IT-SIG 2.0

So bleiben Sie auf der sicheren Seite

Manuel Noe
Geschäftsführer IS4IT KRITIS GmbH

IS4IT KRITIS

SO BLEIBEN SIE AUF DER SICHEREN SEITE

Ihre Fragen

Welche **Veränderungen** hat das IT-Sicherheitsgesetz 2.0 bei der Absicherung der kritischen Infrastrukturen gebracht?

Welche wichtigen **technischen Neuerungen** kommen auf mein Unternehmen zu?

Welche sind die **wichtigsten Kriterien** bei der Auswahl einer Angriffserkennung?

Welche Argumente sprechen für die Zusammenarbeit mit einem **Managed-Security-Services-Anbieter**?

IS4IT KRITIS

RISIKEN UND CHANCEN

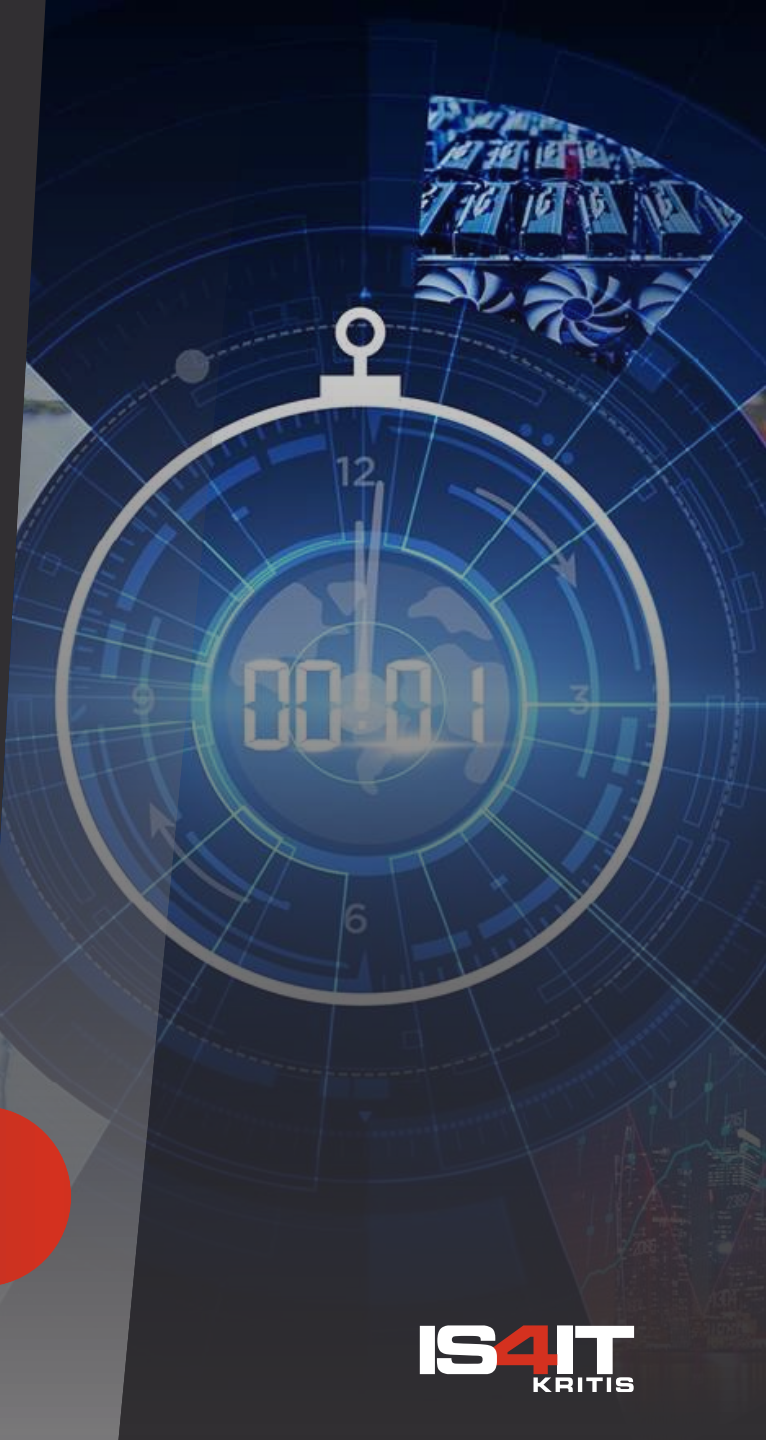
Das bringt das IT-SiG 2.0 mit sich

01 Deutlich höhere
Investitionen in Security

02 Enormer
Zeitdruck in der Umsetzung

03 Notwendiger Schritt, hin zu
mehr (Cyber)Sicherheit

Wer jetzt noch wartet, schafft es nicht bis Mai 2023!



