CISO Sprechstunde

02.04.2025

Aktuelles aus der FAU

SIEM (SIEM-DV)

- Die Dienstvereinbarung wurde durch Kanzlerbüro/CISO erstellt und mit GPR final besprochen
- Es folgen noch:
  - Erstellen einer Liste der ersten Server für Loginformationen (ca. 100 Server in Testphase)
  - Datenschutzfolgenabschätzung (DSFA, Risikobetrachtung)

Allg. Informationssicherheitsrichtlinie (IS-RL)

- Erstellung mit Kanzlerbüro erfolgt aktuell (nahezu fertig)
- Danach Vorstellung und Absprache mit GPR

Aktuelles aus der FAU

Handreichung für kritische Länder

- Es entsteht eine Handreichung mit sicherheitsrelevanten Hinweisen und Maßnahmen für Dienstreisen nach

  - China
  - USA

  Wichtig: Vorbereitung, Reisedurchführung, Nachbereitung

- In Abstimmung mit unserer Exportkontrolle

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

SPAM, Phishing Mails @ FAU

Dubiose Mails im Postfach

Beispiel

Von: Joachim Hornegger <officeonline.org581@gmail.com>
Gesendet: Montag, 3. März 2025 14:12
An: CISO (Chief Information Security Officer) <ciso@fau.de>
Betreff: Michael Tielemann

Hello , Are you less busy at the moment? I got a request for you to manage confidentially. I will be into meeting in a few minutes, no calls so kindly respond via email

Joachim Hornegger
President
FAU
Sent by my mail.

Was sind SPAM-Mails?

SPAM-Mails sind unerwünschte oder unerlaubte Massen-E-Mails, die oft zu Werbezwecken oder für betrügerische Zwecke versendet werden. Sie sind meist an eine große Anzahl von Empfängern gerichtet, ohne dass diese zugestimmt haben.

Typische Merkmale von SPAM-Mails:

- **Unpersönliche Anrede** („Sehr geehrter Kunde“ statt deines Namens)
- **Unerwartete Inhalte** (z. B. „Sie haben gewonnen!“ oder „Dringende Zahlung erforderlich“)
- **Verdächtige Links oder Anhänge** (könnten Phishing-Seiten oder Malware enthalten)
- **Schlechte Grammatik & Rechtschreibung** (oft von automatisierten Übersetzungen)
- **Falsche Absenderadresse** (sieht aus wie eine offizielle Adresse, ist aber gefälscht)

SPAM

Frag ChatGPT

Gefahren von SPAM-Mails:

❌ **Phishing:** Betrüger versuchen, deine Passwörter oder Bankdaten zu stehlen
❌ **Malware:** Anhänge oder Links können Viren oder Trojaner enthalten
❌ **Betrug:** Versprechen hohe Gewinne, verlangen aber eine Vorauszahlung

Wie kann man sich schützen?

☑ **Misstrauisch sein** – Öffne keine verdächtigen Anhänge oder Links
☑ **Absender prüfen** – Ist die Adresse wirklich von einer vertrauenswürdigen Quelle?
☑ **Spam-Filter nutzen** – Moderne E-Mail-Dienste erkennen und blockieren viele SPAM-Mails
☑ **Keine persönlichen Daten preisgeben** – Seriöse Unternehmen fragen nicht per E-Mail nach Passwörtern oder Bankdaten

Was sind Phishing-Mails?

Phishing-Mails sind betrügerische E-Mails, die dich dazu bringen sollen, vertrauliche Informationen preiszugeben, z. B. **Passwörter, Kreditkartendaten oder persönliche Daten**.
Sie geben sich oft als seriöse Unternehmen oder Behörden aus.

Typische Merkmale von Phishing-Mails

- **Gefälschte Absenderadresse** („support@paypal-security.com“ statt „@paypal.com“)
- **Dringlichkeit & Druck** („Ihr Konto wird gesperrt, wenn Sie nicht sofort reagieren!“)
- **Links zu gefälschten Webseiten** („Klicken Sie hier, um Ihr Konto zu verifizieren“)
- **Schlechte Grammatik & Rechtschreibung**
- **Unerwartete Anhänge** (könnten Viren oder Trojaner enthalten)

Phishing

Frag ChatGPT

Beispiele für Phishing-Angriffe

- **Bank-Phishing:** E-Mail behauptet, dein Bankkonto sei gesperrt
- **PayPal/Netflix/Apple-Phishing:** Fake-E-Mail fordert dich auf, Zahlungsdaten zu aktualisieren
- **Gefälschte Rechnungen oder Paketzustellungen** (z. B. von „DHL“, „UPS“)
- **CEO-Fraud:** Gibt sich als Chef oder Kollege aus, um Geldüberweisungen zu fordern

Wie kannst du dich schützen?

