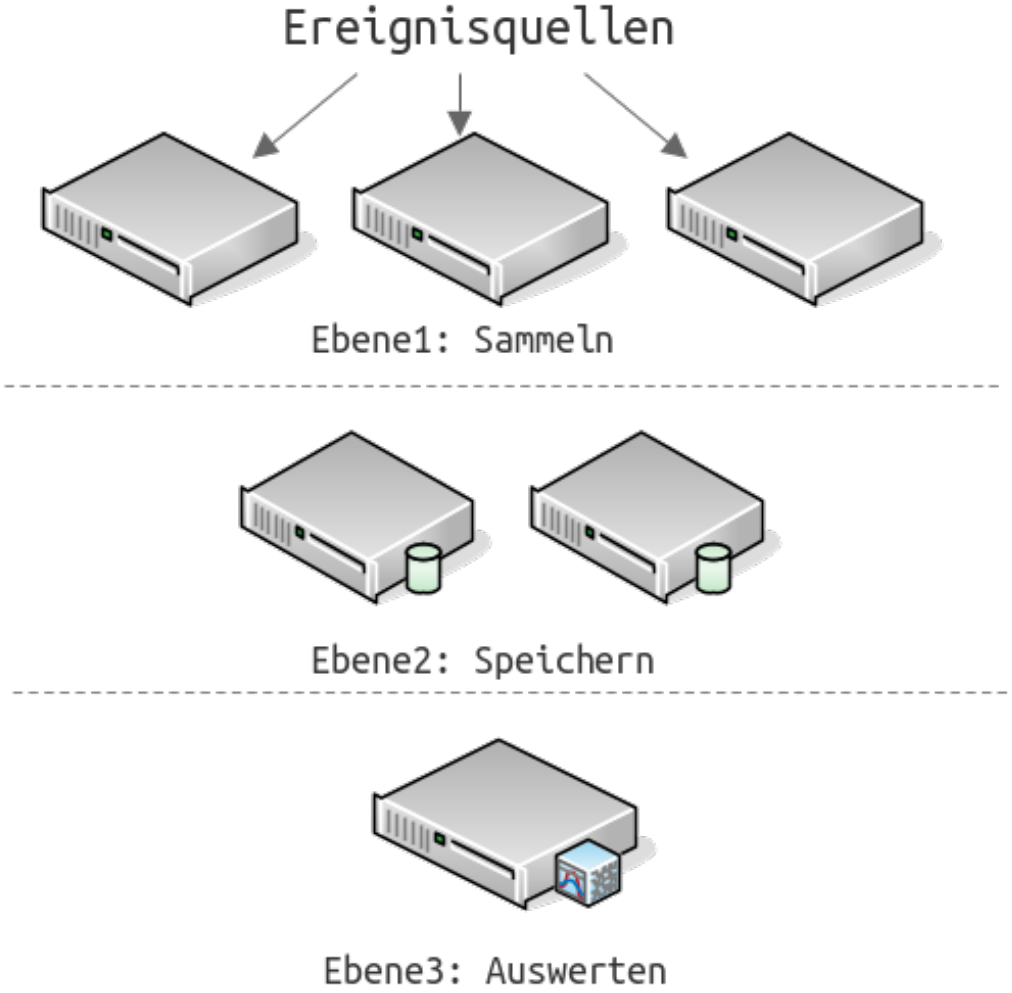


- Use Cases erstellen
  - Was soll das SIEM in welchem Fall tun?
  - Welche Rollen müssen eingebunden werden?
  - Welche Ereignisquellen senden zum SIEM?
  - Welche Datenfelder werden ausgewertet?
  - Wann soll alarmiert werden? (Schwellwerte)
- Mit wenigen Use Cases beginnen!
  - Ereignisquellen gruppieren
  - Der Reihe nach Implementieren und Testen, aber nicht alles gleichzeitig

Der Plan wird konkret, im Konzept. 4/4

SIEM-Konzept entwickeln:





Jetzt wird's technisch. Ereignisquellen

Herausforderung Protokolldaten (Beispiele):

```
2022-08-25 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp 192.168.1.200 source-address
192.168.100.254'
```

```
firewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106100
```

```
Dec 18 12:06:09 gw.lan.intern kernel: fwlog:IN=eth0 OUT= MAC=11:22:33:44:55:66:aa:bb:cc:dd:ee:ff:08:00 SRC=192.0.2.2
DST=198.51.100.8 LEN=40 TOS=0x00     PREC=0x00 TTL=232 ID=12345 PROTO=TCP SPT=54321 DPT=22 WINDOW=1023 RES=0x00 SYN URGP=0
```

```
05/11/2023-15:54:45.208114  [**] [1:2403365:79334] ET CINS Active Threat Intelligence Poor Reputation IP group 66 [**]
[Classification: Misc Attack] [Priority: 2] {TCP} 198.51.100.57:56633 -> 203.0.113.43:80
```

```
<14>1 2022-08-25T16:23:09.264Z fw1 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.35 source-address="192.0.2.10"
source-port="24065" destination-address="198.51.100.8" destination-port="768" service-name="icmp" nat-source-
address="192.0.2.10" nat-source-port="24065" nat-destination-address="198.51.100.8" nat-destination-port="768" src-nat-
rule-name="None" dst-nat-rule-name="None" protocol-id="1" policy-name="icmp-policy" source-zone-name="trust" destination-
zone-name="untrust" session-id-32="100000165" username="N/A" roles="N/A" packet-incoming-interface="reth2.0"
application="UNKNOWN" nested-application="UNKNOWN" encrypted="UNKNOWN"] session created
```

```
<EventID>4648</EventID><EventRecordID>233200</EventRecordID><Desc>A logon was attempted using explicit credentials</Desc>
```