IS4IT KRITIS

DIE ÄNDERUNGEN IM DETAIL

Neufassung und Steigerung der Bußgeldvorschriften

Standardisierter Anforderungskatalog und Prüfleitfaden

Stärkere Vorsorgepflichten

Angepasste Schwellenwerte

Mehr Branchen betroffen

Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI)

INTRUSION DETECTION IST UNVERZICHTBAR

Wesentliche technische Neuerungen

Lösungsansatz Angriffserkennung

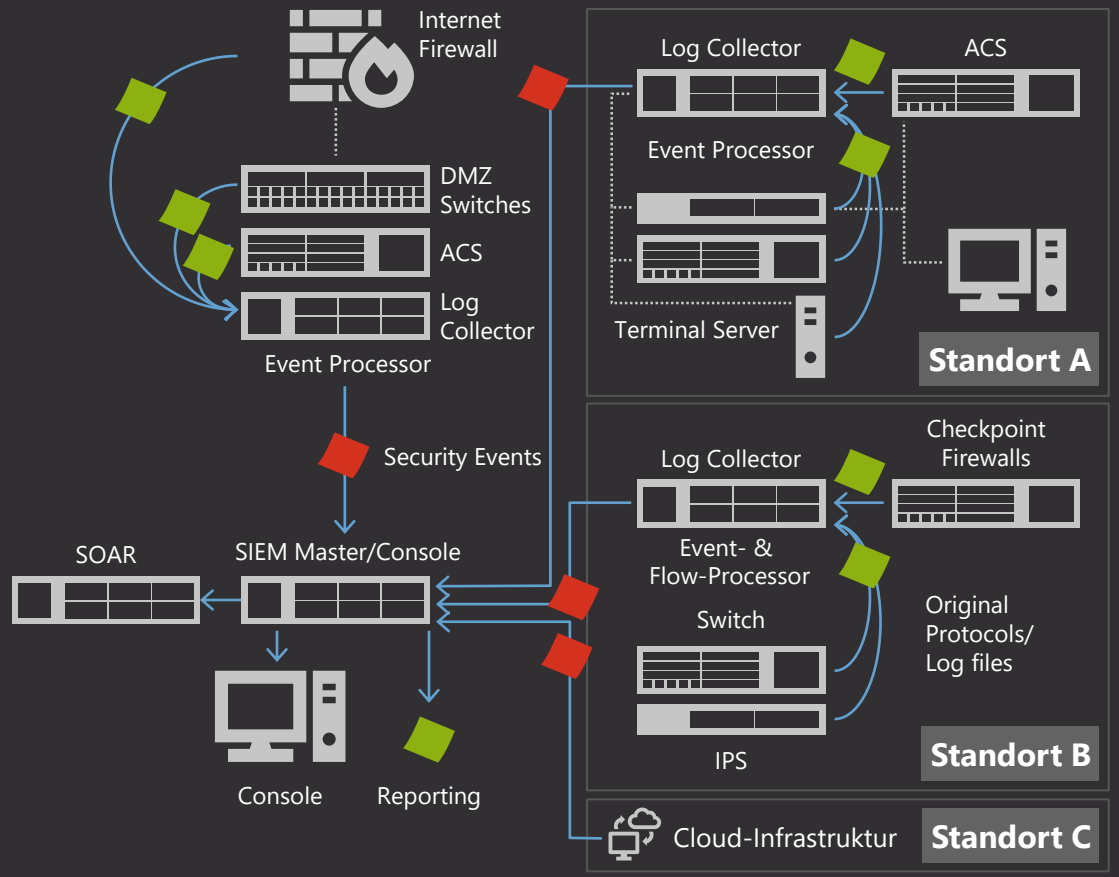
01 Security Information and Event Management (SIEM)

02 Security Operations Center (SOC)

IS4IT KRITIS

EIGENBETRIEB – FUNKTIONSPRINZIP

Erfassung und Korrelation von Daten



- SIEM besteht aus verschiedenen Komponenten: Event-Prozessor & SIEM-Konsole
- Mehrere Event-Prozessoren, z. B. an verschiedenen Standorten oder in unterschiedlichen Sicherheitszonen
- Korrelation der Log-Events findet in den Prozessoren statt
- Weiterleitung von Security Events (Offenses) an die SIEM-Konsole
- Arbeit mit dem System bzw. dessen Bedienung an der Konsole, Erstellung von Reports

IS4IT KRITIS

LÖSUNGSANSATZ SOC

Die Kommandozentrale für IT-Schutz rund um die Uhr

HERAUSFORDERUNGEN

- Einzellösungen schwer zu überwachen
- Erkenntnisauswertung zeitaufwändig und nur für Silo

VORTEILE SIEM

- Anbindung nahezu aller Logquellen möglich
- Korrelation der Events von allen Logquellen
  → Schaffung der 360-Grad-Sicht
- System erlernt Baseline und meldet Abweichungen

IS4IT KRITIS

WAS MÜSSEN DIE SYSTEME LEISTEN?