- ☑ **E-Mail-Adresse genau prüfen** – Sieht die Domain echt aus?
- ☑ **Nicht auf Links klicken** – Besuche die Website lieber direkt im Browser.
- ☑ **Keine Anhänge öffnen** – Vor allem, wenn du nichts erwartest.
- ☑ **Zwei-Faktor-Authentifizierung (2FA) aktivieren** – Selbst wenn ein Passwort gestohlen wird, bleibt dein Konto sicher.

SPAM oder Phishing

Frag ChatGPT

Das klingt verdächtig nach einer **Phishing- oder SPAM-Mail**.
Ein paar Fragen, um das besser einzuschätzen:

- **Wer ist der Absender?**
  Ist die E-Mail-Adresse bekannt oder sieht sie seltsam aus?
- **Wurde dein Name erwähnt?**
  SPAM-Mails nutzen oft nur eine allgemeine Anrede wie „Hallo“ oder „Sehr geehrter Kunde“.
- **Gibt es Druck oder Dringlichkeit?**
  Betrüger setzen oft auf psychologischen Druck („Sofort reagieren“).
- **Erwartest du diese Nachricht?**
  Wenn nicht, sei vorsichtig.

Von: Joachim Hornegger <officeonline.org581@gmail.com>
Gesendet: Montag, 3. März 2025 14:12
An: CISO (Chief Information Security Officer) <ciso@fau.de>
Betreff: Michael Tielemann

Hello , Are you less busy at the moment? I got a request for you to manage confidentially. I will be into meeting in a few minutes, no calls so kindly respond via email

Joachim Hornegger
President
FAU
Sent by my mail.

SPAM oder Phishing

Frag ChatGPT

Was tun?

- ☑ **Nicht antworten** – Warte ab und überprüfe die Echtheit des Absenders.
- ☑ **Keine Links oder Anhänge öffnen** – Sie könnten Schadsoftware enthalten.
- ☑ **Beim Absender direkt nachfragen** – Falls die Mail von jemandem zu kommen scheint, den du kennst, kontaktiere ihn über einen anderen Weg.
- ☑ **Spam melden und löschen** – Falls verdächtig, markiere die Mail als SPAM.

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Anzeige bei der Polizei

Cyberangriff

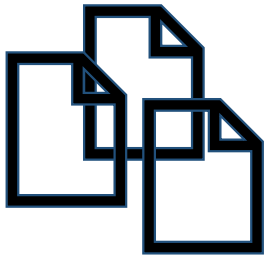
Anzeige bei der Polizei

Intentionelly left blank

Security-Information-and-Event-Management-System (SIEM)