Jetzt wird's technisch. Normalisieren

Datenfelder vereinheitlichen (Beispiele):

Username:

```
User 'root'
User 'enable_15'
username="N/A"
```

Protocol:

```
{TCP}
service-name="icmp"
```

Command:

```
command 'set date ntp…'
executed cmd: show logging mess 106100
```

SRC-IP/SRC-Port/DST_IP/DST-Port:

```
198.51.100.57:56633 -> 203.0.113.43:80
source-address="192.0.2.10" source-port="24065"
destination-address="198.51.100.8" destination-port="768"
```

Jetzt wird's technisch. Das Regelwerk

Informationen auswerten (Beispiele im Pseudocode):

```
If Username == „root“ AND TimeRange(20:00:00-06:00:00)
 Then SIEM-Action(Alert)
EndIf
```

```
If SRC-IP from Feed-Lookup
 Then SIEM-Action(Set-Field:C2-Host=TRUE)
EndIf
```

```
If Command begin-with „delete system login user“
 Then SIEM-Action(Push_Script)
EndIf
```

```
If (Protocol == „TCP“ OR ProtocolID == 6) AND Protocol-Flag == 2
 Then
  If count(5000) per time(5)
   Then SIEM-Action(DOS-Alert)
  EndIf
EndIf
```

- Proprietäre Systeme werden meistens mit einem Basis-Regelwerk ausgeliefert.
- Im Open Source System müsst ihr euch oft selbst um das Regelwerk kümmern.

Jetzt wird's technisch. Feeds

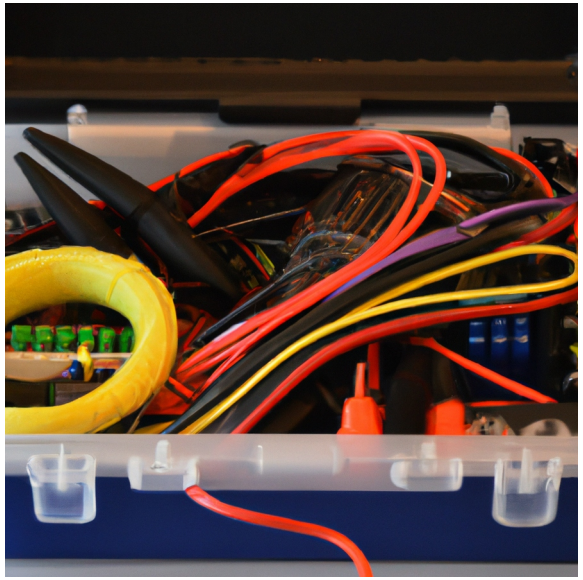
Informationen anreichern:

Grafik: https://www.oasis-open.org

- Feeds einbinden
  - Schnittstellen wie STIX, TAXII, REST-API
  - Lookup-Tables (CSV, Connectors, Tools)
  - „Community“ vs. „Bezahldienst“
- Herausforderungen
  - Risiko: „Fremdquelle“
  - Datenqualität
  - Ärgernis: „Falscher Alarm“

Jetzt wird's technisch. Erweiterungen

Noch lange nicht am Ende:



Grafik: OpenAI Dall-E

- Das SIEM erweitern
  - Einbinden von Agenten auf Endgeräten
  - Verfügbarkeit erhöhen, Last verteilen
  - Dashboards für verschiedene Teams
  - Machine Learning/Deep Learning
- Das SIEM integrieren (Optionen)
  - EDR/XDR/IDS/IPS/Honeypots
  - SOAR
  - ThreatIntel und DFIR
  - SOC/CERT/CSIRT

Was zum Schluss noch wichtig ist.

Dokumentieren:

- Betriebsdokumentation pflegen
  - Ereignisquellen lückenlos erfassen

Wissen erweitern:

- Personal Weiterbilden
- Probealarm erzeugen
  - Funktioniert die Meldekette?
  - Wie lange hat der Durchlauf gedauert

System-Monitoring:

- Systemstatus
  - Alle Ressourcen verfügbar?
  - Zeigen die Trends mögliche Engpässe?
  - Loggen alle Ereignisquellen?

Datum/Uhrzeit:

- Permanenter Abgleich aller Uhrzeiten!

Bleiben wir im Kontakt

Torsten Lange

Tel. +49 30 40 50 51-37
t.lange@heinlein-support.de

Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de