Wichtige Kriterien

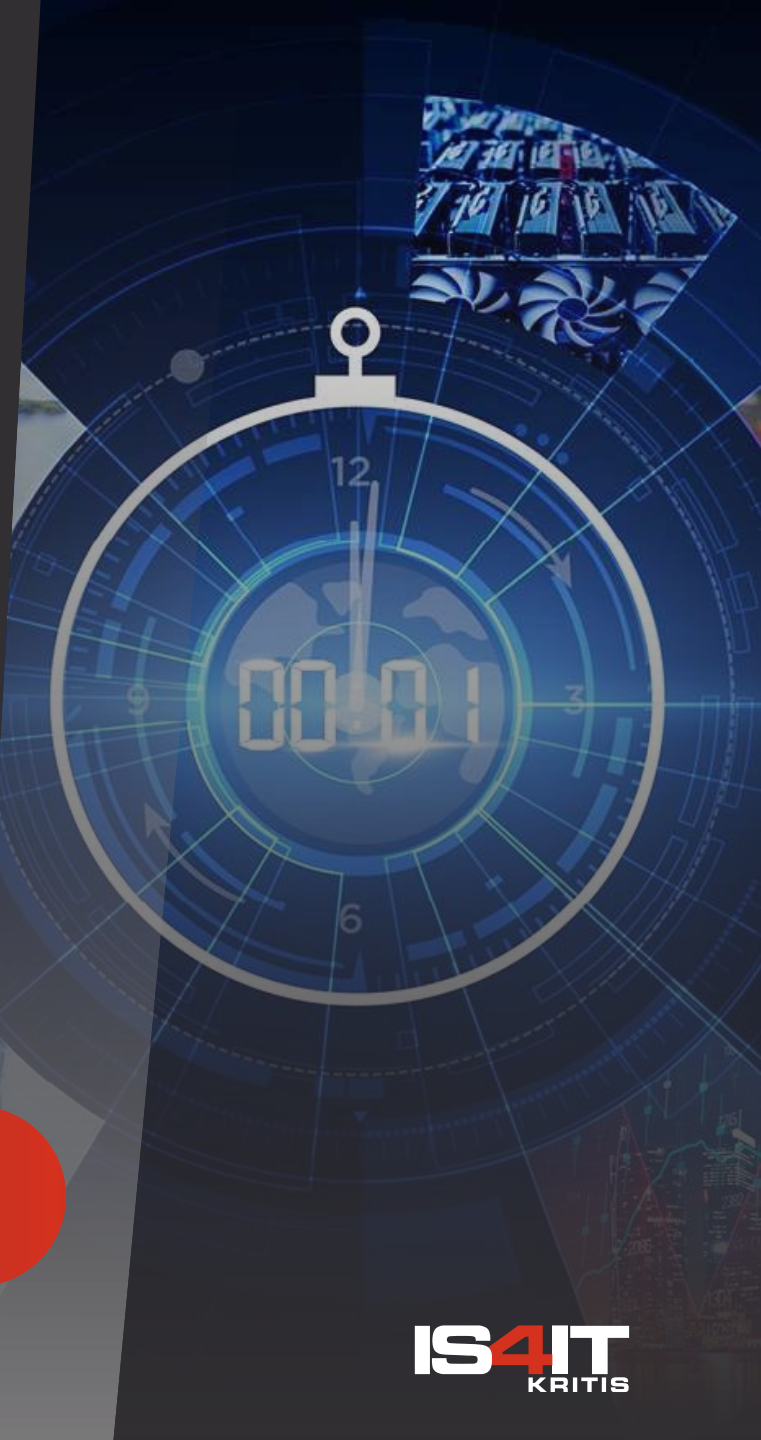
Rechtskonforme Umsetzung der Bereiche

01 Protokollierung

02 Detektion

03 Reaktion

Immer aktuell und auf dem neuesten Stand



IS4IT KRITIS

PROTOKOLLIERUNG

Wichtige Auswahlkriterien bei Planung & Umsetzung

01

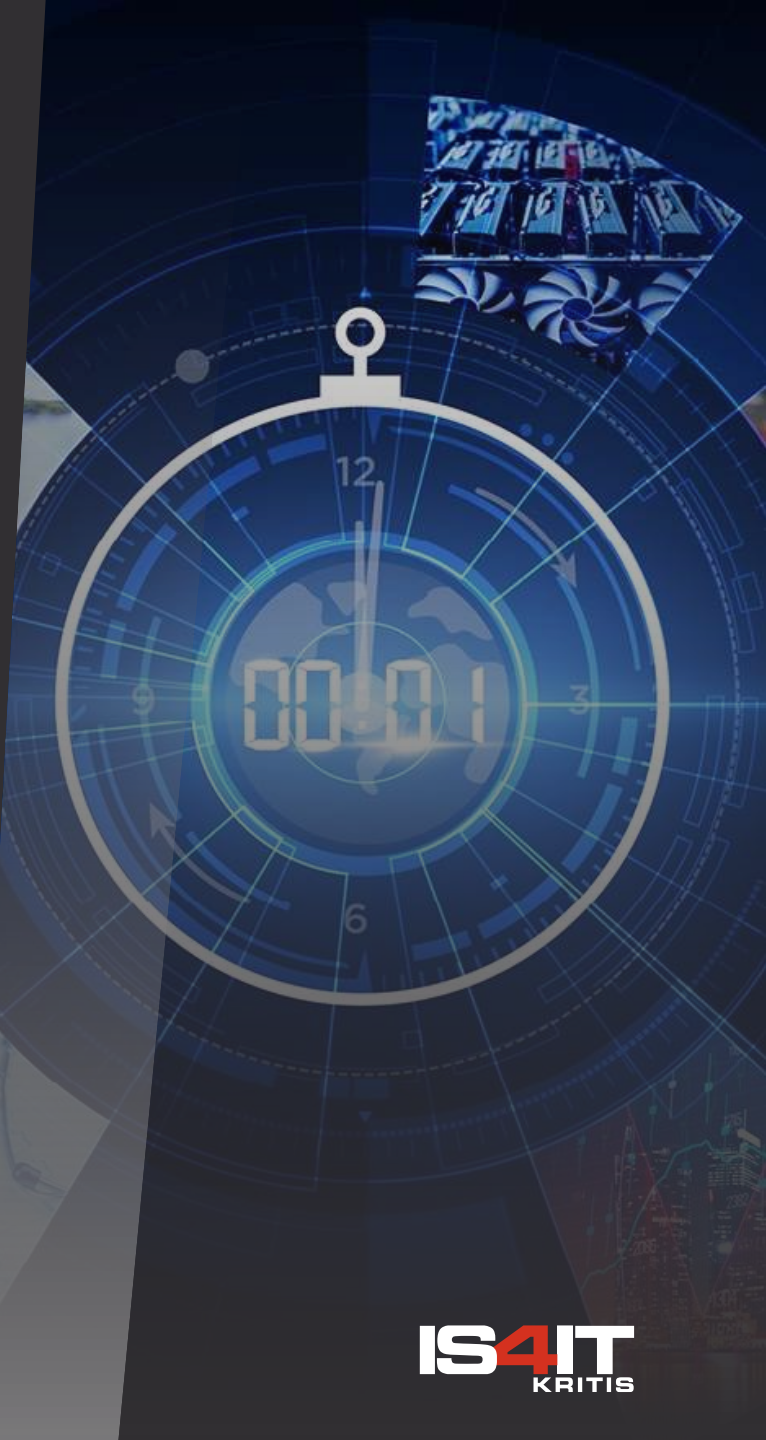
- Bereitstellung aller notwendigen Protokoll- und Protokollierungsdaten
- Bereitstellung der notwendigen Systeme zur Speicherung

02

- Anonymisierung bzw. Pseudonymisierung
- Identifikation aller Systeme
- Aufbau zentralisierter und ausreichend dimensionierter Protokollierungsinfrastrukturen