Ein Schutzschirm für die FAU

SIEM
Übersicht



Logdaten

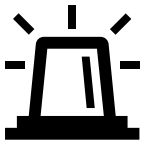
SIEM

- Automatisiertes Monitoring und Analyse von Logdaten

- Erkennung von Anomalien
- Lernen aus Vergangenheit

- Einbeziehen der neusten Attacken und Entwicklungen

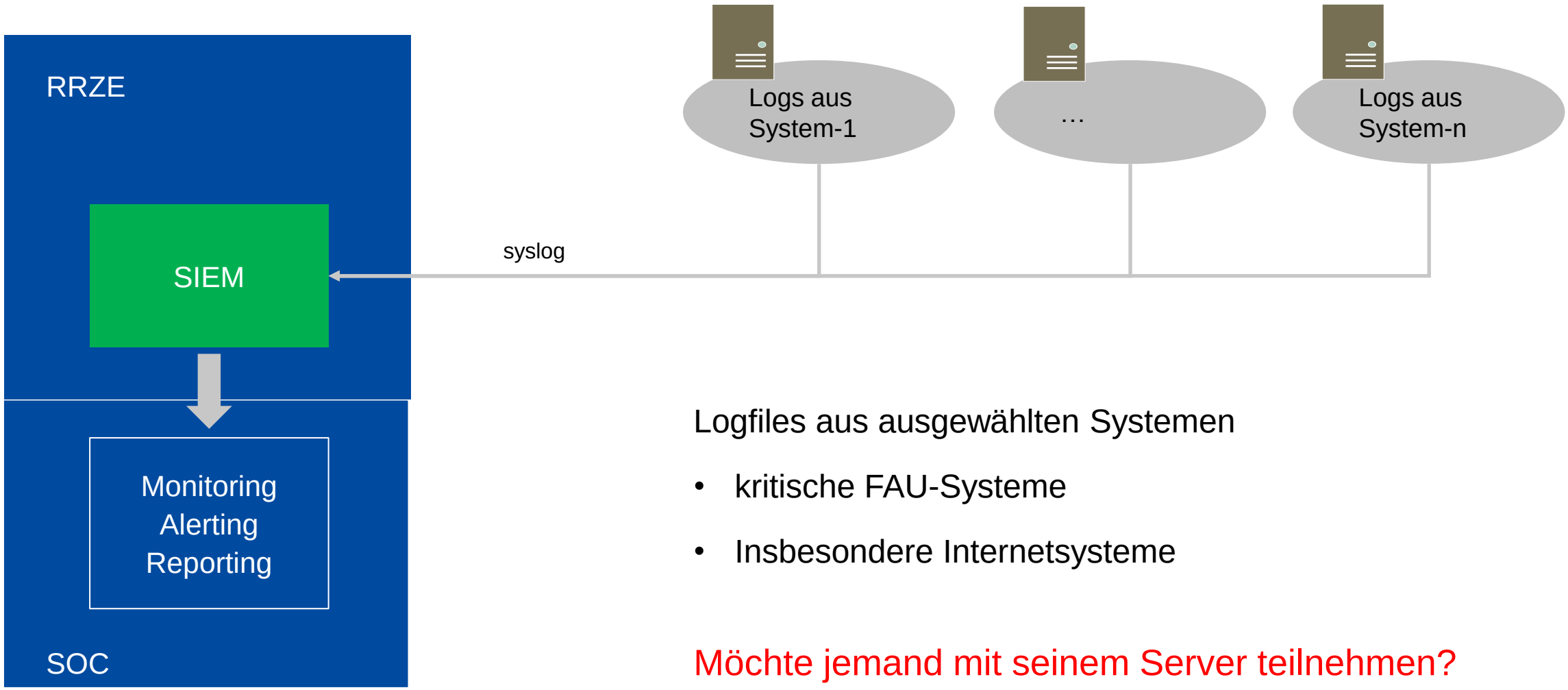
Identifizierung von potentiellen Gefahren in Echtzeit



Alarmierung

- Frühzeitige Erkennung und Reaktion auf potentielle Gefahren vor dem Auftritt des Schadensereignisses
- Gewährleistung der Informationssicherheit nach neustem Stand der Technik
- Absicherung der Geschäftsprozesse

SIEM
Architektur



Logfiles aus ausgewählten Systemen

- kritische FAU-Systeme
- Insbesondere Internetsysteme

Möchte jemand mit seinem Server teilnehmen?

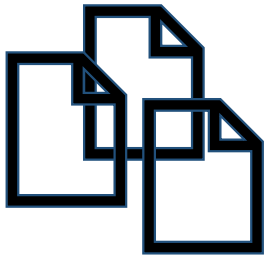
SIEM
Analyseschritte

SIEM Analysetechniken:

1. **Statistische Anomalieerkennung:** Erkennt „Abweichungen vom Normal“
2. **Korrelationsanalyse**: Erkennt Beziehungen zwischen verschiedenen Ereignissen und Datenpunkten, um komplexe Angriffsmuster zu erkennen, die in einzelnen Ereignissen nicht erkennbar sind
3. **Regelbasierte Analyse**: Identifiziert und bewertet ob Aktivitäten gefährlich sind
4. **Machine Learning**: Priorisiert und erlernt neue Bedrohungen (Abweichungen vom Normal)
5. **Indikatoren von bekannten Kompromittierung (IoCs) werden berücksichtigt**

Grundsätzlich wird das SIEM keine Kenntnisse von Inhalten der Kommunikation erlangen