03

- Prüfung der korrekten Umsetzung der Protokollierungsplanung



IS4IT KRITIS

DETEKTION

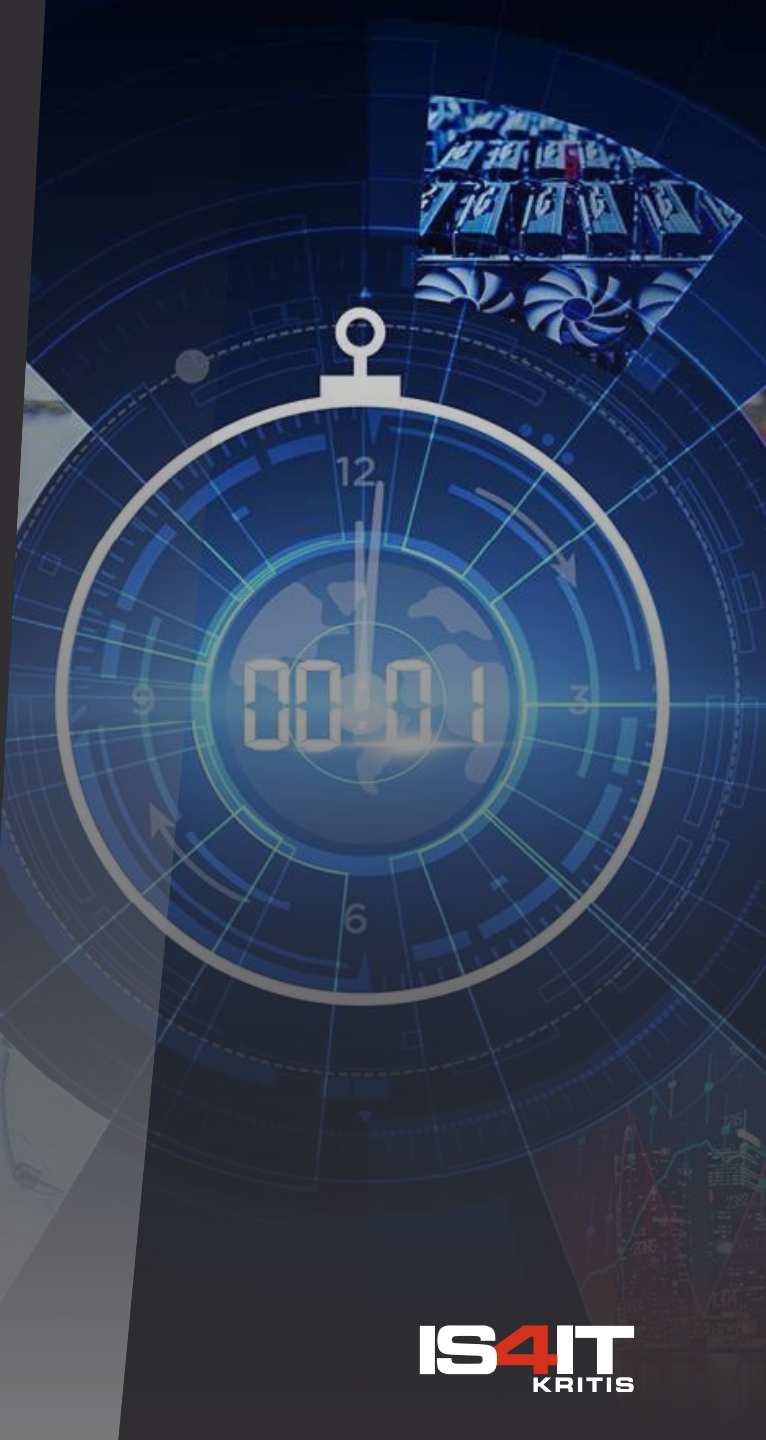
Wichtige Auswahlkriterien bei Planung & Umsetzung

01

02

03

- Umfassende und effiziente Abdeckung der Bedrohungslandschaft für IT und OT
- Gewährleistung der unmittelbaren Alarmierung
- Einsatz dedizierter Mitarbeiter für die Auswertung
- Gewährleistung zentraler Detektion und Echtzeitüberprüfungen
- Berücksichtigung der Meldungen von Herstellern, Behörden, Medien und relevanten Stellen



REAKTION

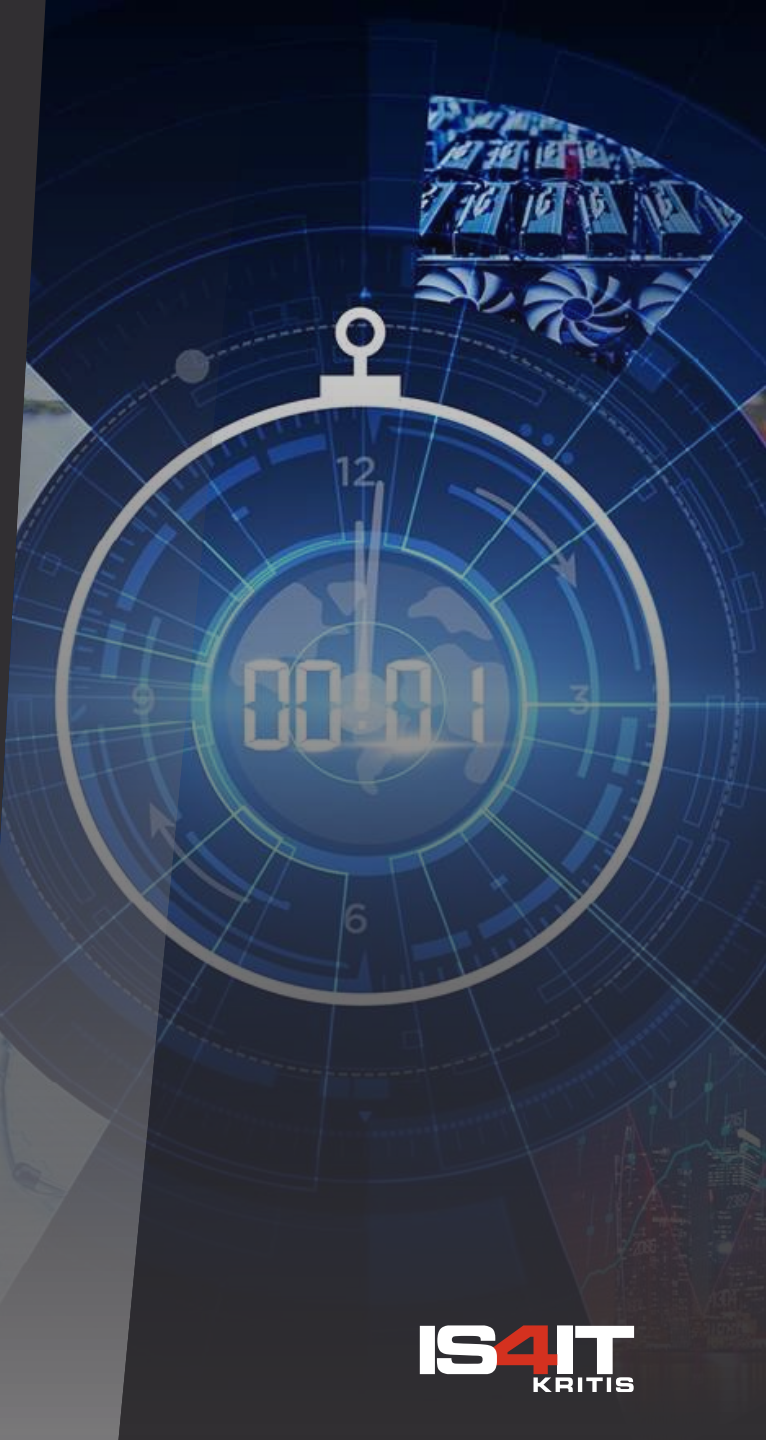
Was tun, wenn ...?

01

02

03

- Automatische Meldung eines sicherheitsrelevanten Ereignisses durch die eingesetzten Detektionssysteme (zwingend notwendig)
- Unterbindung des Sicherheitsvorfalls durch Aktivierung manueller Prozesse und – wenn möglich – Eingriffe in den Datenstrom
- Behandlung festgestellter Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen
- Überprüfung der Meldepflicht an das BSI nach § 8b Absatz 3 BSIG bzw. § 11 Absatz 1c EnWG



IS4IT KRITIS

INTERN ODER EXTERN?

Ihre Herausforderung

Zuverlässige Betriebsabläufe

01 Sind ausreichend kompetente Mitarbeiter verfügbar?

02 Sind diese Experten innerhalb Ihres Betriebs ausgelastet?

03 Können Sie die Security Services 7x24 gewährleisten?

IS4IT KRITIS

INTERN ODER EXTERN?