IDS
Übersicht



Netzwerkdaten

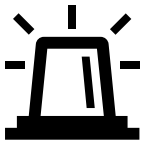
IDS

- Automatisierte Logdatenauswertung

- Erkennung von Anomalien
- Lernen aus Vergangenheit

- Einbeziehen der neusten Attacken und Entwicklungen

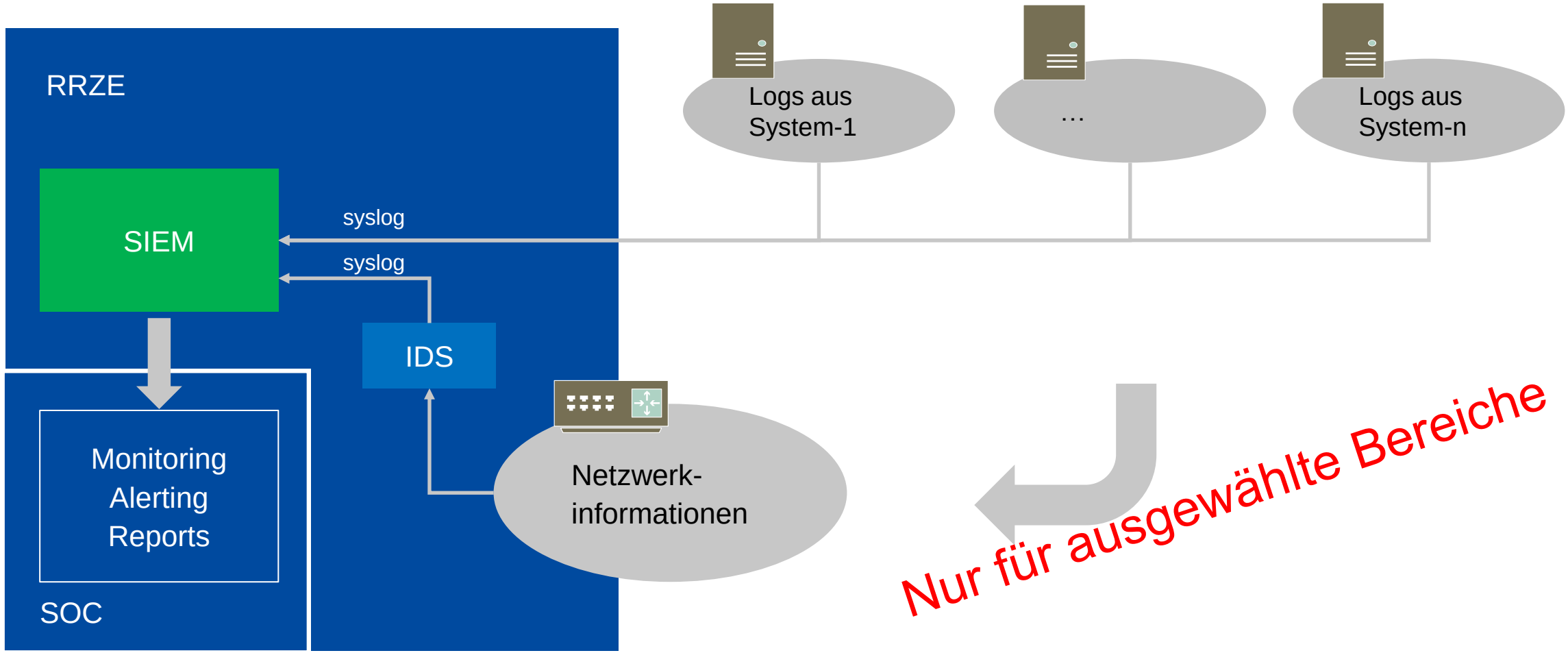
Identifizierung von potentiellen Gefahren in Echtzeit



Alarmierung

- Frühzeitige Erkennung und Reaktion auf potentielle Gefahren vor dem Auftritt des Schadensereignisses
- Gewährleistung der Informationssicherheit nach neustem Stand der Technik
- Absicherung der Geschäftsprozesse

SIEM mit IDS
Architektur



Intrusion Detection System (IDS)
Analyse

Analyseansätze:

1. **Statistische Anomalieerkennung**: Erkennt Abweichung vom Normal (Vergleich mit historischen Daten)
2. **Signaturbasierte Erkennung**: Erkennt im eingehenden Netzwerkverkehr, ähnlich eines Virenscanners, durch bekannte Angriffsmuster und Signaturen
3. **Regelbasierte Erkennung**: Erkennt Verstöße gegen Netzwerkrichtlinien und bewertet Abweichungen im Datenstrom

Das IDS erlangt keine Kenntnisse von Inhalten der Kommunikation

SIEM Dienstvereinbarung

SIEM DV

Ihre Fragen?

Ihre Wünsche?