Outsourcing als Option

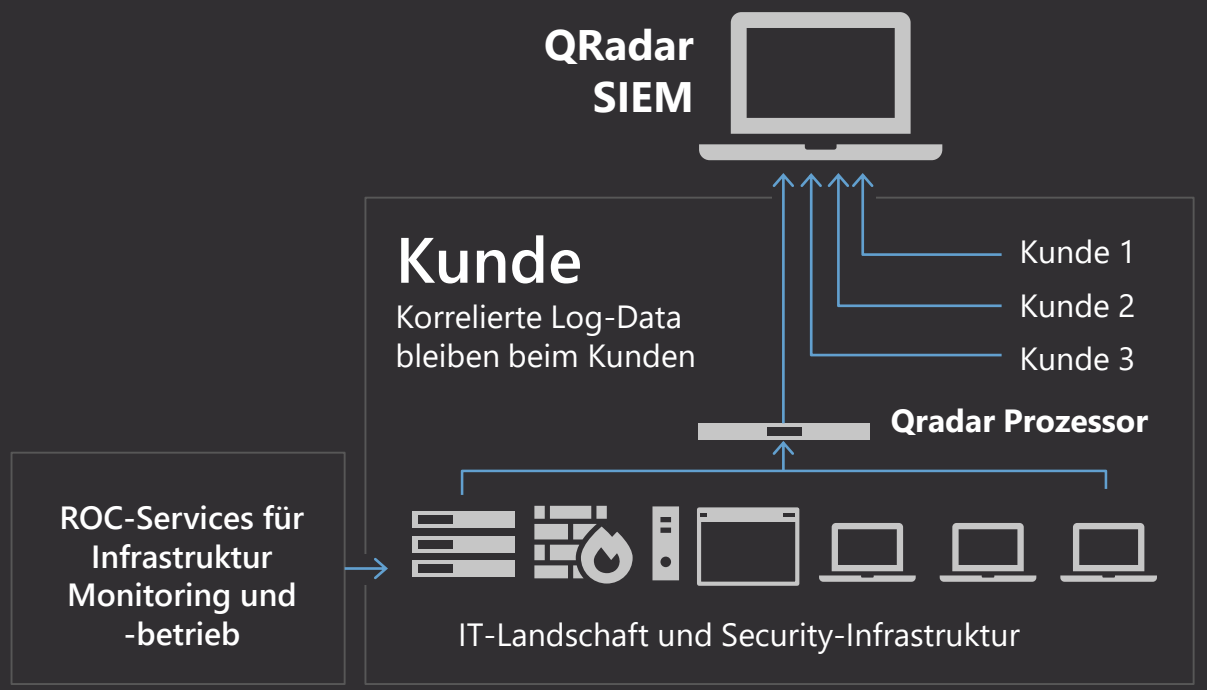
- Keine internen Experten erforderlich, Synergieeffekte durch Monitoring mehrerer Unternehmen, wirtschaftliche Umsetzung von 7x24
- Transparente Kosten – abhängig von Systemen, Geräten und SLAs
- Verantwortung des Partners von der Beratung über die Umsetzung bis zum Betrieb
- Minimierung des Risikos von wirtschaftlichen Folgen aus Cyberattacken
- Definierter Leistungsumfang & definierte SLAs – inkl. Pönale

IS4IT KRITIS

INTERN ODER EXTERN

Managed Security Operations Center – Managed SIEM Service

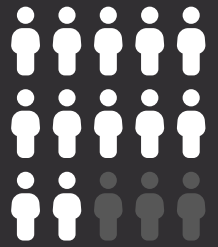
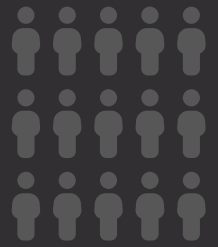
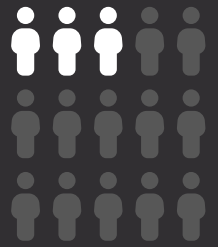
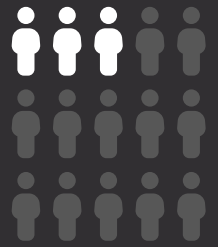
Managed SIEM Service

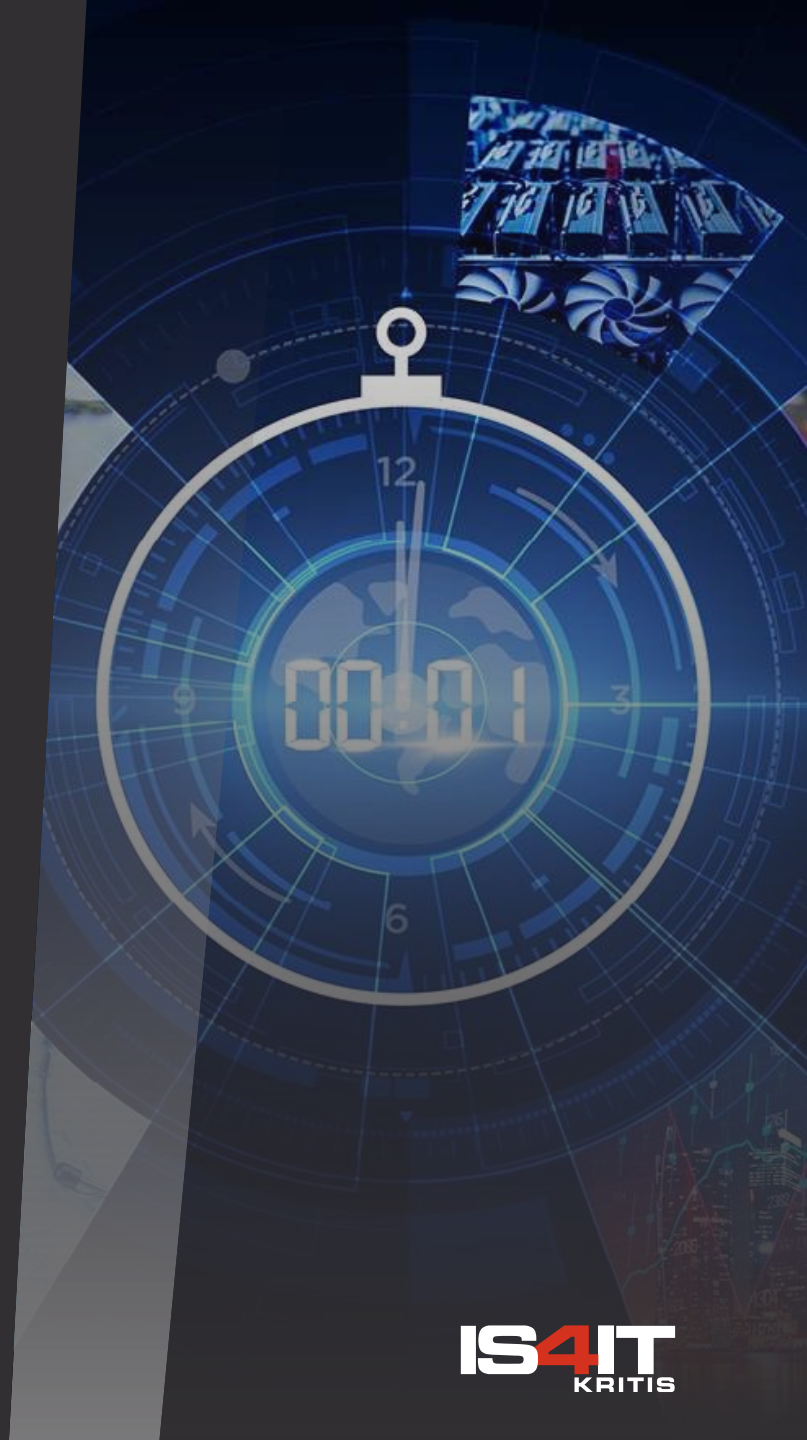


- Architektur für mehrere Standorte
- Zentrale SIEM-Konsole im RZ der IS4IT
- Event- und Flow-Prozessoren
  im Rechenzentrum des Kunden
- IT-Systeme des Kunden (Netzwerkkomponenten, Server, andere) senden ihre Logfiles an die Prozessoren des zugeordneten RZ, welche die Logfiles verarbeiten (korrelieren)
- Bei der Verarbeitung gefundene Vorfälle (Offenses) werden an die zentrale SIEM-Konsole geschickt
- Die Security-Analysten haben mittels der Konsole Zugriff auf die SIEM-Prozessoren in den Kunden-RZ und können sich bei Bedarf mehr detaillierte Informationen holen
- Alarmierung der Verantwortlichen des
  Kunden bei kritischen Vorfällen
- Original-Logdateien verbleiben am Kundenstandort

INTERN ODER EXTERN?

Ressourcen im Vergleich

PERSONAL-BEDARF	EIGEN-BETRIEB	MANAGED SERVICES
Analysten		
SecOps		



IS4IT KRITIS

DARUM IBM & IS4IT KRITIS

Ihr Team für kritische Infrastruktur

Silver Business Partner

IBM QRADAR – SIEM

Vollständiger Überblick über alle Sicherheitsdaten in einem einzigen Fenster

Ereignisse reduziert auf eine nach Prioritäten geordnete Liste der wichtigsten Warnungen

Automatisierte, erweiterte Analysen und Bedrohungsdaten verkürzen Untersuchungszeit

Schnelle Skalierbarkeit mit vordefinierten Anwendungsfällen und Integrationen

12 x führend bei Gartner, 3 x führend bei Forrester Wave, „Best value for Price“ bei den TrustRadius 2022 Summer Awards

IS4IT KRITIS – SOC & MANAGED SECURITY SERVICES

Erfolgreiche erste wesentliche Auslagerung eines **SOC-Services nach Atomgesetz, Änderungsverfahren der Kat. B** in Europa

Etablierung eines neues SOC für das **Landesamt für Sicherheit in der Informationstechnik** Bayern

Offizieller **Partner der IBM** für die Mittelstandsoffensive „Security in Deutschland“

Leistungserbringung und Rechenzentrum 100 % Security „**Made in Germany“**

Serviceerbringung zertifiziert nach **ISO 27001** und **ISO 9001**

ALLES „SICHER“ VERSTANDEN?

Danke für Ihre Aufmerksamkeit

Besuchen Sie uns

Halle 6, Stand 229

Manuel Noe - IS4IT KRITIS

Halle 7, Stand 716

Matthias Sauer - IBM

Silver Business Partner